# Rapport explicatif

**relatif à l'ordonnance sur le système de traitement pour la surveillance de la correspondance par poste et télécommunication (OST-SCPT ; RS 780.12)**

## 1. Contexte

Le Service de surveillance de la correspondance par poste et télécommunication (Service SCPT) du Département fédéral de justice et police est chargé, comme son nom l'indique, d'assurer la surveillance de la correspondance par poste et télécommunication, de suivre l'évolution technique dans ce domaine et de procéder aux modifications nécessaires des bases légales. Pour accomplir ses tâches, le Service SCPT exploite un système informatique qui lui permet de traiter les renseignements et les surveillances des télécommunications, de gérer les affaires et les mandats, de conserver des données pendant une période prolongée et des créer des fichiers de journalisation. Les nouvelles bases légales créées avec la révision de la loi fédérale du 18 mars 2016[1] sur la surveillance de la correspondance par poste et télécommunication (LSCPT) exigent des fonctions supplémentaires (conservation de données pendant une longue durée, infrastructure de formation). Le nouveau système de traitement automatise en outre le plus grand nombre possible de processus et garantit ainsi un traitement fluide et sans rupture médiatique des données issues des renseignements et des surveillances.

Pour que l'ordonnance du 15 novembre 2017[2] sur la surveillance de la correspondance par poste et télécommunication (OSCPT) soit plus lisible, et par respect du principe de transparence, les bases légales du système de traitement, en sus de celles contenues dans la LSCPT, sont inscrites dans une nouvelle ordonnance.

## 2. Commentaire article par article

*Préambule*

L'OST-SCPT se fonde sur l'art. 10, al. 4, l'art. 11, al. 6 et l'art. 12, al. 2, LSCPT. Plus généralement, elle concrétise les art. 6 à 14 LSCPT qui contiennent des dispositions relatives au système informatique que le Service SCPT doit exploiter et qui sont expliqués dans le message[3].

### Section 1 Dispositions générales

*Art. 1* Objet

L'ordonnance règle le fonctionnement et l'utilisation du système de traitement du Service SCPT pour la surveillance de la correspondance par poste et télécommunication.

Le but du système de traitement pour la correspondance par télécommunication est déjà réglé à l'art. 7 LSCPT.

1 RS **780.1**
2 RS **780.11**
3 FF **2013** 2407 à 2417

*Art. 2* Réseau de transmission de données

Selon l'al. 1, les données (renseignements et surveillances) que doivent livrer les fournisseurs de services de télécommunication (FST) – à l'exception de ceux ayant des obligations restreintes en matière de surveillance, conformément à l'art. 51, al. 1, OSCPT – et les fournisseurs de services de communication dérivés ayant des obligations étendues en matière de fourniture de renseignements, conformément à l'art. 22, al. 1, OSCPT ou en matière de surveillance, conformément à l'art. 52, al. 1, OSCPT, sont transmises via un réseau de transmission de données (par ex. fibre optique, VPN) directement des personnes obligées de collaborer vers l'interface du Service SCPT ; les détails techniques, tels que les points de livraison, sont réglés dans l'annexe 2 de l'ordonnance du DFJP du 15 novembre 2017 sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication[4] OME-SCPT (cf. art. 12, al. 3, LSCPT). Les fournisseurs nommés gèrent ce réseau de transmission de données et, en vertu de l'art. 38, al. 1, LSCPT, supportent les coûts de la transmission des données jusqu'à l'interface de livraison des données au Service SCPT. La transmission des données fait partie de la disponibilité à assurer une surveillance et constitue dès lors une obligation des personnes obligées de collaborer. De même, l'art. 53, al. 2, OSCPT prévoit que si l'exécution de la surveillance le requiert, elles mettent gratuitement à la disposition du Service SCPT ou du tiers mandaté par lui les accès existants aux réseaux de télécommunication publics ou les créent, en collaboration avec le Service SCPT ou le tiers mandaté par lui.

Conformément à l'al. 2, ce réseau sécurisé peut servir aussi bien à la transmission des données relatives aux demandes de renseignements et aux ordres de surveillance, qu'à la communication entre les personnes obligées de collaborer et le Service SCPT , par exemple en cas d'incertitudes, de problèmes ou de questions concernant l'exécution des mandats.

L'al. 3 charge le DFJP d'édicter des prescriptions de détail réglant les aspects techniques et administratifs, par exemple la structure, le fonctionnement et l'exploitation du réseau de transmission de données.

## Section 2 Données et traitement des données

*Art. 3* Données

Le contenu du système de traitement est détaillé à l'art. 8 LSCPT. L'*al. 1* décrit de quelle manière les données sont obtenues, indépendamment du fait que celles-ci soient ensuite conservées sur une longue période ou non. L'art. 8 LSCPT mentionne en particulier les données qui peuvent être obtenues dans le cadre d'une surveillance de correspondance par télécommunication. L'art. 3 OST-SCPT énumère les données contenues dans le système de traitement, données relatives à des personnes, mais aussi données purement techniques, ou encore données ajoutées par les autorités elles-mêmes, que ce soit pour simplifier la représentation au moyen de programmes spéciaux ou pour indiquer une caractéristique de traitement, comme l'ajout manuel de commentaires ou d'informations sur les ressources d'adressage.

Les données issues des renseignements et des surveillances mentionnées à la *let. a* sont les données brutes que les personnes obligées de collaborer livrent au système de

4 RS **780.117**

traitement ; elles comprennent aussi les données sur les services de télécommunication (art. 8, let. c, LSCPT). Ces données doivent être transmises dans les formats fixés par l'OME-SCPT. Elles sont ensuite préparées afin d'en faciliter l'exploitation par les autorités qui les ont demandées. Elles sont uniformisées (par ex. formats date/heure uniformes), rendues lisibles, audibles et visibles (par ex. représentation sur des cartes, attribution des numéros à des noms lisibles) et les doublons et erreurs sont éliminés dans la mesure du possible (*let. b*). Ces données peuvent être traitées au moyen d'une procédure d'appel en ligne (accès en ligne).

La *let. c* précise que le système de traitement contient aussi les demandes de renseignements et les ordres de surveillance transmis par les autorités habilitées. Certains éléments des demandes de renseignements, de même que les ordres de surveillance, sont également nécessaires aux fins de l'exécution et du suivi des affaires (let. e). Vu toutefois que l'art. 5 n'énumère pas toutes les données des demandes de renseignements, il y a lieu, par souci de clarté, de les mentionner séparément sous une lettre, avec les ordres de surveillance.

Les autorités qui exploitent les données doivent pouvoir ajouter des caractéristiques de traitement telles que des marquages, des mises en évidence ou des transcriptions sur certaines données (*let. d*).

Les données mentionnées à la *let. e* sont celles dont le Service SCPT a besoin pour effectuer ses tâches : données de gestion des mandats, décisions, autorisations, données pertinentes pour la sécurité, données relatives aux contrôles (gestion de la qualité, données de test) et statistiques du Service SCPT. Le Service SCPT traite aussi des données comptables en vue de la facturation selon l'art. 38 LSCPT, afin de percevoir les émoluments et de verser les indemnités selon l'ordonnance du 15 novembre 2017[5] sur les émoluments et les indemnités en matière de surveillance de la correspondance par poste et télécommunication (OEI-SCPT). Le contrôle de la qualité est réglé à l'art. 18 LSCPT et à l'art. 29 OSCPT, ainsi qu'à l'art. 7 OME-SCPT et dans son annexe. Des explications sont données dans le message du 27 février 2013 concernant la LSCPT[6] (ci-après le message), à la page 2424, ainsi que dans les rapports explicatifs correspondants. Sont également réglés dans l'OME-SCPT, aux art. 23 et 24, les tests visant à contrôler la disponibilité à renseigner et à surveiller, dont les données font aussi partie du système de traitement. Les statistiques du Service SCPT sont réglées aux art. 16, let. k, 35, al. 3, et 36, al. 2, LSCPT et à l'art. 12 OSCPT. Selon la pratique en vigueur, le Service SCPT établit également une statistique concernant les renseignements, et il continuera à le faire sous l'empire du nouveau droit. Les statistiques des ministères publics et des juges d'instruction militaires sont publiées par le Service SCPT et sont réglées dans les art. 269$^{bis}$, al. 2, et 269$^{ter}$, al. 4, CPP[7], les art. 70$^{bis}$, al. 2, et 70$^{ter}$, al. 4, de la procédure pénale militaire du 23 mars 1979[8] et l'art. 13 OSCPT. Ces articles de la LSCPT n'ont été ajoutés qu'au cours des débats parlementaires et ne sont de ce fait pas expliqués dans le message. Des explications se trouvent toutefois dans le rapport explicatif concernant l'OSCPT, dans le commentaire relatif à l'art. 29.

5 RS **780.115.1**
6 FF **2013** 2379 ss
7 Code de procédure pénale du 05.10.2007 (**CPP**, RS **312.0)**
8 RS **322.1**

Selon la *let. f*, des données supplémentaires peuvent être utilisés pour représenter les données issues des renseignements et des surveillance de manière plus compréhensible. Il s'agit par exemple d'informations cartographiques ou de données issues de bases de données de portage de numéro. La représentation doit être comprise au sens large du terme : représentation sur une carte, décodage, comparaison avec d'autres données.

Selon la *let. g*, le système de traitement contient aussi des clés cryptographiques. Il est ainsi possible de décrypter avec une clé privée les communications cryptées avec la clé publique du destinataire. Des communications peuvent être cryptées avec une clé publique du destinataire et signées avec la clé privée. De plus, le destinataire peut vérifier l'authenticité du message reçu en utilisant la clé publique de l'expéditeur (signature).

Les fichiers auxiliaires, tels que données de journalisation ou de filtrage ne sont pas spécifiquement mentionnées dans cet article, mais sont cependant aussi traités dans le système. Le contenu du système de traitement est détaillé à l'art. 8 LSCPT.

Le système de traitement permet au Service SCPT de traiter les données dont il a besoin pour accomplir ses tâches. L'*al. 2* décrit la structure de ce système. Les données y sont traitées de manière centralisée, parce qu'il est utile d'exploiter de manière globale les différentes données (renseignements, données historiques, temps réel, commentaires et traductions, qu'il s'agisse d'une procédure pénale, d'une recherche en cas d'urgence ou de la recherche d'une personne condamnée). Il n'est par ailleurs pas possible de distinguer des sous-systèmes dédiés du système de traitement, car celui-ci constitue une unité logique.

Selon la *let. a*, le système de traitement englobe les tâches de l'actuel « Call Center Information System » (CCIS) et les tâches supplémentaires prévues par la LSCPT. Cela comprend avant tout les renseignements simples sur les ressources d'adressage ainsi que les renseignements techniques et administratifs sur les éléments de contrat et l'infrastructure réseau.

Selon la *let. b*, le système permet le traitement des données issues de surveillances en temps réel. Cela inclut la transmission des données de contenu et des données secondaires en temps réel, c'est-à-dire à mesure qu'elles parviennent aux personnes obligées de collaborer. Des fonctions de traitement permettent de représenter les données obtenues de manière compréhensible pour les autorités qui les exploitent. Le système fournit à cette fin le décodeur et les fonctions d'analyse nécessaires.

Selon la *let. c*, le système de traitement comprend des possibilités de traitement pour les données historiques. Cela inclut la transmission des données secondaires des communications remontant jusqu'à six mois. Là aussi, des fonctions de traitement doivent permettre de représenter les données obtenues de manière compréhensible pour les autorités qui les exploitent. Le système fournit à cette fin le décodeur et les fonctions d'analyse nécessaires.

Selon la *let. d*, le Service SCPT peut utiliser le système de traitement pour l'exécution et le suivi des affaires. Le système documente notamment l'activité du Service SCPT et gère les documents et les dossiers de manière à ce que le Service SCPT puisse traiter ces données. En font partie les données sur le contrôle de la qualité, les statistiques et la facturation avec les données de comptabilité nécessaires. Le système de traitement doit être conçu de manière à soutenir le Service SCPT dans ses tâches concernant la

qualité des données livrées par les fournisseurs et les statistiques. Les données à traiter sont énumérées à l'art. 6.

*Art. 4* Origine des données

L'*art. 4* explique qui a le droit de générer des données et d'où les données proviennent.

Les données peuvent provenir des autorités de poursuite pénale, lesquelles insèrent par exemple des commentaires ou de la documentation via la procédure d'appel en ligne (*al. 1, let. a*).

Elles peuvent provenir des personnes obligées de collaborer, lesquelles transmettent les données au Service SCPT via le réseau de transmission des données ou un autre moyen autorisé par le Service SCPT (*let. b*).

Le Service SCPT génère lui aussi des données, qu'il s'agisse de remarques des collaborateurs ou de fichiers de journalisation (*let. c*).

Les données doivent aussi pouvoir être importées à partir de bases de données (*let. d*), qu'il s'agisse de sources accessibles au public ou non, telles que la base de donnée de portage des numéros « Telecom Data Service » (TelDas) ou, pour des demandes d'adresses IP, les « Réseaux IP Européens » (RIPE).

Des informations géographiques et du matériel cartographique doivent aussi pouvoir être utilisés pour représenter de manière plus simple des coordonnées (*let. e*). De cette manière, il est plus simple de localiser les personnes lors de recherches d'urgence. Par ailleurs, il est possible d'établir des profils de déplacement et de séjour et de les compléter, par exemple, avec le matériel cartographique de Swisstopo (géologie, bâtiments et installations). L'appel du matériel et des informations doit être fait de manière à ne transmettre aucune indication sur des enquêtes en cours aux fournisseurs de services ou aux hébergeurs, car ceux-ci peuvent se trouver sur des serveurs de fournisseurs à l'étranger.

L'*al. 2* expose que les autorités chargées d'évaluer les données (art. 4, al. 1, let. a) ne peuvent ajouter que les caractéristiques de traitement mentionnées à l'art. 3, al. 1, let. d, et les clés cryptographiques mentionnées à l'art. 3, al. 1, let. g. L'importation de clés cryptographiques est indispensable pour pouvoir représenter et traiter des données cryptées (cf. art. 7 LSCPT, en particulier let. a, b et d). Une importation plus étendue de données d'enquête est clairement exclue.

*Art. 5* Fonctions de traitement pour les données issues de renseignements et de surveillances

Les art. 5 et 6 règlent des principes importants du traitement de données dans le système. Étant donné que des données personnelles sensibles y sont aussi traitées, une base légale formelle est nécessaire. Son principe est donné par les articles de la section 2 de la LSCPT. Des données personnelles sensibles sont traitées avant tout dans le cadre de surveillances, et non pas dans le cadre de renseignements. Par données personnelles sensibles, on entend des données sur les opinions ou activités religieuses, philosophiques, politiques ou syndicales, la santé, la sphère intime ou l'appartenance

à une race, des mesures d'aide sociale, des poursuites ou sanctions pénales et administratives (cf. art. 3 de la loi fédérale du 19 juin 1992 sur la protection des données[9] [LPD]). Cette définition est exhaustive.

L'art. 5 énumère désormais à l'échelon de l'ordonnance les fonctions de traitement pour les renseignements et les surveillances selon l'art. 7, let. d, LSCPT. Le système de traitement sert ainsi à offrir des fonctions de traitement pour les données sauvegardées dans le système. À ce sujet, le message explique que l'exploitation par les autorités de poursuite pénale des données collectées lors de surveillances aura lieu dans les systèmes d'information pertinents du réseau de systèmes d'information de police de l'Office fédéral de la police (cf. message, FF 2013 2379, 2410).

La problématique de la délimitation entre les fonctions de traitement selon l'art. 7, let. d, LSCPT et le traitement des données selon la loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération (LSIP) [10] s'est posée dans le cadre des travaux de révision des ordonnances. Le même problème se pose à l'égard du système d'information du SRC. Concrètement, la question était de savoir si des fonctions d'analyse, en particulier celles qui apportent une plus-value pour les enquêtes, peuvent être utilisées dans le cadre des fonctions de traitement du système de traitement. Bien entendu, aucune donnée personnelle non publique n'est importée de sources extérieures à la surveillance des télécommunications. Il n'existe aucune base légale explicite pour ces fonctions dans la LSCPT. De telles fonctions devraient cependant pouvoir continuer à être utilisées, ou être nouvellement mises en œuvre, dans le système de traitement, en application d'une approche d'assainissement progressif de la situation juridique et parce que les fonctions controversées font partie des fonctions standards du système de surveillance des télécommunications acquis par le Service SCPT, et que les systèmes de fedpol et du SRC ne disposent d'aucune fonction comparable. Dans le cas contraire, il faudrait dépenser beaucoup d'argent pour intégrer dans les systèmes selon la LISP et la LRens des fonctions déjà contenues dans le système de traitement du SCPT. La révision déjà prévue de la LSIP doit être l'occasion de bien délimiter les différents systèmes et de créer une base légale claire qui, d'une part, n'entrave pas le développement rapide et les innovations des technologies de l'information et de la communication (TIC), mais qui ne soit pas, d'autre part, condamnée à être toujours à la traîne.

L'art. 5 présente une liste détaillée et exhaustive des fonctions de traitement du système, y compris celles qui offrent une plus-value pour les enquêtes. Toutes les données que les personnes obligées de collaborer fournissent au système peuvent ainsi être traitées par les autorités disposant d'un droit d'accès. L'art. 9, al. 1 et 2, LSCPT indique quelles sont les autorités qui bénéficient d'un droit d'accès et sont ainsi autorisées à traiter les données. La matrice précise les droits d'accès à sa lettre f pour les renseignements et à sa lettre g pour les surveillances. La personne s'occupant des surveillances n'a ainsi accès qu'aux données des affaires qui lui sont attribuées (ch. 2.4 de la matrice). Les lettres *a* à *e* concrétisent par ailleurs la destruction des données dans le système de traitement. Les données que les personnes obligées de collaborer livrent peuvent être complétées par d'autres données (voir art. 4, Origine des données). Cependant, aucune donnée personnelle sensible de sources autres que la surveillance de la correspondance par télécommunication ne peut être utilisée dans le système de traitement, c'est-à-dire notamment aucune donnée issue de surveillances

9 RS **235.1**
10 RS **361**

avec des IMSI-Catcher ou des GovWare selon les nouveaux art. 269*bis* à 269*quater* CPP, ou les art. 70bis à 70quater PPM, à moins que celles-ci soient absolument indispensables à la représentation des données déjà obtenues, comme par exemple des clés cryptographiques. Le système de traitement peut en outre envoyer et recevoir des données de correspondance telles que courriers électroniques, fax, SMS, appels téléphoniques.

Selon la *let. a* peuvent être écoutées avant tout les surveillances en temps réel, par exemple via téléphonie avec ou sans image ou via VoIP. D'autre part, des conversations enregistrées peuvent être écoutées de manière différée (écoute rétroactive).

Selon la *let. b*, les données obtenues peuvent être affichées et imprimées. Cela inclut avant tout les analyses de fichiers de journalisation, mais aussi les indications de statut, comme par exemple de savoir si un téléphone a été allumé ou éteint. Les données tels que les SMS, courriers électroniques, ou informations http, mais aussi les conversations, sont préparées de manière pouvoir s'afficher de la manière la plus compréhensible qui soit et être ainsi facilement exploitables par les autorités de poursuites pénales. Les données livrées par les personnes obligées de collaborer, notamment pour la surveillance d'une connexion internet, se présentent sous la forme d'une succession de chiffres et de lettres en grande quantité. Ces données sont ensuite traitées avec différents outils afin que par exemple des images téléchargées pendant une session internet deviennent à nouveau reconnaissables. Ce sont avant tout des informations sur les dossiers qui sont imprimées, par exemple pour le ministère public.

Selon la *let. c*, les données obtenues sur les téléphones mobiles peuvent être localisées grâce aux coordonnées obtenues dans le cadre d'une mesure. Pour en faciliter l'exploitation, celles-ci peuvent être représentées sur une carte géographique avec des données supplémentaires, de manière par exemple à trouver plus rapidement la position d'une personne disparue lors d'une recherche en cas d'urgence.

Le décodage selon la *let. d* permet de convertir les données reçues dans d'autres formats. Des données reçues ou expédiées sont par exemple souvent converties dans des formats spéciaux pour les comprimer avant leur transmission. Elles doivent ensuite être converties à nouveau dans leur format original. Les données ne sont cependant pas seulement codées, mais aussi encryptées pour les protéger d'une lecture indésirable. Elles peuvent être rendues lisibles à nouveau avec la clé correspondante.

Selon la *let. e*, les différents éléments peuvent être groupés et triés. L'objectif est d'avoir une meilleure vue d'ensemble et de pouvoir mieux comparer les différents éléments.

Selon la *let. f*, il est aussi possible d'effectuer une recherche d'un texte donné ou de filtrer, par exemple, par type de communication (courrier électronique, SMS, conversation, mots clés, période, zones géographiques). Il ne faut pas confondre ce filtrage avec le tri automatique effectué préalablement par le Service SCPT selon l'art. 7 OSCPT ou l'art. 17, let. g, LSCPT. Avec ce tri automatique, les données ne sont pas sauvegardées dans le système de traitement ; le filtrage visé à l'art. 6, let. f OST-OSCPT peut être annulé pour afficher à nouveau l'ensemble des données.

La fonction de traitement selon la *let. g* permet au collaborateur d'une autorité habilitée d'attribuer un enregistrement vocal à une personne. Grâce à l'enregistrement existant, le système peut reconnaître la voix en question et l'attribuer à la personne déterminée. Il est ainsi plus facile, par exemple dans une procédure pénale, de savoir avec qui une conversation est tenue. L'enregistrement vocal ne peut cependant être utilisé que pour les cas attribués à une autorité habilitée et non dans l'ensemble du système.

Cette restriction est précisée dans la matrice pour les autorités habilitées (ch. 2), avec le double astérisque pour le traitement des données issues de surveillance (let. g).

Selon la *let. h*, des documents sonores et des films peuvent être transcrits, c'est-à-dire qu'un procès-verbal est établi de ce qui est dit et vu, avec si nécessaire, une traduction dans une langue nationale. Dans le cas de la surveillance de la correspondance par télécommunication, le procès-verbal des paroles prononcées passe en principe au premier plan.

Selon la *let. i*, les différents éléments peuvent être commentés, par exemple avec des mots-clés sur les impressions et les résultats obtenus ou sur des noms de dossiers.

En donnant l'alarme selon la *let. j*, le système informe par exemple par téléphone ou SMS qu'un événement particulier s'est produit.

Selon la *let. k*, des informations nécessaires peuvent être transmises de manière sécurisée, avant tout à des personnes habilitées des autorités de poursuite pénale, via une interface vers le réseau de systèmes d'information de police (art. 14, al. 1, LSCPT) et le système d'information du Service de renseignement de la Confédération (art. 14*a* LSCPT) ou au moyen d'une procédure d'appel (accès en ligne). Les enquêteurs peuvent ainsi télécharger les données nécessaires.

Selon la *let. l*, le Service SCPT peut détruire des informations. Cette fonction exceptionnelle n'est cependant appliquée que dans le cas du triage sous la supervision d'un tribunal selon l'art. 16, let. e, LSCPT, sur instruction du tribunal compétent, ou pour d'autres destructions prévues par la loi (art. 276 et 277 CPP).

Selon l'*al. 2*, les fonctions ne s'appliquent qu'aux données auxquelles la personne qui les exécute a accès. N'apparaîtront ainsi lors d'une recherche ou d'un filtrage que les données que la personne a le droit de voir.

*Art. 6* Traitement des données pour l'exécution et le suivi des affaires

Le Service SCPT ne travaille que sur ordre, principalement sur ordre des autorités de poursuite pénale car il n'a aucune compétence en matière de poursuite pénale. Il n'est en principe que l'exploitant du système de traitement (art. 6 LSCPT), mais n'est pas le maître des données (art. 13 LSCPT). Les autorités habilitées à ordonner une surveillance sont les propriétaires ou les responsables des données que le Service SCPT collecte dans l'exécution de ses tâches, qu'il reçoit et met à disposition pour l'accès en ligne conformément aux droits d'accès. Le Service SCPT est cependant le propriétaire (responsable) des données qu'il génère pour l'exécution et le suivi des affaires (art. 3, al. 2, let. d) ainsi que pour la journalisation.

Cet article énumère les données traitées par le Service SCPT pour l'exécution des ordres de surveillance de la correspondance par télécommunication et le contrôle de cette exécution.

Le Service SCPT se base sur les données de contact de la personne physique responsable de l'autorité indiquée telles que mentionnées en *let. a*, la plupart du temps l'autorité de police en charge de l'enquête, pour octroyer les droits d'accès au système de traitement ; il prend contact avec elle en cas d'incertitude et envoie la facture aux autorités qui ont ordonné la surveillance. Ces données peuvent être enregistrées dans le système avant un premier ordre, de manière à être immédiatement disponibles le moment venu. De plus, les autorités enregistrées peuvent être informées des nouveautés.

Les données selon la *let. b* servent aux personnes obligées de collaborer et au Service SCPT à contrôler si l'application ou l'accès Internet à surveiller ont un lien avec cette personne. L'indication de la profession permet en outre au Service SCPT de vérifier si les mesures nécessaires selon l'art. 271, al. 1, CPP ont été prises (art. 5 OSCPT).

Le Service SCPT examine de manière formelle, sur la base des données de la *let. c*, si cette infraction ou ces infractions permettent d'ordonner la surveillance en question selon la liste de l'art. 269 CPP ou selon l'art. 273 CPP (surveillance rétroactive). Il a en outre besoin de ces données pour établir chaque année une statistique des mandats de surveillance et des renseignements sur la correspondance par poste et télécommunication.

La *let. d* mentionne les types de renseignements et de surveillances ordonnés. Ces demandes de renseignements et de surveillances font l'objet d'un mandat aux personnes obligées de collaborer, d'une facturation et d'une évaluation statistique.

Selon la *let. e*, peuvent être traitées dans le système toute la correspondance, d'éventuelles notes de discussion, mais aussi communications orales et conversations téléphoniques enregistrées à des fins probatoires selon l'art. 8 OSCPT lorsque ces données sont générées par l'exécution et le suivi des affaires. En font notamment partie des communications orales transmises par courrier électronique.

Selon la *let. f*, les décisions des autorités sont elles aussi conservées dans le système de traitement. Il peut s'agir, d'une part, de décisions de ministères publics et de tribunaux des mesures de contrainte (ordres, autorisations et prolongations) à des fins probatoires. Elles comprennent d'autre part aussi les décisions du Service SCPT (par ex. selon l'art. 40, al. 1, LSCPT), ainsi que des décisions sur recours des autorités judiciaires. L'objectif est de pouvoir enregistrer de manière centralisée toutes les données relatives à un dossier. Les données générées lors de l'élaboration de décisions du Service SCPT sont traitées dans le système de gestion électronique des affaires (GEVER). Seule la décision, lorsque c'est utile, sera enregistrée dans le dossier correspondant dans le système de traitement.

La *let. g* renvoie à l'art. 15, let. h à k, et à l'art. 49, al. 1, let. h à l, de l'OSCPT. Ces dispositions mentionnent certaines données qui doivent être indiquées dans les ordres de surveillance. Le rapport explicatif de l'OSCPT contient de plus amples informations.

Selon la *let. h*, le numéro de référence et le nom d'affaire attribués par les ministères publics peuvent être enregistrés, de même aussi que les numéros de référence (LLID) que le Service SCPT crée pour chaque dossier.

Selon la *let. i*, le Service SCPT traite les coordonnées des personnes obligées de collaborer. Il peut ainsi utiliser ces données pour donner les ordres concernant les renseignements et surveillances aux personnes obligées de collaborer ou à leurs collaborateurs. Ces informations sont aussi utilisées à d'autres fins, par exemple pour le contrôle et la confirmation de l'aptitude à fournir des renseignements et à effectuer les surveillances.

Selon la *let. j*, le Service SCPT traite aussi d'autres données des personnes obligées de collaborer, données dont il a notamment besoin pour la transmission des données que ces personnes lui livrent, pour le contrôle de l'aptitude à fournir des renseignements et à effectuer les surveillances et pour déterminer à quelle catégorie appartient une personne obligée de collaborer ou les services qu'elle fournit (art. 1, al. 2, let. *i* à *m*, OSCPT). Il peut s'agir de données telles que des certificats, des indicatifs (numéro

d'identification de fournisseur, numéro d'identification des entreprises [art. 38, let. a, ORC][11]), des numéros de téléphone, des adresses IP, le statut de l'aptitude à fournir des renseignements et à effectuer des surveillances, des informations sur les prestations de services proposées, des informations sur la faible importance économique selon l'art. 51, al. 1, OSCPT ou des informations sur les sanctions administratives ou pénales selon les sections 10 et 11 de la LSCPT. Enfin, d'autres informations, concernant par exemple le secteur d'activité ou le chiffre d'affaires annuel sont nécessaires pour déterminer si un fournisseur doit être considéré comme ayant des obligations restreintes (art. 51 OSCPT) ou, à l'inverse, comme ayant des obligations étendues (art. 22 et 52 OSCPT).

Les ressources d'adressage servent à l'établissement de la communication et peuvent être rattachées à une personne. L'art. 3 de la loi du 30 avril 1997 sur les télécommunications (LTC)[12] les définit comme des paramètres de communication ainsi que des éléments de numérotation tels que les indicatifs, les numéros d'appel et les numéros courts. Elles sont contenues dans la plupart des ordres et, selon la *let. k*, doivent aussi être traitées dans le système de traitement. Peuvent aussi être traités des identificateurs qui, contrairement aux ressources d'adressage, ne peuvent pas être clairement rattachés à une personne.

Selon la *let. l*, de nombreuses autres informations de nature technique nécessaires à l'exécution des ordres de surveillance de la correspondance par télécommunication, y compris des données pour les dossiers spéciaux, et au contrôle de leur exécution, sont sauvegardées dans le système de traitement. Il s'agit notamment des clés pour la transmission sécurisée des données, des numéros de ports ou d'informations pour le réseau de transmission des données (art. 2) telles que des adresses IP et des mots de passe.

Selon la *let. m*, le système traite aussi des données qui permettent d'une part de facturer des émoluments aux autorités de poursuite pénale et, d'autre part, de verser les indemnités aux personnes obligés de collaborer. Ces données comprennent par exemple le statut du décompte, les émoluments pour des prestations non répertoriées, lesquels sont fixés en fonction du temps consacré et du matériel utilisé (cf. art. 13 OEI-SCPT).

*Art. 7* Droit d'accès au système de traitement

Les droits d'accès au système de traitement des différentes personnes sont réglés de manière globale à l'art. 9 LSCPT. L'art. 7 règle les droits généraux d'accès au système et l'art. 8, les droits d'accès supplémentaires aux différentes surveillances.

Le système de traitement doit répondre à des exigences concernant différentes personnes habilitées, autorités et autres personnes. Il doit aussi posséder des interfaces variées et permettre aux personnes habilitées ou membres des autorités (cf. art. 1, al. 2, let. a à f, OSCPT) ou professions mentionnées d'accéder à différentes fonctions.

L'*al. 1* pose les règles générales pour l'accès au système de traitement. Cet accès est nécessaire entre autres pour pouvoir présenter des demandes de renseignements et ordonner des surveillances. L'accès est demandé au moyen d'un formulaire mis à disposition par le Service SCPT. Ce formulaire pourra à terme être rempli de manière électronique, par exemple via le système en ligne ou le système « ZP-Tool ». L'art. 3 OSCPT règle le dépôt auprès du Service SCPT des modifications des droits d'accès

11 Ordonnance du 17 octobre 2007 sur le registre du commerce (ORC; RS **221.411**)
12 RS **784.10**

qui doivent être effectuées. Tous les droits d'accès octroyés sont rattachés à une personne physique. Cette personne reçoit un compte d'utilisateur qui lui est propre et est responsable des accès effectués. Elle doit pouvoir justifier les raisons pour lesquelles elle a dû accéder aux données pour exécuter ses tâches.

Selon la *let. a*, l'accès peut être donné aux collaborateurs des autorités. Sont visées les autorités qui sont habilitées à ordonner des surveillances selon l'art. 9 LSCPT et à demander des renseignements selon l'art. 15 LSCPT. Ces surveillances et renseignements peuvent être demandés dans le cadre d'une procédure pénale, d'une recherche en cas d'urgence ou d'une recherche de personne condamnée. Les autorités en questions sont principalement les autorités de poursuite pénale, comme fedpol, mais aussi des autorités qui doivent résoudre des affaires de droit pénal administratif. Des autorités d'exécution cantonales peuvent aussi ordonner des surveillances dans le cadre de recherches de personnes condamnées, pour autant que les bases légales cantonales les y autorisent. Mais il s'agit aussi des autorités pénales cantonales des 26 cantons, dont l'accès aux mesures de surveillance dans le cadre de l'exécution de tâches d'instruction ou de tâches judiciaires se fait via un accès sécurisé au système de traitement, ou encore des organisations de police en tant qu'autorité exploitant les données, qui accèdent aux données sauvegardées via un réseau autorisé pour l'accès au système. Le Ministère public de la Confédération, en tant qu'autorité de poursuite pénale de la Confédération appelée à statuer, ou le Tribunal pénal fédéral, ont aussi besoin d'un accès. La loi fédérale du 25 septembre 2015 sur le renseignement[13], entièrement révisée, accorde en outre aussi au Service de renseignement la possibilité de demander des renseignements (art. 25, al. 2, LRens) et d'ordonner des surveillances (art. 26, al. 1, let. a, LRens).

Selon la *let b*, un droit d'accès est donné aux collaborateurs des FST et des fournisseurs de services de communication dérivés, afin qu'ils puissent répondre via le système de traitement aux demandes, qui lui parviennent aussi par le biais du système de traitement, des autorités ayant ordonné une surveillance et exploitant les données obtenues.

Selon la *let. c*, les collaborateurs du Service SCPT ont aussi un droit d'accès pour effectuer les tâches qui leur incombent dans le cadre de la surveillance de la correspondance par poste et télécommunication et pour assurer la maintenance des systèmes et l'assistance.

Enfin, selon la *let. d*, un droit d'accès peut être donné à des tiers auxquels le Service SCPT confie des tâches de maintenance, d'exploitation ou de programmation, lorsqu'il ne peut pas lui-même exécuter ces tâches.

Selon l'*al. 2*, certains collaborateurs (« OrgAdmin ») peuvent aussi octroyer des accès à d'autres personnes. Ces accès peuvent être donnés à tous les collaborateurs de l'autorité en question. C'est le Service SCPT qui donne le droit d'octroyer des accès à des tiers, sur ordre de la personne compétente, par exemple le commandant de police. Ces collaborateurs reçoivent pour cela des accès spéciaux (jetons générant un numéro) qui ne doivent être transmis que de manière limitée. Ainsi, des traducteurs, représentants de tribunaux, et des conseils juridiques, tels que des avocats de la défense, peuvent obtenir un accès pour garantir le respect des droits inscrits dans la loi. Le droit de consultation du dossier est cependant assuré par le propriétaire du fichier (son respon-

13 Loi sur le renseignement du 25.09.2015 (**LRens**, RS **121)**

sable), à savoir, selon l'art. 13 LSCPT, les autorités qui ont accès au système de traitement selon l'art. 9 LSCPT. Ces accès ne se font donc pas depuis l'ordinateur personnel du conseil juridique, mais soit par une procédure d'appel (accès en ligne) dans des locaux désignés par l'autorité en charge du dossier, soit par un autre moyen, par exemple par un support de données mis à disposition par l'autorité. Pour les procédures dans lesquelles des témoins sont protégés, notamment, il est possible que l'autorité ne puisse divulguer que certains extraits d'un message ou qu'elle doive caviarder certains passages des procès-verbaux. Les particuliers qui ont été surveillés ou qui sont indirectement concernés par une surveillance et qui souhaitent faire valoir leurs droits de partie reçoivent, à l'instar des conseils juridiques, un droit d'accès à leurs données. Le Service SCPT n'a aucun contact direct avec les personnes ou conseils juridiques concernés. Lorsqu'un jeton est confié à un tiers, la personne compétente selon l'al. 1, let. a (le collaborateur de l'autorité), demeure responsable, par exemple aussi en cas de perte du jeton. Il doit documenter l'utilisation du jeton de manière détaillée afin que le Service SCPT puisse voir clairement qui a eu accès quand et à quelles données. Le Service SCPT examine si l'attribution des jetons peut être à l'avenir journalisée directement dans le système de traitement en question.

Selon l'*al. 3*, le Service SCPT doit contrôler de manière périodique les conditions requises pour les droits d'accès. Il s'agit notamment d'empêcher que des accès superflus continuent d'exister à cause de changements qui n'auraient pas été annoncés, tels que le départ ou le changement de fonction d'un collaborateur.

Selon l'*al. 4*, les droits d'accès au système de traitement sont réglés en annexe. Il ressort clairement de l'annexe quel accès peut être octroyé pour quelles fonctions et à quel groupe de personnes. Le règlement de traitement du Service SCPT contiendra plus de détails.

*Art. 8* Droits d'accès aux données des surveillances

Comme aujourd'hui, un collaborateur d'une autorité habilitée qui a obtenu un accès au système de traitement peut lancer l'application de traitement des données de surveillance. Cependant les données ne sont pas encore affichées. Selon l'*al. 1*, il doit être habilité pour certaines données de surveillance afin d'avoir accès à celles-ci. L'accès aux différentes surveillances peut se faire de deux manières : soit le Service SCPT octroie l'accès aux personnes mentionnées dans l'ordre de surveillance[14], soit un collaborateur de l'autorité concernée habilité selon l'al. 3 octroie l'accès à un autre collaborateur, pour autant que celui-ci ait besoin d'un accès pour exécuter ses tâches.

Selon l'*al. 2*, les personnes mentionnées aux art. 279 CPP, 70*j* PPM, 33 LRens, 35 et 36 LSCPT, en particulier les prévenus faisant l'objet d'une surveillance et les personnes anciennement disparues ayant fait l'objet d'une surveillance, peuvent déposer une demande auprès des autorités compétentes afin de faire valoir leur droit de consulter leur dossier et d'accéder aux données (cf. art. 10, al. 4, LSCPT), tout comme les personnes concernées au sens de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[15] et leurs conseils juridiques (conformément à l'art. 10, al. 1 à 3, LSCPT). L'exercice de ces droits peut être différé ou limité en fonction des dispositions applicables en l'espèce (par ex. art. 279, al. 2, CPP, art. 70*j*, al. 2, PPM, art. 63,

14 Cf. art. 3 OSCPT Communication au Service SCPT
15 RS **235.1**

al. 2, 4 et 5 LRens). Dans une procédure pénale, c'est l'autorité en charge de la procédure qui est réputée compétente, tant celle-ci n'est pas close. Après la clôture de la procédure, le droit d'accès aux données est réglé par la législation fédérale ou cantonale sur la protection des données (cf. art. 10, al. 1, LSCPT). Il en va de même pour les surveillances dans le cadre de recherches en cas d'urgence ou de recherches de personnes condamnées. Le SRC enregistre dans des systèmes d'information distincts de ceux visés à l'art. 47 LRens, en constituant un dossier par cas, les données provenant de mesures de recherche soumises à autorisation, telles les surveillances de la correspondance par poste ou télécommunication (art. 58, al. 1, LRens). C'est là que les données peuvent être consultées. Seules les données nécessaires à l'exécution du mandat peuvent être versées par le SRC dans les systèmes d'information du réseau, aux fins de leur exploitation. Dans le cas d'une surveillance ordonnée par le SRC, le droit d'accès est régi par l'art. 63 LRens. Le SRC examine tout d'abord s'il peut fournir les données demandées. Il peut reporter sa réponse si des intérêts prépondérants exigent le maintien du secret ou s'il ne traite aucune donnée concernant la personne. Celle-ci peut ensuite s'adresser au Préposé fédéral à la protection des données et à la transparence, qui met en œuvre par analogie l'ancienne procédure du renseignement indirect. Le Service SCPT n'accepte pas de telles demandes, n'étant pas compétent pour statuer. Lorsque la demande est approuvée par l'autorité compétente, les personnes concernées obtiennent l'accès aux données, soit par une procédure d'appel (accès en ligne temporaire, par ex. via un jeton) dans des locaux déterminés par l'autorité en question, soit par un autre moyen, par exemple un support de données mis à disposition par l'autorité. Ils voient ainsi les données de surveillance dont ils ont besoin pour faire valoir leurs droits. Ils peuvent pour cela utiliser des fonctions de visualisation et d'analyse du système de traitement (comme l'impression ou la transmission sécurisée aux personnes habilitées), mais seulement dans la mesure où cela est nécessaire à l'exercice de leurs droits. Au besoin, un support de données supplémentaires, selon l'art. 9 OEI-SCPT, peut être créé. Il revient avant tout à l'autorité concernée de décider si ces personnes peuvent accéder elles-mêmes aux données ou si elles doivent le faire avec l'aide d'un policier formé à cet effet.

Selon l'*al. 3*, le Service SCPT n'est pas le seul à pouvoir octroyer des accès aux données de surveillance, des collaborateurs des autorités doivent aussi pouvoir octroyer des accès. Cette possibilité a du sens lorsque des collaborateurs spécialement formés des autorités de poursuite pénale (appelés « OrgAdmin ») doivent, après que la surveillance a été ordonnée, octroyer ou retirer à des enquêteurs de leur unité administrative l'accès à des données de surveillance d'une affaire donnée. Ces collaborateurs spécialement formés doivent aussi pouvoir octroyer un accès à des personnes habilitées ou à leurs conseils juridiques selon l'al. 2. Étant donné que la mutation doit parfois être très rapidement effectuée, il est utile d'avoir une personne qui puisse l'effectuer sur place. Par ailleurs, le Service SCPT ne donne de toutes les façons accès aux données de surveillance à des personnes déterminées, officiers de police par exemple, que sur instruction des autorités ayant ordonné la surveillance, comme les autorités de poursuite pénale.

Selon l'*al 4*, des règles concernant ces droits d'accès doivent aussi être fixées dans le règlement de traitement du Service SCPT (cf. art. 7, al. 4).

*Art. 9* Interfaces

Le système de traitement possède plusieurs interfaces, pour lesquelles les bases légales nécessaires se trouvent aux art. 14 et 14*a* (disposition de coordination avec la LRens) LSCPT.

Selon la *let. a*, il y a une interface avec les systèmes des personnes obligées de collaborer pour la transmission des mandats, la réception des données et confirmation (confirmation de la réception du mandat, cf. art. 9, al. 2, let. c, OSCPT). Il peut s'agir aussi bien de mandats de renseignement et de surveillance simples que de mandats d'ordre technique ou administratif. Les prescriptions techniques se trouvent dans l'annexe 1 de l'OME-SCPT.

Selon la *let. b*, les données peuvent être exportées dans le réseau de systèmes d'information de police de l'Office fédéral de la police et dans le système d'information du SRC. Le système de traitement permet l'accès en ligne, y compris la copie de données et leur transfert, via une interface, vers le réseau de systèmes d'information de police, concrètement vers la base de données des enquêteurs (JANUS)[16]. Lorsque la LSCPT entrera en vigueur, une interface supplémentaire sera créée vers le système d'information du SRC, grâce à l'art. 14*a* LSCPT. Ainsi, l'art. 9, let. b prévoit aussi la possibilité de copier les données dans le système d'information du SRC. Le système de traitement permet un accès en ligne, y compris la copie de données et le téléchargement des données via une interface vers le système de renseignement du SRC. La copie de données dans les systèmes des cantons doit en principe utiliser un de ces deux systèmes.

Selon la *let. c*, des interfaces peuvent aussi être mises en place pour accéder aux bases de données pour vérifier des ressources d'adressage. Dans ce contexte, les ressources d'adressage peuvent être des paramètres de communication et des éléments de numérotation, tels que des indicatifs, des numéros d'appel et des numéros courts, mais aussi des informations géographiques et du matériel cartographique. Ces données peuvent provenir par exemple de TelDas, RIPE ou swisstopo. Il s'agit de données purement factuelles, c'est-à-dire de données sans lien avec des personnes spécifiques.

## Section 3 Protection des données et sécurité des données

*Art. 10* Mesures pour la sécurité des données

Le système de traitement contenant des données sensibles, des mesures techniques et organisationnelles doivent être prises pour les protéger. La norme de délégation au Conseil fédéral inscrite à l'art. 12, al. 2, LSCPT est mise en œuvre avec le présent article et les autres articles de la section 3.

Selon l'*al. 1*, *let. a*, une protection des accès et contre les modifications est mise en œuvre. Toute personne doit s'annoncer et s'authentifier avec de pouvoir accéder au système de traitement. Cette protection vise avant tout à empêcher les accès non autorisés et le vol ou l'utilisation illégale de données. De plus, les personnes autorisées à accéder au système de traitement n'ont que les droits de lecture et d'écriture dont elles ont besoin pour effectuer leurs tâches. Elles n'ont en particulier pas le droit d'effacer définitivement des données. Les droits sont définis dans l'annexe. Toutes les données du système de traitement sont sécurisées, dans la plupart des cas cryptées. Ne sont par

16 Cf. art. 14 LSCPT

exemple pas cryptées les données qui sont transmises directement au système de traitement par un réseau de fibre optique.

Selon la *let. b*, le système de traitement protège aussi les données en veillant à ce que les données ne puisse pas être lues, copiées, modifiées ou effacées lors du transport de support de données. Les données du système de traitement sont donc transmises de manière sécurisée.

Selon la *let. c*, un contrôle des accès et des modifications doit aussi être mis en œuvre. À cette fin, toutes les modifications, notamment celles effectuées selon l'art. 5, mais aussi les accès visant uniquement la lecture ou les recherches doivent être consignés dans un fichier de journalisation. Le Service SCPT contrôle régulièrement les données et les accès aux données, en procédant par sondages, afin de détecter d'éventuelles irrégularités. Ce contrôle peut aussi s'effectuer par des demandes auprès des aux autorités de poursuite pénale.

L'*al. 2* prévoit que le Service SCPT décide des mesures à prendre sur la base d'une analyse des risques. Les contrôles varient en fonction des groupes d'utilisateurs et peuvent porter sur les accès au système, les utilisateurs, l'accès à des données, le transport et les saisies. Le Service SCPT mène son analyse des risques en se fondant sur l'état de la technique tel qu'il est défini dans des normes internationales, par exemple celles définies par l'ETSI (European Telecommunications Standards Institute). Il s'agit de normes qui ont fait leurs preuves et qui sont connues aussi bien des personnes obligées de collaborer que des autorités de poursuite pénale. Le recours à ces normes permet une meilleure qualité de la transmission de données et simplifie des procédures techniques compliquées.

L'*al. 3* charge le Service SCPT d'édicter à l'attention de tous les utilisateurs (du Service SCPT, mais aussi des autorités de poursuite pénale et des personnes obligées de collaborer) les instructions nécessaires à la mise en œuvre de mesures techniques et organisationnelles en vue d'assurer la sécurité des données. Ces instructions sont nécessaires pour que les données, et notamment les données sensibles, puissent être traitées correctement dans le système et pour qu'elles soient ainsi protégées et qu'elles ne puissent pas, par exemple, être volées. Ces instructions contiendront entre autres des indications sur la manière de traiter les données, sur la manière de procéder en cas de perte d'un jeton ou pour déconnecter un accès.

Selon l'*al. 4*, tous les traitements de données dans le système, tous les accès en lecture et les recherches, de même que toutes les interventions de maintenance, d'entretien et d'assistance sont consignées dans des fichiers de journalisation qui indiquent de manière détaillée qui a fait quoi, où et quand dans le système de traitement du Service SCPT. Ces fichiers de journalisation sont conservés pendant toute la durée de conservation des renseignements et des données issues des surveillances. Conformément à l'art. 10, al. 2, de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD)[17], les procès-verbaux de journalisation sont conservés durant une année. En vertu du principe de *lex specialis*, c'est néanmoins le délai de conservation plus long prévu dans l'OST-SCPT qui prime.

17 RS **235.11**

*Art. 11* Mesures pour la sécurité du système

En cas de dérangement de l'exploitation régulière ou de risque de dérangement, par exemple en cas de surcharge du système en raison d'une mesure de surveillance ou en cas de crash du système, une intervention rapide est nécessaire pour éviter que le système ne soit simplement plus disponible et qu'un grand nombre de données soient ainsi perdues. Sitôt le dérangement constaté, le Service SCPT contacte l'autorité qui a ordonné la surveillance (par ex. ministère public) ou celle qui l'exploite (par ex. police) et discute des mesures à prendre. Le Service SCPT est libre de décider s'il contacte l'autorité ayant ordonnée la surveillance ou celle qui exploite les résultats. Après avoir entendu ces autorités, le Service SCPT décide des mesures à prendre. Dans les cas où une action immédiate est nécessaire, le Service SCPT peut aussi prendre sa décision sans avoir pris contact préalablement avec l'autorité qui a ordonné la surveillance ou celle qui exploite les résultats.

*Art. 12* Anonymisation

Les données peuvent aussi être utilisées à des fins statistiques (art. 12 OSCPT). Elles doivent cependant être anonymisées avant leur publication afin de protéger les données personnelles. Les données transférées aux Archives fédérales suisses ne sont pas anonymisées.

## Section 4 Accès aux données des surveillances par une procédure d'appel, destruction et archivage des données

*Art. 13* Accès aux données des surveillances par une procédure d'appel

L'art. 11 LSCPT expose de manière générale les délais de conservation des données dans le système de traitement.

L'*al.1* prévoit que les données de surveillances, qui comprennent aussi les données correspondantes sur le traitement des opérations et leur contrôle, demeurent à la disposition des autorités dans le système de traitement pendant une durée maximale. Cette durée se termine dans le cas d'une procédure pénale lors de l'entrée en force d'une décision (*let. a*), dans le cas d'une opération du SRC six mois après la fin de celle-ci (*let. b*), dans le cas d'une recherche d'urgence six mois après la fin de celle-ci (*let. c*), dans le cas de la recherche d'une personne condamnée six mois après la fin de celle-ci (*let. d*), et dans le cas d'une procédure d'entraide judiciaire internationale lors de l'envoi des supports de données ou des documents aux autorités pour transmission à une autorité étrangère (*let. e* ; cf. art. 9, al. 4, LSCPT). Lorsque des supports de données ont déjà été préparés avant la fin de la surveillance, les données de la surveillance restent disponibles avec toutes leurs caractéristiques de traitement jusqu'à ce que le dernier support de données ou les derniers documents aient été envoyés aux autorités pour transmission à l'autorité étrangère. Les lettres d et e valent aussi dans le cas d'une extradition et ne se limitent pas aux cas relevant de l'entraide judiciaire accessoire (petite entraide judiciaire). Le droit actuel prévoit que le Service SCPT détruit les données au plus tard trois mois après la levée de la surveillance (art. 10, al. 1, de l'actuelle OSCPT[18]). La pratique a toutefois montré que la police,

18 Ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication

notamment, a besoin de bien plus de trois mois pour exploiter les données. En outre, il peut être nécessaire de traiter ces données lorsque les voies de droit sont utilisées, pendant une procédure en deuxième instance ou devant ou le Tribunal fédéral. En moyenne, les données selon la let. a seraient ainsi disponibles, avec l'ensemble des fonctions de traitement, pendant une durée d'environ cinq ans, jusqu'à l'entrée en force d'une décision. L'autorité peut cependant aussi ordonner que les données ne doivent plus nécessairement être disponibles avec toutes les fonctions de traitement. Elles sont alors conservées dans le système de traitement pendant une période prolongée, conformément à l'al. 2. Cette procédure devrait s'appliquer dans la majorité des cas, car douze mois après la levée de la surveillance, un émolument est dû tous les trois mois, pour la durée entière des trois mois, pour la prolongation de l'accès aux données (art. 11, OEI-SCPT). Les autorités reçoivent un accès aux données de surveillance en général (cf. art. 9, al. 4, LSCPT) via une procédure d'appel (accès en ligne), directement ou via les interfaces avec le réseau de systèmes d'information de police de l'Office fédéral de la police et avec le système d'information du SRC (art. 9, let. b).

L'al. 2 prévoit qu'au-delà des moments prévus à l'al. 1, par exemple l'entrée en force d'une décision, les données sont conservées dans le système pendant une période prolongée mais avec des fonctions de traitement réduites. L'autorité peut cependant informer plut tôt le Service SCPT qu'elle n'a plus besoin de disposer des données avec l'ensemble des fonctions de traitement, de manière à ce que les données puissent être conservées en conséquence (deuxième phrase). Dans ce cas, elle n'a plus à s'acquitter des émoluments dus pour la conservation des données avec l'ensemble des fonctions de traitement (art. 11 OEI-SCPT). Les données ainsi conservées peuvent être nécessaires par exemple pour accorder aux parties le droit de consulter le dossier d'une procédure pénale, selon l'art. 101 CPP. Une autorité peut toutefois avoir de nouveau besoin des données après l'entrée en force d'une décision, par exemple en cas de reprise de la procédure préliminaire (art. 323 CPP), de révision (art. 410 CPP) ou si les données sont utiles pour une autre procédure. Le système de traitement dispose pour cela de solutions techniques qui sont appliquées de manière adaptée en fonction du type de données ou de leur volume. Les données peuvent alors être traitées avec des fonctions réduites comme la lecture, la recherche, le filtrage ou le téléchargement sélectif. En l'état actuel du projet « Programme de surveillance des télécommunications »[19], on ne sait pas encore s'il sera possible de mettre les fonctions de traitement réduites à disposition au-delà d'un cercle restreint d'utilisateurs. Dans ce cas, les autorités qui n'ont pas accès aux données conservées sur une longue période se verront mettre ces données à disposition pour transfert dans leur système d'enquête. Un nouvel accès en ligne avec fonctions de traitement n'est pas prévu. Les accès prévus sont spécifiés dans la matrice, à la let. z. Les différents délais de conservation des données sont régis par l'art. 11 LSCPT. Trente ans après la fin d'une surveillance, le Service SCPT s'enquiert auprès de l'autorité en charge de la procédure ou, si aucune ne l'est plus, auprès de la dernière à l'avoir été, du sort à réserver aux données figurant encore dans le système (art. 11, al. 5, dernière phrase, LSCPT).

L'*al. 3* prévoit qu'en cas de modifications techniques de grande ampleur apportées au système de traitement, les autorités peuvent encore disposer des données avec l'ensemble des fonctions de traitement pendant une durée de six à douze mois. La limita-

19 FF **2014** 6463

tion des possibilités de traitement peut être nécessaire par exemple en cas de changement de système ou de fournisseur. Des modifications techniques de grande ampleur peuvent aussi apparaître lorsque la structure des données se modifie fondamentalement, par exemple suite à une mise à jour logicielle importante. Maintenir les fonctions de traitement pourrait alors nécessiter d'exploiter les anciennes composantes en parallèle des nouvelles pendant plus d'un an, ce qui aurait un coût non négligeable. C'est la raison pour laquelle le traitement des données avec l'ensemble des fonctions n'est plus assuré que pendant douze mois au maximum. La durée exacte (entre six et douze mois) est fixée par le Service SCPT d'entente avec les autorités concernées. Il décide aussi de l'avenir des données en question : migration ou conservation avec des fonctions de traitement réduite, selon l'art. 11 LSCPT.

*Art. 14* Destruction

Selon *l'al. 1*, l'autorité en charge de la procédure ou, si aucune ne l'est plus, la dernière à l'avoir été, peut choisir soit de faire directement détruire les données avant l'échéance du délai de conservation selon l'art. 11 LSCPT, soit de les mettre à disposition, avant leur destruction, d'une autorité par elle désignée (par ex. aux fins de leur archivage, cf. art. 15). Selon la procédure prévue à l'art. 9, al. 4, LSCPT, les données seraient alors mises à disposition de l'autorité, c'est à dire qu'elles lui seraient communiquées, si possible cryptées, au moyen d'envois postaux de supports de données ou de documents. Les données correspondantes du traitement et du contrôle des opérations sont également effacées dans le système. Il est possible qu'après la période prolongée de conservation, la dernière autorité en charge de la procédure oublie de s'annoncer auprès du Service SCPT. Ce dernier doit alors prendre contact avec cette autorité et s'enquérir du sort à réserver aux données. Le Service SCPT s'acquitte ainsi également de ses obligations selon la dernière phrase de l'art. 11, al. 5, LSCPT, selon laquelle il doit, 30 ans après la fin de la surveillance, s'enquérir auprès de l'autorité saisie du dossier du sort à réserver aux données.

Afin que les données dans le système de traitement puissent être effacées à l'échéance de la durée de conservation même lorsque la dernière autorité en charge du dossier n'est plus identifiable ou ne donne pas d'instructions, l'*al. 2* prévoit que le Service SCPT a la possibilité de sauvegarder les données sur un support de données qu'il adresse à la plus haute instance judiciaire cantonale, dans le cas des procédures cantonales, ou au Tribunal pénal fédéral, pour les procédures des autorités fédérales. Ce processus doit être consigné dans un procès-verbal. Une fois obtenue la confirmation que les données sont lisibles, les données dans le système de traitement peuvent être effacées.

L'*al. 3* prévoit que les données liées à des renseignements sont conservées pendant douze mois avec toutes les fonctions de traitement. Ensuite, les renseignements qui peuvent être associés à une mesure de surveillance grâce à un numéro de référence ou un nom d'affaire seront conservés de manière centralisée, avec des fonctions de traitement réduites, pendant la durée de conservation des données en question, avant d'être détruits. La durée de conservation est régie par l'art. 11 LSCPT, qui renvoie notamment à l'art. 103 CPP. Les renseignements sont des informations simples qui servent aux autorités de poursuite pénale de point de départ pour la suite de leurs investigations. Elles peuvent reprendre ces données dans d'autres documents d'enquête et les ajouter ainsi au dossier pénal. Les droits d'accès sont précisés dans la matrice, à la let. z.

*Art. 15* Archivage

Etant donné que c'est en règle générale[20] l'autorité qui ordonne la surveillance qui est maître des données, et non pas le Service SCPT, l'archivage des données se fait conformément aux bases légales applicables aux maîtres des données.

L'*al. 1* définit la marche à suivre dans le cas de données de la Confédération, qui est conforme à la législation sur l'archivage de la Confédération. Selon la loi fédérale du 26 juin 1998 sur l'archivage (LAr)[21], le Service SCPT est tenu de proposer ses documents aux Archives fédérales et celles-ci déterminent, avec le Service SCPT, lesquels de ces documents ont une valeur archivistique. Le Service SCPT prépare les données à valeur archivistique selon l'art. 5, al. 1 de l'ordonnance du 8 septembre 1999 relative à la loi fédérale sur l'archivage (OLAr) [22] ainsi qu'en lien avec l'art. 5, al. 1, et l'art. 8 des instructions du 28 septembre 1999 concernant l'obligation de proposer les documents et le versement des documents aux Archives fédérales[23]. Les données qui n'ont pas de valeur archivistique sont détruites à l'expiration des délais selon l'art. 11 LSCPT.

L'*al. 2* définit la marche à suivre dans le cas de données des cantons et renvoie à l'art. 4, al. 2, LAr et indique que dans le cas de données appartenant à une autorité cantonale, c'est le droit cantonal qui s'applique. Le maître des données, comme l'autorité pénale cantonale, propose les documents aux archives cantonales pour archivage.

## Section 5 Dispositions finales

*Art. 16* Disposition transitoire

L*'al. 1* doit donner au Service SCPT la possibilité de continuer d'établir les fichiers de journalisation selon l'ancien droit jusqu'à la mise en service des composants du système selon la première étape du programme de développement et d'exploitation du système de traitement pour la surveillance des télécommunications et des systèmes d'information de police de la Confédération[24]. Les anciens systèmes, en particulier le CCIS, pour lequel le contrat de maintenance ne peut plus être adapté, ne permettent pas les journalisations souhaitées.

La conservation à long terme doit encore être planifiée et mise en œuvre, et c'est la raison de la disposition transitoire de l'*al. 2*. On ne sait pas encore si la conservation à long terme sera déjà mise en œuvre lors de l'entrée en vigueur de la loi et des ordonnances d'application. Les données continueront donc d'être mises à disposition de l'autorité qui a ordonné la surveillance, ou d'une autorité par elle désignée, sur un support de données (cf. art. 19, al. 4, OEI-SCPT) ; si le système de traitement le permet techniquement déjà, l'autorité concernée pourra aussi télécharger les données dans son système.

20 Cf. commentaire de l'art. 6 OST-SCPT
21 RS **152.1**
22 RS **152.1**
23 https://www.bar.admin.ch/bar/fr/home/archivage/versement-de-documents.html
24 FF **2014** 6463

*Art. 17* Entrée en vigueur

L'ordonnance entrera en vigueur en même temps que la loi fédérale sur la surveillance de la correspondance par poste et télécommunication entièrement révisée et toutes les autres ordonnances d'application.