Berne, le 15 novembre 2023

Révision partielle d'ordonnances d'exécution de la loi sur la surveillance de la correspondance par poste et télécommunication (LSCPT)

Rapport explicatif

Table des matières

1 Contexte 4

2 Procédure préliminaire, notamment procédure de consultation 4

3 Grandes lignes du projet 7

3.1 Modification de l'OSCPT 7

3.2 Modification de l'OEI-SCPT 9

3.3 Modification de l'OME-SCPT 9

3.4 Modification de l'OST-SCPT 9

4 Commentaire des dispositions 10

4.1 Ordonnance sur la surveillance de la correspondance par poste et télécommunication 10

4.2 Ordonnance sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication (OME-SCPT) 57

4.3 Ordonnance sur le système de traitement pour la surveillance de la correspondance par poste et télécommunication (OST-SCPT) 62

5 Conséquences 66

5.1 Conséquences pour la Confédération 66

5.2 Conséquences pour les cantons 66

5.3 Conséquences pour les POC 66

6 Aspects juridiques 67

6.1 Compatibilité avec les obligations internationales de la Suisse 67

6.2 Forme de l’acte à adopter 67

6.3 Sous-délégation de compétences législatives 67

6.4 Protection des données 67

Annexe 67

Tableau « Vue d'ensemble des délais de traitement » 69

1 Contexte 4

2 Procédure préliminaire, notamment procédure de consultation 4

3 Grandes lignes du projet 7

3.1 Modification de l'OSCPT 7

3.2 Modification de l'OEI-SCPT 9

3.3 Modification de l'OME-SCPT 9

3.4 Modification de l'OST-SCPT 9

4 Commentaire des dispositions 10

4.1 Ordonnance sur la surveillance de la correspondance par poste et télécommunication 10

4.2 Ordonnance sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication (OME-SCPT) 57

4.3 Ordonnance sur le système de traitement pour la surveillance de la correspondance par poste et télécommunication (OST-SCPT) 62
5 Conséquences 66
5.1 Conséquences pour la Confédération 66
5.2 Conséquences pour les cantons 66
5.3 Conséquences pour les POC 66
6 Aspects juridiques 67
6.1 Compatibilité avec les obligations internationales de la Suisse 67
6.2 Forme de l'acte à adopter 67
6.3 Sous-délégation de compétences législatives 67
6.4 Protection des données 67
Annexe 67
Tableau « Vue d'ensemble des délais de traitement » 69

1 Contexte

Les ordonnances d'exécution de la LSCPT[1] doivent être révisées pour les motifs suivants :

- À l'occasion de la modification du 22 mars 2019 de la LTC[2], un deuxième alinéa a été ajouté à l'art. 2 de la LSCPT. Ce nouvel alinéa 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 (RO 2020 6159, 6181).
- La technologie 5G exige d'adapter l'OSCPT[3] et des mesures sont nécessaires pour améliorer et assurer de manière générale la fourniture des données. Enfin certaines dispositions de l'OEI-SCPT[4], de l'OME-SCPT[5] et de l'OST-SCPT[6] doivent être adaptées.

Pour ne pas retarder les adaptations rendues nécessaires par la technologie 5G, la révision se fera en deux temps. Le présent volet de la révision ne porte donc pas sur la définition des différentes catégories de POC et leurs obligations respectives. Cette question sera abordée ultérieurement, dans un deuxième volet. La révision totale de l'OEI-SCPT visant à introduire un système de forfaits (cf. art. 38*a* LSCPT, en vigueur depuis le 01.01.2022), est un projet distinct intitulé ordonnance sur le financement de la surveillance de la correspondance par poste et télécommunication (OF-SCPT).

Le projet dont il est question ici adapte l'OSCPT aux progrès technologiques tels que la 5G et l'IP Multimedia Subsystem (IMS, voir ch. 3.1).

2 Procédure préliminaire, notamment procédure de consultation

Une consultation a été menée du 16 février au 23 mai 2022. Le DFJP (Service SCPT) a reçu 70 réponses.

Des avis opposés ont été exprimés : les cantons et les autorités de poursuite pénale ont salué le projet dans son principe, tandis que les organisations de la branche des télécommunications et les POC l'ont fortement critiqué ou, en partie, rejeté. La teneur de ces critiques est que les adaptations ne concernent pas uniquement la 5G, mais que des dispositions sont également modifiées en vue d'une extension de la surveillance

1 Loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (**LSCPT** ; RS **780.1**)
2 Loi du 30 avril 1997 sur les télécommunications (**LTC** ; RS **784.10**)
3 Ordonnance du 15 novembre 2017 sur la surveillance de la correspondance par poste et télécommunication (**OSCPT** ; RS **780.11**)
4 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**)
5 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**)
6 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**)

générale. Ont en particulier été critiqués l'automatisation croissante, le Virtual Private Network (VPN, réseau privé virtuel), l'obligation faite aux fournisseurs de retirer les chiffrements qu'ils ont opérés, l'enregistrement des ports, des adresses IP et d'autres données (considéré comme de la collecte indiscriminée de données à titre préventif)[7], la détermination de la position (LALS), le timbre horodateur, les délais d'exécution raccourcis et les délais de transition trop courts. Ces critiques jugent donc que l'annonce d'une adaptation à l'évolution technologique masquerait en réalité une extension massive des surveillances. Les nouvelles obligations imposées aux entreprises seraient disproportionnées et la sphère privée des utilisateurs, ainsi que la protection des données, seraient mises à mal.

Les points suivants ont été pris en compte lors du remaniement du projet après la consultation :

- Des dispositions ont été adaptées ou même biffées, afin que le travail demandé aux POC par les modifications d'ordonnances (notamment pour l'adaptation des systèmes) soit raisonnable par rapport à l'utilité pour les autorités de poursuite pénale (proportionnalité des modifications).
- Plusieurs participants à la consultation ont critiqué la conservation des numéros de port cibles et des adresses IP cibles, estimant que l'enregistrement de ces données équivaut à une extension de la surveillance, pour laquelle il n'existe pas de base légale et qui est problématique du point de vue de la protection des données. La nouvelle obligation de fournir les ressources d'adressage cibles (NAT cible) est néanmoins reportée au deuxième volet de la révision, pour que les catégories de POC et leurs obligations respectives puissent être introduites en même temps. Dans l'actuel projet, il s'agit d'un renseignement et non d'une surveillance. Les renseignements visés à l'art. 22 LSCPT peuvent aussi s'appuyer sur des données secondaires, s'ils sont nécessaires aux fins d'une identification. Les données secondaires elles-mêmes ne sont pas fournies. Par ailleurs, les fournisseurs sont invités à choisir une procédure dans laquelle les adresses IP et les ports cibles ne sont pas nécessaires à l'identification de l'utilisateur, auquel cas ceux-ci n'ont pas besoin d'être conservés. La LSCPT (en particulier ses art. 21 et 22) constitue une base légale suffisante. Et même s'il s'agissait d'une surveillance, l'art. 269 CPP[8] ne prévoirait pas une telle restriction.
- L'alinéa de l'art. 50 prévoyant que les FSCD ayant des obligations étendues devaient eux aussi supprimer les chiffrements qu'ils avaient opérés a été biffé. L'obligation est maintenue pour les FST, en vertu de l'art. 26, al. 2, let. c, LSCPT.
- Les délais transitoires accordés aux POC pour adapter leurs systèmes ont été prolongés (24 mois à compter de l'entrée en vigueur de l'OSCPT).
- Les émoluments pour les nouveaux types de surveillance visant à déterminer la position ont été légèrement revus à la baisse. L'émolument total dû pour une

7 Concerne les modifications dans les art. 21, 38, 42*a*, 43, 43*a*, 60, 62 et 63 OSCPT.
8 Code de procédure pénale suisse du 5 octobre 2007 (code de procédure pénale, **CPP** ; RS **312.0**)

recherche comprenant le recours à un IMSI-catcher (par ex. pour les recherches en cas d'urgence) a également été réduit (voir ch. 3.2).

Les points suivants n'ont que partiellement pu être pris en compte lors du remaniement du projet après la consultation :

- Les POC et plusieurs partis politiques ont critiqué le fait qu'en plus des adaptations nécessaires pour la 5G, d'autres modifications sont proposées qui constitueraient un développement massif de la surveillance, avec de nouvelles obligations pour les POC. Ont été particulièrement critiqués les données nécessaires à l'identification des usagers, la fourniture automatisée de renseignements, la détermination de la position et les délais de traitement plus courts (sur ces points spécifiquement, nous renvoyons aux explications qui suivent). La réponse que l'on peut apporter à cette critique générale est que les adaptations à la technologie 5G amènent de nouvelles possibilités en termes de surveillance (par ex. la détermination de la position). Les normes ETSI ont d'ailleurs déjà été modifiées en ce sens. Le but des nombreuses modifications dans les différentes ordonnances, et particulièrement dans l'OSCPT, est d'adapter ces actes à l'évolution technologique afin d'éviter que des lacunes n'apparaissent dans les possibilités de surveillance. Les possibilités améliorées de détermination de la position qu'offre la technologie 5G servent également à améliorer la qualité des données de la surveillance. Certaines des adaptations amènent une amélioration de l'identification des utilisateurs sans obligations supplémentaires. Les critiques ont néanmoins été partiellement prises en compte. D'une part, plusieurs dispositions du projet précisent maintenant que les FSCD ayant des obligations étendues ne sont pas concernés par les nouveaux types de renseignements et de surveillance et n'ont donc pas d'obligations supplémentaires à ce titre. D'autre part, quelques-unes des modifications concernant les obligations des POC ont été reportées au deuxième volet de la révision, par exemple les nouveaux types de renseignements sur l'identification des utilisateurs selon les art. 42*a* et 43*a* OSCPT. Les nouvelles obligations pourront ainsi être introduites en même temps que les descriptions plus précises des différentes catégories de POC.
- Les POC exigeaient que la fourniture automatique des renseignements soit une option, et non une obligation. Il est donné suite à cette exigence dans la mesure où l'obligation de fournir les renseignements de manière automatisée n'est imposée qu'aux POC qui le font déjà aujourd'hui et qui ont donc déjà consenti les investissements nécessaires à cette fin. Les renseignements du type IR_13_EMAIL (renseignements sur des usagers de services de courrier électronique) peuvent désormais être fournis manuellement, car avec les nouvelles exigences, l'automatisation serait trop complexe pour les POC. Le nouveau type de renseignements IR_52_ASSOC_TEMP (renseignements immédiats sur les identifiants attribués pour une courte durée) doit en revanche être fourni de manière automatisée, car les données doivent être disponibles immédiatement, ce qui n'est pas possible avec une fourniture manuelle.
- La réglementation concernant la détermination de la position a été limitée à la technologie 5G et le délai pour sa mise en œuvre a été porté de 12 ou 18 mois à 24 mois.

Les points suivants n'ont pas pu être pris en compte lors du remaniement du projet après la consultation :

- Certains cantons, de même que la Conférence des commandantes et commandants des polices cantonales de Suisse (CCPCS), ont exigé que des formulations technologiquement neutres soient utilisées dans les ordonnances. Les détails techniques seraient relégués dans des annexes ou des directives qu'il serait plus facile de modifier. Mais ne formuler que certaines des dispositions de l'OSCPT de manière technologiquement neutre perturberait son unité et la rendrait moins compréhensible. Cette demande ne pourrait donc être prise en compte que dans le cadre d'une révision totale de l'ordonnance. Pour ne pas trop retarder les adaptations à la technologie 5G, cette option sera examinée à nouveau lors de la prochaine révision.
- Les POC ont critiqué le raccourcissement des délais pour la fourniture de certains types de renseignements. Dans la pratique, les autorités habilitées à obtenir des renseignements estiment qu'un délai d'un jour ouvré est trop long lorsqu'ils transmettent une demande durant le week-end ou un jour férié. Avec un délai d'un jour ouvré, un renseignement pourrait arriver trop tard, avec des conséquences possiblement désastreuses, par exemple dans le cas d'une alerte à la bombe anonyme. Le raccourcissement du délai prévu dans l'OME-SCPT semble donc raisonnable, d'autant plus qu'il ne concernerait que les demandes envoyées en dehors des heures de travail ordinaires ou les jours fériés.
- De nombreux fournisseurs, mais aussi plusieurs organisations, ont demandé une augmentation des indemnités versées aux POC, tandis que quatre cantons demandaient au contraire leur diminution. Les POC estimaient en particulier que l'indemnité pour les renseignements simples, fixée à trois francs, est trop basse. Dans son arrêt du 27 juillet 2021 (2C_650/2020), le Tribunal fédéral a cependant tranché qu'une indemnité de trois francs pour la réponse à une demande de renseignements de type IR_7_IP (art. 37 OSCPT) est équitable au sens de l'art. 38, al. 2, LSCPT. Le présent rapport ne revient pas sur ce sujet parce que les émoluments et indemnités pour les nouveaux types de renseignements et de surveillances seront également réglés par l'OF-SCPT, qui introduira un système forfaitaire.

3 Grandes lignes du projet

3.1 Modification de l'OSCPT

L'OSCPT est adaptée au progrès technologique, notamment à la 5G et à l'IMS :

Trois nouveaux types de renseignements et quatre nouveaux types de surveillances sont créés dans l'OSCPT :

- le type de renseignements IR_51_ASSOC_PERM : renseignements sur les identifiants attribués pour une longue durée (art. 48*a* OSCPT) ;
- le type de renseignements IR_52_ASSOC_PERM : renseignements immédiats sur les identifiants attribués pour une courte durée (art. 48*b* OSCPT) ;

- le type de renseignements IR_53_TEL_ADJ_NET : détermination des réseaux voisins de services de téléphonie et multimédia (art. 48*c* OSCPT) ;
- le type de surveillance (en temps réel) RT_54_POS_ONCE : détermination unique et immédiate de la position par le réseau (art. 56*a* OSCPT) ;
- le type de surveillance (en temps réel) RT_55_POS_PERIOD : détermination périodique et récurrente de la position par le réseau (art. 56*b* OSCPT) ;
- le type de surveillance (recherche en cas d'urgence) EP_56_POS_ONCE : détermination unique et immédiate de la position par le réseau (art. 67, let. b, OSCPT) ; et
- le type de surveillance (recherche en cas d'urgence) EP_57_POS_PERIOD : détermination périodique et récurrente de la position par le réseau (art. 67, let. c, OSCPT).

Le nouveau type de renseignements IR_51_ASSOC_PERM est créé pour obtenir les identifiants attribués pour une longue durée à un identifiant dans l'IMS. Le nouveau type de renseignement IR_52_ASSOC_Temp vise à obtenir en temps réel et de manière automatisée l'identifiant permanent associé à un identifiant temporaire de la 5G dans le cadre d'une intervention avec un dispositif technique spécial de surveillance de la correspondance par télécommunication (art. 269bis CPP ; ces dispositifs sont communément appelés IMSI-catchers). Le nouveau type de renseignement IR_53_TEL_ADJ_NET 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 quatre nouveaux types de surveillances sont créés pour exploiter les nouvelles possibilités qu'offre le « Lawful Access to Location Services » (LALS) pour déterminer la position dans la téléphonie mobile. 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, let. b et c).

Le nouvel art. 4*a* OSCPT définit les règles du « dies a quo » pour le calcul du délai de six mois concernant les surveillances rétroactives. Le calcul de ce délai était jusqu'à présent controversé dans la pratique.

L'actuel art. 18 de l'OSCPT 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. Il est précisé que les POC mentionnées à l'al. 1 doivent fournir les renseignements dont il est question de manière automatisée, mais le choix leur est laissé pour tous les autres renseignements entre la fourniture manuelle ou, en accord avec le Service SCPT, automatisée.

L'art. 20 de l'OSCPT (vérification des données relatives aux personnes pour les services de communication mobile) est complété et restructuré avec des dispositions distinctes pour les personnes physiques et pour les personnes morales. L'art. 20*c* OSCPT règle désormais la remise de moyens d'accès et l'activation de services pour les autorités de police de la Confédération et des cantons, et le Service de renseignement de la Confédération (SRC), dans les cas où seul un petit nombre de personnes doivent en avoir connaissance. L'art. 20 prévoyait jusqu'ici une vérification d'identité pour tous

les usagers, et donc aussi pour les membres des forces de police ou du SRC. Ces dernières années, dans la pratique, cette règle s'est révélée particulièrement problématique pour ces autorités.

Pour assurer que l'introduction des nouveaux types de renseignements et de surveillances se déroule sans problèmes pour les POC ou pour le Service SCPT, l'art. 74*b* de l'OSCPT contient des dispositions transitoires détaillées pour les différentes modifications.

3.2 Modification de l'OEI-SCPT

L'annexe de l'OEI-SCPT a été modifiée pour y intégrer les nouveaux types de renseignements et de surveillances qui font leur entrée dans l'OSCPT. Les émoluments et les indemnités concernant les autres types de renseignements et de surveillances ne sont pas modifiés. Cependant, comme il est prévu que la révision de l'OSCPT et la nouvelle OF-SCPT entrent en vigueur en même temps, le 1er janvier 2024, la modification de l'OEI-SCPT n'a plus lieu d'être : les modifications nécessaires seront intégrées dans l'OF-SCPT.

3.3 Modification de l'OME-SCPT

La révision de l'OME-SCPT modifie légèrement les délais de traitement pour les renseignements (art. 14 OME-SCPT) afin de satisfaire le besoin des autorités de poursuite pénale d'avoir des délais plus courts. Par ailleurs, le champ d'application de l'OME-SCPT parle désormais d'autorités (au sens de l'art. 1, al. 2, let. a à f, OSCPT), de sorte que l'art. 3 de l'OME-SCPT, qui règle la communication sécurisée, vaut désormais également pour les autorités.

3.4 Modification de l'OST-SCPT

Le présent projet offre pour finir l'occasion de réviser également certaines dispositions de l'OST-SCPT. Outre les accès à l'affichage de l'état des composants de surveillance dans le système de traitement (PTSS-Dashboard), la révision règle aussi 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).

4 Commentaire des dispositions

4.1 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 présenter, 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 fournir.

Remplacement d'expressions

L'*al. 1* prévoit que le terme « point d'accès au réseau WLAN » est remplacé par celui d'« accès au réseau WLAN », qui couvre aussi bien le point d'accès que la zone d'accès sans fil. Cette modification s'impose parce que 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.

L'*al.2* dispose que la révision de l'OSCPT offre l'occasion d'y introduire le sigle FSCD pour fournisseur de services de communication dérivés (art. 2, let. c, LSCPT), qui est déjà courant dans la pratique aux côtés de FST pour fournisseurs de services de télécommunication (art. 2, let. b, LSCPT ; voir également la modification de l'art. 1, al. 2, let. j).

L'*al. 3* concerne le terme « identifiant surveillé (target ID) », qui est remplacé par la version plus brève « identifiant cible ».

Art. 1, al. 1 et 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 pour éviter de répéter inutilement le texte de la loi dans l'ordonnance. Les FSCD qui ont des obligations étendues en matière à la fois de fourniture de renseignements (art. 22) et de surveillance (art. 52) sont désignés par l'expression *FSCD ayant des obligations étendues*. 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 relation 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). La télécopie, technologiquement obsolète et ne répondant plus aux normes de sécurité actuelles, n'est plus mentionnée à la *let. b*. Il n'y a pas de changement matériel à la *let. 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). Les fournisseurs concernés 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. 5, OSCPT, en relation 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 surveillance rétroactive, ni comment ce délai doit être calculé, ce qui a entraîné des discussions à plusieurs reprises.

Le nouvel *al. 1* définit la règle du « dies a quo » pour le calcul du délai de six mois concernant les surveillances rétroactives. Le jour déterminant 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[9] qui sont déterminants.

Le jour de la réception de l'ordre est préféré à celui de sa transmission pour les motifs suivants : lors d'une transmission usuelle via le composant de gestion des mandats WMC[10], il ne fait aucune différence que le délai soit calculé à compter du jour de la transmission ou de celui de la réception de l'ordre, vu qu'une poignée de secondes à

9 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).

10 Warrant Management Component (WMC) ; composant du système de traitement du Service SCPT (voir le Programme Surveillance des télécommunications [FMÜ]), en fonction depuis le 18 mars 2019.

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 dans des cas exceptionnels 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 (comme dans l'exemple 4 ci-après). L'autorité peut éviter ce délai en annonçant l'ordre par téléphone au Service SCPT, conformément à l'art. 3, let. c. 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).

Un écart d'un ou de plusieurs jours entre le moment où l'autorité transmet l'ordre et celui où le Service SCPT charge le fournisseur d'exécuter le mandat serait problématique parce que les fournisseurs ont aussi l'obligation d'effacer les données historiques à l'issue du délai de conservation de six mois (art. 21, al. 7). Comme le montre l'exemple 4 ci-après, le fournisseur pourrait dans un tel cas avoir déjà détruit les données les plus anciennes requises par l'autorité lorsqu'il reçoit le mandat de surveillance. Le Service SCPT garantit qu'une heure au maximum s'écoule entre le moment où il reçoit l'ordre de l'autorité et celui où il donne les mandats aux fournisseurs. Comme c'est le moment de la réception de l'ordre qui est déterminant pour le calcul du début de la surveillance rétroactive, il n'y a donc pas de conflit pour les fournisseurs entre la conservation et l'effacement des données secondaires.

Il convient de relever que c'est au moment 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[11].

Dans un cas normal, l'ordre est téléversé dans le composant de gestion des mandats (WMC) du système de traitement du Service SCPT et la transmission par l'autorité et la réception par le Service SCPT ont lieu le même jour (voir l'exemple 2 ci-après).

La surveillance rétroactive porte alors sur la période qui commence au plus tôt six mois avant le jour où le Service SCPT reçoit l'ordre. Pour rappel, l'art. 273, al. 3, CPP prévoit un délai calculé en mois, et non en jours ou en heures.

Le calcul du délai de six mois se fonde sur la doctrine[12] et sur la jurisprudence[13] : « 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. »[14]. 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

11 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. »)

12 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

13 En particulier ATF 144 IV 161 (jugement 6B_80/2018 du 25.04.2018)

14 Voir aussi par ex. l'art. 22, al. 2, de l'ordonnance du 30.08.1995 sur la taxe d'exemption de l'obligation de servir (**OTEO** ; RS **661.1**)

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, c'est-à-dire qu'il est plus court que celui où est donné l'ordre, 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[15] heure suisse (voir les exemples 1 à 4 ci-après). Normalement, les surveillances rétroactives ne sont exécutées que l'un des jours suivants (délai de traitement en général de trois jours ouvrés). Mais si la surveillance rétroactive est exécutée le jour même – donc avant 23 h, 59 min, 59 s –, l'autorité habilitée ne reçoit que les données secondaires (données historiques, DH) dont le fournisseur dispose au moment de l'exécution. Il n'y a pas de deuxième envoi ultérieur des DH 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 DH 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 fournir ultérieurement. Si l'autorité qui a donné l'ordre de surveillance a besoin de ces DH, elle doit envisager d'ordonner une nouvelle surveillance rétroactive à une date ultérieure (voir l'exemple 5 ci-après). Exiger des fournisseurs qu'ils fournissent ultérieurement les données qui, pour des raisons objectives, n'étaient pas encore disponibles au moment du premier envoi impliquerait pour ces fournisseurs une charge de travail disproportionnée. L'autorité qui fait la demande peut influencer le moment de l'exécution de la surveillance rétroactive en fonction des DH qui sont importantes pour elle, les plus anciennes ou les plus récentes. Pour les plus anciennes, elle doit ordonner la surveillance le plus vite possible. Pour les plus récentes, elle a le choix entre deux stratégies : soit elle fait une demande ordinaire de surveillance rétroactive avec exécution un des jours qui suit la demande, si elle n'a pas besoin des DH immédiatement, soit elle ordonne une surveillance en temps réel « données secondaires uniquement (IRI only) », si elle veut obtenir les données secondaires les plus récentes immédiatement, sans le délai inévitable pour les DH. Les données historiques et les données secondaires en temps réel (IRI) ne sont toutefois pas absolument identiques : les données IRI sont en général plus étendues et plus détaillées.

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 les délais de traitement prévus aux art. 17 et 18 OME-SCPT. Le

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

fournisseur exécute la surveillance rétroactive dans un délai de trois jours ouvrés pour les cas ordinaires et de six heures dans les cas d'urgence (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[16] (heure suisse) et se termine à 23 h 59, 59 secondes (les secondes ne sont pas indiquées dans les exemples qui suivent). Les surveillances exécutées le jour même font exception, puisqu'elles se terminent à la minute exacte de leur exécution plus 59 secondes. Le fournisseur doit livrer les DH disponibles au moment de l'exécution du mandat.

Exemple 1 : ordre daté du mardi 8 novembre 2022 qui, suite à des retards internes à l'autorité, n'est envoyé par courriel chiffré au Service SCPT que le jeudi **10 novembre 2020**, à 9 h 00, avec réception à la même heure.
→Début jour **JJ = 10**, mois MM : 11 - 6 = 5 → **MM = 5**, année **AAAA = 2022**
La surveillance débute au plus tôt le 10 mai 2022, à 00 h 00 ;
elle se termine au plus tard le 10 novembre, à 23 h 59.

Remarque : Cet exemple illustre le problème posé par le retard dans la transmission d'un ordre. Sans ce retard, l'autorité aurait pu obtenir les DH à partir du 8 mai 2022, soit deux jours plus tôt. La surveillance se serait toutefois également terminée deux jours plus tôt, le 8 novembre 2022.

Exemple 2 : ordre téléversé dans le WMC mercredi **31 août 2022**, à 18 h 00
→ Début **JJ = 31**, MM : 8 – 6 = 2 → **MM = 02**, **AAAA = 2022**
Le mois de février n'ayant pas 31 jours, on « arrondit » la date au dernier jour de février 2022.
La surveillance débute au plus tôt le 28 février 2022, à 00 h 00 ;
elle se termine au plus tard le 31 août 2022, à 23 h 59.

Exemple 3 : ordre donné par téléphone au Service SCPT le dimanche **31 décembre 2023**, à 16 h 50
→ Début **JJ = 31**, **MM** : 12 – 6 = 6 → MM = **06**, **AAAA = 2023**
Le mois de juin n'ayant pas 31 jours, on « arrondit » la date au dernier jour de juin 2023.
La surveillance débute au plus tôt le 30 juin, à 00 h 00 ;
elle se termine au plus tard le 31 décembre 2023, à 23 h 59.

Exemple 4 : l'ordre est daté du mercredi 13 avril 2022, envoyé par la poste le jeudi 14 avril 2022 (cachet de la poste), pas de préavis téléphonique. Le Service SCPT reçoit l'ordre après le week-end pascal, mardi **19 avril 2022**, à 9 h 00. Le mandat de surveillance est transmis au fournisseur le 19 avril 2022, à 9 h 50.
→ Début **JJ = 19**, **MM** : 4 – 6 = -2 + 12 → MM = **10** de l'année précédente, AAAA : 2022 – 1 → **AAAA = 2021**
La surveillance débute au plus tôt le 19 octobre 2021, à 00 h 00 ;
elle se termine au plus tard le 19 avril 2022, 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. exemple 3). Dans cet exemple, une annonce par téléphone le 14 avril 2022 (cinq

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

jours plus tôt) aurait permis de faire remonter la surveillance rétroactive jusqu'au 14 octobre 2021, mais elle se serait aussi terminée cinq jours plus tôt, le 14 avril 2022.

Exemple 5 : ordre pour une surveillance rétroactive **urgente**, téléversé dans le WMC par l'autorité le vendredi **26 août 2022**, **à 16 h 00**, transmis à la POC par le Service SCPT à 16 h 30.
→ Début **JJ = 26**, MM : 8 – 6 = 2 → **MM = 02**, **AAAA = 2022**
La surveillance débute au plus tôt le 26 février 2022, à 00 h 00 ;
elle se termine au plus tard le 26 août 2022.

La fin de la surveillance rétroactive tombant le jour de son exécution, l'heure exacte 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 le mandat, en l'occurrence à 22 h 30 au plus tard). Pour des raisons techniques, les DH qui viennent d'arriver chez la POC ne sont pas encore prêtes à être fournies. L'autorité qui émet l'ordre de surveillance doit donc faire une pesée d'intérêts entre la rapidité de la fourniture et la disponibilité des données secondaires qu'elle souhaite obtenir. Quelques heures peuvent s'écouler avant que la POC ne dispose de toutes les données secondaires. 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 » (voir plus haut).

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

Cette disposition est révisée dans son ensemble en raison des nombreuses modifications qui doivent y être apportées. Elle 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 accordés au Service SCPT et aux POC pour l'exécution des prestations sont fixés dans l'OME-SCPT, pour les services de piquet comme pendant les heures normales de travail. Une POC peut traiter volontairement dans le cadre d'un service de piquet des renseignements ou des surveillances standardisés (resp. art. 26, al. 1 et art. 28) pour lesquels elle n'est pas tenue de le faire ; elle n'est dans ce cas pas liée par les délais d'exécution prescrits.

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 relation 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 ayant des obligations complètes (c'est-à-dire qui ne sont pas exonérées selon l'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, lorsqu'ils y sont tenus en vertu des art. 18 et 50. Cette restriction est faite parce que les FSCD ayant des obligations étendues en matière de surveillance (art. 52) ne sont pas tenus de fournir les nouveaux renseignements selon les art. 48*a* à 48*c*, ni d'exécuter les nouvelles surveillances selon les art. 56*a* et 56*b*, les recherches en cas d'urgence selon l'art. 67, let. b et c, et les recherches de personnes

condamnées selon l'art. 68, al. 1, let. b et c. Ne sont pas mentionnés dans cet alinéa les FST ayant des obligations restreintes en matière de surveillance (art. 51), les FSCD sans 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, car ils ne sont pas tenus d'assurer un service de piquet.

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* règle la fourniture de certains renseignements. Les renseignements visés aux art. 44 à 48 ne doivent pas obligatoirement être fournis pendant le service de piquet. La let b dit quels types de surveillances en temps réel sont activés et la *let c*, quels types de surveillances rétroactives déclarées urgentes sont exécutés pendant un service de piquet. La *let. d* spécifie les types de recherches en cas d'urgence et de recherches de personnes condamnées qui sont exécutées pendant les services de piquet. La let. d[bis][17], en vigueur depuis le 1[er] juin 2022, devient la nouvelle *let. e*.

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 ordres, 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 »). Il 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 qu'elles ne le sont pour les types standardisés. Ces cas spéciaux 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.

L'*al. 4* prévoit désormais que les POC que l'al. 1 n'oblige pas à avoir un service de piquet mais qui sont néanmoins, pour d'autres raisons, joignables en dehors des heures normales de travail et les jours fériés, doivent fournir au Service SCPT les coordonnées du service ou de la personne à contacter. Aucune nouvelle obligation ne leur est imposée à cet égard, elles ne sont notamment pas tenues de mettre en place un service de piquet spécialement pour le Service SCPT. Lorsque cependant un tel service existe déjà, ses coordonnées doivent en être données au Service SCPT. Même si ces contacts ne sont pas des spécialistes de la surveillance (« officiers LI »), ils pourront aider le Service SCPT dans les cas particulièrement urgents en dehors des heures normales de travail et les jours fériés. Les cas « particulièrement urgents » sont par exemple des

17 Ordonnance du 4 mai 2022 sur les mesures policières de lutte contre le terrorisme (**OMPT** ; RO **2022** 301)

alertes à la bombe, des enlèvements ou d'autres situations dans lesquelles la vie ou l'intégrité corporelles d'une personne est en jeu. Dans une telle situation, le Service SCPT ou la police essaieraient de prendre contact avec la POC. Fournir un numéro de téléphone ou les coordonnées d'une personne à contacter simplifiera les choses pour le Service SCPT, les autorités de poursuite pénale et les POC.

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

Cet article est révisé dans son ensemble en raison des nombreuses modifications qui doivent y être apportées. 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 comme principe que les FST ayant des obligations complètes et les FSCD ayant des obligations étendues (art. 22 ou art. 52) doivent fournir les renseignements via l'IRC[18].

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, première phrase* dit quels types de renseignements les FST ayant des obligations complètes doivent livrer de manière automatisée. L'automatisation est imposée pour les renseignements fréquents, simples à fournir ou dont il est essentiel qu'ils soient fournis rapidement. La *deuxième phrase* précise que les FST dont il est question ont le choix entre une fourniture manuelle ou, en accord avec le Service SCPT, automatisée pour tous les autres renseignements standardisés (les autres types de renseignements définis dans l'OSCPT).

Le choix entre fourniture manuelle ou automatisée est également donné aux autres POC (cf. al. 3 et 4), par respect pour leur liberté économique : l'automatisation nécessite des investissements, mais permet ensuite d'économiser sur les coûts d'exploitation. Le Service SCPT décide en concertation avec la POC concernée si l'automatisation d'un certain type de renseignements peut être mise en œuvre dans l'IRC. Un même type de renseignements peut ainsi être fourni manuellement par une POC, tandis qu'une autre préférera automatiser la procédure. Les changements apportés aux types de renseignements automatisés entraînent des dépenses pour les POC concernées, qui doivent modifier leurs systèmes, entre autres celui de gestion de la clientèle, pour être en mesure de fournir les renseignements voulus de manière automatisée. La question de la proportionnalité doit donc également être considérée lors de ces changements, pour voir si par exemple la fréquence du recours à un type de renseignements continue de justifier son automatisation. C'est la raison pour laquelle le type de renseignements défini à l'art. 42 (IR_13_EMAIL), moins fréquemment utilisé, n'est plus dans le groupe de ceux qui sont « obligatoirement » automatisés (cf. actuel al. 2), mais dans

[18] Information Request Component (IRC) ; composant pour le traitement des demandes de renseignements dans le système de traitement du Service SCPT (voir le Programme Surveillance des télécommunications), en service depuis le 18.03.2019.

le groupe des « autres renseignements », pour lesquels même les POC ayant des obligations complètes ont le choix entre fourniture manuelle ou, en accord avec le Service SCPT, automatisée.

Parmi les trois nouveaux types de renseignements, seul le type défini à l'art. 48*b* (IR_52_ASSOC_TEMP) doit être fourni de manière automatisée par les FST concernés, car ces données doivent être mises à disposition immédiatement, ce qui exclut une fourniture manuelle. Pour les deux autres nouveaux types selon l'art. 48*a* (IR_51_ASSOC_PERM) et l'art. 48*c* (IR_53_TEL_ADJ_NET), les FST concernés ont le choix entre fourniture manuelle ou, en accord avec le Service SCPT, automatisée.

La fourniture automatique et la fourniture manuelle via l'IRC sont deux procédures distinctes. 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 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.

La troisième possibilité est la fourniture manuelle des renseignements en dehors du système de traitement (al. 3, let. a) : l'autorité saisit sa demande dans l'IRC et le Service SCPT la relaie à la POC en dehors de l'IRC, 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* règle la fourniture de renseignements par les FST ayant des obligations restreintes en matière de surveillance (art. 51). Ceux-ci sont dispensés de fournir les renseignements visés à l'art. 48*b*, pour des motifs de proportionnalité. Il est en effet essentiel que ces renseignements soient livrés très rapidement, ce qui exige de la part du FST une préparation active comparable à celle que demande l'exécution d'une surveillance en temps réel, et donc proche des obligations de surveillance selon l'art. 26 LSCPT. Pour la mise en œuvre de ce type de renseignements à fournir quasiment en temps réel, un FST doit notamment investir dans une nouvelle interface et dans le système de fourniture automatisée de renseignements. Ces charges supplémentaires ne doivent être imposées qu'aux grands FST. Les renseignements visés à l'art. 48*b* ont ceci de particulier qu'il n'est guère possible pour un FST de les fournir manuellement ou de fournir les indications dont il dispose sans préparation active.

Pour les autres renseignements standardisés (art. 26, al. 1), les FST ayant des obligations restreintes en matière de surveillance sont soumis à l'exigence minimale selon la *let. a* d'une fourniture manuelle par écrit en dehors du système de traitement. Ils peuvent toutefois également choisir de transmettre les renseignements manuellement mais via l'IRC (*let. b*, voir le commentaire de l'al. 2). Un FST ayant des obligations

restreintes en matière de surveillance peut demander à pouvoir fournir certains renseignements sous forme automatisée (*let. c*). Le Service SCPT décide alors, en accord avec le FST en question, si une mise en œuvre dans l'IRC est possible.

L'*al. 4, première phrase,* dit quels types de renseignements doivent être fournis de manière automatisée par les FSCD ayant des obligations étendues (art. 22 ou art. 52). La *deuxième phrase* prévoit que ces mêmes FSCD sont dispensés de fournir les renseignements visés dans les nouveaux art. 48*a* à 48*c*. La question de savoir si ces renseignements devront à l'avenir être fournis par les FSCD sera tranchée dans le cadre de la deuxième révision, lorsqu'une description plus précise des catégories FST et FSCD sera appliquée. La présente révision n'impose donc pas de nouvelles obligations aux FSCD en lien avec ces nouveaux types de renseignements. La *troisième phrase* reprend la réglementation de l'al. 2, deuxième phrase (voir le commentaire correspondant) concernant la possibilité de choisir entre fourniture automatisée ou manuelle via l'IRC.

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 fournir 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 fournir que les données dont ils disposent.

L'*al. 2* précise la manière dont ces données peuvent être fournies. L'exigence minimale est que les FSCD n'ayant pas d'obligations étendues et les exploitants de réseaux de télécommunication internes fournissent 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 fournir ces données via l'interface de consultation (IRC) du système de traitement, manuellement ou, en accord 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, deuxième phrase, et al. 4, deuxième 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 pour les services de communication mobile

Cet article est révisé dans son ensemble en raison des nombreuses modifications qui doivent y être apportées. 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). Cette disposition, tout comme les art. 20*a* et 20*b*, s'appuie 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 (art. 20*a*), et pour les personnes morales, les indications que celles-ci fournissent (art. 20*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 (art. 20*a*) ou des indications fournies par une personne morale (art. 20*b*) 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'usager, 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.

L'*al. 3* prévoit que le FST vérifie de manière appropriée que le revendeur professionnel a correctement enregistré et identifié l'usager et qu'il lui a bien transmis les indications fournies et une copie du document d'identité présenté. Il doit en effet être en mesure de fournir 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 fournira, 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. 20*a* 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[19]. 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 re-

19 Selon l'arrêt de la CourEDH du 30.01.2020 (Az. 50001/12) dans la cause 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.

vendeur 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[20]. 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 »[21] 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, c'est-à-dire 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 (translittération), 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 ;
- 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'adresse à saisir – rue et numéro – est celle du domicile, du domicile secondaire, du lieu de séjour à la semaine ou du lieu de résidence habituel utilisé pour contacter le client.

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

21 finma.ch =>Documentation => Circulaire

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).

La *première phrase* de l'*al. 4* exige du FST ou du revendeur, comme c'est déjà le cas aujourd'hui, qu'il fasse une copie du document d'identité présenté, qui doit être l'original. 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. 4. 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 fixé à trois jours. Un numéro d'appel peut en effet être utilisé dès son acquisition et peut devenir pertinent pour une enquête le jour même. Il est donc important que les données de l'utilisateur et la copie de sa pièce d'identité soient disponibles dans l'IRC le plus vite possible. Le respect de ce délai de trois jours semble raisonnable, même pour les petits revendeurs professionnels. 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).

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 prin-

cipe 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. 20c Remise de moyens d'accès et activation de services pour les autorités de police et le SRC

Dans l'exécution de leurs missions légales, les autorités de police et le SRC doivent pouvoir utiliser des moyens d'accès à des services de télécommunication (par ex. cartes SIM prépayées) pour lesquels ces autorités et leurs collaborateurs n'apparaissent ni dans les annuaires publics selon l'art. 12*d* LTC, ni dans les données d'annuaire selon l'art. 21 LTC, ni dans l'IRC. Ils ont besoin de ces moyens d'accès notamment pour protéger leurs collaborateurs, leurs contacts et leurs sources, mais aussi leurs méthodes et leurs capacités techniques (par ex. pour communiquer lors d'observations de personnes ayant accès à des moyens techniques sophistiqués, dans les milieux du crime organisé ou de l'espionnage).

Ces mesures de protection spéciales sont nécessaires pour les collaborateurs des autorités de police et du SRC qui accomplissent leurs tâches légales en utilisant leur véritable identité, c'est-à-dire sans la protection d'une identité d'emprunt. Les collaborateurs qui utilisent une identité d'emprunt (agents infiltrés selon l'art. 285*a* CPP et personnes dotées d'une identité d'emprunt selon les art. 17 ou 18 LRens) peuvent obtenir des moyens d'accès à des services de télécommunication normalement, en utilisant leur identité d'emprunt, sans dévoiler leur véritable identité. Ils sont donc suffisamment protégés. L'obtention par voie ordinaire de moyens de télécommunication peut même renforcer leur identité d'emprunt.

De toute façon, l'art. 12*d* LTC n'impose pas la publication des données des clients dans des annuaires publics : les clients ont la liberté de choix. Chez les FST et les revendeurs professionnels, un nombre de personnes important et difficile à contrôler a cependant accès aux systèmes et donc aux données enregistrées pour la fourniture des renseignements.

Grâce à cette nouvelle disposition, les FST sauront que des autorités sont usagères de certains moyens d'accès et services protégés, tout en ayant l'obligation de protéger le mieux possible ces données et en ne les communiquant qu'aux autorités concernées, sur demande, via le Service SCPT. Les FST s'acquittent ainsi de toutes leurs obligations selon les art. 21ss de la LSCPT concernant l'identification des usagers et la fourniture de renseignements aux autorités habilitées à les demander, mais empêchent des éléments potentiellement criminels d'en avoir connaissance et protègent de la sorte les opérations des autorités de police et du SRC.

Pour les motifs et les circonstances exposés ci-dessus, l'*al. 1* prévoit qu'un contrat peut être conclu entre un FST et une autorité, avec le Service SCPT dans le rôle de l'intermédiaire. Il ne s'agit pas d'un contrat d'abonnement, mais d'un contrat supplémentaire entre un FST et une autorité, conclu aux fins de régler les modalités de la remise de moyens d'accès et de l'activation de services. Pour garantir un niveau de protection

uniforme le plus élevé possible, les FST définissent en accord avec le Service SCPT les mesures à utiliser pour empêcher une diffusion des informations sur les identités véritables des détenteurs des moyens de communication au-delà du cercle de personnes autorisées, qui doit être aussi limité que possible. La procédure sera probablement comparable à celle que les FST utilisent aujourd'hui déjà pour bloquer les données des personnes politiquement exposées.

L'*al. 2* règle la procédure de remise des moyens d'accès et d'activation des services à des autorités de police ou au SRC. L'autorité (autorité de police ou SRC) désigne une personne responsable qui est habilitée, au nom de l'autorité en question, à se faire remettre des moyens d'accès ou à faire activer des services. Cette personne connaît l'identité des usagers qui utilisent ces moyens d'accès et ces services. La personne responsable du côté du FST documente à l'interne les moyens d'accès remis à l'autorité et les services activés. Le FST est alors en mesure de fournir au Service SCPT les renseignements demandés sur les usagers, comme il y est obligé et se prémunit ainsi contre une plainte qui serait déposée au Service SCPT sur la base de l'art. 39, al. 1, LSCPT.

L'*al. 3* précise que les moyens d'accès et les services en question ne peuvent être utilisés que dans le cadre des dispositions légales pertinentes régissant l'action de l'autorité concernée (par ex. des art. 298*a* ss CPP [recherches secrètes] ou des art. 7 et 35 LRens). Les autorités de police et le SRC gardent néanmoins la possibilité d'obtenir des moyens d'accès et de recourir à des services dans les conditions normales prévues aux art. 20*a* et 20*b*.

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. Il s'agit de régler quelles POC doivent conserver quelles données pendant combien de temps. 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 4), les données relatives à l'identification des utilisateurs 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. 2) et les données d'utilisation (*usage data*) pendant six mois à compter du moment où elles sont générées (al. 3). La formule générale des données ou indications *saisies aux fins de l'identification*, déjà utilisée dans l'ordonnance, figure désormais dans les différents alinéas (al. 1, 3 et 5).

L'*al. 1* correspond à l'actuel al. 1, première phrase. L'obligation de conserver des données (*let. a*) vaut pour toutes les POC ayant des obligations actives en matière de fourniture de renseignements (soit tous les FST et les FSCD ayant des obligations étendues selon l'art. 22 ou l'art. 52). L'obligation de conserver les indications sur les identifiants attribués pour une longue durée a été ajoutée pour les renseignements visés à l'art. 48*a* (*let. b*). Cette obligation ne vaut que pour les FST, puisque les FSCD sont dispensés de livrer les renseignements visés à l'art. 48*a* (cf. art. 18, al. 4).

L'*al. 2* ne s'applique qu'aux FST car il traite d'un accès au réseau et reprend la réglementation actuelle, avec une adaptation rédactionnelle (« accès au réseau WLAN » au

lieu de « point d'accès au réseau WLAN » ; cf. le commentaire concernant le remplacement d'expressions, al. 1). La précision est en outre ajoutée qu'il n'est question que des réseaux WLAN exploités à titre professionnel (cf. le commentaire introductif du présent article).

L'*al. 3*, qui ne concerne lui aussi que les FST puisqu'il est également question d'accès au réseau, règle la conservation des données sur l'attribution univoque d'adresses IP (art. 37). Les données relatives à l'attribution et à la traduction d'adresses IP et de numéros de ports (art. 37, 38 et 39) étaient jusqu'à présent mentionnées ensemble dans l'al. 2, let. b. Pour des raisons de proportionnalité, il convient cependant de distinguer, quand on parle d'attribution dynamique d'adresses IP, entre l'attribution univoque (art. 37) et l'attribution non univoque avec procédure de traduction (NAT) d'adresses IP et de numéros de port (art. 38 et 39 ; cf. nouvel al. 5, let. b). Pour les adresses IP attribuées de manière univoque, il y a des attributions fixes et des attributions dynamiques. Les données relatives aux attributions fixes doivent, comme toutes les données clients, être conservées pendant la toute durée de la relation commerciale et six mois au-delà (al. 1). Pour les attributions dynamiques, la durée de conservation des données d'attribution n'est en revanche que de six mois (al. 3), car il s'agit de données d'utilisation. La différence est que pour les adresses IP fixes, l'attribution ne dépend pas de l'utilisation (l'adresse IP est attribuée de manière permanente, que l'accès internet soit ou non utilisé). Lorsque l'attribution est dynamique, l'adresse IP n'est attribuée que pendant l'utilisation effective de l'accès internet. La même adresse IP peut être attribuée à différents utilisateurs à différents moments, mais elle n'est jamais attribuée simultanément à plus d'un utilisateur (c'est pour cela qu'elle est qualifiée d'« univoque »).

L'*al. 4* règle explicitement la durée de conservation des indications sur les usagers et des copies des documents d'identité dans le domaine de la téléphonie mobile. L'obligation de conserver ces données ne vaut que pour les FST qui offrent des services de communication mobile (opérateurs de téléphonie mobile). 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 subsumés de manière implicite dans l'actuel al. 1.

Les données visées à l'*al. 5* sont des données d'identification selon l'art. 22, al. 2, deuxième phrase, LSCPT et, par nature, ce sont des données secondaires. L'obligation de conserver ces données est comparable avec l'obligation de conserver des données pour les surveillances rétroactives. En raison de la grande quantité de données et de la charge de travail considérable que leur conservation implique, l'obligation ne vise que les grands FST, afin de respecter le principe de proportionnalité.

Cet alinéa est fondé sur l'actuel al. 2. La let. a reste inchangée (seuls les renvois aux différentes dispositions sont adaptés). La *let. b* correspond à l'actuelle let. b, mais ne mentionne plus les données pour l'identification visées à l'art. 37 (adresses IP attribuées de manière univoque), qui se trouvent maintenant à l'al. 3. La *let. c* fixe 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 (« conserver pendant six mois » au lieu de « conserver et être en mesure de livrer pendant six mois ») 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 fournir dans le cadre d'une demande de renseignements, à moins qu'elles ne fassent explicitement partie des données à fournir pour le type de renseignements demandé. Ces données secondaires qui n'ont pas besoin d'être fournies ne servent alors aux POC que pour évaluer et effectuer l'identification des utilisateurs. Ne doivent être fournies que les indications demandées sur l'identification des utilisateurs (art. 38) ou sur le contexte de traduction d'adresses de réseau (art. 39). Une POC ne peut livrer les autres données secondaires que dans le cadre d'une surveillance (en temps réel ou rétroactive), puisque les données secondaires visées à la let. b ne font pas partie d'un type de surveillance standardisé.

Les données visées à l'*al. 6* correspondent de par leur nature aux données visées à l'al. 5, let. a et b, et le délai de conservation est le même. C'est pour une meilleure lisibilité que cet alinéa distinct est consacré aux FSCD ayant des obligations étendues en matière de surveillance (art. 52), car l'al. 5, let. c ne les concerne pas. Pour le reste, voir le commentaire de l'al. 5, let. a et b.

L'*al. 7* correspond à l'actuel al. 3, avec adaptation du renvoi. Il règle la destruction des données secondaires décrite à l'al. 5 et concerne tous les fournisseurs (al. 5 et 6) qui conservent ces données secondaires.

Il convient de relever qu'il n'est pas nécessaire de conserver des indications concernant les identifiants attribués pour une courte durée visés au nouvel 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 quasiment réel (voir le commentaire de l'art. 48*b*.)

Art. 26 Types de renseignements

L'*al. 1* de cet article, qui présente une vue d'ensemble des différents types de renseignements, est restructuré. Pour en améliorer la lisibilité, la liste des types de renseignements comprend désormais uniquement des lettres, et non plus un mélange de chiffres et de lettres.

À la let. d, 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. La *let. h* mentionne les deux nouveaux types de renseignements prévus aux art. 48*a* (IR_51_ASSOC_PERM, renseignements sur les identifiants attribués pour une longue durée) et 48*b* (IR_52_ASSOC_TEMP, renseignements immédiats sur les identifiants attribués pour une courte durée) et la *let. i*, le nouveau type de renseignement défini à l'art. 48*c* (IR_53_TEL_ADJ_NET, détermination des réseaux voisins de service de téléphonie et multimédia).

À l'*al. 2*, l'expression « fournisseurs » est remplacée par celle plus indiquée ici de « personnes obligées de collaborer » (POC). En effet, les exploitants 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, deux pour les recherches en cas d'urgence). Quelques adaptations sont faites dans les désignations des types de surveillances existants. L'article est par ailleurs restructuré pour une meilleure lisibilité. La division en alinéas est supprimée et les actuels al. 1 à 5 deviennent les *let. a* à *e*. De ce fait, les lettres deviennent des chiffres dans la nouvelle sous-structure.

À la *let. a*, les *ch. 1 à 3* restent pour l'essentiel inchangés. Le *ch. 4* est nouveau 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 le *ch. 5*.

Le type de surveillance visé à la *let. b, ch. 3* se nomme désormais « localisation lors de la dernière activité » (voir aussi le commentaire de l'art. 63).

À la *let. c, ch. 1*, le type de recherche en cas d'urgence visé est désormais la localisation lors de la dernière activité (voir art. 67, let. a). Le *ch. 2* est nouveau et renvoie aux deux nouveaux types de recherche en cas d'urgence visant à déterminer une position (LALS, voir art. 67, let. b et c). Les *ch. 3*, *4* et *5* restent inchangés et correspondent aux actuelles let. b, c et d de l'actuel al. 3. Seuls les renvois entre parenthèses aux dispositions correspondantes sont adaptés.

Le type de surveillance visé à la *let. d, ch. 1* se nomme désormais « localisation lors de la dernière activité » (voir aussi le commentaire de l'art. 63). Le *ch. 2* est nouveau 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 ch. 3, 4 et 5 restent inchangés et correspondent aux actuelles let. b, c et d de l'actuel al. 4. Seuls les renvois entre parenthèses aux dispositions correspondantes sont adaptés. Le *ch. 6* 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).

La *let. e* a été légèrement raccourcie et reprend matériellement l'actuel al. 5 entré en vigueur en même temps que l'OMPT[22] le 1er juin 2022.

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

22 Ordonnance du 4 mai 2022 sur les mesures policières de lutte contre le terrorisme (**OMPT** ; RO **2022** 301)

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 le texte allemand), et ch. 2 et 9 à 13, 2, phrase introductive et let. g et i à k, et 3

À l'*al. 1, let. b*, les indications à fournir sont structurées plus clairement grâce à une sous-division en trois chiffres. Au *ch. 1*, les renvois 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* est ajoutée la mention « d'autres adresses » et la période de validité de ces « autres adresses et coordonnées ». Les fournisseurs disposent souvent non seulement de l'adresse au moment de l'enregistrement du client, mais aussi d'autres adresses consécutives à un déménagement ou des adresses alternatives utilisées pour la livraison ou la facturation. Les autres coordonnées sont par exemple des adresses électroniques, ou encore des numéros de téléphone qui auraient été communiqués. Par période de validité, on entend la période (date de début et, le cas échéant, date de fin) pour laquelle les adresses et autres coordonnées sont ou ont été annoncées à la POC. La POC fournit les données et les périodes de validité dont elle a connaissance. Elle n'a pas l'obligation de saisir et de tenir à jour toutes les adresses et coordonnées de ses utilisateurs.

À la let. c, les mêmes modifications sont faites qu'à la let. b, sauf pour l'adaptation des renvois au ch. 1, qui ne sont modifiés que pour les services de téléphonie mobile. 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 fournies. 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 fournir. Elles peuvent donc être restructurées avant la fourniture, mais elles doivent être désignées de manière claire afin que les autorités qui les ont requises puissent mieux comprendre leur signification (par ex. 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 la *let. d*, une adaptation rédactionnelle est faite dans le texte allemand pour répondre aux règles de la formulation non sexiste.

Au *ch. 2,* deux modifications sont apportées. 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 numéros ou plusieurs cartes SIM qui peuvent être utilisés 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 numéro principal (maître) et des numéros annexes (esclaves). L'utilisateur peut lui-même modifier cette hiérarchie en déterminant laquelle des cartes SIM ou lequel des appareils utilise le numéro principal ou les numéros annexes. Plusieurs MSISDN peuvent par exemple être subordonnés à un IMSI. Dans un cas simple, un seul MSISDN est subordonné à un IMSI. Les numéros annexes peuvent aussi être des numéros techniques qui ne sont en général pas connus de l'utilisateur. 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* tend à gagner 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 fourni (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 un accès non-3GPP (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 (défini dans l'annexe), 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 utilisateur 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 peut communiquer son *SUPI* au réseau sous forme chiffrée (par ex. lors de la connexion au réseau), ce qui a des implications pour l'utilisation de dispositifs techniques spéciaux de surveillance selon l'art. 269bis CPP (voir art. 48*b*). 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 (par ex. numéro de téléphone « MSISDN ») ou identifiants de service (par ex. numéro SIM « ICCID ») 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…). 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 en fonction de l'utilisation (données d'utilisation), ce n'est pas cette recherche qui est prévue mais la nouvelle décrite à l'art. 36. Doit désormais également être indiquée la période de validité de la ressource d'adressage ou de l'identifiant.

Au *ch. 13*, un champ est ajouté pour communiquer la désignation du service d'accès au réseau sur lequel porte la requête (par ex. nom du produit, de l'offre, de l'abonnement ou du tarif), afin de faciliter la tâche à l'autorité qui a demandé les renseignements et qui doit évaluer les réponses qui lui sont fournies. L'information les aide aussi à mieux comprendre de quel type de service il s'agit. C'est par exemple le nom sous lequel un abonnement est commercialisé qui peut être indiqué ici. 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 le LEI (voir le commentaire de l'art. 20*b*, al. 1, let. b). À la *let i*, l'identifiant de l'usager (par ex. numéro de client) est ajouté comme critère de demande, ce qui peut être utile pour obtenir tous les services d'un usager donné ou pour la demande d'un identifiant alternatif comme prévu à l'art. 36, al. 1, let. b, ch. 3 (par ex. dans le cas d'un accès au réseau WLAN exploité à titre professionnel). Par ailleurs un autre exemple d'identifiant du service (GPSI) est cité en lieu et place de « l'identifiant DSL » (voir le 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).

La *première phrase* de l'*al. 3* 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

En raison des nombreuses modifications qui y sont apportées, cet article est intégralement révisé afin d'en améliorer la lisibilité et la compréhension.

L'*al. 1* est restructuré avec une *let a* (qui reste inchangée) et une *let. b* à laquelle sont énumérées, dans les chiffres 1 à 6, les indications à fournir pour chacun des services. En effet, d'autres services peuvent être liés à celui sur lequel porte la demande. L'actuelle deuxième phrase introductive de l'al. 1 n'a plus lieu d'être puisque la fourniture de la période de validité est précisée, quand il y a lieu, pour chacune des indications.

Le *ch. 1* reprend matériellement, sans changement, l'actuelle let. b. Le *ch. 2* définit les autres identifiants de service, qui peuvent être non seulement le MSISDN, mais d'autres identifiants aussi. Ce type de renseignements concerne tous les types de services d'accès au réseau, pas uniquement la téléphonie mobile. La période de validité des identifiants de service visés au ch. 2 doit désormais également être fournies, afin que les autorités de poursuite pénale puissent juger de leur pertinence. Le *ch. 3* est nouveau et sert à l'identification des utilisateurs d'accès publics au réseau WLAN exploités à titre professionnel. Avec l'identifiant reçu, l'autorité peut ensuite faire une demande de renseignements de type IR_4_NA (art. 35) pour recevoir les données d'identification selon l'art. 19, al. 2. Le *ch. 4* correspond pour l'essentiel à l'actuelle let. d et règle les indications à transmettre concernant les équipements utilisés au cours des six derniers mois en lien avec chacun des services auprès du fournisseur. Un nouvel identifiant de la 5G est ajouté, le « *Permanent Equipment Identifier* » (PEI), 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. Le *ch. 5* réunit les actuelles let. e (ICCID au lieu du numéro SIM, voir le commentaire de l'al. 1, let. d, ch. 9) et f (PUK), en y ajoutant la période de validité et d'autres identifiants comme l'IMSI et le MSISDN afin de donner aux autorités habilitées une meilleure compréhension de la chronologie, pour chaque accès au réseau, des cartes SIM et autres moyens d'accès utilisés. Les deux nouveaux identifiants de la téléphonie mobile 5G sont ajoutés : le SUPI (voir le commentaire de l'art. 35, al. 1, let. d, ch. 10) et le GPSI (voir le commentaire de l'art. 35, al. 1, let. d, ch. 2). Un nouveau *ch. 6* fait son apparition, pour la transmission d'informations sur les offres multi-appareils. La hiérarchie entre l'appareil principal et les appareils secondaires pouvant être modifiée en tout temps par l'usager, ces informations sont dynamiques et doivent être obtenues via une demande de type IR_6_NA, visant les données d'utilisation.

L'*al. 2* prévoit comme aujourd'hui que seules les indications qui sont ou étaient valables pendant la période sur laquelle porte la demande doivent être fournies. Comme ce type de renseignements vise des données d'utilisation, il s'agit de données que les POC qui y sont tenues ne doivent conserver que pendant six mois. Pour les demandes portant sur des périodes plus éloignées dans le passé, les POC ne doivent fournir que les données dont elles pourraient encore disposer.

À la *let. a*, l'identifiant DSL est remplacé dans les exemples par le GPSI (voir le commentaire de l'art. 35, al. 1, let. d, ch. 2) et la possibilité est ajoutée de faire une demande avec un identifiant servant à l'identification des usagers d'accès publics au réseau WLAN exploités à titre professionnel. Les *let. b* et *c* restent inchangées, seuls les

nouveaux identifiants du système 5G y sont ajoutés : le SUPI (voir le commentaire de l'art. 35, al. 1, let. d, ch. 10) et le PEI (voir art. 36, al. 1, let. b, ch. 4). La *let. d* reste inchangée. Une nouvelle *let. e* est ajoutée pour standardiser les demandes de codes PUK et les rendre ainsi plus efficaces. 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 d'un ICCID donné.

Art. 37, al. 1, phrase introductive 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.

À la *let. b*, l'identifiant DSL est remplacé, dans les exemples, par le GPSI, un identifiant du système 5G (voir le commentaire de l'art. 35, al. 1, let. d, ch. 2). La nouvelle possibilité ajoutée d'un « identifiant qui permette de demander les données d'identification selon l'art. 19, al. 2 » sert à l'identification des utilisateurs d'accès publics au réseau WLAN exploités à titre professionnel. Avec l'identifiant reçu, l'autorité peut ensuite faire une demande de renseignements de type IR_4_NA (art. 35) pour recevoir les données d'identification selon l'art. 19, al. 2.

Art. 38, al. 1, phrase introductive et let. b, et 2, phrase introductive et let. f

La phrase introductive de l'*al 1* est raccourcie mais ne change pas sur le fond. À la *let. b*, l'identifiant DSL est remplacé, dans les exemples, par le GPSI, un identifiant du système 5G (voir le commentaire de l'art. 35, al. 1, let. d, ch. 2). La nouvelle possibilité ajoutée d'un « identifiant qui permette de demander les données d'identification selon l'art. 19, al. 2 » sert à l'identification des utilisateurs d'accès publics au réseau WLAN exploités à titre professionnel (voir le commentaire de l'art. 37, al. 1, let. b).

À l'*al. 2*, la phrase introductive précise désormais que la demande porte sur le contexte général de la traduction d'adresses de réseau, plutôt que sur une procédure de traduction en particulier, car les différentes traductions NAT sont les mêmes pour l'ensemble du contexte. La précision « à des fins d'identification » peut être omise ici puisqu'elle figure déjà à l'al. 1.

Avec les modifications à la *let. f*, le moment (désormais appelé moment déterminant) est redéfini. Selon l'arrêt du Tribunal administratif fédéral A-6807/2019 (ch. 4.5.1, p. 24), 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. 5, let. b, OSCPT) d'une manière qui lui permette d'identifier les utilisateurs à chacun des moments exigés par l'autorité dans sa demande et de fournir 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. Avec cette modification, le texte dit clairement que l'autorité qui demande les renseignements peut choisir n'importe quel moment, au début, au cours ou à la fin d'un contexte donné de traduction. 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.

Ce type de renseignements standardisé ne permet que des réponses univoques, c'est-à-dire qu'un seul identifiant peut être trouvé. Si la POC trouve plusieurs résultats valables, ceux-ci ne peuvent pas être fournis au titre de résultat de ce type de renseignements. Cette restriction est importante parce que ce type de renseignements ne permet pas d'évaluer la pertinence des différents résultats.

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

De nombreuses modifications mineures sont apportées à cette disposition, notamment pour en améliorer la lisibilité et la compréhension. À la différence de l'art. 38, qui traite des renseignements habituels relatifs à l'identification des abonnés dans le contexte d'une traduction d'adresses de réseau (NAT), cet article met l'accent sur les aspects très spécifiques de cette procédure NAT. Les spécialistes recourent à ce type de renseignements pour « retracer » (*backtracking*) les connexions au-delà de la frontière que constitue la procédure NAT. Des explications détaillées sur cette procédure figurent aux pages 43 et 44 du rapport explicatif du 15 novembre 2017 sur la révision totale de l'OSCPT.

La phrase introductive de l'*al. 1* précise désormais, comme le fait l'art. 38, que la demande porte sur le contexte général de la traduction d'adresses de réseau, plutôt que sur une procédure de traduction en particulier, car les différentes traductions NAT sont les mêmes pour l'ensemble du contexte. Les *let. a* et *b* restent inchangées.

À l'*al. 2*, comme à l'al. 1, le terme « procédure de traduction » est remplacé par celui de « contexte de la traduction » car les différentes traductions NAT sont les mêmes pour l'ensemble du contexte. L'al. 2 précise par ailleurs que la demande doit contenir non pas toutes les indications, mais uniquement celles qui sont connues. L'autorité qui fait la demande doit toutefois s'attendre à ce que le fournisseur ne puisse pas trouver le bon contexte de traduction si les informations fournies sont rudimentaires.

Le contenu matériel des *let. a à d* n'est en rien modifié, seul l'ordre des termes « avant » et « après » (let. a et b) est inversé pour correspondre au texte allemand. À la *let. e*, la précision « si nécessaire pour l'identification » est ajoutée, car l'enregistrement du type de protocole doit être limité au minimum nécessaire, pour des motifs de protection des données. À la *let. f*, le moment déterminant est précisé de la même manière qu'à l'art. 38, al. 2, let. f (voir le commentaire de cette disposition).

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

À l'*al. 1, let. b* et *c*, la précision de la période de validité est ajoutée concernant les autres adresses et coordonnées (voir le commentaire de 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 fourni, 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 (offres multi-appareils, multi-SIM), qui ont donc plus

d'un identifiant (par ex. MSISDN). Les autres identifiants à fournir sont indiqués au ch. 7.

Selon la *let. d, ch. 6*, la période de validité de chaque statut de service peut désormais être fournie, 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 (par ex. numéro de téléphone) ou les identifiants (par ex. numéro SIM « ICCID ») 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 en fonction de l'utilisation (données d'utilisation), ce n'est pas cette recherche qui est prévue mais la nouvelle décrite à l'art. 41. 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 le 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 2017. 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 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 les services de téléphonie et multimédia

En raison des nombreuses modifications qui y sont apportées, cet article est intégralement révisé afin d'en améliorer la lisibilité et la compréhension. L'actuelle deuxième phrase introductive de l'*al. 1* n'a plus lieu d'être puisque la fourniture de la période de validité est précisée, quand il y a lieu, pour chacune des indications.

L'*al. 1* a une nouvelle structure ne comprenant plus que deux lettres. La *let. a* reste inchangée. La *let. b* est *subdivisée en quatre chiffres* qui détaillent les indications à fournir pour chaque service. En effet, d'autres services peuvent être liés à celui sur lequel porte la demande. Dans la phrase introductive, le mot « associés » est ajouté pour exprimer que les ressources d'adressage et leurs 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). Le *ch. 1* reprend sur le principe l'actuelle let. b, avec désormais une distinction entre les ressources d'adressage publiques et privées, et l'indication de la période de validité (date de – à) pour chaque ressource d'adressage. Le *ch. 2* correspond sur le principe à l'actuelle let. d et règle les indications à transmettre concernant les équipements utilisés au cours des six derniers mois en lien avec chacun des services auprès du fournisseur. L'IMEI et le PEI sont mentionnés à titre d'exemples, comme à l'art. 36, al. 1, let. b, ch. 4. L'adresse MAC, plus rare, n'est plus dans les exemples mais fait encore partie des identifiants des équipements. Le *ch. 3* réunit les actuelles let. c (IMSI), e (ICCID) et f (PUK), en y ajoutant d'autres identifiants tels que le SUPI, le MSISDN, le GPSI et l'identifiant de l'eUICC, et leurs périodes de validité respectives, afin de donner aux autorités habilitées une meilleure compréhension de la chronologie des moyens d'accès (SIM) et des identifiants utilisés pour chaque service. Les deux nouveaux identifiants de la téléphonie mobile 5G sont ajoutés : le SUPI (voir le commentaire de l'art. 35, al. 1, let. d, ch. 10) et le GPSI (voir le commentaire de l'art. 35, al. 1, let. d, ch. 2). Le terme ICCID remplace celui de numéro SIM (voir le commentaire de l'art. 35, al. 1, let. d, ch. 9). Le *ch. 4* est nouveau et sert à savoir, dans le cas d'une offre multi-appareils, s'il s'agit de l'équipement principal ou d'un équipement secondaire.

À l'*al. 2, 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. Dans les *let. b et c* sont ajoutés des nouveaux identifiants du système 5G : le SUPI et le PEI (voir les commentaires respectivement de l'art. 35, al. 1, let. d, ch. 10 et de l'art. 36, al. 1, let. b, ch. 4). Les *let. d* et *e* restent inchangées. À la *let. f*, le numéro SIM (ICCID) est ajouté comme critère de demande (voir le commentaire de la même modification à l'art. 36, al. 2, let. e).

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

Comme pour les autres types de renseignements sur des services de communication (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). Une adaptation rédactionnelle est apportée au texte français de la phrase introductive de la let. c (« sur tout service »). 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 le 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. 43, al. 1 et let. c, phrases introductives et ch. 6, 2, phrase introductive et let. g, i et j, et 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). Une adaptation rédactionnelle est apportée au texte français de la phrase introductive de la let. c (« sur tout autre service »).

L'*al. 2, let. g*, prévoit désormais que la demande peut aussi être faite avec le 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 par exemple concerner un identifiant univoque spécifique à une application, qui sera indiqué ici. Cet identifiant est utilisé pour les notifications d'une application. Concrètement, il 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* est matériellement inchangé et correspond aux troisième et quatrième phrases de l'actuel al. 2.

Art. 44, al. 1, phrase introductive (ne concerne que le texte italien), let. c et f (ne concerne que le texte allemand), et 3, phrase introductive (ne concerne que le texte italien), let. c, d (ne concerne que le texte allemand) et f

À l'*al. 1, let. c et f*, de même qu'à l'*al. 3, let. c et d*, des adaptations rédactionnelles sont apportées au texte allemand pour répondre aux règles de la formulation non sexiste. Sur le fond, rien ne change.

À l'*al. 3*, une *let. f* est ajoutée pour permettre les demandes à partir des codes qui sont d'ordinaire 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. Ainsi ces demandes peuvent désormais être effectuées selon une procédure standardisée.

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

Cet article est intégralement révisé afin d'en améliorer la lisibilité et la compréhension. 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. La demande fondée sur l'identifiant de l'équipement (restreinte par la mention « le cas échéant ») n'est disponible que lorsque c'est le fournisseur qui a remis l'équipement en question et qu'il en a noté le numéro, ce qui n'est en général pas le cas pour les services de téléphonie mobile.

Art. 46, al. 1 (ne concerne que le texte allemand)

Le texte allemand de cet alinéa est adapté pour répondre aux règles de la formulation non sexiste.

Art. 47, al. 1 (ne concerne que le texte allemand) et 2

Le texte allemand de 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. La demande fondée sur l'identifiant

de l'équipement (restreinte par la mention « le cas échéant ») n'est disponible que lorsque c'est le fournisseur qui a remis l'équipement en question et qu'il en a noté le numéro, ce qui n'est en général pas le cas pour les services de téléphonie mobile.

Art. 48 Type de renseignements IR_21_TECH : données techniques

En raison des nombreuses modifications qui y sont apportées, cet article est intégralement révisé afin d'en améliorer la lisibilité et la compréhension. L'*al. 1* précise que cette demande de renseignements porte sur des éléments réseau « à la localisation indiquée dans la demande ». Il est également précisé que seuls sont concernés les accès publics au réseau WLAN « exploités à titre professionnel ». Le terme « point d'accès au réseau WLAN » est remplacé par le terme plus général d'« accès au réseau WLAN » (voir le commentaire du *remplacement d'expressions*, al. 1, au début de l'ordonnance).

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[23] (5G). Les trois exemples donnés pour une Area Identity (SAI[24], RAI[25] et TAI[26]) sont désormais couverts par le terme générique d'identifiant de zone géographique. Ces modifications rédactionnelles n'ont cependant aucune influence sur la fourniture des actuels CGI, ECGI, SAI, RAI et TAI. Lorsque c'est techniquement applicable, ils doivent être fournis comme auparavant.

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 réseau, 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 mettent donc 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

23 **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.

24 **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)

25 **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)

26 **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)

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[27] ne doive plus être fourni : s'il est connu, il doit l'être. Les *let. b, c et d* restent quasiment inchangées.

Une *let. e* est ajoutée car dans les réseaux 5G, les indications de localisation 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 « localisation » 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_51_ASSOC_PERM : renseignements sur les identifiants attribués pour une longue durée

Lors de la fourniture de services de télécommunication fondés sur l'architecture 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 fournir (art. 21, al. 1).

Art. 48b Type de renseignements IR_52_ASSOC_TEMP : renseignements immédiats sur les identifiants attribués pour une courte durée

Selon l'*al. 1*, il est possible d'utiliser, lors de la fourniture de services de téléphonie mobile 5G, 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 quasi réel les identifiants permanents associés à un identifiant temporaire. Cela signifie que la réponse doit généralement être fournie en une fraction de seconde. Il n'est pas nécessaire de conserver ces données.

L'*al. 2* définit les indications qui doivent figurer dans la requête. Comme les identifiants temporaires ne peuvent être attribués de manière univoque qu'à l'intérieur d'une

27 **BSSID** (*Basic Service Set Identifier*) : élément (adresse MAC) qui identifie l'accès au réseau WLAN.

zone de téléphonie mobile donnée, celle-ci doit impérativement être précisée. Les détails techniques sont définis dans l'annexe 1 de l'OME-SCPT.

Pour la technologie 5G, l'exemple suivant est un cas d'application important : dans le cadre de l'utilisation d'un dispositif technique spécial selon l'art. 269bis CPP, une autorité intercepte, grâce à un dispositif technique (par ex. une fausse station de base), un identifiant temporaire (par ex. le 5G-GUTI ou le SUCI). Elle fait une demande de ce nouveau type pour obtenir immédiatement l'identifiant permanent correspondant (par ex. un SUPI).

Le temps de réponse à ce nouveau type de renseignements doit être très court (quasiment en temps réel), car les identifiants temporaires changent fréquemment. Ce renseignement doit donc être demandé et fourni de manière automatisée via une nouvelle interface de consultation. Une requête peut porter simultanément sur plusieurs identifiants. S'agissant d'une consultation en temps quasi réel, il n'est pas possible d'indiquer un moment particulier : c'est le moment de la requête qui est déterminant, avec une brève marge technique de tolérance. Il n'est pas possible d'effectuer des recherches au-delà de cette période, ni dans le passé ni dans le futur.

Art. 48c Type de renseignements IR_53_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. Il 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 ou l'adresse de l'expéditeur sont usurpés ou inconnus, les autorités ont besoin d'un moyen pour retracer l'appel ou la communication.

L'*al. 1* règle les indications à fournir. Le fournisseur doit donner la dénomination du réseau immédiatement voisin « de » et du réseau immédiatement voisin « vers » sur la voie de communication, lorsque ces réseaux ont participé à la communication ou tentative d'établissement de la communication. Il ne doit cependant pas fournir d'indication sur des réseaux plus éloignés dans la chaîne de communication. Supposons qu'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 comme réseaux voisins 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 ». Le fournisseur peut se contenter de fournir ses appellations internes usuelles, par exemple un *Inter Operator Identifier* qui désigne un fournisseur donné ou l'adresse IP du réseau voisin.

L'*al. 2* définit les critères à indiquer dans la demande afin d'identifier clairement la communication ou la tentative d'établissement de la communication en question.

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. 5, let. c, et art. 61, let. j) pour les FST ayant des obligations complètes 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 délais de traitement sont fixés à l'art. 14 de l'OME-SCPT.

Art. 50, al. 1 et 5 à 9

De la même manière qu'à l'art. 18 (obligations concernant la fourniture de renseignements), l'*al. 1* est complété pour préciser les obligations concernant l'exécution des nouveaux types de surveillances introduits par les art. 56*a*, 56*b*, 67, let. b et c, et 68, al. 1, let. b et c. La *deuxième phrase* exempte les FSCD ayant des obligations étendues en matière de surveillance (art. 52) de ces obligations. La question de savoir si ces surveillances devront à l'avenir également être exécutées par les FSCD sera tranchée dans le cadre de la deuxième révision de l'OSCPT, lorsqu'une description plus précise des catégories FST et FSCD sera appliquée. La présente révision n'impose donc pas de nouvelles obligations aux FSCD en lien avec ces nouveaux types de surveillance.

L'*al. 5* est modifié pour que la POC doive apporter son soutien au Service SCPT lorsque celui-ci le demande (plutôt que « si nécessaire »).

L'*al. 6* règle la manière de procéder pour les identifiants associés au début de la surveillance, de la recherche en cas d'urgence ou de la détermination de la position, tandis que l'al. 9 traite le cas d'identifiants associés qui viennent s'ajouter pendant une surveillance en temps réel active ou une détermination périodique de la position. 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 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 la position, recherche en cas d'urgence, recherche de personnes condamnées). Si par exemple le MSISDN ou l'IMSI d'un abonnement est surveillé, tous les numéros principaux et secondaires de cet abonnement doivent être surveillés et, par conséquent, tous les appareils associés, tels que les montres connectées, qui utilisent les numéros de téléphone ou les SIM associés à cet abonnement. Sont exclus les identifiants de cible secondaires avec lesquels il n'est pas possible de communiquer (par ex. numéros techniques) et d'autres numéros d'appareils si l'identifiant de la cible est lui-même un numéro d'appareil (c.-à-d. que si le numéro d'appareil x est surveillé, d'autres numéros d'appareils qui lui sont éventuellement indirectement liés via l'abonnement utilisé ne doivent pas être surveillés). Aucun émolument supplémentaire n'est dû et aucune indemnité

supplémentaire n'est versée pour les équipements terminaux, numéros ou cartes SIM supplémentaires. Si cela est nécessaire pour mettre la surveillance en place, le fournisseur peut demander au Service SCPT des numéros d'identification administratifs supplémentaires de la surveillance (LIID : Lawful Interception Identifier). 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.

À l'*al. 7*, 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[28], le HSS[29] et l'UDM[30], aux fins de la saisie et de la fourniture 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. 8* prévoit que dans l'architecture 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. 9* prévoit que la POC doit observer d'éventuelles modifications et en particulier l'ajout de nouveaux équipements terminaux multi-appareils, numéros ou SIM pour un service surveillé. Elle doit de sa propre initiative adapter la surveillance à ces changements et, le cas échéant, l'étendre aux nouveaux identifiants cibles. 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 (voir le commentaire de l'al. 6).

Art. 53 Accès aux installations

L'*al. 1* précise que même les POC qui ne sont tenues que de 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 la qualité d'une surveillance en cours, même si elle est mise en œuvre techniquement par le Service SCPT.

L'*al. 2* est identique à l'actuel al. 2, hormis une adaptation rédactionnelle dans la deuxième phrase (« en accord avec » au lieu de « en collaboration avec »).

28 **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.

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

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

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

En raison des nombreuses modifications qui y sont apportées, cet article est intégralement révisé afin d'en améliorer la lisibilité et la compréhension. La technologie 5G permet des accès multiples au réseau (*multiple registrations*) et des raccordements multiples (*multiple attachments*) dans le même réseau ou dans des réseaux fournisseurs de services différents, ce qui permet également à la cible de la surveillance de changer de réseau ou de technologie[31].

L'*al. 1* reste inchangé.

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.

La *let. b* reste inchangée.

Aux *let. c* et *e*, la précision « dans le cas de la téléphonie mobile » est supprimée. Comme tout l'article concerne maintenant la téléphonie mobile, elle est redondante.

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. b, ch. 4 pour le PEI).

À la *let. d*, l'ajout « et aux équipements terminaux surveillés » vise à préciser que doivent également être fournies les adresses IP attribuées aux autres appareils d'une offre multi-appareils. La mention des plages d'adresses IP est supprimée, car elle n'est pas pertinente ici.

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 considérées comme des modifications des caractéristiques techniques par exemple :

- la modification du service support ;
- des modifications du PDP Context, du Bearer ou de la PDU Session ;
- les informations de signalisation NAS de la cible ;
- l'actualisation de la position de la cible, par exemple *Location Update* et *Mobility Registration Update*.

Les informations de signalisation NAS sont échangées via l'interface NAS (*Non-Access Stratum*) entre l'équipement terminal et le cœur du réseau de téléphonie mobile.

31 Cf. 3GPP TS 33.501, ch. 6.3.2

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 informations 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 transmises, 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 savoir dans quelle mesure elles peuvent se fier à ces indications de localisation. La disposition prévoit par ailleurs que les données de localisation de la cible provenant des informations de signalisation NAS doivent désormais également être fournies. Les systèmes de téléphonie mobile de quatrième génération (EPS) et de cinquième génération (5GS) ont parfois un timbre horodateur et des indications sur l'âge des données de localisation. Ces timbres horodateurs et ces indications doivent dès lors également être fournies. On entend par l'âge des données de localisation le temps qui s'est écoulé entre le moment où cette localisation a été déterminée et le moment où l'indication a été transmise.

Les *let. i à k* règlent la fourniture de données secondaires importantes qui peuvent être saisies lors de la surveillance de bases de données techniques d'usagers telles que le HLR, le HSS et l'UDM (voir le commentaire de l'art. 50, al. 7).

La *let. i* concerne les 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).

La *let. j* concerne :

- les 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 ;* il s'agit en particulier de fournir des identifiants temporaires, même s'ils n'ont qu'une brève durée de vie ;
- les informations sur des événements relatifs à la localisation et, le cas échéant, sur leur motif (par ex. événements de type *register location* / *cancel location* / *register termination*) ;
- les informations sur le changement de l'élément réseau fournissant le service (par ex. SGSN, MME, MSC, AMF) ;
- les 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 la *let. k*, une disposition est ajoutée qui ne concerne que la technologie 5G et qui prévoit que les informations sur l'attribution d'un nouvel identifiant temporaire de la cible doivent également être fournies. Cette disposition concerne en particulier la dissimulation (*concealing*) d'identifiants d'usagers (par ex. SUCI en lieu et place du SUPI). Les identifiants temporaires doivent être fournis à chaque réattribution, même s'ils n'ont qu'une brève durée de vie.

À l'*al. 3* une modification rédactionnelle est apportée : le terme « type de technologie de communication mobile » (utilisé précédemment dans les let. a à c) est remplacé par celui plus général de « technologie d'accès au réseau », parce que les technologies d'accès non 3GPP (par ex. les accès WLAN) sont également concernées. À la *let. a*, c'est désormais le terme général d'identifiant de cellule ou de zone géographique qui est utilisé, comme à l'art. 48, al. 2, let. a (voir le commentaire s'y rapportant). Un nouveau cas est ajouté, celui de l'utilisation par la cible d'un groupe de cellules (« *combined cell* », cellule de téléphonie mobile composée de plusieurs antennes disséminées géographiquement). En raison de la complexité de cette disposition, nous renvoyons à ce sujet à l'annexe 1 de l'OME-SCPT. Les indications de localisation dans le cas d'un accès au réseau WLAN (désormais : accès non 3GPP) ne sont plus réglées ici mais à la nouvelle let. d. La *let. b* reste inchangée sur le fond. Les indications de localisation pour les accès au réseau WLAN disparaissent également de la *let. c*, vu qu'elles sont maintenant traitées à la let. d. Enfin la *let. d* précise donc les informations de localisation à fournir dans le cas d'un accès non 3GPP au cœur du réseau de téléphonie mobile. Il y a deux cas de figure : le ch. 1 pour les accès au réseau WLAN et le ch. 2 pour les accès via le réseau fixe.

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

En raison des nombreuses modifications qui y sont apportées, cet article est intégralement révisé afin d'en améliorer la lisibilité et la compréhension. L'actuel al. 1 est scindé en deux.

L'*al. 1* correspond à l'actuel al. 1, première phrase.

La phrase introductive de l'*al. 2* correspond à l'actuel al. 1, deuxième phrase. La *let. a* est inchangée et correspond à l'actuel al. 1, let. a. À la *let. b*, l'expression « services de téléphonie mobile » remplace celle de « téléphonie mobile » et un nouvel identifiant du système 5G, le SUPI, est ajouté à l'IMSI (voir le commentaire de l'art. 35, al. 1, let. d, ch. 10). Le contenu de l'actuelle let. b^{bis} est ajouté à la fin de la let. b sans modification. Les *let. c* et *d* sont inchangées et 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.

À la *let. e*, le terme de « technologie d'accès au réseau » remplace celui de « technologie de télécommunication mobile », puisque le passage de la cible à un accès non 3GPP doit également être signalé. Les *ch. 1 à 9* correspondent aux chiffres de l'actuelle let. e de l'al. 1, avec les modifications suivantes : au *ch. 2*, l'adjectif « respectif » est ajouté pour préciser que c'est bien le rôle de chacun des participants qui doit être indiqué. Le GPSI, un identifiant de la 5G, est en outre ajouté (voir le commentaire de l'art. 35, al. 1, let. d, ch. 2). Au *ch. 4*, l'identifiant de la 5G PEI est ajouté (voir le commentaire de l'art. 36, al. 1, let. b, ch. 4). Au *ch. 9*, le peu courant « services mobiles » est remplacé par « services de téléphonie mobile ». Il est aussi précisé que les données de localisation de la cible doivent dans la mesure du possible être déterminées par le réseau et signalées comme telles (déterminées par le réseau / pas déterminées par le réseau ; voir le commentaire de l'art. 54, al. 2, let. h). Il est précisé que les données de localisation sont les données « actuelles ». Un renvoi à l'art. 54, al. 3 est ajouté

pour une description plus détaillée des données de localisation, de sorte que l'actuel al. 2 n'a plus de raison d'être. La cible pouvant utiliser plusieurs cellules simultanément, ce terme est désormais au pluriel. L'expression « point d'accès au réseau WLAN » est remplacée par le terme plus universel d'« accès non 3GPP ». Il est enfin précisé que les données de localisation de la cible provenant des informations de signalisation NAS doivent également être fournies. Pour l'EPS et la 5GS, les données de localisation doivent être complétées, si ces données sont disponibles, par le timbre horodateur associé ou l'âge des données (voir le commentaire de l'art. 54, al. 2, let. h).

Une nouvelle *let. f* est ajoutée pour régler la fourniture de données secondaires importantes qui peuvent être saisies lors de la surveillance de bases de données techniques d'usagers telles que le HLR, le HSS et l'UDM (voir le commentaire de l'art. 50, al. 7 et art. 54, al. 2, let. i, j et k).

Art. 56a Type de surveillance RT_54_POS_ONCE : détermination unique et immédiate de la position par le réseau

La détermination de la position selon la LSCPT (LALS, *Lawful Access to Location Services*) est une nouvelle fonction de la téléphonie mobile introduite dans l'ordonnance. Elle est considérée comme une surveillance au sens de l'art. 269 CPP, ce qui signifie qu'elle n'est possible que dans les conditions strictes prévues pour les surveillances en temps réel. Cette disposition règle le premier type de surveillance par LALS : la détermination unique (« ONCE ») 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 information*). On entend désormais par *localisation* l'emplacement des antennes des cellules qui ont fourni le service, si possible enrichie par d'autres indications comme la principale direction d'émission de l'antenne. Cette localisation n'est en général qu'une approximation grossière de l'endroit où se trouve effectivement la cible (équipement terminal). La cellule qui fournit le service est celle où se situe l'antenne à laquelle la cible est connectée ou était connectée en dernier. Plus la portée de l'antenne est grande, plus l'écart peut être grand entre l'emplacement réel de la cible et la localisation indiquée. En milieu rural, l'écart entre l'emplacement de l'antenne et l'emplacement effectif de la cible peut atteindre trente kilomètres. Dans des cas extrêmes, dans une zone montagneuse, l'écart peut être encore bien plus important. Lors de surveillances en temps réel, la localisation actuelle de la cible est indiquée en continu. Pour les surveillances rétroactives, les indications de localisation sont données pour le début et pour la fin de la communication ou de la session d'accès au réseau. Il est par ailleurs possible de demander individuellement la dernière localisation connue de la cible par une recherche en cas d'urgence EP_35_PAGING ou une surveillance 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. Deux types de surveillance relatifs à la détermination de la position par LALS sont introduits dans l'ordonnance :

1) la détermination unique et immédiate de la position (selon le présent article),

2) la détermination périodique et récurrente 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. Lorsque l'identifiant surveillé est un numéro d'appareil, seul cet appareil est concerné. Mais lorsque l'identifiant surveillé est une ressource d'adressage (par ex. MSISDN/GPSI) ou un numéro d'identification d'un usager (par ex. IMSI/SUPI), plusieurs équipements terminaux tels que smartphones, tablettes et montres connectées peuvent être utilisés avec la relation commerciale en question (abonnement ou prépaiement), en particulier dans les offres avec plusieurs cartes SIM. Comme on ne sait généralement pas quel appareil la personne surveillée a avec elle à un moment donné, il convient de déterminer les positions respectives de tous les appareils actuellement associés (voir aussi le commentaire de l'art. 50, al. 6).

Selon l'*al. 2*, les prescriptions techniques de mise en œuvre sont édictées par le DFJP dans l'OME-SCPT et son annexe 1. Il n'y a pas encore d'expérience pratique de cette nouvelle détermination unique et immédiate 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.

L'*al. 3* précise les indications à fournir. 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 fournies si elles sont disponibles.

Selon la *let. d*, le motif de l'échec (code d'erreur) doit être communiqué lorsque la position n'a pas pu être déterminée. Pour que l'autorité qui a émis l'ordre reçoive au moins les données de localisation, en cas d'échec de la détermination de la position, un scénario de repli est prévu sous forme d'un *paging* au sens de l'art. 63.

Art. 56b Type de surveillance RT_55_POS_PERIOD : détermination périodique et récurrente de la position par le réseau

Les remarques introductives faites dans le commentaire de l'art. 56*a* valent également pour le présent article, qui traite du deuxième type de surveillance LALS : la détermination périodique et récurrente de la position par le réseau (« PERIOD »).

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). La position de tous les équipements terminaux associés à l'identifiant surveillé doit être déterminée (voir le commentaire de l'art. 56*a*, al. 1).

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 de temps fixes prédéterminés. Par manque d'expérience pratique avec cette nouvelle fonction LALS pour déterminer la position de chaque équipement terminal de manière périodique et récurrente, 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*, le motif de l'échec (code d'erreur) doit être communiqué lorsque la position n'a pas pu être déterminée. L'exécution de ce type de surveillance est automatisée, de sorte qu'un scénario de repli, comme prévu à l'art. 56*a*, n'est pas possible ici en l'état actuel des connaissances.

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

En raison des nombreuses modifications qui y sont apportées, cet article est intégralement révisé afin d'en améliorer la lisibilité et la compréhension. Les *let. a* à *c* et *j* (anciennement i) restent matériellement inchangées. La let. c subit une légère adaptation rédactionnelle.

À la *let. d*, le terme « plages d'adresses » est supprimé. Il s'agit ici de l'adresse IP effectivement attribuée à la cible à ce moment-là. Sont ajoutées les indications pour un accès non 3GPP, puisque l'accès au cœur du réseau de téléphonie mobile peut aussi se faire autrement que par une antenne de téléphonie mobile (accès 3GPP), par exemple via le réseau WLAN du domicile ou un réseau WLAN public. Si aucune antenne de téléphonie mobile n'est impliquée, les données de localisation de celle-ci n'ont plus lieu d'être (let. g). La localisation de l'accès est possible via cette adresse IP source et numéro de port.

Dans les *let. e* et *f*, la restriction « si ces données sont disponibles » est supprimée, car ces paramètres sont obligatoires. Par ailleurs, dans les *let. e* et *g*, le terme « téléphonie mobile » est remplacé par « services de téléphonie mobile ».

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. b, ch. 4 pour le PEI).

À la *let. g* 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 fournis. Les différentes indications de localisation ne sont plus décrites à cette lettre, car elles sont désormais trop complexes pour ce format. En lieu et place, il est fait référence aux règles pertinentes du DFJP, qui se trouvent à l'annexe 1 de l'OME-SCPT.

À la *let. h*, il est précisé que la disposition ne vaut que pour les accès publics à un réseau WLAN exploité à titre professionnel. Compte tenu de l'expérience de la pratique, la possibilité est ajoutée d'indiquer une autre désignation appropriée, telle que le « nom de la zone d'accès sans fil », au lieu d'un identifiant. Une désignation suffisamment précise de l'accès au réseau WLAN suffit, ce qui signifie que la désignation

fournie doit désigner l'accès au réseau sur place de manière suffisamment précise (voir aussi le commentaire de l'art. 48, al. 2, let. a).

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.

Art. 61, phrase introductive, 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. b, ch. 4 pour le PEI).

À la *let. g*, les descriptions détaillées des différentes indications de localisation sont abandonnées, car elles sont désormais trop complexes pour ce format. En lieu et place, il est fait référence aux règles pertinentes du DFJP, qui se trouvent à l'annexe 1 de l'OME-SCPT.

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. Le *ch. 4* renvoie aux règles pertinentes du DFJP, c'est-à-dire à l'annexe 1 de l'OME-SCPT.

Selon la *let. j*, les indications sur les réseaux immédiatement voisins sur la voie de communication, c'est-à-dire le réseau d'où proviennent les données (« de ») et celui vers lequel elles vont (« vers ») doivent également être fournies 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 et l'exemple de l'art. 48*c*). Cela peut être utile, notamment 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'autres indications pour retracer le chemin de l'appel ou de la communication en amont ou en aval.

Pour obtenir des informations fiables, comme chaque fournisseur ne peut contrôler que ses propres interfaces avec le réseau, le fournisseur ne doit conserver que les indications sur le réseau immédiatement voisin « de » et sur le réseau immédiatement voisin « vers », lorsque ces réseaux ont participé à la communication ou tentative d'établissement de la communication. Ces données secondaires doivent être conservées pendant six mois (art. 26, al. 5, LSCPT), uniquement par les fournisseurs ayant des obligations en matière de surveillance.

Les fournisseurs ne sont en particulier pas tenus de conserver des indications sur des réseaux plus éloignés dans la voie de communication. Ils doivent cependant fournir, sur demande, les autres données secondaires dont ils disposent (art. 26, al. 6, art. 27, al. 2, art. 28, al. 2, et art. 29, al. 2, LSCPT). Ces données supplémentaires ne font pas partie de ce type de surveillance standardisée. Elles peuvent être demandées au titre d'une surveillance spéciale selon l'art. 25 OSCPT.

La fourniture d'informations sur les réseaux immédiatement voisins 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 celle de l'art. 56, al. 2, let. e.

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

Cet article est intégralement révisé afin d'en améliorer la lisibilité et la compréhension. À la *let. a*, les numéros de port sont ajoutés aux adresses IP, afin que l'identification de ces serveurs et clients soit possible même dans les cas de traduction d'adresses de réseau (NAT).

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 ayant des obligations complètes et les FSCD ayant des obligations étendues en matière de surveillance (art. 52). Toutes les autres POC ne fournissent que les données dont elles disposent.

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

En raison des nombreuses modifications qui y sont apportées, cet article est intégralement révisé afin d'en améliorer la lisibilité et la compréhension. 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 l'emplacement de la dernière activité. Par ailleurs, il est maintenant question des équipements terminaux mobiles, au pluriel, car la localisation de la dernière activité doit être déterminée pour tous les appareils (pas uniquement pour un seul) associé à l'identifiant surveillé (voir le commentaire de l'art. 56*a*, al. 1).

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). La *let. h* renvoie par ailleurs aux règles pertinentes du DFJP, c'est-à-dire à l'annexe 1 de l'OME-SCPT.

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). Il est également précisé que seuls sont concernés les accès

publics au réseau WLAN « exploités à titre professionnel ». 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).

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

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

En raison des nombreuses modifications qui y sont apportées, cet article est intégralement révisé afin d'en améliorer la lisibilité et la compréhension. La disposition est structurée différemment. 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. offres 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 de la personne disparue ou de tiers. Cette précision concerne principalement les abonnements mobiles avec carte SIM supplémentaire (offres multi-appareils ou multi-SIM, voir aussi le commentaire de l'art. 56*a*, al. 1). 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 fournissent 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_56_POS_ONCE 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_54_POS_ONCE (voir aussi le commentaire de l'art. 56*a*).

La *let. c* introduit elle aussi un nouveau type de recherche, le type EP_57_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_55_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 détermination de la position plus 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 approprié 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). Voici un 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 à 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 et où il n'y a dès lors pas de données actuelles disponibles. 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 (voir le commentaire de l'art. 50, al. 6). Les règles usuelles pour les surveillances rétroactives s'appliquent (pas de mandat de levée de la mesure, le début et la fin de la surveillance sont définis selon l'art. 4*a*). 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. b, ch. 4 pour le « PEI »).

Art. 68 Recherche de personnes condamnées

Cet article est intégralement révisé afin d'en améliorer la lisibilité et la compréhension. 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 localisation 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).

Les autres lettres demeurent inchangées, elles sont simplement décalées (la *let. a* devient la *let. d*, … et la *let. d* 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. 74b **Dispositions transitoires relatives à la modification du 25 octobre 2023**

Pour que l'introduction des nouveaux types de surveillances et de renseignements se passe bien tant pour les FST que pour le Service SCPT, il est judicieux de prévoir des dispositions transitoires détaillées pour les différentes modifications. Des délais sont impartis aux FST et au Service SCPT pour qu'ils procèdent aux adaptations techniques requises et effectuent les tests nécessaires, pour 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. Des

délais de transition ne sont pas nécessaires pour les FSCD, car les nouveaux types de renseignements et de surveillances ne concernent que les FST. Les FSCD en sont explicitement exemptés (voir les commentaires des art. 18, al. 4 et 50, al. 1).

L'*al. 1* prévoit pour tous les FST un délai de transition de 24 mois à partir de l'entrée en vigueur de l'ordonnance révisée pour les nouveaux types de renseignements visés à l'art. 48*a* (IR_51_ASSOC_PERM : renseignements sur les identifiants attribués pour une longue durée) et à l'art. 48*c* (IR_53_TEL_ADJ_NET : détermination des réseaux voisins de services de téléphonie et multimédia). Il convient de noter que les FST ayant des obligations restreintes en matière de surveillance (art. 51) ne sont pas tenus de conserver les données secondaires nécessaires pour répondre aux demandes selon l'art. 48*c*. Ils répondent dès lors aux demandes fondées sur cette article avec les informations dont ils disposent. S'ils fournissent ces informations en dehors du système de traitement, l'adaptation de leurs systèmes ne leur demandera presque aucun effort.

L'*al. 2* ne fixe pas de délai transitoire en mois mais dispose que la disponibilité à fournir les renseignements visés doit être effective dès l'introduction commerciale d'un service utilisant la nouvelle fonction de la 5G qui dissimule les identifiants permanents des usagers sur l'interface radio de l'accès mobile au réseau (accès 3GPP). Sont concernés les opérateurs de téléphonie mobile qui exploitent un réseau 5G. Ils devront être en mesure d'exécuter le nouveau type de renseignements selon l'art. 48*b* (IR_52_ASSOC_TEMP : renseignements immédiats sur les identifiants attribués pour une courte durée) dès la mise en service commerciale de leur premier accès au réseau dissimulant les identifiants permanents sur l'interface radio, ce qui sera possible avec la technologie 5G autonome (5G *standalone*). En d'autres termes, ce n'est qu'une fois qu'un fournisseur utilisera effectivement cette nouvelle fonctionnalité de la 5G qu'il devra assurer la transmission automatique des informations visées à l'art. 48*b*. Cet alinéa ne concerne que les FST ayant des obligations complètes. Les FST ayant des obligations restreintes en matière de surveillance (art. 51) sont exemptés de ce type de renseignements (voir art. 18, al. 4).

L'*al. 3* prévoit pour la mise en œuvre des deux nouveaux types de détermination unique et immédiate de la position selon les art. 56*a* (RT_56_POS_IMMED) et 67, let. b (EP_58_POS_IMMED) un délai transitoire de 24 mois, comme à l'al. 1. 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. Cet alinéa ne concerne que les FST ayant des obligations complètes. Les FST ayant des obligations restreintes en matière de surveillance (art. 51) ne sont pas tenus d'exécuter les surveillances standardisées (voir art. 50, al. 1).

L'*al. 4* 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 FST ayant des obligations complètes ont 18 mois à compter de l'entrée en vigueur de l'ordonnance révisée pour assurer la conservation des données nécessaires et 24 mois pour être en mesure de fournir rétroactivement ces données. L'obligation de conservation commence six mois avant l'obligation de fourniture, pour que les données historiques des six derniers mois soient bel et bien disponibles dès le début de l'obligation de fourniture. Cet alinéa ne concerne que les FST ayant des obligations

complètes. Les FST ayant des obligations restreintes en matière de surveillance (art. 51) ne sont pas tenus d'exécuter les surveillances standardisées (voir art. 50, al. 1).

L'*al. 5* définit le délai transitoire accordé aux FST ayant des obligations complètes pour les deux nouveaux types de détermination périodique de la position selon les art. 56*b* (RT_55_POS_PERIOD) et art. 67, let. c (EP_57_POS_PERIOD). Mettre en œuvre ces deux nouveaux types de surveillances dans le composant actuel de surveillance en temps réel (ISS) 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. La faisabilité d'une mise en œuvre dans le composant actuel n'est en outre pas garantie, car le fabricant n'en développe plus cette version. 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 (« FLICC[32] 2.0 »), pour adapter leurs systèmes et effectuer les tests requis avec le Service SCPT. Cet alinéa ne concerne que les FST ayant des obligations complètes. Les FST ayant des obligations restreintes en matière de surveillance (art. 51) ne sont pas tenus d'exécuter les surveillances standardisées (voir art. 50, al. 1).

L'*al. 6* est le pendant des al. 1, 3 et 4 et donne un même délai transitoire de 24 mois, à compter de l'entrée en vigueur de l'ordonnance révisée, au Service SCPT concernant les types de renseignements et de surveillances visés (voir al. 1, 3 et 4). La *let. a* porte sur la mise en œuvre des deux nouveaux types de renseignements visés aux art. 48*a* et 48*c* dans l'IRC et sur la mise en œuvre dans le nouveau composant de surveillance en temps réel du système de traitement du Service SCPT des deux nouveaux types de surveillances de la détermination unique et immédiate de la position par le réseau selon l'art. 56*a* (RT_54_POS_ONCE) et l'art. 67, let. b (EP_56_POS_ONCE), afin que les mandats puissent être transmis et les données visualisées par les utilisateurs. En outre, les renseignements et surveillances concernés doivent pouvoir être saisis dans les statistiques du Service SCPT. La *let. b* fixe, en se calquant sur l'al. 4, un délai de 24 mois au Service SCPT pour être en mesure de réceptionner les données historiques.

L'*al. 7* donne au Service SCPT le même délai que l'al. 2 (art. 48*b*) pour adapter son système de traitement et être en mesure de recevoir les données visées en temps quasi réel et de saisir les renseignements dans ses statistiques.

L'*al. 8* est le pendant de l'al 5 (art. 56*b* et 67, let. c) et fixe au Service SCPT un délai identique.

Annexe

Concernant les définitions et les abréviations, certaines qui étaient obsolètes sont supprimées, de nouvelles sont ajoutées et quelques précisions ont ponctuellement été ajoutées aux définitions existantes. Les définitions et abréviations étant classées dans

32 Federal Lawful Interception Core Component (FLICC)

l'ordre de leur première apparition dans l'ordonnance, la numérotation a dû être un peu adaptée.

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

Remplacement d'expressions

Les abréviations FST et FSCD sont également employées dans l'OME-SCPT, les dispositions concernées sont adaptées en conséquence.

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 les autorités (selon l'art. 1, al. 2, let. a à f, OSCPT) et le Service SCPT. La disposition est également applicable à la communication sécurisée entre le Service SCPT et les POC (selon l'art. 2) et, le cas échéant, entre les autorités et les personnes obligées de collaborer. Sont considérés des moyens de communication sûrs le système de traitement du Service SCPT (*let. a*) et les solutions de cryptage de courriels (*let. b*) définies plus en détail dans l'annexe 1 de l'OME-SCPT. Après concertation 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. 2bis

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 des télécommunications (art. 16, al. 1, 17, al. 1 et 18, al. 1) sont repris dans ce nouvel alinéa pour les surveillances du courrier postal. Le délai pour la transmission au fournisseur de services postaux 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 Surveillance rétroactive

Le nouvel *al. 1* fixe, par analogie avec les art. 10, al. 2bis, 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. 2bis).

L'*al. 2* correspond à l'actuel art. 11.

Art. 14, al. 2, 3 et 4

L'*al. 2* définit les délais de traitement que doivent respecter différentes catégories de POC : les FST, à l'exception de ceux qui ont des obligations restreintes en matière de surveillance (art. 51 OSCPT), les FSCD ayant des obligations étendues en matière de fourniture de renseignements (art. 22 OSCPT) et les FSCD ayant des obligations étendues en matière de surveillance (art. 52 OSCPT). Une restriction est apportée par la précision que les règles ne s'appliquent que dans la mesure où les POC sont tenues de fournir des renseignements selon l'art. 18 OSCPT. En vertu de l'art. 18, al. 4, OSCPT, les FSCD ayant des obligations étendues selon les art. 22 ou 52 OSCPT sont dispensés des trois nouveaux types de renseignements définis dans les art. 48*a* à 48*c* OSCPT.

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 fractions de seconde), car les identifiants temporaires changent fréquemment. Ce renseignement doit donc être demandé et fourni de manière automatisée via une nouvelle interface de consultation. 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 convient de souligner que les FST ayant des obligations restreintes en matière de surveillance, comme l'indique la phrase introductive, de même que les FSCD ayant des obligations étendues selon les art. 22 ou 52 OSCPT, pour des raisons de proportionnalité, sont dispensés de fournir des renseignements selon l'art. 48*b* OSCPT (voir art. 18, al. 3 et 4, OSCPT). La let. a ne leur est donc pas applicable.

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 fournis 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 rel. avec art. 35), IR_6_NA (art. 36), IR_7_IP (art. 37), IR_10_TEL (art. 40), IR_11_TEL_FLEX (art. 27, en rel. avec art. 40), IR_12_TEL (art. 41). Le délai d'une heure vaut aussi pour le nouveau type de renseignements selon l'art. 48*a* (IR_51_ASSOC_PERM : renseignements sur les identifiants attribués pour une longue durée). Il convient de noter qu'en cas de demandes de renseignements automatisées, une annonce du Service SCPT dans le cadre du service de piquet n'est pas nécessaire.

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, comme c'est déjà le cas, les types de renseignements « manuels » suivants : IR_8_IP (NAT) (art. 38), IR_9_NAT (art. 39), IR_15_COM (art. 43), IR_16_COM_FLEX (art. 27, en rel. avec art. 43). Ce délai d'un jour ouvré ou de six heures s'appliquera également aux types de renseignements IR_13_EMAIL (art. 42) et IR_14_EMAIL_FLEX (art. 27, en rel. avec art. 42) – pour lesquels le délai était précédemment d'une heure (voir actuel art. 2, let. a) –, parce que ces renseignements peuvent désormais être livrés manuellement (voir commentaire de l'art. 18, al. 2, OSCPT). S'y ajoute le nouveau type de renseignements IR_53_TEL_ADJ_NET (détermination des réseaux voisins 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* en cas de demandes portant sur ces types de renseignements en dehors des heures normales de travail ou les jours fériés. Ce délai de six heures correspond à celui des surveillances rétroactives déclarées urgentes. La pratique montre que seul un faible nombre de demandes de renseignements et d'ordres de surveillances sont transmis pendant le service de piquet, mais ces mandats sont urgents et ne peuvent être mis en attente jusqu'au jour ouvré suivant. Cette disposition ne devrait donc pas entraîner de 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 de travail ordinaires, afin de ne pas entraver les investigations de la police et la poursuite pénale. Il convient de souligner que le ch. 2 ne s'applique qu'aux POC qui sont tenues, en vertu de l'art. 11 OSCPT, al. 1, de mettre en place un service de piquet, ce qui n'est pas le cas des FST ayant des obligations restreintes en matière de surveillance (art. 51 OSCPT) ou des FSCD ayant des obligations étendues en matière de fourniture de renseignements (art. 22 OSCPT). Le ch. 2 de la let. a ne leur est donc pas applicable.

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 le composant IRC (voir commentaire de l'art. 18 OSCPT) 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 concernant des demandes selon la let. c :

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 fournir 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. La demande étant faite en dehors des heures de travail ordinaires, l'autorité qui en est à l'origine doit aviser le Service SCPT si elle souhaite que sa demande soit traitée dans le cadre du service de piquet. Si tel est le cas, le Service SCPT en informe immédiatement la POC, qui dispose alors d'un délai de six heures à compte de la réception du mandat pour y répondre, soit jusqu'à 23 h 05 le jour même.

Exemple 3 : Lorsqu'une demande de renseignements est transmise le samedi à 18 h 50 (en dehors des heures ordinaires 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.

En cas de procédure manuelle, le délai de réponse est également d'un jour ouvré pour les renseignements cités à la let. d. Comme ces renseignements prévus aux art. 44 à 48 ne doivent pas obligatoirement être livrés dans le cadre d'un service de piquet, ils sont traités séparément plutôt que d'être inclus dans la let. c. Pour les renseignements 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), le délai de réponse reste le même que dans l'actuel art. 14, al. 2, let. b.

L'*al. 3* règle les délais de traitement pour les « petites » POC que sont 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 fournir 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 se conformer aux types standardisés prévus dans l'OSCPT (art. 18*a* OSCPT).

Pour le détail des délais de traitement, 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 et 68, al. 1, OSCPT, il y a lieu d'adapter également les renvois aux. al. 2 et 3.

Annexe 1

Trois 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_ASSOC_PERMl : renseignements sur les identifiants attribués pour une longue durée (art. 48*a* OSCPT) ;
2) le type de renseignements IR_52_ASSOC_PERM : renseignements immédiats sur les identifiants attribués pour une courte durée (art. 48*b* OSCPT) ;
3) le type de renseignements IR_53_TEL_ADJ_NET : détermination des réseaux voisins de services de téléphonie et multimédia (art. 48*c* OSCPT) ;
4) le type de surveillance (en temps réel) RT_54_POS_ONCE : détermination unique et immédiate de la position par le réseau (art. 56*a* OSCPT) ;
5) le type de surveillance (en temps réel) RT_55_POS_PERIOD : détermination périodique et récurrente de la position par le réseau (art. 56*b* OSCPT) ;
6- le type de surveillance (recherche en cas d'urgence) EP_56_POS_ONCE : détermination unique et immédiate de la position par le réseau (art. 67, let. b, OSCPT) ; et
7) le type de surveillance (recherche en cas d'urgence) EP_57_POS_PERIOD : détermination périodique et récurrente de la position par le réseau (art. 67, 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.

Annexe 2

L'annexe 2 de l'OME-SCPT définit les exigences techniques auxquelles doivent satisfaire les réseaux de transmission utilisés pour la surveillance des télécommunications entre les POC et le système de traitement du Service SCPT. Le principal motif de la révision partielle de cette annexe a été l'abandon par les FST suisses de la technologie ISDN, devenue obsolète, et la mise hors service des connexions de transmission fondées sur cette technologie. L'ISDN utilisait encore la commutation de circuits, alors que désormais seuls des réseaux utilisant la commutation de paquets peuvent être utilisés pour la transmission. Les passages de l'annexe 2 concernant l'ISDN ont été supprimés. Les interfaces de transmission ISDN (HI2 pour CS IRI et HI3 pour CS CC), le réseau de transmission ISDN pour CS CC, le réseau de transmission pour CS IRI et les séquences de signalisation pour le réseau à commutation de circuits (CS) sont supprimés. Une POC qui souhaite encore transmettre des données de surveillance à partir de réseaux utilisant la commutation de circuits devra d'abord convertir ces données en paquets IP et les transmettre par un réseau à commutation de paquets.

La révision de l'annexe a par ailleurs été l'occasion de mettre à jour la vue d'ensemble des interfaces de transmission, les explications relatives aux différentes instances et composants du système de traitement et le modèle suisse de référence pour la surveillance des télécommunications (architecture fonctionnelle pour la surveillance des télécommunications fondée sur l'architecture de référence de l'ETSI).

Enfin certains termes ont été rectifiés et l'interface LI_HIQR (pour les renseignements selon l'art. 48*b*) a été ajoutée, ainsi qu'une référence à l'OST-SCPT.

4.3 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'OSCPT – 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 fournies 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. Ces personnes pourront continuer de n'octroyer des accès qu'à l'intérieur de leur organisation ou à des personnes directement concernées par la procédure et à leurs conseils juridiques. Elles pourront désormais également donner des accès aux membres des autorités chargées d'autoriser les mesures. Ces autorités sont le tribunal des mesures de contrainte ou, pour le SRC, le Tribunal administratif fédéral. 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 OrgAdmin pourront dorénavant aussi le faire. Les droits ainsi octroyés donnent uniquement accès au système WMC (*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.

Lors de la consultation, le souhait a été exprimé que les collaborateurs autorisés par le Service SCPT (OrgAdmin) des autorités ordonnant, approuvant et évaluant des mesures puissent à leur tour octroyer des accès à des personnes extérieures à leur organisation. L'argument avancé était que cette possibilité simplifierait la collaboration et déchargerait le Service SCPT de cette tâche administrative, ce qui serait particulièrement utile lorsque le temps est compté (par ex. lors de recherches en cas d'urgence, qui doivent souvent être menées en dehors des heures de bureau). Il n'a pas été possible de donner suite à cette demande de modification, car elle contreviendrait à l'art. 9, al. 1, LSCPT, qui prévoit que c'est au Service SCPT de permettre l'accès aux données collectées en relation avec une procédure.

Les al. 4 et 5 précisent les modalités de l'accès aux données par le 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, si possible 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[33] 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[34] 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

33 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**)

34 Loi fédérale du 30 mars 1911 complétant le Code civil suisse (Livre cinquième : Droit des obligations ; RS **220**)

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 notamment 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 ?), ainsi que 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 est nécessaire rapidement pour identifier les causes 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 de traitement.

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 opéré par la POC 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, fournies 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 ou des autorités est à l'origine du problème. Il n'est donc pas possible, dans ce type de situation, d'obtenir un accord préalable.
Selon la *let. b*, le consentement de l'autorité n'est pas non plus requis lorsqu'il est disproportionné de contacter toutes les autorités compétentes en raison du grand nombre de surveillances concernées. Dans ces cas, le système fonctionne encore correctement mais il pourrait devenir instable ou perdre en qualité. Il faut bien souvent confronter – automatiquement – un très grand nombre de données pour détecter des anomalies, identifier les surveillances ou les formats 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). Pour l'analyse automatique des données, il faut généralement accéder à un grand nombre de surveillances issues de différents ordres et de différentes autorités avant de pouvoir identifier la problématique. Il est difficile d'estimer à l'avance le nombre et le type de surveillances concernées par une problématique. Identifier et contacter toutes les autorités concernées serait quasiment impossible et impliquerait une charge de travail disproportionnée. Par conséquent, si une problématique ne peut être résolue que grâce à l'accès à un grand nombre de surveillances, l'accord de toutes les autorités individuelles n'est pas nécessaire.

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.

L'art. 6 OPDo[35] constitue une base légale suffisante sur laquelle le Service SCPT peut se fonder pour concrétiser les al. 3 à 6 dans le règlement de traitement. Le contenu de l'actuel al. 4 n'a donc pas besoin d'être repris dans le nouvel art. 8.

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'*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).

La destruction des données doit également être consignée. Une disposition fait toutefois défaut dans l'ordonnance en vigueur concernant la durée de conservation des fichiers de journalisation de la destruction des données. Cette question est réglée par la nouvelle *deuxième phrase*. 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. 4 OPDo n'est pas applicable ici.

Art. 11 Mesures pour la sécurité du système

Dans la première phrase, 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. La *deuxième phrase* reprend la disposition actuelle selon laquelle le Service SCPT entend préalablement les autorités concernées par un dérangement lorsqu'il est possible de les contacter (voir art. 8, al. 5).

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

35 Ordonnance du 31 août 2022 sur la protection des données (**OPDo** ; RS **235.11**)

la performance des différents composants de surveillance. PTSS est la désignation anglaise du Service SCPT. C'est sur cette application 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. 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.

5 Conséquences

5.1 Conséquences pour la Confédération

Les adaptations prévues des trois ordonnances d'exécution de la LSCPT (OSCPT, OME-SCPT et OST-SCPT) n'auront pas, en l'état actuel des choses, de conséquences importantes pour la Confédération en termes de finances ou de personnel.

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 les ressources actuellement prévues dans son budget.

5.2 Conséquences pour les cantons

En l'état actuel des choses, les adaptations prévues n'auront pas non plus de conséquences financières ou personnelles importantes pour les cantons. Les émoluments pour les nouveaux types de renseignements et de surveillances sont pris en compte dans les forfaits introduits par l'ordonnance sur le financement de la surveillance de la correspondance par poste et télécommunication (OF-SCPT, projet distinct).

5.3 Conséquences pour les POC

Les nouveaux types de renseignements et de surveillances, ainsi que les adaptations à la technologie 5G dans l'OSCPT, pourront avoir des conséquences financières et économiques pour les FST en fonction des adaptations qu'elles devront apporter à leurs systèmes suite à cette révision partielle. Les FST auront notamment des frais d'investissement pour assurer la mise en œuvre des nouveaux types de renseignements et de surveillances. Selon l'art. 74*b* OSCPT, ils auront des délais plus longs (24 mois au lieu de 12) pour adapter leurs systèmes.

6 Aspects juridiques

6.1 Compatibilité avec les obligations internationales de la Suisse

Le projet est compatible avec les obligations internationales de la Suisse.

6.2 Forme de l'acte à adopter

Il s'agit d'une révision partielle d'ordonnances du Conseil fédéral au sens de l'art. 182 Cst.[36]

6.3 Sous-délégation de compétences législatives

Le projet ne contient pas de sous-délégation de compétences législatives (voir néanmoins l'art. 70 OSCPT et l'OME-SCPT).

6.4 Protection des données

Les modifications prévues concernent aussi le traitement de données personnelles sensibles (art. 4 LSCPT).

Annexe

Tableau « Vue d'ensemble des délais de traitement »

36 Constitution fédérale de la Confédération suisse du 18 avril 1999 (**Cst.** ; RS **101**)

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 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_51_ASSOC_PERM**	≤ 1 heure	≤ 1 heure	≤ 1 jour ouvré
	48*b*	IR_52_ASSOC_TEMP**	Immédiatement	Immédiatement (sauf FSCD ayant des obligations étendues en matière de fourniture de renseignements, art. 22 OSCPT)	--
	38 39 42 27, 42 43 27, 43 48*c*	IR_8_IP (NAT) IR_9_NAT IR_13_EMAIL IR_14_EMAIL_FLEX IR_15_COM IR_16_COM_FLEX IR_53_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
	44 45 46 47 48	IR_17_PAY IR_18_ID IR_19_BILL IR_20_CONTRACT IR_21_TECH	≤ 1 heure	≤ 1 jour ouvré	≤ 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 68*a*	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_54_POS_ONCE*** RT_55_POS_PERIOD*** RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI ML_50_RT	≤ 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 68*a*	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_54_POS_ONCE*** RT_55_POS_PERIOD*** RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI ML_50_RT	≤ 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 68*a*	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_54_POS_ONCE*** RT_55_POS_PERIOD*** RT_25_TEL_CC_IRI RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI ML_50_RT	≤ 1 heure	≤ 2 heures
Surveillance rétroactive pendant les heures de bureau	60 61 62 63 64 65	HD_28_NA HD_29_TEL HD_30_EMAIL HD_31_PAGING AS_32_PREP_COV**** AS_33_PREP_REF	≤ 1 heure	≤ 3 jours ouvrés

	66	AS_34		
Surveillance rétroactive situations déclarées urgentes (pendant les heures de bureau ou le service de piquet)	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	≤ 6 heures
Recherche en cas d'urgence pendant les heures de bureau ou le service de piquet	67, let. a 67, let. b 67, let. c 67, let. d 67, let. e	EP_35_PAGING EP_56_POS_ONCE*** EP_57_POS_PERIOD*** EP_36_RT_CC_IRI EP_37_RT_IRI	≤ 1 heure	≤ 1 heure
	67, 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. d 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_54_POS_ONCE*** RT_55_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	RT_22_NA_IRI RT_23_NA_CC_IRI RT_24_TEL_IRI RT_55_POS_PERIOD*** RT_25_TEL_IRI_CC	≤ 1 heure	≤ 1 jour ouvré

	58 59 67, let. c 67, let. d 67, let. e	RT_26_EMAIL_IRI RT_27_EMAIL_CC_IRI EP_57_POS_PERIOD*** EP_36_RT_CC_IRI EP_37_RT_IRI		

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

** Les FSCD ayant des obligations étendues (art. 22 et 52 OSCPT) en sont dispensés.

*** Les FSCD ayant des obligations étendues en matière de surveillance (art. 52 OSCPT) en sont dispensés.

**** 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).