Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP
Service Surveillance de la correspondance par poste et télécommunication SCPT

Rapport annuel 2022
Service SCPT

La surveillance des télécommunications s'inscrit dans un contexte mondial. Dans les conférences internationales, les organes réunissant plusieurs pays et, avant tout, dans l'industrie des télécommunications, la langue commune est l'anglais. Le terme utilisé en anglais pour la surveillance conforme à la loi – Lawful Interception (LI) – s'est ainsi également fait une place en Suisse. Le Service SCPT se plie à cet usage depuis 2010, date à laquelle il a mis en ligne son propre site internet à l'adresse :

www.li.admin.ch

Éditorial de René Koch 4

01 Vue d'ensemble

Brève présentation du Service SCPT 7
L'année 2022 en bref 11

02 Informations de fond

Une équipe pour des interventions spéciales 15
De nombreux fournisseurs de services de télécommunication ne sont pas tenus de réaliser eux-mêmes la surveillance. Si la justice s'intéresse à l'un de leurs clients, l'équipe des cas spéciaux du Service SCPT prend le relais..

À la pointe de la technologie 20
Le système de traitement de la surveillance des télécommunications du Service SCPT a pris de l'âge. La partie « en temps réel » sera entièrement remaniée.

« Plusieurs milliers d'employés des services secrets étrangers » 22
Jürg Bühler, directeur suppléant du Service de renseignement de la Confédération, parle de l'importance de la surveillance des télécommunications, du contre-espionnage, de la lutte contre le terrorisme et des cyberattaques.

03 Faits et chiffres

Le détail des mesures de surveillance 27
Collaborateurs, prestations et finances 30

Chère lectrice, cher lecteur,

Toute mesure de surveillance de la correspondance par poste et télécommunication constitue une atteinte grave aux droits fondamentaux de la personne concernée. Les atteintes à ces droits protégés par la Constitution ne sont possibles que si une loi le prévoit expressément. L'exécution concrète des mesures est réglée dans les ordonnances de mise en œuvre. Chaque mesure de surveillance doit en outre être autorisée par un juge.

Pour être absolument clair : il ne peut y avoir le moindre écart entre l'exécution d'une mesure par le Service SCPT et la base légale qui permet cette mesure.

La technologie des télécommunications se développe de manière exponentielle et offre toujours plus de nouveaux services et de nouvelles possibilités de communication. Pour pouvoir suivre le rythme, la surveillance des télécommunications doit être régulièrement adaptée sur les plans technique, organisationnel et administratif. C'est le Service SCPT qui est à la manœuvre, avec le concours des autorités pénales et des fournisseurs de services de télécommunication.

Même si la surveillance des télécommunications évolue très rapidement, le mandat que nous donne la loi ne change pas : contribuer à l'efficacité de la poursuite pénale. Un des instruments dont nous disposons à cette fin est l'équipe des cas spéciaux.

« Même si la surveillance des télécommunications évolue très rapidement, le mandat que nous donne la loi ne change pas : contribuer à l'efficacité de la poursuite pénale. »

Cette unité mobile peut, sur ordre du juge, exécuter une mesure de surveillance chez n'importe quel fournisseur de services de télécommunication ayant des activités en Suisse. Pour tout savoir sur ces interventions spéciales et sur le déploiement de nos experts chargés de mettre en œuvre les mesures de surveillance, rendez-vous à la page 15.

Personnellement, ce récit m'a rappelé mes débuts au Service SCPT, il y a maintenant 15 ans. À l'époque, nous étions tributaires de partenaires externes pour ces cas spéciaux. Avec ma formation de technicien des télécommunications et d'ingénieur, j'ai vite compris que ce modèle n'avait plus d'avenir, au vu de la rapidité de l'évolution technologique. C'est pour cela que depuis 2010, le Service SCPT s'attache à développer des compétences propres dans tous ses domaines d'activité, afin d'être capable de répondre au mieux aux défis qui se présentent dans son environnement complexe et hautement spécialisé.

Bonne lecture !

René Koch
Chef du Service SCPT (jusqu'en mai 2023)

01

VUE D’ENSEMBLE

On entend par fournisseur de services de télécommunication des opérateurs tels que Swisscom, Sunrise ou Salt qui proposent de la téléphonie fixe ou mobile, ainsi que des services d'accès à internet et de messagerie électronique.

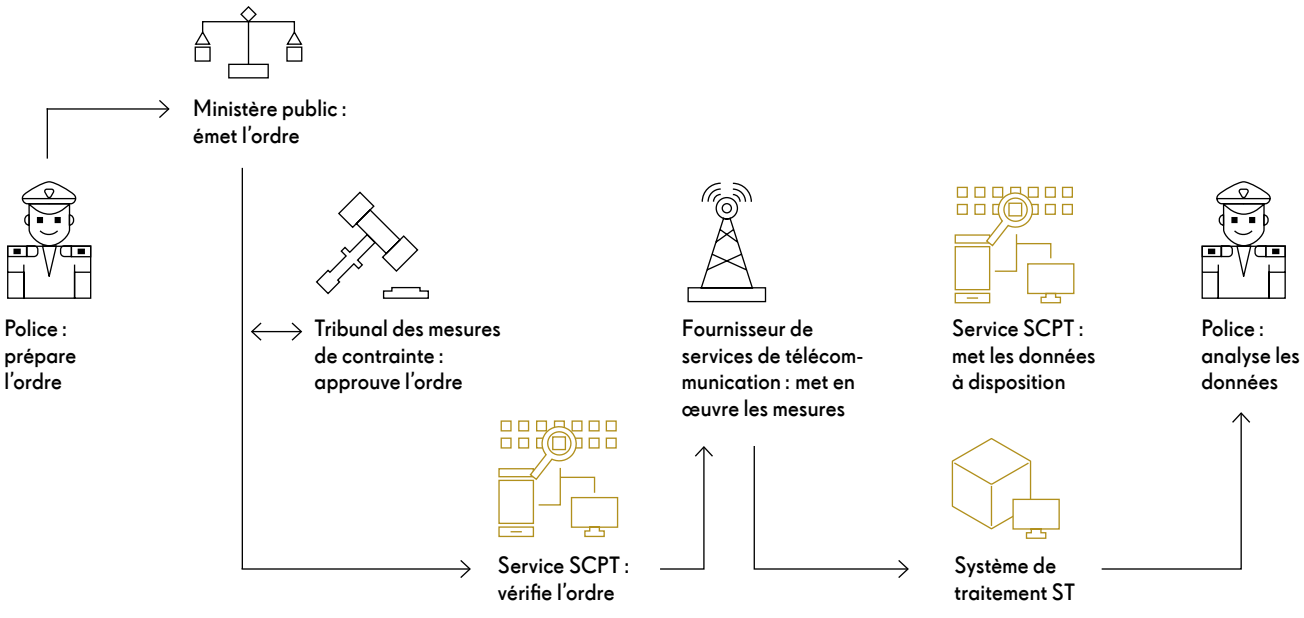
Brève présentation du Service SCPT

Pour élucider des infractions graves, les autorités de poursuite pénale de la Confédération et des cantons peuvent ordonner des mesures de surveillance de la correspondance par poste et télécommunication. Depuis le 1er janvier 1998, le Service SCPT est compétent pour la mise en œuvre de ces mesures. Il veille parallèlement au respect des prescriptions en vigueur. Il récupère auprès des fournisseurs de services de télécommunication (FST) les données requises par les autorités pénales ou par le Service de renseignement de la Confédération (SRC) et les transmet aux enquêteurs chargés de les évaluer et de les analyser.

Ni la criminalité, ni les télécommunications modernes ne connaissent de frontières. La collaboration internationale joue dès lors un rôle important dans la lutte contre le crime. Le Service SCPT participe à cette fin à la définition de normes internationales, et partage connaissances et informations avec des services homologues d'autres pays.

Le Service SCPT est compétent pour mettre en œuvre la surveillance de la correspondance par poste et télécommunication. Il accomplit sa mission de façon autonome, sans être assujetti à des instructions. Sur le plan administratif, il est rattaché au Centre de services informatiques du Département fédéral de justice et police (CSI-DFJP). Il est structuré en quatre sections.

La procédure de surveillance



Les quatre sections

La direction du Service SCPT (de gauche à droite) : René Koch (chef du Service SCPT et de la section Procédures pénales administratives), Jean-Louis Biberstein (chef adjoint du Service SCPT et chef Droit et contrôle de gestion), Alexandre Suter (chef Provider management) et Michael Galliker (chef Gestion de la surveillance)

Provider Management

L'équipe compte 22 personnes, qui sont notamment chargées d'élaborer et de tenir à jour les prescriptions techniques que doivent observer les FST lorsqu'ils échangent des données avec le Service SCPT.

Cette section a également la responsabilité des procédures dites de vérification de la conformité (*compliance*), qui permettent au Service SCPT de s'assurer de la disponibilité des opérateurs à surveiller et à fournir des renseignements. Selon la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT), les opérateurs doivent en tout temps être capables de surveiller les services qu'ils proposent et de fournir les renseignements et informations nécessaires concernant ces services, à moins qu'ils n'aient obtenu en bonne et due forme d'être exonérés de l'obligation d'exécuter eux-mêmes les surveillances.

La section Provider Management développe et exploite des solutions spéciales sur mesure pour la mise en œuvre de surveillances

chez les opérateurs qui ne sont pas tenus, ou pas en capacité, de le faire eux-mêmes. C'est là qu'intervient l'équipe dite des « cas spéciaux », lorsqu'il faut exécuter une surveillance chez un petit fournisseur – par exemple l'exploitant d'un réseau câblé local ou un hôtel. Un article en page 15 est consacré à ces interventions spéciales.

Les collaboratrices et les collaborateurs de la section gèrent par ailleurs les relations avec plus de 900 fournisseurs, les conseillent sur des questions techniques ou juridiques et, dans le cadre de leurs compétences de supervision, édictent des prescriptions et rendent des décisions.

Une équipe de quatre personnes assure le bon fonctionnement des applications du système de traitement vers lequel sont envoyées les données.

Les experts de la section Provider Management soutiennent par ailleurs le développement de nouvelles applications et s'engagent dans divers organismes nationaux et internationaux de normalisation, où sont par exemple développées les spécifications des interfaces pour les réseaux 4G et 5G.

Gestion de la surveillance

Comptant 17 personnes, la section Gestion de la surveillance veille à la bonne collaboration du Service SCPT avec les autorités pénales et avec le SRC.

L'équipe conseille les corps de police, les ministères publics, les tribunaux des mesures de contrainte et le SRC pour toutes les questions juridiques, techniques, organisationnelles et administratives concernant la surveillance de la correspondance par poste et télécommunication.

Les collaboratrices et les collaborateurs réceptionnent les mandats de surveillance, les transmettent aux opérateurs, après un examen formel, et s'assurent que les autorités reçoivent les données requises. Font également partie des tâches de la section la facturation aux autorités pénales et au SRC, et le versement des indemnités aux FST.

La section est aussi l'interlocuteur principal en cas de problèmes avec le système de traitement ou pour toute autre difficulté que rencontrent les utilisatrices et les utilisateurs. Elle accompagne le développement de nouvelles applications.

La Gestion de la surveillance est par ailleurs responsable des formations proposées aux utilisatrices et utilisateurs.

En dehors des heures de bureau, la Gestion de la surveillance assure un service de piquet opérationnel, avec un soutien technique fourni principalement par la section Provider Management. Le Service SCPT est ainsi joignable 24 heures sur 24.

Droit et contrôle de gestion

Les technologies de l'information et de la communication (TIC) sont une des branches les plus innovantes qui soient. De nouvelles normes sont régulièrement mises en place, des services nouveaux apparaissent en permanence, destinés à des équipements toujours plus puissants. Pour la surveillance des télécommunications, ce dynamisme n'est pas sans conséquences : l'interface technique entre le système de traitement du Service SCPT et les fournisseurs – plusieurs centaines – est soumise à une forte pression pour s'adapter en continu.

Les spécialistes de la section Droit et contrôle de gestion font en sorte, avec leurs col-

lègues de la section Provider Management, de garantir en tout temps la capacité de surveiller les télécommunications même dans un environnement technologique en constante évolution. Grâce à leur expertise, ces spécialistes soutiennent la planification et le pilotage de tous les projets informatiques critiques pour la mission du service.

L'équipe de 16 personnes veille non seulement à ce que les projets informatiques soient menés à bien de manière compétente, elle s'occupe aussi d'élaborer les bases légales nécessaires pour assurer la surveillance des télécommunications.

Dans de nombreux cas, il s'agit de reprendre au niveau d'une ordonnance l'évolution de la technique. L'ordonnance du département sur la mise en œuvre de la surveillance de la correspondance par poste et télécommunication (OME-SCPT), par exemple, est examinée périodiquement et, au besoin, adaptée.

La section Droit et contrôle de gestion s'occupe enfin de la conduite financière, des rapports et des relations publiques. L'équipe traite les demandes des médias et répond aux questions de la population.

Procédures de droit pénal administratif

La nouvelle LSCPT et ses ordonnances d'exécution ont donné de nouvelles tâches au Service SCPT, parmi lesquelles celle de diriger des procédures de droit pénal administratif. La responsable de ces procédures agit ici de manière indépendante, à la manière d'un ministère public.

Depuis mars 2018, le Service SCPT est donc habilité à agir contre les personnes qui ne remplissent pas leurs obligations légales en matière de surveillance de la correspondance par poste et télécommunication.

L'équipe de deux personnes de la section Procédures pénales administratives instruit les plaintes, établit les faits, procède à l'analyse juridique et sanctionne, s'il y a lieu, les contraventions. La direction de la procédure peut ordonner des mesures de contrainte telles que séquestres ou perquisitions, et mener des auditions.

Au terme d'une procédure, le Service SCPT rend un prononcé pénal, un mandat de répression ou une ordonnance de non-lieu.

Rétrospective

Janvier

Début du déploiement de SLDT pour les utilisateurs
La solution SLDT (*secure large data transfer*) permet de transférer électroniquement en toute sécurité d'importants volumes de données aux utilisateurs. On peut ainsi dans certains cas se passer d'envoyer par la poste des supports de données. Les premières organisations de police ont testé SLDT avec le Service SCPT. Au vu du succès de ces essais, l'accès est maintenant progressivement ouvert aux utilisateurs.

Février

Reprise des formations en présentiel et en petits groupes
Après une longue interruption pour cause de pandémie, les formations en présentiel ont repris. L'offre didactique en ligne développée dans l'intervalle sera non seulement maintenue, mais étoffée.

Mars

Entrée en vigueur des bases légales pour les fonctions d'analyse
Le 11 mars 2022, le Conseil fédéral a fixé au 1er mai 2022 l'entrée en vigueur des bases légales autorisant l'utilisation des fonctions d'analyse. Les art. 7 et 8 LSCPT permettent désormais explicitement d'analyser les données des surveillances dans le système de traitement du Service SCPT.

Avril

Web-série « La Suisse sous couverture »
Le 25 avril 2022, la RTS annonce la diffusion de la deuxième saison de sa web-série « La Suisse sous couverture » avec un épisode consacré au système de surveillance du Service SCPT. Ce court documentaire d'une douzaine de minutes est visible sous le lien suivant : https ://www.youtube.com/watch ?v=kfJ2lQ1aok8.

Mai

Proposition au Conseil fédéral « Surveillance des télécommunications : besoins supplémentaires en personnel et en moyens financiers pour le Service SCPT et le CSI-DFJP »
Le programme « Surveillance des télécommunications » (programme « FMÜ »)* a pour but de remplacer le système de traitement du Service SCPT et de le développer. Lancé en 2015, il s'achèvera en 2024. Le Service SCPT reprendra alors de l'organisation du programme des nouveaux composants et les tâches qui y sont associées. La proposition vise à assurer que le Service SCPT dispose des ressources nécessaires à cette fin. Le Conseil fédéral a examiné la proposition, et l'a acceptée, le 4 mai 2022.

Révision des ordonnances d'exécution (concernant en particulier la 5G)
La consultation lancée sur la révision partielle des quatre ordonnances d'exécution de la LSCPT s'est terminée le 23 mai 2022. Le Service SCPT a reçu 68 prises de position et retravaillé les projets sur la base des avis recueillis.

Juin

Entrée en vigueur de la loi fédérale sur les mesures policières de lutte contre le terrorisme
La loi fédérale sur les mesures policières de lutte contre le terrorisme (MPT) institue différentes mesures de police préventive. Elle est entrée en vigueur le 1er juin 2022 et modifie, entre autres actes, la LSCPT, avec notamment l'introduction d'un nouveau type de surveillance pour la localisation par téléphonie mobile dans le cadre des mesures en question.

Juillet

Première lettre d'information du Service SCPT aux autorités pénales
La première lettre d'information destinée aux utilisateurs du système de traitement du Service SCPT a été rédigée et diffusée en juillet 2022. Elle contient des informations pratiques sur le travail quotidien dans la surveillance des télécommunications. Il est prévu que cette lettre d'information paraisse deux fois par an.

* Pour plus d'informations: www.li.admin.ch > Thème > Programme «Surveillance des télécommunications»

Septembre

Préparation de la réorganisation du Service SCPT
Le Service SCPT a été chargé de mener une réorganisation dans le but d'optimiser l'exécution des tâches dans le cadre organisationnel actuellement défini par la loi. Une série d'ateliers ont été menés à ce sujet au cours du deuxième semestre 2022. La nouvelle organisation sera effective au 1er mai 2023.

Octobre

Enquête 2022 sur la satisfaction des clients
Tous les deux ans, le Service SCPT mesure le niveau de satisfaction des bénéficiaires de ses prestations. Les résultats montrent que cette satisfaction reste élevée. Sur une échelle de 1 (très insatisfait) à 6 (très satisfait), les valeurs suivantes ont été mesurées :
Satisfaction globale des autorités qui exploitent les données : progression de **4,7** à **4,9**
Satisfaction globale des autorités qui ordonnent les surveillances : progression de **4,6** à **4,9**
Satisfaction globale des autorités qui autorisent les surveillances : recul de **5,7** à **5,5**

Décembre

Ordonnance sur le financement de la surveillance de la correspondance par poste et télécommunication (OF-SCPT) : fin de la consultation des offices
Le projet d'ordonnance prévoit l'introduction de forfaits, dans le but de simplifier l'actuel système de financement et de facturation. Un autre objectif est d'augmenter le taux de couverture des coûts du Service SCPT. La consultation des offices s'est terminée le 28 novembre 2022. Une procédure de consultation a suivi au cours du premier semestre 2023. L'entrée en vigueur est prévue pour le 1er janvier 2024.

02

INFORMATIONS DE FOND

Mobile, flexible et compétente

Une équipe pour des interventions spéciales

Les petits fournisseurs de services de télécommunication, par exemple l'exploitant d'un réseau WLAN ou câblé local, peuvent demander à être exonérés de l'obligation légale d'assurer une disponibilité à surveiller. En cas d'activités suspectes sur leurs réseaux – et lorsqu'un juge a autorisé une surveillance – c'est l'équipe du Service SCPT chargée des cas spéciaux qui intervient.

Eichenweg 3, à Zollikofen, sur le site de l'administration fédérale. Deux membres de l'équipe des cas spéciaux remplissent des boîtes de transport avec des outils, des câbles, des prises et des composants électroniques. Ils utilisent le monte-charge pour amener le matériel au départ des livraisons.

Le chef de l'équipe les y attend déjà. Entretemps, une fourgonnette s'est approchée. Une fois le véhicule chargé, le film adhésif avec le logo de la Confédération suisse est retiré de la portière, et c'est parti. « Il ne faut pas qu'on puisse nous repérer de loin », explique l'homme au volant.

Son chef prend place sur le siège du passager. Il est un spécialiste internationalement reconnu dans le domaine de la *lawful interception*, la surveillance des télécommunications dans le cadre prévu par la loi. Ayant achevé des études d'informatique, il travaille ensuite pour des fournisseurs internationaux de télécommunication et des exploitants de réseaux. Après plusieurs missions en tant qu'expert externe de l'interception légale, il est recruté par le Service SCPT en 2012. Il dirige l'équipe depuis 2017.

Sa spécialité, c'est la conversion de données, qui est aussi au cœur des interventions de l'équipe des cas spéciaux : les données interceptées localement doivent être converties pour correspondre aux standards de l'Institut européen des normes de télécommunication (ETSI).

L'an dernier, quelque 10 000 mesures de surveillance ont été exécutées en Suisse, pour l'immense majorité d'entre elles dans les réseaux des grands fournisseurs de services de télécommunication (FST). La loi oblige les leaders du marché tels que Swisscom, Sunrise ou Salt à être en mesure d'intercepter des données de leurs réseaux et de les transférer dans le format prescrit vers le système de traitement du Service SCPT.

La loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) prévoit différentes catégories de personnes obligées de collaborer : celles qui doivent activement participer aux mesures et celles qui ne doivent que les tolérer. Cette distinction est guidée principalement par un souci de proportionnalité. Les PME qui ne sont pas concernées par un grand nombre de surveillances sont ainsi dispensées des investissements nécessaires. Elles n'ont pas besoin de développer leurs propres compétences en matière d'interception légale et doivent simplement tolérer qu'une surveillance soit exécutée. « C'est alors notre équipe des cas spéciaux qui fait le travail et assure la disponibilité à surveiller », explique Alexandre Suter, qui dirige la section Provider management au Service SCPT.

Il estime à plus de 1000 le nombre d'entreprises en Suisse qui peuvent être concernées par un cas spécial : de l'hôtel qui propose un accès WLAN gratuit à ses clients jusqu'au fournisseur

Une fois le cadre juridique clarifié, la discussion technique débute.

d'applications pour téléphones, en passant par les fournisseurs d'accès à internet.

Depuis l'entrée en vigueur de la LSCPT révisée en mars 2018, la section Provider management a exécuté des mandats pour des cas spéciaux dans près de 40 entreprises. Et chaque année, entre cinq et dix fournisseurs supplémentaires, ou plus exactement certains de leurs clients, se retrouvent dans le collimateur des autorités pénales.

« Notre travail commence par un appel au responsable désigné pour les interceptions légales chez le fournisseur concerné », raconte le chef d'équipe. Une fois que le contact est établi, les informations critiques sur les raccordements et les appareils concernés sont échangées via des courriels chiffrés.

Lorsque les conditions juridiques ont été clarifiées, l'équipe des cas spéciaux ouvre la discussion sur les aspects techniques de la mise en œuvre. Cette discussion peut être brève – si une surveillance a déjà été réalisée – ou plus longue, si c'est le premier cas spécial auprès du fournisseur en question.

Des problèmes peuvent se présenter avant tout en raison de la très forte hétérogénéité des infrastructures de télécommunication. Chaque fournisseur utilise le matériel et les logiciels de son choix. Il n'est pas rare non plus que plusieurs générations de systèmes tournent en parallèle. L'équipe doit être prête à faire face à d'innombrables combinaisons de types de raccordements, de connecteurs et de protocoles. « Une fois », se rappelle le chef d'équipe, « un composant réseau dont nous avions absolument besoin n'était plus disponible qu'en Espagne ».

La fourgonnette est arrivée à sa destination, un centre de données dans la banlieue de

Zurich. Un collaborateur ouvre la porte. Dehors, le soleil brille. À l'intérieur, les baies de serveurs informatiques clignotent, quelques plafonniers dispensent une lumière blafarde. On entend le bourdonnement des serveurs et le chuintement des systèmes de refroidissement.

« Depuis quelques années, les conversations téléphoniques et le trafic de données passent quasiment toujours par le cloud », explique le chef d'équipe. Lorsqu'il existe des ressources d'adressage claires pour une personne suspecte, les interventions de l'équipe chargée des cas spéciaux se déroulent donc principalement dans des centres de données comme celui-ci. Le chemin ne mène vraiment sur le terrain – par exemple dans les locaux d'un câblo-opérateur local – que si des raisons techniques rendent nécessaire la proximité avec la cible.

L'équipe se trouve une place entre les serveurs et s'installe. Elle a amené elle-même l'équipement de base nécessaire à la surveillance. Les fabricants auxquels elle l'achète fournissent aussi

les autorités pénales et les services de renseignements d'autres pays. Il arrive cependant que ces outils standards atteignent leurs limites. L'opération se poursuit alors sur deux fronts :

Pendant qu'une partie de l'équipe met en place la surveillance sur place, les collègues restés au bureau développent une solution logicielle spécifique pour le cas. Dès que le serveur est en ligne, des tests de connectivité sont lancés. D'éventuelles modifications logicielles peuvent ainsi être chargées jusqu'à la dernière minute.

Des modifications logicielles peuvent être chargées jusqu'à la dernière minute.

En arrière-plan, un spécialiste du fournisseur se tient à disposition. Il répond aux questions qui surviennent durant l'intervention. « Normalement, la collaboration se passe bien », dit le chef d'équipe. Mais les exceptions confirment la règle. Il arrive par exemple qu'un fournisseur oppose une résistance passive et veuille consulter un avocat avant de laisser les collaborateurs du Service SCPT faire leur travail. Dans de très rares cas – lorsqu'un fournisseur entend empêcher physiquement l'accès à son infrastructure – le Provider management du Service SCPT est obligé de demander le soutien des forces de l'ordre.

Les motivations des fournisseurs récalcitrants sont souvent peu claires. D'autant plus que les fournisseurs soupçonnés par les autorités pénales d'être de mèche avec les cibles ne sont pas contactés. « Dans ce genre de situations », indique le chef de l'équipe des cas spéciaux, « nous approchons la cible par des voies détournées ». Il ne révèle pas ce qui se passe concrètement lorsqu'un accès direct à l'infrastructure d'un fournisseur d'accès est interdit. « Mais il est clair que nous trouvons toujours un moyen ».

Les interventions de l'équipe des cas spéciaux concernent le plus souvent des surveillances en temps réel. Pour l'équipe, cela veut dire que son travail est terminé quand les données de communication peuvent être transmises au fur et à mesure, sans délai et sans interférences, au système de traitement du Service SCPT.

Vers 15 h 00, c'est fait. L'équipe remballe son matériel et le recharge dans la fourgonnette. Seule une boîte d'apparence banale reste chez le fournisseur d'accès. C'est le serveur des cas spéciaux, qui intercepte les conversations et les échanges de données de la personne suspecte.

C'est maintenant aux enquêteurs et aux procureurs compétents de jouer.

Le grand chantier

Le composant pour la surveillance en temps réel du système de traitement du Service SCPT doit être remplacé. Les travaux de réalisation du Federal Lawful Interception Core Component (FLICC) ont débuté à l'été 2021.

Lorsque le procureur général Urs Hubmann combine les lettres CIO, ce n'est pas pour parler du Comité international olympique, mais du crime organisé italien. « C'est actuellement l'une des plus grandes menaces à notre sécurité intérieure », dit-il.

Ce juriste de 65 ans dirige depuis 2011 le ministère public II (STA II) du canton de Zurich, qui s'occupe principalement des infractions poursuivies sur la base de soupçons, et non suite au dépôt d'une plainte. L'objectif est de créer, au moyen de mesures de contrainte secrètes, une base de preuves qui permette de traduire en justice les suspects.

« La criminalité organisée italienne est actuellement une des plus grandes menaces pour notre sécurité intérieure. »

Urs Hubmann, procureur général, canton de Zurich

Brigandage aggravé, trafic de stupéfiants et traite d'êtres humains

L'attention se concentre sur les cas de criminalité organisée et de grand banditisme. La palette des infractions va du brigandage aggravé à la cybercriminalité qualifiée, en passant par le trafic de stupéfiants, la traite des êtres humains et les cas graves de blanchiment d'argent.

Pour enquêter, le STA II dispose d'une boîte à outils bien garnie. Outre les recherches secrètes, l'analyse de transactions financières, le placement de microphones et de caméras, il y a aussi l'interception légale (*Lawful interception*, LI), c'est-à-dire la surveillance des télécommunications, en temps réel ou rétroactivement, dans les limites fixées par la loi.

La surveillance en temps réel permet aux enquêteurs de suivre les déplacements de la cible et les échanges qu'elle a avec ses interlocuteurs. En 2022, le STA II du canton de Zurich a ordonné plus de 200 surveillances en temps réel, environ 20 pour cent du total pour la Suisse.

Du point de vue technique, les surveillances passent par l'*Interception System Schweiz* (ISS), le composant pour la surveillance en temps réel du système de traitement du Service SCPT. « Cette plateforme a été acquise en 2013 et elle a pris un coup de vieux », explique Ernesto Ruggiano. Chef de projet au Service SCPT, il est chargé de piloter le remplacement d'ISS par le nouveau *Federal Lawful Interception Core Component* (FLICC). Le projet a été lancé il y a cinq ans et la phase de réalisation a commencé en été 2021.

Le STA II attend la mise en service de FLICC avec une grande impatience, nourrie principalement par l'évolution des technologies dans l'industrie des télécommunications. ISS n'a tout simplement pas été conçu pour surveiller des télécommunications telles qu'elles se font aujourd'hui – on pense en particulier à la 5G. « L'analyse d'une seule session de surveillance, par exemple d'un bref appel téléphonique, demande beaucoup d'efforts et de temps », explique Urs Hubmann.

À ces difficultés s'ajoute un changement des comportements de communication. Les criminels échangent aussi beaucoup de banalités. Les enquêteurs font face à une quantité énorme de données.

La surveillance en temps réel de communications vocales et de messages textes devrait être disponible à partir du milieu de l'année 2023. Par la suite, il est prévu d'intégrer la surveillance des données internet et des courriels. Enfin, il faudra s'occuper de ce que l'on pourrait appeler l'aménagement intérieur : l'intégration de fonctions plus avancées.

Visualisation et transcription automatique

Par exemple, une visualisation claire des résultats de la surveillance. Ou une transcription automatique des messages vocaux avec option de traduction. Ou encore l'évaluation de localisations plus précises des appareils surveillés. « Avec FLICC, nous faisons de la surveillance en temps réel un outil d'enquête moderne, efficient et simple à utiliser », se réjouit Ernesto Ruggiano.

Entre 2016 et 2022, le nombre de surveillances en temps réel réalisées en Suisse a diminué de 2800 à un peu plus de 1200. Cette diminution s'explique notamment par le fait que les procédures dans lesquelles une surveillance en temps réel peut être un moyen de preuve deviennent toujours plus complexes et nécessitent de plus en plus souvent des connaissances spéciales. Voilà qui devrait changer avec FLICC.

« Nous faisons de la surveillance en temps réel un outil d'enquête moderne et efficient. »

Ernesto Ruggiano, responsable du projet FLICC, Service SCPT

Le maintien d'une pression policière élevée – les experts sont unanimes sur ce point – empêche le crime organisé et le grand banditisme de prendre pied dans la société. La poursuite systématique des infractions en question empêche notamment les bandes de régler leurs conflits dans l'espace public, avec les risques que ce genre d'altercations violentes présente pour des personnes qui se trouveraient au mauvais endroit au mauvais moment.

« Des excès de violence sur la voie publique sont des phénomènes qu'à ce jour, nous connaissons surtout de l'étranger », commente Urs Hubmann, « nous devons absolument veiller à ce que cela reste ainsi ».

« La Suisse est un objectif intéressant. »

Sur la piste des espions, des terroristes et des cybercriminels: Jürg Bühler est directeur suppléant au Service de renseignement de la Confédération*

Êtes-vous un avide lecteur de journaux, Monsieur Bühler ?
À titre personnel, pas vraiment. Mais tous les contenus publiés par des journaux suisses ou étrangers peuvent comporter des informations potentiellement instructives pour un service de renseignement. Nous parlons dans ce cas d'informations « open-source », que le SRC collecte et évalue systématiquement. J'ai ainsi une bonne vue d'ensemble des nouvelles les plus importantes.

Quelles sont les autres sources dont le Service de renseignement de la Confédération (SRC) tire ses informations ?
Elles sont nombreuses. Nous avons ainsi la possibilité d'obtenir des informations utiles auprès de tous les services administratifs de la Confédération et des cantons. Et via la collaboration avec les cantons, nous avons aussi accès aux services des communes.

Tout ça n'est pas encore très palpitant …
Nous travaillons ensuite avec de l'intelligence humaine, c'est-à-dire des sources recrutées par nos officiers traitants. Ceux-ci entretiennent des contacts avec des personnes qui ont accès à des informations importantes pour la mission du SRC. Ces officiers traitants correspondent tout à fait à l'image que le public a d'un « agent secret ». Nos autres sources d'information sont enfin les services partenaires étrangers et les services de renseignement des cantons.

Combien d'officiers traitants le SRC emploie-t-il ?
Ça, c'est une information que nous ne donnons qu'à notre organe de surveillance.

Le pendant de l'intelligence humaine est le renseignement d'origine électromagnétique. De quoi s'agit-il exactement ?
Il s'agit d'interpréter des signaux générés par des dispositifs techniques, en général par des équipements de communication : par exemple l'exploration radio de signaux émis à partir de l'étranger ou par des satellites, ou l'exploration du réseau câblé. Nous pouvons dans certaines conditions écouter des flux de données transfrontaliers et les filtrer en fonction de critères de recherche correspondant à nos mandats légaux, notamment en fonction de certains noms, projets ou ressources d'adressage de télécommunication telles que des numéros de téléphone.

* L'entretien avec Jürg Bühler a été réalisé en décembre 2021, avant le début de la guerre en Ukraine.

Voilà qui nous amène au thème de l'interception légale et au Service SCPT. Quelle est l'importance de la surveillance des télécommunications pour le travail du Service de renseignement ?
Elle nous permet d'obtenir des renseignements que nous ne pourrions pas avoir autrement. En 2022, le SRC a mené deux opérations pour lesquelles il a eu recours à ce type de mesures de recherche soumises à autorisation. Une dans le domaine de la lutte contre le terrorisme et l'autre concernant des activités de renseignement interdites.

Plus de 10 250 mesures de surveillance des télécommunications ont été exécutées en Suisse en 2022, dont 95 seulement ont été ordonnées par le SRC. Pourquoi si peu ?
Les conditions légales que le SRC doit respecter pour recourir à des mesures de surveillance sont très strictes. S'il veut ordonner une mesure d'interception légale, le SRC doit d'abord en faire la demande au Tribunal administratif fédéral. Si celui-ci donne son accord, il nous faut ensuite l'aval de la cheffe du DDPS, qui doit au préalable consulter ses homologues du DFAE et du DFJP. Ce n'est qu'une fois que la cheffe du DDPS a donné son feu vert que nous pouvons lancer la mesure.

Un des pères fondateurs du Service SCPT

Jürg Bühler fait partie de la direction du Service de renseignement de la Confédération (SRC) depuis sa fondation en 2010. Ses activités pour la Confédération dans le domaine de la police et du renseignement remontent aux années 1990. Il se rappelle encore comment fonctionnait la surveillance des télécommunications à l'époque du monopole des PTT, avec des opérations décentralisées dans les directions d'arrondissement des télécommunications : « c'étaient le plus souvent des femmes spécialement formées qui s'en occupaient. Casque sur les oreilles, elles écoutaient et notaient les échanges pertinents. » La libéralisation du secteur des télécommunications a placé le législateur devant un double défi : il devait d'abord définir quelles seraient les obligations des fournisseurs, désormais privés, en matière de surveillance, puis créer un service qui serait chargé de cette tâche régalienne en toute neutralité par rapport à ces fournisseurs. Âgé aujourd'hui de 58 ans, Jürg Bühler dirigeait à l'époque les enquêtes judiciaires à la police fédérale : « dans un groupe de travail national, nous avons élaboré, avec le service juridique des PTT, des propositions pour un service de surveillance géré par la Confédération ». C'est ainsi qu'est né le Service des tâches spéciales (STS), qui est entré en activité le 1er janvier 1998. Exactement dix ans plus tard, le STS a été transféré du DETEC au DFJP, où il a pris sa nouvelle appellation de Service SCPT.

« Les cyberattaques qualifiées sont quasiment toujours transfrontalières. »

Jürg Bühler, directeur suppléant du SRC

Même si vous soupçonnez que la sécurité nationale de la Suisse est menacée ?
Cette condition est de toute façon nécessaire pour pouvoir mettre en œuvre de telles mesures. Suite à l'affaire des fiches, dans les années 1990, le législateur a volontairement restreint la marge de manœuvre du service de renseignement de l'époque à l'intérieur du pays. Jusqu'à l'entrée en vigueur de la loi sur le renseignement, en septembre 2017, nous n'avions pas le droit de procéder à des surveillances des télécommunications en Suisse. Depuis, nous faisons usage de cette possibilité, mais nettement moins fréquemment que ne le craignaient à l'époque les opposants à la loi, comme le montrent les statistiques que nous publions chaque année.

Le contre-espionnage fait partie des principales missions du SRC. Qui fait de l'espionnage en Suisse ?
Nous estimons le nombre d'agents de services secrets étrangers qui séjournent durablement en Suisse à plusieurs milliers. Dans les représentations diplomatiques de certains pays – je ne vous dirai pas lesquels – près d'un quart des collaborateurs sont chargés de tâches liées au renseignement.

La Suisse est-elle si importante pour les puissances étrangères ?
La Suisse est une nation technologiquement très avancée. À ce titre, elle présente un grand intérêt pour l'espionnage industriel. On a aussi Genève, qui accueille un grand nombre d'agences de l'ONU. En tant qu'État abritant le siège d'organisations internationales, nous avons une responsabilité d'empêcher les activités d'espionnage politique contre des tiers sur notre territoire. Concrètement, le SRC collecte et évalue aussi des informations qui permettent de conclure qu'un gouvernement agit en Suisse contre des organisations non gouvernementales, des minorités ethniques ou des groupes d'opposition.

Venons-en à la lutte contre le terrorisme, à l'origine de trois mesures de surveillance des télécommunications sur quatre l'an dernier. Quelle est la priorité du SRC ?
En ce moment, l'« État islamique ».

De quel groupe de personnes le danger émane-t-il ?
En Suisse, la menace vient, d'une part, de personnes qui se radicalisent ici au contact de la propagande djihadiste ou par des contacts dans leur entourage. De plus en plus souvent, cependant, la radicalisation et la propension à la violence sont liées à des crises personnelles ou des problèmes psychiques. Ces personnes sont suscep-

tibles de commettre des attentats spontanés, principalement sur des cibles faciles. Mais les plus dangereux sont les terroristes arrivant de l'étranger avec des ordres de mission pour des attentats ciblés. Et nous voyons que ces deux groupes peuvent parfois coopérer : ceux qui arrivent de l'étranger recrutent des novices locaux et tentent de les former.

La menace de sécurité la plus présente dans l'opinion publique est celle d'une cyberattaque visant des infrastructures publiques, un hôpital ou la distribution d'électricité par exemple. Selon vos informations, cette menace est-elle réelle ?

Le nombre d'attaques utilisant des ordinateurs contre des cibles militaires ou civiles augmente constamment dans le monde. Elles représentent une menace considérable pour la Suisse aussi, qui a une infrastructure numérique très développée.

Le SRC est-il prêt à faire face à cette menace venant du cyberespace ?

Notre unité Cyber a pour mandat de déceler à temps et de prévenir les attaques visant des systèmes informatiques d'infrastructures critiques. Il faut cependant voir que la base légale de notre activité est entrée en vigueur il y a plus de cinq ans. Lors des débats au Parlement en amont de la votation populaire de l'automne 2016, la menace provenant du cyberespace paraissait encore peu importante. Le Parlement et le peuple ont donné une priorité élevée à la protection de la sphère privée. Nous devons donc être en mesure de montrer que la sécurité nationale est gravement et directement menacée avant de pouvoir surveiller des activités suspectes au moyen de GovWares ou avec le concours du Service SCPT. Mais c'est précisément ce point qui pose problème.

Pourquoi ?

Parce que les attaques qualifiées sont quasiment toujours transfrontalières. La cible finale d'une cyberattaque se situe pratiquement toujours au-delà des frontières nationales. Cela signifie que les cyberattaques qui utilisent abusivement des infrastructures en Suisse sont dirigées contre des systèmes à l'étranger. Elles ne représentent donc pas une menace directe contre la Suisse au sens de la loi. Du point de vue de la défense, il est néanmoins important d'élucider ces attaques, afin de mieux en protéger la Suisse.

Comment les services de renseignement de nos voisins traitent-ils les attaques transfrontalières ?

Les pays qui nous entourent sont des États de droit, qui ont une conception tout aussi stricte de la notion de « menace pour la sécurité nationale ». Ils n'ont donc eux non plus pas toujours de bases légales leur permettant de déjouer de possibles actes préparatoires d'attaques sur des cibles en Suisse. Il s'agit d'un problème structurel que les attaquants peuvent exploiter. Il doit donc être réglé au niveau national comme au niveau international.

La Suisse a-t-elle déjà entrepris des démarches dans ce but ?

La loi sur le renseignement est en cours de révision. Il est prévu d'inclure la menace contre d'importants intérêts de sécurité internationaux comme motif permettant le recours à des mesures de recherche soumises à autorisation. Nous aurions alors aussi davantage de possibilités dans le domaine cyber.

03

FAITS ET CHIFFRES

Motifs de surveillance

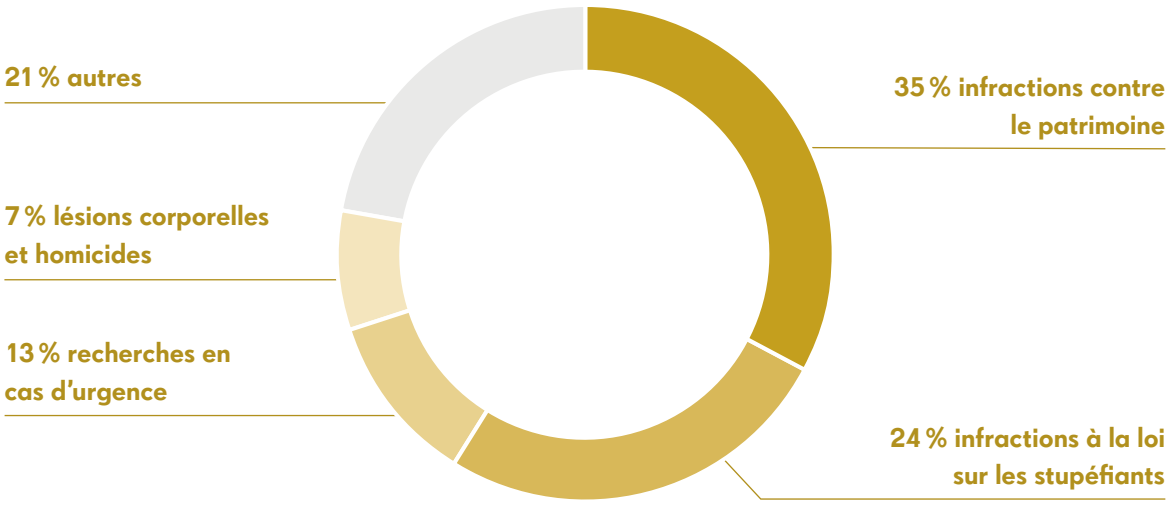
Selon la statistique policière de la criminalité, 549 404 infractions ont été signalées en Suisse en 2022. Une mesure de surveillance des télécommunications a été ordonnée dans 10 253 cas, ce qui signifie que le recours à cette mesure est relativement rare.

Il convient encore de relever qu'une infraction, ou une mesure de recherche soumise à autorisation, peut donner lieu à plusieurs mesures de surveillance, par exemple en surveillant le raccordement fixe et plusieurs raccordements mobiles d'un suspect. De plus, un même numéro de téléphone mobile fait fréquemment l'objet de mesures de surveillance auprès de différentes personnes obligées de collaborer, afin de couvrir tous les cas d'itinérance. Le nombre de personnes concernées par une mesure de surveillance est donc considérablement moins élevé que le nombre de mesures.

Les surveillances le plus souvent ordonnées sont celles liées aux infractions contre le patrimoine (35 %). En deuxième place, avec 24 %, on trouve les infractions à la loi sur les stupéfiants. Au quatrième rang (7 %) suivent les infractions contre la vie et l'intégrité corporelle.

Une surveillance des télécommunications peut aussi être ordonnée pour retrouver une personne disparue. Les recherches en cas d'urgence se trouvent à la troisième place, avec un total de 13 %.

Vous trouverez de plus amples informations sur les statistiques du Service SCPT à l'adresse : **www.li.admin.ch / fr / stats**



Définitions et nombre de mesures de surveillance et types de renseignements

Surveillance en temps réel (1)
Dans le cas d'une surveillance en temps réel, les données de la correspondance par poste ou télécommunication sont transmises aux autorités de poursuite pénale via le système de traitement de manière simultanée, légèrement différée ou périodique.

Surveillance rétroactive (2)
Une surveillance rétroactive collecte avant tout les données de connexion permettant par exemple de savoir qui a téléphoné à qui, quand, où et la durée de l'appel.

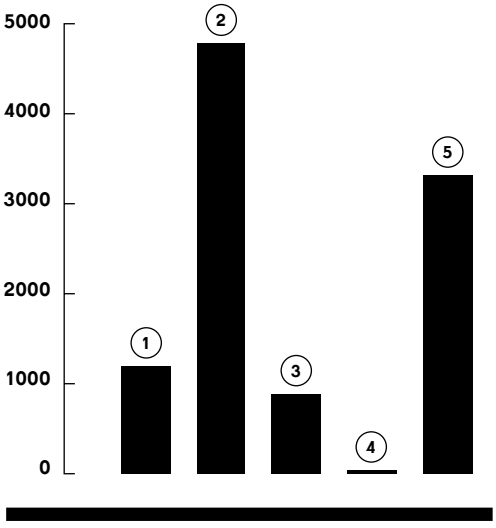
Recherche en cas d'urgence (3)
Une recherche en cas d'urgence est ordonnée par exemple pour retrouver et secourir un randonneur accidenté ou un enfant disparu.

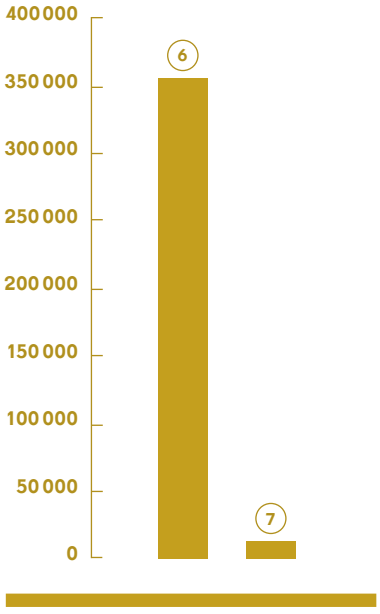
Recherche de personnes condamnées (4)
La recherche de fugitifs permet aux autorités de poursuite pénale de retrouver la trace de personnes condamnées à une peine privative de liberté ou qui font l'objet d'une mesure entraînant une privation de liberté, sur la base d'un jugement définitif et exécutoire.

Recherche par champ d'antennes (5)
Une recherche par champ d'antennes concerne une cellule de téléphonie mobile ou un point d'accès public au réseau WLAN. Les données transmises couvrent toutes les communications, les tentatives d'établissement d'une communication et les accès au réseau pendant une période déterminée.

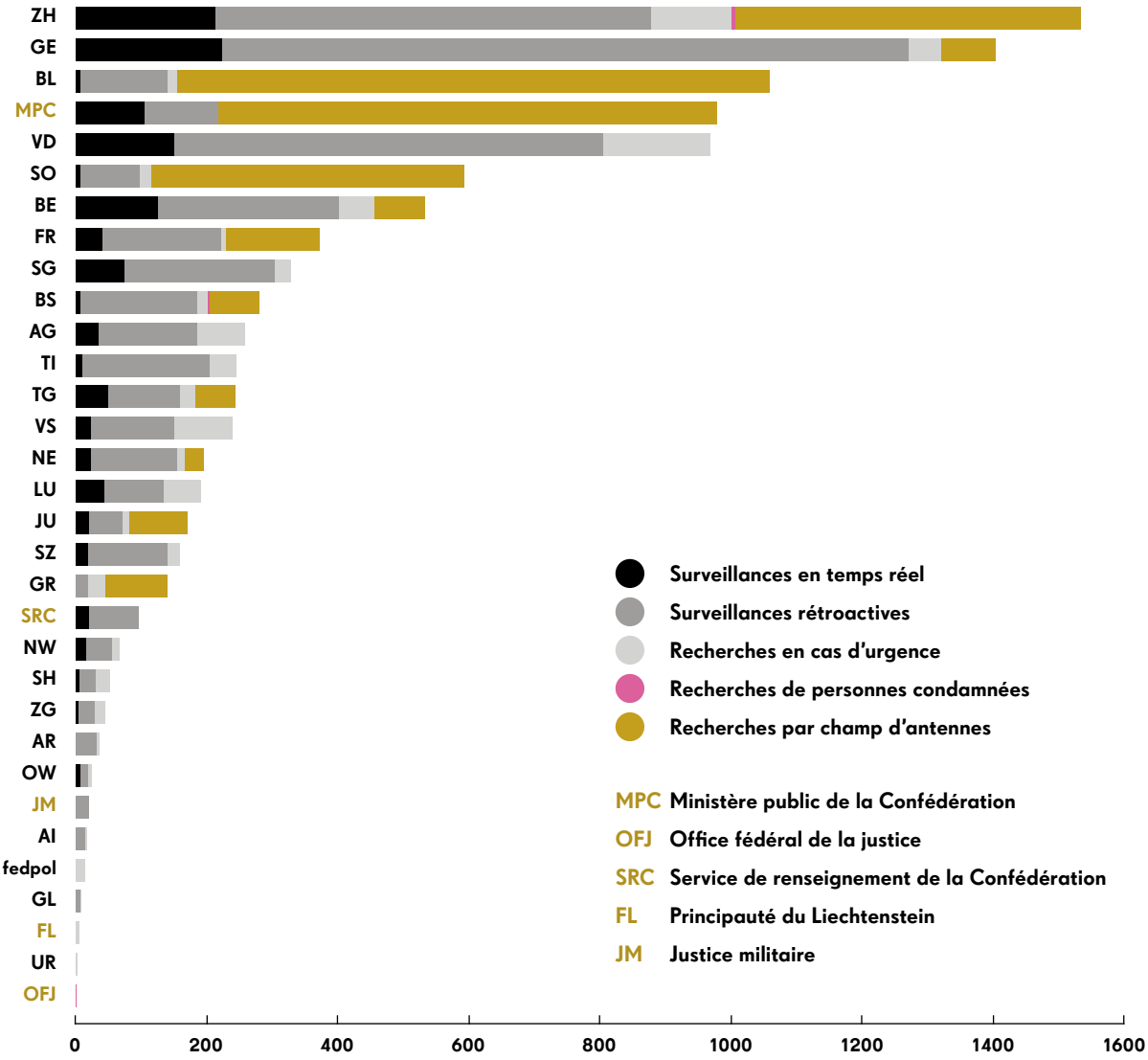
Renseignements simples (6)
Les renseignements simples sont des informations de base sur les raccordements téléphoniques, permettant en particulier de savoir à quel abonné un numéro de téléphone ou une adresse IP est attribué.

Renseignements complexes (7)
Les renseignements complexes permettent d'obtenir des informations plus détaillées concernant des raccordements de télécommunication telles que des copies de contrats ou de pièces d'identité.





Mandats pour la Confédération, les cantons et le Liechtenstein

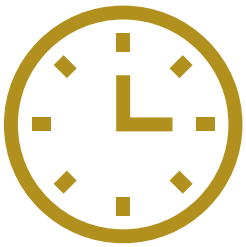


Mandats de surveillance de l'Office fédéral de la justice
La loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) ne prévoit pas seulement des surveillances pour les procédures pénales qui sont en cours dans le pays. Des mesures de ce type peuvent également être prises lors de l'exécution d'une demande d'entraide judiciaire présentée par des autorités étrangères. L'Office fédéral de la justice (OFJ) est compétent pour les cas d'entraide judiciaire.

Nombre de demandes de citoyens

24

Nombre d'interventions du service de piquet



870

Utilisateurs enregistrés système de traitement

WMC 2400
Warrant Management Component (gestion des mesures de surveillance)

IRC 4300
Information Request Component (renseignements)

RDC 2200
Retained Data Component (surveillances rétroactives)

ISS 2450
Interception System Schweiz (surveillances en temps réel)

Nombre de cas spéciaux

83

(voir p. 8 / 9, Provider Management ainsi que pp. 15 – 19 « Une équipe pour des interventions spéciales »)

Compte de résultats du Service SCPT, en millions de CHF

Total des revenus
12,4

Total des charges
31,7

Contribution de la Confédération à la couverture des coûts
19,3

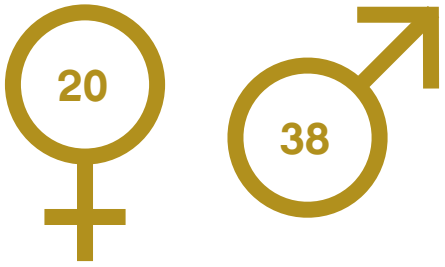
Nombre de demandes de médias

21

Nombre de collaborateurs

58

Proportion de femmes et d'hommes



Âge moyen

46,5

Répartition linguistique

67 % Allemand

6,4 % Italien

24,5 % Français

2,1 % Autres

Tranches d'âge

20 à 29 ans
10 %

30 à 39 ans
19 %

40 à 49 ans
26 %

50 à 59 ans
40 %

60 à 69 ans
5 %

« Le travail proprement dit, à savoir l'établissement de la capacité à mener une surveillance, est effectué par notre équipe des cas spéciaux. »

Alexandre Suter, chef de la section Provider management

Impressum

Conception : Service SCPT
Rédaction : Service SCPT
Collaboration :
bureau des journalistes JNB, Lucerne
Design et réalisation : Schön & Berger, Zurich
Impression : Druckerei Ruch, Ittigen
Photos : Lia Lüthi, Barbara Hesse, David Kelly
Polices : Minion Pro, Drescher Grotesk
Papier : Z-Offset
Versions linguistiques : allemand,
français, italien et anglais

■

Pour faciliter la lisibilité et la compréhension, nous essayons de ne pas utiliser une terminologie technique ou juridique trop complexe. Des formulations neutres sont utilisées lorsque c'est possible, mais il va de soi que les désignations de personnes au masculin ou au féminin incluent aussi bien les femmes que les hommes.

Département fédéral de justice et police DFJP
Service Surveillance de la correspondance par poste et télécommunication SCPT
3003 Berne