Peer-reviewed academic journal

Innovative Issues and Approaches in Social Sciences

IIASS – VOL. 8, NO. 1, JANUARY 2015

Innovative Issues and Approaches in Social Sciences

IIASS is a double blind peer review academic journal published 3 times yearly (January, May, September) covering different social sciences: political science, sociology, economy, public administration, law, management, communication science, psychology and education.

IIASS has started as a SIdip – Slovenian Association for Innovative Political Science journal and is now being published in the name of CEOs d.o.o. by Zalozba Vega (publishing house).

Typeset
This journal was typeset in 11 pt. Arial, Italic, Bold, and Bold Italic; the headlines were typeset in 14 pt. Arial, Bold

Abstracting and Indexing services
COBISS, International Political Science Abstracts, CSA Worldwide Political Science Abstracts, CSA Sociological Abstracts, PAIS International, DOAJ.

Publication Data:
CEOs d.o.o.

Innovative issues and approaches in social sciences, 2015, vol. 8, no. 1

ISSN 1855-0541

Additional information: www.iiass.com

BORDERS OF COMMUNICATION PRIVACY IN SLOVENIAN CRIMINAL PROCEDURE – CONSTITUTIONAL CHALLENGES

Sabina Zgaga [1]

Abstract

Due to fast technological development and our constant communication protection of communication privacy in every aspect of our (legal) life has become more important than ever before. Regarding protection of privacy in criminal procedure special emphasis should be given to the regulation of privacy in Slovenian Constitution and its interpretation in the case law of the Constitutional Court. This paper presents the definition of privacy and communication privacy in Slovenian constitutional law and exposes the main issues of communication privacy that have been discussed in the case law of the Constitutional Court in the last twenty years. Thereby the paper tries to show the general trend in the case law of Constitutional Court regarding the protection of communication privacy and to expose certain unsolved issues and unanswered challenges. Slovenian constitutional regulation of communication privacy is very protective, considering the broad definition of privacy and the strict conditions for encroachment of communication privacy. The case law of Slovenian Constitutional Court has also shown such trend, with the possible exception of the recent decision on a dynamic IP address. The importance of this decision is however significant, since it could be applicable to all forms of communication via internet, the prevailing form of communication nowadays. Certain challenges still lay ahead, such as the current proposal for the amendment of Criminal Procedure Act-M, which includes the use of IMSI catchers and numerous unanswered issues regarding data retention after the decisive annulment of its partial legal basis by the Constitutional Court.

Key words: privacy, communication privacy, Constitution, criminal procedure, modern technology

DOI: http://dx.doi.org/10.12959/issn.1855-0541.IIASS-2015-no1-art12

[1] Sabina Zgaga, PhD Assistant Professor for Criminal Law, Faculty of Criminal Justice and Security, University of Maribor

Introduction

Due to technological development and our constant communication, communication privacy or better, its protection has become more important than ever before. Protection of communication privacy in criminal procedure is regulated also by Slovenian Constitution (1991, 1997, 2000, 2003, 2004, 2004, 2006 and 2013) and interpreted in the case law of Slovenian Constitutional Court. Due to constant technological development, Slovenian Constitutional Court had to adapt its case law on communication privacy. This influenced also the definition of privacy.

This paper therefore discusses the definition of privacy and communication privacy in Slovenian constitutional law and focuses on the main issues of communication privacy that have been exposed in the case law of Slovenian Constitutional Court in connection to criminal procedure in the last twenty years, such as the system regulation of undercover police measures, seizure and search of electronic devices, the monitoring of international communications, anonymity of a dynamic IP address, privacy of legal persons, privacy in other procedures and data retention. Thereby the paper tries to show a general trend in the case law of Constitutional Court regarding communication protection and to expose certain still unanswered questions and challenges for the future, for example the current proposal for the amendment of Criminal Procedure Act-M, which includes the use of IMSI catchers and numerous unanswered issues regarding data retention after the decisive annulment of its partial legal basis by the Constitutional Court.

Privacy in Slovenian Constitution and case law of the Constitutional Court

Slovenian Constitution, adopted in 1991, is very generous regarding the protection privacy and human rights in general. In comparison to other European states, as well as international and regional human rights protection mechanisms, which are often very general and seek the lowest common denominator between states signatories, Slovenian Constitution often guarantees a higher standard of human rights protection. As we will see, this applies also to the regulation of communication privacy. Furthermore, a safety clause exists in Slovenian Constitution, according to which no human right or fundamental freedom regulated by legal acts in force in Slovenia (including the international and regional human rights protection mechanisms) may be restricted on the grounds that Slovenian Constitution does not recognise that right or freedom or recognises it to a lesser extent. Meaning that in case certain right is regulated in international or regional convention on human rights

protection, such convention should be applied in Slovenia directly, notwithstanding the potential absence of its regulation in Slovenian Constitution.

Privacy is however regulated in a very broad manner already in Slovenian Constitution (1991, 1997, 2000, 2003, 2004, 2004, 2006 and 2013) in its articles 35 to 38. Article 35 generally guarantees the inviolability of the physical and mental integrity of every person, his privacy and personality rights. Territorial privacy or inviolability of dwellings is protected (art. 36), as well as communication privacy (art. 37) and the information privacy or personal data protection (art. 38) (Šturm et al., 2002).

What is privacy?

The Constitutional Court has interpreted the concept of privacy, provided for in the Constitution, in its case law and thereby decided, when to offer the constitutional protection of privacy and when not. The preliminary question therefore has always been, whether in certain case protection of privacy was applicable or not.[1] Of course, for making such decision, the definition of privacy is required.

First major decision of the Constitutional Court on communication privacy in criminal procedure was the decision on undercover police measures, especially eavesdropping and recording - U-I-25/95 (1997), which is still considered as one of the ground-breaking and landmark decisions of Slovenian Constitutional Court. In this decision privacy was understood as "the complexity of all more of less comprehensive actions, feelings, relationships and dealings of a person inside his or her living area, for which it is typical and constitutional that a person sustains it alone or together with his closest persons, with whom he or she shares intimate community, and that he lives there with the feeling of security from invasion of public or anyone unwanted."[2]

The Constitutional Court also referred to the established opinion of the European Court of Human Rights, according to which "the right to privacy means protection of individuals in his or her living space, protection from encroachments of a state or others into his or her private sphere, personality and dignity." (U-I-25/95, 1997: 38) Right to privacy is therefore firstly a human right of a negative status (Kavčič, Grad, 2007: 106), which means that the state should refrain from interfering into the private sphere.

1 See for example the cases Up-540/11 (2014) and Up-106/05 (2008).

2 See also the case Up-32/95 (1995).

And last, but not least, the Constitutional Court referred also to the well-established theory of *the reasonable expectation of privacy*, which originates in the case law of the American Supreme Court, and according to which privacy is awarded in places and situations, where an individual expects privacy *and* where such expectation is reasonable. Accordingly home is certainly such place, where one expects privacy and is such expectation reasonable. However, what an individual willingly exposes to the public, although in his or her home, is not protected by privacy. Contrary, what someone tries to keep private, even though in a publicly accessible place, could be constitutionally protected. Constitutional protection is therefore awarded only in cases, when an individual is situated in a space, where he or she reasonably expects to be alone (U-I-25/95, 1997: 38).

As presented in the following chapters, the Constitutional Court has held tightly to this definition of privacy in its future case law. In all privacy cases the Constitutional Court therefore as a rule firstly discussed the substance of the measure, which allegedly contradicts the constitutional protection of privacy, whether (considering its substance) the measure represents an encroachment of privacy and lastly, whether constitutional protection of privacy should be awarded in this concrete case at all. The latter has been answered by applying the reasonable expectation of privacy test. Only case of reasonable expectation of privacy, the constitutional protection of privacy has been awarded and consequently decided that the measure in question represents an encroachment of constitutional right to privacy. Only then a further decision was made, whether the constitutional conditions for such encroachment had been respected or not.

What is communication privacy?

As Slovenian Constitution regulates different forms of privacy, a further definition of communication privacy should be made. Communication privacy is explicitly protected and regulated by Slovenian Constitution. The title of article 37 of Slovenian Constitution sounds a bit old-fashioned for these days (even more so in Slovene language); privacy of correspondence and other means of communication (Slovene *tajnost pisem in drugih občil*). However, the time period and the technological development of time, when Slovenian Constitution was drafted (1991), should be taken into consideration. At that time we actually still sent letters and postcards, already fewer used stationary telephones or had one at home and very rarely computers were used. Rarely anyone communicated through internet and practically no one imagined internet chats, like google hangover or Facebook messenger.

The already mentioned technological development in communication devices and ways has posed many issues to law, including in criminal procedure. Perpetrators of criminal acts have been always one step ahead; using new communication devices and technologies, which has caused the law enforcement authorities to respond to it by using new powers for the investigation of criminal acts, not rarely without legal basis for,[1] which is necessary for any encroachment of constitutional rights (of privacy). The Constitutional Court had to follow this technological development as well, to protect individuals' privacy from its unconstitutional encroachments.

Despite its old-fashioned wording it has soon become clear that article 37 does not protect only communication via in 1991 existing letters, phone calls, etc. Article 37 of Slovenian Constitution protects all forms of indirect communication or communication via a communication device, notwithstanding its form, and includes any message with a subjective value (Šturm et al., 2002: 397). This has reflected also in the interpretation of the Constitutional Court, which awarded constitutional protection also to indirect communication via means of communication that did not exist in 1991, such as, data on SIM card, e-mails, file sharing in internet, etc.

Despite the fact that at the time of the drafting of article 37 of Slovenian Constitution its drafters only had scruples regarding the powers of law enforcement agencies in criminal procedure and intelligence services, based on the unpleasant experiences from the previous state (Cepec and Zgaga, 2012: 84), especially the latest years exposed certain other (legal) issues, namely regarding similar powers of other state authorities and bodies, which also encroach the constitutional right to communication privacy, such as the Slovenian Competition Protection Agency. This phenomenon has been (more or less successfully) addressed by the Slovenian Constitutional Court as well.

And last, but not least, it is also relevant, whether only data regarding the content of communication is protected or also the data regarding the traffic of communication (who, with whom, when, where, etc. communicated). Slovenian Constitution does not offer an explicit answer, but Slovenian Constitutional Court has offered one. Accordingly, communication privacy foremost protects the content of the message, communicated via communication devices. Constitutional protection however expands also to the circumstances and facts, connected to the

1 I am referring for example to the case Up-106/05 (2008) and also to the alleged use of IMSI catchers without current legal basis.

communication. Slovenian Constitutional Court thereby followed the case law of the European Court of Human rights[1] and stated that in connection to a phone call, all data on phone calls, which are an integral part of communication, is protected as well, such as the last made or missed phone calls (Up-106/05, 2008: 8; Up-540/11, 2014: 13). The simplest way to imagine, what such data includes, is to remind ourselves of the specification of the mobile phone invoice, issued by the mobile provider every month. In 2014 the Constitutional Court subsumed under the integral part of communication and thereby under communication privacy also the data about a dynamic IP address (Up-540/11, 2014: 13).

Contrary to a broad understanding of means and content of communication under constitutional protection, the conditions for suspension of communication privacy are very strict, also in European perspective. Namely, only a law may prescribe that on the basis of a court order the protection of the privacy of correspondence and other means of communication and the inviolability of personal privacy be suspended for a set time where such is necessary for the institution or course of criminal proceedings or for reasons of national security.

Especially strict is the cumulative application of court order and necessity for criminal procedure or national security. The condition of a court order has made difficulties for the police in cases, when they could not have obtained one and they have tried to execute certain measures nevertheless. The condition of necessity for criminal procedure or national security on the other hand has caused certain controversies regarding the powers of state authorities, other than police, that have powers, which encroach communication privacy, but are not performed for the reasons of criminal procedure or national security.

Issues of communication privacy in the case law of the Constitutional Court

System regulation of undercover police measures

Soon after the independence, Slovenian Constitutional Court adopted three major decisions regarding (communication) privacy in criminal procedure. All three decisions were connected to undercover police measures in criminal procedures. These measures were after the independence regulated in two set of legislation; police and criminal. Accordingly, the Internal Affairs Act (1980, 1988, 1989, 1990, 1991, 1992, 1993, 1997) and subsequently the Police Act (2009, 2010, 2011, 2012, 2013) regulated secret surveillance with the use of technical

1 See for example the case Malone v. the United Kingdom, No. 8691/79, 2 August 1984.

devices for recording, undercover operations and feigned documents and identification marks, whereas the others were regulated in the Criminal Procedure Act (CPA, 2012, 2013). All the mentioned legal acts were therefore assessed by the Constitutional Court and declared partially unconstitutional. They all dealt with similar system constitutional issues (U-I-25/95, 1997).

Interestingly, the Constitutional Court distinctly decided that the regulation and application of undercover police measures, specifically eavesdropping and recording and feigned purchase, feigned acceptance or giving of gifts or feigned acceptance or giving of bribes, does not *a priori* violate the Constitution, because such measures are necessary even in a democratic society, however they should be regulated in law in a constitutional manner and applied accordingly (U-I-25/95, 1997; U-I-272/98, 2003; U-I-158/95, 1998).

One of the reasons, why the former regulation was in contradiction to the Constitution, was the breach of the general constitutional principle of proportionality. Namely, the standard of proof, required for allowing such measures, was only grounds for suspicion, the lowest possible according to the criminal procedure legislation, whereas the Constitutional Court demanded a higher standard, closer to reasonable suspicion, analogous to American standard of probable cause, which should be based on concrete, specific, precedent and articulated facts (U-I-25/95, 1997; U-I-272/98, 2003; U-I-158/95, 1998) due to high invasiveness of the measures. Second problem regarding the proportionality principle was the (too) broad list of criminal acts, for which such measures were allowed (U-I-25/95, 1997; U-I-272/98, 2003; U-I-158/95, 1998). One of the major problems was also the indefiniteness of the legislation; the definitions, preconditions and procedural issues were namely regulated in a very vague and indefinite manner (*lex incerta*), which contradicted the principle of legality. One of the elements of the principle of legality and rule of law is namely also the *lex certa;* the requirement that the legislation is clear and definite (U-I-25/95, 1997; U-I-272/98, 2003; U-I-158/95, 1998). These were few of the main reasons for unconstitutionality of former legislation and based on the intervention of the Constitutional Court, all undercover police measures have now been regulated in a comprehensive and very detailed manner in CPA only.

Seizure and search of electronic device

Another legal issue arose, when the data acquired by police in criminal procedure, was not the content of the communication, but "only" data regarding the circumstances of communication.

In case Up-106/05 (2008) the police therefore seized the suspect's mobile phone and SIM card and thereby acquired the list of phone numbers and the mobile phone's memory, which were all used as evidence against the suspect. The constitutional problem at hand was that the police had no explicit legal basis for acquiring the data regarding the circumstances of communication and the Constitutional Court had to decide, whether the data only on the circumstances of the communication is also constitutionally protected by communication privacy or not.

The police claimed that seizure and search of the mobile phone and SIM card could be understood as the power of seizing the objects, which may prove to be evidence in criminal proceedings, on the basis of article 220 of the CPA (Up-106/05, 2008: 2).

However, the Constitutional Court set a pretty high standard. It made a distinction between the physical seizure of a mobile phone and a SIM card, for which the police had legal basis in CPA and which represents encroachment of the right to private property on one hand and search of mobile phone and SIM card, which produces data about circumstances of communication (who called whom, when, where, etc.) and which encroaches communication privacy on the other hand (Up-106/05, 2008: 6). Secondly, as mentioned before, the Constitutional Court broadened the definition of communication privacy and its constitutional protection to "protection of all individual's interest that without his authorisation no one learns the content of the message, sent via any means of communication, which enables exchange of information, and the individual's interest to freely decide, to whom, to which extent and under which conditions he would sent a certain communication. It is about protection of free and uncontrolled communication and privacy of relationships, of which the individual is a part of while communicating." (Up-106/05, 2008: 7) Furthermore, communication privacy does not protect only data on the content of communication, but also circumstances and facts in relation to the communication – in fact any data on communication, which is integral part of communication (including the data on the last performed and unanswered calls and the content of SMSs) (Up-106/05, 2008: 8). Later on, this data was referred to as "traffic data" (Up-540/11, 2014: 13). Such interpretation obviously enormously broadened the scope of constitutional protection of

communication privacy. Since in this case the measure was not authorised by a court order and had no legal basis, it was performed in unconstitutional measure and the evidence was obtained in violation of human rights and basic freedoms provided by the Constitution (Up-106/05, 2008: 10).

It is also worth mentioning that the Supreme Court of Slovenia dealt with a similar case one year before. In that case the police acquired data from the mobile provider regarding the calls made from and to the suspect's phone. Again, the police referred to article 143[1] of the CPA as the legal basis for this measure, however the Supreme Court decided that the acquisition of traffic data represents a violation of communication privacy and represented grounds for compensation, because it was performed without legal basis and court order (II Ips 474/2005, 2007).

IP address anonymity

A more recent case at the Constitutional Court has dealt with the identification of the user of a dynamic IP address. As internet has become more and more integrated in our lives, the perpetrators have also been using it for criminal purposes, in this case for sharing child pornography, and the data regarding internet communication has become relevant also for criminal procedure.

In case Up-540/11 (2014) the Constitutional Court therefore discussed the privacy of internet communication. The Swiss police namely performed a systematic sweep of all users of the Razorback network, who exchanged files via E-mule, including child pornography, and thereby discovered, which dynamic IP addresses share child-pornography over E-mule. The Slovenian dynamic IP address was delivered to Slovenian police, which obtained the information on the identity of the user of such dynamic IP address from the internet provider without court order, performed house search based on a court order, seized and searched computer hard drive - again without a special court order, and found child pornography (Up-540/11, 2014: 2).

The Constitutional Court took in my opinion a very strict approach and decided upon all three major issues in a negative manner. Regarding the issue, whether the acquisition of a dynamic IP address, which had

1 Article 143 of the CPA: »The personal data controller must submit to the court, at its request and free of charge, the personal data from the filing system also without a personal consent of the individual whom the data refer to if the court states that the data are required for conducting a criminal procedure.«

shared child pornography, by the Swiss police without court order violates article 37 of Slovenian Constitution, the Constitutional Court decided that identification of a dynamic IP address is traffic data and thereby potentially protected by article 37 of Slovenian Constitution (Up-540/11, 2014: 13), but also that there was no reasonable expectation of privacy. The defendant probably expected privacy of the content of his communication while using E-mule to exchange files with other Razorback network members due to general internet anonymity, but such expectation was not reasonable, since his IP address was not covered up in any way or anonymised. Contrary to that it was visible to anyone in this network and the access to the Razorback network was not limited to anyone via passwords or other tools. Therefore, anyone who was interested, could access the files, the communication in question was open with an unidentified range of unknown internet users, who are interested in such files on the other side - like in case of a notice board. Consequently, there is no reasonable expectation of privacy of the content of the communication and identification of the dynamic IP address (Up-540/11, 2014: 14-22). The Swiss police therefore did not need a court order for the identification of the IP address.

This decision was not adopted unanimously. Two of the judges namely contradicted with separate opinions, emphasising especially that even though the individual gave up the privacy of the content of his communication he did not give up the privacy of his identity, emphasising also the fact that by such decision we lost privacy of all electronic communication over internet, since the police could always identify us (Up-540/11, dissenting opinions of Jadek Pensa, Sovdat, 2014). This decision also means, for example, that the police could perform random sweeps of certain internet sites and identify the IP addresses, which use certain site, etc. This applies to all sites that are not encrypted with password or any other way.

I agree with the dissenting opinions. Based on such decision, someone, who is smarter and uses encrypted communication channels, is awarded protection of privacy, whereas someone who does not use such protection due to various reasons, is not protected. Further, it is true that thereby we in fact lost the anonymity and privacy of the whole type of communication – internet communication. Namely, unencrypted communication with the use of nicknames is the typical for our participation in internet, although we live in a (false) idea, that we are anonymous behind our nickname. Not anymore, if the anonymity of our participation in internet is not protected in any way.

Based on this conclusion the Constitutional Court similarly discussed the reproaches regarding the identification of the user of the dynamic IP address. The user namely renounced his privacy protection and reasonable expectation of privacy by publicly disclosing his IP address and content of communication. His identity could therefore be disclosed without court order, since it was not constitutionally protected (Up-540/11, 2014: 18). And last, but not least, regarding the potential violation of article 37 due to the seizure and search of files on computer's hard drive the court concluded that there indeed was no special court order for the seizure and search of hard drive, however it was allowed in the court order for house search (Up-540/11, 2014: 21).

Monitoring of international communications systems[1]

Another sensitive issue in Slovenia is the monitoring of international communications systems. To this question however the Constitutional Court still avoids giving a clear answer. This power has been given to the Slovenian Intelligence and Security Agency and represents a strategic surveillance of communication on the basis of search parameters, which should not involve identification marks that would enable surveillance of communication of a certain telecommunication connection or person in Slovenia (Britovšek, 2008). The Slovenian Intelligence and Security Agency Act (2006) also clearly prohibits monitoring of a determinable telecommunication connection or a specific user of such a connection in the territory of the Republic of Slovenia (Slovenian Intelligence and Security Agency Act, 2006).

The Constitutional Court in U-I-45/08 (2009) formally rejected the request of the Information Commissioner for the review of the constitutionality of the Agency's power to monitoring international communications systems from the viewpoint of communication privacy and protection of personal data, especially due to the lack of court order, disproportionality and indefiniteness (*lex incerta*) of the measure. The Constitutional Court rejected this request due to the lack of the procedural condition of the Information Commissioner (U-I-45/08, 2009). A similar formal decision was reached in case U-I-216/07 (2007), which was initiated by the Supreme Court of Slovenia – again due to the lack of a procedural condition. Namely, the President of the Supreme Court has only jurisdiction to authorise eavesdropping and recording and not monitoring international communication systems. Thereby, he or she cannot challenge the monitoring international communication systems (U-I-216/07, 2007).

[1] See also Zgaga, 2014.

Despite ascetically formal decisions, the Constitutional Court made certain partial substantive observations. Thus, it used the territorial theory of protection of constitutional rights, and (wrongly) concluded that monitoring the international communication systems obviously involves only the territory outside of the Republic of Slovenia (U-I-216/07, 2007; Britovšek, 2008), because it could only include the surveillance of communication between two or more foreign[1] telecommunication connections (U-I-45/08, 2009), and that consequently Article 37 of the Constitution, including the request for a court order, would only then be relevant, in the event this measure could be executed also in the territory of Slovenia and when performed against a specific person in Slovenia (U-I-216/07, 2007). Therefore, when the monitoring international communication systems is performed in Slovenia, it falls under the governance of Article 37 of the Constitution.

It is necessary to perform a generally established constitutional test in the event that the privacy of communicating in international communication channels is reasonably be expected (Britovšek, 2008). In my opinion and in line with the above-mentioned case law, in which the Constitutional Court defined communication privacy in a broad manner (U-I-25/95, 1997), the Constitutional Court could only adopt a conclusion that there is reasonable expectation of privacy in such case. Once such decision is made, the safeguards of Article 37 are implemented automatically. Yet, lower standards can be taken into account on the basis of the constitutional condition of the necessity of suspension of privacy for the reasons of national security. Therefore, the principle of proportionality, embodied in this necessity condition, should therefore allow for less strict standards of proof and other conditions, but should not allow the exclusion court order for authorising such measure.[2] I also agree with the former Commissioner Nataša Pirc Musar (Pirc Musar, 2014) that is high time for the Constitutional Court to issue a substantive decision on monitoring of international communication systems.

The privacy of legal persons

Another controversy, which Slovenian Constitutional Court had to find answer to, was the issue, who could be the holder of the constitutional right to communication privacy; only natural persons or also legal persons. This issue arose in case U-I-40/12-31 (2013), where it was discussed, whether the power of the Slovenian Competition Protection Agency to examine the books, contracts, papers, business correspondence, business records and other information relating to the

1 Although the issue remains unanswered, what is actually foreign telecommunications connection.

2 In such manner the Constitutional Court in Up-1293/08 (2011) and U-I-40/12-31 (2013).

business of the investigated undertaking, irrespective of their medium (Prevention of Restriction of Competition Act-1, 2008, 2009, 2011, 2012, 2013 and 2014: 29) violates article 37 of Slovenian Constitution in relation to legal persons. Namely, the investigated undertakings are mostly legal persons (Prevention of Restriction of Competition Act-1, 2008, 2009, 2011, 2012, 2013 and 2014: 3).[1]

Before issuing the final decision, the Constitutional Court had to make certain partial decision. Accordingly, it was decided that legal persons could be holders of (constitutional) rights, but only of those rights, which could be awarded to legal persons - considering the nature and content of such rights (U-I-40/12-31, 2013: 17). Furthermore, the privacy of a legal person could also be constitutionally protected. However, the level of protection is lower than with natural persons, since legal persons are artificially formed and their privacy is constitutionally protected only in order to indirectly protect the natural persons "behind" the legal person (U-I-40/12-31, 2013: 20). And last but not least, legal persons could also have communication privacy according to the article 37 of Slovenian Constitution. Consequently, when encroaching the communication privacy of legal persons, conditions from article 37 should be respected, including the court order and the necessity for criminal procedure (U-I-40/12-31, 2013: 38). The court's decision on the latter was in my opinion a bit controversial and dubious, since the Constitution clearly uses the term criminal and not the broader term punitive procedure and the Slovenian Competition Protection Agency is not authorised to conduct criminal, but only misdemeanour procedure.[2] However the Constitutional Court concluded that except the court order, all constitutional conditions from article 37 are fulfilled in case of the agency's powers.

Privacy in other legal procedures and the influence on criminal procedure

It is not unusual in criminal procedure that evidence that has been gathered in other, non-criminal procedures. This enhances the efficiency of the procedures, but simultaneously introduces a problem, since non-criminal procedures are usually satisfied with a lower threshold for initiating the procedure and for the execution of relevant measures due to efficiency reasons. They thereby represent fruitful grounds for bypassing the higher constitutional and legal safeguards of criminal procedure for obtaining evidence (Zgaga, 2014), including in regard to the protection of privacy.

1 Although this could also be interpreted as the issue of the employees' privacy.

2 See Cepec and Zgaga, 2012.

The evidence from non-criminal procedures could be used in criminal procedure, but under certain conditions (Zgaga, 2014). Hence, the real issue is related to the question of what these conditions are. As the most constitutionally conformed and also efficient solution a compromise position has been developed, according to which the conditions of the *lex specialis* legislation must be fulfilled, as well as constitutional conditions for the infringement of the relevant constitutional right (Zgaga, 2014; Selinšek, 2010). The common denominator for using evidence, obtained in non-criminal procedures by encroaching privacy, is therefore the respect of constitutional conditions, notwithstanding the form of legal procedure. It is therefore again essential to assess the substance, nature and degree of the invasion of a concrete measure, which constitutional right it thereby encroaches and what the constitutional limitations to this encroachment are and in our case that the measure is performed according to the constitutional limits of the constitutional right of privacy (Up-1293/08, 2011).

Slovenian Constitutional Court has dealt with the issue of obtaining evidence via encroachment of privacy in non-criminal procedures and their subsequent use in criminal procedure in two major decisions. The first Up-1293/08 (2011) dealt with the power of the Custom Service to search the vehicle at the border. The evidence was ruled admissible, however the court also gave a clear instruction that constitutional rights (including to communication privacy) do not apply only in the formal criminal procedure, but from the moment of the *de facto* beginning of the criminal procedure and from the focus of investigation on a single suspect. Further, they be applied also in (non)criminal procedures, in which criminal investigation is run under the pretences of other (inspection or supervisory) procedures and in which officials actually focus on the collecting of evidence for subsequent criminal procedures (Up-1293/08, 2011).

The second case, which was already mentioned, (U-I-40/12-31) deals with the powers of the Slovenian Competition Protection Agency. The Constitutional Court assessed the agency's power to inspect business communication and stated that a court order is necessary in order to prevent abuses and discrimination. Hence it is no doubt that in every case an assessment should be made considering the substance, nature and invasiveness of a certain measure (U-I-40/12-31, 2013) and regarding the constitutionality of the measure, no matter what kind of procedure we are dealing with. Consequently, the measure is lawfully executed and evidence admissible, also in criminal procedure.

Data retention

The most recent decision of the Constitutional Court regarding privacy was U-I-65/13-19 (2014) on data retention. Data retention is a necessary prerequisite for the police to be able to perform certain undercover police measures, such as metering (acquiring traffic data), eavesdropping and recording, etc. Data retention has been regulated in Slovenia by the Electronic Communications Act-1 (2012, 2013 and 2014), which represents the implementation of the Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (2006) into Slovenian law.

The Information Commissioner of Slovenia started a procedure at the Constitutional Court to assess the data retention regulation in the Electronic Communications Act-1, especially regarding its disproportional encroachment of communication privacy. Since the act represents the implementation of the EU legislation and since there was already a procedure regarding the proportionality of the data retention directive at the European Court of Justice, Slovenian Constitutional Court stayed its procedure. After the European Court of Justice ruled the data retention directive invalid *ab initio*, the Slovenian Constitutional Court also issued its decision (U-I-65/13-19, 2014).

The Electronic Communications Act-1 (2012, 2013 and 2014) allowed the providers to storage listed traffic data of all persons for 14 or 8 months. Due to the disproportionality of the measure, more exactly due to the preventive and unselective storage of data and unsubstantiated time period of the storage of data, the Constitutional Court ruled the whole chapter XIII of the Electronic Communications Act-1 on the storage of data invalid. Furthermore, all data that has been stored on the basis of article 163/I of the Electronic Communications Act-1 (2012, 2013 and 2014)[1] must have been destroyed immediately after the publication of the court's judgment in the Official Gazette (U-I-65/13-19, 2014). Especially the last part of the court's decision seems very human rights protective and radical. However, the fact is that Slovenian Constitutional Court pretty much had no other choice after the decision of the European Court of Justice.

1 But not also others.

Conclusions

The regulation of communication privacy in Slovenian Constitution is very protective, especially considering the broad definition of the concept of privacy, developed in the case law of the Constitutional Court, the addressees of article 37 of the Constitution (legal and natural persons, private and public sector) and considering the very strict conditions for encroachment of communication privacy.

The same applies to the case law of the Constitutional Court. However the recent decision on a dynamic IP address might unfortunately show a significant turn in constitutional case law. Namely, this decision is very widely applicable to a form of communication (internet), which is used very frequently nowadays. It is the prevailing form of communication and by such decision we actually lost the anonymity of our internet communication, unless in cases, when we clearly show with our actions that we want to keep our identity and communication concealed (passwords, encrypting, etc.). Even though - in my opinion at least – the essence of nature of internet participation lies in its anonymity.

Certain challenges still lay ahead. The legislator is namely trying to amend the CPA with the proposal for CPA-M, which includes also the legal basis for using the IMSI catchers for identifying a mobile device in order to be able to execute eaves dropping on it later. This measure could be constitutionally problematic due to its disproportionality; the extent of an IMSI catcher's operation is namely limited only by the number of mobile devices active in its range at a given time. It therefore "catches" all mobile devices inside its range. The problem is (as with data retention) the collateral damage of communication privacy invasions.

Speaking of data retention, numerous open issues arose after the decisive annulment of the Electronic Communications Act-1, for example what data could still be stored on the basis of the Electronic Communications Act-1, what should happen with the data already imported into criminal procedure, how should the new regulation of data retention, considering the principle of proportionality, look like, etc.[1] It is no doubt that partial data retention is necessary for effective prosecution of serious forms of crime, however the principle of proportionality and the interpretation of the Constitutional Court should be taken into consideration while drafting the new legislation. Until the new legislation is adopted, the police are more or less paralysed, when they need the recent traffic data.

1 See Gorkič, 2014.

Generally speaking, (criminal) legislation is always a step behind the technology development and human imagination and thereby very sensitive to technological development, however this is even more true for communication privacy, since forms and modes of communication (devices) change daily. Therefore, a special precaution should be given by the legislator that the legislation is general enough in regard to technical terms, to cover all currently available forms of communication and devices, and at the same time still keeping in mind the principle of legality.

References

Britovšek, P. (2008). Spremljanje mednarodnih sistemov zvez kot domnevni poseg v komunikacijsko zasebnost posameznika v povezavi s teritorialnim principom varovanja te pravice. Available at http://www.fvv.uni-mb.si/dv2008/zbornik/clanki/BritovsekP.pdf (1 October 2014).

Cepec, Jaka & Zgaga, Sabina (2012): Constitutional right to the privacy of correspondence and other means of communication as a potential obstacle to enforcement of EU and national Antitrust Law in Slovenia. In: A. Gerbrandy & W.-J. Berends (Eds.): Removing obstacles: a mutual learning experience towards good practices in competition law enforcement. The Hague: Eleven International Publishing (pp. 83-104).

Constitution of Republic of Slovenia, Official Gazette of Republic of Slovenia, 33/91-I, 42/97, 66/00, 24/03, 69/04, 69/04, 69/04, 68/06, 47/13 and 47/13.

Constitutional Court (1995): Up-32/95.

Constitutional Court (1997): U-I-25/95.

Constitutional Court (1998): U-I-158/95.

Constitutional Court (2003): U-I-272/98.

Constitutional Court (2007): U-I-216/07.

Constitutional Court (2008): Up-106/05.

Constitutional Court (2009): U-I-45/08.

Constitutional Court (2011): Up-1293/08.

Constitutional Court (2013): U-I-40/12-31.

Constitutional Court (2014): U-I-65/13-19.

Constitutional Court (2014): Up-540/11.

Criminal Procedure Act, Official Gazette of Republic of Slovenia, 32/12 and 47/13.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and

amending Directive 2002/58/EC, Official Gazette of European Union, 2006 L 105.

Electronic Communications Act-1, Official Gazette of Republic of Slovenia, 109/12, 110/13, 40/14 and 54/14.

Gorkič, Primož (2014): Hramba in obdelovanje prometnih podatkov za namene kazenskega postopka po razveljavitvi ZEKom-1. Pravna praksa, Vol.: 33, No.: 33, pp.: 6-10.

Internal Affairs Act, Official Gazette of Republic of Slovenia, 28/80, 38/88, 27/89, 8/90, 19/91, 4/92, 58/93, 87/97, 87/97 and 49/98.

Kavčič, Igor & Grad, Franci (2007): Ustavna ureditev Slovenije. Ljubljana: Gospodarski vestnik.

Malone v. the United Kingdom, No. 8691/79, 2 August 1984.

Pirc Musar, Nataša (2014): Po desetih letih dela ponosno zapuščam mesto informacijske pooblaščenke. Pravna praksa. Vol.: 33, No.: 28, p. 3.

Police Act, Official Gazette of Republic of Slovenia, 66/09, 22/10, 26/11, 58/11, 40/12, 96/12, 15/13 and 15/13.

Prevention of Restriction of Competition Act-1, Official Gazette of Republic of Slovenia, 36/08, 40/09, 26/11, 87/11, 57/12, 39/13, 63/13 and 33/14.

Slovenian Intelligence and Security Agency Act, Official Gazette of Republic of Slovenia, 81/06.

Šturm, Lovro et al. (2002): Komentar Ustave Republike Slovenije. Kranj: Fakulteta za državne in evropske študije.

Supreme Court (2007): II Ips 474/2005.

Zgaga, Sabina (2014): The use of intelligence data in law enforcement and judicial processes: constitutional aspects. In: D. Čaleta & P. Shemella (Eds.): Intelligence and combating terrorism: new paradigm and future challenges. Ljubljana: Institute for Corporative Security Studies; Monterey: Center for Civil-Military Relations, Naval Postgraduate School (pp. 185-200).