# L'enregistrement systématique des données secondaires de communication

**Auteur :** Emilie Jacot-Guillarmod

**Date :** 17 mai 2018

ATF 144 I 126 - TF, 02.03.2018, 1C_598/2016*

*L'enregistrement systématique des données secondaires de communication (*Randdaten*) constitue une atteinte admissible au droit à la vie privée (*art. 8 CEDH *et* art. 13 Cst. féd.*). En particulier, cette atteinte n'est pas disproportionnée au regard des conditions strictes posées par les* art. 269 ss CPP *pour la remise ultérieure de ces données aux autorités pénales et de l'obligation des opérateurs de garantir la sécurité des données concernées.*

**Faits**

Plusieurs individus demandent au Service fédéral surveillance par poste et communication (le "Service SCPT") **d'interdire** à leur opérateur téléphonique de **conserver les données relatives au trafic** et à la facturation les concernant. Le Service SCPT rejette ces requêtes. Les demandeurs recourent contre cette décision auprès du Tribunal administratif fédéral, sans succès.

Saisi de la cause, le Tribunal fédéral doit déterminer si **l'obligation faite aux opérateurs téléphoniques de conserver durant six mois les données permettant l'identification des usagers ainsi que les données relatives au trafic et à la facturation** (art. 15 al. 3 aLSCPT) viole le droit fondamental à la **vie privée**.

**Droit**

Aux termes de l'art. 15 al. 3 aLSCPT, les fournisseurs de services de télécommunications sont tenus de **conserver durant six mois les données** permettant l'identification des usagers ainsi que les données relatives au trafic et à la facturation ("**données secondaires de télécommunication"**).

Les recourants font valoir que l'enregistrement systématique de leurs données par les opérateurs téléphoniques viole leurs droits fondamentaux, en particulier leur **droit à la vie privée** et à la protection de leurs **données personnelles** (art. 8 CEDH et art. 13 al. 2 Cst.). Le droit à la vie privée protège notamment les particuliers contre l'emploi abusif de leurs données personnelles. En principe, chacun a le droit de déterminer librement le traitement de ses données personnelles, notamment l'enregistrement de celles-ci (art. 13 al. 2 Cst. *cum* art. 3 let. d LPD). Les données secondaires de télécommunication constituent en principe des **données personnelles**, dans la mesure où elles se rapportent à une personne identifiée (art. 3 let. a LPD). L'enregistrement systématique prescrit à l'art. 15 al. 3 aLSCPT porte dès lors **atteinte** au droit à la sphère privée.

Une telle atteinte n'est admissible que si elle (1) repose sur une **base légale suffisante**, (2) intevient dans **l'intérêt public** et (3) est **proportionnée** au but visée (art. 36 Cst.). L'art. 8 par. 2 CEDH pose des conditions similaires.

Les exigences quant à la précision de la **base légale** sont plus élevées en présence d'une atteinte **grave** au droit fondamental concerné. Les données secondaires de télécommunication ne sont en tant que telles **pas particulièrement sensibles**. Les recourants font cependant valoir qu'on peut en déduire diverses informations quant aux habitudes des intéressés, le cas échéant par

recoupement avec d'autres données. Cela étant, de telles déductions ne peuvent intervenir qu'en cas de **remise ultérieure des données secondaires de télécommunication aux autorités pénales** conformément aux dispositions du CPP (art. 269 ss CPP). La décision litigieuse porte exclusivement sur l'enregistrement des données par les opérateurs. Les recourants ne font du reste pas valoir que leurs données auraient été remises aux autorités pénales. Dans ces circonstances, **on ne saurait retenir une atteinte grave à leurs droits**. Partant, l'art. 15 al. 3 aLSCPT constitue une base légale suffisante.

L'enregistrement des données litigieuses vise à permettre la résolution d'enquêtes pénales, afin de garantir la **sécurité publique** et les **droits d'autrui**. Il poursuit dès lors un but d'intérêt public.

Les recourants se prévalent de la jurisprudence de la **CJUE**, selon laquelle le droit de l'Union ne permet pas, sous l'angle de la **proportionnalité**, l'enregistrement des données secondaires de communication de tous les utilisateurs, indépendamment de soupçons d'une infraction pénale (CJUE, décision du 8 avril C-293/12 et C-594/12, *Digital Rights Ireland*, et décision du 21 décembre 2016 C-203/15 et C-698/15, *Tele2 Sverige*). Si ces décisions mettent en lumière la situation juridique en droit européen, elles ne lient pas le Tribunal fédéral et **ne peuvent être transposées** sans autre **au droit suisse.** En effet, **le législateur suisse** a expressément réitéré le choix de prescrire l'enregistrement de l'ensemble des données secondaires de télécommunication dans le cadre de la révision intégrale de la LSCPT (cf. Message nLSCPT).

Il sied en revanche de tenir compte de la jurisprudence de la **CourEDH** en la matière. Cette dernière retient que certaines mesures propres à protéger la sécurité publique peuvent s'avérer inadmissibles, notamment lorsqu'elles résultent en une **surveillance généralisée antidémocratique** (cf. p. ex. CourEDH, arrêt *Szabó et Vissy c. Hongrie* du 12 janvier 2016, N. 37138/14). Ainsi, la CourEDH a jugé disproportionnés la **surveillance systématique** du **contenu** de toutes les télécommunications en Russie et **l'accès illimité des autorités** aux données correspondantes (CourEDH, arrêt *Zakharov c. Russie* du 4 décembre 2015, N. 47143/06), ainsi qu'un dispositif de surveillance anti-terroriste en Hongrie, dans la mesure où il touchait **presque l'entier de la population sans garanties appropriées** (CourEDH, arrêt *Szabó et Vissy c. Hongrie* du 12 janvier 2016, N. 37138/14).

Il convient de relever qu'**en Suisse**, les **autorités pénales n'obtiennent accès** aux données secondaires de télécommunication qu'aux **conditions strictes des** art. 269 ss CPP, lesquels prescrivent notamment une **pesée des intérêts dans chaque cas** ainsi que l'intervention d'un **tribunal indépendant**. En outre, les opérateurs téléphoniques sont tenus de garantir la **sécurité** et l'intégrité des données pendant leur durée de conservation (art. 9 aOSCPT *cum* art. 20 LPD; cf. ég. lignes directrices techniques, opérationnelles et administratives du Service SCPT). Au demeurant, l'enregistrement des données pour une **durée de six mois** n'apparaît **pas excessif** au regard du temps que nécessitent typiquement les enquêtes pénales, en particulier en matière de terrorisme ou de criminalité organisée. **Au regard de l'ensemble des circonstances susvisées**, l'enregistrement des données secondaires de télécommunication au sens de l'art. 15 al. 3 LSCPT apparaît **proportionné**.

L'atteinte au droit à la vie privée résultant de l'enregistrement des données secondaires de communication est dès lors conforme aux exigences de l'art. 8 par. 2 CEDH et de l'art. 36 Cst. Partant, le recours est rejeté.

**Note**

La **LSCPT actuelle**, entrée en vigueur le 1er mars 2018, prévoit toujours l'obligation pour les opérateurs de conserver les données secondaires de télécommunication pendant six mois (art. 26 al. 5 LSCPT).

Le Tribunal fédéral relève que l'enregistrement de ces données pourrait aussi nuire indirectement à la **liberté d'expression** (art. 10 CEDH et art. 17 Cst.) en créant un sentiment dissuasif de surveillance généralisée ("*chilling effect*"). Au regard de l'issue de la cause, il s'abstient toutefois de trancher la question.