YEARBOOK OF ESTONIAN COURTS 2015

YEARBOOK OF ESTONIAN COURTS 2015

Editor: Margus Mõttus
Translated by Luisa Translation Agency
Published by the Public Relations Department
of the Supreme Court of Estonia
Printed by Dada

Contents

Foreword

"Ladies and Gentlemen of the Jury,"

These seem to be the appropriate opening words for the Yearbook of Estonian Courts 2015. This time the focus of the Yearbook is on criminal procedure with special emphasis on surveillance operations. Articles on surveillance provide the reader an opportunity to put themselves in judge's shoes– former Chief Justice of the Supreme Court Mr. Uno Lõhmus and attorney-at-law Mrs. Küllike Namm point to shortcomings in the system of judicial review of surveillance and criticise the scarce and ambiguous legal provisions that allow too much free rein to public authorities in conducting surveillance operations. Their claims are refuted by prosecutor Mr. Aro Siinmaa who insists that prosecutors and judges strictly observe the principle of *ultima ratio* and that applications for surveillance operations are filed with judges only in the cases where surveillance is absolutely indispensable. Having heard the arguments of both sides it is for the reader to decide whether to agree with the prosecution or the defence.

I would like to extend my sincerest gratitude to all the authors, members of the editorial board and the managing editor for the time and energy they devoted to the Yearbook.

I wish you, dear colleagues, a pleasant reading of the Yearbook!

Priit Pikamäe
Chief Justice of the Supreme Court

1
Yearly summaries

Development of legal and court systems

Report delivered at the Plenary Meeting of Judiciary held on 12 February 2016 in Tallinn

***Dr. iur.* Priit Pikamäe**, Chief Justice of the Supreme Court

Dear Colleagues and Guests,
Members of the Parliament, and
Minister of Justice,

Honouring traditions, I begin with acknowledgments to those judges emeritus who have deemed it important to participate in the work of the Plenary of Judiciary even after leaving the service. I am very happy to note that, as usual, many of our former colleagues are attending the Plenary Meeting and thus cherishing their lasting ties with the judicial system even after retirement.

We are gathered today in the Plenary of Judiciary, which is the fifteenth regular plenary meeting in the Estonian history – it is almost a jubilee. Therefore, there is reason to take a look at how the self-government of judiciary has operated so far and also to consider possible developments of our judicial system in the near future. To begin with history, it must first be noted that the Courts Act, which was adopted by the Parliament on 19 June 2002, entered into force on 29 July of the same year and is still in place today, was one of the reform laws – in the best sense of the word – passed at the beginning of the last decade. The entry into force of the Courts Act ended a long process designed to replace the fragmented judiciary-related legal acts of the transition period with a more comprehensive piece of legislation that takes into account the developments of our own judicial system, as well as current international trends. In a situation where mass replacement of laws has become a standard and the development of the legal system has become hyperdynamic, the year of publication of a law is an indication of its quality. Indeed, the Courts Act has stood the test of time and proved its viability in every way. Although the Courts Act has meanwhile undergone some major and minor amendments, the text of the Act as a whole has retained its original principles. While a number of the amendments were regarded as fundamental changes back in 2002, they have now become an integral part of the judicial system, so that one cannot even imagine that courts could work in some other way. Examples include, among others, the introduction of the full

court as an administrative body in every court, and the division of tasks plans as the basis of distribution of work within a court.

The Courts Act of 2002 is the birth certificate of the Plenary of Judiciary and self-government organisation of judges. Paraphrasing the Constitution's clause that provides guarantees to local authorities, we could say that all matters related to the judiciary are determined and administered by judges' self-government bodies, which discharge their duties autonomously in accordance with the law. The Plenary of Judiciary, which for the first time convened in the Assembly Hall of the University of Tartu on 5 September 2002, certainly holds the central place among the self-government bodies created by the Courts Act. The venue of the plenary meeting was appropriately chosen, considering the significance and solemnity of the event – after all, it was the first time in the history of the Estonian judicial system that the right to decide on the key issues of the judiciary was transferred to the Plenary representing the judiciary as a whole. The Plenary legitimises the activities of the more specific bodies within the judiciary – the Council for Administration of Courts, the Judges' Examination Committee, the Assistant Judge Competition Committee and the Judicial Training Council. The 15-year anniversary of the tradition of holding the Plenary of Judiciary is thus very significant and all the more valuable for the history of our judicial system as such a self-government right of the judiciary was not provided for in the first Courts Code of Estonia adopted in 1938. The experience so far confirms that the role of the Plenary is, however, more than just electing the members of the judiciary's self-government bodies. Plenary of Judiciary is the place to discuss the most important issues related to the administration of justice and has the important task of reinforcing collegiality within the judiciary. While in terms of procedural law each judge adjudicating a case acts within the limits of the powers conferred on judges in a particular court instance, the Plenary represents the judiciary as a sum of individual administrators of justice, and has the task to stand for the common interests of the third independent branch of government. Collegiality of judges is not, therefore, a mere slogan used in anniversary speeches, but a reality expressed through the Plenary.

However, the right to self-organisation through the self-government system implies the obligation to also assume the accompanying responsibility. This means, first of all, the obligation to foresee the consequences of one's decisions in the long run. It should also be borne in mind that, typically of the system of representative democracy, decisions of the self-government bodies of judges bind the judiciary as a whole. The impact of the various self-government bodies on the judicial system definitely varies in weight, but it should not be underestimated in any event. For example, the Judges' Examination Committee plays a significant role in shaping the future composition of the judiciary, especially in the current period of a major generational change within the judiciary. On the

other hand, the word 'self-government' implies that all judges should assume an additional duty to participate, where necessary, in the activities of a self-government body in addition to their daily work for no additional compensation. This is an issue that points to some self-government fatigue, at least when looking at the electoral lists of the bodies. While the number of candidates for posts in the Council for Administration of Courts as the most popular self-government body is by far the highest, there are also bodies that are lucky when at least one candidate is nominated from each court instance.

It should be remembered that even the most independent and self-organising judiciary does not operate in a vacuum. The judicial system cannot ignore, in particular, demographic processes, but neither can it ignore economic and other processes that affect the society as a whole. Unfortunately, the decline of the population of Estonia continues to be the bitter truth. To be honest, our population projections are rather bleak in the longer run. According to the population projection published by Statistics Estonia in 2014, the population of Estonia is estimated to decline by 4% by 2025 and by around 10% by 2040. Specialists estimate that in the more distant future, or over the next thirty years, the population of Estonia will decrease by a total of 125,000 people if the current trends of decline and negative migration balance persist. This number is almost equal to the total number of people currently living in Tartu, Võru and Rakvere. According to the population projections of the UN, there will be only 0.9 million people living in Estonia in 2100. Statistics Estonia has also pointed to the constant internal relocation of people within the country. We need to realise that the same demographic processes that have already triggered the consolidation of the school network and the administrative-territorial reform will soon begin to affect other areas of our statehood, including the judicial system. In view of this, a discussion on appropriate locations of courthouses is probably inevitable in the near future. When shops, schools, post offices, jobs and hence also people disappear one after another not only from rural areas but also from small towns, it is clear that ultimately there will be no one left for whom justice could be served. Of course, there will always be the regional policy aspect of the problem, i.e. the question of how the government should combat the marginalisation of certain regions, and to what extent. Any regional policy measure has, by definition, a financial dimension, which means that certain state functions are deliberately maintained even in the regions where this might not be completely reasonable in financial terms. Also, it should not be forgotten that even when setting regional policy aside we have regions in Estonia where the presence of public authorities, including the judiciary, is strategically necessary. Should the decision to prepare plans for reorganisation of the judicial network be taken, however, such plans should not – for constitutional considerations – be reduced to trivial closure of regional offices, as has already happened with state institutions on several occasions. Section 15 of the Constitution provides

for everyone's right of recourse to courts. Consequently, the legislative and executive powers have a responsibility to ensure that everyone has access to justice. The latter is not reducible to the ability to use a computer at a public Internet access point, whose continued operation in rural areas is a small miracle, but real access to justice must be literally guaranteed to everyone whose subjective rights have been violated. Therefore, development of the criteria of access to justice is an indispensable precondition for any geographical restructuring of the judicial network. Such an analysis has to be specific to the right of recourse to courts, as the relevant experience of other sectors can hardly be transferred to the administration of justice.

Considering the trends that I have described, one has to agree with one of the main directions of the public administration policy developed by the Government of the Republic, which consists in the reduction of the total number of people employed in the public domain in sync with the overall decline in the population. Thus, the number of people who contribute to the gross domestic product which is necessary for sustaining the state apparatus is shrinking. Against the backdrop of the concurrent aging of the population, this means that while at present there are 54 dependents per 100 working-age people, the number of dependents will grow to 70 by 2040. The plan for reduction of the number of civil servants also concerns the judicial system. According to the figures provided by the Ministry of Justice to the Council for Administration of Courts last year, it is intended to limit the number of people employed in the first and second instance courts to one thousand persons. The reduction of the number of public sector employees will also affect constitutional institutions, including the Supreme Court.

While these propositions, which are based on empirical data, can be upheld in theory, the devil is in the details. From the judiciary's point of view, one of the problematic aspects of the plan proposed by the Government of the Republic relates to the unjustifiably different treatment of the different branches of government. For example, the quota of one thousand people set for the judicial system in the coming years will include both judges and other judicial personnel. The judiciary is the institution that directly exercises judicial power, just as the Parliament exercises legislative power through the activities of the members of the Parliament, and the Government of the Republic exercises the executive power through the activities of the members of the Government. Since it is hard to argue against this view, one has to admit that in a situation where in the case of the Parliament and the Government of the Republic the staff reduction will only involve downsizing the administrative apparatus, while in the judicial system the reduction will also concern judges, the plan in question does not treat the branches of government equally. While no reasonable justification can be found for the establishment of different standards for the judicial branch, I

believe that judges should be considered a separate group of civil servants and they should not be included in the quota set for the judicial system. It should also be noted that, if the number of cases remains unchanged or increases, a reduction of the number of judges will automatically result in an increase in the workload of judges and in the longer duration of proceedings, i.e. it will ultimately impair access to justice. Indeed, it has already been pointed out in the public domain – and rightly so – that a reduction of the number of civil servants can only follow, not precede a critical review of the volume of tasks performed by the public sector. In the judicial system, this could happen as a "natural process", i.e. by people giving up the right of access to courts or, alternatively, in the form of a deliberate revision of the tasks currently imposed on courts. The latter approach could include the establishment of alternative dispute resolution methods, decisive reassessment of the rights of appeal, or alteration of the procedure under which court cases move between different court levels. There may be reason to also consider assigning some duties to bodies outside the judicial system in issues that are not directly related to the administration of justice.

Simultaneously with these developments, however, a much larger opposite trend can be observed, which will increasingly bring new cases to courts. I will mention only two major changes that will have to take effect later this year according to the will of the legislature. The first of them concerns civil proceedings and the other criminal proceedings. As you know, the Parliament decided on 6 May last year to amend the Constitution so that, in the future, in elections to local authority councils, the right to vote is held by persons who have attained at least sixteen years of age. This amendment was explained by the need to bring more issues affecting young people into social focus and to improve the demographic balance in the electorate. From the perspective of legal practice, this amendment also means that the current paradigm can no longer serve as the basis for divesting a person of the active legal capacity with regard to the right to vote. Currently, a person is considered to lack the active legal capacity with regard to the right to vote if a guardian has been appointed for management of all of his or her affairs. However, when the constitutional voting age is lowered, a brand new procedure will have to be created within the civil procedure that would allow courts to assess whether a 16-17-year-old person can sufficiently understand the significance of the vote in elections to the local authority council.

The other example concerns the legislative changes aimed to strengthen the protection of fundamental rights in criminal proceedings, which have been extensively discussed in the public and which the Parliament approved on 18 February 2015. The explanatory memorandum states that the entry into force of the draft Act on 1 September this year will affect the work of courts the most, as the right to authorise many procedural acts that have the potential of infringing fundamental rights will be transferred from prosecutor's offices to courts.

The authorisation of searches alone is estimated to increase the workload of courts by 956 new cases that would be decided by preliminary investigation judges. It is also quite rightly noted in the explanatory memorandum that since courts must be able to verify the legality of searches even in time-critical situations, the implementation of the draft Act requires changes in the organisation of the work of preliminary investigation judges to avoid situations where the judge is also involved in hearings at the same time. As a practical consequence for the judicial system of the amendments introduced to provisions on taking a person into custody, the explanatory memorandum estimates that there will be 1849 additional court sessions.

The two draft Acts described above illustrate the yawning abyss between the different policies in our country. On the one hand, an objective is set to reduce the number of personnel involved in the judicial system, while on the other hand, legal provisions are devised whose impact analyses state the dry fact that even the existing personnel is not enough to implement these large-scale amendments to the law. Obviously, there is no disagreement that young people should be more involved in public affairs and that the protection of fundamental rights, in particular in criminal proceedings, needs special attention. Of course, the number of cases is not constant over time, but rather a figure whose up-and-down movement resembles an encephalogram. The problem is that, as regards the judicial system, the public administration policy pursues several different and mutually exclusive goals simultaneously. It seeks to reduce the number of people involved in the administration of justice, while significantly increasing the scope of judicial functions. The whole situation is rendered especially mind-boggling by the fact that the impact analyses and budget processes relating to the explanatory memoranda to the draft Acts adopted by the Parliament appear to be originating from parallel universes. Common sense would tell that, if the Parliament has passed an Act whose cost of implementation in respect of the judicial system is estimated to amount to half a million euros according to the thorough calculations of the body initiating the adoption of the Act, then this additional cost should be taken into account in the budget procedure. The reality, however, has less to do with common sense. Thus, for example, the Ministry of Justice managed to narrowly secure the additional funding required for the implementation of the amendments to the Code of Criminal Procedure coming into force on 1 September for the last four months of this year, while further funding is completely unclear. I am of the view that if funding of the implementation of these amendments proves impossible, the legislature will probably have to return to the criminal procedure-related amendments that should take effect on 1 September this year.

Then again, it would be improper to say that politicians have always utterly disregarded the resource needs of courts. As I have stressed earlier, the introduction

of the institution of judicial clerks during the period 2013–2015 has been the most significant investment in the human resources of courts in recent history. It should be recalled that it was based on the indubitable objective of offering extensive judicial protection to everyone, while ensuring a reasonable duration of proceedings. In light of this, the movement in the opposite direction, by planning staff redundancies in the judicial system, seems even stranger now. Can there be a better example of the chaotic nature of our public administration?

Let me conclude this sub-theme by stating that the judicial system – as any other organisation – is capable of performing its tasks within the limits of the resources allocated to it. In public debates, including in parliamentary procedure, one can often hear voices saying that the court will have a final say in solving one or another matter of dispute. This attitude demonstrates the great trust of society in the third power, and it is, indeed, the task of the judicial system to settle disputes. On the other hand, the right of recourse to courts is only illusory if the judiciary is deprived of the resources that it needs to deal with the complaints submitted to it. Considering the risk of loss in effectiveness, the "consolidation" of the state cannot be limited to the number of people employed in the public sector, but should also concern the functions performed by the public sector. The effectiveness of the judicial system determines the extent to which fundamental rights are protected, as well as the economic environment of Estonia in general. I would point out that international comparisons of the attractiveness of economies include the guaranteed right of everyone to assert their claims in court as one of the main indicators for the situation of investment opportunities in the country. Therefore, I strongly feel that any staff reductions in the judicial system must be preceded by a review of the tasks performed by courts. Since the administration of the first and second instance courts is organised by the Ministry of Justice in collaboration with the Council for Administration of Courts, any structural rearrangements in the judicial system should first be discussed with the Council for Administration of Courts. Obviously, supporting the changes planned in the judicial system can be considered only on the condition that the budgetary funds saved as a result of those changes will remain at the disposal of the judicial system.

I would like to finish, however, on a completely different note. The venue of today's meeting is the creative hub "Kultuurikatel" (Culture Cauldron). The name consists of two parts – 'culture', for which there is an indeterminate number of definitions, and 'cauldron', the main functions of which are known to include heating, mixing and combining. There can be no doubt that the administration of justice is an example of a cultural phenomenon. Despite this, the judiciary has only rarely been concerned with placing its main task – the administration of justice – in a broader cultural context. Now that we are in the Culture Cauldron, we should not miss this intriguing opportunity. As we know, the administration

of justice is a constantly evolving phenomenon in the general development of culture and the search for compromises based on negotiations is the current trend in trials. These days, a good judicial proceeding ends with an agreement between the parties, rather than a court judgment. In this regard, history keeps repeating itself and everything new is the well-forgotten old.. While in the Middle Ages state authorities worked hard to uproot parties' agreements from the criminal process and replace them with the public trial against the offender, the modern state makes every effort to avoid the court hearing through the reconciliation of the offender and the victim. Keeping such twists and turns of history in mind, one can only hope that the zeal for reviving ancient practices will not affect the procedure for appealing against judicial decisions. Namely, in the time of chivalry one way to appeal against a judgment made in the criminal process was to challenge the judge, and if the judge lost the duel then the judgment handed down by him had clearly been wrong and hence Divine justice was established!

Thank you for your attention. I wish everyone a successful continuation of the Plenary!

2
Criminal procedure and criminal law

Supervision over surveillance

Uno Lõhmus, Visiting Professor at the University of Tartu

Modern technology has created enormous opportunities to obtain data on people and their behaviour and to process these data. Some of the data are disclosed or made available by people themselves, either deliberately or out of carelessness. The means and methods offered by technology are also used by intelligence and law enforcement agencies to perform their tasks. The term 'surveillance' refers to activities which these agencies carry out covertly, without the knowledge of the person subjected to the surveillance. In the European legal space, covert surveillance of citizens and collection of evidence is a permissible means of prevention or detection of crime, provided it is a proportionate measure used for the purpose of ensuring national security and public safety. The development of surveillance means and the admissibility of their use should be accompanied by the development of legal regulation providing for adequate and effective guarantees against abuse of powers.[1] Otherwise, fundamental rights, especially the right to confidentiality of communications, privacy and inviolability of home will become mere slogans.

The following analysis is limited to a few aspects of surveillance. I am going to focus on the review of those surveillance operations that are conducted for the purpose of detecting the preparation of or preventing criminal offences, and for the purpose of establishing criminal offences in criminal proceedings. I believe that the supervision of surveillance operations conducted for these purposes is subject to similar requirements.

1. Standards arising from international law

The principle of legality requires that any interference of the executive power with the fundamental rights of a person must be subjected to effective supervision, which is usually assured – at least in the last resort – by the judiciary. According to the standards established by the European Court of Human Rights (ECtHR), judicial supervision, due, due to its independence, impartiality and

1 ECtHR 06.09.1978, Klass and others v. Germany, p. 50.

procedure, offers the best quarantees in a field where abuse is potentially so easy and could have harmful consequences for democratic society as a whole.[2]

Supervision is exercised over surveillance in three stages: (1) at the time when the decision to commence a surveillance operation is taken, (2) at the time when the surveillance operation is conducted, and (3) after the completion of the surveillance operation.

Given the secret nature and logic of surveillance, in the first two stages a surveillance operation and the supervision of its legality take place without the knowledge of the person concerned. Since the person who is the subject of the surveillance operation cannot use any legal remedies or take part in the supervision, it is therefore essential to ensure that the supervision of surveillance provides adequate and effective guarantees safeguarding the person's rights in these stages.[3] According to European standards, supervision over surveillance should be exercised by an independent authority or public official. The practice of the ECtHR gives rise to the requirement that an authority which authorises a surveillance operation must be an independent authority, normally a court, an authority which is subject to judicial review or an authority which is subject to supervision by an independent authority.[4] The requirement that an authorisation should be granted by an independent authority, normally a court, is a rule, and any other options are an exception.[5]

What other options can there be? The ECtHR has held that an *ex ante* judicial authorisation of a surveillance operation is not an absolute requirement *per se*, if there is *post factum* judicial oversight which may counterbalance the shortcomings of the authorisation process.[6] In so stating, the Court of Human Rights had in mind the specific rules and legal practice of the United Kingdom.[7] Since the law and practice of the United Kingdom can be classified as an 'other option' i.e. an exception, the rules applicable in the United Kingdom should be briefly explained in order to understand the position of the ECtHR. In the United Kingdom, interception of communications is governed by the Regulation of Investigatory Powers Act 2000 (RIPA). Practical recommendations are given in The Interception of Communications Code of Practice. The interception of com-

2 ECtHR 12.01.2016, Szabó and Vissy v. Hungary, p 77.

3 See ECtHR 06.09.1978 (reference 1) p. 55; ECtHR 04.12.2015, Roman Zakharov v. Russia, p. 233.

4 ECtHR 26.04.2007, Dumitru Popescu v. Romania (no. 2), p. 70–73.

5 ECtHR 12.01.2016 (reference 2), p. 77.

6 Ibid.

7 See ECtHR 18.05.2010, Kennedy v. The United Kingdom.

munications is authorised by the Secretary of State, if it is necessary (a) in the interests of national security, (b) in order to prevent or detect a serious offence, or (c) in order to protect the economic prosperity of the United Kingdom. Thus, in the United Kingdom, surveillance operations are not authorised by courts, but by a high-ranking official representing the executive power. However, the authorisation and conduct of surveillance operations are subject to review by an independent public official appointed by the Prime Minister – the Interception of Communications Commissioner. A person who holds or has held a high judicial office may be appointed to that office for three years. The Interception of Communications Commissioner is required to annually submit to the Prime Minister a report on mistakes made in the conduct of surveillance operations. The Prime Minister will submit the report to the Parliament. In addition to the Commissioner, there is the Investigatory Powers Tribunal whose members must hold or have held a high judicial office or be a qualified lawyer of at least 10 years' standing. It is important to emphasise that anyone who suspects that his or her communications have been tapped may bring a complaint before the Tribunal. The Tribunal is required to consider each complaint, and it has access to all confidential documents and the right to request the Commissioner to provide clarification and assistance. The Tribunal has the power to revoke authorisations of surveillance operations, to require the destruction of intercepted material and to award compensation for violations of fundamental rights.

In the recent case law, the ECtHR has pointed to two important aspects of the review of authorisation of surveillance operations. First, persons granting the authorisations should be capable of verifying the existence of a reasonable suspicion against the person concerned. Applicants for authorisations should present the factual indications for suspecting the person of planning or committing an offence.[8] Second, persons granting the authorisations should assess whether the surveillance operation is necessary in democratic society, i.e. whether the desired result could be achieved by less restrictive means.[9]

The ECtHR also recommends subjecting the second stage, i.e. the conduct of a surveillance operation, to judicial review. Supervision exercised by an authority other than a court is compatible with the Convention when two conditions are met. First, the supervisory authority should be independent of the authority conducting the surveillance operation, and second, the supervisory authority should be vested with sufficient powers and competence to exercise effective control.[10]

8 ECtHR 04.12.2015 (reference 3), p. 260.

9 Ibid.

10 Ibid., p. 275.

After a surveillance operation has been completed, notification of the person about the surveillance operation will determine whether the person will be able to effectively defend his or her interests in court and contest the operation which the person considers to be unlawful. If a person is not informed about surveillance, or if no legal remedy is available to a person who suspects a surveillance operation, the person has only limited opportunities to protect his or her rights. If the person is not notified about the surveillance operation, the effectiveness of a legal remedy will depend on whether the legal system provides for *post factum* review of the surveillance operation irrespective of the will of the person.

2. Estonian law and practice

2.1. Who is competent to authorise surveillance operations?

In Estonian law, the granting of authorisations for surveillance operations is entrusted to prosecutor's offices and preliminary investigation judges. The authorisation of a preliminary investigation judge is required for covert examination of postal items (section 126^6 (5) of the CCP), for wiretapping or covert observation of messages transmitted by a public electronic communications network or information communicated by other means (section 126^7 (3) of the CCP) and for staging a criminal offence (section 126^8 (3) of the CCP). The authorisation of a preliminary investigation judge is also required for covert entry into a building, premises, vehicle, enclosed area or computer system for the purpose of conducting a surveillance operation or installing or removing technical means necessary for surveillance (section 126^4 (5) of the CCP). The wording of the law suggests that the legislator does not consider the covert entry in these places and the installation of technical means there to be a surveillance operation, but rather the creation of the necessary conditions for the conduct of an operation. In addition, the case law does not clarify whether the installation of spyware in a computer system should be regarded as the installation of a technical means. Since the installation of spyware in a computer system and the collection of data with its help significantly infringe the fundamental rights of privacy and confidentiality of communications, such an operation should be permissible only under the authorisation of the court.

In other cases a surveillance operation may be conducted under the authorisation of a prosecutor's office. As of 1 January 2013, examination of traffic and location data in electronic communication is not considered to be a surveillance operation.

In the case of authorisations issued by courts, the law refers to preliminary investigation judges and in the case of authorisation by prosecutor's offices, the law

points to that particular authority. According to an interpretation of the Supreme Court, surveillance operations may also be authorised by assistant prosecutors.[11]

In the light of the principles developed by the Court of Human Rights, the conduct of surveillance operations under the authorisation of a prosecutor's office is not completely unproblematic. The reasons are as follows. First, the law imposes contradictory duties on prosecutor's offices. On the one hand, a prosecutor's office exercises oversight over the compliance of surveillance operations with the authorisations which are granted by courts or by the prosecutor's office itself (section 12615 (1) of the CCP). The Prosecutor's Office Act[12] entrusts prosecutor's offices with the task of ensuring the legality of pre-trial proceedings (sections 1, 4 and 5 of the POA). On the other hand, prosecutor's offices participate in the planning of surveillance necessary to combat and detect criminal offences, and direct pre-trial proceedings (sections 1, 4 and 5 of the POA). Prosecutor's offices are required to ensure both the legality and effectiveness of the activities of surveillance agencies.[13] When a prosecutor's office directs pre-trial proceedings and has to ensure their effectiveness, it is interested in the collection of evidence that will help take the accused to court. Surveillance provides effective means for collection of evidence. The prosecutor's office has a difficult if not impossible task to consider whether the interference with fundamental rights is a proportionate measure. Furthermore, the law grants a wide margin of discretion to prosecutor's offices in conducting surveillance operations.

Secondly, according to the ECtHR, there is no contradiction with the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) if a surveillance operation is authorised by an authority which is not a court, provided that the authority is sufficiently independent of the executive power.[14] The ECtHR did not consider the Romanian Prosecutor's Office to be independent of the executive power, since prosecutors have a relationship of subordination with the Prosecutor General and the Minister of Justice.[15] While the Prosecutor's Office Act declares the independence of prosecutor's offices and prosecutors (sections 1 (11) and 2 (2)), prosecutor's offices are government agencies within the area of government of the Ministry of Justice, which exercises

---

11 Although surveillance operations undoubtedly restrict the rights of persons subjected to surveillance, there is no reason to take the view that these operations differ from other procedures performed in criminal proceedings, which infringe fundamental rights, to such an extent as to preclude the authorisation of surveillance operations by assistant prosecutors" (ruling of the Criminal Chamber of the Supreme Court, 15.06.2015, 3-1-1-49-15, p. 17).

12 RT I, 10.03.2015, 17.

13 See section 20 (4) of the Statutes of the Prosecutor's Office, RT I, 01.04.2015, 4.

14 ECtHR 26.04.2007 (reference 4), p. 71; ECtHR 04.12.2015, p. 258.

15 ECtHR 03.06.2003, Pantea v. Romania, p. 238.

supervisory control over them (section 9 (1)).[16] According to the Government of the Republic Act,[17] government agencies are accountable to the Government of the Republic, to a relevant minister or to the State Secretary, who directs and coordinates their activities and exercises supervisory control over them pursuant to the procedure provided by law (section 41 (1)).

Prosecutors are subject to supervisory control (section 9 (2)). The procedure for appointment of prosecutors to office (section 16 of the POA), the appointment of the majority of prosecutors to office for an indefinite term (section 17 of the POA), the procedure for initiation of disciplinary proceedings against a prosecutor (section 32 of the POA), hearing of prosecutors' offences (section 36 (1) of the POA) and imposition of disciplinary penalties (sections 41 and 42 of the POA) call the declaration of prosecutors' and prosecutor's offices' independence into question. In this context, the right of chief state prosecutors to issue orders to district prosecutor's offices and the duty of chief prosecutors to account for the activities of the district prosecutor's offices to the Prosecutor General and to chief state prosecutors under the Statutes of the Prosecutor's Office (sections 15 and 22) are also worth mentioning.

2.2. Scope of supervision by persons granting authorisations

According to the Code of Criminal Procedure (CCP), the following requirements have to be met when granting authorisations:

A. Substantive requirements:

1) it is permitted to conduct surveillance operations in respect of a person (a) in the case of whom there are serious grounds for believing that he or she will commit a criminal offence; (b) who is a suspect; (c) in the case of whom there are serious grounds for believing that he or she has committed a criminal offence; (d) in the case of whom there are serious grounds for believing that he or she interacts with a person who is a suspect or in the case of whom there are serious grounds for believing that he or she has committed or will commit a criminal offence (section 126^2 (3) and (4) of the CCP);
2) an authorisation may be granted for the purpose of preventing or detecting a criminal offence specified by law (section 126^2 (2) of the CCP);
3) it is permitted to conduct a surveillance operation if (a) collection of data by other activities is impossible; (b) timely collection of evidence by other procedural acts is impossible; (c) collection of data or evidence by other activities or procedural acts is especially complicated; (d) collection of data or evidence by other activities or procedural acts may damage the interests of the criminal proceedings (section 126^1 (2) of the CCP).

16 The scope of supervisory control is different under the Prosecutor's Office Act and the Statutes of the Prosecutor's Office (cf. section 9 of the Act and section 4 of the Statutes).

17 RT I, 30.12.2015, 72.

B. Formal requirements:
1) an authorisation should generally be issued in writing (section 126[4] (1) of the CCP);
2) an application of a prosecutor's office to a preliminary investigation judge must be reasoned (section 126[4] (1) of the CCP);
3) a preliminary investigation judge will decide the grant of authorisation by a ruling (section 126[4] (1) of the CCP).

2.3. Substantive requirements applicable to authorisation of surveillance operations

2.3.1. Does a reasonable suspicion constitute a prerequisite for authorisation?

In the context of substantive requirements, it is necessary to ascertain whether an authority authorising a surveillance operation is required to verify the existence of a reasonable suspicion, as required by the ECtHR.[18] The CCP does not expressly require the existence of a reasonable suspicion to allow the conduct of a surveillance operation. The law uses different terminology: "in the case of whom there are serious grounds for believing that he or she has committed or will commit a criminal offence". It can be assumed that this wording does not imply the existence of a reasonable suspicion, because in the cases where a surveillance operation arises from the need to collect information about a criminal offence in criminal proceedings, the operation may also be conducted – in addition to a suspect – in respect of a person "in the case of whom there are serious grounds for believing that he or she has committed or will commit a criminal offence". A suspect is defined as a person who has been detained on suspicion of a criminal offence, or a person in the case of whom there are sufficient grounds to suspect that he or she has committed a criminal offence (section 33 (1) of the CCP). Since the element of a reasonable suspicion is already included in the term 'suspect', it follows that a person "in the case of whom there are serious grounds for believing that he or she has committed or will commit a criminal offence" must be different from a suspect.

The Criminal Chamber of the Supreme Court has explained that a reasonable suspicion of a criminal offence can be established if "concrete evidence points to facts that, based on human, forensics and criminal procedure-related experience, give rise to a considerable probability that the person in question may have committed an act that contains elements of a specific criminal offence".[19] Authorisation of a surveillance operation is not conditional only on a suspicion

18 ECtHR 04.12.2015 (reference 3), p. 260.

19 Ruling of the Criminal Chamber of the Supreme Court 31.10.2013, 3-1-1-97-13, p. 9.

of a criminal offence, but on a suspicion of a criminal offence listed in section 1262 (2) of the CCP. As regards applications for arrest, all the members of the Criminal Chamber concurred that the description and legal assessment of an act need not be final in terms of adjudication of a criminal case, but they still have to be consistent with one another and make it possible to ascertain the act of the commission of which the person concerned is accused.[20] In the judgment given in the so-called land swap case, the members of the Criminal Chamber concurred that a ruling authorising a surveillance operation should "clearly set out the circumstances and available evidence that give rise to a reasonable suspicion of a criminal offence"[21], noting, however, that like when verifying the existence of a reasonable suspicion of a criminal offence in applying section 142 of the CCP, the court's duty of reasoning concerning the verification of the prerequisites specified in section 1261 (2) of the CCP is of a lesser scope than in the case of making a judgment on an offence.[22]

A reasonable suspicion of a criminal offence requires the existence of facts based on which it can be decided which criminal offence a person is preparing or has committed, and which facts confirm this.[23] However, evidence supporting a reasonable suspicion of a criminal offence does not have to be so compelling as to enable the person in question to be convicted merely on the basis of that evidence.[24]

The current case law does not clarify how a person "in the case of whom there are serious grounds for believing that he or she has committed or will commit a criminal offence" differs from a person "in the case of whom there are sufficient grounds to suspect that he or she has committed a criminal offence". There is no reason to assume that the wording of the legislator does not have a meaningful content, but the author of this article does not have enough information or imagination to understand it, and the Explanatory Memorandum to the draft Act, which explains the background of amendments to the Code, is not helpful either. According to the Explanatory Memorandum, information on the preparation of a criminal offence can be collected where there are no sufficient data to commence criminal proceedings, but there is a reasonable suspicion.[25]

---

20 Ruling of the Criminal Chamber of the Supreme Court 01.02.2012, 3-1-1-105-11, p. 19.

21 Judgment of the Criminal Chamber of the Supreme Court 30.06.2014, 3-1-1-14-14, p. 772.

22 Ibid., p. 773.

23 See ECtHR 04.12.2015 (reference 3), p. 260.

24 Ruling of the Criminal Chamber of the Supreme Court 31.10.2013 (reference 19), p. 9.

25 Explanatory Memorandum to the draft Code of Criminal Procedure Amendment and Other Related Acts Amendment Act. – Online: http://www.riigikogu.ee/tegevus/eelnoud/eelnou/86dde8ff-c50e-48ba-a39e-a325fe15a3f0/Kriminaalmenetluse%20seadustiku%20muutmise%20ja%20sellega%20seonduvalt%20teiste%20seaduste%20muutmise%20seadus/.

The Explanatory Memorandum to the draft Act and the case law allow for one conclusion, though. A prediction of the threat of a criminal offence cannot serve as the basis of a surveillance operation unless it is supported by facts.

The Code of Criminal Procedure also permits the conduct of surveillance operations in respect of persons who are not involved in a criminal offence which is being prepared or which has been committed. The only prerequisite is that the person interacts with a suspect or with a person in the case of whom there are serious grounds for believing that he or she has committed or will commit a criminal offence, communicates information to such person, provides assistance to the person or allows the person to use his or her means of communication. The phrase "in the case of whom there are serious grounds for believing" is used twice, which makes it even more difficult to define the already broad circle of persons whose fundamental rights may be affected. What is clear, however, is that the law allows surveillance agencies to infringe the fundamental rights of individuals who are not involved in a criminal offence. The Criminal Chamber of the Supreme Court has held that the collection of evidence in criminal proceedings by conducting a surveillance operation in respect of a person regarding whom there are no grounds to suspect that the person has committed or will commit a criminal offence, is permissible only in justified exceptional cases,[26] but has failed to explain what these exceptional cases are.

The law permits surveillance operations to be conducted in the case of criminal offences listed in section 126^2 (2) of the CCP. Consequently, a surveillance agency must have facts that point to a criminal offence specified in the law, not just any criminal offence. The Supreme Court has accepted the position of the prosecutor's office, according to which "in pre-trial proceedings, the body conducting the proceedings must often act on the basis of limited knowledge, which is why it may be difficult to predict the necessary elements of a criminal offence".[27] The difficulties of bodies conducting proceedings are understandable, but the position of the Supreme Court entails the risk of legitimising surveillance operations that are conducted for the purpose of preventing or detecting criminal offences not listed in section 126^2 (2) of the CCP.

2.3.2. Ultima ratio requirement

It is permitted to conduct a surveillance operation if collection of data by other activities or taking of evidence by other procedural acts is impossible, is impossible on time or is especially complicated or may damage the interests of the criminal proceedings (section 126^1 (2) of the CCP). According to the Supreme

26 Ruling of the Criminal Chamber of the Supreme Court 16.12.2014, 3-1-1-68-14, p. 17.

27 Ibid., p. 18.2.

Court, these conditions represent the principle of last resort or *ultima ratio*.[28]

The Criminal Chamber of the Supreme Court has provided explanations to courts on the application of the *ultima ratio* principle. For example, the Supreme Court has stated that the reasoning of the existence of prerequisites of a surveillance operation should not be limited to a declaratory finding of the necessity of the operation. "It is not sufficient to merely refer to the application of the prosecutor and state that the court deems the content of the application to be reasoned."[29] According to the Supreme Court, impossibility or significant difficulty of collecting evidence by other procedural acts may be due to, for example, "the high level of organisation of the criminal offence, secrecy, use of front men, supposed lack of witnesses ready to give testimony, the fact that the offence has no obvious victim, the cost of time and resources spent on the so-called conventional procedural acts, etc."[30] The Supreme Court believes that while the conclusions of a court should be linked to the available evidential base,[31] it is sufficient if, based on the circumstances of the particular case, there is reasonable cause to assume that the use of other means of taking evidence is precluded.[32]

The wording of the CCP effective until 1 January 2013 justified the conduct of a surveillance operation by two factors: collection of evidence by other procedural acts is impossible or especially complicated. The interpretations given by the Supreme Court so far are based on that wording. The *ultima ratio* principle was diluted in the wording valid from 1 January 2013. In addition to the grounds set out in the previous wording, it is now also permitted to collect evidence by a surveillance operation in the cases where collection of evidence by other procedural acts is impossible on time or may damage the interests of the criminal proceedings. This extension widens the margin of discretion of surveillance agencies and prosecutor's offices, causing *ultima ratio* to lose the significance of a 'last resort'.

The legality of any restriction of fundamental rights is conditional on its proportionality. To evaluate proportionality, it is necessary to consider the extent of the infringement of fundamental rights and the strength of the arguments justifying the infringement. The extent of infringement of fundamental rights, particularly the right to confidentiality of communications, privacy and the inviolability of

---

28 See the ruling of the Criminal Chamber of the Supreme Court 16.12.2014 (reference 26), p. 20; judgment of the Criminal Chamber of the Supreme Court 06.04.2015, 3-1-1-3-15, p. 10.

29 Judgment of the Criminal Chamber of the Supreme Court 30.06.2014 (reference 21), p. 772.

30 Ibid. Judgment of the Criminal Chamber of the Supreme Court 06.04.2015 (reference 28), p. 14.

31 Ibid.

32 Judgment of the Criminal Chamber of the Supreme Court 30.06.2014 (reference 21), p. 773.

home, is not the same for all surveillance operations, and all criminal offences that warrant surveillance operations are not equally dangerous. Unfortunately, the procedural law does not contain an express requirement to deliberate, when considering authorisation of a surveillance operation that will infringe fundamental rights, whether the measure is proportionate to the objective pursued. The analysis scheme of the ECtHR requires an assessment of whether the surveillance operation is necessary in democratic society, i.e. whether the desired result could be achieved by less restrictive means.[33] While the conditions established by law, which the Supreme Court calls the *ultima ratio* principle, restrict the conduct of surveillance operations to some extent, their wording does not require authorising authorities to consider the constitutionality of the infringement of a fundamental right. Moreover, according to the guidance provided by case law, an authorising authority is only required to justify why the evidence can only be collected by the surveillance operation.[34]

The possible counter-argument that the legislator considered the principle of proportionality when formulating the conditions under which a surveillance operation is warranted is not convincing. While the position of the Constitutional Review Chamber of the Supreme Court, according to which the principle of proportionality should be considered both by authorities applying the law and by the legislature[35], obligates the legislator to already ensure the proportionality of an infringement of a fundamental right by a legal provision at the stage of adoption of the provision, it does not release courts from the obligation to assess the proportionality of an infringement of a fundamental right in view of the circumstances of a particular case.

The conclusion that can be made from the foregoing is as follows. The *ultima ratio* principle applicable to authorisation of surveillance operations that infringe fundamental rights does not replace the proportionality test, but it is a requirement that has to be taken into account when assessing the proportionality of an operation. Although the law requires authorities applying the law only to look into the *ultima ratio* principle when granting authorisations, the Constitution provides for the obligation to consider the proportionality of a measure that restricts a fundamental right.

---

33 ECtHR 04.12.2015 (reference 3), p. 260.

34 See the judgment of the Criminal Chamber of the Supreme Court 30.06.2014 (reference 20), p. 773; judgment of the Criminal Chamber of the Supreme Court 06.04.2015 (reference 28), p. 15–16.

35 Judgment of the Constitutional Review Chamber of the Supreme Court 28.04.2000, 3-4-1-6-2000, p. 13.

2.4. Formal requirements applicable to authorisation of surveillance operations

The law is quite laconic on the formal requirements for authorisations. An authorisation granted by a prosecutor's office or a preliminary investigation judge should generally be issued in writing (section 126[4] (1) of the CCP). A preliminary investigation judge decides the grant of an authorisation by a ruling on the basis of a reasoned application of the prosecutor's office (section 126[4] (1) of the CCP). Although the format of the application of the prosecutor's office is not explicitly mentioned, it is to be assumed that the application should be in writing. The Supreme Court has explained that the requirements for a ruling of a preliminary investigation judge are set out in section 145 of the CCP.[36] This provision requires a ruling to be reasoned. It does not specify, however, what the requirement of reasoning means in the case of an authorisation of a surveillance operation. The case law of the Supreme Court explains that the reasoning of a ruling should clearly and comprehensibly set out why it is not possible to collect the evidence in a manner other than by a surveillance operation.[37] A declaratory finding of the necessity of the surveillance operation is not enough. The conclusions of a court should be linked to the evidential base. It is not sufficient to merely refer to the application of the prosecutor and state that the court deems the content of the application to be reasoned.[38] According to the law, an authorisation of a surveillance operation has to specify the term of the authorisation (sections 1264 (4), 1265 (1) and 1267 (3) of the CCP). It is unclear, however, whether an authorisation of a surveillance operation has to set out the names of the persons whose communications are allowed to be intercepted, the means of communications to be tapped, and the premises where the surveillance operation will be conducted. The case law of the Supreme Court does not provide any clarity, although this question has been raised before the Supreme Court at least once.[39]

Although the law and the explanations of the Supreme Court emphasise the need to reason the authorisation of a surveillance operation, a lack of such reasoning does not, in the opinion of the Supreme Court, render a surveillance operation illegal. According to the Supreme Court, insufficient reasoning of a surveillance operation is not tantamount to a lack of authorisation. "The fact that the court has failed to duly reason the grant of the authorisation to conduct the surveillance operation does not mean that the surveillance operation was an arbitrary act of the executive power, undertaken outside judicial review."[40]

---

36 Judgment of the Criminal Chamber of the Supreme Court 26.05.2010, 3-1-1-22-10, p. 14.3.

37 Judgment of the Criminal Chamber of the Supreme Court 30.06.2014 (reference 21), p. 772.

38 Judgment of the Criminal Chamber of the Supreme Court 06.04.2015 (reference 29), p. 10.

39 See the ruling of the Criminal Chamber of the Supreme Court 15.06.2015 (reference 11), p. 20.

40 Judgment of the Criminal Chamber of the Supreme Court 30.06.2014 (reference 21), p. 778.

The law is more specific as regards authorisations granted in a format that can be reproduced in writing. The law specifies the data that such an authorisation has to set out (section 1264 (4) of the CCP). The format and the requirements for the contents of authorisations issued by prosecutor's offices, however, are not regulated.

The requirement of written format is a general rule, to which exceptions may be made under the procedural law. A prosecutor's office may deviate from that rule "in cases of urgency" (section 1264 (2) of the CCP), and a court may do so "in cases where requesting or documenting an authorisation on time is impossible" (section 1264 (3) of the CCP). How these phrases should be understood is currently unclear.

The inadequacy of substantive and formal requirements for the contents of authorisations of surveillance operations explains (at least in part) why the content and form of rulings vary by region and why the reasoning of the authorisations is often vague and stereotyped.[41]

2.5. Supervision over surveillance operations

Estonian laws do not provide for *ex officio* judicial supervision over surveillance operations, whether at the time they are conducted or afterwards. The law states that supervision over the compliance of a surveillance operation with the authorisation specified in section 126^4 of the CCP is exercised by the prosecutor's office (section 126^{15} (1) of the CCP). On the one hand, the mixing of competencies, which is reflected in the fact that the prosecutor's office participates in the planning of surveillance, directs pre-trial criminal proceedings and must ensure their effectiveness (section 1 (1) of the POA), authorises the surveillance operation (section 126^4 of the CCP), and at the same time oversees the legality of the surveillance operation, may not result in effective control over infringement of fundamental rights. On the other hand, it is not clear from the wording of section 126^{15} (1) of the CCP whether the supervision is limited (compliance of the surveillance operation with the authorisation) or absolute.

A person affected by a surveillance operation cannot file an appeal, i.e. he or she does not have a legal remedy to protect his or her rights, unless the person is aware of the surveillance operation. A person normally learns about a surveillance operation when the person is notified about the operation or when the conduct of the surveillance operation becomes clear from the materials of

41 See the analysis by the Supreme Court: M. Kruusamäe and T. Reinthal."Pre-Approval of Surveillance by Court in Estonia", 2013, page 23. – Online: www.riigikohus.ee/vfs/1503/6_Lisa%205_Jalitustegevuse%analuus.pdf.

the criminal case. The law distinguishes a person in respect of whom a surveillance operation was conducted from a person whose privacy or family life was significantly infringed by a surveillance operation (section 126^{13} (1) of the CCP). The former person is obviously the one in whom the surveillance agency was interested and in respect of whom an operation was authorised. The surveillance agency is required to immediately notify that person about the surveillance operation, unless there are circumstances that, according to law, justify non-notification (section 126^{13} (2) et seq. of the CCP). A person whose fundamental rights are infringed because of another person is treated in a different manner. The person is notified about the infringement of his or her rights by a surveillance operation if both of the following conditions are met: (1) the infringement related to the privacy and family life of the person; and (2) the infringement was significant. It is not clear whether the legislator deliberately chose to mention only two fundamental rights. If this was the case, then surveillance agencies are not required to notify about infringements of confidentiality of communications and of the inviolability of home. The notification obligation applies if the infringement of a fundamental right was significant. The law does not state whether the significance of an infringement is evaluated by the surveillance agency or the prosecutor's office. In any case, the law gives the opportunity to not notify, due to a variety of reasons, a large number of persons about an infringement of their fundamental rights, thereby restricting their right to go to court, as guaranteed by section 15 (1) of the Constitution. The exercise of the right to file an appeal is also affected by the restrictions on access to data collected by a surveillance operation (section 12614 of the CCP).

The Code of Criminal Procedure provides for two different procedures for filing an appeal. The first concerns the filing of an appeal against a court ruling authorising a surveillance operation (section 126^{16} (1) of the CCP), and the second concerns the filing of an appeal against the course of a surveillance operation, non-notification about the operation and refusal to grant access to data collected by the operation (section 126^{16} (2) of the CCP).

The first procedure provides limited protection of fundamental rights. This is for two reasons. First, by an appeal against ruling filed directly with a circuit court, a person can contest only the authorisation, granted by a preliminary investigation judge, of the conduct of the surveillance operation. The person cannot contest infringements of his or her rights by the surveillance operation in this appeal.[42] In addition to limiting the effectiveness of the legal remedy, these rules are also unjustified for procedural economy considerations: a person who

42 See the Explanatory Memorandum (reference 25), page 21.

wishes to contest an authorisation of a surveillance operation and the conduct of the surveillance operation has to initiate two different proceedings.

Secondly, the right to contest an authorisation of a surveillance operation granted by a preliminary investigation judge is limited by the Supreme Court's interpretation of section 126[16] (1) of the CCP. The Criminal Chamber of the Supreme Court has explained that "according to historical, teleological and systematic interpretation, this provision must be understood as stating that the legality of an authorisation granted by a court for a surveillance operation cannot be contested by filing an appeal against the court ruling during the hearing on the merits of the criminal case".[43] The Chamber argues that such a lack of a right to file an appeal does not distort the nature of *locus standi* arising from section 11 of the Constitution.[44] According to the Supreme Court, a court hearing a matter of offence can evaluate whether an authorisation of a surveillance operation and the operation itself were legal and, on the basis of this evaluation, decide on the admissibility of the evidence collected by the operation.[45] When hearing a matter, a court only decides what evidence can be used to convict or acquit the person charged. The court does not consider the proportionality of the infringement of a fundamental right or decide how to remedy any damage caused by the infringement of the fundamental right.

The Supreme Court holds that the situation is different when a criminal case has not yet been sent to a court for hearing on the merits. At the time of pre-trial proceedings, it is not yet known whether the criminal case will be sent to a court and what evidence the prosecutor will want to rely on. "In a situation where a person has no other effective opportunities to exercise his or her right of appeal, refusal to review the appeal against a ruling is not justified. While waiting for the outcome of pre-trial proceedings, the person may lose the opportunity to contest the legality of surveillance operations conducted in respect of him or her."[46] It should be repeated, however, that with an appeal against a ruling filed with a circuit court a person can contest only the legality of the authorisation of a surveillance operation, not the legality of the operation itself.

The law unduly restricts legal remedies (1) for contesting the authorisation of a surveillance operation issued by a prosecutor's office and for contesting the operation itself, (2) for contesting the legality of an operation conducted under

43 Ruling of the Criminal Chamber of the Supreme Court 16.06.2015, 3-1-1-48-15, p. 20.

44 Ibid.

45 Ibid., p. 15.1 and 15.2.

46 Ruling of the Criminal Chamber of the Supreme Court 02.12.2015, 3-1-1-106-15, p. 7. See also the ruling of the Criminal Chamber of the Supreme Court 20.10.2015, 3-1-1-76-15, p. 7.

the authorisation of a court, and (3) available to persons in respect of whom a surveillance operation has not been authorised, but whose rights have been infringed by a surveillance operation.

First, the law allows an appeal to be filed against the course of a surveillance operation conducted under the authorisation issued by a prosecutor's office, but it is not possible to appeal against the decision authorising the operation (section 12616 (2) of the CCP). This at least is the conclusion that results from the literal interpretation of the legal provision. This interpretation is indirectly supported by the different procedures for contesting an authorisation granted by a court and the surveillance operation conducted under that authorisation.

Secondly, an appeal can be filed against a surveillance operation until the preparation of a statement of charges (section 228 (1) and (2) of the CCP). There are no judicial interpretations that rule out the application of the time limit for filing an appeal set out in that section. However, it may happen that the person affected by a surveillance operation learns about the infringement of his or her rights after that time.

Thirdly, the use of a legal remedy is time-consuming, unnecessarily complicated and therefore also costly. The review of the legality of a surveillance operation authorised by the Office of the Prosecutor General or by a district prosecutor's office begins at the prosecutor's office (possibly the district prosecutor's office) and can then be continued at the Office of the Prosecutor General. The right to file an appeal with a court arises after the review of appeals at the prosecutor's office. In a county court, an appeal is adjudicated by a preliminary investigation judge. The ruling of a preliminary investigation judge can also be contested in a circuit court and ultimately in the Supreme Court (sections 231 (5) and 385 (14) of the CCP).

Fourthly, the right of appeal does not guarantee effective legal protection. A preliminary investigation judge may accept that there has been a violation of rights, but he or she has no right to award fair compensation for the violation. While a preliminary investigation judge can stop the conduct of a surveillance operation, this remedy is only an apparent one, because the operation is authorised and conducted secretly from the person affected by it, which is why the person can contest the infringement of a fundamental right only after becoming aware of the operation.

When acceding to the European Convention for the Protection of Human Rights and Fundamental Freedoms, the state undertook to ensure the right to an effective remedy before a national authority even in the cases where a violation has been committed by persons acting in an official capacity, as prescribed by Article

13. A remedy is effective in practice and in law if it prevents or remedies the violation of a fundamental right or provides adequate redress for the violation.[47]

In conclusion

The author of this article cannot give an optimistic answer to the question of whether supervision, established by legal acts and case law, over surveillance operations that are conducted secretly from the persons concerned and society in general, infringe constitutionally protected rights and entail a threat of abuse which is greater than in the case of public operations, is adequate and effective.

First, full judicial pre-approval of surveillance operations, judicial supervision of the operations at the time of conduct thereof, and effective review of the operations after their completion are not ensured. Second, the rules on surveillance are laconic, incomplete and ambiguous, and the case law has not been able to improve this situation. In other words, legal clarity of the law is not ensured. This adds to the complexity of judges' work and may also contribute to superficiality.

47 ECtHR 06.09.1978 (reference 1), p. 64; ECtHR 11.06.2009, Petkov and others v. Bulgaria, p. 74.

To engage or not to engage in surveillance – that is the question

Aro Siinmaa, prosecutor

A spectre is haunting Estonia – the spectre of surveillance. This paraphrasing seems to be a fitting introduction to my reflection on surveillance, the role surveillance plays in the process of furnishing proof regarding criminal offences, and the fears that it evokes. In fact, it is probably appropriate to start with the latter, as otherwise the discussion would be quite short. The effective investigation of some complex crimes requires the collection of evidence using covert operations. This mode of proof is strictly regulated by law and subject to multilevel judicial review. And that's it? Oh, no. When reading and listening to the statements recently made in the media, the legislature and courtrooms by representatives of various walks of life, including some lawyers, which are full of high-flown emotions, rhetorical superlatives and popular clichés, an uninformed audience might easily start to believe that Estonia is indeed a police state where every enterprising citizen is being spied on, everyone and everything is tapped, and each word of a person would certainly be interpreted to his or her detriment. Nothing could be further from the truth, but, unfortunately, the discreet truth often goes unnoticed in the midst of noisily presented, colourful and sensational conspiracy theories. No wonder, because conspiracy theories rely on preconceptions, and these are so powerful as to generally make common sense, facts and logic powerless against them.

In order to begin to untie the difficult knot of controversial perceptions and opinions related to surveillance, it seems reasonable to move away from legal abstractions for a moment and to approach the topic from a real-life point of view. One of the most effective ways to solve a problem that seems complicated at first glance is to strip off everything that is irrelevant, illusory and misleading, and dig as close to the heart of the matter as possible. So – why is surveillance carried out? When listening to the loudest critics of surveillance operations, one could get the impression that surveillance is a recent Estonian invention like Skype, only it has been created for mean motives – so that the government would be able to freely intrude in the privacy of citizens and cause as many inconvenience to them as possible. I am not going to tire the reader with the history of covert operations that has developed for thousands of years. Instead,

I would like to take you to Great Britain in the 19th century, where a medical doctor, due to a lack of patients, sat down to write detective stories. His name was Arthur Conan Doyle. Being a practicing general doctor he had no experience with criminal investigation. We are talking about the 1880s when forensic science was still in its infancy and the working methods of Sûreté and Scotland Yard, set up in the first half of the century, were far from being general knowledge. Nevertheless, the doctor-writer decided to create the character of a brilliant detective who would outstrip the state police with his scientific and methodological approach to the investigation of crimes. This is how Sherlock Holmes, the consulting private detective was created. One can imagine that, when depicting the character of the ingenious detective, the most difficult task of the author was to actually make him do something clever. So, what did Sherlock Holmes (with the help of Sir Arthur Conan Doyle) do to win worldwide recognition and, over time, become a symbol of a successful criminalist whose popularity has not abated to this day? Of course, he thoroughly questioned witnesses, carefully looked at the scenes of events, examined traces and gathered evidence – or took the steps that we today consider to be the most elementary primary investigative measures, and subjected his findings to a comparative analysis, which we call the gathering of evidence through forensic examination and investigative experiments. What else did he do? When noticing a suspect passing in a cart, he would secretly jump on the frame of the cart or follow the suspect in another cart to see where the suspect was going and what he or she was doing. Noticing a suspicious person talking to someone in a coffee-shop, he would quietly find a place at a neighbouring table and try to listen in on the conversation. To collect information, he would disguise himself and infiltrate into groups of grooms or port workers, even in an opium den, where he created a relationship of trust with criminals. In order to collect an important piece of evidence, he pretended to faint and, having been carried into to the room he was interested in, secretly searched the room. What was all this about? In terms of today's criminal procedure, these measures amounted to discreet surveillance, interception of a conversation, use of an agent, staging of a crime, covert entry, and examination. More than a hundred years ago, all these activities, which we today treat as surveillance operations, occurred to a doctor-writer who fantasised about investigation of criminal offences and made his fictional detective gather the necessary evidence. Consequently, surveillance operations are not some ill-omened scheme of a police state, but rather something that an ordinary intelligent person deems to be self-evidently required for effective resolution of crimes.

Who cares if surveillance enables the truth to be established and crimes to be solved? It is still too serious an infringement of fundamental rights and there is too much of it! This is what critics say, and at least some of them probably actually start to believe it themselves in the long run. By the way, it should be noted

that the public opinion of the rights and practices of the police is always influenced by the rate and dangerousness of crime in society. When an average citizen perceives a real danger of falling victim to, for example, robbery, extortion or burglary, he or she enthusiastically supports the extension of the powers of the police and the intensification of the fight against crime. However, if this threat diminishes over time and the person (or the person's relative, friend, business partner, fellow party member or customer) is more likely to find him or herself in the spotlight of the police due to some latent violations, the activities of the police will, as if by magic, start to seem disproportionate and excessive.

A person who is the subject of a baseless complaint concerning a crime should reasonably prefer that surveillance operations be carried out to thoroughly check the complaint. Otherwise, the body conducting proceedings may be compelled to declare the person to be a suspect merely on the basis of the complaint, organise searches or otherwise disrupt the person's life. Even if the proceedings are stopped in the absence of evidence, the operation of the principle "where there is smoke, there is fire" means that the person's reputation will always be tarnished due to failure to dispel doubts. The paradox lies in the fact that only those people who actually would not commit any crime and who, therefore, can be confident that surveillance operations will confirm their compliance with law can afford the way of thinking described above. However, from the point of view of a person who actually has criminal ambitions, it is only logical to regard any surveillance as a disproportionate infringement.

As regards infringement of fundamental rights, I have to admit that I cannot remember any other act of law that has been so brutally and consistently abused in rhetoric than the Constitution. Most of the worried rhetoric concerning constitutionality is a pure bluff. Why? Because the Constitution is not interpreted in a systemic manner; instead, people prefer to pick certain provisions out of it and amplify them. In fact, the Constitution represents a comprehensively balanced legal foundation which, on the one hand, guarantees everyone's rights and freedoms while, on the other hand, enabling the rights and freedoms to be restricted when a person abuses them and disrespects the rights of others. We should not forget that, besides state authorities, fellow citizens also can infringe a person's fundamental rights if they endanger the person's life, health, property or other constitutionally guaranteed values. When the rights of a person are under attack, the Constitution guarantees the person's right to protection by law and state authorities. Indeed, the Constitution requires state authorities to respond to crime at a level of intensity that ensures actual and effective protection of citizens. Rights and freedoms are not absolute and may be restricted in order to protect other people's rights and freedoms, as well as for crime detection and prevention. The constitutional framework enables state authorities to investigate criminal offences, establish the truth, conduct surveillance operations in respect

of suspects and prosecute offenders, while avoiding the repression of innocent people and precluding any arbitrary action on the part of state authorities. In no way does the Constitution support the commission of crimes or the evasion of responsibility. Nor does it tip the scales so that the rights of suspects could be protected proportionally to a greater extent than those of the rest of the people.

Why does this prosecutor throw around fiction and general provisions of the Constitution, when surveillance is subject to the principle of *ultima ratio*?! This is how another critical remark could sound, and it would be based on completely appropriate grounds. Quite another question is how the 'last resort' should be interpreted. As is known, it is possible to approach each subjective evaluation criterion in an open and constructive manner, as well as in a limiting and narrow manner. Fortunately, the case law of the Supreme Court has so far been practical and realistic, with its position, according to which criminological knowledge can lead to the conclusion that it is impossible or significantly more difficult to gather evidence without resorting to surveillance operations, deserving special attention. This may be due to, for example, the high level of organisation of the criminal offence, secrecy, use of front men, supposed lack of witnesses ready to give testimony, the fact that the offence has no obvious victim, the cost of time and resources spent on the so-called conventional procedural acts, etc. (judgment of the Criminal Chamber of the Supreme Court of 30 June 2014 in criminal case no. 3-1-1-14-14, p. 772). All this is true. To be honest, the principle of *ultima ratio* is still a significant source of unease for investigators and prosecutors. In the absence of psychic powers it is unspeakably difficult to predict what the results of other procedural acts may be, whether they will result in a sufficient body of evidence, which of the evidence may prove unusable during judicial proceedings for one or another reason, and what will remain of the body of evidence. We must not forget that, unlike subsequent evaluators, the prosecutor does not have a complete file available to him or her at that time and has to make these choices on the basis of a small and incomplete body of information. In addition, the prosecutor has to realise that the choice is final and any mistakes cannot be corrected. If the prosecutor should decide that the case can be solved on the basis of other evidence, but that evidence cannot be gathered or used for any reason, then it is impossible to go back to the covert phase and make a new attempt of surveillance, as the suspicion of an offence is already public. Hypothetical sceptic: "Well, so what? Who cares if a couple of crimes go unpunished?" But we should care, because each successfully committed crime that is not prosecuted will reinforce the perpetrators' feeling of impunity, encourage them to commit new offences and, in a wider sense, harm the well-being and security of all law-abiding people. I would really like to hope that no police officer, prosecutor or judge practices the "so what?" attitude to crime, either today or in the future.

Although the format of this article does not enable me to analyse individual cases, I cannot resist the opportunity to discuss a hypothetical situation. The text of a review of case law compiled at the Supreme Court in 2013, entitled "Pre-Approval of Surveillance by Court in Estonia", which is generally meaningful in other respects (except the unrealistic discussion of the practice of setting out persons' telephone numbers in the authorisations of surveillance operations), contains a conclusion to the effect that the *ultima ratio* criterion is not satisfied in cases where surveillance involves wiretapping with a view to avoiding 'word against word' situations in court, i.e. gathering additional incriminating evidence with the help of surveillance operations before the questioning of the person. I dare to state that, on the contrary, such surveillance is a classical example of an *ultima ratio* situation in which it is extremely likely that the truth cannot be established using traditional evidence. This is where criminological knowledge and experience come into play, such as the knowledge that the summoning and questioning of the suspect based on the testimony of a person who is a victim of blackmail generally does not yield any result other than making the suspect aware of the complaint filed with regard to him or her and enabling the suspect to prepare a denial which is difficult to refute. But what if the suspect is not making anything up and it is actually the victim who is lying? The solution is to record telephone calls and face-to-face conversations between the victim and the suspect, which will allow the situation to be objectively evaluated and the truth to be established. This is what the gathering of evidence through surveillance activities is intended for.

I will now mention some myths which continue to arise in relation to surveillance. First there is the opinion that the police prefer to gather evidence through surveillance operations for the sake of convenience. This notion is as far from the truth as can be. Anyone who has the slightest idea of what, for example, wiretapping actually looks like knows very well that there is nothing less comfortable than following the communication of a strange person day in, day out. In addition to the fact that there are no breaks in this work, one has to be consistently focused so as to not miss important data in the flow of irrelevant information. Essentially, a surveillance officer is forced to live the life of a stranger for some time, and the majority of those strangers are people with whom one would not think of exchanging a word under normal circumstances. When comparing the resources needed for tapping just one suspect with the staff figures of an average police unit, it is instantly clear that conspiracy theories about massive wiretapping are even more fantastic than stories about flying saucers. Related to this myth is another sporadically spread myth that preliminary investigation judges issue authorisations of surveillance operations too easily. As any grotesque false allegations, this opinion is based on tendentious interpretation of statistical data. After all, prosecutors are very well aware of the principle of *ultima ratio* which is why, given also the resource-intensity of surveillance, applications

for surveillance operations are filed with preliminary investigation judges only in the cases where surveillance is absolutely indispensable. Since the need for surveillance is obvious in the majority of such cases, it would be rather strange if the number of applications granted were lower.

Finally, I would like to set adrift a cry for help, like a message in a bottle, in the hope that it will reach the right addressee, be it the judiciary or legislative institutions. Namely, the notion that the issuance of an authorisation of surveillance operations is independently actionable seems to have rooted in judicial practice by now. Such authorisations are often disputed in parallel with the hearing on sending the criminal case to court or with the hearing of the main proceedings, because the defence counsel and the suspect usually become aware of the surveillance operations in the final stages of pre-trial investigation. Thus, a situation may occur where the report on surveillance operations which is the backbone of the body of evidence and on which the prosecutor has built the charges and the analysis of the evidence suddenly disappears, while the prosecutor has no time left for restructuring the case or modifying the concept of proof. Sending a criminal case to adversarial proceedings resembles an equation with too many variables anyway these days. While it is understandable that parties to proceedings cannot have a hundred percent guarantee for any evidence, there still should be elementary certainty that a piece of compelling objective evidence will not perform a vanishing trick. Of course, the legality of surveillance should be subject to judicial review but, given the secret nature of surveillance operations and the related procedural situation, it would be wise to perform the review in the course of the trial. This way the prosecutor will retain an opportunity to try to protect the evidence in its actual context, and the evaluation of the evidence, including any exclusion or declaration as unreliable, will follow a logical linear progression in the adjudication of the case.

Problems related to surveillance – the perspective of a defence counsel

Küllike Namm, attorney-at-law

Various articles have recently been published on surveillance. In this article, I am not going to raise again the problems that are related to the limited opportunities of a defence counsel to ensure effective defence in pre-trial proceedings, especially in a situation where the application for arrest filed with a court is substantiated with evidence gathered in the course of surveillance. At the same time, the evidence is not presented to the defence counsel before or during the hearing of the application for arrest. The same issue has arisen in the adjudication of applications for exclusion from office.

Section 126[1] (1) of the Code of Criminal Procedure (CCP) states that a surveillance operation means the processing of personal data for the performance of a duty provided by law with the objective of hiding the fact and content of data processing from the data subject. According to subsection (2) of that section, it is permitted to conduct a surveillance operation if collection of data by other activities or collection of evidence by other procedural acts is impossible, is impossible on time or is especially complicated or may damage the interests of the criminal proceedings. Subsection (4) states that information obtained by a surveillance operation is evidence if application for and grant of the authorisation of the operation and the conduct of the operation were in compliance with the requirements of law.

This wording means, in principle, that surveillance can be ordinary practice, rather than an exceptional way of collecting evidence in criminal proceedings. In the text of the CCP, which permits surveillance if the collection of data by other procedural acts could damage the interests of the criminal proceedings, surveillance is essentially undefined and can therefore be applied in any case, provided it is skilfully justified.

The restriction set out in section 126[2] (2) of the CCP is the only limiting condition in most of the cases in practice. This provision specifies the criminal offences

in the case of which surveillance is permitted. In reality, there are few criminal offences for which surveillance is not permitted, as from 1 January 2013, surveillance is also permitted in the case of offences for which the maximum penalty is one year of imprisonment (such as threatening, section 120 of the Penal Code). In addition, section 1262 (3) and (4) of the CCP provide for restrictions in the case of persons regarding which surveillance operations may be conducted under a special procedure, but these cases are of a marginal significance in reality.

Since section 1261 of the CCP sets virtually no limits on the conduct of surveillance operations, which are permitted for a large part of criminal offences, the prosecutor's office generally refers to reports on surveillance operations as evidence in the statements of charges in criminal cases heard pursuant to general procedure.

Given the regularity of collection of evidence by surveillance operations, one gets the impression that reports on surveillance operations and information collected by surveillance operations have become the prevailing evidence for the prosecution. A justified question arises: since surveillance is permitted without almost any restrictions, is it even necessary to collect other evidence in criminal proceedings and submit it to the court if information needed to establish a person's guilt can be obtained by listening to the person's telephone calls, reading the person's e-mails and covertly observing the person?

Notification about surveillance operations, providing access to information collected by surveillance operations, and exculpatory information collected by surveillance operations

The widespread use of surveillance operations in criminal proceedings has led to the situation where state authorities are clearly unable to notify persons about the surveillance operations carried out and provide access to the information collected by these operations. Section 126[13] of the CCP provides for the general right of a person who was the subject of a surveillance operation, or of any person the inviolability of whose privacy or family life was infringed by a surveillance operation, to know about this. Section 126[14] of the CCP lays down the ways a person can examine information collected in the course of surveillance operations. Notification, however, does not provide actual access to the data collected by the surveillance operations, and examination does not give the opportunity to exercise the right to defence where necessary.

I am not going to analyse situations where persons in respect of whom criminal proceedings are not being conducted are notified about surveillance operations. Instead, I will focus on those individuals who have the status of a suspect or an accused person in proceedings.

In a situation where a person has not been arrested and/or excluded from office, the person can become aware of the surveillance operations conducted in respect of him or her in two ways: the defence counsel presents to the person the materials on the criminal file that contain reports on the surveillance operations, or the person is notified about the surveillance operations by the surveillance agency. In practice, the latter notification can reach the person at any time. It is not uncommon that a person receives the notification only after the statement of charges has been sent to the court and the preliminary hearing on the adjudication of the defence counsel's requests has been held. In such a situation, the defence counsel has only limited opportunities to rely on any exculpatory information obtained by the surveillance operations conducted in respect of the person and to submit this information as evidence to the court, given that, according to section 286[1] (2) 2) of the CCP, the court may refuse to accept evidence and return the evidence, or refuse to take evidence, if the evidence is not listed in the statement of defence and the party to the court proceedings fails to state a good reason why the person was unable to submit the request earlier.

Section 126[13] (1) of the CCP states that upon expiry of the term of an authorisation of a surveillance operation and, when several surveillance operations are conducted that coincide at least partly in time, upon expiry of the term of the last authorisation, the surveillance agency is required to immediately notify the person in respect of whom the surveillance operation was conducted and the person the inviolability of whose privacy or family life was seriously infringed by the surveillance operation and who was identified in the course of the proceedings. The person has to be notified of the time and type of the surveillance operation conducted. However, according to section 126[13] (2) 1) of the CCP, with the permission of the prosecutor's office, the surveillance agency need not give notification of the conduct of a surveillance operation if notification could significantly damage the criminal proceedings. The law does not provide for the form of the permission of the prosecutor's office. Nor does it specify the circumstances that amount to 'significant damage' to criminal proceedings. Thus the law legalises the absence of specific time limits for notification about surveillance operations. The statutory obligation of a surveillance agency to 'immediately' notify a person about a surveillance operation is not complied with in reality. There have even been instances where notification about a surveillance operation is given years after the expiry of the authorisation of the operation.

The Government of the Republic has, by a regulation, established the procedure for notification about surveillance operations and submission of surveillance files (hereinafter referred to as the 'Procedure') under section 126[14] (3) of the CCP. Among other things, the Procedure provides for the time limit for access to data collected by a surveillance operation. Namely, a person has the right to submit an application for examination of the data within 30 days of being notified

about the surveillance operation. The surveillance agency will, within 30 days, notify the person about the time when the data can be examined and the person has the right to examine the data within three months after the date of his or her application. This term can be extended in exceptional cases.

Thus, supposing that the examination reveals information that would have to be submitted to the court, this can be done, depending on the surveillance agency, within four months after the person has submitted the application. By this time, however, it is possible that the court proceedings have come to an end and the judgment has taken effect. Therefore, it is in fact possible that a person is neither aware of, nor given the opportunity to find out, the contents of materials on a surveillance operation during court proceedings. The person thus cannot claim in court that the data collected by the surveillance operation contain exculpatory information.

The situation is particularly difficult in the case of prisoners for whom the right to examine the information obtained in the course of surveillance operations is not guaranteed in any way. Based on a particular criminal case heard in a court, I can state this with certainty. The prisoner has received more than 10 notifications about the opportunity to examine the data of surveillance operations conducted in respect of him. The prisoner has, via the defence counsel, given notice of his desire to examine the relevant information, and the surveillance agency has responded as follows: the prisoner can examine the information in Tallinn on a particular date if the prisoner pays the costs of his transportation; the prisoner can examine the information at the detention facility, followed by the notification that the suggested date is not suitable. The surveillance agency has also suggested that the defence counsel can examine the information, provided the date and time are agreed upon. Thus, prisoners usually do not have an actual opportunity to examine information on the surveillance operations conducted with regard to them, and they do not have even a hypothetical possibility of requesting the submission of any exculpatory information. Imposing the task to examine the information on the defence counsel is not feasible, given the time and costs involved. It is particularly unthinkable in proceedings where defence is provided via state legal aid, given the fee rates of state legal aid.

Even where examination of the data is possible, section 5 (7) of the Procedure (access to information collected by surveillance operations) states that no copies may be made of the data to which access is provided. Thus, neither the defence counsel nor the suspected/accused person has the opportunity to take possession of the evidence containing information that can vindicate the person. This issue is completely unregulated by the Code of Criminal Procedure and there is no case law with regard to it. If such information is known to the defence counsel before the preliminary hearing, a possible solution is for the defence counsel

to request the making of a copy of the recording at the preliminary hearing. Should the prosecutor's office dispute the request on the basis of the Procedure, it is for the court to decide whether or not to grant the request. If the court decides to grant the request, another question arises: will the recording serve as the evidence or should a report be drawn up on the recording? Also, it is unclear who will draw up the report and, in the case that this obligation is imposed on the defence counsel and the latter draws up the report or another document, whether this document is admissible as evidence in the criminal proceedings. Another way to solve the situation is to listen to the recording at the hearing and enter the text of the recording in the minutes of the hearing.

If the exculpatory information collected by surveillance operations is not known by the time of the preliminary hearing, but becomes known later during the proceedings, the above request can be submitted under section 284 (2), 12610 or 297 of the CCP as a request for taking of additional evidence. In this situation, all other evidence can have been examined already, and it is impossible to use the information obtained by surveillance operations during cross-examination of persons. It is hardly believable that the court will, based on that evidence, re-summon persons who have already been questioned (if it decides to accept the evidence at all).

Another issue relating to access to the criminal file during pre-trial proceedings is the defence counsel's opportunity to examine the recordings that serve as the basis for the reports on surveillance operations. According to section 224 (3) of the CCP, a recording made in a criminal proceeding or physical evidence has to be submitted to the defence counsel at the request of the latter. The defence counsel can examine the recording, but the prosecutor's office is not obliged to make a copy of it. Thus, the defence counsel is unable to present the recording to his or her client. Presenting a recording to an arrested person is completely excluded. However, the defence counsel lacks information about, inter alia, the persons participating in the conversation and the circumstances that they are talking about. The assessment independently given by the defence counsel, therefore, might not reflect the reality and the counsel might not be able to effectively defend his or her client purely due to lack of knowledge. The law does not regulate how, in a situation where a recording contains information that can vindicate the client, a defence counsel can present that information as evidence acceptable under law.

Review of the legality of surveillance operations in judicial proceedings

The legality of surveillance operations is reviewed by courts. This statement, however, does not say much. The law does not regulate when and how the review takes place or how the defence counsel can learn about the results thereof.

Defence counsels usually file requests to review the legality of surveillance in their statements of defence. Courts generally grant these requests. Thereafter, the review takes place in the manner and at the time decided by the court. Some judges do not accept reports on surveillance operations from the prosecutor as evidence, or do not disclose these reports before the legality of surveillance operations is reviewed. Some judges allow the prosecutor's office to disclose materials on surveillance operations and order that the legality of surveillance will be reviewed either at the time of or after the disclosure of these materials. While the law does not oblige courts to review the legality of surveillance operations prior to the disclosure of the materials on the surveillance operations, it is precisely this practice that should be regarded as the most rational and the most compatible with the principle of fair and equitable judicial proceedings. Otherwise, there is a situation where the court has already heard surveillance recordings, the court is in possession of the reports on surveillance operations, the explanations given at the hearing have been entered in the minutes of the hearing, and the judge inevitably, purely due to the human factor, remembers the recordings and develops his or her inner convictions. In addition, depending on the volume of proceedings, a considerable amount of time has been spent on listening to the recordings in the court, which later may prove to be unnecessary, because the surveillance may not have been legal.

How do courts review and how can defence counsels obtain information on the review of the legality of surveillance operations?

According to the current established practice, the prosecutor's office presents both applications and authorisations for conducting surveillance operations on the request of the defence counsel. The problem is that most of the text based on which the authorisation has been requested and granted is deleted/hidden both in the application and the authorisation, and consequently these documents do not provide any information as to why the authorisation to conduct surveillance operations was sought. I admit that the prosecutor's office is entitled to withhold some information under section 126[14] (1) of the CCP. In such a situation, however, it is very difficult for the defence counsel to give his or her assessment and provide the reasons of possible illegality of the surveillance operations.

The next issue is what kind of information the defence counsel is entitled to receive after having requested the court to review the legality of surveillance operations, and whether the court is obliged to give answers to the questions raised by the defence counsel in the request to review the surveillance operations or if it is sufficient if the court states that the court has reviewed surveillance and finds it to have been conducted legally.

Being a defence counsel, I have submitted requests asking the court to provide answers to various questions in relation to the review of the legality of surveillance, for example: on what date and under whose decision were the surveillance operations started; was the commencement of the surveillance operations consistent with law; what is the purpose of the surveillance operations; what was the motive and legal basis of commencement of the surveillance operations; what are the reasons for commencement of the surveillance operations as set out in the decision on the surveillance operations; how is it reasoned that the requested information cannot be obtained in a manner that is less intrusive on the constitutional rights of the person; which operations were carried out and have these operations been carried out and documented in accordance with the provisions of law; have reports been drawn up on all surveillance operations; and when was the surveillance file opened.

At times, courts have responded on a question-by-question basis, and at times not. The situation is understandably complicated when surveillance operations have been conducted for a long time, dozens of authorisations have been issued for the operations, and many people are being tried. Then again, a court has to thoroughly review the legality of surveillance, as it is impossible to create lawful evidence through a surveillance operation that has been carried out unlawfully, and a defence counsel has both the right and the duty to request the review of the legality of each surveillance operation. Since it is the prosecution's evidence and if the prosecutor has found it necessary to present dozens of reports on surveillance operations, the legality of all of them must be reviewed. Given that the CCP does not specifically regulate the judicial review of the legality of surveillance operations, it is possible for the court to not answer the defence counsel's questions and confine itself to the statement that everything has been legal. In such a situation, it is impossible for the defence counsel to evaluate all the circumstances related to the charges against his or her client, because without knowledge of what motivated the commencement of surveillance it is not clear whether the surveillance operations have a legal basis and whether they have been conducted in accordance with their purpose.

There has been one positive experience in my practice, where the prosecutor's office accepted the defence counsel's request and the counsel was able to examine, in the presence of the prosecutor and the judge, the materials on the surveillance file. This happened during a criminal proceeding conducted at the time when the wording of the CCP valid before 1 January 2013 was applied. In that particular case, the prosecutor determined the extent to which the defence counsel could have access to the surveillance file, but the counsel was nevertheless able to examine most of the file. Access was not granted to some paragraphs of some documents, which were redacted. The defence counsel was also enabled to make excerpts from the surveillance file. At present, such requests of defence counsels are not granted by courts.

Reports on surveillance operations

Section 126[10] (1) 6) of the CCP states that a report on a surveillance operation should set out information collected by the operation which is necessary to achieve the objective of the operation or to adjudicate a criminal case. There is no doubt that information necessary to support the charges is included in reports on surveillance operations. In legal practice, I have not come across a single report on surveillance operations containing information relevant to the refutation of the charges, although the Supreme Court has, in its judgment in case No. 3-1-2-1-13, pointed out that since an investigative body and a prosecutor's office are required to ascertain the facts vindicating or accusing the suspect or the accused according to section 211 (2) of the CCP, which is done through investigative activities, the data obtained as a result of these investigative activities must be included in a duly documented criminal file. Consequently, if information that can probably vindicate the suspect or the accused is obtained as a result of surveillance operations, this information should also be recorded in the report on the surveillance operations and included in the criminal file, regardless of whether or not the prosecutor would like to add this evidence to the statement of charges. Only information that is insignificant in terms of the subject of proof may be omitted from the criminal file.

In a situation where an accused person and the defence counsel do not know all the information – for example, if the accused person has no information about the interaction between other accused persons and third parties and there is no legal basis for the accused person to obtain this information – it may happen that the evidence that can actually vindicate the accused person is not submitted to the court, although the prosecutor's office has an obligation to ascertain also the facts that vindicate the person.

Execution of reports on surveillance operations and information included therein

It is usual in judicial proceedings that the time of a surveillance operation indicated in the report on the operation does not coincide with the actual recording time. Prosecutors have often stated that this is only a technical problem and that it is the content of the telephone call that should be considered. At least county courts accept this situation and do not consider it a violation of the criminal procedure law. Reports drawn up on the basis of recordings resulting from wiretapping or covert observation, under section 126[7] of the CCP, of messages transmitted via a public electronic communications network or information communicated by other means often contain the note "irrelevant text" in the middle of the text of the conversation or telephone call. Given that such a report is drawn up by a surveillance officer, not a person conducting the proceedings,

it does not seem to be appropriate to grant such a wide margin of discretion to the surveillance officer. As the defence counsel cannot present the recordings of surveillance operations to the accused, the recording of a wiretapped telephone call disclosed at the court hearing is essentially surprising evidence for the accused. If, after having listened to the recording at the hearing, the accused person argues that the recording and the report on the surveillance operation fail to objectively reflect the reality and that the continuation of the telephone call should be heard because it would disclose exculpatory facts, the law does not state whether there is a basis for meeting the request of the accused person, and if there is, how the facts disclosed on the accused person's request should be documented or how they should be established as evidence. The law does not state whether, in such a situation, a new report on the surveillance operation has to be drawn up and who should do so, or whether it is sufficient if the information heard from the recording is entered in the minutes of the court hearing. Nor is the extent to which the information should be entered in the minutes or the person determining the extent specified by the law.

Owing to the fact that the information obtained by surveillance operations is almost always obtained by using technical means and in many cases as a result of a covert entry, judicial review of that information should be substantive and thorough. Defence counsels have often wanted to know, for example, how the persons having a conversation in a windowless room, where a recording device had been installed, were identified, or how was it possible to record in the report, for example, "a sound resembling counting of money", "the person goes to another room" or "goes and takes the document". How and using which technical means the surveillance agency was able to ascertain these facts in a situation allegedly involving only wiretapping will become clear only in the course of judicial review, and the court should take this review very seriously.

Conversations with defence counsels entered in reports on surveillance operations

Criminal files on cases related to organised crime have recently come to include reports on surveillance operations which contain recordings of telephone calls between defence counsels (lawyers) and suspected/accused persons. These reports are also included in the list of evidence of the statement of charges. My view as a defence counsel is that reports containing such calls may not be presented as evidence or disclosed, given the clear prohibition in section 126^{7} (2) of the CCP. The criteria for applying the exemptions listed in that section (clauses 1–3) in cases where information submitted to a person with an obligation to maintain a professional secret are generally not met in the case of the reports on surveillance operations listed as evidence for the statement of charges.

The usual position of the prosecutor's office according to which the reports drawn up on the basis of the recordings of telephone calls between lawyers/defence counsels and their clients do not contain any confidential information is both irrelevant and incorrect. That position is irrelevant because, in the context of applying section 126[7] (2) of the CCP, there is no need to specifically analyse the nature of the information (i.e. whether it was confidential or not). That position is incorrect because section 43 (2) of the Bar Association Act expressly qualifies this information as confidential. One cannot deny the complexity of a situation where one and the same report on surveillance operations contains telephone calls between the accused person and third parties, as well as telephone calls between the accused person and the defence counsel. Owing to the foregoing, reports on surveillance operations containing such information should be dismissed as inadmissible evidence in their entirety.

In summary, I believe that wiretapping of a telephone conversation between a person and his or her lawyer/defence counsel and later inclusion of the conversation – in the form of a report on the surveillance operation – in the criminal case materials and use of the report as evidence are not acceptable. This practice should be condemned and a principled position should be taken that a lawyer has the right and duty to request the removal of such a report from the materials of the criminal case. In cases where the lawyer whose telephone calls are included in the materials of the criminal case does not act as the defence counsel at the court hearing and who, therefore, cannot submit such a request, the court should regard the report on the surveillance operation containing these telephone calls as inadmissible evidence on its own initiative.

Reports on surveillance operations as prosecution's evidence

According to section 154 (2) 4) of the CCP, the main part of a statement of charges has to set out the evidence in proof of the facts which are the basis of the charges and a reference to the facts which are intended to be proven with each piece of evidence. A list of evidence for the statement of charges also includes reports on surveillance operations.

When setting specific requirements for reports on surveillance operations, the legislature was guided by a desire to ensure the substantive quality of the procedural document, because the report reflects not only the result of the surveillance operation, but also its course and the conditions that serve as the basis for evaluating the admissibility of the information obtained by the operation as evidence.

Reports on surveillance operations used as evidence may have a length of 1 to 500 or more pages. The question is how the content of this evidence should be

described in the statement of charges and whether and to what extent the prosecutor's office may expand, modify or otherwise deviate from what is described in the statement of charges during the judicial proceedings. If the report on surveillance operations contains, e.g., 100 tapped telephone calls, is the brief description in the statement of charges applicable to all the calls wiretapped and recorded in the report? If the description does not apply to each and every call, what about the recordings heard in the courtroom that are in no way associable with the description, given in the statement of charges, of what the report on surveillance operations is supposed to prove? There have been heated disputes between prosecutors and defence counsels in the courtroom on the ground that the counsels are not able to exercise the right of defence, because they do not understand what the particular report and recording of a surveillance operation are intended to prove, considering the charges. The usual response of prosecutors is that they would explain this in the summations. It is obvious that the exercise of the right of defence is not guaranteed in such a case.

However, especially at the beginning of a trial, the court is in a situation where it can base its decisions on the statement of charges and the statement of defence, as well as on the assumption that the evidence presented by the prosecutor's office will support the charges. Since the court has to decide on a request of disclosure of evidence before the evidence is actually submitted, not knowing the content of the evidence and being based only on the request of the party wishing to submit the evidence, the only way to refuse to accept the evidence is to rely on the argument that the evidence was obtained by unlawful surveillance. If the court has not reviewed the legality of the surveillance by that time, it will usually solve the situation by stating that it will give its assessment of the evidence in the judgment. As a result, hundreds of pages of reports on surveillance operations are submitted and disclosed for weeks and months, and most of the reports have no bearing on the proof of the charges.

It is natural to expect – and the idea of the legislature was – that reports on surveillance operations provide information to the court on the facts relating to charges which the prosecutor's office cannot prove by other evidence. Reports on surveillance operations are normally not needed to prove facts that are proved by other evidence whose disclosure and review is less labour-intensive for the court. There is no need to submit reports on surveillance operations in order to prove facts that no one has ever questioned (e.g. that persons know each other), yet it is done. If the prosecutor's office abandoned this practice, the duration of court hearings would become significantly shorter and thus the costs of legal proceedings would also be lower.

Problems relating to the regulation of surveillance operations in the Code of Criminal Procedure

I will now point out the surveillance operations in the case of which the law allows for different interpretations.

Police agent

In the absence of judicial practice involving the application of these surveillance operations under the Code of Criminal Procedure effective from 1 January 2013, I will present a theoretical discussion of the problems that may arise in the event of the use of police agents.

According to section 126[9] (1) of the CCP, a police agent is a person who collects evidence in a criminal proceeding by using a false identity. According to subsection (2) of that section, a police agent may be used under the written permission of the prosecutor's office, which is granted for a period of up to 6 months. This term may be extended by 6 months. The law – specifically section 126[9] (5) of the CCP – gives the opportunity to indefinitely keep secret, based on an order of a prosecutor's office, the fact of using a police agent or the identity of the police agent after the completion of the surveillance operation if disclosure of that information may endanger the life or health, honour and good name or property of the police agent or the persons connected with him or her or his or her further activities as a police agent. Therefore, it is very likely that persons will never be notified about the surveillance operations conducted with regard to them in which a police agent was used. In addition, the law does not state whether and how information on using a police agent should be included in the materials of the criminal case, or whether and how the defence counsel can obtain that information. It is possible that, due to the secrecy requirement, the defence counsel and the suspect/accused will never know that a person who was questioned as a witness during pre-trial proceedings and/or in court is actually a person who actively participates in surveillance operations and whose aim is to gather evidence supporting the suspicion of crime or the charges. The reliability of the testimony given by such a person as a witness is not clear. In the cases where a police agent is used, only the prosecutor's office knows about the surveillance operation. Thus, the court does not and cannot know that persons whom the prosecutor's office requests to be heard in court as witnesses are actually police agents. In a situation where the statement of charges does not refer to reports on surveillance operations as evidence, the defence counsel cannot request the court to review the legality of the surveillance and the court cannot take possession of the surveillance files. Nor will the court know that the witness who gave incriminating information was in fact a police agent. This situation may seem unbelievable, but none of the provisions of criminal procedure law provides assurance that it cannot happen.

A situation where, in the judicial proceedings of a criminal case, the defence counsel requests the review of the legality of surveillance, referring to the data of surveillance operations, is complicated. Section 126[11] of the CCP regulates the keeping of surveillance files, stating that data obtained by a surveillance operation have to be recorded in a surveillance file. Analysing the Code and the "Procedure for keeping and storage of surveillance files" established by the Government of the Republic Regulation No. 3 of 3 January 2013 under the Code, it can be concluded that it is possible to a prepare a surveillance file for each surveillance operation, which also excludes the possibility of information on the use of police agents reaching the court. However, even if that information reaches the court, it is not possible for the court to disclose that information to the defence counsel due to the need for protection mentioned above. Such a situation is clearly contrary to the principle of adversarial proceedings and enables the prosecutor's office to present evidence to the court whose reliability cannot be verified by the defence counsel. It should also be kept in mind that the testimony of a person who carries out surveillance operations in cooperation with the body conducting pre-trial proceedings does not have the same quality as the testimony of a "regular witness".

Staging

According to section 126[8] (1) of the CCP, the staging of a criminal offence is the commission of an act with the elements of a criminal offence with the permission of a court. Unlike the provisions on the use of police agents, section 126[8] (2) of the CCP states that, if possible, a staged criminal offence should be photographed or filmed or audio or video recorded. Thus, there is hope that all the events can be reproduced in the court proceedings. However, the CCP does not specify how the person staging the offence should be treated. I am currently acting as the defence counsel in a criminal proceeding where the pre-trial proceeding has been completed and a person staging an offence was used for supporting the charges. Because the proceedings are in the phase in which the prosecutor's office is making decisions on the defence counsel's requests to issue applications and authorisations for conducting surveillance operations, I can state at this moment that the materials of the criminal case do not include a report on surveillance operations containing information on the use of a person staging a criminal offence, and I do not know whether such a report has been drawn up or not. The person who participated in the criminal offence by staging it has been questioned as a witness and as he has met with the suspects, I presume that the prosecutor's office will request that he be heard as a witness in the court proceedings. The law, however, does not provide for such an opportunity, and rightly so, because a witness is a person who knows the circumstances related to the subject of proof. A person staging an offence, on the other hand, is a person who commits an act with the elements of a criminal offence. Therefore,

this person has no information on the circumstances related to the subject of proof; he or she is a person who commits a crime with the suspected person. Despite the fact that this criminal offence took place under the control of public authorities, the person who committed it cannot be a witness and questioning him or her as a witness should not be allowed.

Covert surveillance

According to section 126[5] (1) of the CCP, a prosecutor's office has to issue an authorisation for covert surveillance of persons, things or areas, covert collection of comparative samples and conduct of initial examinations and covert examination or replacement of things for up to two months. The prosecutor's office may extend the term of the authorisation for up to two months at a time.

Covert surveillance of a person and place and wiretapping with the permission of a court usually take place at the same time. According to the current practice, a single report on surveillance operations is drawn up on the different surveillance operations carried out under the authorisation of a prosecutor's office and a court. As criminal cases involving such evidence have not been subjected to judicial review yet, it is not clear whether such combined evidence has the quality of the evidence set out in section 2861 of the CCP or should separate reports still be drawn up on different surveillance operations. Judicial review of such a combined report might prove difficult because at the court hearing recordings of intercepted calls would have to be disclosed alternately with video clips taken during covert surveillance. When analysing and evaluating the text of reports on covert surveillance, it appears that they do not set out the source of the initial data concerning the object of covert surveillance or the person who knew the individuals so well as to be able to specify their personal identification codes in the descriptive part of the report (I mean those individuals with regard to whom an authorisation for conducting a surveillance operation had not been issued). As a result of covert surveillance, the verbal activity, such as instructing, is described in exact terms. The question is how such information can be collected by covert surveillance and what is the role of presumptions and assumptions about possible events in such a report. This leads to the question of whether, in such a case, the surveillance officer has entered his or her assumptions in the report or if such an operation amounts to illegal surveillance in the course of which the surveillance officer clearly exceeded the limits specified in the authorisation.

Does an authorisation to conduct surveillance operations contain a state secret?

As a rule, documents underlying surveillance operations – in particular, authorisations of the prosecutor's office, applications of the prosecutor's office, and court rulings – are deemed to constitute a state secret under section 8 (1) of the State Secrets and Classified Information of Foreign States Act. According to that provision, the following are treated as state secrets related to the maintenance of law and order: "information collected by surveillance agencies in the course of surveillance, and the methods, tactics and tools used for collection thereof, except information whose disclosure would not damage the security of the Republic of Estonia. Such information is classified at the 'top secret' or lower level for a maximum period of 50 years. Classification will expire insofar as such information was included in a criminal file or communicated to the person with regard to whom the surveillance operation was conducted or to another person whose privacy or family life was violated by the operation."

Thus, only information that concerns the methods, tactics and tools used for surveillance and information collected in the course of the surveillance whose disclosure would damage national security can be a state secret. Admittedly, disclosure of information on the methods, tactics and/or tools used for surveillance may be a threat to national security in many cases. The disclosure of such information may mean that these tools or methods cannot be used any more. At the same time, however, disclosure of information collected by surveillance generally is not a threat to national security, which is why classification of such information is not appropriate. Information collected in the course of surveillance carried out for the purpose of investigating the offences against the state specified in Chapter 15 of the Penal Code probably constitute an exception to the rule in the previous sentence.

For many years, defence counsels were refused access to both prosecutor's offices' applications for authorisation to conduct surveillance operations and the authorisations issued by courts, not to mention other materials on surveillance files, referring to provisions concerning state secrets. The procedural practice has changed somewhat in this respect recently. Usually, defence counsels are given access to authorisations of surveillance issued by courts and, in some cases, prosecutor's offices' applications for authorisation to conduct surveillance operations.

I am not aware of any cases where, regardless of the content of an authorisation of surveillance issued by a court or a prosecutor's application for an authorisation of surveillance, these documents were not classified from the moment of their issuance. This policy of indiscriminate classification is not consistent with the requirement of fair proceedings. As a rule, all other information collected

in the course of or in connection with surveillance and included in surveillance files remains classified. Yet this information is often essential to effective defence.

To ensure fair proceedings, given the current rather general practice of excessive and unjustified classification of information, courts should assess whether the classification of information related to surveillance operations is justified and develop their position in this regard.

An interesting example from the practice of the European Court of Human Rights (ECtHR) in relation to obstacles to the exercise of the right of defence under the pretext of a state secret is the judgment in the case of Mirilashvili v. Russia. This judgment highlights the need to ensure that the withholding of information, which is considered to be a state secret, from a defence counsel is counterbalanced, in particular, by active measures of the court.

The ECtHR considers that in situations where a defence counsel is not able to examine certain information, as it is declared a state secret, this information should be made available for examination to the court adjudicating the case. The duty of the court is to ascertain whether the materials to which the defence counsel was refused access would have been of assistance for the defence of the accused and whether their disclosure would have harmed any identifiable public interest (or national security for the purposes of section 8 (1) of our State Secrets and Classified Information of Foreign States Act).

In conclusion

This article focuses on the questions that have arisen in connection with surveillance operations and to which the current law does not provide answers. The discussion of these issues is intended to point out that the activities of public authorities in organising surveillance are inadequately regulated by the Code of Criminal Procedure. This creates a situation where the provisions on access to information on surveillance operations do not guarantee that a person subjected to surveillance can examine the data collected by surveillance operations and, where necessary, take possession of the data in a format that can be played back. This opportunity, however, may prove necessary to exercise both the right of appeal and the right of defence. Deciding on the use of reports on surveillance operations as evidence in judicial proceedings remains a discretionary power of courts. Discretionary power, however, should be used in a framework defined by law. The current criminal procedure law does not set such a framework. Without disputes initiated by the accused and his or her defence counsel, judicial proceedings could be shorter, if the Code of Criminal Procedure provided for the rules on when and how a court should review the legality of surveillance and evaluate the admissibility of reports on surveillance operations as evidence.

Leading questions – the concept and the prohibitions related thereto in cross-examination

Margus Kurm,
Lecturer in criminal law and criminal process, Faculty of Law of the University of Tartu

This article discusses two issues that, in the author's opinion, have been a little crosswise in the current provisions of cross-examination from the beginning, or gone crosswise in case law. Both relate to leading questions and prohibition thereof during first and second examinations.

Leading questions during a first examination

According to section 288 (2) of the Code of Criminal Procedure (CCP), it is prohibited to pose leading questions during a first examination without the permission of the court. The law does not explain what these questions are. The need for a legal definition of leading questions was discussed in 2010, when the CCP's provisions on judicial inquiry were supplemented considerably.[1] The prevailing opinion back then was, however, that the definition of a leading question, as well as other inadmissible questions, should be left to case law. The Supreme Court has now made the first step but, unfortunately, in the wrong direction, as the author of this article believes.

I am thinking of the ruling of the Criminal Chamber of the Supreme Court in case no. 3-1-1-50-13, which provides the following in respect of leading questions in paragraph 15.2:

1 I am referring to the draft Code of Criminal Procedure Amendment and Other Related Acts Amendment Act (599 SE), the amendments introduced by which entered into force on 27 January 2011.

> "Since the charges brought against H. Vatter contained, inter alia, hitting the victim, the question of **whether the victim was hit** cannot be regarded as anything other than a leading question. Unlike the prosecutor's submission, even specifying questions posed during a first examination within the scope of cross-examination must be asked, for example, as follows: what happened then, what else did the accused do, did anything else happen, and so on. The cross-examination of the witness in the manner described above, therefore, did not comply with the first sentence of section 288 (2) of the CCP."

Thus, the Supreme Court has declared a simple yes-no question to be a leading question and forced persons who are the first to question a witness to "beat about the bush". In addition to being incorrect, this approach also works against the objective of a first examination to present the facts relevant to the adjudication of the case in an understandable manner, through the witness and without wasting time.

A simple yes-no question such as "Did A hit B?" is not a leading question, as it does not suggest an answer that the questioner is expecting. There are two equal answers – "yes" and "no" – and the question itself does not contain any guidance as to which of the answers would please the questioner. The situation is different if the question is worded, for example, as follows: "And then A hit B, right?" or "Do I understand correctly that A then hit B?" or "I think you forget that A then hit B. Was that so?" These questions, too, can be answered with "yes" or "no". The difference, however, lies in the fact that the question says what the questioner knows, i.e. which answer the questioner believes to be correct. "Right?", "Do I understand correctly?" and other similar expressions give a clear hint as to what is the right answer in the questioner's view.

The nature of leading questions is especially evident when putting oneself in the shoes of the person questioned, who does not know the right answers, but would like to know. For such a person there is a big difference between the questions "Did A hit B?" and "A hit B, right?". Indeed, the need for the prohibition on leading questions derives from the fact that during a first examination the witness is usually favourably disposed towards the questioner. Therefore, there is reason to believe that the witness tends to agree with the questioner, i.e. follow the direction given by the questioner.[2] This is not at all about unlawful pre-trial influencing, but just a general human observation that people want to please an authority (and the prosecutor or lawyer often is an authority for a witness).

---

2 Edward J. Imwinkelried. Evidence Foundations. 7th ed. LexisNexis 2008, page 5.

In short, a leading question suggests a certain answer.[3] A simple yes-no question does not contain a suggestion and should thus not be prohibited, either in a first or a second examination. If anything, a yes-no question points to what is considered relevant. But there is nothing wrong with that. On the contrary, the witness should be asked the things that are relevant to solving the case.

That brings me to the objective of a first examination, and I will try to show how the prohibition on yes-no questions established by the Supreme Court can hinder its achievement. A first examination is not an examination in its traditional sense. In normal circumstances, questions are asked with a view to learning something. A person who gets to examine a witness first has a different goal. The questioner will not pose questions so as to learn some information, but in order to have the witness tell the court what the questioner already knows from the data of the preliminary investigation. Thus, the objective of a first examination is not to ascertain what the witness has experienced, but have the witness retell this to the court.[4] The questions are intended to aid the witness in this. They have to help the witness tell his or her story, while also ensuring that the

---

3 This definition of 'leading question' is rooted in the common law countries, where cross-examination comes from. For the United States see, for example, E. J. Imwinkelried (reference 2), page 5, or Thomas A. Mauet. Trial Techniques. 7th ed. Aspen Publishers 2007, page 465; for England, see Adrian Keane, Paul McKeown. Modern Law of Evidence. 9th ed. Oxford University Press 2012, page 165; for Scotland, see Alastair L. Stewart. The Scottish Criminal Courts in Action. Edinburgh, Butterworths 1990, page 132. The definition of 'leading question' was also provided in section 489 of the first Code of Criminal Procedure of the Republic of Estonia: "Questions posed to a witness shall be concise and easy to understand, and a question shall not be presented in a form which inspires the answer."

4 This is why the intention of the Estonian legislature to regulate a hearing carried out in the investigator's office similarly to cross-examinations at a court hearing (see the cross-references in sections 68 and 288 of the CCP) seems somewhat strange. After all, the investigator is not aware of what the witness knows. A hearing is conducted precisely in order for the investigator to learn this. The task of the investigator is to determine, as accurately as possible, what the witness saw, heard, or otherwise sensed. If the witness needs to be helped with leading, hypothetical or alternative questions, then this must be done. All people are just not able to explain things in a free form and in an understandable manner, and all do not know what the necessary elements of criminal offences are. It may also happen that the witness is hostile towards the investigator or hides the truth for some other reason (such as fear of the suspect). Hearing such a witness without the right to ask leading questions (section 68 (4) allows leading questions to be asked only in the cases specified in section 2881 (2)) is an impossible task. If an investigator were to strictly observe section 68 (4), he or she would not have the right to ask even the reason for the witness' reluctance, because it is not part of the subject of proof. Section 68 (4) is strict in this respect: "A witness may be heard only as regards the facts relating to a subject of proof." In summary, a hearing carried out during the preliminary investigation and a cross-examination in court are fundamentally different things. In the former case questions are asked in order to learn information from the witness, and in the latter case questions are posed so as to demonstrate the knowledge of the witness to the court. The author cannot understand the desire to subject them to the same rules and also deems it unrealistic. Strict observance of the rules specified in section 68 (4) may render an effective hearing impossible in many cases.

witness (a) tells about relevant things (b) in a comprehensible manner and (c) without wasting the court's time.[5]

But why are questions necessary after all? Why could witnesses not just submit their story as a free narrative? In theory, they could, but in practice the vast majority of people are not capable of doing so. Even the message of the simplest narrative tends to get lost in the jumble of digressions and remarks. This is quite understandable, because even a simple event (such as witnessing a beating) is composed of more than one dimension – the time and place, the actions of the offender, victim and witness, the location of the witness, etc. Telling about everything fluently and comprehensibly is generally not accomplishable for a person. In addition, the problem could also be in the listener. In his book *Articulate Advocate*, Brian K. Johnson, who specialises in enhancing litigators' process-related skills, emphasises that the human brain acquires information best when it comes in small chunks.[6] If a witness tells the whole story fluently at once, then the general impression is stored, but not the details. This is why, in order to ensure that the court understands everything, the story of the witness must first be disassembled into bits and then reassembled with the help of specific questions. It should be remembered that in England (the home of cross-examination) and other common law countries, the guilt of a person is decided by a jury, i.e. people in the street. Therefore, ensuring that they can understand everything is not their own worry (as one might say of professional judges), but primarily the responsibility of the state. The rules of cross-examination have been developed over time to ensure the best understanding of the jurors.

I will give a simple example to show that the prohibition on yes-no questions does not in any way ensure a better understanding of the relevant circumstances or save the time of the court. Let us assume that the question of whether or not the sun was shining on the day of a criminal act is of great importance in the proceedings (it can be very important in the case of, e.g. a road accident). Since the sun must not be mentioned, the person who examines the witness first has to begin in an indirect manner, asking, for example: "What was the weather on that day?" Then the dialogue could proceed as follows:
"It was warm."

---

5 For example, in the Federal Rules of Evidence (hereinafter: FRE) of the United States, the prohibition on leading questions can be found under Rule 611 entitled "Mode and Order of Examining Witnesses and Presenting Evidence", in which the general clause reads as follows: "The court should exercise reasonable control over the mode and order of examining witnesses and presenting evidence so as to: (1) make those procedures effective for determining the truth; (2) avoid wasting time; and (3) protect witnesses from harassment or undue embarrassment." The FRE are available online at http://federalevidence.com/rules-of-evidence.

6 Brian K. Johnson, Marsha Hunter. The Articulate Advocate. New Techniques of Persuasion for Trial Lawyers. Crown King Books 2009, page 79.

"What do you mean by warm?"
"Well, it was a warm summer day."
"How warm?"
"I don't know exactly. Some 20 degrees for sure, I think."
"Can you say where the warmth came from?"
"What do you mean, "where it came from"? It was actually warm outside. The air was warm."
"What made the air warm?"
"The sun."

Time passes, but nothing of importance is clear. The word "sun" has been uttered, but it will take some more time to find out whether it was shining or just warmed the air through the clouds. It cannot be asked directly. The worst thing that this game of guessing entails is that the witness will be absolutely confused by the fourth question. He understands that he does not understand anything. But what? Rising adrenaline levels further inhibit the thinking process. The result may be that the witness never regains self-confidence, resulting in a large part of his evidence going unrealised. Is this in the interests of proceedings? I do not think so. Judicial proceedings are not a word guessing game such as Alias where the rules have been designed so as to make the game more difficult and thus also more fun for the players. The rules of judicial proceedings should support bona fide witnesses instead of misleading or confusing them. During a first examination, a witness must not be prompted for answers, but it must be possible to ask all the questions that are needed.

Leading questions during a second examination

Another fundamental problem involving leading questions in the current law relates to second examinations. Namely, according to section 288 (3) of the CCP, leading questions must not be posed concerning new facts without the permission of the court during the second examination.[7] In light of the classical canons

7 The situation is even worse when the text of the CCP is strictly observed. Namely, section 288 (51) requires courts to consider the provisions of section 2881 when permitting leading questions. Section 2881 (1), however, expressly states that a court may permit leading questions to be posed during the first examination. Consequently, during the second examination leading questions may be posed only in accordance with section 2881 (2). However, if the obstacles specified in subsection (1) are encountered – the witness is hostile, hides the truth or absconds from replying to questions – the obstacles must not be overcome with the help of leading question during the second examination.

of cross-examination,[8] this prohibition is incomprehensible and contrary to the objective of a second examination.

A second examination is not a first examination in respect of new facts, as it is sometimes thought. First and second examinations are two different things with fundamentally different functions. As explained above, the purpose of a first examination is to help the witness tell a story concerning a fact of an offence (or concerning the proceedings). The stories necessary for the prosecutor are told by the prosecutor's witnesses, and the stories necessary for the defence counsel are told by the counsel's witnesses. This is why in the case of the prosecutor's witnesses the prosecutor is the person who examines a witness first, and the defence counsel is the second person to examine that witness, and vice versa. A second examination is mainly intended to undermine or attack the credibility of the counter-party's witness. The questions are not posed with a view to letting the witness tell his or her story, but in order to show that the witness cannot be believed. The witness is wrong, hides the truth for some reason or is simply a liar, a person who cannot be blindly trusted.[9]

This usually means that uncomfortable questions are posed to the witness in a second examination which he or she does not want to or cannot honestly answer. Therefore, the relationship between the questioner and the witness is expected to be different compared to the first examination. While in a first examination it is assumed that the witness is friendly, the assumption is *a priori* the opposite in the second examination – the witness is hostile or evasive. In other words, the exceptional cases set out in section 288[1] (1) of the CCP in which leading questions are allowed are the rule in a second examination. Consequently, leading questions which are allowed during a first examination by way of exception should be allowed during the second examination without the judge's permission. Otherwise, there will be no effective attack on credibility and hence there will be no effective defence. After all, there is not much that a defence counsel can do other than undermine the credibility of the prosecutor's witnesses.

---

8 The second sentence of Rule 611 c of the FRE (reference 5) simply states that leading questions are generally allowed during the second examination, regardless of which facts the questions would be asked about. For explanations, see E. J. Imwinkelried (reference 2), page 7. Similar rules exist in the English and Scottish law; see, A. Keane, P. McKeown (reference 3), page 194, and A. L. Stewart (reference 3), page 132, respectively. Guidance for practitioners is more straightforward in this regard. The generally accepted recommendation is to only use leading questions; see, for example, T. A. Mauet (reference 3), page 258, or Irving Younger. The Art of Cross-Examination. The Section of Litigation Monograph Series. No 1. American Bar Association, 1976, page 22.

9 For the objectives of a second examination in the United States, see, for example, T. A. Mauet (reference 3), page 254; in England, see A. Keane, P. McKeown (reference 3), page 194; and in Scotland, see A. L. Stewart (reference 3), page 134.

As to why leading questions are effective can be explained from the viewpoint of the answerer. First, a leading question does not leave time for reflection. Suppose, for example, that the defence counsel has obtained a fake diploma from the University of Tartu allegedly issued to the witness, and the defence counsel knows that the witness used it when applying for a job three years ago.

If leading questions are permitted, the counsel can go straight to the point and ask directly: "When you applied for the job, you used a fake diploma from the University of Tartu to demonstrate your education. Was that so? Please answer yes or no." The witness must answer immediately because time is working against him. The longer the witness thinks, the more the judge is convinced that the defence counsel's argument must be true. Forging a university diploma is not the kind of thing that an honest person would simply forget. Consequently, the witness must choose the answer within a couple of seconds. And all the options are bad. If he says "yes", he admits his dishonest behaviour. If he says "no", he risks being caught in a lie in the next few questions. Moreover, the first answer shows that the witness can lie even in court. The third option is to answer "I don't remember". This is not better than denial, however. Not remembering using a fake diploma is not believable, i.e. it sounds like a lie in court. An experienced defence counsel would let the lie be repeated, asking again in astonishment: "You don't remember whether or not you used a forged document?"

When approaching the issue with open-ended questions, the witness will have a lot more time for reflection. For example, the defence counsel could start with this question: "Which documents did you present when applying for the job?" Now the witness can immediately take some time off and answer, for example: "Oh, it was a long time ago. I have to think about it." A person who does not know what it all is about will not consider thinking about such a question to be suspicious. The answer "I don't remember" is not, *a priori*, out of the ordinary either. So there will be time during which the witness can collect his thoughts and make a plan for how to get out of the plight. Ultimately, of course, he has to say something. The examination can then proceed as follows:
"I remember there being the CV and a letter of motivation. It's possible that there was something else." *(There is no obvious lie in this answer. Nor is there clear hostility, reluctance or failure to recall, which would entitle the defence counsel to apply for the permission to pose leading questions under section 2881 (1).*
"Try to remember then. Was there anything else?" (*Of course, this question can be asked on the condition that the court does not regard simple yes-no questions as leading questions.)*
"I can't remember right now."
"Did you present a document to demonstrate the required level of education?
"I did present something, yes."
"What?"

"A bunch of continuing education certificates, as I recall."
"Anything else?"
"A diploma, I guess."
"Which diploma was it?"
"From the University of Tartu."
"Was the diploma genuine?"
"What do you mean by that?"
"Well, authentic, not forged?"
"I haven't forged anything."
"I never indicated that you did."I asked whether the diploma was forged."
"I don't know. I got it from a friend."
"Have you graduated from the University of Tartu?"
"No."

It is also possible to start at the other end, asking, for example, right away:"Have you studied at the University of Tartu?"This way, the question about the diploma can be asked sooner, but more time will be spent to get to the fact and circumstances of the use of the fake diploma. After all, forging a document without an objective of using it is not equally as objectionable as the intentional use of the forged document. In any event, it will take much more time getting to the point, using open-ended questions, and all that time the witness can think about what he is going to say. In addition, it makes it possible for the witness to check what the questioner knows, or guess, based on the conduct of the questioner, whether or not the latter actually has got the fake diploma. In the case of a"straight-to-the-point" leading question, the witness has to make a decision within a few seconds, because as was noted, time is working against him.

The second advantage of a leading question is, indeed, the fact that it gives a clear message that the questioners knows how things really are. First, the questioner wins attention. The court will immediately realise that the defence counsel has something to say and is not angling or just wasting time. The third advantage is that in the case of a straightforward question the answerer tends to think that the questioner actually knows the truth, and will thus confess. A person faced with a fact and having too little time to think is a poor decision-maker. It is good when the deceit of the witness comes to light in court.

The foregoing is not intended to argue that leading questions are the only effective tactic to reveal untruth and cover-up. A defence counsel can also expose the weaknesses of a witness insidiously, catching the witness out on a lie with the help of cleverly arranged open-ended questions. What I want to say is that a defence counsel should be able to choose the tactic of a second examination. It is part of the right to real and effective protection provided for in section 8 of the CCP. And the question is not only about the right of defence, but also about the

ultimate objective of judicial proceedings to find out the truth or at least come close to the truth. Effective means that can be used in a second examination are equally necessary for the prosecutor, who is the second person to question the accused and the defence counsel's witnesses.

It should be noted for the sake of clarity that, apart from undermining a witness' credibility, a second examination has another function – to make the witness admit the facts that are in the interests of the party conducting the second examination.[10] Of course, the testimony given in the first examination can be clarified or re-examined during the second examination. However, such clarification or re-examination must have a certain purpose, and this purpose usually is the idea of having the witness state more clearly or repeat the facts that are useful for the person conducting the second examination. There is little point in clarifying harmful testimony – and the testimony of the witness summoned by the person conducting the first examination is usually harmful. Why let the witness repeat something that is painful to listen to? The first sentence of section 288 (3) of the CCP mentions the verification of the testimony given in the first examination. This can be interpreted as meaning, on the one hand, re-examination of the testimony as described above or, on the other hand, verification of credibility by means of highlighting any inaccuracies or inconsistencies in the testimony. However, verification of credibility on the basis of other circumstances – those relating to the person of the witness – must take place in accordance with the second sentence, i.e. without the right to pose leading questions. *De lege ferenda* it might be wise to reformulate section 288 (3) based on the circumstances that constitute the subject matter of questions, rather than the objective of the person posing the questions. Prior to that, of course, it is necessary to determine the purpose of subsection (3) – prohibiting leading questions – which the author believes to be wrong – or delimiting the issues that can be discussed during a second examination. Common law countries have opted for the latter in order to keep the cross-examination and thus the whole trial within reasonable limits. For example, Rule 611 b of the Federal Rules of Evidence of the United States (reference 5) states that a second examination should not go beyond the subject matter of the first examination and matters affecting the witness's credibility. The court may allow inquiry into additional matters.

10 In English, the word 'elicit' is also used, which dictionaries define as 'call forth', 'draw out' as well as 'provoke'. See, for example, T. A. Mauet (reference 3), page 254; A. Keane, P. McKeown (reference 3), page 194; or A. L. Stewart (reference 3), page 134.

In conclusion

Cross-examination and leading questions appeared in Estonian criminal procedure law in 2004 when the Code of Criminal Procedure was adopted. Twelve years is a short time for a Code and so it is not surprising that some of the new concepts and institutes are still looking for their appropriate content and purpose. If the above ideas and references can show the way in searches related to leading questions and prohibitions related thereto, then the article will have accomplished its purpose. The author would be particularly pleased, however, if this article could facilitate the settlement of disputes over the admissibility of one or another question in a specific court case. The admissibility of an individual question is rarely so important as to warrant an argument that lasts for more than a few minutes. Then the court should make a decision and the parties should continue their work.

Corruption in the private sector, or the private sector in corruption: significance of the Supreme Court's case law for the relationship between corruption offences and offences against property

Dmitri Teplõhh, attorney-at-law
Marko Kairjak, attorney-at-law

1. Introduction

This article was inspired by the participation of one of the authors in the criminal case involving T. Elias, a former employee of Rimi, as the representative of the victim (rulings of the Criminal Chamber of the Supreme Court in cases no. 3-1-1-84-14 and 3-1-1-41-15). To the other author, the issue of relationship between corruption offences and possible offences against property in the private sector loomed when the current cornerstone of criminalisation of private-sector corruption (sections 402[3] and 402[4] of the Penal Code, PC) was prepared during the recent revision of the PC, with the author being the head of one of the working groups involved in the revision.

In principle, one must welcome the first serious and substantive judicial decisions made in respect of private-sector corruption as such.[1] Several recent and widely discussed criminal cases have ensured the necessary public attention to this phenomenon and the first academic writings have been published.[2] It should be noted, however, that the discussion of this subject is still in its infancy in terms of theoretical treatise and we will have to wait for more case law and pinpoint academic positions for many more years to get answers to the questions

1 See, in particular, the abovementioned rulings of the Criminal Chamber of the Supreme Court in cases no. 3-1-1-84-15 and 3-1-1-41-1.

2 See, in particular, S. Kruusma. Erasektori korruptsiooni regulatsioon Eestis. Juridica 2015, 7, pages 490–497.

that are currently unclear. There are plenty of problems involved in the interpretation of the necessary elements of offences. The authors will not attempt to go into the probably must burning problem – relationships between the recently adopted sections 402^3 and 294. Also, the apparently problematic elements in section 402^3 – 'interests' and 'person with authority to carry out economic activities' – will have to wait for interpretation in future case law.[3] Consideration will also have to be given to the issue of social adequacy mainly raised in German legal literature (and section 402^3 is presumably largely based on section 299 of the German Penal Code (StGB)): should we treat borderline cases in the private sector with a greater degree of tolerance, i.e. accept free business lunches, expensive souvenirs etc., which, at least in the public sector, are not considered to be admissible these days.[4]

However, the authors will make a modest attempt to address the questions which are the most important from the point of view of a private legal person in the context of private-sector corruption: which duty is breached by a corrupt act on the part of an employee or a member of a management body of a legal person and, in the cases where a person receives something, should the person be blamed for receiving that "something" (section 402^3) or for thereby damaging the interests of the legal person (an offence against property – either section 201 or section 217^2 of the PC). To clarify the following – it so happened that one of the authors of this article had to run a workshop at the conference on corruption organised by the Ministry of Justice on 11 February 2016, where the participants were asked to resolve the following case (described in brief):

> Indrek works at the procurement unit of a large manufacturing company. He is in charge of procuring supplies necessary for the operation of the company – from office supplies to production equipment, seeking to find the best value for money. At one point, the employer needs to upgrade the company's IT equipment, and Indrek's task is to organise the procurement procedure. One of the participants in the procurement procedure is Indrek's classmate Rain, who contacts Indrek personally and offers him an incentive of 5% of the transaction value if Rain's company will be declared the successful bidder. Indrek takes a couple of days to think about it and eventually agrees to Rain's offer. He finds that no harm will be done, as the bid of Rain's company was one of the two best anyway, so no one will suffer any direct damage. Rita, the second best bidder, learns

3 See in this regard the judgment rendered by Tartu County Court in settlement proceedings, 11.05.2015, 1-15-3054.

4 For an introduction to this issue, see U. Kindhäuser. H. Paeffgen. Strafgesetzbuch. 4. Aufl. Baden-Baden, 2013, section 299, page 39. Examples: H.-J. Rudolphi (Hrsg.). SK-StGB. sections 267–323c. Köln, 2013, section 299, pages 43-44.

through an employee of Rain's company about how the successful bidder was selected, and she notifies Indrek's employer.

Mr. Ginter, a colleague who ran the workshop together with the author, aptly summed up the main problem of the case as the "everybody-is-smiling problem"[5]: the procurement manager was left with some extra, Rain got the order and Indrek's employer got the contract based on the lowest bid. Prior to embarking on further analysis, it seems appropriate to take a look at the question of which legal values are damaged by corruption in the private sector. The most adequate source for this is the aforementioned Rimi case (ruling of the Criminal Chamber of the Supreme Court in case no. 3-1-1-84-14). Then it is appropriate to address the question of whether the harmfulness of an act performed as a return favour for a bribe should be evaluated in substantive terms (i.e., whether the transaction is in line with the duty of due diligence) or not (the fact of accepting a bribe alone represents a breach of the duty of loyalty and the transaction need not be evaluated in substantive terms).

2. 2. Legal values protected in the context of private-sector corruption

Until 2014 there was no case law identifying legal values (in German, "Rechtsgut") in private-sector corruption cases protected by the pre-2015 section 293 of the PC. As a general principle, the general legal value protected under the provisions on breaches of the duty to maintain integrity (i.e., in particular, accepting and granting of gratuities or bribes) in the public sector is the persons' belief in the incorruptibility of those performing public functions and thus in the legitimacy of the decisions and activities of public authorities.[6] In relation to private-sector corruption, collective legal values such as economic development and free competition have been mentioned.[7]

Essentially, the impact of private-sector corruption on collective legal values should be different from that of corruption in the public sector.[8] Endangering an individual private legal person cannot have a significant impact on economic

5 "Everybody is smiling" (the workshop was held in English).

6 J. Sootak. P. Pikamäe (eds.). Karistusseadustik. Kommenteeritud väljaanne. Tallinn 2015 (comment 1 on section 294).

7 See also about the German StGB, U. Kindhäuser. U. Neumann. H. Paeffgen. Strafgesetzbuch. 4. Aufl. Baden-Baden, 2013, section 299, page 4. See also J. Sootak. P. Pikamäe (eds.). Karistusseadustik. Kommenteeritud väljaanne. Tallinn 2015 (comments 1.1.–1.2. on section 402^3).

8 Cf. the position that the legal values protected by section 402^3 of the PC are "honest and corruption-free economic activities in the private sector, as well as economic development and free competition" – J. Sootak. P. Pikamäe (eds.). Karistusseadustik. Kommenteeritud väljaanne. Tallinn 2015 (comment 1.1 on section 402^3).

development as a whole. Corruption in the private sector undermines, in particular, the employer's trust in its employees and increases the need to exercise additional supervision over employees and spend more funds on protecting the legal person's assets. If information on the corruption case becomes public, the company's reputation will suffer.

In the context of free competition, the opinion of counterparties, consumers and partners about the incorruptibility of those performing the legal person's functions and thus about the legitimacy of the legal person's decisions and activities is manifested in whether or not the consumers and partners continue cooperation with the company concerned. In an economy of free market and free competition, it is possible to choose the counterparty to a transaction. The existence of a good reputation and the question of reliability are often the decisive factors when making such a choice. In the private sector, a good reputation and reliability enable long-term business relationships to be established and a strong and stable company to be built. When reputation is damaged, it is the company itself that will suffer: customers leave for competitors, thus reducing the revenue; suppliers lose trust and refuse to continue cooperation, which inevitably increases costs, including due to the need to find new suppliers. Where partners' trust in a person is completely lost, that person's business can be considered ended. Thus, in the private sector, corruption ultimately damages the reputation and financial status of the employer if the latter is a company. The economy as a whole (and thus also collective legal values) does not suffer, at least as long as there are enough alternatives in the market – the bankruptcy or dissolution of a medium or even large company will hardly lead to a situation where collective legal values such as economic development and free competition can – even theoretically – be claimed to have been damaged. The place of a company that is bankrupt or has ended its business will soon be occupied by a new company. The authors find, therefore, that it is damage to individual legal values that should always be assumed in the case of corruptive practices in the private sector, while damage to collective legal values can occur only in exceptional circumstances.

However, before the abovementioned *Rimi* case the case law had emphasised that "many of the provisions specifying the necessary elements of a criminal offence, which were established first and foremost with a view to protecting collective legal values, essentially also protect individual values, and thus victims who are private individuals cannot be excluded."[9] In the criminal case of T. Elias, a former employee of Rimi, which has repeatedly been cited above, the Supreme Court held that the duty to maintain integrity applicable to an official governed by private law, which was provided for in section 293 of the wording

9 Ruling of the Criminal Chamber of the Supreme Court in case no. 3-1-1-97-10, p. 18, 19, 23.

of the PC valid until 1 January 2015, had been established primarily in the interests of the employer (e.g. a private legal person). The main reason why section 293 of the PC in conjunction with section 288 (2) penalised the acceptance of gratuities, including by an official with a position in a private legal person, is the need to protect the relationship of trust and loyalty between the official and the employer (legal person) which the official violates when accepting a gratuity.[10] Thus, section 293 of the PC was intended to protect the same legal value whose violation resulted in damage being caused to Rimi within the meaning of section 37 (1) of the Code of Criminal Procedure (CCP). The same also applies, mutatis mutandis, to section 4023 of the PC that entered into force on 1 January 2015.[11]

If we proceed from the assumption that in the case of corrupt acts committed in the private sector it is the individual legal values that should be assumed having been attacked, while the compromising of collective rights should be precluded (in particular because damage to collective legal values in the conditions of free competition is rather hypothetical), it follows that the legal provisions on private-sector corruption protect only individual legal values, particularly employers' right to the loyalty of their employees. Since in the private sector it is the employer who determines the extent of employees' duty of loyalty, corruption in the private sector can be a real challenge for criminal law. If we change only one fact in the case described in the introduction – Indrek's employer (company) knows about Indrek's activities, i.e. acceptance of the 5% incentive and declaration of the successful bidder on this basis, and tacitly approves it – then the case becomes quite controversial. Should, in this case, the employee's duty of loyalty be regarded as having been breached and the employee's behaviour considered to be unlawful, or is the behaviour lawful because the victim consents to it? If, in this case, the behaviour of the employee contains the necessary elements of an offence and is unlawful, the next question that may arise is that of the responsibility of the legal person, i.e. Indrek's employer, who is the victim according to the current case law. In turn, when such behaviour is no longer unlawful, because the victim consents to it, it is even more difficult to prove the necessary elements of a private-sector corruption offence, and they sometimes depend on the employer's desire to punish the person.

10 Ruling of the Criminal Chamber of the Supreme Court in case no. 3-1-1-84-14, page 40.

11 Ruling of the Criminal Chamber of the Supreme Court in case no. 3-1-1-41-15.

3. 3. Abuse of authority as a breach of the duty of loyalty

In the absence of current Supreme Court case law regarding the necessary elements of the offence, the authors will now describe the objective criteria of the offence as set out in section 402[3] of the PC (at least as the authors see them) to facilitate further analysis:

- criteria applicable to the subject: a person having authority to carry out economic activities in the interests of a person in private law, or an arbitrator;
- requesting, consenting to promising, or accepting a favour;
- in return for an abuse of authority (an equivalence relationship[12]).

The main question arising from the hypothetical case described in the introduction relates to the notion of abuse of authority, rather than the act of bribery as such. One cannot claim that the remaining objective criteria set out in section 402[3] of the PC are not met. The conformity of the employee's behaviour in that case to the objective criteria of an abuse of authority raises the question of whether the entry into a transaction which appears to be advantageous for the employer can be regarded as an abuse of authority at all. To put it simply – the authority of the employee included the right and duty to get the best offer, which he did and based on which he entered into the agreement.

Of course, it is possible to put forward a variety of arguments to the effect that the value of the bid could have been 5 percent lower without the bribe or that one should also consider whether the successful bid and the second best bid differed by 5 percent. During the revision of criminal law, section 402[3] of the PC was initially included among provisions on offences relating to competition (probably following the example of Germany where section 299 can be found under anti-competition offences and its stated objective is to protect competition).[13] This plan (fortunately) did not materialise in the case of our Penal Code. In the light of what has been discussed in section 2 of this article, therefore, the legal value protected by the provision concerned is quite clearly related to the duty to maintain integrity, or the individual legal value (i.e. property) of private legal persons (i.e., in our case, Rain's employer). Specifying any additional legal values should be avoided: first, due to the risk of excessive vagueness (for example, legal values such as 'fair competition', 'honest public procurement which is not subject to the Public Procurement Act', etc. seem absolutely frightening to the authors at first sight), and second, because the abovementioned Rimi

12 J. Sootak. P. Pikamäe (eds.). Karistusseadustik. Kommenteeritud väljaanne. Tallinn 2015 (comment 3 on section 402[3]). For specifying criteria in the German law, see H.-J. Rudolphi (Hrsg.). SK-StGB. Sections 267–323c. Köln, 2013, section 299, page 41.

13 U. Kindhäuser. U. Neumann. H. Paeffgen. Strafgesetzbuch. 4. Aufl. Baden-Baden, 2013, section 299, page 39.

case clearly illustrated the prosecutor's office's fear of finding itself in a situation where the number of victims is increased considerably in cases of private-sector corruption.

Thus, any alternative scenarios ought to be avoided. The legal question boils down to whether a transaction concluded by an employee or a member of a management body on behalf of a person in private law, which is advantageous for the company but is made in return for a bribe, constitutes an abuse of authority. In the ruling of the Criminal Chamber of the Supreme Court in case no. 3-1-1-84-14, the relationship between an employee and the employer, in relation to the employee having taken a bribe, was interpreted by reference to the provisions on authorisation agreements, which means that an employee essentially has to comply with the duties of loyalty and due diligence specified in section 620 (1) of the Law of Obligations Act (LOA). In our case used as the example, the duty of due diligence was complied with, i.e. the transaction was concluded on the best terms for the principal (according to a formalistic approach, i.e. the transaction was concluded with the best bidder).

Section 402[3] of the PC does not define 'abuse of authority', but the term 'abuse' is also used in sections 217[2], 349 and 446 of the PC. 'Abuse of authority' is a concept which belongs to a dignified list of other concepts burdened with fundamental significance in terms of criminal law protection of economic turnover but which are known to cause a fair share of problems for those enforcing the law. The most conspicuous example of these concepts is the act termed as 'illegal use of a right' among the necessary elements of an abuse of trust in section 217[2] of the PC, for the cryptic wording of which a quite clear interpretation has been given both in the legal literature and case law – it is a transaction.[14] An equally simple and succinct interpretation of 'abuse of authority' is not yet available. The scarce legal literature has attempted to provide a mere literal interpretation of the concept based on its content, with 'power' meaning jurisdiction, authority or competence, and 'abuse' meaning deliberate improper or excessive use of something.[15]

Leaving aside the specific content, it is clear that an abuse of authority must be composed of two elements, namely: (i) authority, i.e. the right to do something within certain limits; and (ii) an act that exceeds the authority, i.e. the predeter-

14 See the judgment of the Criminal Chamber of the Supreme Court in case no. 3-1-1-100-09 (however, the author cannot agree with the conclusion of the judgment, according to which the necessary elements of the offence are present even though the transaction in question is not legally binding); for breach of the duty of loyalty, see the judgment of the Criminal Chamber of the Supreme Court in case no. 3-1-1-43-13, p. 27.

15 S. Kruusma. Erasektori korruptsiooni regulatsioon Eestis. Juridica 2015, 7, page 494.

mined limits. Limits, therefore, imply certain obligations. In addition to German law, the foregoing interpretation appears to also be supported by Article 1 of Council Framework Decision 2003/568/JHA, which was one of the sources for section 402[3] of the PC. As regards the term 'breach of duty', Article 1 stresses that it is to be understood in accordance with national law, but still states that the concept of breach of duty in national law should cover as a minimum any disloyal behaviour constituting a breach of a statutory duty, or, as the case may be, a breach of professional regulations or instructions, which apply within the business of a person who in any capacity directs or works for a private sector entity.[16] It must be possible to abuse authority; hence, the authority must have certain limits. Limits can be related to certain obligations, which must be complied with when exercising the authority. Thus, the obligations which a person exercising his or her authority must comply with must be determined.[17] When transferred strictly into the context of private-sector corruption, the question largely boils down to whether the entry into any transaction should be treated as a breach of the duty of loyalty and therefore an abuse of authority if the transaction is made in return for a bribe, or should the transaction be evaluated in substantive terms.[18]

In its ruling in the Rimi case, the Supreme Court linked the authority of an official in a private legal person to the need to protect the relationship of trust and loyalty between the private legal person and the official (i.e. the person meeting the specific criteria of the subject under section 402[3] of the PC).[19] Of course,

16 Council Framework Decision 2003/568/JHA. Attaching significant weight to the framework decision in further analysis is questionable, given the different terms used in different language versions, e.g. 'kohustuse rikkumine' (breach of obligation, non-performance) in Estonian, 'breach of duty' in the English version and 'pflichtverletzung' in the German version. Also, there is no analysis of the implementation of Article 1 in the Member States; see report of 2007 on the implementation of the framework decision, COM (2007) 328, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52007DC0328&from=EN.

17 This reasoning is quite similar to the aforementioned interpretation provided in the case law for 'illegal use of a right' as one of the necessary elements of an abuse of trust specified in section 217[2] of the PC, according to which the illegal use of a right means the entry into a transaction that violates an internal relationship. See the judgments of the Criminal Chamber of the Supreme Court in the following cases: 3-1-1-4-08 (p. 25-26); 3-1-1-55-09; 3-1-1-61-09; 3-1-1-100-09. However, it must be considered that in the case of this offence it is appropriate to point to the internal relationship between the representative and the principal, as the offence consists in a transaction concluded in the context of a relationship of representation. The offence specified in section 4023 of the PC, however, can also be committed by means of an act which does not involve a transaction made on behalf of a private legal person.

18 For an overview of the object of the discussion, see S. Kruusma. Erasektori korruptsiooni regulatsioon Eestis. Juridica 2015, 7, page 494.

19 Ruling of the Criminal Chamber of the Supreme Court in case no. 3-1-1-84-14, p. 40. The term 'relationship of trust' has been used when interpreting corruption in the public sector. See L. Feldmanis. Soodustus ametialase teo eest kui pistise ja altkäemaksu koosseisuline osa. Juridica 2012, 1, 42. Juridica 2012, 1, 42.

account must be taken of the fact that it is a position which was expressed in the context of defining the legal values protected by the former bribery provisions, which have been amended by now. This is clear from the use of the terms 'relationship of trust' and 'relationship of loyalty'. However, it is important to note that the court interpreted the duty to maintain integrity applicable to an official governed by private law by direct reference to the general duty of loyalty (section 620 (1) of the LOA, section 15 (1) of the Employment Contracts Act (ECA), or section 35 of the General Part of the Civil Code Act (GPCCA)).[20] Bear in mind that in the context of offences against property the same Chamber has previously interpreted the duty of loyalty of a management board member as the duty of the management board member to preclude any personal interest in the consequences of his or her decisions and avoid conflicts of interests with the legal person when managing the legal person.[21] At least at first glance, it seems that this issue has been resolved and Indrek, the employee responsible for procurement in the case used as the example, meets the objective criteria under section 402[3] of the PC.[22]

4. Bribery in a relationship governed by private law, and offences against property

The case used as an example in his article describes a situation where the financial interests of a legal person are not damaged despite the facilitation payment. This fact is not relevant in terms of exclusion of responsibility, though. As described above, it seems that at least Estonian case law is going down the road where bribery as such is essentially a breach of a duty (i.e., abuse of authority, whatever that might mean), and whether or not financial interests have thereby been damaged is, therefore, irrelevant under section 402[3] of the PC.

This, in turn, raises an intriguing question if one considers the reasoning provided above: if we were to agree that section 402[3] of the PC protects individual legal values and that there is also a breach in a situation where the legal person does not appear to have sustained any damage, can the breach amount to an

---

20 For criticism, see T. Ploom. M. Kärner. Kannatanu huvide realiseerimine kriminaalmenetluses. Juridica 2015, 7, page 513.

21 Judgment of the Criminal Chamber of the Supreme Court in case no. 3-1-1-43-13, p. 27.

22 Before going any further, it is also interesting to point out that the foregoing position coincides with what has been written in the literature about section 299 of the German StGB. In the past, this provision has very clearly been interpreted as intended to protect competition. Case law, however, has supplemented the offence of distortion of competition with the breach of a specific duty of due diligence or loyalty to a company. Thus, the elements of the offence resemble the structure and logic of the offence specified in section 2172 (1) of the PC (abuse of trust). H. W. Laufhütte. R. Rissing-van Saan. K. Tiedemann. Leipziger Kommentar. StGB. 12. Aufl. Bd 10. Sections 284–305a. Berlin, 2008, section 299, page 45.

offence against property in respect of that legal person?

Let us first recall that a legal person governed by private law (as well as a legal person governed by public law)[23] is protected against a malicious employee or member of a management body by sections 201 (embezzlement) and 217[2] (abuse of trust) of the PC. These provisions have a clear relationship of subordination between them. Section 2172 of the PC comes into play only in the cases where the act committed by a person does not meet the criteria specified in section 201 of the PC. The wording of section 217[2] of the PC clearly points to this negative element. Despite this, the authors of this article do not dare to express a conclusive view about the relationship between the necessary elements of offences specified in these two provisions. The scarce case law of the Supreme Court in this regard seems to point to a distinction which is based on the intention of or agreement on embezzlement:[24] if the property is used for the benefit of the offender or a third party, it is an embezzlement, and if not, it is an abuse of trust (provided, of course, that the criterion of significant material damage set out in section 217[2] of the PC is met).[25] To avoid the dispute mentioned above, it is necessary to analyse possible responsibility for both of the offences.

For further analysis, the term 'illegal' in sections 201 and 217[2] of the PC needs to be interpreted. There is solid case law available on this element of the two offences by now.[26] Furthermore, in relation to the offence specified in section 217[2] of the PC (abuse of trust), the Supreme Court has emphasised that both a breach of the duty of due diligence and a breach of the duty of loyalty is to be considered an 'illegal' act for the purposes of the necessary elements of the offence. The Chamber has stated that the duty of loyalty of a management board member set forth in section 35 of the GPCCA requires, among other things, that the management board member has to preclude any personal interest in the consequences of his or her decisions and avoid conflicts of interests with the legal person when managing the legal person.[27] Thus, the Supreme Court has affirmed responsibility under both criminal law and company law in a situation

23 Judgment of the Criminal Chamber of the Supreme Court in case no. 3-1-1-92-13.

24 The terms 'intention of embezzlement' and 'agreement on embezzlement' were made up by the authors, i.e. the case law has not used them. Nevertheless, they convey the content of the elements of two offences: taking something permanently for oneself or for another person (with agreement with that other person) (section 201 of the PC), and intentional transaction made in contravention of a duty, which happens to result in major damage (section 217[2] of the PC).

25 Judgment of the Criminal Chamber of the Supreme Court in case no. 3-1-1-100-09.

26 See the judgments of the Criminal Chamber of the Supreme Court in cases no. 3-1-1-23-14; 3-1-1-52-14; 3-1-1-66-14; 3-1-1-55-09, etc.

27 Judgment of the Criminal Chamber of the Supreme Court in case no. 3-1-1-43-13, p. 27.

where a management board member encumbers the property of the company with a mortgage and usufruct for the benefit of persons related to the member.[28] Hence, the question arises as to whether the conclusion in the ruling of the Criminal Chamber of the Supreme Court in case no. 3-1-1-84-14 that the fact of bribery alone essentially constitutes a violation of the relationship of loyalty and trust means that this violation constitutes a breach of the duty of loyalty and therefore an illegal use of a right within the meaning of section 217[2] of the PC.[29] This question is in addition to the question, raised in section 2 of this article, of whether an abuse of authority and an illegal use of a right as the necessary elements of the offences specified in sections 402[3] and 217[2] of the PC, respectively, can be equated.[30]

It should be noted, however, that the position expressed by the Criminal Chamber of the Supreme Court in its judgments in case no. 3-1-1-61-09 and particularly in case no. 3-1-1-43-13 allows for two alternative interpretations of 'illegality' and 'duty of loyalty' where section 217[2] of the PC is concerned.

Namely, the element 'illegal use of a right' in section 217[2] of the PC criminalises an illegal use of the right to dispose of property in a manner that causes significant material damage to the victim. Thus, it is a transaction[31] (illegal use of the right to dispose of property) that meets the criteria of the offence.[32] In terms of the relationship between sections 2172 and 4023 of the PC, everything is clear in a situation where an illegitimate agreement made by a person results in a transaction which is essentially harmful to the company, i.e. the person has breached the duty of due diligence.[33] In such a case, sections 217[2] and 402[3] of the PC can apply in combination depending on whether there is a concurrence of offences or whether transactions are to be regarded

28 Judgments of the Criminal Chamber of the Supreme Court in cases no. 3-1-1-61-09 and 3-2-1-34-14.

29 See also footnote 18.

30 See a similar discussion in respect of section 299 of the German Penal Code (equivalent to section 4023 of our PC) and section 266 (equivalent to section 2172 of our PC) – H. W. Laufhütte. R. Rissing-van Saan. K. Tiedemann. Leipziger Kommentar. StGB. 12. Aufl. Bd 10. Sections 284–305a. Berlin, 2008, section 299, page 45.

31 Judgment of the Criminal Chamber of the Supreme Court in case no. 3-1-1-4-08.

32 This position is somewhat doubtful in the light of the judgment of the Criminal Chamber of the Supreme Court in case no. 3-1-1-100-09, according to which the necessary elements of the offence are present even though the transaction in question is not legally binding (see footnote 14 above).

33 For examples of breaches of obvious duties of due diligence, see the judgments of the Criminal Chamber of the Supreme Court in cases no. 3-1-1-55-09 and 3-1-1-61-09 (management board member) and 3-1-1-84-10 (accountant).

as offences which are related to each other but which are legally different.[34]

In the case of the procurement manager described at the beginning of this article, it is difficult to see a direct breach of the duty of due diligence at first glance. Basically, one could speculate, as discussed in section 3 of this article, that the bid could have been even lower, had there not been the 5-percent payment, but let us stick to the actual circumstances. It follows from the foregoing that there can be two alternative solutions, considering the "everybody-is-smiling problem" and in particular the position expressed in the judgment of the Criminal Chamber of the Supreme Court in case no. 3-1-1-43-13:

- Restrictive interpretation. The right of disposal has been illegally used if the counterparty to the transaction is directly related to the employee concluding the transaction, i.e. there is a connection and it is expressed in personal interest.
- Wide interpretation. The right of disposal has been illegally used if, together with the transaction, an illegitimate agreement has been concluded, which is to be considered a breach of the duty of loyalty in itself.

No exhaustive conclusions can be drawn from the rulings concerning Rimi cited above. After all, the approach to the relationship of trust and loyalty set out there is based on interpreting section 293, not section 402^3 of the PC. However, such a discussion is also presumably of a fairly insignificant practical value. One should not forget that the offence specified in section 217^2 of the PC is about consequences and presupposes 'significant material damage' as one of the necessary elements. Thus, even if the entry into an illegitimate agreement is immediately found to be an illegal act within the meaning of section 217^2 of the PC, then this act must have caused damage to a private legal person, and in an "everybody-is-smiling situation" the affirmation of the damage would imply the risk that section 217^2 of the PC no longer deals with an offence that damages a legal right and it loses its contours the same way its predecessor, section 289 of the PC, did.

Section 201 of the PC, on the other hand, does not presuppose damage as a necessary element of an offence; there have been quite a few situations in practice where the elements of the offence were seemingly easy to establish in borderline cases, i.e. in cases where the question of whether the making of payments

34 For more recent case law on concurrence of offences, see the judgment of the Criminal Chamber of the Supreme Court in case no. 3-1-1-6-16, p. 31. According to German case law, there is concurrence of offences if in addition to the simultaneity of transactions also the evolution of the intent underlying the transactions is largely overlapping. – See W. Joecks. K. Miebach. Münchener Kommentar zum StGB. Bd 5. Sections 263–358 StGB. 2. Aufl 2014, section 299, änr 41. H. W. Laufhütte. R. Rissing-van Saan. K. Tiedemann. Leipziger Kommentar. StGB. 12. Aufl. Bd 10. Sections 284–305a. Berlin, 2008, section 299, page 61.

was permissible or not was not so clear (at least this is the impression when reading the facts in the judgments of the Supreme Court).[35]

In the case of section 201 of the PC, case law does not create an explicit link between a breach of the duty of loyalty and illegality: in the judgment made in case no. 3-1-1-23-14 (p. 22), the Criminal Chamber of the Supreme Court emphasised that 'illegality' as a necessary element of the offence specified in section 201 of the PC is present if the company as the victim does not agree to the transaction. Unfortunately, the Supreme Court confined itself to that statement. In an earlier discussion of this offence, one of the authors of this article has already regretted that this statement left unanswered the question of whether a transaction can be considered illegal due to the mere fact of a breach of the duty of loyalty arising from section 35 of the GPCCA. This issue is important from the point of view of interpreting section 201 (1) of the PC: after all, any transaction between a management board member with himself or herself or with a person related to the member is always about the duty of loyalty, which calls the weight to be attached to an interpretation of 'illegality' as a necessary element of an offence into question.[36] Admittedly, one can also take the view that requiring a clear statement to that effect would be slightly unnatural. At least in the case of embezzlement as defined in section 201 of the PC it is difficult to imagine a situation where a management board member or an employee who possesses a movable asset of a private legal person or with whom such asset has been entrusted does not breach the duty of loyalty in conjunction with the embezzlement.

The concurrence or multiplicity of offences under sections 201 and 402[3] of the PC is possible in a relatively limited number of cases, considering the natural course of events. In the "everybody-is-smiling" situation described in this article, the intention of embezzlement is not manifested, because Rain's counter-performance is supposed to be in line with market conditions.[37] Thus, in principle, a concurrence of offences can be assumed, in particular, in a situation where an employee or a management board member arranges for the disposal of the property of a private legal person in such a way that a part of the property is transferred to the employee or the member and later a part of it will be used for the benefit of a third party. As noted, this situation has nothing to do with the

35 See the judgment of the Criminal Chamber of the Supreme Court in case no. 3-1-1-92-13 cited above.

36 Judgment of the Criminal Chamber of the Supreme Court in case no. 3-1-1-23-14. See the note in J. Sootak. M. Kairjak. Varavastaste süütegude uuemaid lahendusi Riigikohtus. Kriminaalkolleegiumi otsus asjas 3-1-1-23-14, – Juridica 2014, 4, page 344.

37 For the criteria, see the judgment of the Criminal Chamber of the Supreme Court in case no. 3-1-1-100-09.

case described in the introduction. How, in this case, should one go about a possible concurrence of offences under sections 201 and 402^3 of the PC? Essentially, one could argue that in such a situation a facilitation payment could also be regarded as 'use for one's benefit' and the concurrence of offences can actually be established. This apparently complex situation will probably have to be solved in future case law.

5. Conclusion

It is difficult to overestimate the significance of the rulings made in the Rimi case for interpretation of the main issues relating to corruption in the private sector – the more so as the case law now provides a very clear definition of what is considered to be an offence related to private-sector corruption. The authors are convinced that, in this respect, the case law has rightly concluded that the brand new section 402^3 of the PC must be viewed as primarily protecting the interests of a private legal person against a disloyal employee or board member, rather than focusing on some ambiguous values such as free competition, or the like. However, this company-centred approach has a clear deficiency: the question of delimitation of possible concurrence and multiplicity of an offence under section 402^3 of the PC and other offences essentially directed against the same legal value, i.e. the property of a company, should be made very clear in judicial practice. At least this much can already be concluded from the available interpretations that in an "everybody-is-smiling" situation the responsibility to be considered is that for private-sector corruption, rather than for an offence against property.

Some problems encountered in computer system searches

Eneli Laurits,
Adviser to the Penal Law and Procedure Division of the Ministry of Justice

Digital evidence, its collection and the issues of reliability directly connected therewith have been the hottest topic in the landscape of criminal procedure law in recent years. In addition to the overall understanding of the field of digital evidence, the ways of fitting this relatively recent outcome of technological development into criminal procedure with the help of strict rules raise questions. Are prosecutors, lawyers and judges with traditional education in law even capable of grasping the fine nuances related to digital evidence and asking accurate and relevant questions?

The terms of reference of the revision of Estonian criminal procedure law pay attention, inter alia, to digital evidence, stating as follows: "Digital evidence is increasingly collected in criminal proceedings, but since the current law does not provide for specific rules of procedure or the principles of collecting such evidence, the provisions on collection and investigation of conventional evidence remain the basis. However, physical and digital evidence are inherently fundamentally different, which is why the current state of affairs leads to confusions in practice."[1] Professor Orin S. Kerr emphasised the importance of special provisions on the collection of digital evidence as early as in 2005. Orin S. Kerr points out that digital evidence is collected differently from personal or other physical evidence and that these new methods of collecting evidence are so special that the existing rules are often not applicable anymore.[2]

When talking about digital evidence, its specific features compared to physical evidence are highlighted in particular. Digital evidence is latent in the same sense as, for example, DNA evidence; digital evidence is easily movable across different jurisdictions, and this often happens regardless of the will of the suspect or the body conducting proceedings; digital evidence can be easily altered, damaged or destroyed, and all of this can happen even in the course of the

1 Terms of reference of the revision of Estonian criminal procedure law, 2015, page 9. – Online: http://www.just.ee/sites/www.just.ee/files/kriminaalmenetluse_revisjoni_lahteulesanne.pdf.

2 Orin S. Kerr. Digital evidence and the new criminal procedure. – Columbia Law Review 279 (2005), page 280.

so-called conventional evidence-gathering process.[3] There is a significant difference between analogue and digital evidence. While evidence recorded by an analogue device can be manipulated, it requires great skill. For example, the negative of a photographic film can be altered, but such alterations can be easily detected, while digital images are easy to alter.[4] Just like in our legal landscape, continuous efforts have also been made elsewhere in order to adjust the provisions on physical evidence collection to digital evidence.[5]

This article highlights the various problems that are encountered in the course of one of the most common investigative measures – search – which are related to the specific features of the digital world and the issues arising in the collection of digital evidence, in particular the issue of jurisdiction. In the cases where digital evidence is located in different jurisdictions, the collection of evidence in reliance on traditional mutual cooperation agreements has proved to be ineffective for a long time, which is why efforts have been made to find ways of collecting evidence pursuant to a simplified procedure in investigating cybercrime. Thereby a balance needs to be found between the collection of evidence and the sovereignty of states.[6]

Search

Provisions on searching[7] have been established, are applicable and presume a so-called single-step procedure, i.e., looking for physical evidence. A search is generally limited in both time and physical space. Also the Code of Criminal Procedure (CCP) clearly relates a search to a particular physical location and physical items: the objective of a search is to find an object to be confiscated or used as physical evidence, a document, thing or person necessary for the adjudication of a criminal matter, property to be seized for the purposes of compensation for damage caused by a criminal offence or of confiscation, or a body,

3 Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, page 10.

4 Stephen Mason. International Electronic Evidence. – British Institute of International and Comparative Law (2008), page xxxv.

5 The admissibility of electronic evidence in court (2005), page 34. – Online: https://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/libro_aeec_en.pdf.

6 See, e.g., the positions of the Ministry of Justice at the informal meeting of EU justice and home affairs ministers held on 25 and 26 January 2016. – Online: http://www.riigikogu.ee/download/73fe0c45-17f9-439c-8dc7-37d9a6ea6acf.

7 For example, the US Supreme Court has held in the case of Katz v. United States that the Constitution protects people's right to privacy rather than ownership. Thus, a search typically occurs when a public authority intrudes into an area where a person has a subjective expectation that his or her privacy will be respected, and this expectation is objectively reasonable. – Online: https://supreme.justia.com/cases/federal/us/389/347/case.html.

or to apprehend a fugitive in a building, room, vehicle or enclosed area.[8] Thus, the situation with looking for digital evidence has been solved quite simply: a data medium (usually initially with the casing, i.e., the computer) is seized in the course of a search, and actual searching of digital evidence will take place at an investigative or forensic institution.[9] Neither the current wording of the CCP nor the amendments entering into force on 1 September 2016 mention a computer system as a place that can be searched.

Professor Orin S. Kerr points out that the procedure of searching for digital evidence is a two-step process,[10] finding that these steps differ significantly from each other: the two searches occur at different times, in different places, and are usually performed by different people.[11] Seizure of data media in the course of a physical search is fairly standard, since it is common knowledge that they may contain a variety of evidence on the commission of criminal offences.[12]

The Code of Criminal Procedure treats the search of a data medium as an 'inspection' and the legislature has so far not found it necessary to afford greater protection of fundamental rights in respect of personal information held electronically.[13] However, an electronic data medium usually contains so much

---

8 Section 91 of the CCP.

9 For more details, see also Susan W. Brenner & Barbara A. Frederiksen. Computer Searches and Seizures: Some Unresolved Issues, 8 MICH. TELECOMM. & TECH. L. REV. 39, 82 (2002).

10 In his article "Search Warrants in An Era of Digital Evidence" (page 88), Orin S. Kerr finds that a search warrant for search for digital evidence should clearly indicate the two-step nature of the process. First, the body conducting proceedings should specify the devices and data media from which digital evidence is hoped to be found. Then the particular digital evidence looked for should be indicated. To safeguard fundamental rights, the law should provide for the investigative body's obligation to make a copy of the data medium and promptly return the data medium to the person concerned. Where a data medium is used only as a data storage device, it should be returned more quickly. If there is reason to believe that the data medium is the instrument of committing a criminal offence or used for storage of data prohibited by law, the investigative body should be obliged to ascertain this within a specified period of time.

11 Orin S. Kerr. Search Warrants in an Era of Digital Evidence. Mississippi Law Journal, Vol. 75, 2005, page 87.

12 For example, in his article "Fighting Against Cybercrime in Europe: The Admissibility of Remote Searches in Spain" (European Journal of Crime, Criminal Law and Criminal Justice 19 (2011), page 368), Ortiz Pradillo writes that the forensic examination of hard drives and peripheral elements of computer equipment seized after a search has become a habitual and the most effective practice for obtaining evidence on all types of criminal offences, whether or not they can be classified as a computer crime.

13 Actually, there is a need for a debate on the protection of fundamental rights in connection with digital information. For example, in his dissenting opinion on the judgment rendered in case no. 3-1-1-93-15, Justice Kergandberg pointed out that, as regards the protection of the confidentiality of communications, it is doubtful whether an electronic message really deserves protection only during the couple of fractions of a second when the message, broken down into pieces, moves from one server to another. The duration of a communication process

personal information (and not only on the possible suspect, but also on family members, etc.) that a search of such information should be regarded as a major infringement of the person's privacy.[14] During an inspection, the body conducting proceedings can look through the data medium, which could be relevant to the proceedings, essentially during an unlimited period of time and for unlimited number of times. Moreover, the body conducting proceedings even does not have to know what in particular is to be found. The body can just look for something that will be useful, provided it has enough time. In physical space, i.e., in the course of an actual situation of a search, however, this activity of a body conducting proceedings is excluded. The amendments to the CCP's provisions on searches, which will take effect on 1 September 2016, are intended to provide more effective protection of fundamental rights in connection with searches, and this investigative measure (of the physical world!) will be subjected, in most cases, to judicial review. The amendments will also specify the obligation of bodies conducting proceedings to set out more clearly what will be looked for, as well as rules on the admissibility of evidence subject to the plain view exception.[15]

According to the current law, a search warrant must indicate the objective of and reasons for the search.[16] The amendments taking effect in September specify that in addition to the reasons for a search a search warrant should also indicate what will be looked for and where. The current wording of the law is too vague, making it possible to merely indicate in a search warrant that the objective of the search is to find evidence relevant to the criminal case.[17]

---

is negligible in the case of electronic messages, and the possibility of an infringement is thus limited. In addition, it is highly questionable when a message is received in the recipient's computer, because the fact that it is displayed on a computer screen does not mean that the message is actually on the computer (the information displayed on the computer screen is usually located on some server).
Given that people are accustomed to the use of digital technologies in their daily lives, the data media of home computers contain photos, videos, documents, records, etc. stored for many years, i.e. the digital footprint is so deep that searching this information for an unlimited period of time should deserve more consideration than a mere decision of a body conducting proceedings to execute an inspection.

14 Ortiz Pradillo. Fighting Against Cybercrime in Europe: The Admissibility of Remote Searches in Spain. – European Journal of Crime, Criminal Law and Criminal Justice 19 (2011), page 383.

15 Explanatory Memorandum to the draft Code of Criminal Procedure Amendment and Other Related Acts Amendment Act (2014), page 2. – Online: http://www.riigikogu.ee/tegevus/eelnoud/eelnou/d5492f26-424d-42ad-83e4-cce202a5524d/.

16 Section 91 (4) of the CCP.

17 Ibid., page 9.

Thus, while in the case of the "physical world" a body conducting proceedings has to clearly indicate the object for searching which the warrant is issued, the same principle does not apply to a search for digital evidence. In essence, it is sufficient for the body conducting proceedings to determine that there is a need to look for digital evidence and that a data medium (data media) will be taken away from the place of the search. The subsequent course of the inspection is not limited in any way, and only data relevant to the subject of proof will be recorded. The course of the inspection will be set out in the inspection report, but the body conducting proceedings can decide on its level of detail. While a physical place is searched in the presence of a representative of the local authority, the body conducting proceedings has no obligation to engage anyone in the inspection.

With the amendments to the CCP coming into force on 1 September 2016 (section 91 (10) of the CCP), the legislature will also regulate evidence collected during a search of a physical place that comes under the so-called plain view exception. Digital evidence subject to the plain view exception, however, is not regulated. Although investigators can accidentally see and discover evidence of another criminal offence in the course of a physical search (for example, child pornography displayed on the computer screen), such evidence is usually found during a later examination of the data medium. The CCP's provisions on inspections do not restrict the activities of bodies conducting proceedings in the performance of an inspection that could result in a finding of incriminating materials which were not expected to be found in the first place.

For example, in the case of United States v. Wong,[18] the body conducting proceedings discovered child pornography files when searching a data medium in order to find digital evidence related to a murder. Since the body conducting proceedings actually had the right to look for graphics files on the data medium, and the data medium had been seized correctly, following all the procedures prescribed by law, the child pornography files were recorded as a "plain view exception". However, if the body conducting proceedings had been entitled to search only document files, the examination of videos or image files would not have been justified and such evidence could not have come under the plain view exception. In the case of a digital search, a situation where the name of a file clearly points to the illicit content of the file has also been accepted as a plain view exception.[19] Relying on the German case-law, Eerik Kergandberg has also highlighted that regulation of digital searches should at least be considered.[20]

---

18 United States v. Wong, 334 F.3d 831, 838 (9th Cir. 2003). – Online: https://casetext.com/case/us-v-wong-18.

19 Online: http://www.leagle.com/decision/2003912196Misc2d716_1803/PEOPLE%20v.%20EMERSON.

20 E. Kergandberg, M. Sillaots. Kriminaalmenetluse seadustik. Kommenteeritud väljaanne (2012), page 269.

Computer system searches

Searching a computer system is – or rather could be – a rather customary investigative measure. It is an indisputable fact that people use electronic devices countless times during the day. For a body conducting proceedings in a criminal case, this means, in particular, that significant traces are stored: photos taken, location data, letters sent, documents drawn up, websites viewed, articles commented on, travel tickets bought, hotels booked, etc. A very large amount of data, however, is not stored in a data medium (hard drive of a computer), but will remain in the random access memory (RAM) or other places where the computer keeps temporary files or links to the activities of the particular user. In addition, an enormous part of personal information processing takes place using cloud computing (Google Docs, Dropbox, e-mail accounts, etc.).

A few years ago the "pull the plug" method was the prevailing practice of working with computers running at the place searched, i.e., the computer was simply unplugged and taken away, along with the data medium, to be examined by a forensic unit. Now it has been understood that by so doing, very valuable information on the use and users of the computer, as well as indications of other possible evidence is voluntarily abandoned. Investigators are constantly faced with the situation where data are encrypted or located outside of a computer's data medium. In such a case, working with volatile data is what can provide valuable information.[21]

The Estonian Code of Criminal Procedure does not contain specific provisions on computer system searches.[22] However, the need to search a computer system will most likely arise in almost all criminal proceedings. For example, there can be a computer at a home being searched, in which different e-mail boxes are open (let us assume that the mailboxes contain information stored on Estonian servers, servers located abroad and servers of a company providing a common cloud service). Similar situations also arise in the course of skilful detention of a suspect: the body conducting proceedings plans the detention for a moment when he or she is sitting on a park bench with a running computer, with e-mail

21 Association of Chief Police Officers' (ACPO) Good Practice Guide for Computer-Based Electronic Evidence, page 3. – Online: https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence[1].pdf.

22 Recommendation No. R (95) 13 of the Committee of Ministers of the Council of Europe on problems related to criminal procedure and information technology contains a recommendation to member states to include clear provisions on, inter alia, searches of computer systems in their criminal procedure law (Article 1). Council of Europe Committee of Ministers. Recommendation No. R (95) 13 of the Committee of Ministers to member states concerning problems of criminal procedural law connected with information technology. Adopted on 11 September 1995. – Online: http://www.coe.int/t/dghl/standardsetting/media/Doc/CM/Rec(1995)013_en.asp.

accounts opened. In such cases, the law does not provide for the obligation "to conduct kind of a search", as the data would be examined in the course of an inspection,[23] which would be solely for the investigator to decide. Who should authorise such a significant infringement of a person's privacy, and how, is not clear.

There are several problems to be solved, both in relation to situations where a person has provided the body conducting proceedings with user names and passwords necessary to enter accounts, as well as situations where the body conducting proceedings fails to obtain the consent of the person, but still finds a way to examine the accounts. Other questions to be answered are: how should the proportionality of inspections and searches be ensured, and whether and how criminal proceedings conducted in Estonia are affected by the fact that the data that we see displayed on a computer screen in Estonia are actually not located here. It is possible to discuss just a fraction of the issues related to cloud computing in this article.

Cloud computing and criminal proceedings

People are actively using cloud services both for the sake of convenience and the large data space offered by these services. Bodies conducting proceedings, however, are faced with the problem that information on any crime is now often stored in electronic form on various computer systems.[24] For a body conducting proceedings, this means that the data sought are not located on the data medium of the computer seized, and if the computer is unplugged in the place of the search there often will be no information on the services that the person may use for data storage. Materials are stored, shared and often also compiled on the Internet, and indications of such activities might not be found during a later inspection/expert examination carried out at a forensic unit, i.e. they must be searched for in the computer that is still running. The use of the opportunities offered by cloud computing (as well as data encryption) is not characteristic only of a criminal mindset – the vast majority of computer users act this way.

Examining a running computer on a scene of events deserves attention for two reasons. First, it enables the body conducting proceedings to ascertain, in

23 In terms of procedural tactics, it would be useful in such cases to take care that access to data will be preserved until the computer is taken to the investigative body where investigative measures can be continued.

24 Criminal justice access to data in the cloud: challenges. Discussion paper. Prepared by the T-CY Cloud Evidence Group (2015), page 5. – Online: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2015/T-CY(2015)10_CEG%20challenges%20rep_sum_v8.pdf.

the course of the initial examination, whether, for example, the user has any encrypted data / media; whether a virtual machine is used, etc. before the computer is turned off and the encryption is closed (and probably cannot be opened later) or before it even will not occur to anyone to look for indications of the use of a virtual machine. Also, it makes it possible to establish the data that will be destroyed when the computer is turned off: chats in instant messaging programs, open forum pages with posts, or downloads.

On the other hand, looking around on a running computer is a very important source of information for the body conducting proceedings, for example data used in a cloud, mailboxes, social networking sites, etc. While the data mentioned in the previous paragraph are searched for in the data medium and the procedural risks relate to the alteration (and sometimes also destruction) of the information in the data medium, the second type of information is generally located outside the territory of Estonia (on foreign servers), and the computer is just a door that allows the body conducting proceedings to enter a completely different space, which is huge.

Cross-border searches of computer systems are especially important in the context of cybercrime,[25] as well as in the prosecution of a variety of other criminal offences. In theory, there are a number of opportunities to obtain evidence from the territory (server) of another state, e.g. through cooperation with the law enforcement agencies of that state. Unfortunately, however, official cooperation is often quite futile. It has been complained that acting on a request of another state may be hindered by a lack of technical skills or resources, the entire official legal assistance process is sometimes too slow,[26] and at times the state from which assistance is requested is not the most helpful. For these and other reasons, the state requesting assistance may take the collection of evidence into its own hands: sitting at the running computer and having access to various

25 The Internet and the Legitimacy of Remote Cross-Border Searches. – University of Chicago Public Law & Legal Theory Working Paper No. 16, 2001, page 3. – Online: http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1316&context=public_law_and_legal_theory.

26 Mutual legal assistance remains the principal means to obtain evidence from foreign jurisdictions for use in criminal proceedings. In December 2014, the functioning of the system of mutual legal assistance was assessed. It was concluded that the mutual legal assistance process is considered inefficient in general, and with respect to obtaining electronic evidence in particular. Response times to requests of 6 to 24 months appear to be a norm. Many requests are abandoned. (Criminal justice access to data in the cloud: challenges. Discussion paper. Prepared by the T-CY Cloud Evidence Group (2015), page 14. – Online: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2015/T-CY(2015)10_CEG%20challenges%20rep_sum_v8.pdf).

data storage sites on the Internet, investigators trace, copy and freeze data located on other computer systems, outside the territory of their own state.[27]

The question of unilateral cross-border access by one state to data stored on computer systems in the territory of another state without using traditional mutual legal assistance requests is a very complex one as it touches upon agreed upon principles of international law (particularly the territoriality principle and thus the question of national sovereignty) and procedural law safeguards protecting the rights of individuals. The need for cross-border access to electronic evidence has been discussed since the 1980s.[28]

Cloud computing raises a number of challenges for criminal justice, in particular with regard to the applicable law and the jurisdiction to enforce. Independence of location is a key characteristic of cloud computing. Therefore, it is often not obvious for law enforcement authorities in which jurisdiction the data is located or stored and/or which legal regime applies to the access to the data. Also, it is quite common that a service provider has its headquarters or the parent company in one jurisdiction, while the legal regime of a second jurisdiction or – in the cases where data are moved – several jurisdictions may apply to the data.[29] In addition, data may be scattered over several servers and thus be located in different states, or may be mirrored for reasons of security or availability and may thus be located in different servers at the same time.[30]

Cloud computing offers the user a convenient way to access data from different locations, and (also simultaneous) access to the data can be given to an undefined circle of persons.[31] "Cloud computing" means that data is not held in a specific data medium or in a closed network but is distributed over different services, providers, locations and often jurisdictions. In traditional computer

---

27 The Internet and the Legitimacy of Remote Cross-Border Searches. – University of Chicago Public Law & Legal Theory Working Paper No. 16, 2001, page 3. – Online: http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1316&context=public_law_and_legal_theory.

28 Transborder access to data and jurisdiction: Options for further action by the T-CY (2014), pages 6–7. – Online: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8.

29 Criminal justice access to data in the cloud: challenges. Discussion paper. Prepared by the T-CY Cloud Evidence Group (2015), pages 10–11. – Online: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2015/T-CY(2015)10_CEG%20challenges%20rep_sum_v8.pdf.

30 Transborder access to data and jurisdiction: Options for further action by the T-CY (2014), page 9. – Online: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8.

31 For more detailed information on cloud computing, see http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

forensics, due to the centralised nature of the information technology system, investigators can have full control over the forensic artefacts (router, process logs, hard disks, etc.). However, in cloud computing, due to the distributed nature of the information technology systems, control depends on the service model and investigators' access is therefore very limited.[32]

Even if theoretically data may always have a location, even when stored on cloud servers, it is far from clear which rules apply to access by law enforcement authorities. It may be argued that the location of the headquarters of the service provider or of its subsidiary determines the jurisdiction. On the other hand, the applicable law could be determined on the basis of the location of the data and server, or the place where the suspect has subscribed to the cloud service, or the location or citizenship of the suspect. Additional problems arise when the data owner is unknown.[33]

These changes in technology have resulted in the "loss of location" in the legal world: the location of data cannot be linked to a particular territory, because the data are "somewhere in the cloud".

Cybercrime is extensive, the number of victims affected by this type of crime is very high and the collection of evidence is most complicated. All this has created a situation where the vast majority of victims cannot expect that justice will be served. This raises serious questions regarding the performance of the state's obligations, incl. ensuring the rule of law in cyberspace, combating crime in society and protecting the rights of victims.[34] The state has a positive duty to protect the rights of its citizens, including through effective application of criminal law and law enforcement measures.[35] Collection of evidence is important in this regard. One of the main goals of criminal proceedings is to establish the objective truth through the collection of comprehensive evidentiary information.[36]

---

32 Criminal justice access to data in the cloud: challenges. Discussion paper. Prepared by the T-CY Cloud Evidence Group (2015), pages 9-10. – Online: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2015/T-CY(2015)10_CEG%20challenges%20rep_sum_v8.pdf.

33 Criminal justice access to data in the cloud: challenges. Discussion paper. Prepared by the T-CY Cloud Evidence Group (2015), page 11. – Online: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2015/T-CY(2015)10_CEG%20challenges%20rep_sum_v8.pdf).

34 Ibid., page 10.

35 For the state's responsibility to protect its citizens, see e.g. ECtHR ..., K.U. v. Finland. – Online: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-89964#{"itemid":["001-89964"].

36 See also section 211 of the CCP, "Objective of pre-trial procedure".

The Convention on Cybercrime (Budapest Convention, hereinafter referred to as the "Convention")[37] establishes a number of procedural guarantees which are specifically targeted at the searching for, collecting, preserving, etc. of electronic evidence. These procedural law provisions are applicable to any crime (not just "traditional cybercrime").[38] At the same time, however, the most disputable situations have been left open in the Convention and the drafters have acknowledged that it would be difficult to introduce a uniform regime.[39]

Convention on Cybercrime

Access to cross-border data is governed by Articles 19 and 32 of the Convention. Article 19 provides for a state's opportunities to expand searches in its territory, while Article 32 regulates the expansion of searches into the territory of another Party. Unfortunately, these Articles of the Convention are not enough to ensure effective proceedings where cloud computing is concerned,[40] due to the problem of the "loss of location". In addition, states' opportunities to collect data located in the territory of another state are limited, as such collection jeopardises several principles of international cooperation in criminal matters. For example, one of the main principles of international cooperation in criminal matters is that of dual criminality, which would be rendered meaningless by unlimited cross-border access to and use of data.[41]

---

37 RT II 2003, 9, 32.

38 Transborder access and jurisdiction: What are the options?, page 8. – Online: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8.

39 T-CY Guidance Note # 3. Transborder access to data (Article 32) (2014), page 4. – Online: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a.

40 Markko Künnapu. Cybercrime Convention Committee: an Update, presentation at the Octopus Conference Cooperation Against Cybercrime, 04.12.2013. – Online: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802f2384.

41 This is illustrated by a situation where police of State A suspect that a person in State B has committed an act that is a crime in State A but not a crime in State B. If the police of State A reach into State B to gather evidence against the person in State B, this may raise significant legal and policy interests for State B. Initially, State B may require dual criminality to provide assistance, or it may require it in cooperation treaties. Even where it does not require dual criminality, it may reserve the right to deny assistance in situations in which it considers that providing cooperation would be contrary to its principles. For example, State B, whose people exercise broad freedom of expression, may not want to collect evidence for another state where this freedom is not respected. (Transborder access to data and jurisdiction: Options for further action by the T-CY (2014), page 12.) – Online: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8).

The question of unilateral cross-border access to data has been discussed at length (but in vain) for a long time. Even the drafters of the Convention have not been successful in this regard: the Explanatory Report to the Convention expressly states that no consensus was reached and no solutions would be offered. In part, this was due to a lack of concrete experience with such situations; and, in part, this was due to an understanding that formulating uniform rules is essentially impossible, given the numerous nuances of particular cases. Therefore, it was decided to limit the regulation of cross-border access to data to the specific provisions of Article 32 and not to regulate other situations until such time as further experience has been gathered. No clarifications have been provided on this issue so far.[42]

Article 32 describes two situations in which a Party may, without the authorisation of another Party:

(a) access publicly available (open source) stored computer data, regardless of where the data are located geographically;

(b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Publicly available computer data include, for example, websites, forums and social networking sites, which are freely visible and accessible to everyone. Neither the owners nor the holders of the data have imposed any restrictions on access to these data (such as protection with a password or the like). It is also worth noting that the location of the data is not relevant in this case – the data may be located in the territory of another Party, the location may be unknown, or it may be established that the data is located in the territory of a State which is not a Party.

While seemingly allowing the collection of evidence from another computer system, Article 32b still imposes a number of restrictions on a body conducting proceedings. First, it is possible to access only data located in another Party, which implies that the body conducting proceedings knows where the data are located. Thus, there is no right to access data in situations in which a person provides consent but the body conducting proceedings is uncertain where the data are located or in which the data are not located in the other Party.[43]

---

42 Ibid., page 19.

43 Transborder access to data and jurisdiction: Options for further action by the T-CY (2014), page 21. – Online: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8.

As regards the 'lawful and voluntary consent', it is important that the person providing access or agreeing to disclose data may not be forced or deceived.[44] What constitutes consent is to be governed by the domestic law of the Party seeking access to data.[45] For example, domestic law may provide that a minor cannot give such consent.[46]

Who is a person who has lawful authority to disclose data through a particular computer system is also arguable. The Explanatory Report to the Convention states that it can be, e.g., the person who has stored the data on a foreign server or who uses the particular e-mail account.[47]

---

44 The Gorshkov/Ivanov case is often cited as an example of voluntary consent under Article 32b. This, however, is not correct, since the accused did not consent to provide access voluntarily, but were coaxed to do so. (Transborder access to data and jurisdiction: Options for further action by the T-CY (2014), page 21, footnote).
The facts of the case were briefly as follows. In autumn 2000, the FBI discovered a series of intrusions into the computer systems of banks, Internet service providers and other US businesses. Examining the computers in the US, the FBI established that the attacks originated from servers located in Russia. The FBI attempted to cooperate with Russian law enforcement agencies, but the attempt failed. Then the FBI decided to act unilaterally. Investigators were authorised by a court to use spyware in order to find out the user names and passwords of the persons behind the attacks. Then the investigators used that information to download incriminating information from the suspects' computers in Russia. Later, the investigators managed to entice the suspects to the United States in order to detain them and gather more evidence. The investigators organised a "test-hacking", in the course of which the suspects disclosed data "voluntarily", i.e. being trapped. In court, one of the suspects stressed that the evidence obtained from Russia was collected in a manner that violated both US and Russian law. The court disagreed, finding the evidence collected with the help of spyware to have been obtained lawfully, since the suspect could not have an expectation of privacy when he entered his user name and password on a "foreign" computer, thereby creating access to his personal information located on a Russian server. As to the investigators' downloading files from the territory of another state, the court held that the US law did not apply because the search and the collection of data were conducted outside the territory of the United States, and that even if the US law did apply, the investigators' actions were justified and necessary. (S. Brenner, J. J. Schwerha IV. "TRANSNATIONAL EVIDENCE GATHERING AND LOCAL PROSECUTION OF INTERNATIONAL CYBERCRIME", 20 J. Marshall J. Computer & Info. L. 347 2001-2002, pages 348–350.)
This is one of the most analysed cases of cross-border collection of evidence. The suspects were convicted. Another interesting discussion of this case can be found in Philip Attfield's article "United States v Gorshkov
Detailed Forensics and Case Study; Expert Witness Perspective" (2005). – Online: http://ieeexplore.ieee.org/stamp/stamp.jsp?reload=true&arnumber=01592518.

45 For example, general agreement by a person to terms and conditions of an online service used might not constitute voluntary consent under domestic law even if these terms and conditions indicate that data may be shared with law enforcement authorities. Instead, an explicit consent is required in each specific case. (Transborder access to data and jurisdiction: Options for further action by the T-CY (2014), page 22.) – Online: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8.

46 Ibid., page 21.

47 Explanatory Report to the Convention on Cybercrime, page 53. – Online: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b.

Article 19 of the Convention provides for the rules on searches of computer systems and seizure of stored computer data. According to that provision, each Party has to adopt such legislative and other measures as may be necessary to ensure that where its authorities access a specific computer system or part of it and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities will be able to expeditiously extend the search and can access the other system.[48] In addition, the Party should provide for guarantees of data protection and secrecy of communication in its domestic law. States may, for example, consider an e-mail stored on a server of a service provider as data in transfer and part of a communication until it is retrieved or downloaded by the addressee for his or her use.[49]

The opportunities provided by this Article can be used only within the state, i.e., when conducting a so-called physical search, discovering a running computer during the search and obtaining access, through the computer, to data on an Estonian server,[50] the investigators of Estonian law enforcement authorities are

---

48 Article 19. Search and seizure of stored computer data
1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
a. a computer system or part of it and computer data stored thereon; and
b. a computer-data storage medium in which computer data may be stored in its territory.
2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1(a), and have grounds to believe that the data sought is stored on another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.
3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2.
These measures shall include the power to:
a. seize or similarly secure a computer system or part of it or a computer-data storage medium;
b. make and retain a copy of those computer data;
c. maintain the integrity of the relevant stored computer data;
d. render inaccessible or remove those computer data in the accessed computer system.
4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data thereon to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

49 Transborder access to data and jurisdiction: Options for further action by the T-CY (2014), page 24. – Online: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8.

50 Whether the data are located on an Estonian server or elsewhere can be ascertained using a 'whois' search, which is freely available on the Internet.

entitled to expand the search under this provision of the Convention. Of course, this is not much of a gain in the context of Estonia, as very few people use Estonian service providers for their everyday electronic affairs.

The Convention does not prescribe how an extension of a search is to be permitted or undertaken; this is left to domestic law. As a possible solution it is suggested that the authority which authorised the search of the initial computer system could be empowered to also authorise the extension of the search[51].

The Estonian legislature has so far not attempted to regulate this field. However, it is possible to find interesting approaches in the practice of other states. While there are quite many states that still resort to legal assistance requests in order to solve the issue of using data located in the territory of another state in criminal proceedings, and are also often forced to give up due to a lack of balance between the resource cost and effectiveness of this process, I would like to highlight the practice of two states – Belgium and Portugal – that approach this issue in a different manner.

Since 2000, the Belgian Criminal Code of Procedure contains Article 88ter, which addresses the question of jurisdiction in relation to searches of computer systems. This provision allows the investigating judge, after having authorised a search on a computer system, to extend the search to another computer system or to a part of another computer system, which may also be located within the territory of another state. The judge can only decide this extension when it is necessary to find the truth in an investigation and when other investigative or procedural measures are not proportionate to the objective pursued (for example, if different search warrants would have to be issued for different premises) or there is a clear risk that evidence would disappear (a condition that is almost always fulfilled in cybercrime cases). In addition, the investigating judge has to restrict the extended search to the parts of another computer system to which the users of the initial system have access (this condition is mostly met when the investigating judge allows the investigative body to enter a computer with the login and password of the suspect). After the extended search, the person responsible for the computer system has to be informed by the investigating judge if he or she can reasonably be identified (most of the time this is not the case).[52]

---

51 Transborder access to data and jurisdiction: Options for further action by the T-CY (2014), pages 24-25. – Online: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8.

52 Transborder access to data and jurisdiction: Options for further action by the T-CY (2014), page 32. – Online: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8.

According to the Belgians, the most innovative part of this provision of their Criminal Code of Procedure lies in its paragraph 3, which states that when it seems that the data discovered is not stored within the Belgian territory, then the data is only copied.[53] When this has happened, the investigating judge only needs to inform the Ministry of Justice through the Public Prosecutor Office, and the Ministry of Justice will inform the state in whose territory the copied data were located, if that state can reasonably be determined (it is rarely the case). This, in turn, means that Belgian police can collect digital evidence starting the computer system search from a computer located in Belgium (not necessarily the computer of the suspect) and go from there to servers located in any state. They can start examining a user account the moment they have the required user names and passwords. This is a major advantage in gathering digital evidence.[54] The Portuguese Code of Criminal Procedure also entitles bodies conducting proceedings to search a computer system outside the national territory if, during the search of the initial computer system in Portugal, it appears that the information sought is stored on a computer system located in the territory of another state, provided that these data are lawfully accessible from the initial system; in this case the search can be extended by authorisation of the competent authority. This right of extension applies both to other computer systems located within Portuguese borders or outside them, provided that access to the initial system was obtained lawfully. Regarding the admissibility of the evidence obtained by such a process, in the absence of a specific regulation, the general rule applied in Portugal is that all the evidence that is not forbidden by law is admissible. Portuguese law enforcement authorities are equally liberal about situations where data are collected in this way in their national territory: the Law on Cybercrime states that where the law enforcement authorities of another state gain, without prior authorisation from the Portuguese authorities, access to data physically located in Portugal, they have the right to obtain the data (this applies to the data that are publicly available as well as to the data to which access was granted by a person legally authorised to disclose the data).[55]

Summary

The Code of Criminal Procedure of Estonia does not regulate computer system searches. It is relatively difficult to apply the existing rules to the collection of

53 The Belgians specifically stress that the data are copied, not taken away, as in the "physical world".

54 Transborder access to data and jurisdiction: Options for further action by the T-CY (2014), pages 32-33. – Online: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8.

55 Ibid., page 38.

evidence in the manner described in this article, but it is still possible. During the revision of the Code of Criminal Procedure, serious consideration should be given to making this investigative measure subject to a specific procedure. When searching a computer system, a body conducting proceedings can currently rely on the provisions of the Code of Criminal Procedure, interpreting them or applying the analogy. However, it is also possible to rely on the Convention. In some cases, evidence can be collected by surveillance operations.

In the case of an inspection, however, the question is whether this measure, considering the extent of infringement of fundamental rights entailed thereby, should be subject merely to the investigator's view of its necessity? When performing an inspection, the body conducting proceedings is not entirely free of jurisdiction-related issues: for example, if the object of inspection is the social media website of a victim or a suspect, then the inspection of the website is complicated in theory, but simple in practice – a mouse click is enough to display various data within the territory of Estonia. An inspection can be based on cooperation (the subject voluntarily provides the user IDs and passwords), but there is always the possibility that voluntary cooperation fails. An investigative body should be able to rely on a legal regime in such cases.

Should the suspect's consent to the inspection of information located in a foreign territory be recorded, and how? Where the consent has been given, should the right of defence be guaranteed? How can situations in which the suspect expressly prohibits the inspection of data be dealt with? Searching computer systems in the course of a so-called physical search of a place provides somewhat more certainty. This procedure is currently generally subjected to the prosecutor's supervision and from 1 September 2016 it will be subjected to judicial review. Thus, when considering an application, the prosecutor and – in future – the court will consider, inter alia, whether the collection of digital evidence is necessary and justified, and to what extent. However, the inspection of data in the course of other investigative procedures is not subjected to direct supervision by the prosecutor's office or the court in most cases.

In a situation where there is uncertainty about the state in whose territory data are located it is not clear whether it can be acknowledged that the exact location is not known and there is no need to find it out (cloud computing) or whether the location of the parent company should serve as the basis (Gmail, Facebook and other common service providers). If it is known that the data are located in the territory of a state which is not party to the Convention and may also refuse to provide friendly mutual legal assistance, should the proceedings be declared hopeless? Indeed, in such cases it can be accepted that other investigative and procedural measures are ineffective and that permitted surveillance measures should be taken (in this case, data would always be inspected, stored and copied

in the territory of Estonia). The fact is, however, that surveillance cannot solve all the problems, because only a part of measures can be taken secretly from a data subject during proceedings. Computer system searches could be, and often are, public investigative measures.

It is recognised that law enforcement authorities are faced with increasing difficulties in determining the actual location of servers, also because persons committing criminal offences deliberately make the choices that make the establishment of the state of location of data as complicated as possible. Perhaps this "loss of location" is the straw (or more hopefully – the branch) at which it is possible to clutch in judicial disputes.

Given the volume of digital information, the issues described throughout this article can arise in the proceedings of almost all criminal offences. The specificity of criminal procedure rules is what bodies conducting proceedings and decision-makers apparently crave and for which also the legislature bears responsibility: how can a good balance between the prevention of unjustified infringement of persons' fundamental rights and the possibility to still collect evidence be struck? How can breaches of the national sovereignty of other states be avoided and respect for the fundamental principles of criminal procedure be ensured, but digital evidence still be obtained which can be destroyed quickly and easily moved across jurisdictions? The legislature has to solve quite a difficult task.

3
Court statistics

Summary of statistics on cases adjudicated pursuant to criminal and misdemeanour procedure in 2015

Külli Luha, Analyst in the Ministry of Justice

In 2015, a total of 30,703 civil cases, 17,189 cases subject to criminal procedure (incl. 7540 criminal cases) and 11,695 misdemeanour cases were filed with county courts for hearing. Administrative courts received 3371 actions. In appeal procedure and appeal against ruling procedure, 2949 civil cases, 1790 administrative cases, 2399 cases subject to criminal procedure and 197 misdemeanour cases were filed with circuit courts.

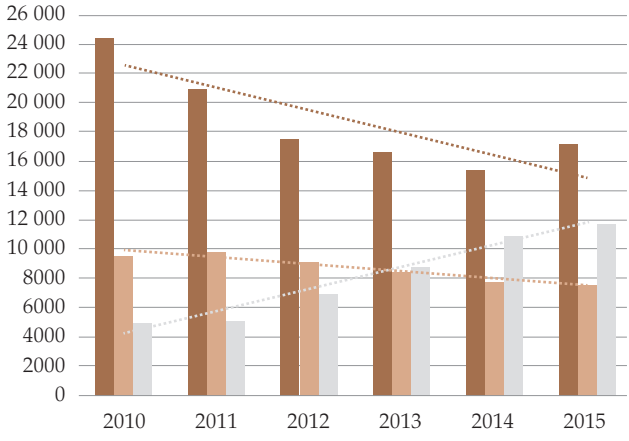
In 2015, a total of 31,158 civil cases, 16,927 cases subject to criminal procedure (incl. 7359 criminal cases) and 10,872 misdemeanour cases were adjudicated in county courts. Administrative courts adjudicated a total of 3523 administrative cases. Circuit courts adjudicated a total of 2950 cases in civil proceedings, incl. 1734 civil cases in appeal procedure; a total of 2377 cases in criminal proceedings, incl. 556 criminal cases in appeal procedure, and 198 cases in misdemeanour proceedings. Total 1696 administrative cases were adjudicated in circuit courts, incl. 797 cases in appeal procedure.

More detailed statistical data about the proceedings conducted in courts of first and second instance in 2015 are available by type of procedure on the courts' website at http://www.kohus.ee/et/eesti-kohtud/kohtute-statistika.

About the statistics of proceedings of criminal and misdemeanour cases in 2015

The trend of cases received by county courts in criminal procedure has been negative in the past five years (Figure 1), i.e. the total number of cases filed has decreased by 29.7% compared to 2010 (in particular due to the decline in the number of cases received by judges in charge of execution of judicial decisions), but in comparison with 2014 the number of cases has increased by approximately 11% (also in connection with the cases received by judges in charge of execution of judicial decisions). In addition, the number of cases referred to preliminary investigation judges has increased by approximately 3% (compared to 2014). The trend of criminal cases adjudicated by courts pursuant to general or simplified procedure has steadily declined from year to year (the number of such criminal cases has decreased by approximately 20% compared to 2010 and by approximately 2% compared to 2014).

Figure 1. *Cases subject to criminal or misdemeanour procedure received in county courts, 2010–2015*



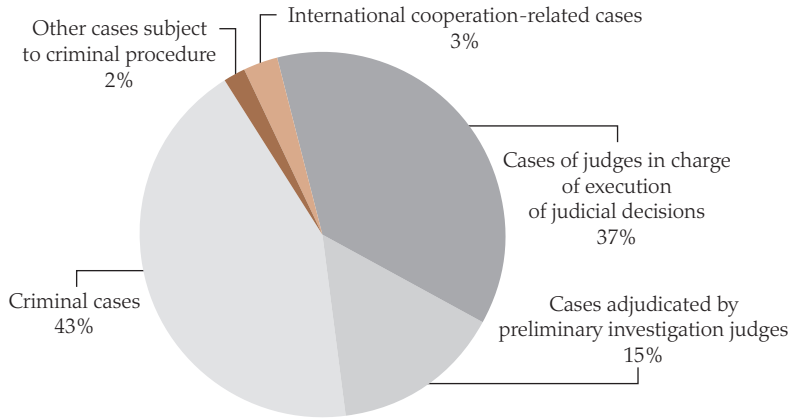
	2010	2011	2012	2013	2014	2015
Cases subject to criminal procedure	24 450	20 908	17 484	16643	15 434	17 189
incl. criminal cases	9473	9848	9129	8418	7699	7540
Cases subject to misdemeanour procedure	4875	5111	6917	8790	10861	11 695

In 2015, county courts received a total of 17,189 cases subject to criminal procedure, incl. 7408 in Harju County Court, 2011 in Pärnu County Court, 4029 in Tartu County Court and 3741 in Viru County Court. A total of 16,927 cases subject to criminal procedure were adjudicated in 2015, including 7203 in Harju

County Court, 2029 in Pärnu County Court, 3993 in Tartu County Court and 3702 in Viru County Court (the rate of adjudication is 98.5% in this type of procedure).

Within the type of procedure, cases were distributed as follows (Figure 2): of the cases adjudicated in 2015, criminal cases accounted for 43%, cases referred to judges in charge of execution of judicial decisions represented 37%, cases adjudicated by preliminary investigation judges accounted for 15%, international cooperation-related cases accounted for 3% and other cases subject to criminal procedure represented 2%. There were no significant differences between county courts in terms of substantive distribution of cases. The proportion of criminal cases was 43% in all county courts, and international cooperation-related cases accounted for around 2–4%. The proportions of cases adjudicated by preliminary investigation judges differed the most, with these cases representing 11% of all cases adjudicated by Viru and Tartu County Courts, 14% of all cases adjudicated by Pärnu County Court, and 19% of all cases adjudicated by Harju County Court.

Figure 2. *Proportions of cases adjudicated pursuant to criminal procedure by county courts in 2015*

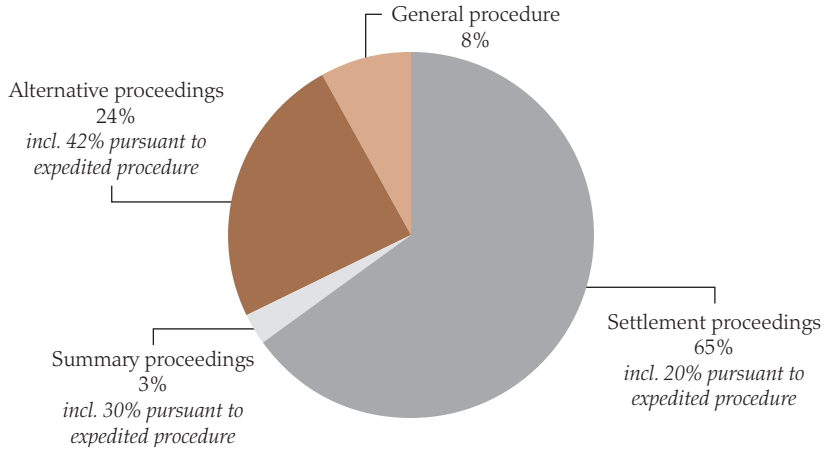


Criminal cases adjudicated by county courts

County courts received a total of 7540 criminal cases in general procedure and simplified procedure, incl. 3068 in Harju County Court, 1133 in Pärnu County Court, 1882 in Tartu County Court and 1457 in Viru County Court.

Around 4926 criminal cases were adjudicated in settlement proceedings (incl. 1031 pursuant to expedited procedure), 1786 in alternative proceedings (incl. 752 pursuant to expedited procedure), 228 in summary proceedings (incl. 68 pursuant to expedited procedure) and 600 pursuant to general procedure (Figure 3). While the proportions of cases adjudicated pursuant to general procedure were relatively similar in county courts (from 7% of the total number of criminal cases in Harju County Court to 9.7% in Pärnu County Court), the proportions of various types of simplified proceedings were quite different. For example, cases received in settlement proceedings accounted for 46.3% of the criminal cases adjudicated by Harju County Court, but 87.8% and 82.5% of the criminal cases adjudicated by Tartu and Pärnu County Courts, respectively, and 62.9% of the criminal cases adjudicated by Viru County Court. There were also differences in the proportions of cases adjudicated in alternative proceedings (46.3% in Harju County Court, 3.6% in Pärnu County Court, 2.9% in Tartu County Court and 18.7% in Viru County Court) and cases adjudicated in summary proceedings (0.4% in Harju County Court, 4.1% in Pärnu County Court, 1.0% in Tartu County Court and 10.4% in Viru County Court).

Figure 3. *Distribution of criminal cases by type of procedure in county courts, 2015*



In 2015, criminal cases were heard in county courts by a total of 70 judges (24 in Harju County Court, 14 in Pärnu County Court, 20 in Tartu County Court and 12 in Viru County Court) who adjudicated a total of 7359 criminal cases, incl. 421 pursuant to general procedure, 1733 in alternative proceedings, 4962 in settlement proceedings and 243 in summary proceedings. The following table provides a more detailed overview of the distribution of adjudicated criminal cases by type of procedure in county courts and of the average duration of proceedings.

Court	General procedure		Alternative proceedings		Settlement proceedings		Summary proceedings	
	Adjudicated cases	Average duration of proceedings (in days)	Adjudicated cases	Average duration of proceedings (in days)	Adjudicated cases	Average duration of proceedings (in days)	Adjudicated cases	Average duration of proceedings (in days)
Harju County Court	115	118	1376	19	1412	24	13	4
Pärnu County Court	113	206	53	103	924	18	54	4
Tartu County Court	108	290	60	94	1693	29	19	5
Viru County Court	85	265	244	77	933	30	157	11
Average of county courts	**421**	**215**	**1733**	**33**	**4962**	**26**	**243**	**6**

The average duration of proceedings of cases adjudicated pursuant to general procedure was 215 days or significantly shorter (by 131 days) and also more even across county courts (by 63 days) than in 2011.

Court	Average duration of proceedings of cases adjudicated pursuant to general procedure (in days)				
	2015	2014	2013	2012	2011
Harju County Court	118	124	157	190	317
Pärnu County Court	206	213	249	284	258
Tartu County Court	290	187	244	302	310
Viru County Court	265	359	332	578	468
Average of courts	**215**	**214**	**233**	**327**	**346**

At the end of 2015, 785 criminal cases remained to be adjudicated, incl. 270 in Harju County Court, 93 in Pärnu County Court, 197 in Tartu County Court and 225 in Viru County Court. "Old" cases (criminal cases heard by county courts for longer than 365 days pursuant to general procedure and for longer than 150 days in simplified proceedings) represent 6.6% of the cases that remain to be adjudicated, as described in more detail in the table below:

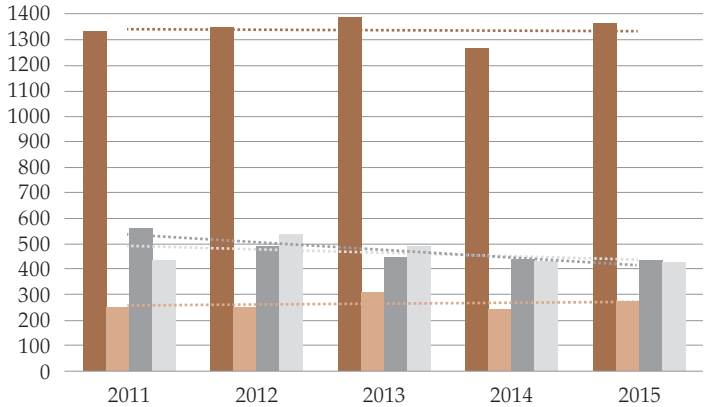
Court	Proportion of "old" cases in the number of cases that remain to be adjudicated (31.12.2015)			
	General procedure	Alternative proceedings	Settlement proceedings	Summary proceedings
Harju County Court	3,5%	9,4%	-	-
Pärnu County Court	6,7%	20,0%	2,3%	-
Tartu County Court	10,4%	-	6,1%	-
Viru County Court	7,4%	1,9%	-	-
Average of county courts	**6,6%**	**1,9%**	**2,2%**	**-**

Cases adjudicated by preliminary investigation judges in county courts[1]

Cases adjudicated by preliminary investigation judges are not characterised by a clear-cut trend in recent years (Figure 4), as the number of those cases has been quite variable from year to year (for example, the number of such cases was around 5% lower last year than in 2013, but approximately 5% higher than in 2014). The number of cases adjudicated by preliminary investigation judges grew in Harju and Pärnu County Courts (by 8% and 13%, respectively), but remained on previous levels in Tartu and Viru County Courts (declining by around 1% in both county courts).

1 The summary is provided on the basis of cases entered in the information system of courts and does not include statistics on authorisations of surveillance operations. Statistics on surveillance operations is available at: http://www.kriminaalpoliitika.ee/search/searchbuilder/landing?searchbuilder_id=1428&title=&document=&fields%5Bfield_doc_type%5D=K%C3%B5ik&fields%5Bfield_valdkond%5D=J%C3%A4litustegevus&fields%5Bfield_date%5D=between&aasta=&fields%5Bfield_author%5D=&order=Kuup%C3%A4ev&sort=desc&Vaata=Vaata.

Figure 4. *Cases adjudicated by preliminary investigation judges in county courts, 2011–2015*

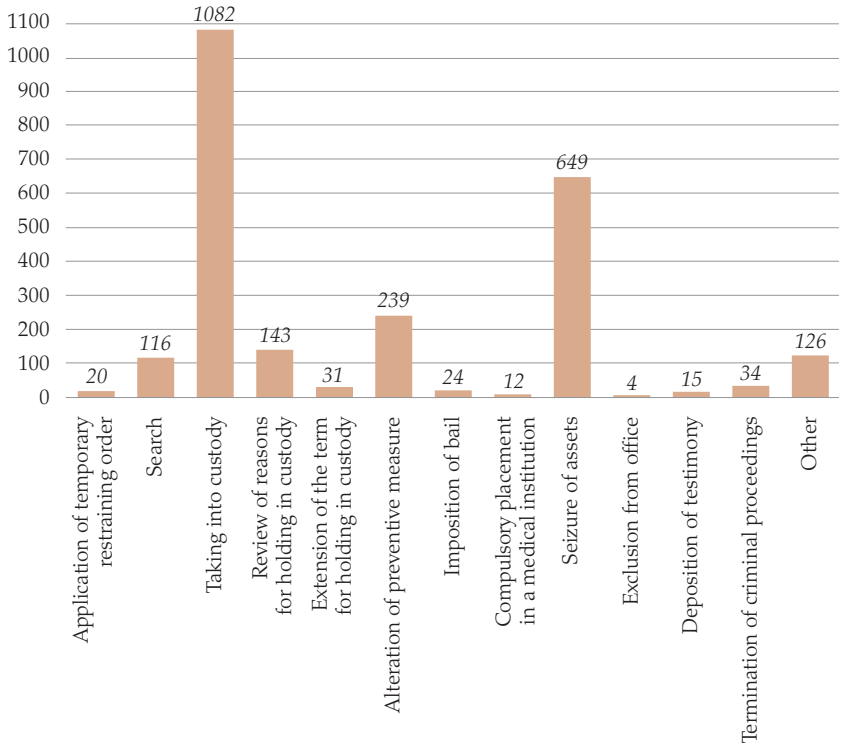


	2011	2012	2013	2014	2015
Harju County Court	1333	1348	1390	1265	1364
Pärnu County Court	250	250	308	240	272
Tartu County Court	556	490	449	440	436
Viru County Court	435	538	491	431	423

In 2015, judges adjudicated 2495 preliminary investigation judge's cases (Figure 5), including 1364 in Harju County Court, 272 in Pärnu County Court, 436 in Tartu County Court and 423 in Viru County Court. The number of judges serving as preliminary investigation judges is very different in courts: 4 in Harju County Court, 16 in Pärnu County Court, 22 in Tartu County Court and 12 in Viru County Court.

Cases of taking into custody represented the majority of the cases of preliminary investigation judges (around 43%), cases of seizure or confiscation of assets accounted for approximately 26%, cases of alteration of a preventive measure represented approximately 10% and reviews of the reasons for taking a person into custody accounted for around 6%. There were no significant differences between county courts in terms of distribution of cases.

Figure 5. *Cases adjudicated in county courts by preliminary investigation judges, by type, 2015*



The average duration of proceedings of cases adjudicated by preliminary investigation judges in county courts was 6 days in 2015, but the durations varied considerably across types of cases. The following table presents the differences between durations of proceedings, without distinguishing between county courts.

Decision-making by preliminary investigation judges, by types of cases	Average duration of proceedings
Search	1-2 days
Taking into custody	0-1 days
Alteration of preventive measure	20 days
Imposition of bail	18 days
Seizure of assets	8 days
Exclusion from office	3-4 days
Review of reasons for holding in custody	7-8 days
Application of temporary restraining order	4-5 days

The durations of proceedings adjudicated by preliminary investigation judges differed across types of cases and across county courts. The following table sets out the main differences in county courts (in addition to the average duration of proceedings the table also sets out the numbers of cases adjudicated):

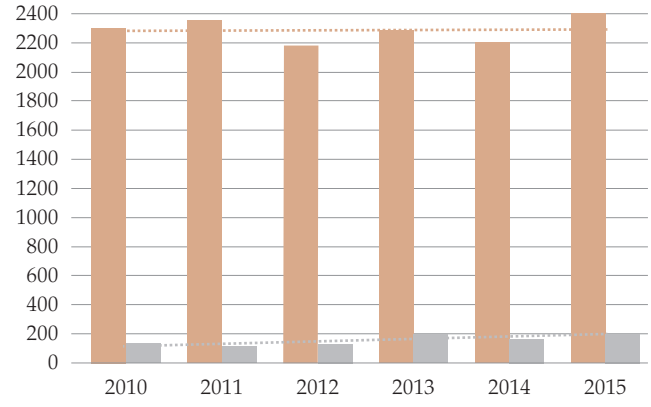
	Harju County Court		Pärnu County Court		Tartu County Court		Viru County Court	
	Number of cases	Average duration (in days)	Number of cases	Average duration (in days)	Number of cases	Average duration (in days)	Number of cases	Average duration (in days)
Taking into custody	583	0,9	109	0,6	188	1,4	203	0,6
Confiscation/seizure of assets	355	10	76	2	109	6	91	5
incl. in urgent cases	*18*	*7*	-	-	-	-	-	-
Search	69	2,7	19	0,8	23	1,1	5	0,4
Alteration of preventive measure	113	18	39	18	37	20	51	27

At the end of 2015, 23 cases remained to be adjudicated in county courts by preliminary investigation judges (mostly cases received in December).

Cases subject to criminal procedure in circuit courts

The trend of cases appealed to circuit courts has remained unchanged in recent years (Figure 6), which means that circuit courts receive around 2200–2300 new cases each year. In 2015, circuit courts received a total of 2399 new cases in appeal procedure and appeal against ruling procedure (9% more than in 2014), including 1283 in Tallinn Circuit Court and 1116 in Tartu Circuit Court.

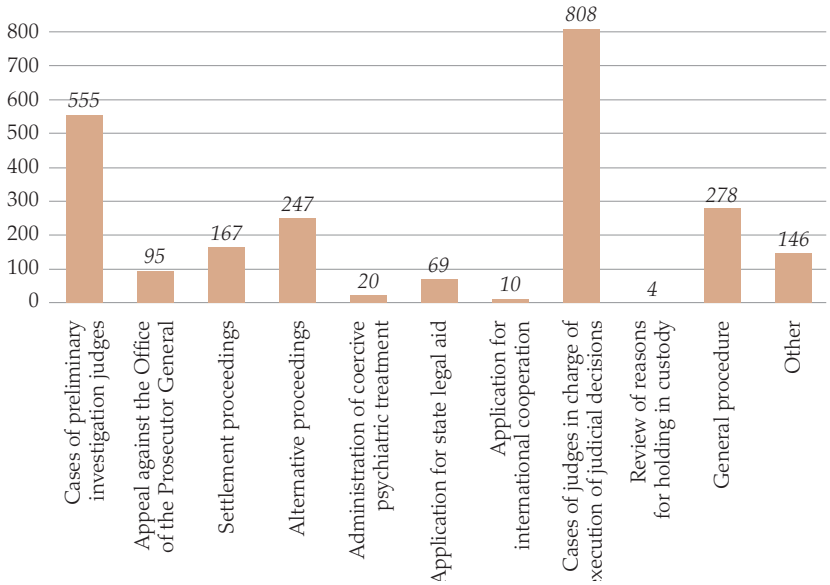
Figure 6. *Cases subject to criminal or misdemeanour procedure received in circuit courts*



	2010	2011	2012	2013	2014	2015
Cases subject to criminal procedure	2311	2356	2182	2284	2200	2399
Cases subject to misdemeanour procedure	120	115	126	195	167	197

By type, the cases received by circuit courts in 2015 were distributed as follows (regardless of whether the cases were filed in appeal procedure or in appeal against ruling procedure): cases of judges in charge of execution of judicial decisions accounted for a third (808 appeals), cases adjudicated by preliminary investigation judges accounted for around 23% (555 appeals) and cases adjudicated pursuant to general procedure represented approximately 12% (278 appeals), with all these cases accounting for 68% of cases filed with circuit courts.

Figure 7. *Substantive distribution of cases appealed to circuit courts in 2015*



While the most common appeal cases mentioned above dominated in both circuit courts, their proportions were somewhat different. For example, the proportion of cases of judges in charge of execution of judicial decisions was around 42% of the appeals filed with Tartu Circuit Court and around 26% of the appeals filed with Tallinn Circuit Court. Then again, the proportion of cases adjudicated by preliminary investigation judges was higher in Tallinn Circuit Court (approximately 25%), while accounting for around 20% of the appeals filed with Tartu Circuit Court. Appeals adjudicated pursuant to general procedure represented around 11–12% in both circuit courts. Appeals heard in alternative proceedings accounted for approximately 10% in Tallinn Circuit Court.

Tallinn and Tartu Circuit Courts adjudicated 2377 cases, incl. 1265 in Tallinn and 1112 in Tartu. The average durations of proceedings in cases adjudicated in recent years are set out in the following table:

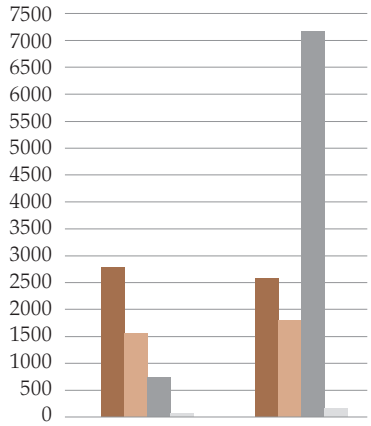
Court	Average duration of proceedings in cases adjudicated pursuant to criminal procedure (in days)				
	2015	2014	2013	2012	2011
	in appeal procedure				
Tallinn Circuit Court	30	34	39	40	48
Tartu Circuit Court	38	42	41	53	65
Average of courts	**33**	**37**	**40**	**44**	**54**
	in appeal against ruling procedure				
Tallinn Circuit Court	13	17	19	7	8
Tartu Circuit Court	17	14	15	10	14
Average of courts	**14**	**15**	**18**	**9**	**11**

At the end of 2015, a total of 113 cases remained to be adjudicated by circuit courts, incl. 81 by Tallinn Circuit Court and 32 by Tartu Circuit Court. There were no "old" cases (cases heard by circuit courts in appeal procedure for longer than 365 days or in appeal against ruling procedure for longer than 45 days) at the end of 2015.

Cases subject to misdemeanour procedure

The trend of cases subject to misdemeanour procedure filed with county courts has been rising steadily in recent years (Figure 1). The number of cases adjudicated in this type of procedure has grown by 128% compared to 2011 (by 9.3% compared to 2014). The main reason for the growth of workload in this type of procedure is the approximately ten-fold increase in the number of enforcement cases (Figure 8).

Figure 8. *Number of cases subject to misdemeanour procedure*



	2011	2015
Misdemeanour cases	2774	2572
Appeals against decisions in misdemeanour cases	1553	1801
Enforcement	752	7170
Other	32	152

Review of cases in the Supreme Court in 2015

Signe Rätsep, Chief Specialist of the Legal Information Department
Karolyn Krillo, Adviser to the Civil Chamber
Rauno Kiris, Head and Analyst of the Legal Information Department

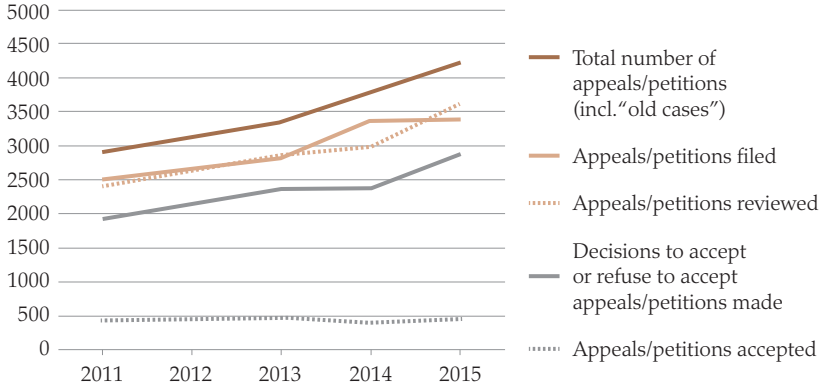
Statistical information characterising the work of the Supreme Court is collected with regard to pre-trial proceedings in the Supreme Court and proceedings in the Supreme Court. Data on appeals in cassation, appeals against a ruling, petitions for the review of court decisions and on cases adjudicated are collected for civil, administrative and offence proceedings. In constitutional review proceedings, data are collected only with regard to cases that have been adjudicated. Data regarding pre-trial proceedings are recorded about appeals and petitions filed (e.g. appeals in cassation, appeals against a court ruling and petitions for review). For cases reviewed and accepted for proceedings, the data are registered by the numbers of the cases. It should be noted that one court case may be based on several appeals or petitions, which were reviewed and accepted for proceedings during the pre-trial proceedings.[1]

Pre-trial proceedings in the Supreme Court

The number of appeals and petitions filed with the Supreme Court is growing steadily. For example, the number of appeals and petitions filed has increased by 72% in comparison with 2005 (1972 appeals and petitions filed with the Supreme Court in 2005, and 3395 in 2015). Along with the growth in the number of appeals and petitions filed, the number of appeals and petitions reviewed has consistently increased, as well; in 2015, the number of appeals and petitions reviewed by the Supreme Court exceeded the number of petitions filed in 2015 (see Figure 1).

1 More detailed data regarding the review of petitions and cases in the Supreme Court since 1993 is available on the website of the Supreme Court at http://www.riigikohus.ee/?id=79.

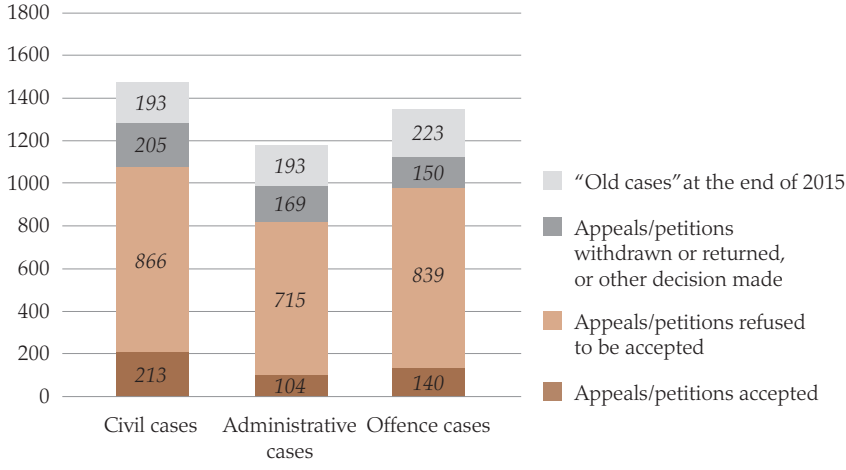
Figure 1. *Pre-trial proceedings in the Supreme Court, 2011–2015*



According to law, the Supreme Court has the right to decide whether to accept or refuse to accept an appeal or a petition for proceedings. The Supreme Court accepts an appeal or a petition in order to ensure the legitimacy of the decisions of courts of lower instance, harmonise judicial practice or develop procedural law.

In 2015, 16% of appeals and petitions reviewed were accepted (457 of 2877). In 2014, 18% of appeals and petitions reviewed were accepted (422 of 2391). In 2013, 20% of appeals and petitions reviewed were accepted (478 of 2361). A year earlier the same figure was higher by two percent, i.e. 22% (464 of 2151). The number of appeals and petitions that were accepted in relation to the appeals and petitions reviewed declined consistently during the period 2012–2015.

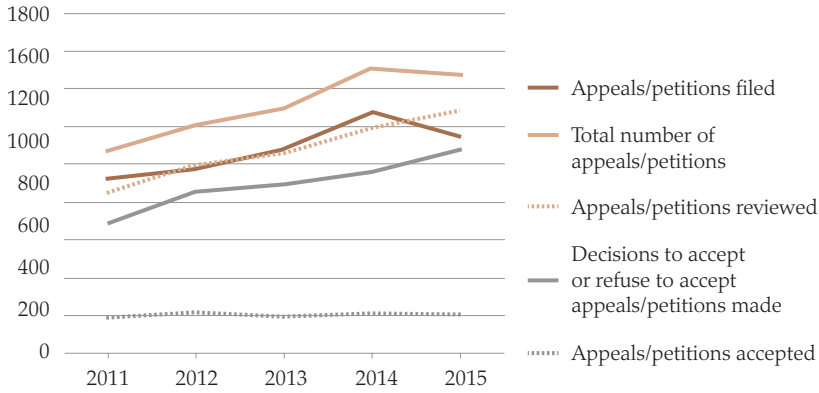
Figure 2. *Pre-trial proceedings by type of proceedings in 2015*



In 2015, as in previous years, the Civil, Administrative Law and Criminal Chambers of the Supreme Court had a high workload (see Figure 2).

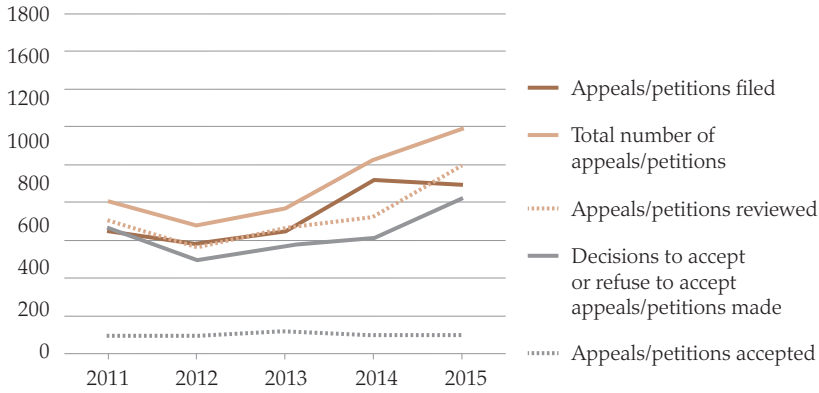
In the Civil Chamber, the number of appeals and petitions totalled 1477 (1505 in 2014), 1152 of which were filed in 2015. The chamber reviewed 1284 appeals or petitions (1195 in 2014). Decisions to accept or refuse to accept an appeal or a petition were made for 1079 appeals or petitions (963 in 2014). 213 appeals and petitions were accepted (209 in 2014).

Figure 3. *Pre-trial proceedings in the Civil Chamber*



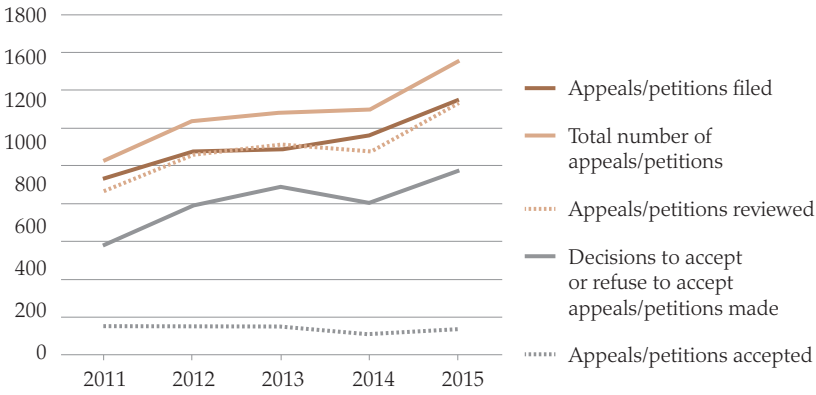
In the Administrative Law Chamber, the number of appeals and petitions totalled 1192 in 2015 (1026 in 2014), 894 of which were filed in 2015. The Administrative Law Chamber reviewed 997 appeals or petitions (728 in 2014) and made decisions to accept or refuse to accept an appeal or a petition for 819 appeals or petitions (616 in 2014). 104 appeals and petitions were accepted (103 in 2014).

Figure 4. *Pre-trial proceedings in the Administrative Law Chamber*



In the Criminal Chamber, the number of appeals and petitions totalled 1556 (1296 in 2014), 1349 of which were filed in 2015. The Criminal Chamber reviewed 1332 appeals or petitions (1082 in 2014). Decisions to accept or refuse to accept an appeal or a petition were made for 979 appeals or petitions (812 in 2014). 140 appeals and petitions were accepted (110 in 2014).

Figure 5. *Pre-trial proceedings in the Criminal Chamber*



Outcome of adjudication of cases in the Supreme Court

Constitutional review

In 2015, 41 cases were subject to constitutional review proceedings in the Supreme Court. The following Table 1 describes the outcome of the adjudication of cases in the Constitutional Review Chamber in more detail. In the cases adjudicated by the Constitutional Review Chamber and the Supreme Court en banc, a petition or appeal was satisfied in 9 cases. A provision of a contested legislative act was declared to be in conflict with the Constitution in 8 cases. 14 appeals or petitions were dismissed; 17 were returned without having been reviewed.

Table 1. *Outcome of the adjudication of cases in the Constitutional Review Chamber in 2015*

		Total		Legislative acts	Regulations of the Government of the Republic	Acts of local government	Decisions or measures of the National Electoral Committee	Decisions of the Parliament or the President of the Republic	Other
	Cases adjudicated in the Constitutional Review Chamber in 2015	**41**	*100%*	**22**	**2**	**2**	**15**	**1**	**1**
Petitioner	Chancellor of Justice	**3**	*8%*	2	1				
	Court	**18**	*43%*	16	1	1			
	Local government council	**2**	*5%*	2					
	Other person	**18**	*45%*			1	15	1	1
Outcome	**Petition satisfied or provision of a contested legislative act declared to be in conflict with the Constitution**	**9**	*23%*	**8**			**1**		
	Petition dismissed; provision of a contested legislative act declared to be constitutional	**14**	*35%*	6	1	1	6		
	Petition returned without review	**17**	*43%*	5	1	1	8	1	1
	Entry into force of the judgment postponed	**1**	*3%*	1					

Adjudication of cases in Criminal, Administrative Law and Civil Chambers

The Criminal Chamber adjudicated 118 cases of offence, including 98 criminal cases and 20 misdemeanour cases. The Criminal Chamber refused to amend the contested judicial decision in 28 criminal cases and in 2 misdemeanour cases.

The contested decision was annulled in 65 criminal cases and 13 misdemeanour cases. Reasoning of a contested judicial decision was amended in three cases.

The Civil Chamber adjudicated a total of 203 cases in 2015. The Civil Chamber annulled 77% (156) of the contested judicial decisions, refused to amend 26 decisions and amended the reasoning of 13 decisions.

The Administrative Law Chamber adjudicated 90 administrative cases. The contested decision was annulled in 51 administrative cases (nearly 57%). The Administrative Law Chamber refused to amend a decision in 18 cases and amended the reasoning of a contested judicial decision in 11 cases.

Figure 6. *Adjudication of cases in Criminal, Administrative Law and Civil Chambers in 2015*