Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP
Secrétariat général SG DFJP
Service d'information

État au 18 août 2014

FAQ- Questions fréquentes

Les statistiques du Service SCPT montrent que les autorités de poursuite pénale ont ordonné nettement plus de surveillances ces dernières années. Pour quelle raison ?

Le Service SCPT est chargé de mettre en œuvre les mesures de surveillance de la correspondance par poste et télécommunication ordonnées par les autorités de poursuite pénale. Il est vrai que le nombre des surveillances a augmenté au cours des dernières années : les statistiques 2013 révèlent que les mesures de surveillance dite rétroactive, qui permettent de recueillir les données relatives aux liaisons établies par la personne surveillée, affichent une hausse d'un quart par rapport à 2008. Cette hausse est toutefois nettement inférieure à la progression enregistrée en matière d'utilisation des outils de télécommunication : la durée globale des liaisons a augmenté d'un tiers entre 2008 et 2012 (augmentation d'environ 8000 millions de minutes à 10 500 millions de minutes), tandis que le volume des données transmises par téléphone portable est plus de 20 fois plus élevé (hausse de près de 700 à 16 600 téraoctets). De manière générale, on compte aujourd'hui bien plus de raccordements mobiles qu'il y a encore quelques années. Leur nombre a doublé depuis 2002, passant de 5,2 millions à 10,6 millions (source : statistiques 2012 des télécommunications ; Statistique suisse ; ComCom).

L'arrêt du 8 avril 2014 de la Cour de justice de l'Union européenne (CJUE) concernant la conservation des données secondaires lie-t-il la Suisse ?

Non, la Suisse n'a pas repris la directive de l'UE sur la conservation des données, qui ne s'applique donc pas en Suisse.

Les données secondaires dont il est question n'incluent pas le contenu des conversations, mais exclusivement les données permettant de savoir qui a communiqué avec quelle personne, quand, pendant combien de temps, à partir de quel endroit et avec quels moyens techniques. Ces informations peuvent être utiles pour reconstituer des comportements criminels ou pour localiser des personnes disparues (recherche en cas d'urgence).

Dans son arrêt, la CJUE n'interdit pas en soi la conservation des données secondaires mais exige des règles plus strictes concernant l'accès à ces données, ainsi que leur conservation et leur utilisation. Ce cadre strict qui fait défaut dans la directive de l'UE est cependant posé par la législation suisse, de sorte que, selon une première appréciation de l'Office fédéral de la justice, l'arrêt de la CJUE ne remet pas indirectement en cause la conservation des données secondaires en Suisse. Cette constatation vaut pour le droit actuel comme pour la

révision proposée, qui ferait passer la durée de conservation des données en question de six à douze mois.

Pour quelle raison la conservation des données secondaires est-elle admise en Suisse ?

En Suisse, l'atteinte aux droits fondamentaux liée à la conservation des données secondaires est réduite au strict nécessaire. Les données sont certes conservées et gardées en réserve en l'absence de soupçon d'infraction, mais la police et les autorités de poursuite pénale n'y ont pas un accès illimité. Les données ne sont pas conservées par l'État, mais par les fournisseurs de services de télécommunication. La loi fixe un cadre strict et subordonne la consultation de ces données à plusieurs conditions. Une surveillance ne peut ainsi être ordonnée, dans le cadre d'une procédure pénale ou d'entraide judiciaire, que s'il existe de graves soupçons qu'un crime ou un délit a été commis. La surveillance doit en outre se justifier au regard de la gravité de l'infraction et les mesures prises jusqu'alors dans le cadre de l'instruction doivent être restées sans succès ou l'enquête n'avoir aucune chance d'aboutir ou être excessivement difficile en l'absence de surveillance. Lorsqu'il s'agit de rechercher une personne disparue, la surveillance n'est admise que si des indices sérieux donnent lieu de penser que la santé ou la vie de la personne sont gravement menacées. Un juge vérifie d'office dans chaque cas que ces conditions sont remplies. La surveillance ne reste pas non plus secrète : le motif, le type et la durée de la surveillance sont communiqués à la personne surveillée au plus tard lorsque la procédure préliminaire est close.

Quelles seraient les conséquences d'une non-conservation des données secondaires ?

Si les données secondaires n'étaient plus conservées, la poursuite des infractions deviendrait plus compliquée, ce qui aurait des répercussions sur la sécurité publique. La police ne pourrait plus analyser les traces que les auteurs d'infractions laissent par leurs activités sur les réseaux de communication téléphonique ou sur internet, que ces infractions relèvent de la cybercriminalité, de la pornographie enfantine, du trafic de stupéfiants, des homicides, des infractions contre le patrimoine ou du terrorisme. Sans conservation des données secondaires, il serait aussi plus difficile de rechercher des personnes disparues ou condamnées : il serait par exemple difficile d'établir à quel endroit une personne se trouvait lorsqu'elle a téléphoné pour la dernière fois.

Dans quels cas le recours à des chevaux de Troie fédéraux (Government Software ou GovWare) est-il autorisé et qui exactement peut ordonner leur utilisation ?

Le Conseil fédéral a décidé de créer une base légale claire pour le recours à des GovWares. Leur utilisation ne sera admise qu'en présence d'une infraction grave, figurant dans une liste plus restreinte que celle qui vaut pour la surveillance classique de la correspondance par poste et télécommunication (art. 269 ss CPP). Il s'agit d'infractions dont la poursuite justifierait également d'ordonner une investigation secrète (art. 286, al. 2, CPP). De plus, l'intervention doit se limiter à la surveillance des communications. La perquisition en ligne d'un ordinateur ou la surveillance d'une pièce au moyen de la caméra ou du micro d'un ordinateur sont donc interdites. Le recours à un GovWare devra par ailleurs dans tous les cas être ordonné par le ministère public et autorisé par le tribunal des mesures de contrainte.

Pourquoi a-t-on besoin de GovWares ou de chevaux de Troie fédéraux ?

L'utilisation de GovWares est indispensable pour que la poursuite pénale des criminels reste techniquement à niveau. L'objectif n'est pas de surveiller davantage, et encore moins de « fouiner » ou perquisitionner un ordinateur à titre préventif. Les autorités de poursuite pénale doivent toutefois pouvoir recourir aux outils dont elles ont besoin pour poursuivre les infractions graves. Autrement, les criminels pourraient utiliser des moyens de communication modernes et les autorités de poursuite pénale ne pourraient pas suivre : les trafiquants de drogue pourraient ainsi traiter leurs affaires via des communications cryptées sur internet en ayant la certitude qu'elles ne peuvent pas être surveillés.

Que font les autorités de poursuite pénale pour rendre l'utilisation de GovWares aussi sûre que possible et pour empêcher les abus ?

Pour empêcher l'utilisation abusive de GovWares, une combinaison de mesures techniques et organisationnelles est nécessaire. Sur le plan technique, les autorités de poursuite pénale définissent les fonctions de sécurité nécessaires. Une autorité indépendante vérifie que ces fonctions de sécurité sont complètes et installées selon les normes reconnues. Sur le plan de l'organisation, les autorités de poursuite pénale doivent décrire en détail le processus d'installation et d'exploitation du GovWare. Il s'agit notamment de définir les autorisations des personnes ayant accès au programme et de régler l'utilisation du système informatique. Enfin une journalisation exhaustive est mise en place, qui permet, notamment au juge, de reconstituer toutes les étapes de la procédure, depuis la demande jusqu'à la fin de la surveillance, en passant par l'octroi de l'autorisation. Toutes ces précautions réduisent autant que possible la probabilité d'une utilisation abusive des GovWares. Devant un tribunal, les résultats d'une surveillance téléphonique ne peuvent être reconnus comme moyens de preuve que s'il s'agit bien des preuves pour l'obtention desquelles la surveillance a été ordonnée et si la surveillance a été autorisée dans les formes.

On prétend que le Département fédéral de justice et police (DFJP) et le Département fédéral de la défense, de la protection de la population et des sports (DDPS) entendent acquérir et utiliser ensemble un GovWare. Est-ce exact ? Des préparatifs sont-ils déjà en cours ?

Il n'est pas prévu que le DFJP et le DDPS collaborent pour l'acquisition ou pour l'utilisation de GovWares. Aucun préparatif n'est en cours.

La crainte d'un État fouineur ou d'atteintes à la sphère privée sont-elles vraiment sans fondement ?

Oui, car l'écoute du contenu des conversations téléphoniques ou la surveillance des activités sur internet à titre préventif, comme le ferait un service secret, est interdite. La surveillance n'est possible que si une procédure pénale visant à réprimer une infraction grave a été ouverte ; elle doit aussi dans tous les cas être autorisée par un tribunal. Les statistiques montrent qu'une surveillance n'intervient que pour environ 1,5 % des infractions. Concrètement, en 2013, les 725 678 infractions répertoriées ont donné lieu à 10 860 surveillances, sachant, qui plus est, que plusieurs surveillances peuvent concerner la même

affaires, par exemple lorsqu'il s'agit de surveiller le raccordement fixe et plusieurs téléphones cellulaires appartenant à un trafiquant de drogue.

Qu'en est-il de l'introduction du système d'interception Suisse (Interception System Schweiz, ISS) ? Ne faudrait-il pas d'abord boucler la révision de la LSCPT ?
Le Service SCPT gère un système informatique qui lui permet de mettre à la disposition des autorités de poursuite pénale les données des fournisseurs de prestations de communication, lorsque les conditions légales sont remplies. Ce système est arrivé en fin de vie et est actuellement en cours de remplacement, par un système appelé « Interception System Schweiz » (ISS). Les fonctions de ce nouveau système correspondent à celle du système qu'il remplace et satisfont donc aux exigences légales actuelles. Lorsque la nouvelle loi révisée sur la surveillance de la correspondance par poste et télécommunication (LSCPT) entrera en vigueur, l'ISS pourra être adapté aux nouvelles exigences. Selon la planification actuelle, le système ISS sera mis en fonction durant la première moitié de l'année 2015, d'entente avec les fournisseurs de services de téléphonie et d'accès internet, de même qu'avec les autorités de poursuite pénale.