NEJVYŠŠÍ SPRAVNI SOUD

Seminar organized by Supreme Administrative Court of the Czech Republic and ACA-Europe

Supreme administrative courts and evolution of the right to publicity, privacy and information.

Brno, 18 May 2015

Answers to Questionnaire: Estonia

Seminar co-funded by the "Justice" programme of the European Union

Supreme Administrative Courts and evolution of the right to publicity, privacy and information

(Questionnaire)

1. Briefly describe the administrative institutional backing of free access to information and of the protection of personal data. Whenever those agendas are institutionally linked, provide for a brief description of such relations.

Free access to information

Free access to information is primarily regulated by the Public Information Act[1] (PIA). According to § 1 of the PIA the purpose of the Act is to ensure that the public and every person has the opportunity to access information intended for public use.

When a person is interested in certain information they need to make a request for information to a holder of the information. Pursuant to § 5 of the Act holders of information are: state and local government agencies, legal persons in public law, as well as legal persons in private law and natural persons, if they perform public duties. According to § 13 of the Act the request of information can be made either orally (directly, telephone) or in writing (post, fax, e-mail). A request for information shall be dealt with promptly but not later than within five working days. § 23 of the Act prescribes the conditions for refusing to comply with the request of information.

The Data Protection Inspectorate supervises the holders of information during compliance with requests for information and the disclosure of information (§ 45). The Data Protection Inspectorate is a government authority in the area of government of the Ministry of Justice. The Inspectorate performs functions in the field of access to information and personal data protection. A person whose rights provided for in the PIA are violated may file a challenge with the Data Protection Inspectorate or an action with an administrative court either personally or through a representative.

Protection of personal data

The Personal Data Protection Act[2] (PDPA) aims to protect the fundamental rights and freedoms of natural persons upon processing of personal data, above all the right to privacy. The PDPA provides the conditions and procedure for processing of personal data, for the state supervision upon processing of personal data, and liability for the violation of the requirements for processing of personal data.

[1] Available in English: https://www.riigiteataja.ee/en/eli/522122014002/consolide.
[2] Available in English: https://www.riigiteataja.ee/en/eli/529012015008/consolide.

According to § 22 of the PDPA, a data subject has a right of recourse to the Data Protection Inspectorate or a court if his or her rights are violated in the processing of personal data, unless a different procedure for contestation is provided by law. If the rights have been violated upon processing of personal data, the data subject has the right to demand compensation for the damage caused to him or her: 1) on the basis of the State Liability Act if the rights were violated in the process of performance of a public duty, or 2) on the basis of the Law of Obligations Act if the rights were violated in a private law relationship (§ 23).

Criminal law

The Estonian Penal Code incorporates two offences concerning the illegal disclosure of personal data. According to § 157 it is illegal to disclose information obtained in the course of professional activities by a person who is required by law not to disclose such information. § 157[1] provides that the illegal disclosure or provision illegal access to sensitive personal data is punishable.

2. Describe in general terms the regular administrative and court procedure in a typical disputable case of free access to information. Describe also the procedural role of your supreme administrative instance.

The holder of information shall notify the person making the request for information of refusal to comply with the request for information and the reason for such refusal within five working days. A person whose rights provided for in the PIA are violated may file a challenge with a supervisory body (the Data Protection Inspectorate or the Estonian Information System's Authority – the latter only in cases related to the establishment, introduction and maintenance of databases and information systems) or an action with an administrative court. Either of these has to be filed within 30 days after the date on which the refusal to comply with the request for information (or the unsatisfactory response) was notified to the applicant. The Code of Administrative Court Procedure[3] provides a special time-limit for the case of delay: one year after the time-limit for responding has elapsed.

If the person turns to the Data Protection Inspectorate (which may also act of its own initiative), the Inspectorate may issue a precept which requires a holder of information to bring its activities into accordance with law if the Inspectorate finds that the holder of information:
1) has refused illegally to comply with a request for information;
2) has not responded to a request for information within the prescribed term;
3) has not complied with a request for information as required;
4) has not processed a request for information as required;
5) has failed to disclose information subject to disclosure as required;

[3] Available in English: https://www.riigiteataja.ee/en/eli/509022015001/consolide.

6) has not performed the obligation to maintain a website as required;
7) has established restrictions on access to information illegally;
8) has failed to establish restrictions on access to information provided by law;
9) has released information to which restrictions on access are established pursuant to the PIA.

The holder of information shall, within five working days as of receipt of a precept, take measures to comply with the precept and shall notify the Inspectorate thereof. Upon failure to comply with a precept, the Inspectorate may impose a penalty payment with the upper limit of 9600 Euros. In addition, the Inspectorate may address a superior agency, person or body of the holder of information for organisation of supervisory control or commencement of disciplinary proceedings against an official.

If the Inspectorate does not issue a precept or the precept does not satisfy the person whose rights were violated, the person can bring an action to the administrative court against the Inspectorate. In that case, the holder of information normally joins the proceedings as a third party. Since the Inspectorate has a wide discretionary power, the judicial control is limited to the verification of the compliance by the Inspectorate with the rules of procedure and the limits and objective of the discretionary power. The court does not engage in an exercise of the discretionary power in the place of the Inspectorate and cannot issue a precept in the Inspectorate's stead.

With or without previously turning to the Inspectorate, the person whose rights were violated can bring an action to the administrative court against the holder of information. The most effective type of action is a mandatory action – if it is granted, the court may either order the respondent to comply with the request for information or, if the holder of information has a discretionary power in deciding whether to comply with the request, the court may order the respondent to make a (new) decision on the issue within a time-limit set by the court. The person can also seek a declaration of unlawfulness of the information holder's delay or refusal, but only in the absence of more efficient remedies for protecting the right in question.

The judgment of the administrative court of first instance can be appealed to the circuit court, and the judgment of the circuit court to the Supreme Court (appeal in cassation). The Supreme Court (Riigikohus) acts as the supreme administrative instance in Estonia, and administrative matters are normally heard in written proceedings by a three-member panel of the Administrative Law Chamber. The Supreme Court opens proceedings on an appeal in cassation if:

1) the positions stated in the appeal warrant the conclusion that the circuit court has incorrectly applied a rule of substantive law, or has significantly infringed the rules of court procedure, which has resulted or could have resulted in an incorrect judgment, or

2) the determination of the appeal is of considerable import from the point of view of ensuring legal certainty or uniformity of approach in the case-law of the courts.

The Supreme Court's refusal to open proceedings is formalised as a ruling which only sets out the legal basis of the refusal (i.e. no substantial reasoning).

In its judgment, the Supreme Court is bound by the facts as ascertained by the circuit court, except in the case that ascertainment of a fact is contested in the appeal in cassation and, in relation to that ascertainment, the rules of procedure were significantly infringed. When hearing an appeal in cassation, the Supreme Court has the power to:
1) dismiss the appeal in cassation and uphold the judgment of the circuit court;
2) annul the judgment of the circuit court in full or in part and return the matter insofar as it annulled the judgment, for a new hearing to the same, or other, circuit court;
3) annul the judgment of the administrative court and the judgment of the circuit court and return the matter to the administrative court for a new hearing, or refuse to hear the appeal or terminate proceedings in the matter;
4) annul the judgment of the circuit court and uphold the judgment of the administrative court;
5) vary the judgment of the circuit court or the judgment of the administrative court, or enter a new judgment without returning the matter for a new hearing provided it is not necessary to take new evidence in the matter or vary the assessment of that evidence stated in the appeal against the judgment of the administrative court;
6) vary the reasons stated in the judgment of the circuit or in the judgment of the administrative court while upholding the operative part of the judgment.

In case of failure to execute a court decision, the court imposes a fine with the upper limit of 32,000 Euros on the participant of the proceedings whose fault this is. The fine may be imposed several times if necessary.

3. Describe the procedural role of your supreme administrative instance in the agenda of protection of personal data.

The procedure and powers of the Supreme Court in the agenda of protection of personal data are the same as described in question 2. As explained in question 1, there is one supervisory body that handles both matters concerning free access to information and protection of personal data. However, the administrative and judicial options for the person whose rights are violated are somewhat different.

According to the PDPA, a data subject has a right of recourse to the Data Protection Inspectorate or a court if his or her rights are violated in the processing of personal data, unless a different procedure for contestation is provided by law. If the rights of a data subject have been violated upon processing of personal data, the data subject has the right to demand compensation for the damage caused to him or her.

If the rights are violated in the process of performance of a public duty, the procedure is the same as described in question 2. In addition to the mandatory and declaratory actions referred to in question 2, another type of action that may be relevant to the protection of personal data is the prohibition action. A prohibition action may only be filed if there is reason to believe that the respondent is going to take an administrative measure which will infringe the applicant's rights and those rights cannot be effectively protected by subsequently contesting the measure. A prohibition action may be filed without a time-limit. Compensation for the damage may also be demanded in the administrative court, and the time-limit for a compensation action is three years after the day when the applicant became aware or should have become aware of the harm and of the person who caused the harm.

However, if the rights are violated in a private law relationship, the Inspectorate only handles cases in which a fast intervention is needed and which are in public interest. The Inspectorate's refusal to initiate proceedings can be contested in the administrative court, but, as explained in question 2, the judicial control is limited.

In other cases, the person has to file an action with the county court (i.e. initiate a civil procedure). The judgment of the county court can be appealed to the circuit court and the judgment of the circuit court to the Supreme Court, but civil matters are normally heard by the Civil Chamber, so the Supreme Court does not play the role of supreme administrative instance.

4. Provide for a general overview of historical development of access to information rights in your jurisdiction while focusing on most important legislative and judicial milestones. Also, please try to generally describe the main driving forces behind the development of these rights.

Legislative milestones

The PIA was elaborated and enacted in order to implement the principle of free access to information provided in the Constitution of Estonia (§ 44). Prior the adoption of the PIA in 2000, no complex regulation providing access to public information existed. Until then requests for information were based on different specific laws. Until the adoption of the PIA the general procedure of granting access to information was unregulated. In addition, it was unclear what information could be restricted and what information had to be disclosed. The principle shortcoming lay in the fact that the grounds for classification of the information as "internal" were not regulated.

The first version of the PIA established the conditions of, procedure for and methods of access to public information, the bases for refusal to grant access to information and the procedure for the exercise of state supervision over the organisation of access to information. The elaboration of the PIA was based on the principle of social justice and democratic government founded on the rule of law as laid down in § 10 of the

Constitution of Estonia and aimed at enhancing transparent exercise of public authority. From the start the principle goal has been to grant easy and low-cost access to public information to anyone unless the law states otherwise.

Before the adoption of the PIA the general standpoint regarding the access to public information was that, unless stated in law, access to public information was restricted. With the adoption of the PIA this principle was reversed. The PIA is based on the principle that unless stated in law access to public information is granted.

In 2007 a chapter concerning the state databases was inserted in the PIA. This was the result of advancements of technology – almost all the information that results from the exercise of public authority is stored in databases.

The adoption of the law implementing the Directive 2006/123/EC on services in the internal market in 2009 resulted in supplementing the PIA with a provision on the Estonian information gateway (§ 32^1). The Estonian information gateway is a website allowing access to public information related to the fields of activities of holders of information and the public services provided by them, and allowing access to public electronic services and to reusable information.

In 2012 first provisions concerning the re-use of public information were adopted. The goal of the amendments was to bring the PIA in line with the principles laid down in the Directive 2003/98/EC on the re-use of public sector information.

As a result of the reform of the Estonian Law Enforcement regulation, amendments concerning the separation of state and administrative supervision (§ 44, § 45, § 50) were introduced into the PIA in 2014.

In order to reduce over-criminalisation, the PIA was amended in 2015 so that the provision stating that the failure to comply with the precept of the Data Protection Inspectorate constituted a misdemeanour was repealed.

Judicial milestones

In the case 3-3-1-57-03 (judgment of the Supreme Court, 23.10.2003), a legal person had asked a county's vital statistics department for access to the data concerning persons with a certain family name, as well as copies of archive data concerning specific persons. The purpose of the request was genealogy. The Supreme Court explained that a document may, at the same time, contain data with restricted access and data with no restrictions. If the grant of access to information may cause the disclosure of restricted information, it shall be ensured that only the part of the document to which restrictions on access do not apply may be accessed (§ 38 (2) of the PIA). Therefore, it is not legal to refuse to comply with a request for information simply because the document concerned also contains sensitive personal data.

Genealogical research is complicated, if not impossible without the use of documents held by vital statistics departments. A person's interest in genealogy is socially substantiated. The holder of information should weigh this interest with other persons' interest in protecting their privacy. If the scope of the request is unclear, the holder of information should aid the person making the request in specifying the request.

In the case 3-3-1-19-14 (judgment of the Supreme Court, 19.06.2014), the government of a municipality had made a request for information to a legal person in private law performing the public duty of providing a kindergarten for children living in the municipality. The municipal government requested access to accounting documents concerning all expenses financed by the municipality. The kindergarten refused to comply with the request, but the Data Protection Inspectorate ordered the person to comply with the request.

The Supreme Court agreed that the kindergarten was considered a holder of information, but only considering the information related to the performance of public duties. The accounting documents concerning expenses financed by the municipality are encompassed by the definition of public information. However, the Supreme Court explained that since the municipal government was also performing its public duties when requesting the information, the PIA was not applicable. The relationship between two public authorities is regulated by the Administrative Co-operation Act, according to which a request for information is considered a request for professional assistance. Thus, the municipality had based its request for information on the wrong legal basis and the Data Protection Inspectorate had no supervisory power in the case.

There is currently a pending case (3-3-1-90-14) in the Supreme Court concerning a journalist's request to the Chancellery of the Parliament for information about the recordings of the sittings of a committee of investigation of the Parliament (Riigikogu). The Chancellery refused to comply with the request because the sittings of the committee were closed and normally not recorded, and even if the sittings were recorded, the recordings were intended for internal use. The problem is that while the Riigikogu Rules of Procedure and Internal Rules Act provides that the committee sittings are closed, unless declared public, there are no rules about the access to the recordings of the sittings. The courts of first and second instance have decided in favour of the journalist.

5. Give basic subjective observation as to the role and importance of free access to information in political system of your country. In particular, focus on how the importance of freedom of information is perceived by general public and by non-governmental sector.

The underlying principle of the PIA is that access to public information is granted unless otherwise stated in law. The PIA states that the Chancellery of the Parliament, the Office of the President of the Republic, the Office of the Chancellor of Justice, the National

Audit Office, courts, government agencies, city and rural municipalities, and legal persons in public law are all required to maintain websites for disclosure of information. As the PIA puts the public institutions under the obligation to disclose information concerning their duties, people are used to consulting these websites. In certain situations fragmentation of data can pose drawbacks. Often websites of different institutions need to be consulted in order to solve a practical problem (i.e. in order to have the full review of requirements that need to be met when organising a public event with sale of food websites of local authorities, the Veterinary and Food Board and the Police need to be consulted).

Recently the "openness" of the Estonian Parliament (Riigikogu) has been publicly much discussed. The polemic was caused by the draft legislation initiated by the Parliament concerning the verbatim records and the minutes of Parliament commissions' sittings. The current Riigikogu Rules of Procedure and Internal Rules Act provides that minutes are taken of the sittings of Riigikogu committees. However, description on what needs to be recorded in the minutes is very brief. The draft legislation foresaw making the minutes of the sittings more detailed. To this end the committee sittings would be voice recorded. The draft legislation however also provided that verbatim records of the sittings will not be considered as documents to be archived and will only be stored until the expiry of the mandate of the Riigikogu. The plan of destroying the verbatim records of the sittings met strong public opposition. Due to public pressure the Parliament proposed that the verbatim records of sittings will be handed to the National Archive that is to decide what is to be stored and what can be destroyed. The Riigikogu proceedings for the adoption of the bill have currently been stayed as the bill has been withdrawn.

Taking into consideration the principles incorporated into the PIA, one could conclude that transparency is important to the general public as well as to the public institutions. However, events such as described above illustrate that despite the principles incorporated in laws the views of the general public and the politicians can at times and in certain questions strongly collide.

6. Give subjective general observation as to whether and eventually how free access to information rights are in practice abused or misused by the petitioners.

It can be stated that free access to information rights are in practice sometimes abused or misused. This is done intentionally as well as due to ignorance. Below are presented some examples of misuse or abuse of free access to information rights based on the experience of the Supreme Court's legal information department (listed in discretionary order):

1. A person submits requests for information that are too extensive, for example the person requests copies of all the acts the institution has issued.

2. There are also problems regarding similar content of the requests sent by one or several persons:

- A person submits requests with the same content to many institutions without specifying that the same request has already been submitted to tens of other institutions or that the request has actually already been answered by some other institution.

- A number of connected persons submit requests for information that have the same content. For example one prisoner submits a request to get copies of some documents that are quite extensive. When he/she gets the copies, other prisoners start to submit the same requests. In order to solve this problem, some documents have been forwarded to the prison libraries.

- In some cases requests for information that have the same content are submitted by the same person very frequently. If the request has been answered before then there is no obligation to give a full-scale answer again but if the content or the wording of the request has changed by a margin then it is difficult to say if it is still the same request. If it is considered to be another request (although almost identical to the previous request) it has to be answered again.

3. Sometimes questions are asked about general terms of language etc. For example in one request for information a question was asked: "What is homeland?"

4. The submitted applications are entitled with a wrong title to get the answer in a shorter period of time (there are different deadlines for answering different applications) regardless of the fact that a person has been informed several times that the title is incorrect and the deadline for answering is longer.

5. Sometimes a person submits the request in writing but after that calls and the answer is given verbally. But the obligation to give a written answer remains and if a written answer is not given, a complaint is frequently submitted.

6. In requests for information, people often ask for copies of certain documents – that is not a misuse or abuse of the right of access to information. However, when people request several copies of the same document (for example 20 copies) then it can be said that this is a misuse or abuse of right of access to information.

7. The right of access to information is sometimes misused by students: for example students have submitted requests for information to courts in which they want to know all the court decisions made concerning the topic of their thesis, although the decisions are available on public databases or the court's webpage with adequate searching capabilities.

8. Problems with misuse or abuse of the right of access to information sometimes occur from the fact that a prisoner has a right to submit requests/applications/etc to some institutions without a posting charge. Sometimes a prisoner writes to one of the mentioned institutions and asks to forward his/her letter to another institution (where he/she has to pay the posting charge). The institution that receives the request has an

obligation to forward the letter to the correct institution. So in this way it is possible to post requests everywhere for free, even if it is not the intention of the law.

9. It is possible a person submits several requests a day (for long periods of time) and then from time to time wishes to get a review of his requests, statistics or copies of requests and copies of answers to them. If a person has had for example over 1000 requests in one year then it is quite difficult to fulfil his/her claim.

7. Give a list and brief explanation of security, law enforcement and/or defence institutions that can benefit in your country from the exceptions laid down in Art. 7(e), Art. 8(4) and 8(5) of the Directive 95/46/EC.

The directive 95/46/EC has been transposed in the PDPA. The Act contains, *inter alia*, the general rules for the processing of personal data without the consent of the data subject in the course of performance of public duties. While processing the data, the administrative authority is required to adhere to the principles of processing personal data, including the principles of purposefulness and minimalism. The rights of a data subject to receive information and personal data concerning him or her upon the processing of the personal data is restricted if this may damage rights and freedoms of other persons, endanger the protection of the confidentiality of filiation of a child, hinder the prevention of a criminal offence or apprehension of a criminal offender, or complicate the ascertainment of the truth in a criminal proceeding.

Certain special rules for the processing of personal data are found in the Security Authorities Act[4] for the security institutions (the Estonian Internal Security Service and the Information Board). A security authority collects and processes information, including personal data, insofar as this is necessary for performing its functions. Information, including personal data, shall be collected, for the performance of the functions of a security authority, directly by the security authority or the authority authorised for such purpose or by a person recruited for co-operation. A security authority may, within the limits of its competence, restrict a person's right to the confidentiality of messages (via examination of a postal item or wire-tapping) in order to combat a criminal offence if there is sufficient information to indicate that a criminal offence is being prepared or committed. A person's right to the inviolability of home, and family or private life is restricted by, *inter alia*, collection of personal data, covert surveillance and collection of information on the fact, duration, manner and form of transmission of messages over an electronic communications network, and on the personal data and location of the sender or receiver of such messages. The restriction of a person's right to the confidentiality of messages or the covert entry into a building or other property for the purposes of covert collection or recording of information or installation of technical aids necessary for such purposes requires the administrative court's permission (granted for a period of up to two

[4] Available in English: https://www.riigiteataja.ee/en/eli/525062014010/consolide.

months or extended for the same period at a time). Other restrictions of a person's right to the inviolability of home, and family or private life are decided by the head of the security authority or an official authorised by him or her. The person whose aforementioned rights have been restricted shall be notified immediately of the measures used and the circumstances relating to the restriction if this does not endanger the aim of the restriction, or after such danger ceases to exist. The activities of the security authorities are supervised by a committee of Estonian parliament (Riigikogu).

The processing of personal data by the police is regulated in the Police and Border Guard Act[5]. For the adherence to the law, an international agreement or a legislation of the European Union, the police have the right to process personal data and transfer it to a foreign country. Usually this requires the consent of the person. The police also have the right to process personal data covertly, that means by concealing the purpose of the processing of personal data from the data subject. The following data may be processed covertly: the person's name, the route and destination of the person's trip, the persons in the accompany of the person or the persons travelling in a vehicle, ship or aircraft in whose case it is reasonable to assume that they are connected to the person concerned, the data on the vehicle, ship, aircraft or container used by the person and the items carried by the person. On the basis of the Code of Criminal Procedure[6], the Police and Border Guard Board, as well as the Security Police Board, the Tax and Customs Board, the Military Police and the Prisons Department of the Ministry of Justice and prisons may conduct surveillance activities on the following bases:

1) a need to collect information about the preparation of a criminal offence for the purpose of detection and prevention thereof,
2) the execution of a ruling on declaring a person a fugitive,
3) a need to collect information in confiscation proceedings,
4) a need to collect information in a criminal proceeding about a criminal offence.

Surveillance activities may be conducted with a written permission of the Prosecutor's Office or a preliminary investigation judge. In cases of urgency, the permission may be issued in a format which can be reproduced in writing, with the written permission formalised within 24 hours as of the commencement of surveillance activities. Normally, the person with respect to whom the surveillance activities were conducted and the person whose private or family life was significantly violated by the surveillance activities and who was identified in the course of the proceedings needs to be notified upon expiry of the term of permission. The notification is not needed if this may significantly damage the criminal proceedings or the rights and freedoms of another person, or endanger the confidentiality of the methods and tactics of a surveillance agency, the equipment or police agent used in conducting surveillance activities, of an undercover agent or person

[5] Available in English: https://www.riigiteataja.ee/en/eli/520012015012/consolide.
[6] Available in English: https://www.riigiteataja.ee/en/eli/520012015017/consolide.

who has been recruited for secret cooperation. The non-notification requires the permission of the Prosecutor's Office or, upon expiry of one year as of the expiry of the term of the permission for surveillance activities, the permission of a preliminary investigation judge. Both the permission for surveillance activities and the non-notification may be appealed.

Estonian Defence Forces Organisation Act, Taxation Act, Weapons Act, Strategic Goods Act, Customs Act, Witness Protection Act, Security Act, Imprisonment Act, Aliens Act and Obligation to Leave and Prohibition on Entry Act also give bases for the processing of personal data.[7] The Defence Forces conduct military intelligence and have the right to process data for that purpose. The other acts mostly specify the processing of data on the basis of the Code of Criminal Procedure by law enforcement authorities in specific domains and background checks of potential employees or persons applying for permits.

In addition, the Ministry of Justice is currently working on the draft for an act concerning the security clearance and the conducting of background checks.

There has also been a recent case in the Supreme Court concerning the processing of data in a criminal proceeding (3-3-1-11-13; judgement of the Supreme Court, 22.03.2013). In criminal proceedings against a well-known politician due to the suspicion of money laundering, the prosecutor had made a request for international legal assistance to the Swiss Confederation, asking for information from the Swiss Banks. The person brought an action to the administrative court, asking the court to prohibit the processing of data by the prosecutor, to order the prosecutor to withdraw the request for legal assistance and to refute the incorrect allegations. The Supreme Court found that the procedural acts of the prosecutor can be contested in criminal proceedings, and therefore, the administrative court is not competent to adjudicate this type of disputes. Even though the applicant claimed that his purpose was not directed toward the ends of the criminal proceedings, but to protect his personal data, privacy and reputation, the Supreme Court explained that the competence of the administrative court does not depend on the purpose of contesting the procedural acts, but on the nature of the acts. The rights referred to by the applicant also have to be protected in criminal proceedings.

8. Subjectively identify most emerging actual problems that arise from processing of personal data by aforementioned security, law enforcement and/or defence institutions. Whenever appropriate, demonstrate them on particular examples.

1. The most acute problems concerning the processing of personal data are related to surveillance activities.

The first issue that arises is the justification of permissions granted for conducting surveillance activities: in particular, whether the principle of *ultima ratio*, which requires

[7] All these acts can be found in English on the following website: https://www.riigiteataja.ee/en/search.

that permission for surveillance should only be granted as a last resort, is duly followed in practice. To illustrate the potential problem, periodically published official statistics show that on average courts refuse to grant permission in less than 1% of the cases where it is applied for. The legal requirements and necessary preconditions for the grant of such permissions have been thoroughly dealt with and explained in the case law of the Supreme Court. In the great majority of cases the decision of a court of first instance to either grant or refuse to grant the permission is indeed justified. Nevertheless, from time to time the Supreme Court still has to decide cases where the permission has been granted unfoundedly, i.e. without all the relevant conditions and criteria being met (or, at least, appearing not to be met on the basis of the court's order).

Secondly, there have been problems regarding notification of the subjects of surveillance activities. It is often unclear what is the time limit in which a person should be notified that he or she has been subjected to surveillance activities, in which circumstances and for how long can this notification be deferred, how the justification of such deferral should be supervised, etc. These uncertainties are especially strong in connection with surveillance activities which were conducted before a significant legislative reform on surveillance in 2013. For example, there is a lack of effective supervision over deferral of notification in cases, where the surveillance activities took place before the year 2013, and a) the conduct of surveillance activity did not need the permission of the court, but the permission of the Prosecutor's Office; or b) where the information collected through surveillance was not used as evidence in the proceedings and is therefore not included in the criminal file.

Apart from the persons directly subjected to surveillance, problems of notification arise with regard to third persons who should also be informed about the fact that they have been involved in a surveillance activity. At present, the law requires third persons to be notified only if they have been "identified in the course of the proceedings" and their rights have been "significantly" violated. It is not clear how these criteria should be interpreted and applied in practice (including how far one should go with the attempt to identify third persons, when are their rights "significantly" violated, etc.). It is also arguable whether the law is sufficiently clear to ensure that the legitimate interests and rights of third persons are duly protected.

Problems also arise in connection to the storage of the data collected by surveillance activities: for how long and for what purposes should it be allowed to store this data, considering that storage of such potentially sensitive information may violate a person's legitimate interests and fundamental rights. At the moment effective control over whether the storage of the data is legitimate and purposeful might be lacking.

2. Another topical issue is the declaration of invalidity by the Court of Justice of the European Union of the data retention directive (2006/24/EC) (cases C-293/12 and C-594/12). Since the legislation which implemented the directive continues to be in force in

Estonia, its constitutionality is unclear. This question indirectly arose in a recent case before the Supreme Court (case no 3-1-1-51-14). Although the Criminal Chamber did not provide a complete analysis of, nor a clear answer to this question in its judgment, attention was drawn to the problem in dissenting opinions which emphasized the need to assess the constitutionality of the relevant data retention regulation as a whole.

3. A practical problem has also been misuse of access rights to registers and databases which contain personal and/or sensitive information. There have been cases where public officials have used data obtained from these sources for personal purposes. The majority of these cases concern police officials who have made queries in the police database (e.g. for a person's phone number or for identifying the person using a particular phone number) and forwarded the results to an acquaintance. A potential source of the problem is that officials have been granted too broad access rights, including to information which they actually do not need. This problem is effectively being dealt with by strengthening internal control and supervision over the use of registers and databases.

4. One of the problems currently actual in the administrative court system is the use of data gained from secret sources as evidence to issue an administrative act (or a court judgment) to the detriment of a person, while not allowing the person to examine the evidence. This has occurred in several cases concerning prisoners (the data being collected by the prison's security department), but the most recent case (appealed to the Supreme Court, but proceedings were not opened) concerned a residence permit. The residence permit's reasons included the explanation that the addressee of the act was considered as a threat to national security, but that the data the allegation was based on was classified as state secret. The relevant data was sent to the court, but kept in a separate court file and only examinable by the judges (i.e. not by the applicant). There is a legal basis for this in the Code of Administrative Court Procedure, limiting the removal of the participant of the proceedings from a procedural act to the smallest extent possible. The court discloses the content of the procedural act to the participant to the maximum extent which is possible without prejudicing the purpose of the removal. If it is inevitably necessary, the court may give the participant in the proceedings access to the evidence in question. The circuit court considered that in this case, the public interest for protecting the state secret outweighed the applicant's right to participate in the proceedings. However, the court considered it necessary to examine the evidence and control the reasonableness of the classification of the data as secret in each instance.