LEGISLATION CHANGES - PERMANENT PART OF CRIMINAL PROCEDURAL LAW IN SLOVENIA

Mojca Rep, MSc[1]
District Court Celje; Higher Court in Ljubljana, Slovenia

Abstract: In 2016, the legislator has changed or tried to change the Criminal Procedure Act (hereinafter: CPA) for the fourteenth time since 1995 in order to achieve a more efficient and economical performance of criminal proceedings while ensuring an appropriate level of rights protection of participants in proceedings, a more adversarial nature of criminal proceedings, elimination od shorcomingof shortcomings and greater legal certainty and legality in proceedings. Unfortunately, the Act was not adopted by the National Assembly. However, the latter has changed this year. The aim of the revision was also the different regulation of certain investigative acts. Taking into account the recent practice of the Constitutional Court of the Republic of Slovenia and the European Court of Human Rights, the Act systematically regulates the seizure of objects, files and electronic devices of lawyers and other persons in the case of their material containing privileged communication, or if it is necessary to investigate the electronic device that was seized and contains information that are is not secured and sealed but may also be part of the so-called (professional) secrecy. A large part of the novelty also refers to the modification and completion of the regime of undercover investigative measures. Moreover, according to the needs of the police, a catalogue of serious criminal offences has been completed, in respect of which this measure is permissible. CPA – N (Official Gazette RS, 22/2019) thus improves the legal basis for the cooperation of competent authorities and a faster progress of criminal proceedings. In this way, the balance between the guarantee and the protective function of the procedure is ensured.

Keywords: criminal proceedings, investigative acts, legal certainty, legality, judicial practice.

INTRODUCTION

Criminal Procedure Act (hereinafter CPA) has been amended fourteen times since 1995. As always, the reason for the change is mandatory implementation of transnational regulations, decisions of the Constitutional Court, and more im-

1 mojca_rep@yahoo.com

portantly, achieving a more efficient and economical performance of criminal proceedings while ensuring an appropriate level of rights protection of participants in proceedings, a more adversarial nature of criminal proceedings, elimination of deficiencies, and greater legal certainty and legality in criminal proceedings. According to some of the reactions to the amendment to the proposal of the CPA-N (Act Amending the Criminal Procedure Act, Official Gazette RS, 22/2019) in the legislative procedure in 2017, the proposal for the amendment to the act clarifies more clearly the possibility of carrying out certain individual investigative acts. Taking into account the recent decisions of the Constitutional Court of the Republic of Slovenia and the European Court of Human Rights, the seizure of objects, files and electronic devices of lawyers and other persons is systematically regulated providing that the material contains privileged communication. The arrangement of the house investigation is corrected by, on the one hand, protecting the rights of the property owner, where the latter is unavailable. In terms of increasing the effectiveness of the work of law enforcement agencies and investigating criminal offenses and gathering evidence, the issues of using traffic data and obtaining confidential bank data are regulated in a more clear, definite, and constitutional manner. When joining cases in pre-trial procedures, in filing a chargeable act and requesting an investigation, the state prosecutor should proceed more rationally. Nevertheless, in addition to respecting rights, this is the guideline of the entire criminal procedure.

NEW REGULATION OF CERTAIN INVESTIGATIVE ACTS

The article further introduces some investigative acts and their new arrangements which, in practice, should have long-term positive consequences in regard to successful prosecution of perpetrators of criminal offenses.

Undercover investigative measures:

Pthe proposed act amending and supplementing CPA-N (Ministry of Justice, 2018) directs undercover investigative measures, the conditions and procedures for their imposition and execution in Articles 149a to 155a and Article 156a: secret surveillance, acquisition of traffic data in the electronic communications network, control of electronic communications, control of letters and other shipments, computer systems of banks, eavesdropping and recording of conversations, eavesdropping and watching a person in a foreign residence or other premises, quasi buying-in, activities of secret service. The measure of secret surveillance is permissible in the light of the needs of the police for criminal offenses for which the Act prescribes a prison sentence of five years or more; criminal offenses of unlawful deprivation of liberty, stalking, threats, misuse of personal data, illegal employment, fraud, concealment, fraud to the detriment of the European Union, attacks on the information system, falsification or destruction of business documents, disclosure and unjustified acquisition of business secrets, misuse of the information system, abuse of office or official rights, disclosing classified information, public incitement to hatred, violence and intolerance, forbidding the crossing of the border or territory of the country, pollution of drinking water, food or feed contamination, and torture of animals (CPA-N, Official Gazette RS, 22/2019). Acquisition of data on participants, circumstances and facts of telecommunications traffic, such as numbers or other means of identifying users of electronic communications services, the type, date, time and duration of the call or other electronic communications service, the amount of data transferred and the place from which the service was provided is regulated in such a way that it specifies that such information shall be communicated by the operator to the competent authority on the basis of a prosecution order, suggested by the public prosecutor, providing that the prescribed conditions are given. In the meantime, the third paragraph stipulates that the operator must, upon written request of the police, communicate to the police the information about the owner or user of a particular communication medium for electronic communications traffic from an unpublished directory and the time at which the user used or still uses such an asset, e.g.for example, a mobile phone (Ministry of Justice, 2018).. Thus, it is the duty of the operators to provide such data at the request of the police (i.e. without the investigating judge's order) because such data do not constitute content or messages in terms of the constitutionally protected secrecy of information. The Constitutional Court of the Republic of Slovenia (2013) abolished the entire chapter XIII of the Electronic Communications Act, which stipulated compulsory fourteen or eight months of storage of certain traffic, location and subscriber data for public communications service operators for the purpose of their subsequent acquisition in accordance with the proposed act amending and supplementing CPA-N (Official Gazette RS, 22/2019) , Slovene Intelligence and Security Agency (Official Gazette RS, 81), or the Defense Act (Official Gazette RS, 95/15). Among other things, it was considered that the above measure was not necessary because the legislature did not merely restrict the use of personal data stored in the course of criminal proceedings solely to investigation, detection and prosecution of grave crimes, which is also the opinion of the Court of Justice of the European Union (2014). The legislator interfered with the right to the protection of personal data by defining the obligatory storage of traffic data, while at the same time it did not carefully assess the circumstances on the basis of which the interference would be interrupted. Taking into account the judgment of the Constitutional Court of the Republic of Slovenia (2013), it was therefore necessary to also adapt the provisions on the acquisition of traffic data in the course of criminal proceedings in a manner that would define a more procedurally determined approach. The proposed act amending and supplementing CPA-N (Official Gazette RS, 22/2019*)* provides a new, more detailed and up-to-date regime for the acquisition of traffic and related data. The measure is divided into two separate measures, namely on the renewed Article 149b, which regulates the acquisition of traffic data, which includes the acquisition of stored traffic data already legally stored by the operators, and a new article 149c governing freezing and forwarding traffic data forwards. The part of the transfer of the Budapest Convention on the Contract for the Carriage of Goods by Inland Waterways (Official Journal of the European Union L 276/3 2015) to the Slovene legislation is also mentioned. In this way, in order to access stored traffic data, which also affects a large number of subscribers or users, according to the requirements of the aforementioned decision of the Constitutional Court, it is bound to a narrower catalog of criminal offenses (Gorkič, 2014). At the same time, the measure of obtaining certain subscriber data is clearly and precisely regulated in the new Article 149.č. Moreover, Article 149d is added and it regulates the access to subscriber data by the private prosecutor. The latter was necessary in particular to prosecute crimes against honor and good name made on the internet (Ministry of Justice, 2018). Article 149b must also be harmonized with the provisions of the Electronic Commerce Market Act (Official Gazette RS, 96/09) (hereinafter ECMA), since the current text only allows the acquisition of traffic data from operators, but not from providers of other services performed via electronic communication networks. These are services that are usually provided for remuneration, remotely, by electronic means and at the individual request of the recipient of services, and for which the police often have to obtain information about the final recipient of the service or the communication itself through which the service was performed. ECMA (Official Gazette RS, 96/09) already stipulates that service providers should notify the competent authorities at their request no later than within three days of receipt of the information on the basis of which it is possible to identify the recipients of their services (name and surname, address, company, e-mail address). However, it also adds that providers must communicate such information on the basis of a court order and, without a court order, if so provided by a sectoral law. The rules for obtaining data from banks, savings banks, payment institutions or electronic money issuing companies are set out in Article 156 of the proposed act amending and supplementing CPA-N (Official Gazette RS, 22/2019) , where it is also stated which data the police can obtain from these institutions without the order of the investigating judge. The investigating judge's order is required for data on application forms, deposits, balance and turnover in invoices or other transactions. What is more, the basis for obtaining data on traffic on the use of these services was arranged as well. The detection and investigation of complex and serious crimes and rapid technological development are the reasons why the competent authorities for the detection and prosecution of offenders must have effective investigative measures. The latter is even more important for organized criminal groups in a narrow and closed circle of persons with precise roles and a high level of caution in the conduct of criminal activity. Their operation is organized in such a way that individuals who carry out criminal acts in a criminal organization use only known telephone devices and numbers, and at short intervals. They change both the apparatus and the numbers during personal contact. The aforementioned means that the police cannot acquire telephone numbers used for communication with criminal organization through classical methods of investigation, and consequently also do not intercept these communications with established undercover investigative measures. In the light of the above and given the fact that there are technical possibilities, authorities that detect, investigate and prosecute such offenses and perpetrators must also be enabled the use of technical means for identifying data for identifying the number of the communication medium and the electronic communication numbers for the purpose of identifying location of the communication medium (Ministry of Justice, 2018). The Constitutional Court of the Republic of Slovenia (2013) annulled the entire section XIII of the Electronic Communication Act (hereinafter ECA) (Official Gazette RS, 96/09), whereby the then regime of storage and use of traffic data was blamed for not being necessary and, consequently, disproportionate for several reasons. Taking into account the said decision, a more tangible approach is proposed to obtain traffic data in pre-criminal or criminal proceedings. At the same time, the evidential standard for obtaining traffic data in order to comply with the constitutional principle of proportionality is lifted on justified grounds for suspicion (Supreme Court, 2018). The content of the previous measure of obtaining existing (already stored) traffic data with the so-called. ex tunc provisions (Ministry of Justice, 2018). There are also solutions for some problems that have been detected in practice. In exceptional (urgent) cases, an oral order of the investigating judge is permitted with an obligation of a subsequent written copy (Supreme Court, 2018=. For these exceptional (urgent) cases, an ex post system of supervision of this measure is prescribed by laying down the obligation to inform the person concerned about the information which has been transmitted to the police. For other cases, a clause is added which temporarily restricts the withdrawal from the general rules regarding the familiarisation with own personal data. At the same time, it is explicitly defined that the order may relate only to uniquely defined means of communication (the identification of a communication medium must be sufficiently precise to restrict the claim to a pre-defined and determinable list of persons) and that, pursuant to this Article, it is not possible to require data relating to the content of the communication, or that the acquired data can be used only in the case in which they are obtained. The new Article 149.c of the proposed act amending and supplementing CPA-N (Official Gazette RS, 22/2019). regulates the so-called ex nunc provisions, i.e. orders to start storing traffic data for each subscriber or user. As this is a forward-looking action, which means greater focus and, consequently, lower invasiveness compared to pre-nonselective storage, the catalog of criminal offenses is appropriately broadened, thus respecting the principle of proportionality. Such a way of obtaining traffic data could replace most of the deficits that the police would suffer due to the loss of access to stored traffic data under the previous article. Specifically, according to the available information of the proposer, a relatively large proportion of the proposals under the previous article 149.b deals primarily with the crimes of denial, theft and big theft for which this article may apply (Ministry of Justice, 2018). It should be emphasized in particular that, on the basis of this article, it is possible to do the so-called real-time tracking if technical conditions are given for this purpose, for the catalog criminal acts referred to in Article 149a or if the consent of the legal user is given. This last example covers statistically common situations in using this measure, such as theft or failure to use a mobile phone. With the proposed new Articles 150a and 150b of the proposed act amending and supplementing CPA-N (Official Gazette RS, 22/2019) , the conditions and procedure for the use of an IMSI catcher are defined. It is a special technical tool that can simulate certain functions of the base station of mobile telephony and in this way perform certain investigative actions on nearby mobile phones. Due to the difficulties in ensuring control over the legality of the implementation of the measure (in comparison with the existing control measures for communications that require the participation of the operator or service provider), the permissible uses of the catcher are limited to the identification of a particular mobile telephone connection, or to a more precise determination of the location of such a connection. Thus, the police will not be allowed to perform »eavesdropping from the air«, passive (deciphering existing traffic) and not active (i.e. man-in-the-middle attack), nor other advanced investigative actions. As a systemic safeguard against possible misuse or misapplication of this article, there are two measures provided. The Act predicts the possibility of an operator or an information service provider to forward information directly (in writing) to the competent court instead of the police or public prosecutor at its own expense. The investigating judge then performs a proper assessment and collects the collected data for the police or destroys them. If he destroys them, he shall make an official note thereof and forward it to the operator or service provider of the information service provider, the head of the district state prosecutor's office or the competent state prosecutor and the Ministry of the Interior and the Police, who have the opportunity to introduce the necessary (e.g. internal organizational) measures. The last system safeguard is ex post control, which is provided through the possibility of informing the person whose information was provided by the operator or the provider. The scope of the persons liable for the transmission of traffic data is extended from only the operators under the ECA-1 (Ministry of Justice, 2018)also to providers of other information society services (according to ECMA - Official Gazette RS, nr. 96/09). Given that practice has shown that the inability to test the decision of rejection made by an individual investigating judge (in terms of ordering undercover investigative measures) is blocking the development of case law and the clarity as well as the certainty of criteria in more borderline or sensitive cases.

Hearing of the suspect and witnesses by the state prosecutor or the police in the pre-trial procedure

According to Article 148a of the proposed act amending and supplementing CPA-N (Official Gazette *RS,* 22/201*)*, a suspect may also be interrogated without the presence of an advocate. A prerequisite for a »valid« hearing of a suspect without the presence of an advocate is that after the legal instruction he has waived the right to the presence of an advocate, and this is recorded in the audio and image recording of the hearing. On the one hand, audio and video recording acts preventively (in terms of possible abuse) and, on the other hand, it strengthens the quality and credibility of the evidence thus obtained, since the defense, the court and, finally, the public prosecutor, as a quasi judicial guarantor of the lawfulness of police tasks in pretrial procedure get the possibility of a more accurate and credible test and verification of the legality and correctness of the conduct of law enforcement and prosecution authorities. The sound and image recording medium of the hearing shall be attached to the record of the hearing. If the suspect does not have an advocate, and the hearing will not be recorded (according to the judgment of the interrogator), so the record will not have a procedural value in the proceedings. The possibility of hearing a witness before the state prosecutor or police is envisaged, and the court can base its decision on this type of test under certain conditions. Regarding who is the person who can do the hearing, the provisions governing the questioning of the suspect shall apply mutatis mutandis. The provisions governing the questioning of the suspect shall also apply mutatis mutandis as regards the acquisition of the sound carrier of the audio-visual recording of the hearing itself. The question whether the court will be able to base its decision on hearing a witness before the public prosecutor or the police depends largely on the witness himself who can refuse to have the hearing recorded (Ministry of Justice, 2018). Given the fact that it is a hearing of a witness before the state prosecutor or the police (and that during the hearing from the point of view of the suspect the contradiction is not guaranteed) and that the court can base its decision on such a confession under certain conditions, a somewhat broader legal instruction is foreseen: a person should be taught that the hearing is voluntary and that it will be recorded acoustically and impersonally, unless the person has explicitly opposed it.

House search with an emphasis on the search of the law firm

The Constitutional Court of the Republic of Slovenia (2013) has assessed the initiative of the Bar Association of Slovenia (hereinafter: BAS). In this case, questions were raised as to the extent to which the police had intervened in the confidentiality of the relationship between a lawyer and the client (in cases where the lawyer is not a perpetrator of the crime), as well as the possibility of a representative of the BAS to prevent the seizure of objects from being examined by the lawyer's office protect the rights of third parties, especially when seizing and investigating an electronic device. The Constitutional Court of the Republic of Slovenia (established the unconstitutionality of the two aforementioned laws with the Constitution (Ministry of Justice, 2018). The explanation states that the legal privacy protected by Articles 35, 36 and 37 of the Constitution (Official Gazette 33I/91-I, 42/97, 66/00, 24/03, 69/04, 68/06, 47/13 in 75/16) refers to facts, relationships, things, premises, data and communications that have a substantive relationship with the practice of a lawyer's profession. Through it, both the privacy of the lawyer and the privacy of his clients are protected and they are connected into an inseparable complex whole based on mutual trust and expectation of confidentiality which forms the core of the relationship between a lawyer and his client. The collection of confidential information related to the legal profession, which consists of lawyer privacy, is not only protected in law firms but everywhere the lawyer performs his business. Therefore, all such sites are protected within the spatial aspect of the lawyer's privacy. An admissible judgment is required for the admissibility of interventions; even if it is an interference with that part of the lawyer's privacy that is protected only by Article 35 of the Constitution, as this interference by the nature of things is so severe and intertwined with specific aspects of privacy. House investigation at a law firm, seizure of documents and objects and search of electronic devices interfere with the lawyer's privacy. Effective prevention, detection and prosecution of criminal offenses, or the introduction and the course of criminal proceedings are constitutionally permissible for the purpose of interfering with human rights and fundamental freedoms, as a rule also in the legal profession. However, the defendant's right to defense and the privilege against self-incrimination preclude the issuance of a court order for an investigative act by a lawyer who is the advocate of the person against whom the pre-trial or criminal proceedings are being conducted with regard to the information concerning the confidentiality of advocacy between a lawyer as an advocate and a charged person. If there is a constitutionally admissible target for interference with the lawyer's privacy, the interference with investigative acts is admissible if this is necessary for the initiation or conduct of criminal proceedings. An interference with the lawyer's privacy is necessary if it is evident from a court order that permits it why the information or data directly related to a precisely determined criminal procedure can only be obtained through the investigation of the lawyer's office and why other investigative actions to obtain them are not enough. In addition, the Constitution requires that, in the light of the urgency of the interference, any interference with the lawyers' privacy is limited to a sufficient degree. In a lawyer's office and other equally protected premises and on an electronic device of a lawyer, confidential information are concentrated which, according to the nature of the matter, needs to be regulated by a special way of investigating them in order to satisfy the constitutional requirement for the demonstrated necessity of intervention in each individual case. Therefore, according to the opinion of the Constitutional Court of the Republic of Slovenia (2013), the law should further regulate the mere implementation of an otherwise appropriately ordered interference with lawyer privacy. In order to limit interference with lawyer privacy to constitutionally admissible and urgent cases, two more lenient measures are taken into consideration: the presence of a lawyer and a representative of the BAS in the investigation activities of a lawyer and the possibility of a lawyer and a representative of the BAS to object to access to certain data or their seizure. However, the judge shall be obliged to have the final word on the admissibility of the interference and the judge shall make a final and neutral decision on this. The question of the investigation of the lawyer's office must also take into account the previous constitutional practice of the Constitutional Court (Ministry of justice, 2018). In the past, the European Court of Human Rights (hereinafter: ECtHR) has already made a statement on issues relating to the protection of the confidentiality of lawyer-client relationships and the investigation of the lawyer's office or the seizure and investigation of electronic devices. The ECtHR does not distinguish between the investigation of a lawyer's residence and his office; it is decisive whether there are objects, files or data in whatever form that the lawyer has been provided with. At the same time, the proceedings contain procedural safeguards during the investigation (the presence of the investigating judge, a representative of the state prosecutor's office and a representative of the Bar Association). The latter must have an active role in declaring the investigation and seizure itself and recording statement in regard to the investigation and the case dealt with (European Court of Human Rights, 2010, 2012). Following the experience from the practice, it is necessary to ensure the protection of the rights of the owner of an apartment or premises in the house investigation when the owner or his representative is unavailable. The arrangement of the house investigation shall be corrected in such a way as to protect the rights of the holder of the immovable property. In cases where the holder of property is not available, the court shall appoint an attorney from among the lawyers. In this way, indirect exclusion of the evidence obtained is prevented. However, it would be necessary to consider who can apply for a court order for a house or personal investigation, and whether, as in the case of undercover investigative measures, it would be necessary to provide for the transmission of an opinion to the Out-of-court Chamber in the event of a dispute with the investigating judge, disagreeing with a written petition for a home or personal investigation.

CONCLUSION

The proposed act amending and supplementing CPA-N (Official Gazette RS, nr. 22/201) takes into account the principle of effectiveness with adequate protection of the rights of defendants, victims and third parties. In this context, the proposer highlights, in particular, the proposed new undercover investigative measures (and the modified regulation of the conditions for the use of traffic data), as well as proposals regarding the improvement of the legal bases for the cooperation of competent authorities and speeding up of procedures. The principle of the rule of law or the principles of clarity and precision of legal regulations included in the aforementioned constitutional personal investigations are also taken into account. By completing the seizure of lawyer's articles, files and electronic devices, the intervention of competent authorities in the confidentiality of the relationship between a lawyer and a client is more appropriately regulated. The same holds true for other confidentiality relationships that are otherwise protected by the proposed act amending and supplementing CPA-N (*Official Ga-*

zette RS, nr. *22/2019.* The proposed regulation, which follows the practice of the ECtHR and the Constitutional Court of the Republic of Slovenia, regulates the issue systemically, thus taking into account other types of confidential communication. Following the experience from the practice, the proposed solution is the basis on which the protection of the rights of the owner of the apartment or premises in the house investigation is ensured (the latter can be either a suspect or a third person). Where the holder or his representative is unavailable, the court shall, ex officio, appoint an authorized representative from among the lawyers. The proposed solution indirectly prevents the exclusion of the evidence obtained. In addition, it is envisaged that the court will issue an order for a home or personal investigation based on a reasoned letter from the state prosecutor, who is otherwise responsible for law enforcement and police direction. In the same way as with the proposed change in the decision of the investigating judge in relation to undercover investigative measures, if the investigating judge fails to agree with the received letter of the public prosecutor for a home or personal investigation, the investigating judge shall forward the proposal and his reasoned request for review to the senate. The change in the hearing of the suspect is that it can be done without the presence of an advocate, except in cases of compulsory defense. The recording remains at the discretion of the interrogator, as is also the case with the proposed act amending and supplementing CPA-N. (Official Gazette RS, 22/2019*).* Amendments are also connected to modification of the arrangements for undercover investigative measures. The amending act also brings a new, more detailed and up-to-date regime for acquiring traffic and related data, thereby reducing interference with the protection of personal data. The amendment also improves the legal basis for the cooperation of competent authorities and speeding up of procedures in line with sectoral legislation, taking into account and respecting the rights of persons in the procedure, as well as ensuring security which is one of the main objectives of the criminal procedure.

REFERENCES

1. Act Amending the Criminal Procedure Act (CPA-N). *Official Gazette RS,* nr. *22/2019.*
2. Budapest Convention on the Contract for the Carriage of Goods by Inland Waterways (2015). *Official Journal of the European Union L 276/3.* Accessed on 12 May 2019 on https://eur-lex.europa.eu/legal content/SL/TXT/?uri=CELEX:22015A1021(01)
3. Constitution of the Republic of Slovenia. *Official Gazette* nr. 33I/91-I, 42/97, 66/00, 24/03, 69/04, 68/06, 47/13 in 75/16.
4. Constitutional Court of the Republic of Slovenija (June 3 2013). *Court decision nr. U-I-65/13-19.* Accessed 2 May 2019 on http://odlocitve.us-rs.si/sl/odlocitev/US30439

5. Constitutional Court of the Republic of Slovenija (Aopril 15 2010). *Court decision nr. Up-2530/06*. Accessed 2 May 2019 on http://odlocitve.us-rs.si/sl/odlocitev/US29112
6. Court of Justice od the European Union (April 8 2014). *Joined Cases C- 293/12 and C-594/12*. Accessed 2 May 2019 on https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293
7. Defence Act, *Official Gazette RS*, nr.95/15.
8. Electronic Commerce Market Act (ECMA-UPB2). *Official Gazette RS*, nr. 96/09.
9. European Court on Human Rights (January 21 2010). *Xavier Da Silveira v. Francija*, nr. 43757/05. Accessed 2 May 2019 on http://echr.ketse.com/doc/43757.05-en-20100121/
10. European Court on Human Rights (July 5 2012). *Golovan v. Ukrajina*, št. 41716/06. Accessed 2 May 2019 on https://www.philippe-derouin.com/en/expertise/litigation/golovan-ukraine-echr-of-5-july-2012/
11. Gorkič , P. (August 28 2014). Preservation and processing of traffic data for the purposes of criminal proceedings after the annulment of ECA- 1. *Legal Practice nr. 33/14*, page 6-10.
12. Ministry of Justice (2018). *Draft Act Amending the Criminal Procedure Act – N*. Accessed on December 5 2018 on http://www.mp.gov.si/fileadmin/mp.gov.si/pageuploads/Mandat_2018-2022/Zakonodaja/ZKP-N_20181026.pdf
13. Slovene Intelligence and Security Agency Act . *Official Gazette RS*, nr. 81
14. Supreme Court of the RS (February 2 2018). *Court Decision Kp 23071/2014*. Accessed on 12 May 2019 on http://www.sodnapraksa.si/?q=id:2015081111418603&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&_submit=i%C5%A1%C4%8Di&page=0&id=2015081111418603