



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation

Federal Department of Justice and Police FDJP
Post and Telecommunications Surveillance Service PTSS

Annual Report PTSS 2018

■
The mobile network is by far the most monitored. It is not just the content of communications that is monitored. Traffic and connection data (also referred to as 'communications data'), automatically generated by telecommunications, are also important for prosecution: for example, information such as who called, texted or emailed whom. This data can be used, for example, to identify relationship networks in cases of human or drug trafficking. Every mobile phone automatically connects to the nearest cell tower, making it possible to use mobile communications.



www.li.admin.ch/en/stats



01**INTRODUCTION**

- 5 Shedding light on our secret work
- 6–7 Review of 2018 – The highlights

02**PTSS**

- 9–10 The PTSS
- 11–15 4 Divisions
- 16–17 Special case

03**HOW SURVEILLANCE WORKS**

- 19 Surveillance for the purpose of prosecution
- 20 Parties involved
- 21 How surveillance works
- 22–23 Surveillance measures 2018 in figures
- 24–25 Definition and number of surveillance measures

04**EMERGENCY SEARCH**

- 27–30 Emergency search

05**LEGAL ASPECTS**

- 32–33 A new legal framework

06**TECHNOLOGIES AND SYSTEMS**

- 35 Technologies and systems
- 36–38 The Telecommunications Surveillance Programme

07**FACTS AND FIGURES**

- 40–41 Facts and figures

08**OUTLOOK**

- 43–44 2019

01

INTRODUCTION

Shedding light on our secret work

It's a familiar feeling: you hear a word and instantly a stream of thoughts and images runs through your mind. For instance, the term 'compulsory measures' immediately conjures up images of searches, seizure or pre-trial detention, evoking feelings of unease, possibly even curiosity. The scenes playing out in our minds are like those of a crime film: it's quite normal for the imagination to run wild.

However, when it comes to the Post and Telecommunications Surveillance Service (PTSS), the imagination is of little use: the abstract concepts that we juggle on a daily basis elicit the same reaction in most people, namely a big question mark. For example, what do 'real-time surveillance', 'incidents', 'communications data' or 'special case' mean to you? In all likelihood, very little. And with good reason: the PTSS operates in an abstract world. We conduct post and telecommunications surveillance by order of the prosecution authorities. These so-called 'covert surveillance activities', as the name suggests, are conducted in secret. The persons concerned are unaware that their mobile phone, internet connection or email account are being monitored.

These measures are often used in large, complex criminal proceedings and have become indispensable. They are employed, for example, to catch suspects red-handed, committing a crime while being monitored by the prosecution authorities. They can also be used retrospectively to provide important evidence of guilt or innocence.

The use of covert surveillance is limited to serious offences. This is because it represents a considerable encroachment on the right to privacy of the individuals concerned. In order to ensure that the intervention remains proportionate, surveillance may only be conducted for certain serious offences or, for example, in the search for missing persons or escaped prisoners. The authority to issue orders rests, in particular, with public prosecutors and the Federal Intelligence Service.

This first annual report seeks to shed light on our daily work and explain some abstract terms that conceal a raft of exciting activities.

Review of 2018 – The highlights

Today everybody writes emails, communicates via apps, surfs public networks and pays for clothes ordered online by credit card. There is no doubt about it: we are moving increasingly towards a digital society.

This shift places new demands on security and affects the very core of our work. Telephone tapping alone is by no means enough: criminals are savvy when it comes to technical equipment and exploit digital loopholes.

The implementation of the revised Federal Act on Post and Telecommunications Surveillance (APTS) in 2018 created the necessary framework in order to adapt telecommunications surveillance methods to modern means of communication. To us, this was undoubtedly a milestone in 2018.

In our annual report, however, we shall also give you a behind-the-scenes look at our day-to-day work at the PTSS. We shall present the PTSS structure as well as our activities and the issues and challenges we face on a daily basis. We shall also explain what ‘telecommunications surveillance for the purpose of prosecution’ actually means.

Using an example of deployment of the Provider Management team, we shall illustrate how teamwork and being prepared for unexpected technological challenges can be decisive for the success of a surveillance operation. Did you know that, in specific cases, telecommunications surveillance measures can also be implemented outside of criminal proceedings? They can also be used for so-called emergency searches and tracing operations: here, technology is used to trace missing persons such as hikers involved in accidents or missing children or to track down escaped prisoners. Around 5,000 reports of missing persons are received in Switzerland every year – almost 14 a day!

What do you do if a 10-year-old boy suddenly goes missing? The Zurich cantonal police explains how the police proceeds in such cases by way of an example. In an interview, the special task force police officer explains when he is called in in such cases and how it is decided when to deploy a search dog or a helicopter or even to launch an emergency search.

We shall also address controversial issues such as the debate that has been ongoing since the service was set up, namely that concerning the fees charged and the related issue of the financing of the PTSS. The debate, conducted in the relevant bodies and in the working group set up for this purpose, has been intense and constructive in recent months.

Finally, I would like to thank the federal and cantonal prosecution authorities, the Federal Intelligence Service, the chairpersons and members of the bodies and committees involved, the persons required to cooperate, and our partners involved in providing and maintaining the necessary IT and telecommunications infrastructures for their excellent cooperation, as well as the staff of the PTSS for their tireless work.

I wish you an enlightening and stimulating read.



René Koch, Head of PTSS

■ For the sake of greater clarity and readability, technical and legal jargon has been kept to a minimum, and, wherever possible, gender-neutral language has been used. Any references to persons in the masculine or feminine form only shall refer equally to men and women.

„We shall
also address
controversial
issues.“

René Koch, head of PTSS

02

PTSS

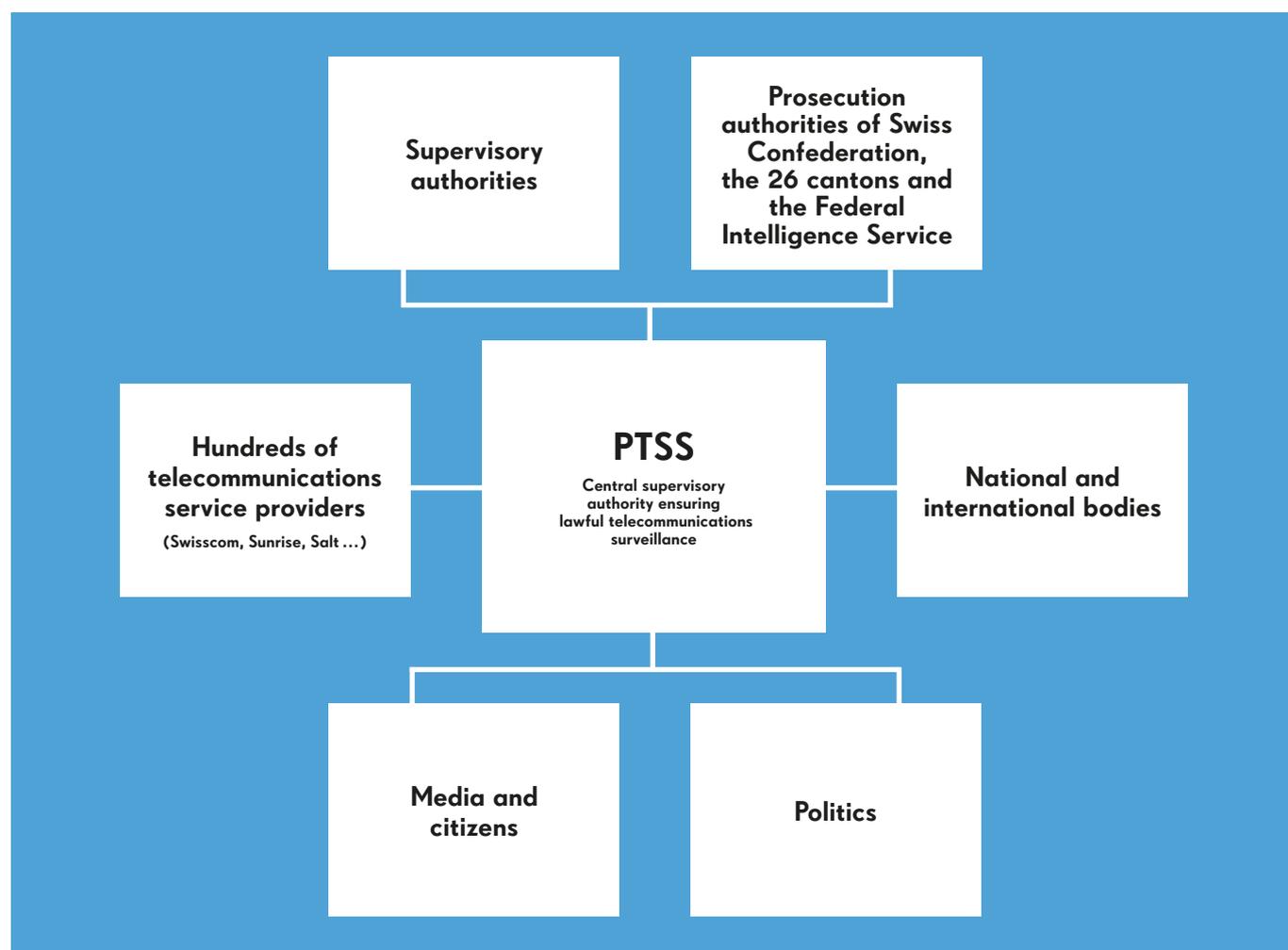
PTSS

The Post and Telecommunications Surveillance Service (PTSS) is responsible for monitoring post and telecommunications in Switzerland. It acts independently and autonomously and is not bound by instructions. For administrative purposes, the PTSS reports to the Federal Department of Justice and Police (FDJP).

Lawful execution of post and telecommunications surveillance under the rule of law is indispensable in order to protect the privacy of the population. The PTSS ensures compliance with the applicable regulations, acting as a central interface between the authorities and the telecommunications service providers.



Definition: Telecommunications service providers are for example mobile communications, telephone or internet access providers such as Swisscom, Sunrise or Salt.



The main duty of the PTSS is to implement surveillance measures by order of the prosecution authorities. Previously, its main ‘clients’ were the public prosecutors of the 26 cantons and the Office of the Attorney General of Switzerland. In September 2017, its client base expanded to include the Federal Intelligence Service.

As part of its surveillance activities, the PTSS collects data from telecommunications service providers that the prosecution authorities have requested for the purpose of solving serious crimes. The authorities may order emergency searches to locate missing persons. Within this context, mobile phones – which the police can locate via the PTSS – can save lives.

Another important task of the PTSS is to provide technical and legal advice to the prosecution authorities and telecommunications service providers on all matters relating to post and telecommunications surveillance.

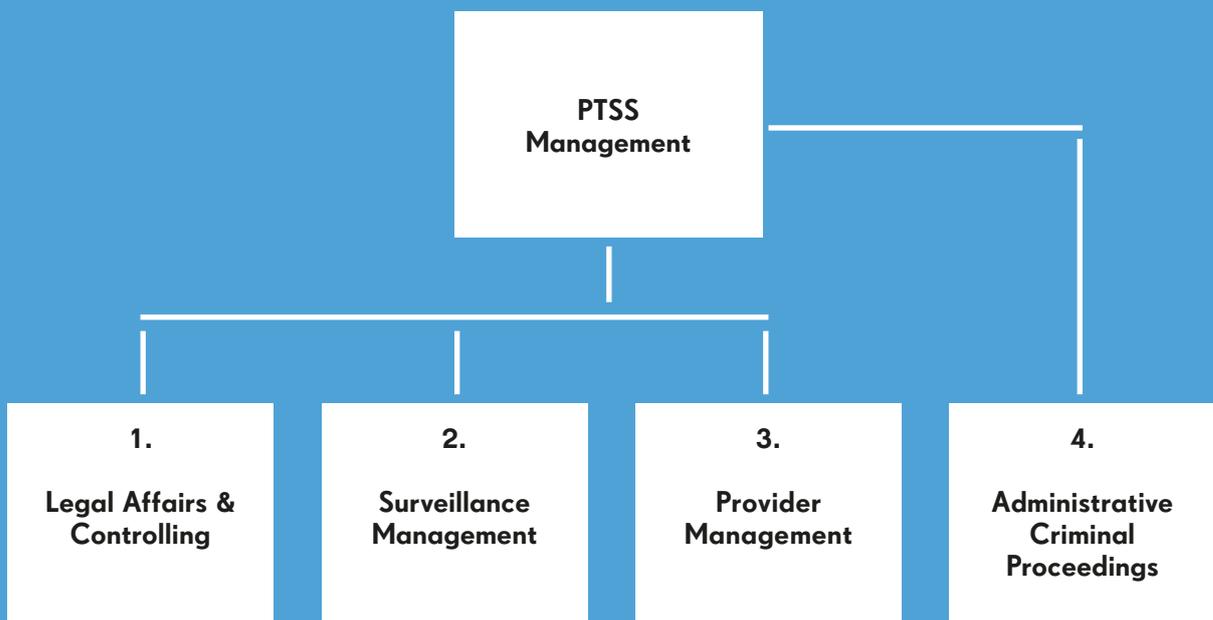
The PTSS is involved in various national and international bodies and works together with various authorities to execute its statutory mandate in accordance with the Federal Act on Post and Telecommunications Surveillance (APTS).

Since crime and modern telecommunications know no geographical boundaries, transnational exchanges and effective international cooperation are essential. Only that way can we exchange technical knowledge and influence international standardisation.

With the new APTS and the associated implementation ordinances of March 2018, Switzerland received a clear, up-to-date legal framework in order to monitor post and telecommunications services. At the same time, the PTSS was given additional responsibilities. As a result, it has created the new Administrative Criminal Proceedings division. This division conducts administrative criminal proceedings against persons who fail to fulfil their legal obligations in connection with the surveillance of post and telecommunications. These include, for example, proceedings against sellers who, when selling SIM cards, fail to record their customers’ personal details. This new provision and the corresponding penalty are intended to ensure that SIM card users can be reliably identified.

PTSS organisational structure

From lawyer to telecommunications engineer, from test manager to business analyst and from chief investigator to business data processing specialist: the team is as diverse as the topics it deals with on a daily basis.



1

Legal Affairs & Controlling

The 15-strong team is responsible for legal compliance of the PTSS as well as political affairs. The employees develop the legal framework and deal with enquiries from the public. Their activities include answering questions from citizens and the media. In 2018, media interest in the PTSS was relatively high with 33 press enquiries. This was due to the new Federal Act on Post and Telecommunications Surveillance (APTS), rules governing wireless LANs, and case-related surveillance.

The employees are also responsible for finance and reporting for the entire PTSS. They are the number crunchers and are responsible for processing vast amounts of figures and complex statistics, generated daily by IT systems in particular, and presenting them to the service's management and public in a comprehensible manner. The Legal Affairs and Controlling division is also responsible for data and information protection.

Its duties also include implementation of IT projects, project portfolio management, requirements engineering and business architecture.

Finally, the Legal Affairs and Controlling division also manages knowledge management. It controls and implements process management, taking into account the business strategy and customer requirements. The team monitors the internal control system and systematically implements organisation-wide risk management.

Successful planning
and management
thanks to systematic
business controlling:
we maintain an overview
of compliance,
finances, IT systems
and risks.

2

Surveillance Management

The name itself reveals the area in which the 18 employees operate on a daily basis. The Surveillance Management division deals with all matters relating to cooperation between the PTSS and the prosecution authorities, specifically surveillance orders, emergency searches and tracing operations. The orders are checked, recorded in the processing system and transmitted to the telecommunications service providers.

The team is also responsible for invoice processing and advises the prosecution authorities on all legal, technical, organisational and administrative matters relating to post and telecommunications surveillance.

The division is also jointly responsible with the IT operator for incident and problem management. This refers to IT fault management, which covers the entire organisational and technical process relating to detected or suspected IT faults. A separate digital ticket is opened for each incident.

Outside office hours, the division provides a duty service, particularly for setting up surveillance measures. The ordering authorities announce the surveillance operations (including emergency searches and tracing operations) via the duty service mobile number.

Thanks to its duty staff, the PTSS is available 24/7. Standby deployments, which occur about 500 times a year, can be quite hectic. It is important to keep a cool head, for example when the Bern cantonal police contacts the service in connection with real-time surveillance of a drug ring; at the same time, the public prosecutor of the Canton of Zurich is actively searching for a person; plus, incidentally, the Federal Intelligence Service has issued an urgent retroactive surveillance order.

Therefore, other, plannable tasks such as organising all training courses offered by the PTSS provide a welcome balance.



Definition: 'Ordering authorities' are primarily the Office of the Attorney General of Switzerland, public prosecutors of the cantons, military examining magistrates, the Federal Intelligence Service and the Federal Office of Justice in extradition and legal assistance cases.

A solution-oriented partner of the prosecution authorities, assisting them in their investigations by providing high-quality telecommunications surveillance solutions.

3

Provider Management

The Provider Management division of 21 employees deals with technical issues. Among other things, the team is responsible for creating and maintaining the technical specifications and the compliance procedure.

Within this context, the PTSS ensures that telecommunications service providers are ready to conduct surveillance and are able to supply the data required by the prosecution authorities. Telecommunications service providers must, in principle, be able at all times to monitor the telecommunications services they offer and to provide the associated data and information. If they meet certain criteria, such as an annual turnover of less than CHF 100 million, they can be exempted from the obligation to conduct active surveillance. To this end, they need to submit a so-called downgrade application to the PTSS. In 2018, a total of 136 such applications were submitted, 135 of which were approved.

The Provider Management division also develops and operates special tailor-made solutions for implementing surveillance measures, such as technical equipment for 'special cases'.

In addition, Provider Management experts are actively involved in various standardisation committees, for example for the development and implementation of interface specifications for 4G/5G networks. This is necessary in order to ensure lawful monitoring of telecommunications in the future as well.

In order to guarantee a smooth-running, secure IT system, the division is responsible for managing all PTSS applications. The staff advise the telecommunications service providers on technical and legal matters and issue corresponding orders and decisions within the scope of their supervisory authority.

The focus is most definitely on cooperation with the telecommunications service providers. This involves, in particular, supplying information and surveillance data to the PTSS's processing system promptly and correctly.

The division also develops technical solutions for telecommunications service providers that are not obliged or are unable to carry out surveillance. If it is established that a telecommunications service provider is unable to compile the data required by the prosecution authorities, this often leads to a 'special case' for Provider Management staff. This essentially means 'ready, steady, action': the aim is to make the technically impossible possible.



Find out more about a special case on page 16.

A reliable partner of telecommunications service providers, ensuring that all surveillance is conducted lawfully and in a technically and economically viable manner.

4

Administrative Criminal Proceedings

The duties of the chief investigator for administrative criminal proceedings include conducting administrative criminal proceedings.

What does that mean? The chief investigator is responsible for analysing the reported facts from a legal perspective as well as for issuing decisions such as summary penalty orders and decisions and orders to dismiss proceedings. He or she is also responsible for ordering and managing the compulsory measures to be implemented (e.g. seizure, searches and questioning), cooperating with the prosecution authorities and bringing complaints before the courts.

„The aim is to find
pragmatic lawful
solutions.“

Interview with chief investigator Roberta Arnold

Since September 2018, you have been the chief investigator for administrative criminal proceedings at the PTSS, a newly created division following the full revision of the APTS. How do you go about setting up a new competence centre like that?

In 2018, I began by assessing the situation. In particular, this involved analysing the possible scenarios that could lead to the institution of administrative criminal proceedings. The focus then was on creating the necessary infrastructure and work processes. It took a long time to prepare all the procedural documents in three national languages: from the opening ruling, to the summonses, to requests for assistance, to police-enforced appearance and summary penalty orders to name just a few of the procedural documents.

You are fluent in several languages. You must have found that useful these past few months.

Indeed. I was born in the Ticino, and so my mother tongue is Italian. However, I am also fluent in English, French and German.

You have dealt intensively with administrative criminal proceedings. What legal challenges do you see?

Gambling, taxes, competition, money laundering, telecommunications, weapons and animal protection are just a few of the areas in which criminal treatment is regulated in whole or in part by Administrative Criminal Law. The law grants the federal authorities extensive investigative and prosecution powers, which, in some cases, deviate from both the Criminal Code and the Criminal Procedure Code.

As the law dates back to the 1970s, it is to be interpreted within a contemporary context. However, there is a lack of interpretation aids, and because its application in connection with APTS is new, there is currently no case law on the subject.

Have you already conducted the first administrative criminal proceedings since the new division was set up?

Yes, the first proceedings have been opened and have resulted in sanctions.

What do you consider to be particularly important in the future?

In order to benefit from experience gained and lessons learnt in criminal prosecution, we find it valuable to network with other prosecution authorities and to share know-how. In addition, there should also be an exchange between theory and practice. The aim is to find pragmatic lawful solutions.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation

Federal Department of Justice and Police FDJP
Post and Telecommunications Surveillance Service PTSS
Administrative Criminal proceedings Unit

[VStrV.2019.XXX/xxx] 1. November 2018

PENALTY ORDER

In the accelerated proceedings under Art. 65 para. 1 of the Federal Act of 22 March 1974 on Administrative Criminal Law (ACLA; SR 313.0) in the administrative criminal law investigation against

[redacted] son of [redacted] and [redacted] born in [redacted] Swiss citizen, from 3303 Wohlen bei Bern (BE), resident at [redacted] 3003 Bern, kiosk owner.

relating to

an infringement of Art. 39 para. 1 let. c of the Federal Act of 18 March 2016 on the Surveillance of Post and Telecommunications (APTS; SR 780.1).

[...]

The Administrative Criminal proceedings Unit division of the PTSS finds:

1. [redacted] son of [redacted] and [redacted] born in [redacted] guilty of committing a breach of duty by failing to fulfill the obligation to record the required customer data when establishing a customer relationship (in accordance with Art. 39 para. 1 let. c APTS); breach committed in Bern (BE) on [redacted] and sentences the above-mentioned individual to:

a) a fine of CHF [redacted];
b) payment of a copying fee of CHF [redacted].

2. The fine and the copying fee specified in no. 1 lett. a) and b) of the judgment conclusions will be charged separately after this decision has become final and are payable within 30 days of receipt of the invoice.

[...]

Special case

From the lido to the crime scene



The special case described below is fictitious but based on real events. The deployment scenario presented illustrates the type of work carried out by the Provider Management division.

It's a Friday... a hot summer's day in July. Activities are winding down at the PTSS offices. The weekend is within reach; the clatter of keyboards is dying down, gradually being replaced by the sounds of the cleaning team...

Few people are aware, at this point, that a ring of human traffickers has come onto the radar of the Zurich police. In order to convict them, the PTSS has requested real-time surveillance from a Zurich internet provider. The provider has spent several hours trying to set up surveillance. Despite the greatest urgency, surveillance still is not working for technical reasons.

13 July, 4.30pm, Bern – The phone rings: „PTSS, Surveillance Management.“

The PTSS staff member replies: „Okay, yes... I understand. They couldn't find a technical solution to conduct surveillance. I'll inform our special-case team right away.“ The moment the staff member hangs up, a network-based 'mission impossible' begins.

In such cases, only a well coordinated, multidisciplinary team that does not know the meaning of 'impossible' can help.

The Provider Management team immediately assesses the situation (case analysis, feasibility, technical information etc.). There follows a lengthy, technically complex and, due to the urgency, hectic telephone exchange with the internet provider. The provider has already done everything it can to try

to obtain the urgently needed data. To no avail!

After the phone call, it is clear to the special-case team that immediate on-site personal intervention with special technical equipment is required. A meeting place is agreed.

The location must be inconspicuous. A team with cases packed full of computer equipment must not attract attention.

Meanwhile, another member of the Provider Management team is currently enjoying his Friday off at the Auslikon lido. Not for much longer, as it turns out. His phone rings. The moment he learns of the emergency, he leaves the lido and hurries to the 'crime scene' in Zurich to provide support. While the team in Bern provides the necessary equipment and sets off for Zurich, he begins coordinating operation on site. The first priority is to set up monitoring of all the suspects' means of communication (telephone, internet etc.) as quickly as possible.

Within a short space of time, various possible approaches are discussed with all authorities involved. Most of the options are considered 'too risky' based on the criminals' profiles. That is because the criminals must not, under any circumstances, know that surveillance is being set up. Even the slightest malfunction of their router could arouse suspicion and jeopardise investigations. Secret dialogues laden with impenetrable technical jargon follow: setting up the server, installing TAP,

interception point, target-identifier, setting up a VPN etc.

Then comes installation and testing. It takes several hours before the team can finally breathe a sigh of relief.

Surveillance of the human trafficking ring has been successfully set up unnoticed.

Meanwhile it is midnight. The data is successfully transmitted to the PTSS's internal processing system and made available to the prosecution authorities. The relief is great.

You have to try the impossible again and again in order to achieve the possible.

A few months later, surveillance is terminated, and the final steps are taken, including deactivation, deletion and archiving.

Shortly thereafter, the media report the successful arrest of the suspects, who are charged with human trafficking and aiding and abetting prostitution. In cases such as this, the impossible becomes possible only thanks to the excellent cooperation and tireless efforts of all the persons involved.

„Such special cases pose a major challenge owing to their complexity and the interplay of technical, administrative and organisational factors.“

Alexandre Suter, head of Provider Management

03

HOW SURVEILLANCE
WORKS

Surveillance for the purpose of prosecution

The core activity of the PTSS is telecommunications surveillance for the purpose of prosecution.

Covert surveillance is a constant balancing act between protecting privacy and collecting data in order to fight crime.

The PTSS takes a number of measures to protect data during transmission, storage and deletion. Every surveillance order or ruling issued by a public prosecutor must be examined and approved by the competent judicial approval authority ('compulsory measures court'). In the case of the Federal Intelligence Service, the authority responsible is the Federal Administrative Court. The PTSS checks to ensure that approval has been obtained and then carries out a formal check. It checks to ensure that the ordering authority is in fact competent and that the surveillance order relates to a criminal offence in accordance with the crimes referred to in Article 269 of the Criminal Procedure Code (e.g. murder, human trafficking, sexual acts with children, rape or genocide). The seriousness of the offence must justify surveillance.

The PTSS then instructs the telecommunications service provider to transmit the information requested to it, which it then makes available to the prosecution authorities via its processing system. That means that the prosecution authority that ordered the surveillance can analyse the data in the PTSS processing system within a

framework defined and approved by the court (e.g. listening to recorded conversations, creating notes and entering translations).

The diagrams on the following pages offer a simplified view of the parties involved and of how lawful surveillance is conducted.

„Covert surveillance must be regulated by a legal framework, be in the public interest and be proportionate to the objective pursued. This is something we are fully aware of every day and in all areas of our work.“

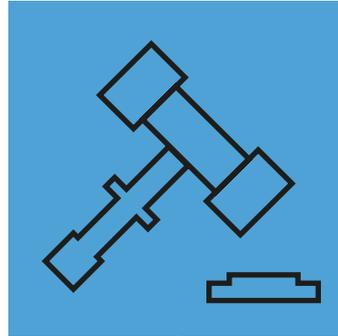
Jean-Louis Biberstein, head of Surveillance Management, deputy head of PTSS

Parties involved



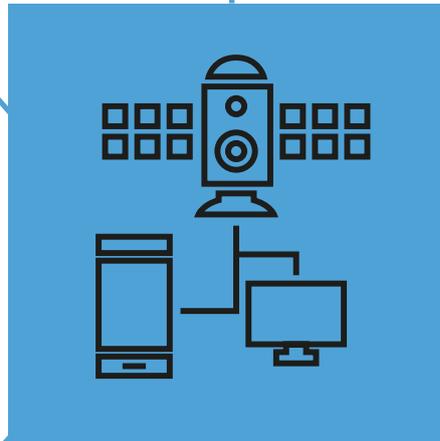
Evaluating authority

These authorities, for example police officers, prepare the desired surveillance measures as part of an order, working together with the ordering authority, for example a public prosecutor. Finally, the persons authorised by the ordering authority are given access to the surveillance content.



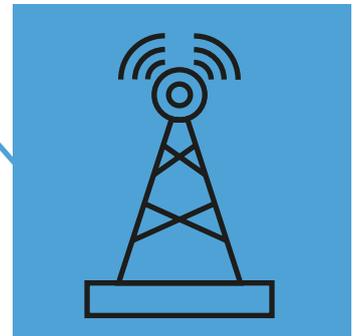
Approval authority

This authority, for example the Compulsory Measures Court, examines the surveillance measures contained in the order from a legal point of view. It approves them, rejects them or approves the order subject to certain conditions.



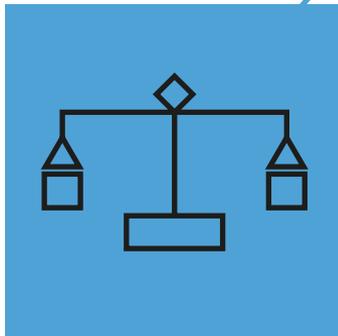
PTSS

The PTSS conducts a formal review of the surveillance measures contained in the order and instructs the telecommunications service providers involved to implement them.



Telecommunications service providers

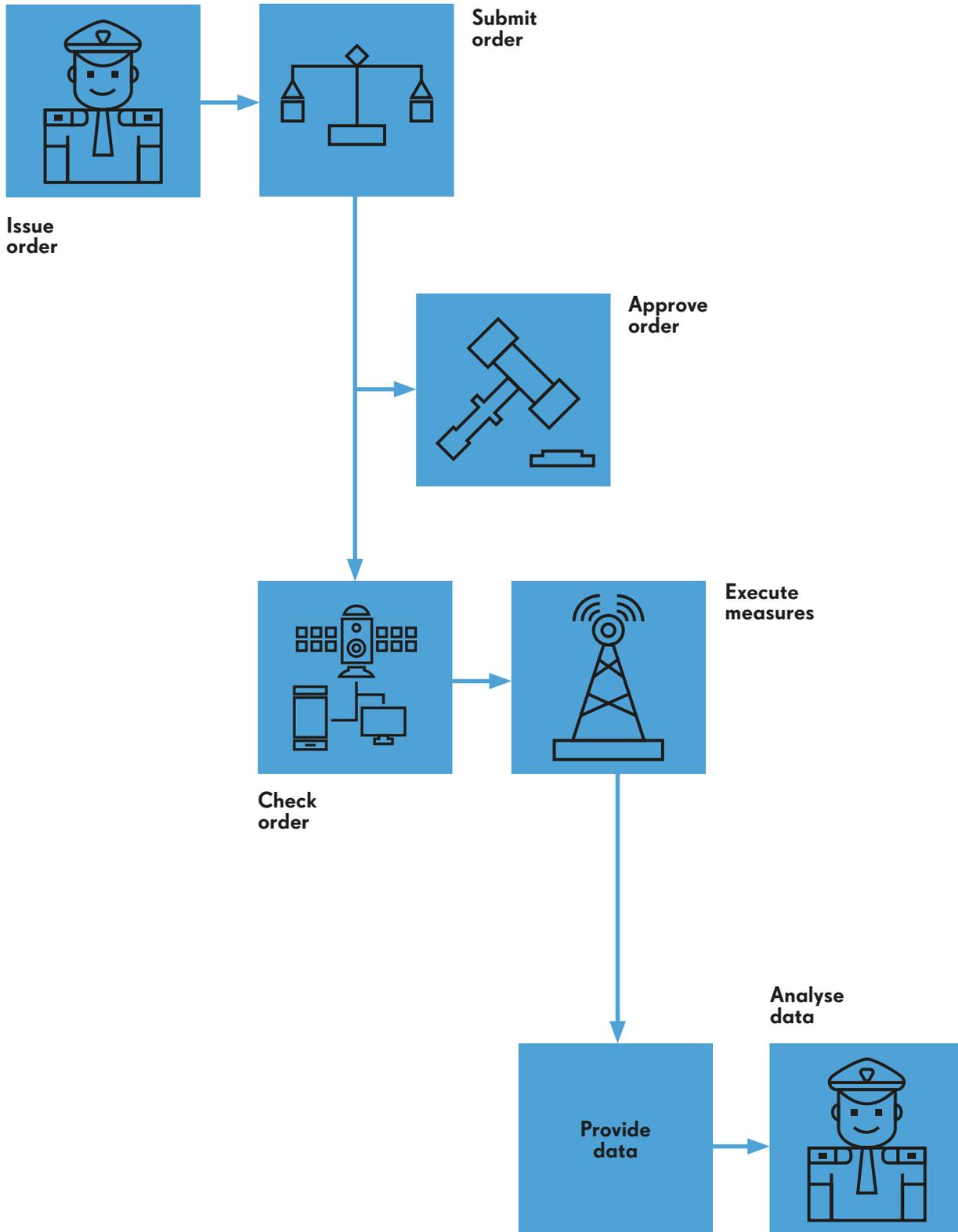
The telecommunications service providers (e.g. Swisscom, Sunrise or Salt) provide the requested data (retroactive surveillance) or set up real-time surveillance.



Ordering authority

This authority, for example a public prosecutor, submits the order to the PTSS. The order and, in particular, the measures contained therein are examined from a legal point of view by the approval authority, for example the Compulsory Measures Court.

How surveillance works



Surveillance measures in 2018 (figures)

Drug trafficking, offences against property and violent crime

Since the PTSS started recording detailed statistics in 2011, the largest share of surveillance measures has been ordered in connection with serious violations of the Narcotics Act.

A glance at the categories of offences in the 2018 statistics shows that, for the first time, serious offences against property rank first, accounting for 35% of all measures. Violations of the Narcotics Act are in second place at 34%. In third place are offences against life and limb (8%), followed by felonies and misdemeanours against liberty (3%). The remainder relate to offences such as those against sexual integrity and felonies and misdemeanours against public order.

The proportion of surveillance measures ordered in connection with very serious offences, such as membership of a criminal organisation, terrorism or rape, is low. These offences generally represent a very small proportion of overall crime.

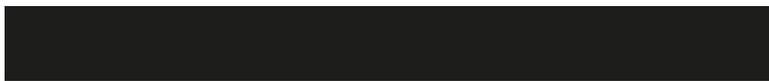


www.li.admin.ch/en/stats

35% offences against property



34% drug offences



8% assault and homicide



3% offences against liberty



3% sexual offences



2% breaches of the peace



15% other



Definition and number of surveillance measures and types of information in 2018

1. Real-time surveillance

Real-time surveillance is the simultaneous, slightly delayed or periodic transmission of post or telecommunications data, for example telephone or email monitoring (listening in on telephone conversations or reading of email messages).

2. Retroactive surveillance

Retroactive surveillance concerns, in particular, telephone records (who called whom, when and for how long etc.) relating to the previous six months.

3. Emergency search

Outside of criminal proceedings, telecommunications surveillance measures can be ordered for the purpose of finding and rescuing missing persons such as hikers involved in accidents or missing children.

4. Tracing of persons

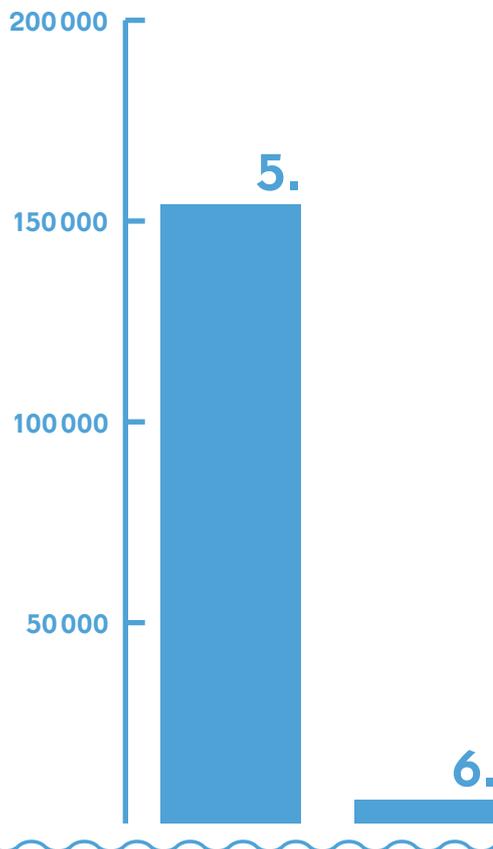
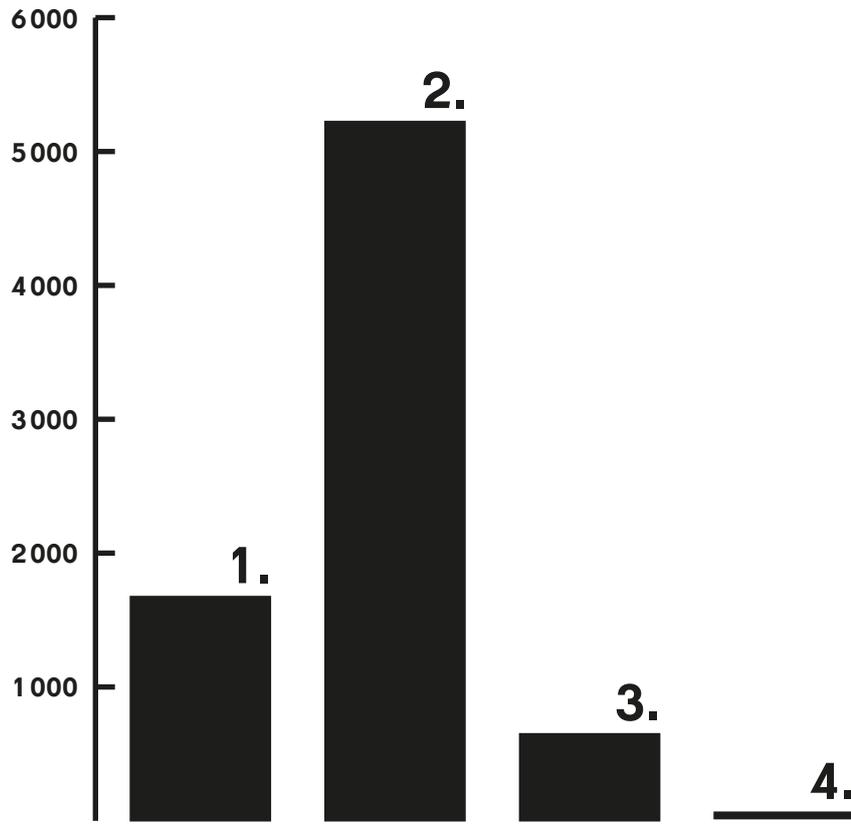
As part of a tracing operation, the prosecution authorities can track down persons on whom a custodial sentence has been imposed or against whom a measure involving deprivation of liberty has been ordered in a legally binding and enforceable decision.

5. Simple information

Simple information can be basic information on subscribers (telephone directory enquiries) or can provide the authorities with information such as who a particular telephone number or IP address is registered to.

6. Complex information

Complex information provides more detailed information relating to telecommunications connections such as copies of contracts or ID.



04

EMERGENCY SEARCH

Emergency search

A contribution from the Zurich cantonal police.
When a mobile phone can be a life-saver ...



The event described is real; the locations, date, times and names are fictitious.



Tuesday, 20 November 2018, 2.10 pm: the Zurich cantonal police operations centre receives a missing persons report via the emergency number 117. Ten-year-old Jonas has gone missing.

His worried mother is on the phone: Jonas' grandmother had expected him for lunch at 12.00 noon as per usual but he had not turned up. He is not answering his mobile phone. She has already contacted all Jonas' friends but no one has seen him since school. She is very worried. It is afternoon now and there is still no trace of the ten-year-old boy.

The operations centre calls in the Zurich cantonal police officer stationed in and responsible for the Hausen am Albis area, who goes to Jonas' home: a block of flats directly on the main road.

According to the school's principal, Jonas was in class until 11.45am. Calls to the boy's mobile phone are now going to voicemail, indicating that the battery might be flat. Temperatures around freezing are expected for the night, and dusk is less than three hours away...

The police officer is given a description of Jonas: **ten-year-old boy of medium build, about 1.35 metres tall, brown hair, brown eyes and wears glasses. At the time he went missing he was wearing jeans and brown-beige winter shoes, a dark blue windcheater, a black backpack and possibly a green woollen hat.**

The Zurich cantonal police operations centre alerts the traffic and municipal police patrol officers. The police search the school grounds, the area around the parents' home and the area around the grandmother's home. Friends and neighbours also begin combing the area. The distance between home and school is just under three kilometres.

The search area is extended. The missing persons alert is sent online to all Zurich cantonal police officers. The police operations centres of neighbouring cantons Zug and Aargau are also alerted.



3.30 pm: Jonas has been missing for almost four hours now.

The manager responsible for the Affoltern am Albis area is also called in and brought up to speed on the investigation and all the action already taken. The hospitals in the region are also contacted: there is still no sign of Jonas.

Meanwhile it's getting colder and darker. A Zurich cantonal police dog handler is called in via the operations centre. At Jonas' primary school, the search dog picks up the boy's scent. The dog moves purposefully in a specific direction: from the school building along the pavement and over the pedestrian crossing. At the crossroads leading to Jonas' grandmother's house, however, the dog turns in the opposite direction, towards the town centre.

The search dog follows the trail undeterred... all the way to the 'Post' bus stop, where it loses the boy's scent. The police assume that Jonas has got on the bus.

According to his mother, he probably has around twenty francs' pocket money on him. But where was he going?

From the 'Post' bus stop in Hausen am Albis, there are four bus lines running out of the town centre. The Zug and Zurich police corps are alerted to step up the search on public transport and at the corresponding stations. Nightfall is an hour away. Time is of the essence. It is getting colder and darker, and nobody has a clue what could have happened to Jonas. With every passing hour, everyone is growing increasingly worried. Could something have happened to the child? Could he have been kidnapped or involved in an accident?

A Zurich cantonal police helicopter equipped with a thermal imaging camera and searchlights is on standby. **But where are the pilots to fly to?**

An emergency search is launched – a telecommunications surveillance measure aimed at tracing the last active location of Jonas' mobile phone. This could provide important information as to his whereabouts.

The officer on duty in the PTSS Surveillance Management division in Bern is contacted and notified of the situation. The 'emergency search' surveillance measure is used to determine the location of the mobile phone mast which Jonas' mobile phone last connected to.

The Zurich cantonal police operations centre then prepares the necessary surveillance request to locate the telephone and sends it to the officer on duty at the PTSS, who immediately contacts the telecommunications service provider concerned for the purpose of ordering an emergency search. The cantonal police also contact the competent compulsory measures court.

It takes almost an hour for the telecommunications service provider to communicate the location of the mobile phone mast which Jonas' mobile phone last connected to. Jonas must have taken the PostBus from Hausen to Thalwil. Did he get off there and what was he doing there?

Emergency search:
which mobile phone
mast last communicated
with the missing
person's mobile phone?

Result: last connection
at 2pm at the Albis Pass
between Hausen and
Langnau am Albis.

Meanwhile, night has fallen. Despite the mobile phone having been located, there is still no sign of life from Jonas. With the new information that the PTSS has received from the telecommunications service provider, the helicopter can now take off from Dübendorf. The helicopter crew systematically fly over the entire area of the Albis Pass and search for the boy with their thermal imaging camera. Meanwhile, police patrols scour the surrounding trails.

It is exactly 5.44 pm when the helicopter crew spot a person in the vicinity of the watch tower, a short distance from the path, with their thermal imaging camera. The nearest police patrol is immediately guided to the location.

A few minutes later they reach an exhausted, freezing boy, albeit in good health. He is crying and says that he only wanted to visit the viewing platform that his schoolmates had told him about. He is terribly sorry and wants his mother.

Trembling, he says that it grew dark far too quickly and so he lost his way in the woods. He accidentally switched off his mobile phone, and his PIN was in his desk drawer at home ...

Police trace missing boy via his mobile phone.

Interview with Peter Bächer, special task force police officer of the Zurich cantonal police

Mr. Bächer, what does your job as a special task force police officer involve?

The special task force police officer manages special police situations. My job is to identify the challenges of a specific situation and decide which should be tackled as a matter of priority so that the police can successfully complete its mission.

At what point are you involved in the case of a missing persons report?

As soon as the missing person can be assumed to be in serious danger. In the case of schoolchildren – as in this case – I am called in shortly after the missing persons report has been filed, after an initial search of the area has been conducted.

For family members, a situation like this is a nightmare. How do you deal with the parents in a situation like this?

The police ensure that the persons concerned are adequately looked after by their own or external specialists.

How do you decide when to deploy a search dog or helicopter or even launch an emergency search?

The police assess the situation on an ongoing basis and use the most suitable resources available to them to ensure a successful outcome. The aim is to find the missing person in good time, safe and sound.

05

LEGAL
ASPECTS

Crime is increasingly shifting to the virtual world and employing digital means. The new APTS is one of the tools used to address the new challenges.

A new legal framework

The new APTS and the associated ordinances came into force on 1 March 2018. These provide Switzerland with a clear, modern legal framework for analysing post and telecommunications data for the purpose of solving serious crime. With the fully revised law, Switzerland's prosecution authorities now have the tools they need also to investigate offences committed using new technologies.

As well as providing the prosecution authorities with additional resources, it reduces the burden on small and medium-sized telecommunications service providers, which benefit considerably as they are not required to invest as much in their surveillance capability.

What has changed?

- Training of the authorities is now a legal duty of the PTSS. In 2018, around 70 training courses were held for more than 2,300 employees of public prosecutors' offices and police stations.
- The PTSS is now also responsible for centralised long-term data storage. The data obtained from surveillance measures is to be stored in a central system operated by the PTSS until the case is time-barred. The aim is to ensure readability of the data for evidence purposes. This system will be implemented within the Telecommunications Surveillance Programme.
- The law now includes penal provisions, enabling the PTSS to penalise any violations of the legal obligations arising out of the APTS. The PTSS can now conduct administrative criminal proceedings (see p. 14 f.).

■ „The complete revision of the Federal Act on Post and Telecommunications Surveillance (APTS) is intended to prevent the necessary post and telecommunications surveillance operations from being thwarted now or in the future by the use of new technologies such as encrypted internet telephony. The idea is to improve surveillance, not to increase it. The APTS and the Criminal Procedure Code (CrimPC) have therefore been adapted to the technical developments of recent years and, as far as possible, to future developments in this area.“
(Excerpt from the dispatch on the Federal Act on Post and Telecommunications Surveillance (APTS).

- The new APTS allows surveillance measures for the purpose of tracing escaped prisoners.
- Outside the remit of the PTSS, the prosecution authorities now have a clear framework for the use of IMSI catchers, special technical devices for monitoring telecommunications. Simply put, these are devices that pose as mobile phone towers in order to trick mobile phones into connecting to them. These IMSI catchers have been used successfully to, for example, locate missing people such as hikers lost in the mountains.
- The prosecution authorities now also have an explicit legal framework for GovWare outside the remit of the PTSS. GovWare is understood to mean computer programs that can intercept and read the contents of communications in unencrypted form in a mobile phone or computer for example.
- Telecommunications service providers can now apply to the PTSS to have their surveillance obligations reduced (downgrade) so that all they have is a duty of tolerance. Since this possibility was introduced, the number of telecommunications service providers required to make the corresponding investments has fallen.
- The obligations to identify users of public wireless LAN hotspots have been set out in writing. The provisions are clear: anyone operating a public wireless LAN at a single location ('non-professional operation') is not required to take any measures to identify users.

The main objective has been achieved, namely that of designing the legal framework in such a way as not to increase surveillance but rather to improve it in order to be able to continue offering post and telecommunications surveillance services in the future.

„Decisive steps
have been taken
with the complete
revision of
the APTS.“

Nils Guggi, head of Legal Affairs & Controlling

06

TECHNOLOGIES AND
SYSTEMS

‘Circuit-switched’ technology, which, for the past 100 years, seemed perfectly suited to telephony and telecommunications surveillance – providing clear, reliable data transmission – has run its course.

Technologies and systems

We are in the middle of a digital revolution. For example, the next generation of mobile communications (5G) is being developed right now. Networks are becoming faster and more powerful and are increasingly geared to the needs of users.

What network and service providers view as achievements and a source of new opportunities pose major challenges for those intending on using these technologies for prosecution purposes. The diversity and complexity of data and technologies is vast. The PTSS must not only keep pace but must remain one step ahead. Surrendering to new technologies is not an option!

Telecommunications have undergone virtualisation: they are no longer visible or tangible and are no longer confined by borders, cantonal, national or international. The digital world pays little heed to the territorial principle of the legislation – advantages that criminals also know how to exploit. Criminals are increasingly communicating via encrypted channels. Security in applications and transmission routes using such encryption technologies and network security itself are set to become increasingly important in the future. However, encryption technologies should not be seen as a dilemma but rather as an opportunity:

After all, what we all want are simple, cost-effective, reliable and, above all, secure communications.

If criminal prosecutors and the PTSS are to keep pace with technological change, they will require not just specialist knowledge but also a high degree of flexibility and agility as well as an organisational structure enabling them to respond promptly, flexibly and proactively to future changes. Therefore, navigating this abstract world requires well-trained experts, cooperation between cantons and countries and high-performance IT systems capable of adapting quickly and intelligently to changing circumstances.

What are the upcoming technological trends?

Telecommunications service providers are constantly launching new products and services. In 2018, for example, several providers introduced the possibility of combining smartwatches and smartphones. Today, a tablet, a smartphone and a watch can all have the same telephone number, which places completely new demands on monitoring. Active participation on the relevant standardisation committees will enable us to overcome these challenges.

The Telecommunications Surveillance Programme

In September 2014, the Federal Council set up a programme with the longwinded name of 'Development and Operation of the Telecommunications Surveillance Processing System and of the Police Information Systems of the Swiss Confederation' (referred to as the 'Telecommunications Surveillance Programme').

With the Telecommunications Surveillance Programme, the Federal Council intends to update the processing system at the core of the PTSS. The programme pursues three key objectives:

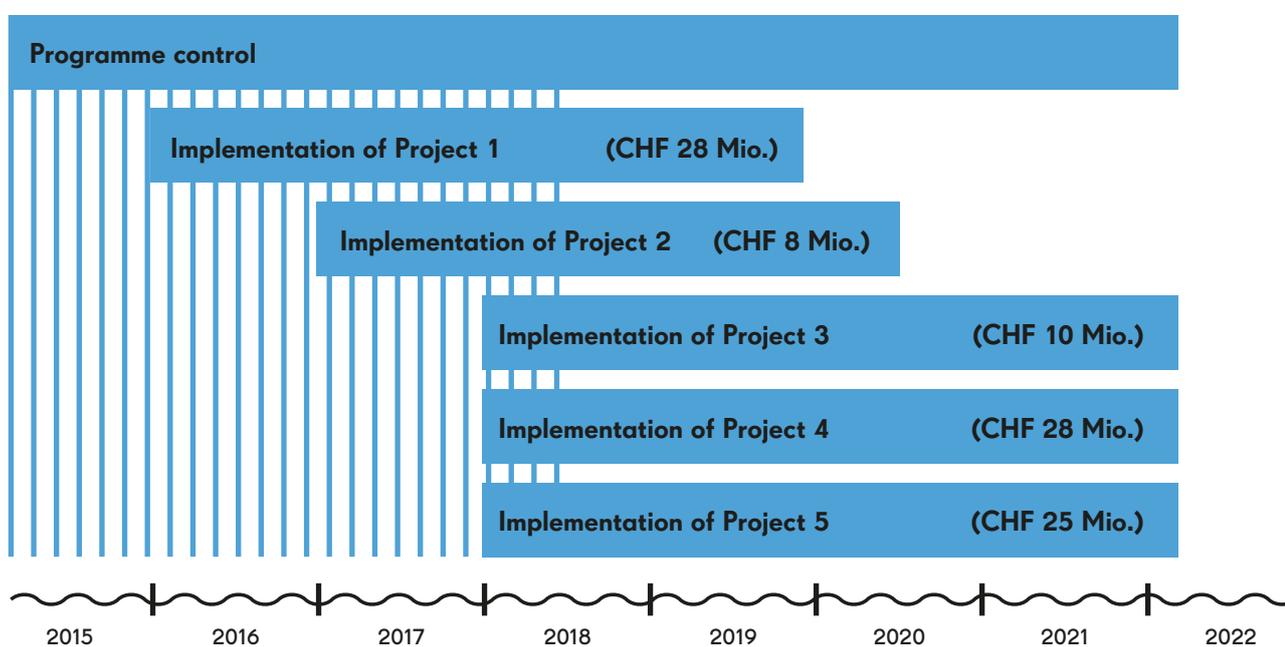
-  **Its system is to be adapted and extended so that it is capable of keeping up with technological developments.**
-  **The PTSS must be capable of performing any new duties that it has received under the new APTS.**
-  **Old components of its system are to be replaced.**

With the envisaged investments in the Telecommunications Surveillance Programme, the Federal Council intends to update the PTSS processing system and the police information systems of the Federal Office of Police (fedpol) to stay abreast of the technical developments of recent years and to meet the requirements of future technologies. This is absolutely essential in order for the IT systems to keep pace with the range of services offered by telecommunications service providers. It also intends to close any potential loopholes in existing and future telecommunications surveillance systems.

Parliament has approved a total allocation of CHF 99 million for the programme. The total investment will be carried out in phases and spread over several years. The necessary system changes and extensions will be implemented in five independent projects.

The five projects of the Telecommunications Surveillance Programme

Programme set-up
+ planning of Projects 1-5



- Project 1: WMC, IRC, RDC
- Project 2: performance adjustments
- Project 3: long-term data storage
- Project 4: system adjustments at fedpol
- Project 5: update of the real-time component

The PTSS started Project 1 of the Telecommunications Surveillance Programme in early 2016 by tackling the Warrant Management Component (WMC), the Information Request Component (IRC) and the Retained Data Component (RDC). The WMC controls and manages all telecommunications surveillance. In addition, the WMC enables the police and public prosecutors to work largely seamlessly. This means that the entire process takes place digitally. The prosecution authorities can enter orders and request surveillance directly via the processing system. This makes for leaner, more efficient and more user-friendly processes. The PTSS uses the IRC to forward requests for information from the authorities to the telecommunications service providers. The PTSS will launch these components in the first quarter of 2019.

The RDC stores the retroactive data supplied by the telecommunications service providers and supports investigators in their work by providing data processing facilities. This component is expected to follow in the final quarter of 2019.

In Project 2, the current real-time component, which has been fully operational since mid-March 2015, is to be developed further.

Back then, a basic system was purchased which now needs adjusting, as far as possible, to take account of the latest technological developments, the increasing load and performance requirements and the needs of the prosecution authorities.

Project 3 of the Telecommunications Surveillance Programme envisages the implementation of a long-term data storage component. This is intended to ensure the availability of telecommunications surveillance data even in thirty years' time. You might be wondering why this is a challenge... Well, ask yourself this: who still owns a cassette recorder today, for example?

A further 28 million francs has been set aside for Project 4 for system adjustments at fedpol.

Project 5 addresses the new technological challenges for telecommunications surveillance.

If new techniques and technologies are used correctly, international cooperation works smoothly, and the prosecution authorities and the PTSS can rely on technically competent, fast and dynamic competence centres, then telecommunications surveillance will continue to contribute significantly to the success of future investigations.

„These complex projects rely on know-how from the fields of engineering, telecommunications, IT architecture, software development, legislation, finance, data protection, law and many more. This knowledge also enables us to keep up with the technologies of the future.“

Vinzenz Lauterburg, deputy project sponsor

07

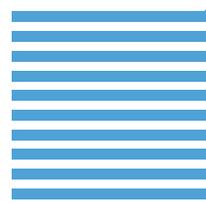
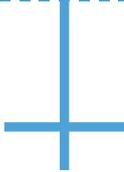
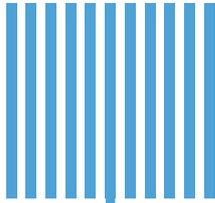
FACTS AND
FIGURES

Number of staff employed

57

of which

18 women



39 men

Average age

44 y.

Age groups

10%: 20–29 y

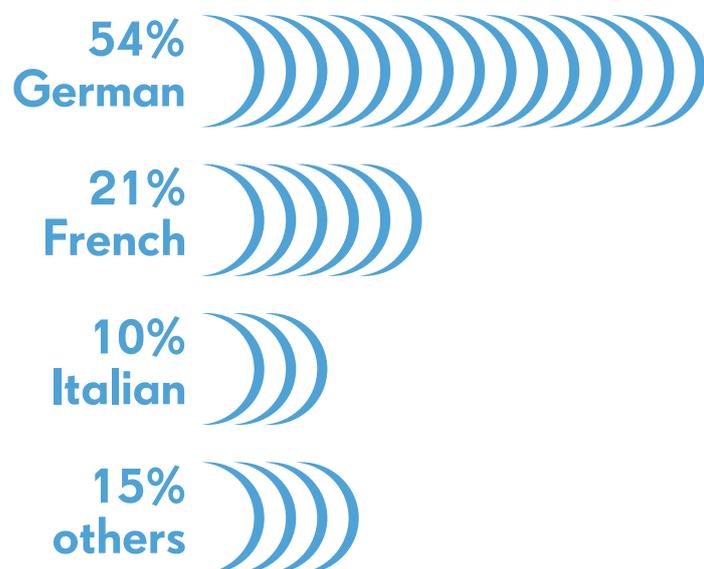
21%: 30–39 y

32%: 40–49 y

32%: 50–59 y

5%: 60–69 y

Languages spoken



PTSS financial performance

Total revenue = **13.8**
million francs

Total expenditure = **28.5**
million francs

Federal contribution = **14.7**
million francs

08

OUTLOOK

Looking ahead to 2019

Although the ink has barely dried on the fully revised APTS and the associated ordinances, the next legislative projects are already in the pipeline.

Selected priorities for 2019

These legislative projects call for broad, systematic and transparent involvement of various stakeholders, including the people, Parliament, the Federal Council, the cantons, the political parties etc.

Legislation is
a collaborative
process.

In the rapidly developing world of telecommunications, our solutions need to be adaptable. Our legal bases also have to keep up with technological developments. The following legislative projects in particular are currently in the pipeline:

Partial revision of the Ordinance on Fees and Compensation for Post and Telecommunications Surveillance Operations

We shall continue to focus on the tariff system again this year. In 2018, the Federal Council instructed the PTSS to set up a working group to deal with the issue of fees. The working group consists of representatives of the PTSS, the Federal Finance Administration, the Office of the Attorney General of Switzerland, the Federal Intelligence Service, fedpol, the cantons (police and public prosecutors), telecommunications service providers and the Conference of Swiss Public Prosecutors.

The working group recommended fundamental changes to the financing system and the creation of a legal basis in order to allow flat annual rates in the future based on the statistics of previous years.

The PTSS's next step is to create the legal basis in the form of a partial revision of the APTS. Meanwhile, the cantons are required to submit a proposal for a concrete flat-rate solution by the end of 2019. In a nutshell, the goal is to issue a single invoice per canton and year, which is expected to noticeably reduce administrative costs, particularly for the prosecution authorities. Until these overall flat rates are implemented, the current fee and compensation model is to be simplified in 2019 by a partial revision of the Ordinance on Fees and Compensation for Post and Telecommunications Surveillance Operations in order to ease the burden on all parties involved.

Partial revision of the Telecommunications Act

The Telecommunications Act currently in force dates from 1997, with the first partial revision becoming effective more than ten years ago. A new revision is required because the spread of the internet has radically transformed the telecommunications industry. The partial revision of the Telecommunications Act also involves changes to two provisions of the APTS. Firstly, the Federal Council will in future be able to describe in greater detail the categories of so-called 'entities obliged to cooperate', which are hard to differentiate. This applies, in particular, to the categories of 'telecommunications service providers' and 'providers of derived communications services'. Secondly, the APTS is to be 'decoupled' from the Telecommunications Act.

Federal Act on Police Counter-terrorism Measures

Unfortunately, terrorism is a non-negligible risk in Switzerland too. In order to protect the population, the police needs more tools to counter terrorist threats. The Federal Act on Police Counter-terrorism Measures is one of the projects envisaged for this purpose. As communications data may now also be collected for mobile phone localisation and transmitted to the competent authority, the scope of the APTS needs to be broadened. At the same time, rules need to be established regarding the right to information and deletion schedules. In concrete terms, this will result, in particular, in new surveillance measures for the PTSS.

Implementation of the Telecommunications Surveillance Programme: completion of Project P1

The new components WMC (order management) and IRC (information) of the processing system are to be put into operation at PTSS in the first quarter of 2019, and the RDC component (retroactive surveillance data) will also become operational in the final quarter of 2019.

The integration of the new system components will noticeably change the PTSS's business processes, as was already the case with the introduction of the new APTS. Many steps in the surveillance process (including invoicing) will be automated. This is necessary for us to be able to fulfil our new tasks in the areas of consulting and training. We are preparing for the innovations ahead through comprehensive change management.

We are aware that successful change requires many ingredients, the most important of which are our staff!

IMPRINT

Concept: PTSS

Editing: PTSS

Layout design:

Stämpfli Kommunikation, Bern

Pictures: PTSS, iStock

P. 27, 28: Zurich cantonal police

Font: Minion Pro, Drescher Grotesk

Printing: Stämpfli AG, Bern

Paper: Z-Offset

German, French, Italian and English

Copyright: PTSS

More information: www.li.admin.ch

Publication: July 2019

**Federal Department of Justice and Police (FDJP)
Post and Telecommunications Surveillance Service
Fellerstrasse 15
3003 Bern**

