Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP

Office fédéral de la justice OFJ
Domaine de direction Droit pénal
Unité Droit pénal et procédure pénale

Courte présentation du projet du Conseil fédéral relatif à la révision totale de la LSCPT

(principaux points)

Présentation de l'OFJ du 19 juin 2013
au Groupe parlementaire pour une informatique durable

Patrick Rohner, avocat, CAS MA, Office fédéral de la justice

N° référence: COO.2180.109.7.104255 / 251.1/2011/00 574

Remarque préliminaire:

Le projet de révision totale de la LSCPT a été approuvé et transmis par le Conseil fédéral au Parlement. Il est actuellement pendant devant la Commission des affaires juridiques du Conseil des Etats.

1. Champ d'application matériel de la LSCPT

La LSCPT et le Code de procédure pénale (CPP) ont pour objet la surveillance de la correspondance par télécommunication effectuée par les **autorités de poursuite pénale** dans le cadre d'une **procédure pénale**, à l'encontre d'une **personne déterminée**, lorsqu'il existe de **graves soupçons** de commission d'une infraction. Une telle surveillance, ordonnée par le **ministère public** pour un **nombre limité d'infractions** et dans le respect du principe de la **proportionnalité**, ne peut être exécutée qu'avec l'**autorisation d'un tribunal**.

Ce cas de figure doit absolument être distingué d'un autre, très différent: La surveillance de la correspondance par télécommunication qui a lieu par les **services de renseignements** en dehors de toute procédure pénale, dans un but de prévention générale de lutte contre les infractions, c'est-à-dire **à titre préventif**, **sans l'existence d'un soupçon** de commission d'une infraction, et à l'encontre de **personnes non déterminées**. C'est ce type de surveillance que permet le programme d'écoute Prism aux USA.

2. But de la LSCPT

Dans le cadre précité (cf. supra, pt 1), il s'agit de faire en sorte d'**adapter les possibilités de surveillance** de la correspondance par télécommunication à l'évolution technique importante ayant eu lieu dans ce domaine ces dernières années.

3. Champ d'application personnel de la loi ("personnes obligées de collaborer")

Y figurent des catégories de personnes susceptibles de posséder des données de communication importantes pour les autorités de poursuite pénale.

A. Catégories figurant déjà dans la loi actuelle:

- Fournisseurs de services postaux (p.ex. La Poste suisse)
- Fournisseurs de services de télécommunication (FST), y compris les fournisseurs d'accès à Internet (p.ex. Swisscom)
- Exploitants de réseaux de télécommunication internes (p.ex. réseau au sein de la Confédération)

B. Nouvelles catégories:

- **Fournisseurs de services de communication dérivés** (p.ex. hosting providers et e-mail providers)

  En résumé: ces personnes se fondent sur des FST pour offrir leurs services mais se distinguent de ceux-ci du fait qu'ils ne transportent pas eux-mêmes des données de communication à partir ou à destination de l'utilisateur.

- Personnes **laissant leur accès** à un réseau public de télécommunication **à la disposition de tiers** (p.ex. hôtels, Internet cafés et hôpitaux pour leurs clients, patients)

- Revendeurs professionnels de cartes ou de moyens semblables qui permettent l'accès à un réseau public de télécommunication (p.ex. Mobilezone, Interdiscount, Media Markt)

4. Obligations de surveillance des personnes obligées de collaborer

A. Les FST

a. Principe: Ils doivent **exécuter** les surveillances eux-mêmes (ou mandater un tiers pour ce faire).

Le Conseil fédéral devra, comme c'est le cas dans le droit actuellement en vigueur, **préciser les types** de surveillance qu'ils doivent exécuter et, pour chaque type, **les données** qui doivent être fournies.

Les FST doivent en particulier:

- **Conserver les données** dites **secondaires** de télécommunication pendant un certain temps.

  Ces données, à la différence des données dites de contenu, ne fournissent pas d'information sur le contenu de la télécommunication, mais uniquement sur le fait de savoir **qui** a été en communication **avec qui**, **quand**, **pendant combien de temps**, **d'où**, etc.

  Ces données sont obtenues dans le cadre d'une surveillance **rétroactive**.

  Durée de conservation depuis la date de la communication: Actuellement 6 mois. Dans le projet du Conseil fédéral, **12 mois** sont jugés nécessaires, 6 mois étant considérés comme insuffisants (motions Schweiger 06.3170 et Barthassat 10.4133).

- Exécuter des surveillances **en temps réel**.

  Ce type de surveillance permet, à la différence de la surveillance rétroactive portant sur des données secondaires, d'obtenir le contenu d'une communication.

b. Exception: Le Conseil fédéral peut **dispenser des FST de certaines obligations légales**, en particulier ceux qui offrent des services de télécommunication de faible importance économique ou dans le domaine de l'éducation. On aboutit ainsi en fin de compte à des exceptions possibles **semblables à celles qui existent actuellement**, au vu du renvoi à l'art. 4, al. 2 de la loi sur les télécommunications (LTC; RS 784.10).

Attention: L'**obligation minimale** des FST de **tolérer** une surveillance exécutée en principe par le Service Surveillance de la correspondance par poste et télécommunication (Service SCPT), en garantissant l'accès à leurs installations et en fournissant les informations nécessaires à l'exécution de la surveillance, de supprimer les chiffrements opérés et de fournir les **données secondaires** de télécommunication **dont ils disposent** (pas d'obligation de les conserver) demeure.

Remarque: Les FST qui bénéficieront de cette exception sont susceptibles de voir les **coûts** qu'ils doivent supporter (en particulier d'équipement) **baisser** en fonction des obligations dont ils sont dispensés.

B. Les autres personnes obligées de collaborer

a. Principe: elles ne doivent que **tolérer** une surveillance exécutée en principe par le Service SCPT.

Elles doivent en particulier:

- Garantir l'accès à leurs installations et fournir les informations nécessaires à l'exécution de la surveillance.

- Fournir les **données secondaires** de télécommunication **dont elles disposent** (pas d'obligation de les conserver).

b. Exception: Si cela est nécessaire pour surveiller de manière adéquate la correspondance par télécommunication, le Conseil fédéral pourra, nouvellement, soumettre tout ou partie des **fournisseurs de services de communication dérivés** offrant des services d'une grande importance économique ou à un grand nombre d'utilisateurs à des **obligations supplémentaires**, c'est à-dire à tout ou partie des obligations qu'ont en principe les FST (cf. supra, pt 4, A, a). Dans ce cas, les dispositions concernant aux FST seront applicables par analogie.

Remarque: Les fournisseurs de services de communication dérivés touchés par une telle extension pourront voir les **coûts** qu'ils doivent supporter (en particulier d'équipement) **augmenter** en fonction des obligations supplémentaires qui seront les leurs.

5. Conservation centralisée de longue durée des données obtenues dans le cadre de la surveillance de la correspondance par télécommunication dans le système informatique du Service-SCPT

Aujourd'hui, les données sont transmises par le Service-SCPT aux autorités de poursuite pénale au moyen de supports de données envoyés **par la poste**. Ensuite, elles sont effacées du système du Service-SCPT.

Au vu du fait que ces données sont **de plus en plus volumineuses** – en particulier celles provenant de surveillances d'Internet – et que cette tendance va continuer, elles peuvent de plus en plus difficilement être transmises, stockées et administrées selon la méthode actuelle.

Avec le changement proposé, ces problèmes peuvent être résolus et la sécurité des données améliorée. Les autorités de

poursuite pénale pourront obtenir les données de surveillance les concernant par un **accès en ligne** au système du Service-SCPT.

6. Allongement de la durée de conservation des données secondaires, en particulier de télécommunication, de 6 à 12 mois

En vertu du droit actuel, la durée de conservation de ces données depuis la communication est de 6 mois.

Dans le projet du Conseil fédéral, cette durée est augmentée à 12 mois, afin de permettre une **poursuite pénale efficace**, notamment dans le domaine de la **pédopornographie**, du **trafic de stupéfiants**, du **crime organisé** et de du **terrorisme**. Cette durée est jugée nécessaire pour atteindre ce but, **6 mois** étant à cet effet considérés comme **insuffisants** (motions Schweiger 06.3170 et Barthassat 10.4133).

Des expériences faites par les autorités de poursuite pénale il ressort en particulier ce qui suit: l'actuelle durée de conservation des données secondaires est trop courte, puisque ce délai est souvent échu, totalement ou en grande partie, lorsque l'autorité de poursuite pénale est en mesure, au vu de l'avancement de l'enquête, d'ordonner une surveillance rétroactive.

7. Informations sur la nature et les caractéristiques des services sur le marché actuellement ou dans les 6 mois

Ces informations doivent être fournies par les FST au Service-SCPT, à la demande de celui-ci.

Le but de cette disposition est de permettre au service d'être en possession des informations nécessaires pour assurer une exécution correcte des surveillances. Il faut lui permettre d'**anticiper les problèmes**, et non seulement de réagir à ceux-ci. Concernant en particulier les services qui vont être mis sur le marché, il s'agit de permettre au service d'entreprendre les démarches nécessaires afin de tenter de rendre à brève échéance possible une exécution correcte des surveillances de ces nouveaux services, si possible déjà au moment où ils arrivent sur le marché.

Remarque: Les FST n'ont nullement besoin d'obtenir une autorisation du Service-SCPT pour mettre un nouveau service sur le marché. Il ne peut par conséquent **pas s'opposer** à sa mise sur le marché. Avec le système proposé, il est donc envisageable qu'un nouveau service arrivé sur le marché ne puisse (momentanément ou durablement) pas être surveillé, occasionnant ainsi une lacune au niveau de la surveillance.

8. Sanction en cas de violation d'obligations susceptible d'entraver les surveillances ordonnées

Les FST peuvent être amenés à **supporter les coûts** découlant du fait qu'ils ne remplissent pas leurs obligations et qu'il doit par conséquent être fait appel au Service-SCPT ou à des tiers pour les exécuter.

En cas de violation de prescriptions dans le domaine de la surveillance de la correspondance, le Service-SCPT peut prononcer un **avertissement**.

Certaines violations d'obligations sont punies au moyen de **dispositions pénales**, p.ex. en cas de non-conservation des données secondaires.

9. Surveillance en dehors d'une procédure pénale

Exceptionnellement, avec l'**autorisation d'un tribunal**, une surveillance peut être autorisée, en dehors d'une procédure pénale en cours, à titre **subsidiaire** par rapport aux autres mesures de recherches, pour:

- Retrouver une personne dont il y a lieu de penser que sa santé ou sa vie sont gravement menacées.

- Retrouver une personne **(en fuite) condamnée** à une peine privative de liberté ou qui fait l'objet d'une mesure entraînant une privation de liberté, sur la base d'un jugement définitif et exécutoire.

10. Recours contre les décisions de surveillance du Service-SCPT

Un FST peut faire valoir des griefs relevant du **droit administratif**, comme p.ex. le fait qu'il ne serait légalement pas obligé d'effectuer une surveillance en temps réel.

Mais un FST ne peut faire valoir des griefs relatifs à la **procédure pénale**, car celle-ci ne le concerne pas. Il ne peut – à la différence de la personne surveillée – p.ex. pas faire valoir le fait qu'il n'existerait au sens du CPP pas de grave soupçon permettant aux autorités de poursuite pénale d'ordonner une surveillance de la correspondance par télécommunication.

11. Frais et émoluments

Même si dans l'avant-projet il a avait été prévu de supprimer l'indemnité versée aux FST, le projet du Conseil fédéral prévoit, en résumé, de conserver le **système actuel**, à savoir:

- Les FST doivent **financer les équipements** nécessaires à la mise en œuvre des surveillances.
- Ils obtiennent une **indemnité équitable** pour les frais occasionnés par l'exécution d'une mesure de surveillance.
- L'autorité qui a ordonné une surveillance continuera doit verser un **émolument** au service pour les prestations de celui-ci liées à l'exécution de la surveillance.
- Le **Conseil fédéral fixe** les indemnités et les émoluments relatifs aux différents types de surveillances.

12. Possibilité d'utiliser des dispositifs techniques de surveillance tels que les IMSI-catchers

Création d'une base légale permettant d'**étendre** la possibilité d'utiliser ces dispositifs. Il n'est plus seulement possible de les utiliser pour localiser des appareils de communication mobile ou leurs utilisateurs et écouter ou enregistrer des communications mais, logiquement, aussi pour **identifier** des appareils de communication mobile ou leurs utilisateurs.

L'IMSI-catcher permet de simuler les effets d'une station de base d'un réseau de téléphonie mobile. Les appareils se trouvant dans son champ s'annoncent et s'identifient auprès de lui comme ils le feraient auprès d'une station de base d'un réseau de téléphonie mobile.

Du fait que l'IMSI-catcher est susceptible de perturber les télécommunications, une **autorisation préalable de l'OFCOM** est nécessaire pour y avoir recours. On ne peut ainsi également recourir à ce mode de surveillance qu'à titre **subsidiaire** par rapport aux mesures de surveillance de la correspondance par télécommunication dites classiques. Pour le reste, les **conditions usuelles** relatives aux mesures de surveillance dites classiques sont applicables, en particulier l'existence d'un grave soupçon de commission d'une infraction figurant dans la liste restrictive prévue, le respect du principe de la proportionnalité, un ordre de surveillance du ministère public et l'autorisation d'un tribunal portant sur la surveillance ordonnée.

13. Possibilité d'utiliser des programmes informatiques spéciaux de surveillance de la correspondance par télécommunication (Government Software [GovWare])

Création d'une **base légale claire** permettant d'avoir recours à ces programmes, dans le but d'intercepter, de lire et de transférer le contenu des communications et des données secondaires de télécommunication **non cryptées**.

Le GovWare est introduit dans le système informatique surveillé, p.ex. un PC, par la police, sur ordre du procureur, afin d'obtenir les données avant qu'elles ne soient cryptées.

Ce mode de surveillance est particulièrement **incisif**, étant donné qu'on ne se contente pas de dévier les communications de la personne surveillée, mais qu'on pénètre dans le système informatique considéré. Il est donc proposé qu'on ne puisse y avoir recours qu'à titre **subsidiaire** par rapport aux mesures de surveillance de la correspondance par télécommunication dites classiques. Pour le même motif, on ne peut utiliser ce mode de surveillance que pour une **partie des infractions** pour lesquelles une surveillance classique peut être ordonnée (liste d'infractions applicable à l'investigation secrète). Pour le reste, les **conditions usuelles** relatives aux mesures de surveillance classiques sont applicables, en particulier l'existence d'un grave soupçon de commission d'une infraction au sens précité, le respect du principe de la proportionnalité, un ordre de surveillance du ministère public et l'autorisation d'un tribunal portant sur la surveillance ordonnée.

Le recours à des GovWare n'est prévu que pour obtenir des données relevant de la correspondance par télécommunication. Il est par conséquent proposé que les autres données qui auraient été collectées au moyen d'un GovWare, p.ex. lors de la **perquisition en ligne** (online Durchsuchung) d'un ordinateur, doivent être **détruites** et que les informations ainsi recueillies **ne puissent être exploitées**.