Surveillance

The Chancellor of Justice verifies whether state agencies that organise interception of phone calls and conversations, surveillance of correspondence, and otherwise covertly collect, process and use personal data operate lawfully.

The purpose of supervision is to ensure that covert measures are taken with justification, i.e. in conformity with legislation and the aim sought, as well as in a manner respecting people's fundamental rights. Even when the actions of the relevant agencies are formally lawful, the Chancellor ensures that people's fundamental rights are reckoned with to the maximum possible extent. This helps to alleviate uncertainty and fear of unjustified surveillance.

In 2019−2020, the Chancellor's advisers checked how the police stations (total 15) of the Police and Border Guard Board (PBGB) had respected people's fundamental rights when carrying out surveillance measures and processing communications and bank data. Also checked were the activities of the Estonian Internal Security Service and the Estonian Foreign Intelligence Service in fulfilling the aims laid down in the Security Authorities Act.

Detailed summaries of inspection visits to security and surveillance agencies are not public since they contain information classified as state secrets or for internal use only. The addressees of the summaries are supervised agencies as well as public authorities (Security Authorities Surveillance Select Committee of the Riigikogu, the court, the prosecutor's office) which are also responsible for the legality of activities of security agencies.

Notifying about measures for collecting information, and amendments to the law

Section 44(3) of the Constitution requires that an individual must be notified of a measure carried out (including covertly) in respect of them. Thus, everyone who wishes may access the data held on them by a government agency. Under the law, this right may be circumscribed, inter alia, to protect the rights and freedoms of other people and to prevent a criminal offence. Notification may be postponed only until the above reasons outweigh the restriction on fundamental rights resulting from the measure. However, the Security Authorities Act (SAA) only obliges notifying an individual but does not prescribe a possibility to access the data.

Notifying an individual about the measures carried out in respect of them is laid down by § 29 of the SAA. When assessing its implementation, the Chancellor has found that if an individual cannot be notified immediately a security agency's own effective and efficient procedures (a control system) should ensure that a ground for non-notification exists in actuality. Once the ground ceases to exist the individual should still be notified about the measure restricting their fundamental rights. Already in 2017 the Estonian Internal Security Service and the Foreign Intelligence Service agreed to revise their guidelines in this regard and to observe this principle in practice.

By judgment of 19 December 2019, the Supreme Court Constitutional Review Chamber (in case No 5-19-38/15) declared unconstitutional the Act amending the Defence Forces Organisation Act (DFOA) adopted on 29 May 2019. The reason was that the Act (specifically § 40) did not lay down effective control over compliance with notifying an individual if the Defence Forces have carried out covert surveillance of the individual under § 54^1(2) clause 2 of the DFOA. The Supreme Court did not support the arguments set out in the application by the President of the Republic that conferring on the Defence Forces the function of surveillance was unconstitutional. The Chancellor reached the same conclusion in her opinion.

In the Chancellor's opinion, this reasoning by the Supreme Court was also directly applicable to § 29 of the Security Authorities Act. The wording of § 29 SAA and § 40 DFOA was identical, and neither of them laid down constitutionally compliant regulation in line with the Supreme Court criteria that would have required verification of reasons for non-notification. On that basis, in a letter sent to the Riigikogu, the Chancellor also asked that, in the course of proceedings initiated for amendment of the DFOA, § 29 of the SAA would also be brought into line with the Constitution insofar as it failed to lay down systematic, regular and independent substantive control of the reasons for non-notification of the measures set out in § 25(1) clauses 1, 2 and 3 and § 26(3) clauses 2, 5 and 6 of the SAA.

On 13 May 2020, the Riigikogu adopted the Act amending the Defence Forces Organisation Act, the Security Authorities Act, and the Chancellor of Justice Act, by which the text in § 29 SAA was also thoroughly changed. This section now lays down clear grounds for non-notification of a measure for collecting information. Section 1 of the Chancellor of Justice Act was supplemented with subsection (9^1), and a new function was conferred on the Chancellor: to verify at least every two years whether non-notification of persons under § 29(2) of the Security Authorities Act and § 40(2) of the Defence Forces Organisation Act about measures

for collecting information was justified.

Control of surveillance files

During inspection visits, the Chancellor's advisers examined surveillance files opened by police stations in 2018−2019 where active proceedings had ended by the time of the inspection. During that period, a total of 115 surveillance files were opened, of which 95 files were inspected.

The Chancellor's advisers assessed the guarantee of fundamental rights and interests of those persons who became objects of covert data collection (i.e. a surveillance measure) in the course of criminal proceedings either as suspects or as 'third parties' (including by chance). The inspection focused primarily on whether, in each specific case, conducting the surveillance measure while collecting information about a criminal offence had been lawful (including unavoidable and necessary), and how the surveillance agencies complied with requirements to notify people about a surveillance measure.

In order to ensure better protection of fundamental rights, the Chancellor made several proposals to the surveillance agencies and the prosecutor's office. For example, she recommended that some police stations should organise training for surveillance officers, so that the officers could update their knowledge of regulation of surveillance measures and of assessing justification for measures, including in terms of guaranteeing people's fundamental rights.

Surveillance authorisations

A surveillance measure is lawful only if the prosecutor's office or the court has issued an authorisation meeting the statutory requirements, i.e. the requirements of form and reasoning. The inspections revealed that, as a rule, surveillance authorisations were reasoned and surveillance was necessary to verify suspicion of a criminal offence. Nevertheless, examination of some surveillance files raised doubts as to whether the information available at that moment (i.e. reasonable suspicion of a criminal offence) was indeed sufficient to warrant collecting evidentiary information through surveillance and thus restrict people's fundamental rights.

Comparison of files examined this year and in previous years shows that reasoning for surveillance authorisations (in particular authorisations issued by preliminary investigation

judges) has improved. Special mention should be made of those authorisations containing reasons for the necessity of a surveillance measure, the principle of *ultima ratio*, i.e. a measure of last resort, as well as the effect of measures on the subject of surveillance and third parties linked to them.

Preliminary investigation judges generally observe the opinion repeatedly expressed in case-law in recent years that reasoning contained in a court order authorising surveillance must also include clear and understandable arguments by the court with regard to the necessity for surveillance.

Some surveillance authorisations issued by the prosecutor's office had not been reasoned in line with the above requirements. Unreasoned authorisations could be found, primarily, in the surveillance files of police stations under the North Prefecture.

Carrying out surveillance

The Chancellor's advisers did not find any surveillance measures that had been carried out without authorisation by a preliminary investigation judge or a prosecutor and without compliance with the conditions set out in the authorisation. In the frame of surveillance files inspected, surveillance had been carried out generally in line with the purpose. However, inspection of some surveillance files in police stations in the North and East Prefectures raised doubts as to whether preparatory actions by the surveillance agency and the prosecutor's office had always been carefully considered, so as to warrant opening a surveillance file to collect evidentiary information through surveillance and thereby restrict people's fundamental rights.

With a view to protecting fundamental rights, the Chancellor deems it highly important to add substantive summaries to surveillance files. This helps both the person inspecting the file as well as the person conducting the proceedings to subsequently assess whether a surveillance measure was indeed fit for the purpose and justified. A substantive summary also provides a better overview of the circumstances of restricting fundamental rights.

Largely thanks to the recommendations given after the Chancellor's earlier inspection visits, this good practice is increasingly prevalent in the majority of police stations.

Notifying a surveillance measure

Under the Code of Criminal Procedure, a surveillance measure is notified to the persons with

respect to whom the surveillance measure was carried out, as well as other persons identified during the proceedings whose right to inviolability of private or family life was significantly interfered with by the measure. Notification may be postponed or waived only in specific circumstances set out by law if permission for this by a prosecutor or the court exists.

Timely notification protects people's fundamental rights and also ensures the right to contest the lawfulness of surveillance measures for suspects and the accused.

In previous years, the Chancellor's advisers found many cases where no such notification was given or people were notified too late. The situation has now significantly improved. Nevertheless, examination of a surveillance file revealed a case where notifying people had been delayed unjustifiably long (more than a year and nine months). In the remaining cases (eight cases among the files inspected), the delay was mostly between three to nine months.

However, examination of some surveillance files raised doubts that persons had been notified of surveillance too early. Under § 126^{13}(2) clause 1 of the Code of Criminal Procedure, the prosecutor's office may authorise postponing notification of surveillance until the end of pre-trial proceedings in a criminal case if earlier notification may significantly prejudice criminal proceedings. However, in these cases this was not done, so that those persons on whose criminal activities evidence was to be collected also became prematurely (i.e. in the initial stage of pre-trial investigation) aware of surveillance (and incidentally also of the interest of the police in them).

Also, it cannot be considered justified to identify and notify people whose inviolability of family or private life is not significantly restricted in the course of surveillance. Since identifying such a person (for example by collecting data on them from an information system or database), in turn, restricts the person's fundamental rights, this should only be done in the case of clear and justified need.

Processing of communications and bank data

The Chancellor's advisers also checked whether requests for submission, and subsequent use, of data set out in § 111^{1}(2) and (3) of the Electronic Communications Act within criminal proceedings (under § 90^{1} of the Code of Criminal Procedure) from communications undertakings (Telia, Elisa, Tele2) had been lawful. In the cases checked, requests for communications data had been in line with the purpose and lawful. The required authorisation by the prosecutor's office and unavoidable necessity existed for making these

enquiries: for example, it was necessary to first check with a measure less restrictive of fundamental rights whether tapping a specific person's phone was justified or not.

As an aside comment, it might be important to note that a similar legal restriction also applies to processing communications data in other cases. During the emergency situation in spring, the wish was voiced that perhaps the Police and Border Guard Board, the Health Board or another government agency might start monitoring the movement of infected people either via a special mobile application or otherwise. No such blanket monitoring is allowed by law. Mobile phone location data might be used only in very limited cases to identify or counter a grave threat (i.e. a threat to someone's life) and if court authorisation for this exists in misdemeanour proceedings and a prosecutor's authorisation in criminal proceedings.

A body conducting pre-trial proceedings is entitled within criminal proceedings to request banks to submit banking secrets of their clients. This means primarily queries with a view to analysing data on people's bank accounts. Officers in all police stations who had made queries with banks in the frame of criminal cases they were dealing with were able to provide sound reasoning for making the queries. Random checks also affirmed that queries were made relatively rarely and only in criminal cases where it is necessary for the purpose of collecting evidentiary information (e.g. fraud and other acts against property, drug offences, maintenance claims, the need to identify criminal proceeds, or to secure a civil claim).

Inspection visits to security agencies

The Chancellor's advisers reviewed how the Estonian Internal Security Service and the Estonian Foreign Intelligence Service have guaranteed the fundamental rights protection of individuals in respect of whom data are covertly collected by measures laid down in § 25 and § 26 of the Security Authorities Act (e.g. interception, covert surveillance, covert examination of items, phone records, covert entry).

The Chancellor's supervision over the activities of security agencies is extremely important since, under currently effective law and established practice, opportunities are extremely limited for cases of information collection by security agencies to come within the ambit of judicial review by superior courts. For example, the Supreme Court has also not heard any cases related directly to authorisations issued for carrying out measures under §§ 25 and 26 of the Security Authorities Act (e.g. as regards the reasoning for such authorisations). Therefore, it is even more important that authorising and carrying out a measure is

thoroughly considered and that this can also be subsequently verified. This precludes the possibility of suspicion of arbitrary action even where judicial follow-up review is essentially absent.

Security agencies have clearly established thorough internal audit procedures over activities carried out under the Security Authorities Act. In-house guidelines set out the duties and liability of officials, as well as overall requirements on how to draw up, register and keep the documents needed to carry out measures for collection of information (including obtaining various approvals). Nevertheless, based on the results of the inspection the Chancellor found it necessary to make some proposals for better protection of individuals' fundamental rights.

Review of information files

The review of information files focused first and foremost on whether carrying out a measure for collecting information was lawful, as well as unavoidable and necessary. The measures set out in § 25 of the Security Authorities Act, which may only be carried out with court authorisation, restrict a person's right to the confidentiality of messages, as well as the right to inviolability of private life, more seriously than several of the covert measures set out in § 26 of the Act, which may be carried out with authorisation from the head of a security agency. Under § 3(2) of the Security Authorities Act, in the event of a choice between several possible measures, the measure that least restricts the fundamental rights of individuals should be chosen. Therefore, every authorisation of a measure for collecting information should enable monitoring whether, prior to issuing the authorisation, consideration was also given to possible alternatives, i.e. using measures that would be less restrictive in terms of fundamental rights.

Opening information files and carrying out measures under §§ 25 and 26 of the Security Authorities Act in the frame of them was justified in all the cases reviewed. Every file contained authorisation either by the administrative court or head of the agency (or person authorised by them). In comparison with authorisations previously contained in information files (i.e. those reviewed in 2017), reasoning for authorisations issued for measures for collecting information has significantly improved (similarly to surveillance authorisations described above). Thanks to very thorough and substantive summaries, information files offered a good overview and enabled understanding clearly why a person's fundamental rights needed to be restricted in a specific case.

Petitions by persons

Besides the Chancellor's own-initiative and regular supervision, she also has to resolve complaints concerning surveillance measures and, if necessary, verify other publicly raised allegations (e.g. in the media) about illegal or insufficiently reasoned surveillance.

For example, when verifying a petition by the East Tallinn Central Hospital, the Chancellor ascertained that a device found connected to a computer in the hospital had been used to carry out surveillance in the frame of criminal proceedings. The review revealed that the surveillance measure in question had been carried out lawfully, i.e. under a properly reasoned judicial authorisation.

In recent years, the Chancellor has had to resolve petitions in which people complained about notification of surveillance. Due to incomplete notices sent by the security agencies, people could not exactly understand why they had been subjected to surveillance in a particular case, and what surveillance measures affecting them had been carried out and to what extent.

The Chancellor has repeatedly (including during inspection visits) emphasised to the surveillance agencies that informing people about surveillance measures always requires clearly distinguishing whether the particular person was the direct subject of surveillance, or whether they were a so-called third party whose privacy was significantly interfered with by the surveillance measure. This helps the recipient of notification to better understand the circumstances of carrying out surveillance affecting them and decide (including in terms of an appropriate remedy) whether they wish to protect their rights.

During the reporting year, the Chancellor explained to several petitioners the substance and functioning of the legislation laying down possibilities for people to access data collected on them in the course of surveillance (§ 126[14] Code of Criminal Procedure). Inter alia, based on a petition by a law office, the Chancellor had to analyse opportunities by remand detainees and convicted prisoners to access data collected on them. The analysis also involved checking the constitutionality of § 99(1) (second sentence) of the Imprisonment Act and § 5(1) of "The procedure for notifying about a surveillance measure and presentation of a surveillance file" established by the Government Regulation.

The Chancellor found that both provisions were constitutional since remand detainees were

ensured the opportunity to access surveillance data also when they could not personally go to the premises of a surveillance agency. In fact, several possibilities exist to access data: for example, if a person cannot go to a surveillance agency during the three months prescribed, in the case of having a sound reason (which may also include the person's stay in a place of detention) the person may apply to the surveillance agency to restore the deadline to access data collected through surveillance. A person may (also with a sound reason) authorise a third party to examine their surveillance data if that third party presents a notarised power of attorney to that effect. Under § 95(1) of the Imprisonment Act, a person remanded in custody may meet a notary for performance of a notarial act. If a person suspected of a criminal offence or an accused wishes to access the data, surveillance data may also be examined by their attorney. A prisoner can also access their surveillance data in a place of detention if this is allowed by the investigative authority and the place of detention consents to this.

Cooperation with the Security Authorities Surveillance Select Committee of the Riigikogu

During regular meetings with the Security Authorities Surveillance Select Committee of the Riigikogu, the Chancellor provides an overview to members of the Riigikogu about the results of inspection visits and problems found in the course of supervision (including in resolving petitions). Members of the Committee, in turn, can make observations on issues in the field of surveillance.

Based on information received from the Riigikogu Committee, the Chancellor reviewed surveillance measures carried out on the basis of (oral) authorisations in cases of urgency. Specifically, in urgent situations the law allows carrying out a surveillance measure (interception, staging a criminal offence, covert examination of a postal item) by court authorisation issued in a reproducible manner (for example, orally by telephone, assuming that the call is recorded). This may only be done if a threat exists to a person's life, bodily integrity or physical freedom, or to high-value pecuniary benefit, and applying for a surveillance measure or drawing it up in line with formal requirements is not possible in a timely manner. In that case, a written application and authorisation shall be formalised within 24 hours as of commencement of the surveillance measure.

It was found that courts issue urgent authorisations only exceptionally and very rarely. For example, in 2017 only one such authorisation was issued, and none in 2018 and 2019. The prosecutor's office has issued so-called oral authorisations for covert surveillance under § 126 [4](2) of the Code of Criminal Procedure somewhat more often: 19 authorisations in 2017, 16 in

2018, and 14 in 2019. The Chancellor's advisers have always thoroughly reviewed the lawfulness of such authorisations (including whether the subsequent written authorisation was formalised in time). No violations of the law have been found.