Oversight of Covert Surveillance



Vilen Künnapu. Paris Pantheon. Acrylic on canvas. 2025 (fragment of the work)

The Chancellor regularly inspects state authorities that conduct the interception of telephone calls and conversations, monitor correspondence, and collect, process and use personal data in other covert ways. Continuous oversight aims to ensure that all covert measures are carried out with proper justification, in accordance with applicable rules and with due regard for people's fundamental rights. Even when the activities of the authorities concerned are formally lawful, the Chancellor seeks to ensure that people's fundamental rights are always respected. It is also important to reduce people's fear of unjustified surveillance.

In a tense security situation, and in the fight against increasingly sophisticated and wide-ranging crime, surveillance agencies and security authorities also need more powerful tools. At the same time, such tools everywhere entail a greater risk of abuse, and Estonia is no exception. Independent external oversight must therefore also be stronger than before.

During the reporting year, there was indeed a tension between, on the one hand, the desire to grant additional powers to law enforcement agencies, surveillance agencies and security authorities and, on the other, a belief that even their existing powers are being abused and that there is effectively no oversight. The results of the Chancellor’s inspection visits confirm, however, that there are no systemic abuses. As in any field of work, errors and inconsistencies may occur in the activities of surveillance agencies and security authorities. They are usually caused by an incorrect interpretation of a provision of law or an internal instruction, inattention or negligence. More serious, and especially intentional, violations are very rare.

The Chancellor regularly inspects the activities of surveillance agencies — the Police and Border Guard Board, the Internal Security Service, the Tax and Customs Board and prisons. Each year, the Chancellor’s advisers make dozens of inspection visits to these authorities. During the inspections, they generally request for examination 70–80 per cent of the surveillance files opened by the authority or its structural unit during the preceding couple of years.

The inspections assess whether covert measures — interception, reading correspondence, surveillance, examination of computers and telephones, entry into vehicles or apartments, and similar activities — have been lawful. For example, the advisers examine whether properly reasoned authorisations exist and whether the surveillance measure was absolutely necessary; whether files are kept in a way that enables possible errors to be detected; and whether people have been notified of covert measures in a timely manner. Where people have not been notified, the advisers assess whether notification was required.

The most troubling cases are those in which a person who has neither been suspected nor accused of anything has to listen to the contents of their telephone call or confidential conversation being read aloud in a courtroom or, worse still, read a transcript of it in a newspaper or on social media. Intercepting a lawyer’s conversation with a client is also impermissible. If this has nevertheless occurred, it is extremely important that the person concerned is informed.

When inspecting the security authorities — the Internal Security Service and the Foreign Intelligence Service — the Chancellor proceeds from the understanding that people themselves are generally unaware of possible violations of their rights in this field and therefore cannot take steps to defend themselves on their own initiative, for example by

applying to a court. Current law and practice leave relatively few opportunities for intelligence-gathering cases involving security authorities to come under review by higher courts. It is therefore all the more important that every decision to authorise and carry out a measure is carefully considered and can subsequently be verified. The Chancellor’s oversight helps to safeguard people’s fundamental rights and also to dispel suspicions of possible arbitrariness in situations where subsequent judicial review is absent.

Inspection visits carried out to date do not support claims that everyone everywhere is constantly under surveillance or that violations are systemic. The inspected authorities deserve recognition for their open cooperation and for almost always taking account of the Chancellor’s comments and proposals. For example, internal instructions and internal control requirements have been improved. In some cases, an official who violated people’s rights has also had to change jobs.

Detailed summaries of inspection visits to surveillance agencies and security authorities are not public because they contain state secrets or information intended for internal use. The summaries are provided to the supervised authorities and to the institutions responsible for ensuring the lawfulness of the activities of surveillance agencies and security authorities: the courts and the Riigikogu’s Security Authorities Surveillance Select Committee.

Inspection Visits to the Police and Border Guard Board

During the reporting year, the Chancellor’s advisers made a total of 12 inspection visits to police stations of the Police and Border Guard Board, where they examined surveillance files opened in 2023–2024 in which active proceedings had been completed by the time of the inspection. They interviewed surveillance officers and, in most police stations, also a prosecutor.

When examining the surveillance files, the advisers focused particularly on the justification for opening a file and for authorising each specific surveillance measure: whether there had been reasonable suspicion of a criminal offence and whether the measure had been absolutely necessary. They checked whether surveillance measures had been carried out in accordance with authorisations issued by a judge or prosecutor and within the time limits specified in those authorisations. They also examined whether the fundamental rights of third parties had

been protected and whether all requirements concerning notification of surveillance and presentation of the collected material had been met. The advisers also assessed whether the Chancellor’s previous comments and proposals had been taken into account and to what extent the surveillance files had been reviewed by the Prosecutor’s Office.

The opening of the surveillance files examined was generally justified. Surveillance measures had been carried out under authorisations issued by a prosecutor or preliminary investigation judge and in compliance with the time limits and conditions laid down in those authorisations. In a couple of cases, at Haapsalu and Kuressaare police stations, surveillance measures had mistakenly been carried out in respect of a different person.

In most cases, the authorisations issued for surveillance measures complied with the rules established in case-law. Some files, however, contained authorisations that did not sufficiently substantiate the suspicion of a criminal offence or explain why the particular surveillance measure had been considered absolutely necessary. In some cases, there was also reason to question whether the practical feasibility of carrying out the surveillance measure had been properly considered when the authorisation was sought.

Significant problems were identified in the handling of several surveillance files at the South-East Police Station. For example, several files lacked a substantive summary of a particular surveillance measure. It was therefore impossible to establish whether the measure had been carried out, in respect of whom and to what extent, or what information the authority conducting the proceedings had obtained through it. In some cases, people had been notified of surveillance measures with a considerable delay.

For the purpose of more effective protection of people’s fundamental rights, including ensuring effective oversight, the Chancellor made several proposals to the Police and Border Guard Board and the Prosecutor’s Office for improving the quality of the organisation of surveillance measures. All the proposals were based on specific circumstances identified in the surveillance files and in interviews with officials.

Notifying People of Surveillance Measures

Under the Code of Criminal Procedure, people with respect to whom surveillance measures have been carried out must be notified of them. Notification must also be given to people identified in the course of the proceedings whose right to the inviolability of private or family

life has been significantly interfered with by the measure. Notification may be postponed or withheld only in the specific circumstances provided for by law and with the permission of a prosecutor or the court.

Timely and proper notification ensures effective protection of the fundamental rights of people caught in the sphere of influence of surveillance. Among other things, this means that suspects and accused persons have the right to contest the lawfulness of surveillance measures.

In recent months, there has been discussion as to whether third parties — people who are incidentally caught in the sphere of influence of surveillance, for example by meeting a suspect or communicating with them by telephone or email — are too often and without sufficient justification not notified of the measure.

The law requires notification only of people who have been identified in the course of the proceedings. A further condition for notification is that the surveillance measure must have significantly interfered with the person’s right to the inviolability of private or family life.

In the past, surveillance agencies often began by assessing the degree of interference and then proceeded to identify people in order to notify them. In doing so, however, they unnecessarily created what amounted to a “mark” against the person in the system. In fact, the process should work the other way round. The first question should be whether identifying the person is necessary at all for the proceedings — for example, in order to question them as a witness or establish particular connections. Only if identification is necessary should the significance of the interference, and thus the need for notification, be assessed.

If a person is not identified, their name will not appear in the file, for example in connection with intercepted telephone calls, and no other adverse consequences will arise. The police will not, for instance, learn that the person uses drugs and initiate misdemeanour proceedings on that basis.

Once the person is identified, all of this changes. Identification may therefore constitute a separate and considerably more intrusive interference than a person being anonymously caught in the sphere of influence of a surveillance measure. Surveillance agencies have now begun, including in response to the Chancellor’s recommendation, to identify people only where this is genuinely necessary for the proceedings. This is probably one reason why fewer such people have been notified of surveillance in recent years.

Each year, the Chancellor has examined surveillance files to check how the police comply with the requirements for notifying people, including whether failure to notify has been justified. Continuous and targeted oversight will continue. For example, an inspection planned for the coming autumn will examine whether lawyers whose conversations with clients have been intercepted have been notified of the interception in a timely and proper manner.

Inspection of the Use of the KAIRI Information System

The Chancellor’s advisers carried out an inspection at the Police and Border Guard Board to examine how compliance with the general requirements for processing personal data and oversight of the use of the information system are ensured in KAIRI, a subsystem of the police information system POLIS.

The covert collection of personal data and the subsequent processing of those data — including entering data in KAIRI and making queries in the system — are lawful only where there is a clear statutory purpose and legal basis for doing so. The rights of people whose personal data are processed in KAIRI, mostly without their knowledge, are protected above all by an effective and properly functioning system of oversight.

The Police and Border Guard Board has adopted internal rules, implemented a system of support persons and introduced regular log checks. These are all effective measures for ensuring the lawfulness of access to and processing of personal data held in KAIRI, including data collected covertly. It is encouraging that the Chancellor’s proposals have also been taken into account in the development of KAIRI and in improving the rules governing its operation.

Although errors occasionally occur when data are entered in KAIRI or documents are drawn up, KAIRI is used for its intended purpose, strictly for the performance of official duties. There have been very few cases of deliberate misuse of KAIRI.

As a follow-up to this inspection, a further inspection visit is planned to assess whether the covert collection of data about people and its storage in KAIRI, including in the preventive activities dataset, is lawful.

Handling Applications from Individuals

In addition to regularly overseeing the activities of surveillance agencies and security authorities, the Chancellor also deals with complaints concerning these authorities and, where necessary, examines other publicly made allegations, for example in the media, concerning unlawful or insufficiently justified surveillance.

The concerns raised by people who contact the Chancellor are often directly related to ongoing proceedings. The law does not allow the Chancellor to intervene in offence proceedings, but this does not necessarily mean that allegations concerning surveillance measures will go unexamined. Where necessary, they can be examined separately at a later stage, for example after criminal proceedings have ended.

Review of the Use of Communications Data

Following an application submitted to the Chancellor, the Chancellor’s advisers inspected security authorities and surveillance agencies to obtain an overview of the implementation of written contracts concluded under § 112(2) of the Electronic Communications Act. These contracts allow communications data to be requested by way of continuous electronic connection.

All the authorities inspected have established multi-level internal controls and procedures for approving requests for communications data and the subsequent processing of those data. Internal rules specify the responsibilities of the officials concerned and the conditions under which communications data may be requested from a communications undertaking. Communications data do not include the content of communications. A record of each request remains on the servers of both the communications undertaking and the authority that made the request. It is also possible to verify in detail afterwards how the data were subsequently processed by the authority that requested them.

During the inspections, sample cases were used to examine how communications data are requested by way of continuous electronic connection and how each authority ensures that requests are justified and properly approved.

The inspection identified no shortcomings or irregularities in requests for communications data.