

Ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT)

du 15 novembre 2017 (État le 1^{er} septembre 2023)

Le Conseil fédéral suisse,

vu la loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (LSCPT)¹,

vu les art. 269^{bis}, al. 2, 269^{ter}, al. 4, et 445 du code de procédure pénale (CPP)²,

vu les art. 70^{bis}, al. 2, 70^{ter}, al. 4, et 218 de la procédure pénale militaire du 23 mars 1979 (PPM)³,

arrête:

Chapitre 1 Dispositions générales

Section 1 Introduction

Art. 1 Objet et champ d'application

¹ La présente ordonnance règle l'organisation et la procédure applicables à la surveillance de la correspondance par poste et télécommunication ainsi que l'octroi de renseignements sur les services postaux et de télécommunication.

² Elle s'applique:

- a. aux autorités habilitées à ordonner une surveillance et aux autorités qui dirigent la procédure;
- b. aux autorités habilitées à autoriser une surveillance;
- c. aux autorités de police de la Confédération, des cantons et des communes;
- d. au Service de renseignement de la Confédération (SRC);
- e. au Secrétariat d'État à l'économie (SECO);
- f. aux autorités fédérales et cantonales compétentes pour régler des affaires relevant du droit pénal administratif;
- g. au Service Surveillance de la correspondance par poste et télécommunication (Service SCPT);
- h. aux fournisseurs de services postaux (FSP);
- i. aux fournisseurs de services de télécommunication (FST);

RO 2018 147

¹ RS 780.1

² RS 312.0

³ RS 322.1

- j. aux fournisseurs de services qui se fondent sur des services de télécommunication et qui permettent une communication unilatérale ou multilatérale (fournisseurs de services de communication dérivés);
- k. aux exploitants de réseaux de télécommunication internes;
- l. aux personnes qui mettent leur accès à un réseau public de télécommunication à la disposition de tiers;
- m. aux revendeurs professionnels de cartes ou de moyens semblables qui permettent l'accès à un réseau public de télécommunication.

Art. 2 Termes et abréviations

Les termes et abréviations utilisés dans la présente ordonnance sont définis en annexe.

Section 2 **Ordre de surveillance**

Art. 3 Communication au Service SCPT

¹ L'autorité qui ordonne la surveillance utilise un des moyens de transmission ci-après pour communiquer au Service SCPT un ordre de surveillance, pour le prolonger ou pour le lever, et pour lui indiquer les droits d'accès à configurer:

- a. un moyen de transmission sûr autorisé par le Service SCPT;
- b. la poste ou une télécopie, si un moyen de transmission au sens de la let. a n'est pas disponible pour des raisons techniques, ou
- c. le téléphone, en cas d'urgence, avec transmission ultérieure de l'ordre conformément aux let. a ou b dans les 24 heures.

² Le Service SCPT peut remplacer le moyen de transmission des ordres de surveillance selon l'al. 1, let. a, par un accès en ligne à son système de traitement.

Art. 4 Mise en œuvre de la surveillance

¹ Le Service SCPT détermine dans chaque cas les mesures techniques et organisationnelles à prendre pour mettre en œuvre la surveillance dès lors qu'elles ne ressortent pas directement des réglementations en vigueur, en particulier des types de renseignements et de surveillance ayant fait l'objet d'une standardisation.

² Si une personne obligée de collaborer est empêchée, suite à des problèmes d'exploitation, de remplir ses obligations en matière de surveillance de la correspondance par poste et télécommunication, elle en avise immédiatement le Service SCPT et lui fait parvenir une justification écrite. Le Service SCPT informe immédiatement les personnes obligées de collaborer de tout problème d'exploitation l'affectant qui empêche l'exécution de la surveillance.

³ Quelle que soit l'origine du problème, la personne obligée de collaborer sauvegarde au moins les données secondaires d'une surveillance en temps réel qui n'ont pas été livrées et les transmet aussitôt qu'elle est en mesure de le faire. Si les données

secondaires de la surveillance en temps réel ne sont plus disponibles ou sont incomplètes, la personne obligée de collaborer doit, sur instruction du Service SCPT, livrer sans délai les données secondaires correspondantes de la surveillance rétroactive.

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

S'il constate que la surveillance concerne une personne tenue au secret professionnel ou au secret de fonction et qu'aucune des mesures prévues dans la loi n'a été prise pour protéger ces secrets, le Service SCPT, dans les situations ci-après, en informe immédiatement l'autorité qui a ordonné la surveillance et l'autorité habilitée à l'autoriser et, dans un premier temps, ne donne accès aux données issues de la surveillance ni à l'autorité qui a ordonné la surveillance ni aux personnes indiquées dans l'ordre de surveillance:

- a. si la surveillance a été ordonnée par une autorité civile de poursuite pénale, qu'elle concerne une personne appartenant à l'une des catégories professionnelles énumérées aux art. 170 à 173 CPP et qu'aucune mesure spéciale de protection au sens de l'art. 271 CPP n'a été prise;
- b. si la surveillance a été ordonnée par une autorité militaire de poursuite, qu'elle concerne une personne appartenant à l'une des catégories professionnelles énumérées à l'art. 75, let. b, PPM et qu'aucune mesure spéciale de protection au sens de l'art. 70b PPM n'a été prise;
- c. si la surveillance a été ordonnée par le SRC, qu'elle concerne une personne appartenant à l'une des catégories professionnelles énumérées aux art. 171 à 173 CPP et qu'aucune mesure au sens de l'art. 58, al. 3, de la loi fédérale du 25 septembre 2015 sur le renseignement (LRens)⁴, en relation avec l'art. 23 de l'ordonnance du 16 août 2017 sur le renseignement⁵, n'a été prise.

Art. 6 Obligation de garder le secret

La surveillance et la fourniture de renseignements doivent être exécutées de façon à ce que ni les personnes surveillées ni des tiers non autorisés n'en aient connaissance.

Art. 7 Tri automatisé des données

Le Service SCPT effectue, à la demande de l'autorité qui a ordonné la surveillance, un tri automatisé des données (filtrage) lorsque la mesure est techniquement possible et qu'elle n'entraîne pas une charge de travail disproportionnée.

Art. 8 Enregistrement des communications téléphoniques
à des fins probatoires

¹ Le Service SCPT enregistre, à des fins probatoires, les communications téléphoniques liées à l'accomplissement de ses tâches.

⁴ RS 121

⁵ RS 121.1

² Le cas échéant, les enregistrements sont exploités par le conseiller à la protection des données du Service SCPT.⁶

³ Le Service SCPT conserve pendant deux ans les communications téléphoniques enregistrées et les détruit ensuite.

Art. 9 Dossier de surveillance

¹ Le Service SCPT ouvre un dossier dans le système de traitement pour chaque ordre de surveillance.

² Ce dossier contient tous les documents concernant le cas, en particulier:

- a. l'ordre de surveillance et ses annexes;
- b. le ou les mandats de surveillance aux personnes obligées de collaborer;
- c. la confirmation indiquant la date de transmission du ou des mandats de surveillance aux personnes obligées de collaborer;
- d. la confirmation d'exécution du ou des mandats de surveillance par les personnes obligées de collaborer;
- e. les décisions de l'autorité compétente autorisant ou refusant la surveillance et, le cas échéant, les décisions sur recours;
- f. le cas échéant, les ordres de prolongation de la surveillance et les décisions de l'autorité habilitée à autoriser la surveillance;
- g. l'ordre de lever la surveillance;
- h. la correspondance échangée au sujet de la mesure;
- i. les mesures de protection particulières ordonnées;
- j. les documents de facturation.

³ Les données issues de la surveillance sont conservées conformément à l'art. 11 LSCPT et détruites conformément à l'art. 14 l'ordonnance du 15 novembre 2017 sur le système de traitement pour la surveillance de la correspondance par poste et télécommunication (OST-SCPT)⁷.

Section 3 Heures de travail et service de piquet

Art. 10 Heures normales de travail et jours fériés

¹ Les heures normales de travail du Service SCPT et des personnes obligées de collaborer vont du lundi au vendredi, de 8 heures à 17 heures sans interruption.

² Les heures normales de travail ne s'appliquent pas les jours fériés. Sont des jours fériés: les 1^{er} et 2 janvier, le Vendredi-Saint, le lundi de Pâques, l'Ascension, le lundi

⁶ Nouvelle teneur selon l'annexe 2 ch. II 85 de l'O du 31 août 2022 sur la protection des données, en vigueur depuis le 1^{er} sept. 2023 (RO 2022 568).

⁷ RS 780.12

de Pentecôte, le 1^{er} août, le 24 décembre à partir de 12 heures, le 25 décembre, le 26 décembre et le 31 décembre à partir de 12 heures.

Art. 11 Prestations en dehors des heures normales de travail

¹ En dehors des heures normales de travail et les jours fériés, le Service SCPT assure un service de piquet qui comprend les prestations suivantes:

- a. la transmission des demandes de renseignements selon les art. 35 à 43;
- b. la transmission des mandats d'activation des surveillances en temps réel selon les art. 54 à 59;
- c. la transmission des mandats d'exécution des surveillances rétroactives selon les art. 60 à 63, 65 et 66 qui ont été déclarées urgentes;
- d. la transmission des mandats d'exécution de recherches en cas d'urgence et de recherches de personnes condamnées selon les art. 67 et 68, excepté l'analyse de la couverture réseau préalablement à une recherche par champ d'antennes selon l'art. 64;
- dbis.⁸ la transmission des mandats de localisation par téléphonie mobile de terroristes potentiels selon l'art. 68a;
- e. la levée de dérangements.

² Les FST, à l'exception de ceux ayant des obligations restreintes en matière de surveillance visés à l'art. 51, et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de surveillance visés à l'art. 52 doivent être en mesure d'apporter un soutien au Service SCPT pour lui permettre de fournir en tout temps les prestations mentionnées à l'al. 1. Le Service SCPT doit pouvoir les joindre en tout temps.

³ Les ordres portant sur des surveillances spéciales, de même que les demandes de renseignements spéciaux (art. 25), ne sont ni réceptionnés, ni traités en dehors des heures normales de travail.

Section 4 Statistiques

Art. 12 Statistique des mesures de surveillance et des renseignements

¹ Le Service SCPT publie chaque année une statistique des surveillances ordonnées et des renseignements fournis pendant l'année civile écoulée. Cette statistique indique en particulier:

- a. le nombre de mesures de surveillance en temps réel;
- b. le nombre de mesures de surveillance rétroactive;
- c. le nombre de renseignements;

⁸ Introduite par le ch. I 12 de l'O du 4 mai 2022 sur les mesures policières de lutte contre le terrorisme, en vigueur depuis le 1^{er} juin 2022 (RO 2022 301).

- d. le nombre de recherches en cas d'urgence;
 - e. le nombre de recherches de personnes condamnées;
 - f.⁹ le nombre de localisations par téléphonie mobile de terroristes potentiels.
- ² La statistique selon l'al. 1 indique:
- a. le type d'infraction;
 - b. le canton dont relève l'autorité qui a ordonné la mesure ou la désignation de l'autorité de la Confédération dont il s'agit; pour des recherches en cas d'urgence, il peut aussi s'agir d'une autorité de la Principauté de Liechtenstein; dans le cas d'une demande de renseignements, l'autorité cantonale ou fédérale ayant fait la demande (art. 1, al. 2, let. c à f);
 - c.¹⁰ le type de renseignements, de surveillance, de recherche en cas d'urgence, de recherche de personnes condamnées ou de localisation par téléphonie mobile de terroristes potentiels;
 - d. le cas échéant, la durée de la surveillance;
 - e. les émoluments;
 - f. les indemnités.

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

¹ Les ministères publics et les juges d'instruction militaires tiennent une statistique annuelle de l'utilisation de dispositifs techniques et de programmes informatiques spéciaux dans le cadre de surveillances pendant l'année civile écoulée (art. 269^{bis}, al. 2, et 269^{ter}, al. 4, CPP et art. 70^{bis}, al. 2, et 70^{ter}, al. 4, PPM). La statistique indique le type d'infraction.

² Les ministères publics et l'Office de l'auditeur en chef du DDPS transmettent leur statistique au Service SCPT au cours du premier trimestre de l'année suivante. La statistique n'inclut que les mesures terminées à la fin de l'année sur laquelle elle porte.

³ Le Service SCPT publie chaque année une statistique consolidée. Celle-ci n'indique pas le canton des autorités qui ont ordonné les mesures ou, pour la Confédération, les autorités dont il s'agit.

⁹ Introduite par le ch. I 12 de l'O du 4 mai 2022 sur les mesures policières de lutte contre le terrorisme, en vigueur depuis le 1^{er} juin 2022 (RO 2022 301).

¹⁰ Nouvelle teneur selon le ch. I 12 de l'O du 4 mai 2022 sur les mesures policières de lutte contre le terrorisme, en vigueur depuis le 1^{er} juin 2022 (RO 2022 301).

Chapitre 2 Correspondance par poste

Art. 14 Obligations des FSP

¹ Chaque FSP doit être en mesure de livrer les renseignements visés à l'art. 20 LSCPT et d'exécuter les types de surveillance énoncés à l'art. 16 dès lors qu'ils portent sur des services qu'il propose.

² Chaque FSP doit être en mesure, pendant les heures normales de travail, de réceptionner et d'exécuter les demandes de renseignements et les ordres de surveillance.

Art. 15 Ordre de surveillance de la correspondance par poste

L'ordre de surveillance transmis au Service SCPT contient les indications suivantes:

- a. les coordonnées de l'autorité qui ordonne la surveillance;
- b. les coordonnées des personnes autorisées auxquelles les données issues de la surveillance sont destinées;
- c. si ces données sont connues: les nom, prénom, date de naissance, adresse et profession de la personne à surveiller;
- d. le numéro de référence et le nom de l'affaire à laquelle se rapportent les surveillances;
- e. le motif de la surveillance, en particulier l'infraction qu'elle doit permettre d'élucider;
- f. le nom des FSP;
- g. les types de surveillance ordonnés;
- h. si nécessaire, les renseignements complémentaires sur la correspondance par poste des personnes concernées;
- i. le début et la fin de la surveillance;
- j. dans le cas de personnes tenues au secret professionnel au sens de l'art. 271 CPP ou de l'art. 70b PPM: une mention indiquant cette particularité;
- k. le cas échéant, les mesures visant à protéger les personnes tenues au secret professionnel et d'autres mesures de protection que les autorités, les FSP et le Service SCPT doivent mettre en œuvre.

Art. 16 Types de surveillance

Les types de surveillance qui peuvent être ordonnés sont les suivants:

- a. l'interception des envois postaux (surveillance en temps réel; type de surveillance PO_1_RT_INTERCEPTION);
- b. la livraison des données secondaires ci-après (surveillance en temps réel; type de surveillance PO_2_RT_DELIVERY), pour autant qu'elles soient disponibles:
 1. l'identité des destinataires des envois postaux,

2. l'identité des expéditeurs des envois postaux,
 3. la nature des envois postaux,
 4. le lieu à partir duquel l'expédition est faite,
 5. l'état d'acheminement des envois postaux,
 6. la signature du destinataire;
- c. la livraison des données secondaires ci-après (surveillance rétroactive; type de surveillance PO_3_HD):
1. dans le cas des envois postaux avec justificatifs de distribution: l'expéditeur et le destinataire, ainsi que, si ces données sont disponibles, la nature, le lieu d'expédition et l'état d'acheminement des envois postaux,
 2. si le FSP enregistre d'autres données secondaires: toutes celles qui sont disponibles.

Chapitre 3 Correspondance par télécommunication

Section 1

Dispositions générales concernant la fourniture de renseignements et les surveillances

Art. 17 Demandes de renseignements

¹ Les demandes de renseignement des autorités visées à l'art. 15 LSCPT aux FST, aux fournisseurs de services de communication dérivés et aux exploitants de réseaux de télécommunication internes, ainsi que les renseignements fournis en retour à ces autorités, sont transmis par le biais du système de traitement, conformément à l'OST-SCPT¹¹, via une procédure d'appel en ligne ou via les interfaces prévues.

² Dans le cas où la transmission en ligne via le système de traitement n'est pas possible pour des raisons techniques, les demandes de renseignements et les réponses correspondantes peuvent être transmises au Service SCPT par poste ou télécopie.

³ En cas d'urgence, les autorités peuvent transmettre au Service SCPT les demandes de renseignements par téléphone, avec transmission ultérieure de la demande selon l'al. 1 ou 2.

⁴ La demande indique, outre les informations prévues pour chaque type de renseignements, le nombre maximal d'enregistrements à livrer et, si ces données sont disponibles, le numéro de référence et le nom de l'affaire.

Art. 18 Obligations concernant la fourniture de renseignements

¹ Les FST et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements visés à l'art. 22 doivent être en mesure de fournir les renseignements visés aux art. 35 à 37 et 40 à 48, ainsi que

¹¹ RS 780.12

ceux visés à l'art. 27 en relation avec les art. 35, 40, 42 et 43, concernant les services qu'ils proposent. Ils peuvent faire appel pour ce faire à des tiers.

² Ils livrent les renseignements visés aux art. 35 à 37 et 40 à 42, ainsi qu'à l'art. 27 en relation avec les art. 35, 40 et 42 de manière automatisée, via l'interface de consultation du système de traitement. Les demandes de renseignements visées aux art. 43 à 48, ainsi qu'à l'art. 27 en relation avec l'art. 43, peuvent aussi être traitées manuellement.

³ Les FST ayant des obligations restreintes en matière de surveillance visés à l'art. 51 peuvent aussi livrer tous les types de renseignements par écrit, en dehors du système de traitement.

⁴ Les FST, à l'exception de ceux ayant des obligations restreintes en matière de surveillance visés à l'art. 51, et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de surveillance visés à l'art. 52 doivent être en mesure de fournir, via l'interface de consultation du système de traitement, les renseignements visés aux art. 38 et 39 concernant les services qu'ils proposent. Ils peuvent faire appel pour ce faire à des tiers.

⁵ Les fournisseurs de services de communication dérivés n'ayant pas d'obligations étendues en matière de fourniture de renseignements et de surveillance et les exploitants de réseaux de télécommunication internes ne sont pas tenus de livrer les types de renseignements visés aux art. 35 à 48 ainsi qu'à l'art. 27 en relation avec les art. 35, 40, 42 et 43. Ils livrent les données dont ils disposent via le système de traitement ou par écrit, via un autre canal.

⁶ Si le nombre d'enregistrements trouvés dépasse le nombre maximal indiqué dans la demande, le fournisseur en communique uniquement le nombre.

Art. 19 Identification des usagers

¹ Les FST, les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements visés à l'art. 22, les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de surveillance visés à l'art. 52 et les revendeurs visés à l'art. 2, let. f, LSCPT veillent à identifier les usagers par des moyens appropriés.

² Les FST veillent à identifier par des moyens appropriés tous les utilisateurs finaux de points d'accès publics au réseau WLAN exploités à titre professionnel.

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

¹ Pour les services de communication mobile, les FST et les revendeurs visés à l'art. 2, let. f, LSCPT vérifient, lors de la remise du moyen d'accès ou de la première activation du service, l'identité de l'utilisateur au moyen d'un passeport, d'une carte d'identité ou d'un titre de séjour au sens des art. 71 et 71a de l'ordonnance du 24 octobre 2007

relative à l'admission, au séjour et à l'exercice d'une activité lucrative¹². Une copie lisible du document d'identité doit être conservée.

² S'agissant des personnes physiques, les indications ci-après sont saisies:

- a. les nom et prénom;
- b. la date de naissance;
- c. le type et le numéro de la pièce d'identité, ainsi que le pays ou l'organisation qui l'a établie;
- d. l'adresse;
- e. si elle est connue: la profession;
- f. la nationalité.

³ S'agissant des personnes morales, les indications ci-après sont saisies:

- a. le nom, le siège et les coordonnées;
- b. le numéro d'identification de l'entreprise (IDE) en application de la loi fédérale du 18 juin 2010 sur le numéro d'identification des entreprises¹³;
- c. si ces données sont disponibles: les nom et prénom des usagers des services du fournisseur.

⁴ Pour les relations commerciales sans abonnement, les indications ci-après sont aussi enregistrées:

- a. la date et l'heure de la remise du moyen d'accès;
- b. le lieu de la remise, comprenant le nom et l'adresse complète;
- c. le nom de la personne qui s'est chargée de la remise.

Art. 21 Délais de conservation

¹ Les FST et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements et de surveillance (art. 22 et 52) doivent, pendant toute la durée de la relation commerciale ainsi que six mois après la fin de celle-ci, conserver les indications relatives aux services de télécommunication et celles saisies aux fins de l'identification, et être en mesure de les livrer. Les FST doivent, pendant toute la durée de l'autorisation d'accès au point d'accès public au réseau WLAN ainsi que six mois après la fin de celle-ci, conserver les données d'identification selon l'art. 19, al. 2, et être en mesure de les livrer.

² Les FST, à l'exception de ceux ayant des obligations restreintes en matière de surveillance visés à l'art. 51, et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de surveillance visés à l'art. 52 doivent conserver et être en mesure de livrer pendant six mois les données ci-après saisies aux fins de l'identification:

¹² RS 142.201

¹³ RS 431.03

- a. les données secondaires relatives aux identifiants des équipements effectivement utilisés pour être en mesure de livrer les renseignements visés aux art. 36, al. 1, let. d, et 41, al. 1, let. d;
- b. les données secondaires relatives à l'attribution et à la traduction d'adresses IP et de numéros de ports pour être en mesure de livrer les renseignements visés aux art. 37, 38 et 39.

³ Les données secondaires selon l'al. 2 doivent être détruites à l'issue du délai de conservation, pour autant qu'aucun autre acte ne prévoit qu'elles doivent ou peuvent être conservées plus longtemps.

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

¹ Le Service SCPT déclare un fournisseur de services de communication dérivés comme ayant des obligations étendues en matière de fourniture de renseignements (art. 22, al. 4, LSCPT) lorsque celui-ci atteint une des valeurs suivantes:

- a. 100 demandes de renseignements au cours des douze derniers mois (date de référence: 30 juin);
- b. un chiffre d'affaires annuel en Suisse de 100 millions de francs pendant deux exercices consécutifs, une grande partie de l'activité commerciale devant consister dans la fourniture de services de communication dérivés, et 5000 usagers.

² Si un fournisseur contrôle, au sens de l'art. 963, al. 2, du code des obligations¹⁴, une ou plusieurs entreprises tenues d'établir des comptes, le fournisseur et les entreprises contrôlées sont considérés comme une unité pour le calcul des valeurs selon l'al. 1.

³ Les fournisseurs qui dépassent ou n'atteignent plus les valeurs selon l'al. 1, let. b, le communiquent par écrit au Service SCPT, pièces justificatives à l'appui, dans les trois mois suivant la fin de l'exercice.

⁴ Les fournisseurs transmettent sur demande au Service SCPT les indications nécessaires, justificatifs à l'appui, aux fins notamment de vérifier les valeurs selon l'al. 1, let. b. Le Service SCPT peut se procurer les données issues de la mise en œuvre de la législation sur la surveillance de la correspondance par poste et télécommunication, ainsi que les données obtenues par d'autres autorités lors de la mise en œuvre du droit fédéral.

⁵ Un fournisseur déclaré comme ayant des obligations étendues en matière de fourniture de renseignements a, à compter de la décision, deux mois pour garantir l'enregistrement des données nécessaires à la livraison des renseignements et douze mois pour assurer la disponibilité à renseigner.

¹⁴ RS 220

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

Les tiers auxquels les fournisseurs font appel pour l'exécution de demandes de renseignements ou d'ordres de surveillance sont soumis aux mêmes règles que les fournisseurs. Les fournisseurs mandatés répondent de l'exécution, selon le cadre prescrit, des surveillances et des demandes de renseignements; ils prennent en particulier toutes les mesures utiles pour que le Service SCPT puisse joindre en tout temps un interlocuteur au sujet de l'exécution de la demande de renseignements ou de la surveillance ordonnée. Tant les fournisseurs mandatés que les tiers auxquels ceux-ci font appel sont les interlocuteurs du Service SCPT.

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

¹ Le Département fédéral de justice et police (DFJP) procède à la standardisation des types de renseignements et des types de surveillance définis dans la présente ordonnance.

² S'il apparaît, à la lumière des normes internationales et des clarifications avec les personnes obligées de collaborer, qu'une standardisation est impossible ou qu'elle demanderait une charge de travail disproportionnée, le DFJP y renonce.

Art. 25 Surveillances et renseignements spéciaux

Pour les renseignements et les surveillances qui ne relèvent pas des types de renseignements et de surveillance ayant fait l'objet d'une standardisation, les FST et les fournisseurs de services de communication dérivés mettent à la disposition du Service SCPT toutes les interfaces et tous les raccordements existants avec le système de traitement. Le contenu des communications et les données secondaires de télécommunication de la personne surveillée doivent, dans la mesure du possible, être livrés conformément à l'art. 26, al. 1, LSCPT. Le Service SCPT détermine les modalités dans chaque cas.

Art. 26 Types de renseignements en général

¹ Les types de renseignements que les fournisseurs concernés sont tenus de livrer concernant des services de télécommunication ou des services de communication dérivés sont les suivants:

- a. renseignements sur les usagers (art. 35, 40, 42 et 43, ainsi qu'art. 27 en relation avec les art. 35, 40, 42 et 43);
- b. renseignements sur les services (art. 36 à 39 et 41);
- c. autres renseignements:
 1. renseignements sur le moyen de paiement (art. 44),
 2. copies de pièces d'identité (art. 45),
 3. copies de factures (art. 46),
 4. copies des documents contractuels (art. 47),

5. renseignements sur les données techniques de systèmes de télécommunication et d'éléments de réseau (art. 48).

² Les autorités ne peuvent demander des renseignements que les fournisseurs sont tenus de livrer sur la base de la présente ordonnance que conformément à la procédure qui y est définie.

Art. 27 Types de renseignements avec recherche flexible de nom

¹ Les demandes portant sur les types de renseignements visés aux art. 35, 40, 42 et 43 peuvent être exécutées au moyen d'une recherche tolérante à l'erreur, qui trouve les concordances phonétiques (recherche flexible de nom). Le cas échéant, il convient d'ajouter le suffixe « FLEX » au nom du type de renseignements: IR_5_NA_FLEX, IR_11_TEL_FLEX, IR_14_EMAIL_FLEX et IR_16_COM_FLEX.

² La demande de renseignements indique le premier critère de recherche et au moins un critère supplémentaire correspondant au type de renseignements auquel elle se rapporte.

Art. 28 Types de surveillance

¹ Les types de surveillance en temps réel que les fournisseurs concernés sont tenus d'exécuter pour des services de télécommunication et des services de communication dérivés sont les suivants:

- a. surveillance en temps réel des données secondaires de services d'accès au réseau (art. 54);
- b. surveillance en temps réel du contenu et des données secondaires de services d'accès au réseau (art. 55);
- c. surveillance en temps réel des données secondaires d'applications (art. 56 et 58);
- d. surveillance en temps réel du contenu et des données secondaires d'applications (art. 57 et 59).

² Les types de surveillance rétroactive que les fournisseurs concernés sont tenus d'exécuter pour des services de télécommunication et des services de communication dérivés sont les suivants:

- a. surveillance rétroactive de services d'accès au réseau (art. 60);
- b. surveillance rétroactive d'applications (art. 61 et 62);
- c. détermination du dernier lieu de localisation enregistré de l'équipement terminal mobile (art. 63);
- d. recherche par champ d'antennes (art. 66) et mesures préalables (art. 64 ou 65).

³ Les types de recherche en cas d'urgence (art. 67) que les fournisseurs concernés sont tenus d'exécuter sont les suivants:

- a. détermination du dernier lieu de localisation enregistré de l'équipement terminal mobile (art. 67, let. a);

- b. surveillance en temps réel du contenu et des données secondaires de services d'accès au réseau et de services de téléphonie et multimédia (art. 67, let. b);
- c. surveillance en temps réel des données secondaires de services d'accès au réseau et de services de téléphonie et multimédia (art. 67, let. c);
- d. surveillance rétroactive des données secondaires de services d'accès au réseau et de services de téléphonie et multimédia (art. 67, let. d).

⁴ Les types de recherche de personnes condamnées (art. 68) que les fournisseurs concernés sont tenus d'exécuter sont les suivants:

- a. détermination du dernier lieu de localisation enregistré de l'équipement terminal mobile (art. 68, let. a);
- b. surveillance en temps réel du contenu et des données secondaires de services d'accès au réseau ou d'applications (art. 68, let. b);
- c. surveillance en temps réel des données secondaires de services d'accès au réseau ou d'applications (art. 68, let. c);
- d. surveillance rétroactive des données secondaires de services d'accès au réseau ou d'applications (art. 68, let. d).

⁵ Les fournisseurs concernés doivent exécuter la localisation par téléphonie mobile de terroristes potentiels au moyen de la surveillance en temps réel des données secondaires de services d'accès au réseau et d'applications (art. 68a).¹⁵

Section 2 Assurance de la qualité

Art. 29 Qualité des données transmises

¹ La qualité des données transmises est réputée préservée lorsque:

- a. la transmission satisfait aux exigences fixées par le DFJP;
- b. elle s'effectue sans perte de données et sans interruption;
- c. les données issues de la surveillance ou les renseignements correspondent au mandat de surveillance ou à la demande de renseignements.

² Les personnes obligées de collaborer répondent, jusqu'au point de livraison, de la qualité des données issues de renseignements et de surveillances transmises.

³ Si un fournisseur ou le Service SCPT constatent un défaut de qualité des données transmises, ils s'en informent mutuellement sans délai. Le Service SCPT entend le fournisseur concerné pour déterminer la gravité des défauts et la marche à suivre pour y remédier. Le fournisseur et le Service SCPT s'informent régulièrement et en temps réel de l'avancement de la résolution des défauts.

¹⁵ Introduit par le ch. I 12 de l'O du 4 mai 2022 sur les mesures policières de lutte contre le terrorisme, en vigueur depuis le 1^{er} juin 2022 (RO 2022 301).

Art. 30 Branchements de test

¹ Le Service SCPT peut effectuer des branchements de test en collaboration avec les autorités de poursuite pénale et le SRC. Les branchements de test servent notamment à:

- a. assurer la qualité des données que les personnes obligées de collaborer transmettent au Service SCPT et aux autorités de poursuite pénale;
- b. contrôler la disponibilité à surveiller et à renseigner des personnes obligées de collaborer;
- c. tester le système de traitement;
- d. effectuer des formations;
- e. produire de données de référence.

² Le Service SCPT peut charger les personnes obligées de collaborer de participer à la production des données de test. Il conçoit un programme de test après avoir entendu les personnes obligées de collaborer.

³ À la demande du Service SCPT, les personnes obligées de collaborer mettent gratuitement et durablement à sa disposition les branchements de test nécessaires et les services de télécommunication ou les services de communication dérivés requis.

⁴ Les autorités de poursuite pénale et le SRC peuvent aussi faire effectuer, à leurs frais, des branchements de test à des fins d'assurance de la qualité ou de formation. Ils transmettent au Service SCPT un ordre à cette fin et acquittent des émoluments.

Section 3 Garantie de la disponibilité à renseigner et à surveiller**Art. 31** Contrôle de la disponibilité à renseigner et à surveiller

¹ Il appartient aux FST et aux fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements (art. 22) ou de surveillance (art. 52) d'apporter la preuve de la disponibilité à renseigner et à surveiller visée à l'art. 33, al. 1, LSCPT.

² La preuve est réputée apportée lorsque les conditions suivantes sont réunies:

- a. les tests effectués conformément aux prescriptions du Service SCPT sont concluants;
- b. le fournisseur confirme, au moyen d'un questionnaire du Service SCPT, qu'il remplit les exigences relatives aux renseignements et aux surveillances ayant fait l'objet d'une standardisation et pour lesquels la preuve ne peut être apportée par des tests.

³ Le Service SCPT effectue le contrôle dans les meilleurs délais, en veillant à ne pas retarder une mise sur le marché. À cet effet, il exécute les tâches suivantes:

- a. il contrôle les résultats des tests visés à l'al. 2, let. a;
- b. il analyse les formulaires visés à l'al. 2, let b;

- c. il consigne les procédures de contrôle dans un procès-verbal;
- d. il délivre aux fournisseurs une attestation selon l'art. 33, al. 6, LSCPT;
- e. il conserve les procès-verbaux pendant toute la durée de validité de l'attestation et pendant dix ans après la fin de la validité de celle-ci.

⁴ Le Service SCPT confirme dans l'attestation que le fournisseur a apporté la preuve de la disponibilité à fournir certains types de renseignements et à mettre en œuvre certains types de surveillance.

Art. 32 Durée de validité de l'attestation

¹ L'attestation de la disponibilité à renseigner et à surveiller est valable trois ans.

² À l'issue de cette durée, le Service SCPT peut prolonger la validité de l'attestation par période de trois ans si la personne obligée de collaborer atteste qu'aucun changement susceptible d'affecter la transmission des données ou sa capacité à renseigner et à surveiller n'est intervenu entre-temps.

³ Le fournisseur qui n'est plus en mesure de garantir sa disponibilité à renseigner et à surveiller en informe sans délai le Service SCPT.

Art. 33 Procédure de contrôle

Le DFJP définit la procédure de contrôle de la disponibilité à renseigner et à surveiller.

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

Le Service SCPT annule immédiatement une attestation de la disponibilité à renseigner et à surveiller pour le type de renseignements ou de surveillance concerné:

- a. si le fournisseur lui indique qu'il n'est plus en mesure de garantir sa disponibilité à renseigner et à surveiller;
- b. si le fournisseur n'est pas en mesure, dans plusieurs cas, de garantir la transmission des données ou la disponibilité à renseigner et à surveiller;
- c. si des indications faites par le fournisseur pour l'obtention de l'attestation ne sont pas conformes à la vérité.

Section 4

Types de renseignements concernant des services d'accès au réseau

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

¹ Le type de renseignements IR_4_NA a pour objet les indications ci-après sur les usagers de services d'accès au réseau:

- a. si disponible, l'identifiant de l'utilisateur (par ex. numéro de client);

- b. pour les services de communication mobile, les indications relatives à la personne physique ou morale selon l'art. 20 et, si ces données sont connues, d'autres coordonnées et le sexe de la personne physique;
- c. pour les autres services d'accès au réseau, les données d'identification selon l'art. 19 et, si ces données sont connues, les indications relatives à la personne physique ou morale, d'autres coordonnées et le sexe de la personne physique;
- d. les indications ci-après sur chacun des services d'accès au réseau du fournisseur utilisés par l'utilisateur:
 1. l'identifiant du fournisseur (par ex. numéro de FST),
 2. l'identifiant du service (par ex. nom d'utilisateur, MSISDN, identifiant DSL),
 3. la période d'utilisation du service (début, première activation et, éventuellement, fin),
 4. le cas échéant, d'autres indications concernant des options supplémentaires ou des restrictions du service d'accès au réseau,
 5. le cas échéant, l'adresse d'installation de l'accès fixe au réseau et la période de validité de celle-ci,
 6. le statut du service selon la désignation interne du fournisseur (par ex. actif, suspendu, bloqué) et la période de validité de chaque statut,
 7. le cas échéant, les adresses IP statiques, les préfixes IP, les plages d'adresses IP, ainsi que les masques de réseau ou les longueurs de préfixe attribués au service d'accès au réseau et leur période de validité respective,
 8. dans le cas de relations commerciales qui ne sont pas fondées sur un abonnement, l'heure et le lieu (nom et adresse complète) de remise du moyen d'accès, ainsi que le nom de la personne qui s'en est chargée,
 9. le cas échéant, le numéro SIM (ICCID) au moment de la remise,
 10. le cas échéant, l'IMSI,
 11. le type de service (par ex. à prépaiement, sur abonnement),
 12. le cas échéant, l'identifiant alternatif de l'utilisateur pour le service d'accès au réseau.

² La demande de renseignements précise la période sur laquelle porte la requête. Elle contient au moins un des critères de recherche ci-après. En cas d'indication d'un critère selon les let. a à e, il y a lieu de préciser un deuxième critère de recherche. Pour les recherches de chaînes de caractères (let. a, c, d et f), le fournisseur effectue une recherche exacte selon les règles pertinentes du DFJP:

- a. les nom et prénom;
- b. la date de naissance;
- c. le pays et le numéro postal d'acheminement ou le pays et la localité;
- d. la rue et, éventuellement, le numéro;
- e. le numéro et, le cas échéant, le type de la pièce d'identité;

- f. dans le cas de personnes morales, le nom et, éventuellement, le siège;
- g. le numéro d'identification de l'entreprise (IDE);
- h. l'identifiant de l'utilisateur (par ex. numéro de client);
- i. l'identifiant du service, hors adresses IP (par ex. nom d'utilisateur, MSISDN, identifiant DSL);
- j. l'IMSI;
- k. le numéro SIM (ICCID).

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

¹ Le type de renseignements IR_6_NA a pour objet les indications ci-après sur des services d'accès au réseau. Pour les indications selon les let. b, c et e, il y a lieu de préciser la période de validité commune:

- a. si disponible, l'identifiant de l'utilisateur (par ex. numéro de client);
- b. l'identifiant du service (par ex. nom d'utilisateur, identifiant DSL);
- c. le cas échéant, l'IMSI et le MSISDN;
- d. la liste des identifiants selon les normes internationales (par ex. IMEI, adresse MAC) des équipements utilisés en lien avec le service auprès du fournisseur et, si disponible, leur désignation en toutes lettres;
- e. le cas échéant, les numéros SIM (ICCID);
- f. le cas échéant, les codes PUK et PUK2.

² La demande de renseignements précise la période sur laquelle porte la requête. Elle contient au moins un des critères de recherche suivants:

- a. l'identifiant du service, hors adresses IP (par ex. nom d'utilisateur, MSISDN, identifiant DSL);
- b. l'IMSI;
- c. l'identifiant de l'équipement selon les normes internationales (par ex. IMEI, adresse MAC);
- d. l'adresse d'installation de l'accès fixe au réseau.

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

¹ Le type de renseignements IR_7_IP a pour objet les indications ci-après à des fins d'identification dans le cas d'une adresse IP attribuée de manière univoque au moment indiqué:

- a. si disponible, l'identifiant de l'utilisateur (par ex. nom d'utilisateur);
- b. l'identifiant du service d'accès au réseau (par ex. nom d'utilisateur, MSISDN, identifiant DSL);

- c. l'identifiant du fournisseur du service d'accès au réseau (par ex. le numéro de FST).

² La demande de renseignements contient les indications suivantes:

- a. l'adresse IP;
- b. le moment sur lequel porte la requête, avec précision de la date et de l'heure.

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

¹ Le type de renseignements IR_8_IP (NAT) a pour objet les indications ci-après à des fins d'identification dans le cas d'une adresse IP qui n'est pas attribuée de manière univoque (traduction d'adresses de réseau):

- a. si disponible, l'identifiant de l'utilisateur (par ex. nom d'utilisateur);
- b. l'identifiant du service d'accès au réseau (par ex. nom d'utilisateur, MSISDN, identifiant DSL).

² La demande de renseignements contient, à des fins d'identification, les indications ci-après concernant la procédure de traduction d'adresses de réseau:

- a. l'adresse IP source publique;
- b. si nécessaire pour l'identification, le numéro de port source public;
- c. si nécessaire pour l'identification, l'adresse IP publique de destination;
- d. si nécessaire pour l'identification, le numéro de port de destination;
- e. si nécessaire pour l'identification, le type de protocole de transport;
- f. le moment sur lequel porte la requête, avec précision de la date et de l'heure.

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

¹ Le type de renseignements IR_9_NAT a pour objet les indications ci-après en lien avec des procédures de traduction d'adresses de réseau, si nécessaire pour l'identification:

- a.¹⁶ l'adresse IP source avant ou après la traduction;
- b.¹⁷ le numéro de port source avant ou après la traduction.

² La demande de renseignements contient les indications ci-après concernant la procédure de traduction d'adresses de réseau:

- a.¹⁸ l'adresse IP source avant ou après la traduction;
- b.¹⁹ le numéro de port source avant ou après la traduction;

¹⁶ Erratum du 9 avr. 2019 (RO 2019 1201).

¹⁷ Erratum du 9 avr. 2019 (RO 2019 1201).

¹⁸ Erratum du 9 avr. 2019 (RO 2019 1201).

¹⁹ Erratum du 9 avr. 2019 (RO 2019 1201).

- c. si nécessaire pour l'identification, l'adresse IP publique de destination;
- d. si nécessaire pour l'identification, le numéro de port de destination;
- e. le type de protocole de transport;
- f. le moment de la traduction, avec précision de la date et de l'heure.

Section 5 Types de renseignements concernant des applications

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

¹ Le type de renseignements IR_10_TEL a pour objet les indications ci-après sur les usagers de services de téléphonie et multimédia:

- a. si disponible, l'identifiant de l'utilisateur (par ex. numéro de client);
- b.²⁰ pour les services de communication mobile, les indications relatives à la personne physique ou morale selon l'art. 20 et, si ces données sont connues, d'autres coordonnées et le sexe de la personne physique;
- c. pour les autres services de téléphonie et multimédia, les données d'identification selon l'art. 19 et, si ces données sont connues, les indications relatives à la personne physique ou morale, d'autres coordonnées et le sexe de la personne physique;
- d. les indications ci-après sur chacun des services de téléphonie et multimédia du fournisseur utilisés par l'utilisateur:
 1. l'identifiant du fournisseur (par ex. numéro de FST),
 2. l'identifiant du service (par ex. numéro de téléphone, SIP URI),
 3. la période d'utilisation du service (début, première activation et, le cas échéant, fin),
 4. le type de service (par ex. installation privée de télécommunication, poste téléphonique payant public, service fixe ou mobile),
 5. le cas échéant, l'adresse d'installation de l'accès fixe au réseau et sa période de validité,
 6. le statut du service selon la désignation interne du fournisseur (par ex. actif, suspendu, bloqué),
 7. le cas échéant, la liste ou la plage des autres ressources d'adressage ou identifiants enregistrés en lien avec le service (par ex. numéros de téléphone, IMPU),
 8. dans le cas de relations commerciales qui ne sont pas fondées sur un abonnement, l'heure et le lieu (nom et adresse complète) de remise du moyen d'accès, ainsi que le nom de la personne qui s'en est chargée,
 9. le cas échéant, les indications relatives aux présélections pour le libre choix du fournisseur des liaisons,

²⁰ Erratum du 3 déc. 2019 (RO 2019 4085).

10. le cas échéant, l'IMSI,

11. le cas échéant, le numéro SIM (ICCID) au moment de la remise.

² La demande de renseignements précise la période sur laquelle porte la requête. Elle contient au moins un des critères de recherche ci-après. En cas d'indication d'un critère selon les let. a à d, il y a lieu de préciser un deuxième critère de recherche. Pour les recherches de chaînes de caractères (let. a, c, d et f), le fournisseur effectue une recherche exacte selon les règles pertinentes du DFJP:

- a. les nom et prénom;
- b. la date de naissance;
- c. le pays et le numéro postal d'acheminement ou le pays et la localité;
- d. la rue et, éventuellement, le numéro;
- e. le numéro et, éventuellement, le type de la pièce d'identité;
- f. dans le cas de personnes morales, le nom et, éventuellement, le siège;
- g. le numéro d'identification de l'entreprise (IDE);
- h. l'identifiant de l'utilisateur (par ex. numéro de client);
- i. les ressources d'adressage ou les identifiants (par ex. numéro de téléphone, SIP URI, TEL URI, IMPU);
- j. l'IMSI;
- k. le numéro SIM (ICCID).

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

¹ Le type de renseignements IR_12_TEL a pour objet les indications ci-après sur des services de téléphonie et multimédia. Pour les indications selon les let. b, c et e, il y a lieu de préciser la période de validité commune:

- a. si disponible, l'identifiant de l'utilisateur (par ex. numéro de client);
- b. les ressources d'adressage ou les identifiants enregistrés pour le service (par ex. numéros de téléphone, SIP URI, IMPI);
- c. si pertinent, l'IMSI;
- d. à des fins d'identification, la liste des identifiants selon les normes internationales (par ex. IMEI, adresse MAC) des équipements utilisés en lien avec le service auprès du fournisseur et, si disponible, leur désignation en toutes lettres;
- e. le cas échéant, les numéros SIM (ICCID);
- f. le cas échéant, les codes PUK et PUK2.

² La demande de renseignements précise la période sur laquelle porte la requête. Elle contient au moins un des critères de recherche suivants:

- a. la ressource d'adressage (par ex. numéro de téléphone, SIP URI, MSISDN, TEL URI);
- b. l'IMSI;
- c. l'identifiant de l'équipement selon les normes internationales (par ex. IMEI, adresse MAC);
- d. les adresses d'installation de l'accès fixe au réseau;
- e. l'identifiant du service (par ex. IMPI).

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

¹ Le type de renseignements IR_13_EMAIL a pour objet les indications ci-après sur les usagers de services de courrier électronique:

- a. si disponible, l'identifiant de l'utilisateur (par ex. numéro de client);
- b. les données d'identification selon l'art. 19 et, si ces données sont connues, les indications relatives à la personne physique ou morale, d'autres coordonnées et le sexe de la personne physique;
- c. les indications ci-après sur le service de courrier électronique du fournisseur utilisé par l'utilisateur:
 1. l'identifiant du fournisseur,
 2. l'identifiant du service (par ex. adresse électronique, nom d'utilisateur),
 3. la période d'utilisation du service (début, première activation et, éventuellement, fin),
 4. le cas échéant, la liste de toutes les autres ressources d'adressage (par ex. alias de messagerie) concernant le service,
 5. le cas échéant, la liste de toutes les adresses auxquelles ont été transférés les messages envoyés à l'adresse indiquée dans la demande (par ex. liste de diffusion);
- d. le cas échéant, les autres ressources d'adressage enregistrées auprès du fournisseur en lien avec le service (par ex. adresse électronique, MSISDN).

² La demande de renseignements précise la période sur laquelle porte la requête. Elle contient au moins un des critères de recherche ci-après. En cas d'indication d'un critère selon les let. a à d, il y a lieu de préciser un deuxième critère de recherche. Pour les recherches de chaînes de caractères (let. a, c, d et f), le fournisseur effectue une recherche exacte selon les règles pertinentes du DFJP:

- a. les nom et prénom;
- b. la date de naissance;
- c. le pays et le numéro postal d'acheminement ou le pays et la localité;
- d. la rue et, éventuellement, le numéro;
- e. le numéro et, le cas échéant, le type de la pièce d'identité;
- f. dans le cas de personnes morales, le nom et, éventuellement, le siège;

- g. le numéro d'identification de l'entreprise (IDE);
- h. l'identifiant de l'utilisateur (par ex. numéro de client);
- i. l'identifiant du service (par ex. adresse électronique, nom d'utilisateur).

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

¹ Le type de renseignements IR_15_COM a pour objet les indications ci-après sur les usagers d'autres services de télécommunication ou de services de communication dérivés (par ex. des services de messagerie, des services de communication intégrés dans des réseaux sociaux, des services d'informatique en nuage et des services de serveur mandataire):

- a. si disponible, l'identifiant de l'utilisateur (par ex. numéro de client);
- b. les données d'identification selon l'art. 19 et, si ces données sont connues, les indications relatives à la personne physique ou morale, d'autres coordonnées et le sexe de la personne physique;
- c. les indications ci-après sur un autre service de télécommunication ou un service de communication dérivé du fournisseur utilisé par l'utilisateur:
 - 1. l'identifiant du fournisseur,
 - 2. l'identifiant du service (par ex. nom d'utilisateur),
 - 3. la période d'utilisation du service (début, première activation et, éventuellement, fin),
 - 4. le statut du service selon les désignations internes du fournisseur (par ex. actif, suspendu, bloqué) et la période de validité respective de chaque statut,
 - 5. la liste des autres ressources d'adressage ou identifiants enregistrés en lien avec le service.

² La demande de renseignements précise la période sur laquelle porte la requête. Elle contient au moins un des critères de recherche ci-après. En cas d'indication d'un critère selon les let. a à d, il y a lieu de préciser un deuxième critère de recherche. Pour les recherches de chaînes de caractères (let. a, c, d et f), le fournisseur effectue une recherche exacte selon les règles pertinentes du DFJP:

- a. les nom et prénom;
- b. la date de naissance;
- c. le pays et le numéro postal d'acheminement ou le pays et la localité;
- d. la rue et, éventuellement, le numéro;
- e. le numéro et, le cas échéant, le type de la pièce d'identité;
- f. dans le cas de personnes morales, le nom et, le cas échéant, le siège;
- g. le numéro d'identification de l'entreprise (IDE);
- h. l'identifiant de l'utilisateur (par ex. numéro de client);

- i. la ressource d'adressage ou l'identifiant (par ex. nom d'utilisateur).

Section 6 Autres types de renseignements

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

¹ Le type de renseignements IR_17_PAY a pour objet les indications ci-après sur la méthode de paiement utilisée par les usagers de services de télécommunication et de services de communication dérivés:

- a. l'identifiant du fournisseur;
- b. l'identifiant de l'utilisateur (par ex. numéro de client);
- c. l'identifiant attribué par le fournisseur à l'utilisateur pour l'établissement des décomptes et la facturation;
- d. l'identifiant du service (par ex. numéro de téléphone, SIP URI, nom d'utilisateur);
- e. la méthode de paiement (débit, virement ou prépaiement);
- f. les renseignements relatifs au compte de l'utilisateur enregistrés auprès du fournisseur, à savoir le nom de la banque, le titulaire du compte et l'IBAN (ou le BIC et le numéro de compte) ou le code pays de la banque et le numéro de compte;
- g. les adresses de facturation (rue et numéro, case postale, NPA, localité, pays) et leurs périodes de validité respectives (début et, le cas échéant, fin).

² Le fournisseur livre les données visées à l'al. 1 pour autant qu'elles soient disponibles.

³ La demande de renseignements précise la période sur laquelle porte la requête. Elle contient au moins un des critères de recherche suivants:²¹

- a. l'identifiant de l'utilisateur (par ex. numéro de client);
- b. l'identifiant du service (par ex. numéro de téléphone, SIP URI, nom d'utilisateur);
- c. l'identifiant attribué par le fournisseur à l'utilisateur pour l'établissement des décomptes et la facturation;
- d. les renseignements relatifs au compte de l'utilisateur, à savoir l'IBAN (ou le BIC et le numéro de compte) ou le code pays de la banque et le numéro de compte;
- e. l'adresse de facturation (rue et numéro, case postale, NPA, localité, pays).

²¹ Erratum du 6 mars 2018 (RO 2018 989).

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

¹ Le type de renseignements IR_18_ID a pour objet la livraison d'une copie électronique de la pièce d'identité de l'utilisateur enregistrée conformément à l'art. 20.

² La demande de renseignements indique le moment sur lequel porte la requête, ainsi que l'identifiant de l'utilisateur ou du service, le numéro SIM (ICCID) ou l'IMSI ou encore, le cas échéant, l'identifiant de l'équipement auquel elle se rapporte.

Art. 46 Type de renseignements IR_19_BILL: copie de factures

¹ Le type de renseignements IR_19_BILL a pour objet la livraison d'une copie électronique de toutes les factures disponibles pour l'utilisateur, sans les données secondaires relatives aux services de télécommunication et aux services de communication dérivés.

² La demande de renseignements précise la période sur laquelle porte la requête, ainsi que l'identifiant de l'utilisateur ou l'identifiant du service ou encore l'identifiant utilisé pour la facturation auquel elle se rapporte.

Art. 47 Type de renseignements IR_20_CONTRACT: copie du contrat

¹ Le type de renseignements IR_20_CONTRACT a pour objet la livraison d'une copie électronique de tous les documents contractuels disponibles pour l'utilisateur concernant des services de télécommunication et des services de communication dérivés.

² La demande de renseignements indique le moment sur lequel porte la requête, ainsi que l'identifiant de l'utilisateur ou du service, le numéro SIM (ICCID) ou l'IMSI ou encore, le cas échéant, l'identifiant de l'équipement auquel elle se rapporte.

Art. 48 Type de renseignements IR_21_TECH: données techniques

¹ Le type de renseignements IR_21_TECH a pour objet la livraison de données techniques de systèmes de télécommunication et d'éléments réseau, en particulier les données de localisation de cellules de téléphonie mobile et de points d'accès publics au réseau WLAN.

² Les données de localisation comprennent:

- a. les identifiants des éléments réseau (par ex. CGI, ECGI, SAI, RAI, TAI, BSSID) et les coordonnées géographiques ou d'autres indications standardisées concernant la position selon les normes internationales;
- b. le cas échéant, l'adresse postale de la position;
- c. le cas échéant, la direction principale d'émission de l'antenne, et
- d. le cas échéant, d'autres caractéristiques disponibles concernant la position.

³ La demande de renseignements précise la période sur laquelle porte la requête. Elle contient au moins un des critères de recherche suivants:

- a. les coordonnées géographiques de la position de l'élément réseau;
- b. l'identifiant de l'élément réseau (par ex. CGI, ECGI, BSSID).

Section 7

Dispositions générales concernant la surveillance de la correspondance par télécommunication

Art. 49 Ordre de surveillance de la correspondance par télécommunication

¹ L'ordre de surveillance transmis au Service SCPT contient les indications suivantes:

- a. les coordonnées de l'autorité qui ordonne la surveillance;
- b. les coordonnées des personnes autorisées auxquelles les données issues de la surveillance sont destinées;
- c. pour autant que ces informations soient connues: les nom, prénom, date de naissance, adresse et profession de la personne à surveiller;
- d. le numéro de référence et le nom de l'affaire à laquelle se rapportent les surveillances;
- e. le motif de la surveillance, en particulier l'infraction qu'elle doit permettre d'élucider;
- f. le nom des personnes obligées de collaborer;
- g. les types de surveillance ordonnés ou le type de surveillance spéciale ordonnée;
- h. les identifiants à surveiller (target ID);
- i. si nécessaire, la demande relative à l'autorisation générale de surveiller plusieurs raccords sans qu'il soit nécessaire de demander à chaque fois une nouvelle autorisation (art. 272, al. 2 et 3, CPP ou art. 70c, al. 2 et 3, PPM);
- j. le début et la fin de la surveillance;
- k. dans le cas de personnes tenues au secret professionnel au sens de l'art. 271, al. 1, CPP ou de l'art. 70b, al. 1, PPM: une mention indiquant cette particularité;
- l. le cas échéant, les mesures visant à protéger les personnes tenues au secret professionnel et d'autres mesures de protection que les autorités et le Service SCPT doivent mettre en œuvre.

² Si l'exécution de la surveillance l'exige, le DFJP peut prévoir que l'ordre de surveillance transmis au Service SCPT doit contenir des indications techniques supplémentaires.

Art. 50 Obligations en matière de surveillance

¹ Chaque FST et chaque fournisseur de services de communication dérivés ayant des obligations étendues en matière de surveillance visé à l'art. 52 doit être en mesure d'exécuter ou de faire exécuter par des tiers les surveillances selon les sections 8 à 12 du présent chapitre (art. 54 à 69) concernant les services qu'il propose. Cette obligation ne s'applique pas aux FST ayant des obligations restreintes en matière de surveillance visés à l'art. 51.

² Le fournisseur doit garantir la disponibilité à surveiller la correspondance par télécommunication dès le début de l'exploitation commerciale d'un service.

³ Il doit garantir qu'il est en mesure, également en dehors des heures normales de travail selon l'art. 10, de réceptionner et d'exécuter, ou de faire exécuter par des tiers, les mandats de surveillance conformément aux prescriptions du DFJP.

⁴ Durant la période fixée dans le mandat de surveillance, il doit garantir qu'il peut exécuter la surveillance de toute la correspondance par télécommunication qui transite par l'infrastructure qu'il contrôle, si cette correspondance est effectuée au moyen des services surveillés et qu'elle peut être attribuée à l'identifiant surveillé (*target ID*).

⁵ Si nécessaire, il apporte son soutien au Service SCPT pour vérifier que les informations recueillies lors de la surveillance correspondent bien à la correspondance par télécommunication indiquée dans le mandat de surveillance.

⁶ Si d'autres identifiants sont associés à l'identifiant surveillé (*target ID*; par ex. IMPI avec IMPU, adresse électronique avec alias de messagerie), le fournisseur veille à ce qu'ils soient aussi surveillés dans le cadre du type de surveillance ordonné.

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

¹ Sur demande d'un FST, le Service SCPT le déclare comme ayant des obligations restreintes en matière de surveillance (art. 26, al. 6, LSCPT):

- a. s'il n'offre ses services que dans le domaine de la recherche et de l'éducation, ou
- b. s'il n'atteint aucune des valeurs suivantes:
 1. des mandats de surveillance portant sur dix cibles différentes au cours des douze derniers mois (date de référence: 30 juin),
 2. un chiffre d'affaires annuel en Suisse de 100 millions de francs pendant deux exercices consécutifs généré par les services de télécommunication et les services de communication dérivés.

² L'art. 22, al. 2, s'applique par analogie pour le calcul des valeurs selon l'al. 1, let. b.

³ Les FST ayant des obligations restreintes en matière de surveillance sont tenus d'informer le Service SCPT par écrit, justificatifs à l'appui:

- a. s'ils n'offrent plus leurs services exclusivement dans le domaine de la recherche et de l'éducation, ou
- b. lorsqu'ils atteignent, pendant deux exercices consécutifs, les valeurs selon l'al. 1, let. b, ch. 2. La communication doit intervenir dans les trois mois suivant la fin d'un exercice.

⁴ Le Service SCPT peut récupérer les données issues de la mise en œuvre de la législation sur la surveillance de la correspondance par poste et télécommunication, ainsi que les données obtenues par d'autres autorités lors de la mise en œuvre du droit fédéral.

⁵ Un FST doit garantir l'enregistrement des données nécessaires pour assurer l'exécution des surveillances et la disponibilité à surveiller respectivement dans les deux et

les douze mois à compter du moment où le Service SCPT décide qu'il n'est plus considéré comme ayant des obligations restreintes en matière de surveillance.

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

¹ Le Service SCPT déclare, par une décision, un fournisseur de services de communication dérivés comme ayant des obligations étendues en matière de surveillance (art. 27, al. 3, LSCPT) lorsque celui-ci atteint une des valeurs suivantes:

- a. des mandats de surveillance concernant dix cibles différentes au cours des douze derniers mois (date de référence: 30 juin);
- b. un chiffre d'affaires annuel en Suisse de 100 millions de francs pendant deux exercices consécutifs, une grande partie de ce chiffre d'affaires devant être générée par la fourniture de services de communication dérivés, et 5000 usagers.

² L'art. 22, al. 2 à 5, s'applique par analogie.

Art. 53 Accès aux installations

¹ Les personnes obligées de collaborer qui sont tenues de garantir l'accès à leurs installations permettent au Service SCPT ou au tiers mandaté par lui d'accéder, dans les limites nécessaires à l'exécution de la surveillance, aux bâtiments, aux équipements, aux lignes, aux systèmes, aux réseaux et aux services.

² Elles mettent gratuitement à disposition les accès existants aux réseaux de télécommunication publics. Si l'exécution de la surveillance le requiert, elles mettent en place, en collaboration avec le Service SCPT ou les tiers mandatés par lui, de nouveaux accès au réseau aux frais du Service SCPT.

Section 8

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

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

¹ Le type de surveillance RT_22_NA_IRI a pour objet la surveillance en temps réel d'un service mobile d'accès au réseau.

² Doivent être transmises en temps réel les données secondaires ci-après des communications émises ou reçues via le service d'accès au réseau surveillé:

- a. lorsque l'accès au réseau est établi ou déconnecté: la date, l'heure, le type d'événement et le motif de la déconnexion;
- b. la nature de l'accès au réseau;
- c. les données d'authentification, d'autorisation et de comptabilité (informations AAA) du service d'accès au réseau surveillé, en particulier l'identifiant d'usager, et, dans le cas de la téléphonie mobile, l'IMSI;

- d. les adresses ou plages d'adresses IP attribuées au service d'accès au réseau, ainsi que la date et l'heure de leur attribution;
- e. les ressources d'adressage disponibles pour le service d'accès au réseau surveillé, par exemple le MSISDN ou l'IMSI dans le cas de la téléphonie mobile;
- f. les identifiants, selon les normes internationales, des équipements terminaux sur lesquels est utilisé le service d'accès au réseau surveillé (par ex. IMEI, adresse MAC);
- g. la nature, la date et l'heure de début et, le cas échéant, de fin des changements techniques enregistrés sur l'accès au réseau (par ex. actualisation de la position, changement de technologie de communication mobile) et, si cette information est connue, la cause de ces changements;
- h. les données de localisation selon l'al. 3 qui sont disponibles pour la cible ou la cellule ou le point d'accès au réseau WLAN utilisé par la cible.

³ Les données de localisation comprennent:

- a. les identifiants ou une combinaison d'identifiants (par ex. CGI, ECGI, SAI, RAI, TAI, BSSID), les coordonnées géographiques, le cas échéant, la direction principale d'émission de la cellule ou du point d'accès au réseau WLAN et, si ces données sont disponibles, le type de technologie de communication mobile utilisée;
- b. la position de la cible déterminée par le réseau et exprimée sous la forme de coordonnées géographiques accompagnées des valeurs d'incertitude correspondantes ou sous la forme de polygones, avec indication des coordonnées géographiques de chaque point de polygonation, ainsi que, si ces données sont disponibles, le type de technologie de communication mobile utilisée, ou
- c. si ces données sont disponibles, d'autres indications, selon les normes internationales, concernant la localisation de la cible ou de la cellule ou du point d'accès au réseau WLAN, ainsi que le type de technologie de communication mobile utilisée.

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

Le type de surveillance RT_23_NA_CC_IRI a pour objet la surveillance en temps réel d'un service d'accès au réseau. Doivent être transmis en temps réel le contenu des communications émises ou reçues via le service d'accès au réseau surveillé, ainsi que les données secondaires s'y rapportant selon l'art. 54, al. 2 et 3.

Section 9 Types de surveillance en temps réel d'applications

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

¹ Le type de surveillance RT_24_TEL_IRI a pour objet la surveillance en temps réel d'un service de téléphonie et multimédia, y compris, le cas échéant, des services convergents, en particulier les SMS, la messagerie vocale et les services de communication riches. Doivent être transmises en temps réel les données secondaires ci-après des communications émises, traitées ou reçues via les services surveillés:²²

- a. la date et l'heure des procédures de connexion et de déconnexion, ainsi que leur résultat;
- b.²³ les données d'authentification, d'autorisation et de comptabilité (informations AAA) des services surveillés et les informations relatives aux événements d'enregistrement et de souscription ainsi que les réponses correspondantes, en particulier l'identifiant d'utilisateur (par ex. SIP URI, IMPI) et, dans le cas de la téléphonie mobile, l'IMSI;
- bbis.²⁴ le cas échéant, les adresses IP et les numéros de port du client et du serveur ainsi que les indications concernant le protocole utilisé;
- c. les informations de signalisation, en particulier celles relatives au système serveur, au statut de l'utilisateur et à la qualité du service;
- d. le cas échéant, les informations de présence;
- e. dans le cas de communications, de tentatives d'établissement de communications et de changements techniques (par ex. intégration de services supplémentaires, intégration de services convergents ou passage à de tels services, changement de technologie de communication mobile, actualisation de la position), le cas échéant:
 1. leur nature, ainsi que la date et l'heure de début et, éventuellement, de fin,
 2. les ressources d'adressage (par ex. MSISDN, numéro E.164, SIP URI, IMPU) de tous les participants à la communication et leur rôle,
 3. l'adresse de destination réelle connue et les adresses intermédiaires disponibles, si la communication ou la tentative d'établissement de la communication a été déviée ou transférée,
 4. les identifiants, selon les normes internationales, des équipements terminaux sur lesquels sont utilisés les services surveillés (par ex. IMEI, adresse MAC),
 5. les autres identifiants disponibles,

²² Nouvelle teneur selon le ch. I 12 de l'O du 4 mai 2022 sur les mesures policières de lutte contre le terrorisme, en vigueur depuis le 1^{er} juin 2022 (RO 2022 301).

²³ Nouvelle teneur selon le ch. I 12 de l'O du 4 mai 2022 sur les mesures policières de lutte contre le terrorisme, en vigueur depuis le 1^{er} juin 2022 (RO 2022 301).

²⁴ Introduite par le ch. I 12 de l'O du 4 mai 2022 sur les mesures policières de lutte contre le terrorisme, en vigueur depuis le 1^{er} juin 2022 (RO 2022 301).

6. la raison pour laquelle la communication a pris fin ou n'a pas pu être établie ou la cause du changement technique,
7. les informations de signalisation concernant des services supplémentaires (par ex. audioconférences, transferts d'appels, codes DTMF),
8. le statut de la communication ou de la tentative d'établissement de la communication,
9. dans le cas de services mobiles, aussi les données de localisation selon l'al. 2 qui sont disponibles pour la cible ou la cellule ou le point d'accès au réseau WLAN utilisé par la cible.

² Les données de localisation comprennent:

- a. les identifiants ou une combinaison d'identifiants (par ex. CGI, ECGI, SAI, RAI, TAI, BSSID), les coordonnées géographiques, le cas échéant, la direction principale d'émission de la cellule ou du point d'accès au réseau WLAN, ainsi que, si ces données sont disponibles, le type de technologie de communication mobile utilisée;
- b. la position, déterminée par le réseau, de l'équipement terminal sur lequel sont utilisés les services surveillés, exprimée sous la forme par exemple de coordonnées géographiques accompagnées de la valeur d'incertitude correspondante ou sous la forme de polygones, avec indication des coordonnées géographiques de chaque point de polygonation, ainsi que le type de technologie de communication mobile utilisée, ou
- c. si ces données sont disponibles, d'autres indications, selon les normes internationales, concernant la localisation de la cellule ou du point d'accès au réseau WLAN, ainsi que le type de technologie de communication mobile utilisée.

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

Le type de surveillance RT_25_TEL_CC_IRI a pour objet la surveillance en temps réel d'un service de téléphonie ou multimédia, y compris, le cas échéant, des services convergents, en particulier les SMS, la messagerie vocale et les services de communication riches. Doivent être transmis en temps réel le contenu des communications émises, traitées ou reçues via les services surveillés, ainsi que les données secondaires au sens de l'art. 56 s'y rapportant.

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

Le type de surveillance RT_26_EMAIL_IRI a pour objet la surveillance en temps réel d'un service de courrier électronique. Doivent être transmises en temps réel les données secondaires ci-après des communications émises, traitées ou reçues via le service surveillé:

- a. la date et l'heure des procédures de connexion et de déconnexion, ainsi que leur statut;
- b. les données d'authentification, d'autorisation et de comptabilité (informations AAA) du service surveillé, en particulier l'identifiant d'utilisateur, ainsi que, le cas échéant, les alias de messagerie;
- c. les adresses IP et les numéros de port du client et du serveur, ainsi que les indications concernant le protocole utilisé;
- d. la date, l'heure, le volume de données, les adresses électroniques de l'expéditeur et du destinataire du message, ainsi que les adresses IP et les numéros de port du serveur d'envoi et du serveur de réception, concernant les événements suivants:
 1. l'envoi ou le transfert d'un message,
 2. la réception d'un message,
 3. le traitement d'un message dans la boîte aux lettres électronique,
 4. le téléchargement d'un message à partir de la boîte aux lettres électronique,
 5. le téléversement d'un message dans la boîte aux lettres électronique.

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

Le type de surveillance RT_27_EMAIL_CC_IRI a pour objet la surveillance en temps réel d'un service de courrier électronique. Doivent être transmis en temps réel le contenu des communications émises, traitées ou reçues via le service surveillé, ainsi que les données secondaires selon l'art. 58 s'y rapportant.

Section 10 Types de surveillance rétroactive

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

Le type de surveillance HD_28_NA a pour objet la surveillance rétroactive des données secondaires d'un service d'accès au réseau. Doivent être transmises les données secondaires ci-après des communications émises ou reçues via le service d'accès au réseau surveillé:

- a. la date et l'heure de début et, le cas échéant, de fin de la session ou sa durée;
- b. le type d'accès au réseau et son statut;
- c. l'identifiant utilisé pour l'authentification de l'utilisateur au point d'accès surveillé, par exemple le nom d'utilisateur;
- d. les adresses ou pages d'adresses IP attribuées à la cible et leur statut;

- e. si ces données sont disponibles, l'identifiant, selon les normes internationales, de l'équipement terminal de la cible (par ex. adresse MAC, IMEI dans le cas de la téléphonie mobile);
- f. si ces données sont disponibles, les volumes de données téléversées et téléchargées pendant la session;
- g. en cas d'accès au réseau via le réseau mobile: les informations GPRS ou EPS (en particulier IMSI ou MSISDN) et les données de localisation au début et à la fin de la session, ainsi que pendant la session si ces données sont disponibles; si ces données sont connues, il y a lieu de transmettre des données de localisation supplémentaires de la navigation maritime ou aérienne; les données de localisation à fournir sont les suivantes:
 - 1. les identifiants de cellule ou de zone géographique, les coordonnées géographiques, l'adresse postale, et, le cas échéant, les directions principales d'émission des cellules utilisées par la cible,
 - 2. les positions de la cible déterminées par le réseau et exprimées sous la forme, par exemple, de coordonnées géographiques accompagnées de la valeur d'incertitude correspondante ou de polygones, avec indication des coordonnées géographiques de chaque point de polygonation, ainsi que les adresses postales correspondantes, ou
 - 3. d'autres indications, selon les normes internationales, concernant les positions de la cible ou les cellules utilisées par elle, ainsi que les adresses postales correspondantes;
- h. en cas d'accès au réseau via un réseau WLAN public: le BSSID et, si disponibles, le SSID et les données de localisation sous la forme des coordonnées géographiques et de l'adresse postale du point d'accès au réseau WLAN utilisé par la cible; le nom d'utilisateur, le type d'authentification, les informations supplémentaires disponibles sur l'authentification de l'utilisateur (numéro de téléphone, adresse MAC, IMSI, identifiant d'utilisateur utilisé pour l'authentification et mot de passe) et l'adresse IP du point d'accès au réseau WLAN; si disponibles, il y a lieu de transmettre des données de localisation supplémentaires de la navigation maritime ou aérienne;
- i. en cas d'accès au réseau via le réseau fixe: les ressources d'adressage de l'accès au réseau et, si ces données sont disponibles, leur adresse postale.

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

Le type de surveillance HD_29_TEL a pour objet la surveillance rétroactive des données secondaires d'un service de téléphonie ou multimédia, y compris, le cas échéant, des services convergents, en particulier les SMS, les MMS et la messagerie vocale. Doivent être transmises les données secondaires ci-après des communications et tentatives d'établissement de communications établies via le service surveillé:

- a. leur nature, ainsi que la date et l'heure de début et, éventuellement, de fin ou leur durée;

- b. les ressources d'adressage (par ex. MSISDN, numéro E.164, SIP URI, IMPU) de tous les participants à la communication et leurs rôles respectifs;
- c. le motif pour la fin de la communication ou de la tentative d'établissement de la communication;
- d. dans le cas de services de communication mobile (s'agissant de services multimédia, si ces données sont disponibles): l'IMEI de l'équipement terminal de la cible et l'IMSI de la cible;
- e. le cas échéant, le type de service support;
- f. dans le cas de SMS et de MMS, des informations sur l'événement, le type (uniquement pour les SMS) et le statut;
- g. dans le cas de services de communication mobile, les données de localisation de la cellule utilisée au début et à la fin de la communication ou de la tentative d'établissement de la communication; si ces données sont connues, il y a lieu de transmettre des données de localisation supplémentaires de la navigation maritime ou aérienne; les données de localisation à fournir sont les suivantes:
 - 1. les identifiants de cellule et de zone géographique, les coordonnées géographiques et, le cas échéant, les directions principales d'émission et les adresses postales, ou
 - 2. les positions de la cible déterminées par le réseau (exprimées sous la forme, par exemple, de coordonnées géographiques accompagnées de la valeur d'incertitude correspondante ou de polygones, avec indication des coordonnées géographiques de chaque point de polygonation), ainsi que les adresses postales correspondantes ou
 - 3. d'autres indications, selon les normes internationales, concernant les positions de la cible ou des cellules utilisées par la cible, ainsi que les adresses postales correspondantes;
- h. dans le cas de services multimédia:
 - 1. l'adresse IP du client, avec précision du type, et le numéro de port,
 - 2. l'identifiant de corrélation généré pour la communication,
 - 3. les types de contenus multimédia,
 - 4. les informations sur les composantes multimédia (heure, nom, description, initiateur, identifiant de corrélation généré pour l'accès), et
 - 5. le cas échéant, les informations sur les services IMS (type de service utilisé, rôle de l'élément réseau dont sont issues les données secondaires, etc.);
- i. dans le cas de services multimédia, les informations sur l'accès au réseau utilisé par la cible:
 - 1. le type d'accès,
 - 2. la classe d'accès,
 - 3. si les informations sur l'accès sont issues du réseau, et

4. les données de localisation ci-après relatives à l'accès au réseau au début et la fin de la session multimédia et, si ces données sont disponibles, aussi pendant la session:
 - en cas d'accès au réseau via le réseau de communication mobile, les données de localisation de la cellule utilisée par la cible selon la let. g, ou
 - en cas d'accès au réseau via le réseau WLAN, les données de localisation disponibles pour le point d'accès au réseau WLAN utilisé par la cible (coordonnées géographiques, adresse postale), ou
 - en cas d'accès au réseau via le réseau fixe, l'adresse postale disponible pour l'accès utilisé par la cible.

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

Le type de surveillance HD_30_EMAIL a pour objet la surveillance rétroactive de données secondaires d'un service de courrier électronique. Doivent être transmises les données secondaires ci-après des communications émises, traitées ou reçues via les services surveillés:

- a. la date, l'heure, le type d'événement, les identifiants d'utilisateur, les éventuels alias de messagerie, les adresses de l'expéditeur et du destinataire, le protocole utilisé, les adresses IP du serveur et du client, ainsi que, le cas échéant, le statut de remise du message pour chacun des événements suivants: envoi, réception, connexion à la boîte de courrier électronique et déconnexion, et, si ces données sont disponibles, téléchargement, téléversement, suppression, traitement ou ajout d'un message;
- b. les adresses IP et les noms du serveur de courrier électronique expéditeur et destinataire.

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

Le type de surveillance HD_31_PAGING a pour objet la détermination de la dernière activité constatée (services d'accès au réseau et services de téléphonie et multimédia) par l'opérateur de communication mobile de l'équipement terminal mobile de la personne surveillée et indication du MSISDN, de l'IMSI et de l'IMEI (si disponible), du type de technologie de communication mobile, de la bande de fréquence, de l'identifiant du réseau de communication mobile, de la date et de l'heure de la dernière activité constatée, ainsi que de l'une des indications ci-après nécessaires aux fins de la localisation:

- a. les indications relatives à la cellule activée: l'identifiant ou une combinaison d'identifiants (par ex. CGI, ECGI, SAI, RAI, TAI), l'adresse postale, la direction principale d'émission ou, dans le cas de cellules complexes, les directions principales d'émission et le type de cellule, les coordonnées géographiques;

- b. l'adresse postale et les indications relatives à la position, déterminées par le réseau, de l'équipement terminal lors de la dernière activité constatée et exprimées sous la forme, par exemple, de coordonnées géographiques accompagnées des valeurs d'incertitude correspondantes ou sous la forme de polygones, avec indication des coordonnées géographiques de chaque point de polygonation, ou
- c. l'adresse postale et d'autres indications standardisées déterminées par le réseau concernant la position de l'équipement terminal lors de la dernière activité constatée ou concernant la localisation de la cellule activée.

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

¹ Le type de surveillance AS_32_PREP_COV a pour objet l'analyse de la couverture réseau préalablement à une recherche par champ d'antennes selon l'art. 66. Il est effectué par les FST afin d'identifier les cellules de téléphonie mobile ou les points d'accès publics au réseau WLAN le plus susceptibles de couvrir la localisation indiquée par l'autorité qui a ordonné la surveillance sous la forme de coordonnées géographiques ou d'une adresse postale, en tenant compte le cas échéant d'indications supplémentaires (par ex. heure du jour, conditions météorologiques, jour de la semaine, localisation à l'intérieur ou à l'extérieur d'un bâtiment).

² Le FST livre au Service SCPT une liste d'identifiants (par ex. CGI, ECGI) ou de BSSID correspondant aux cellules de téléphonie mobile ou aux points d'accès publics au réseau WLAN identifiés.

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

¹ Le type de surveillance AS_33_PREP_REF a pour objet l'identification, préalablement à une recherche par champ d'antennes selon l'art. 66, de cellules de téléphonie mobile ou de points d'accès publics au réseau WLAN au moyen de communications de référence ou d'accès au réseau de référence.

² L'autorité qui ordonne la surveillance fait effectuer, de manière autonome, des communications de référence ou des accès au réseau de référence à la localisation concernée et transmet au Service SCPT une liste avec les indications suivantes:

- a. la nature de la communication ou de l'accès au réseau;
- b. la date et l'heure de la communication ou de l'accès au réseau;
- c. les ressources d'adressage du service de téléphonie ou multimédia ou du service d'accès au réseau utilisé;
- d. le cas échéant, le nom du réseau de communication mobile utilisé.

³ Le Service SCPT charge les FST d'identifier, sur la base des données secondaires, les cellules de téléphonie mobile ou les points d'accès publics au réseau WLAN utilisés au début et à la fin des communications de référence ou des accès au réseau de

référence selon l'al. 2, avec mandat de lui livrer la liste visée à l'al. 2 complétée avec les identifiants de cellule (par ex. CGI, ECGI) ou les BSSID correspondants.

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

¹ Le type de surveillance AS_34 a pour objet la surveillance rétroactive de toutes les communications, tentatives d'établissement de communications et de tous les accès au réseau effectués via une cellule de téléphonie mobile ou un point d'accès public déterminé au réseau WLAN pendant une période pouvant aller jusqu'à deux heures.²⁵

² Le FST livre les données secondaires selon les art. 60 et 61 des communications au sens de l'al. 1.

Section 11

Recherche en cas d'urgence, recherche de personnes condamnées et localisation par téléphonie mobile de terroristes potentiels²⁶

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

Les types de surveillance pouvant être ordonnés pour une recherche en cas d'urgence selon l'art. 35 LSCPT sont les suivants:

- a. le type EP_35_PAGING: détermination de la dernière activité constatée (services d'accès au réseau et services de téléphonie et multimédia) par l'opérateur de communication mobile de l'équipement terminal mobile de la personne disparue ou d'un tiers et indication du MSISDN, de l'IMSI et de l'IMEI (si disponible), du type de technologie de communication mobile, de la bande de fréquence, de l'identifiant du réseau de communication mobile, de la date et de l'heure de la dernière activité constatée, ainsi que de l'une des indications ci-après nécessaires aux fins de la localisation:
 1. les indications relatives à la cellule activée: l'identifiant ou une combinaison d'identifiants (par ex. CGI, ECGI, SAI, RAI, TAI), l'adresse postale, la direction principale d'émission ou, dans le cas de cellules complexes, les directions principales d'émission et le type de cellule, les coordonnées géographiques,
 2. l'adresse postale et les indications relatives à la position, déterminées par le réseau, de l'équipement terminal lors de la dernière activité constatée et exprimées sous la forme, par exemple, de coordonnées géographiques accompagnées des valeurs d'incertitude correspondantes ou sous la forme de polygones, avec indication des coordonnées géographiques de chaque point de polygonation, ou
 3. l'adresse postale et d'autres indications standardisées déterminées par le réseau concernant la position de l'équipement terminal lors de la dernière activité constatée ou concernant la localisation de la cellule activée;

²⁵ Erratum du 3 juil. 2018, ne concerne que le texte italien (RO 2018 2551).

²⁶ Nouvelle teneur selon le ch. I 12 de l'O du 4 mai 2022 sur les mesures policières de lutte contre le terrorisme, en vigueur depuis le 1^{er} juin 2022 (RO 2022 301).

- b. le type EP_36_RT_CC_IRI (surveillance en temps réel du contenu et des données secondaires): combinaison des types de surveillance selon l'art. 55 (services d'accès au réseau) et l'art. 57 (services de téléphonie et multimédia);
- c. le type EP_37_RT_IRI (surveillance en temps réel des données secondaires de télécommunication): combinaison des types de surveillance selon l'art. 54 (services d'accès au réseau) et l'art. 56 (services téléphoniques et multimédia);
- d. le type EP_38_HD (surveillance rétroactive des données secondaires): combinaison des types de surveillance selon l'art. 60 (services d'accès au réseau) et l'art. 61 (services de téléphonie et multimédia).

Art. 68 Recherche de personnes condamnées

Les types de surveillance pouvant être ordonnés pour la recherche de personnes condamnées selon l'art. 36 LSCPT, en veillant à indiquer dans l'ordre de surveillance la mention «recherche de personnes condamnées» sous le motif de la surveillance (art. 49, al. 1, let. e), sont les suivants:

- a. un des types de surveillance en temps réel du contenu et des données secondaires de services d'accès au réseau ou d'applications selon les art. 55, 57 ou 59;
- b. un des types de surveillance en temps réel des données secondaires de services d'accès au réseau ou d'applications selon les art. 54, 56 ou 58;
- c. un des types de surveillance rétroactive des données secondaires de services d'accès au réseau ou d'applications selon les art. 60 à 63;
- d. une recherche par champ d'antennes selon l'art. 66 et les mesures préalables s'y rapportant selon les art. 64 et 65.

Art. 68a²⁷ Type de surveillance ML_50_RT: localisation par téléphonie mobile en temps réel de terroristes potentiels

¹ Le type de surveillance qui peut être ordonné pour la localisation par téléphonie mobile de terroristes potentiels en vertu de l'art. 23q, al. 3, de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure²⁸ est ML_50_RT.

² Ce type de surveillance a pour objet la combinaison de la surveillance en temps réel, à des fins de localisation par téléphonie mobile, des données secondaires de services d'accès au réseau mobile, de services mobiles de téléphonie et multimédia et, le cas échéant, de services mobiles convergents, en particulier les SMS, la messagerie vocale et les services de communication riches.

²⁷ Introduit par le ch. I 12 de l'O du 4 mai 2022 sur les mesures policières de lutte contre le terrorisme, en vigueur depuis le 1^{er} juin 2022 (RO 2022 301).

²⁸ RS 120

³ S'agissant des services d'accès au réseau mobile, les données secondaires des communications doivent être transmises conformément à l'art. 54, al. 2, let. a à c, g et h, et al. 3.

⁴ S'agissant des services mobiles de téléphonie et multimédia et des services mobiles convergents, les données secondaires des communications doivent être transmises conformément à l'art. 56, al. 1, let. a, b, d et e, ch. 1 et 9, et al. 2.

Section 12 Identifiants externes au réseau

Art. 69

Les surveillances selon les art. 56 à 59, 61 et 62 englobent aussi les communications effectuées via les services surveillés qui peuvent être attribuées à l'identifiant surveillé (target ID), même si l'identifiant surveillé n'est pas géré par le fournisseur mandaté.

Chapitre 4 Dispositions finales

Art. 70 Prescriptions organisationnelles, administratives et techniques

Le DFJP édicte les prescriptions organisationnelles, administratives et techniques pour la mise en œuvre de la surveillance de la correspondance par poste et télécommunication. Il fixe en particulier les délais dans lesquels doivent être livrées les données demandées.

Art. 71 Exécution

¹ Le Service SCPT met à disposition des formulaires et des interfaces électroniques, que les services concernés doivent utiliser. Ces formulaires et ces interfaces doivent permettre notamment:

- a. aux autorités qui ordonnent une mesure:
 1. de transmettre un ordre de surveillance au Service SCPT,
 2. de donner l'instruction au Service SCPT d'attribuer ou de modifier des autorisations d'accès;
- b. au Service SCPT:
 1. de charger les personnes obligées de collaborer d'exécuter une mesure de surveillance,
 2. de transmettre une demande de renseignements aux personnes obligées de collaborer et de transférer leurs réponses à l'autorité à l'origine de la demande;
- c. aux autorités habilitées de transmettre une demande de renseignements au Service SCPT.

² Le Service SCPT peut, le moment venu, remplacer les formulaires électroniques par un accès en ligne à son système de traitement et instaurer une procédure d'autorisation

électronique pour les mesures qui requièrent une autorisation. Les formulaires électroniques continueront d'être utilisés lorsque l'accès en ligne au système de traitement n'est pas possible pour des raisons techniques ou lorsque le système de traitement est hors service.

Art. 72 Abrogation d'un autre acte

L'ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication²⁹ est abrogée.

Art. 73 Modification d'autres actes

Les ordonnances mentionnées ci-après sont modifiées comme suit:

...³⁰

Art. 74 Dispositions transitoires

¹ Les modalités d'exécution des surveillances ordonnées avant l'entrée en vigueur de la présente ordonnance demeurent inchangées. Les prolongations et la levée de ces mesures continuent d'obéir aux types de surveillance précédemment en vigueur.

² Les branchements de tests mis en place selon l'ancienne pratique sont supprimés à l'entrée en vigueur de la présente ordonnance.

³ Les FST qui soumettent au Service SCPT, dans les trois mois à compter de l'entrée en vigueur de la présente ordonnance, une demande pour être considérés comme ayant des obligations restreintes en matière de surveillance selon l'art. 51 sont considérés comme tels à partir de l'entrée en vigueur de la présente ordonnance et pendant toute la durée de la procédure. Le Service SCPT peut refuser de considérer un FST comme ayant des obligations restreintes en matière de surveillance pendant la durée de la procédure s'il est vraisemblable que sa demande ne sera pas acceptée. L'art. 51, al. 5, ne s'applique pas aux fournisseurs qui étaient soumis jusqu'alors à l'obligation d'annoncer;

⁴ Au plus tard trois mois après l'entrée en vigueur de la présente ordonnance, les FST et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de renseignements visés à l'art. 22 adaptent leurs systèmes pour être en mesure de satisfaire aux nouvelles exigences concernant l'identification des usagers (art. 19) et la saisie d'indications relatives aux personnes (art. 20).

⁵ Au plus tard six mois après l'entrée en vigueur de la présente ordonnance, les FST, à l'exception de ceux ayant des obligations restreintes en matière de surveillance visés à l'art. 51, et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de surveillance visés à l'art. 52 adaptent leurs systèmes pour être en mesure de livrer les renseignements visés aux art. 38 et 39.

⁶ Au plus tard 24 mois après l'entrée en vigueur de la présente ordonnance:

²⁹ [RO 2001 3111; 2004 1431, 2021 art. 7, 3383; 2006 4705 ch. II 77; 2007 4029; 2011 5955; 2016 4337 ch. II; 2017 4151 annexe 4 ch. II 11]

³⁰ Les mod. peuvent être consultées au RO 2018 147.

- a. les données secondaires de tentatives d'établissement de communications doivent pouvoir être livrées dans le cadre de surveillances rétroactives;
- b. les FST doivent avoir procédé aux adaptations techniques nécessaires de leurs systèmes pour être en mesure de livrer les données des services de courrier électronique selon les art. 58, 59 et 62; jusque-là, ils continuent de livrer les données relatives aux services de courrier électronique comme ils le faisaient auparavant.

⁷ Jusqu'à la mise en service du nouveau système de traitement dont l'acquisition est prévue avec le programme «Surveillance des télécommunications»³¹:

- a. le Service SCPT peut établir les statistiques (art. 12) selon l'ancien droit;
- b. les demandes de renseignements (art. 35 à 48) et les surveillances (art. 54 à 68) continuent d'être traitées avec le système, les formats et les formulaires existants; les données sont transmises par un mode de transmission sûr autorisé par le Service SCPT, par poste ou par télécopie; l'art. 17, al. 1 et 2, n'est pas applicable;
- c. la fourniture de renseignements fondés sur une recherche flexible de nom selon l'art. 27 en relation avec les art. 35, 40, 42 et 43 n'est pas possible; une fois le nouveau système de traitement en service, seuls les FST et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de renseignements visés à l'art. 22 qui auront adapté leurs systèmes seront en mesure de les livrer.

⁸ Au plus tard 12 mois après la mise en service du nouveau système de traitement, les FST et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de renseignements visés à l'art. 22 adaptent leurs systèmes pour être en mesure de livrer les renseignements selon les art. 35 à 37 et 40 à 42, ainsi que l'art. 27 en relation avec les art. 35, 40 et 42 de manière automatisée, via l'interface de consultation du système de traitement (art. 18, al. 2), et d'exécuter les recherches flexibles de nom selon l'art. 27 en relation avec les art. 35, 40, 42 et 43.

Art. 74a³² Disposition transitoire relative à la modification du 4 mai 2022 concernant la localisation par téléphonie mobile de terroristes potentiels

¹ Le Service SCPT adapte son système de traitement dans les douze mois qui suivent le renouvellement de ses composants en temps réel afin de pouvoir exécuter les localisations par téléphonie mobile de terroristes potentiels de manière standardisée et les saisir dans la statistique.

² Les FST, à l'exception de ceux ayant des obligations restreintes en matière de surveillance (art. 51), et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de surveillance (art. 52) adaptent leurs systèmes dans les douze mois qui suivent le renouvellement des composants en temps réel du

³¹ FF 2015 2809

³² Introduit par le ch. I 12 de l'O du 4 mai 2022 sur les mesures policières de lutte contre le terrorisme, en vigueur depuis le 1^{er} juin 2022 (RO 2022 301).

système de traitement afin d'exécuter les localisations par téléphonie mobile de terroristes potentiels (art. 68*a*) de manière standardisée.

³ Tant que les localisations par téléphonie mobile de terroristes potentiels ne peuvent être exécutées de manière standardisée conformément à l'art. 68*a*, les fournisseurs exécutent en lieu et place les types de surveillance prévus à l'art. 54 et, au besoin, aux art. 56 et 63. Le Service SCPT transmet aux autorités habilitées les données visées aux art. 54 et 63. Il ne transmet les données visées à l'art. 56 que dans les limites de l'art. 68*a*. Si son système de traitement ne peut pas assurer ce tri, il ne transmet aucune donnée. Il détruit les données qui ne sont pas transmises. Les émoluments et les indemnités sont calculés en fonction des types de surveillance ordonnés (art. 54, 56 et 63).

Art. 75 Entrée en vigueur

La présente ordonnance entre en vigueur le 1^{er} mars 2018.

Termes et abréviations

1. *Adresse IP (Internet protocol address)*: adresse qui identifie tout équipement connecté à un réseau informatique utilisant le protocole internet. Il existe des adresses IP de version 4 (IPv4) et de version 6 (IPv6).
2. *Usager*: personne qui a conclu avec un fournisseur de services de télécommunication ou de services de communication dérivés un contrat portant sur l'utilisation de ses services ou qui s'est enregistrée auprès d'un tel fournisseur pour utiliser ses services ou qui a obtenu de ce fournisseur un moyen d'accès à ses services.
3. *Service multimédia*: service de communication qui intègre, en plus de la voix, d'autres types de médias et de fonctions, comme la vidéo, le transfert de fichiers, les images, le son, le partage de contenus et des informations de présence (par ex. vidéotéléphonie, communication unifiée, services de communication riches, service de téléphonie multimédia).
4. *Identifiant*: ressource d'adressage, numéro d'identification ou tout autre élément qui identifie un usager, un service ou un équipement déterminé.
5. *MSISDN (mobile subscriber integrated services digital network number)*: numéro de téléphone qui identifie un usager dans un réseau de communication mobile et qui permet de le joindre.
6. *Identifiant DSL (digital subscriber line)*: identifiant d'une ligne d'accès numérique, c'est-à-dire un accès haut débit au réseau qui permet d'envoyer et de recevoir des données via les fils de cuivre traditionnels.
7. *Préfixe IP*: partie d'une adresse IPv6 qui identifie le réseau.
8. *Plage d'adresses IP*: série d'adresses IP qui se suivent.
9. *Masque réseau*: dans le protocole internet version 4 (IPv4), nombre de bits placés en tête d'une adresse IP pour identifier le réseau.
10. *Longueur de préfixe*: dans le protocole internet version 6 (IPv6), nombre de bits placés en tête d'une adresse IP pour identifier le réseau.
11. *SIM (subscriber identity module)*: carte à puce ou puce intégrée dans un équipement terminal sur laquelle sont enregistrés de manière sécurisée l'IMSI et la clé qui permettent l'authentification d'un usager dans un réseau de communication mobile, *USIM (universal subscriber identity module)*, *UICC (universal integrated circuit card)* et *eSIM (embedded SIM)* compris.
12. *ICCID (integrated circuit card identifier)*: numéro de série qui identifie une carte SIM intégrée dans un équipement terminal (par ex. eSIM) ou une carte à puce (par ex. carte SIM).
13. *IMSI (international mobile subscriber identity)*: numéro d'identification international d'un usager dans un réseau de communication mobile.

14. *IMEI (international mobile equipment identity)*: numéro d'identification international d'un équipement de communication mobile.
15. *Adresse MAC (media access control)*: adresse matérielle stockée dans une carte ou un adaptateur réseau et utilisée comme identifiant unique au niveau de la couche 2 du modèle OSI.
16. *Code PUK (personal unblocking key)*: clé secrète qui ne peut être modifiée et qui sert à déverrouiller la puce SIM à laquelle elle est associée en cas de saisie, à plusieurs reprises, d'un NIP erroné.
17. *Code PUK2 (personal unblocking key 2)*: clé personnelle de déverrouillage ayant la même fonction que le code PUK, mais associée au code PIN2.
18. *NAT (network address translation)*: traduction d'adresses de réseau, c'est-à-dire le procédé par lequel un élément réseau (par ex. un routeur) remplace de manière automatisée les informations d'adressage dans des paquets IP par d'autres informations d'adressage.
19. *Adresse IP source*: adresse IP qui se réfère au point terminal de la communication (généralement un client) qui établit la liaison.
20. *Numéro de port*: adresse d'un port, c'est-à-dire le point terminal logique de communications avec un système informatique ou à l'intérieur de celui-ci. Un port est lié à une adresse IP et au type de protocole de communication.
21. *Numéro de port source*: numéro de port qui se réfère au point terminal de la communication (généralement un client) qui établit la liaison.
22. *Adresse IP de destination*: adresse IP qui se réfère au point terminal de la communication (généralement un serveur) à destination duquel la liaison est établie.
23. *Numéro de port de destination*: numéro de port qui se réfère au point terminal de la communication (généralement un serveur) à destination duquel la liaison est établie.
24. *SIP (session initiation protocol)*: protocole utilisé pour la signalisation et la gestion de sessions de communication multimédia.
25. *SIP URI (SIP uniform resource identifier)*: schéma d'identifiants uniformes de ressources (URI) utilisés pour l'adressage des communications SIP et se présentant au format *utilisateur@domain.tld*.
26. *IMPU (IP multimedia public identity)*: identité IP publique multimédia qui permet à un usager de communiquer avec d'autres usagers. Un usager de l'IMS possède, en plus de son IMPI, un ou plusieurs IMPU. Plusieurs IMPU peuvent être attribués à une IMPI. De même, plusieurs usagers peuvent se partager une même IMPU.
27. *TEL URI (telephone uniform resource identifier)*: schéma d'identifiants uniformes de ressources (URI) utilisés pour les numéros de téléphone et se présentant au format *tel:numéro*, par exemple *tel:+41-868-868-868*.
28. *IMPI (IP multimedia private identity)*: identité privée multimédia IP, c'est-à-dire l'identifiant international statique attribué à un usager par son fournisseur

et qui est utilisé, notamment, à des fins d'enregistrement et dans les procédures en lien avec les informations AAA. Tous les usagers du sous-système multimédia IP (*IP multimedia subsystems, IMS*) possèdent une IMPI. L'IMS est un système de communication fondé sur le protocole internet servant à l'intégration de services vocaux et de fonctions internet mobiles.

29. *Alias de messagerie*: adresse électronique supplémentaire que l'utilisateur peut librement créer, modifier ou supprimer, le nombre maximal d'alias et leur structure étant prédéfinis par le fournisseur du service de courrier électronique. Les alias de messagerie sont associés au compte de courrier électronique de l'utilisateur, de sorte qu'un courriel adressé à un alias est réceptionné dans la même boîte que celle à laquelle est associée l'adresse principale.
30. *Liste de diffusion*: également appelée liste de distribution ou de messagerie, liste d'adresses électroniques identifiée par une adresse de courrier électronique en propre, de telle sorte qu'un message expédié à cette adresse est automatiquement réexpédié à toutes les autres adresses qu'elle contient.
31. *Services de messagerie (messaging)*: services proposés indépendamment des services téléphoniques ou multimédia pour la transmission de messages, par exemple la messagerie instantanée, la messagerie IMS, les applications de messagerie et les SMS de fournisseurs tiers (c.-à-d. des services de SMS proposés par un FST autre que celui de l'utilisateur). Ces services peuvent intégrer des fonctions étendues comme la communication multimédia, la transmission de données et les informations de présence (l'utilisateur peut par exemple consulter le statut actuel et, selon le cas, la localisation des autres utilisateurs).
32. *Services d'informatique en nuage (cloud)*: services de communication dérivés, comme des services d'archivage ou des applications, qui sont disponibles en ligne et hébergés dans des centres de calcul répartis en fonction des besoins en ressources.
33. *Serveur mandataire (proxy)*: interface de communication qui réalise, dans un réseau, des fonctions de médiation, en réceptionnant, à une extrémité, les requêtes et en établissant, via sa propre adresse, une liaison avec l'autre extrémité, d'où l'importance des services de serveur mandataire à des fins d'identification.
34. *Point d'accès public au réseau WLAN*: point d'accès sans fil à un réseau public de télécommunication qui peut se trouver aussi bien dans des locaux publics que dans des locaux privés.
35. *CGI (cell global identity)*: identifiant statique d'une cellule dans les réseaux mobiles de deuxième et troisième génération (2G et 3G) (voir 3GPP TS 23.003, ch. 4.3.1).
36. *E-CGI (E-UTRAN cell global identity)*: identifiant statique d'une cellule dans les réseaux mobiles de quatrième génération (4G) (voir 3GPP TS 23.003, ch. 19.6).
37. *S-AI (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).
38. *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).
 39. *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).
 40. *BSSID (basic service set identifier)*: élément (adresse MAC) qui identifie le point d'accès au réseau WLAN.
 41. *Identifiant cible (target ID)*: élément qui identifie la cible de la surveillance.
 42. *Données AAA (authentication, authorisation and accounting)*: données d'authentification, d'autorisation et de comptabilité, c'est-à-dire les informations qui indiquent quel usager est autorisé à utiliser quels services et qui sont utilisées pour facturer l'utilisation des services en question. Au sens de la présente ordonnance, les mots de passe ne font pas partie intégrante des données AAA. L'authentification désigne la procédure par laquelle un usager s'identifie pour accéder à un service. L'autorisation permet quant à elle de déterminer les droits d'accès d'un usager à une ressource ou à un service et de garantir ainsi le contrôle des accès. Enfin, la comptabilité consiste à mesurer, aux fins de la facturation, l'utilisation que l'usager fait des ressources.
 43. *SMS (short message service)*: service qui permet de transmettre de brefs messages texte.
 44. *Messagerie vocale*: dispositif de réception, d'envoi et d'enregistrement notamment de messages vocaux qui est mis à disposition dans un réseau de télécommunication et qui peut intégrer différents types de médias et de services supplémentaires, comme les SMS, le courrier électronique, les fax ou la vidéomessagerie, et des extensions de fonctions, par exemple la conversion d'un type de média en un autre type et l'envoi de messages.
 45. *RCS (rich communications services)*: (à l'origine, *rich communication suite*) services de communication riches, c'est-à-dire une spécification internationale de la GSM Association (GSMA), l'association de branche des fournisseurs de services de communication mobile, qui est utilisée pour la fourniture fondée sur l'IMS de services multimédia interopérables (c.-à-d. indépendants du fournisseur et de l'équipement terminal) dotés de fonctions étendues. Différents types de médias (par ex. voix, musique, photos, vidéos) et de services (par ex. dialogue en ligne, dialogue en ligne de groupe, appels, messages multimédia, messages courts, messagerie instantanée, informations de présence, transmission de fichiers, carnet d'adresses). Les services de communication riches sont fournis à l'usager par son fournisseur de services de communication mobile.

46. *Numéro E.164*: numéro de téléphone selon le plan de numérotation de l'Union internationale des télécommunication (UIT).
47. *DTMF (dual-tone multi-frequency)*: multifréquence à deux tonalités, c'est-à-dire un système de signalisation qui permet, sur pression des touches du téléphone, d'envoyer des signaux pendant une communication téléphonique, par exemple pour utiliser un répondeur téléphonique ou un serveur vocal interactif automatisé.
48. *MMS (multimedia messaging service)*: service qui permet de transmettre des messages multimédia dans des réseaux de communication mobile.

