Nóra Magyar – Bojána Tankó – Gergely Kozma

Trainees of the Hungarian Prosecution Service

Consultant: Zoltán Péter

Public Prosecutor

CROSS-BORDER INTERCEPTION

§

Themis Competition VII.

2012

Table of contents

I. Introduction

The emergence of the European Union has given rise to numerous economic and social benefits for the Member States (hereafter: MS). The measures taken by the European Union not only established the economic union through the single market and created a new currency, but they have also intended to raise living standards and create stability within the EU. As a result of the development of the internal market, EU citizens may trade, move, work and travel freely throughout the Union.

Besides its positive impacts this European integration unfortunately produced some negative effects. We have to bear in mind that globalization offers great prospects and new possibilities not only for law-abiding citizens, but for criminals as well. Liberalization also applies to offenders who by profiting from this deregulation may easily commit crimes with cross-border dimension.

Undeniably, MS deciding on the abolition of border controls made a big step towards integration. Nevertheless, besides its enormous advantages, these measures generated new forms of (trans-border) crimes. To fight effectively and efficiently this new type of criminality, judicial and law-enforcement authorities are obliged to use more and more specialized and sophisticated investigative techniques.

Our study will attempt to analyse (cross-border) interception as one of these specific forms of investigative techniques. This investigative measure facilitates tracking and gaining information directly from perpetrators. In the legal literature one can find different types of definitions concerning the interception of telecommunications. According to one of the most accurate ones, interception "*is the monitoring and scrutiny of private messages between individuals or organisations*."[1]

This essay will present an analysis on the existing EU, international and national regulations and practical difficulties in connection with interception of telecommunications carried out during criminal investigations. One of our aims is to provide a brief overview – with the help of a case study - on the existing legal problems. In addition, we would like to present the

[1] Briefing on the Interception Modernisation Programme, The London School of Econimics and Political Science http://www.lse.ac.uk/collections/informationSystems/research/policyEngagement/IMP_Briefing.pdf

technical aspects and difficulties of the interception as well. Our final goal is to find solutions to the legal loopholes and make proposals for a better legal environment.

II. Interception

II.1. General introduction and related issues

The question how to intercept telecommunication exists since the birth of telecommunication in 1844, when Samuel Morse sent his famous telegraph message "What hath God wrought?" from Washington to Baltimore for the first time.[2]

Telecommunication wormed itself very quickly into everyday lives, and parallel to that the need to intercept private conversations became more important for States. The most widely known type of interception is when legally authorized bodies listen/record conversations through phone lines and cell phones. Let us mention that the first noted interception took place in 1867, in the telegraphic era. Phone intercepting (wiretapping) started in the 1950s; digital network interceptions began in the 1990s.[3] Currently, however, interception of telecommunications covers not only wiretapping but letter opening, postal pocket examination, e-mail tracking, Skype listening, and data capturing as well.

Interception via recording conversations and data through phone lines and internet communication could facilitate detecting different types of crimes, sometimes with cross-border aspects. It is undoubtedly one of the most efficient ways to combat criminality. Intercept as evidence, because of its authentic, direct, accurate and complete nature, can be used very efficiently in judicial proceedings. Even opposers of this method admit that in criminal procedures interception of private conversations play an influential role on judgments, furthermore, recorded conversations provide better understanding on the intention and thoughts of perpetrators at the time of the commission of crime. Even criminals feel defenceless when they are confronted with the intercept materials of their private communication. Finally, law enforcement authorities and prosecutors find themselves in a

[2] History of the Morse Telegraph http://www.radioelectronics.com/info/radio_history/morse/morseteleghstry.php

[3] Technical aspects of Lawful Interception ITU-T Technology Watch Briefing Report Series, No. 6 (May 2008, updated July 2008)

better and more comfortable position when they bring a criminal case with intercept materials before the court.

Besides its undisputable benefits in the criminal procedure, interception of telecommunications raises serious questions of privacy and human rights. No matter what kind of interception of telecommunications we are talking about, proportionality issue has to be taken into account. In a democratic society governed by the rule of law, the legal framework of lawful interception should be clearly regulated. The question of balance between the interference of privacy and the national and public interest in the fight against criminality should be settled.

II.2. In the EU

II.2.1. Differences in the regulations

In the EU, each Member State had a different approach towards these questions. Unsurprisingly, the adopted legal tools differ in many ways; however, there are some similarities as well.

Since the length of this study does not allow to give a comprehensive analysis on the different legal systems, we only intend to indicate some key points very briefly.

Rules concerning the interception of telecommunication are generally incorporated into criminal procedure codes; nevertheless in some countries such provisions are regulated by separate acts.

Differences are more visible if one takes a look at the details: the initiation of proceedings, the duration of the interception, guarantees, data protection issues…etc.

The duration of the interception alters from state to state; there are examples for intervals of 4 weeks, 1 month, 3 months or 180 days…etc.

With regard to the principle of proportionality, the aim is to carry out the monitoring and recording phase within the shortest time possible, although the option to extend the duration of the interception is provided.

In need of urgent decisions, national rules generally allow authorities to carry out interceptions without any delay, upon the authorization of the prosecutor or high

commissioner of the police forces. In these cases the competent judge or higher competent authority should be informed without delay.

Interception can usually be used only for certain types of crimes. In some countries there is a list of crimes when the interception as an investigative measure can be applied, nevertheless in most cases the punishability of the crime determines the possibility of the eventual use of this investigative measure.

In most EU countries, intercept materials can be easily used as evidence in court proceedings; however, there are countries where the intercept is/was intended to support only investigators, but is/was not admissible before courts.

Competent authorities to authorize interception of telecommunication tools differ from State to State. The authorization usually has to be drafted in details e.g. with exact telephone numbers, locations, persons, period of time.

II.2.2. Need for a comprehensive regulation

Despite these differences, it has to be pointed out that due to the jurisprudence of the European Court of Human Rights the legal framework of interceptions is more and more similar in MS.

Moreover, national regulations have to comply with cornerstones laid down in international treaties. There are a lot of international conventions that deal with privacy issues. The European Convention on Human Rights (4 November 1950 Rome), for example, sets forth that: „Everyone has the right to respect for his private and family life, his home and his correspondence."[4]

Via its decisions the European Court of Human Rights plays an active role in safeguarding privacy interests and enforcing the basic principles in this field.

In the case of Valenzuela Contreras v. Spain[5], for example, the Court stated that "the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances

[4] Article 8 paragraph 1 European Convention on Human Rights
http://www.hrcr.org/docs/Eur_Convention/euroconv3.html

[5]Valenzuela Contreras v. Spain (58/1997/842/1048)
http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=valenzuela&sessionid=91849167&skin=hudoc-en

in and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference (wiretapping) with the right to respect for private life and correspondence".[6]

Not only European legal developments in the fields of human rights present a challenge for policy makers and magistrates in the field of interception but also the technical explosions in the area of telecommunication do so.

In the field of legislation, in order to detect crimes better and prosecute criminals more efficiently, it would be necessary to keep up with these fast emerging telecommunication techniques that are used widely by perpetrators.

Legislation is usually far behind the technical features, which makes the tasks of law enforcement and judicial authorities more and more difficult.

It is obvious that regulation of interception is mainly a national issue. Nevertheless, due to the free movement of people and quick technical development, competent authorities often realize that the intercepted persons use their phones and other technical gadgets abroad.

In the beginning, interception on the territory of different Member State could be carried out solely with the technical help of the concerned Member State.

II.2.3. 2000 MLA Convention

International co-operation in this field has existed for a while; however, due to the absence of legal framework, this special investigative technique has been rarely used in cross-border dimension.

Co-operations have been carried out mainly on a case-by-case basis, and it has remained the exclusive competence of the MS whether to provide assistance or not.

Initially cross-border interception was requested on the basis of the European Convention on Mutual Legal Assistance in Criminal Matters of 1959. According to Article 1[7] of this Convention contracting parties afford each other the widest measure of mutual assistance.

[6]Valenzuela Contreras v. Spain judgement, summary, paragraph 60

As a result of the technical developments, nowadays MS are able to carry out interception of telecommunications on the territory of other Member State without the technical assistance of the latter one.

European policy makers realized the lack of relevant provisions and the need to create clear and transparent rules in this field.

The Convention on Mutual Legal Assistance in Criminal Matters between Member States of the EU was adopted in 2000 (hereafter: 2000 MLA Convention).

As 2000 MLA Convention was the first multilateral agreement dealing with international interception of telecommunications, it contains the most detailed regulation of interception of telecommunications involving more than one state.

As it is stated in the explanatory report of the Convention, the regulation was drafted in the light of the latest technical developments, "while keeping its provisions sufficiently general in order to guarantee as far as possible their adaptability to future developments."[8] For this reason, the word 'telecommunication' is not defined in the 2000 MLA Convention, which makes it possible to interpret the meaning of this expression as broadly as possible.

The 2000 MLA Convention makes distinctions between two types of interception. On the one hand, there are cross-border interceptions which can be carried out only with the (technical) assistance of another Member State, on the other hand, the are interceptions which can be carried out on the territory of another Member State without its technical assistance.

MS took a large step by regulating this question in the 2000 MLA Convention, but as it will be indicated later in this study, the regulation is not as comprehensive as it should be. This generates a loophole which creates legal and technical obstacles. Moreover, it may disable authorities to use accurate and important cross-border intercepts as evidence in criminal procedures.

---

[7] The Contracting Parties undertake to afford each other, in accordance with the provisions of this Convention, the widest measure of mutual assistance in proceedings in respect of offences the punishment of which, at the time of the request for assistance, falls within the jurisdiction of the judicial authorities of the requesting Party.

[8] Explanatory Report on the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 379/02)
http://eur lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:379:0007:0029:EN:PDF

In our study we intend to analyze cross-border interceptions carried out abroad, without the technical assistance of the concerned Member State.

Under these circumstances, the main problem occurs when a person under surveillance leaves the country and uses his/her telecommunication tool on another state's territory. As the analysis of the conversations usually takes place well after the recording (real-time surveillance is very rare), authorities – if they do - typically notice the fact that the person involved was abroad after the interception.

For a better understanding the main questions will be presented via a case study:

III. Case study

The Hungarian law enforcement authority has been investigating a criminal organization responsible for stealing masterpieces from different private collectors in Hungary.

In March 2011 a Van Gogh painting was stolen from a private collector in Budapest.

After months of investigation, the law enforcement authority was able to identify one of the potential members of the criminal organization. Upon judicial authorization the police started intercepting the mobile phone of the suspect.

One day the suspect was driving from Hungary to Vienna to an arranged meeting with an antique dealer, while he called one of his friends in Hungary. During this conversation the suspect, who was being wiretapped, mentioned details of the robbery, indicating also the whereabouts of the stolen paintings.

Upon these statements of the suspect, the Hungarian police managed to find later the stolen painting in a basement of a house in Budapest.

Our study will consider three different scenarios concerning this interception, and we will present how the intercept materials could be used as evidence in the criminal procedure.

1) During the investigation the police already have information that the suspect intends to go to a meeting in Austria, therefore, during the interception he will be abroad for a certain period.

2) The police had carried out the interception successfully, nevertheless, only after analyzing the evidence did they notice that the suspect had been abroad at the time of the recorded conversation.
3) It was identified neither during the investigation nor in the court proceeding that the suspect had been abroad during the surveillance.

It has to be pointed out that in this case study Hungarian authorities carry out interception without the technical assistance of the Austrian authorities.

1) **The first scenario deals with the situation when the law enforcement authority, after initiating the interception, is informed that the suspect will be staying abroad.**

The first question arising is how an interception can be lawfully carried out on the territory of another Member State.

The solution can be found in the 2000 MLA Convention, where the rules of cross-border interception without technical assistance are stipulated.

According to Paragraph 2 of Article 20 of the 2000 MLA Convention, "where for the purpose of a criminal investigation, the interception of telecommunications is authorized by the competent authority of one Member State (the 'intercepting Member State'), and the telecommunication address of the subject specified in the interception order is being used on the territory of another Member State (the 'notified Member State') from which no technical assistance is needed to carry out the interception, the intercepting Member State shall inform the notified Member State of the interception:

(a) *prior* to the interception in cases where *it knows when ordering the interception* that the subject is on the territory of the notified Member State;

(b) in other cases, *immediately after it becomes aware* that the subject of the interception is on the territory of the notified Member State".

This Article imposes an obligation on the intercepting Member State to inform the Member State on whose territory the subject is present about the interception.

It is needed to be determined whether paragraph 2 (a) or (b) should be applied in such circumstances. It can be deduced that point (a) cannot be applicable in our case because this provision presumes that the suspect is staying already abroad at the time of ordering the interception.

In our particular case, the interception had already been ordered when the law enforcement authority received information about the suspect's trip abroad.

For this reason our case is covered by point (b) since the law enforcement authority became aware only later, during the interception, that the intercepted person would spend a short period on the territory of another state.

Under these circumstances, according to Article 20, the concerned Member State (Austria) should be informed immediately after the intercepting Member State (Hungary) realizes that the intercepted suspect is abroad.

Analyzing point b) of Paragraph 2, it should be noted in parentheses that the sentence is drafted in the present tense (the subject of the interception is on the territory of the notified MS…), while in our case the Hungarian suspect will be on the territory of Austria only later.

Despite this uncertain regulation we believe that in our case Hungary has an obligation to inform Austria of the interception.

According to paragraph 3 of Article 20, Austria shall receive detailed information of the interception (the competent authority, legal background, expected duration of the interception…etc).

It is also stated in Article 20 that the notified Member State should respond "without delay and at the latest within 96 hours" to the intercepting Member State. /Paragraph 4 (a) of Article 20/

The notified Member State can either approve the interception to be continued or it can also reject it and require the intercepting Member State to terminate the interception. In the latter case the notified Member State "shall give reasons for its decisions in writing". /Paragraph 4 (a) (ii) of Article 20/

If the notified Member State approves the interception, the information gathered from the interception can be used as evidence.

However, if the notified Member State requests the termination of interception, according to Paragraph 4 (a) (iii) of Article 20 any material already intercepted may be subject to conditions set forth by the notified Member State.

If the notified Member State does not allow using any of the information received by interception, then it cannot be used as evidence.

From our point of view this case already describes the existing difficulties of cross-border interception.

The notified Member State has a predominant role in assessing the interception carried out by another Member State.

The notified Member State „may make its consent subject to any conditions which would have to be observed in a similar national case" /Paragraph 4 (a) (i)/, may require the termination of the interception, „where the interception would not be permissible pursuant to the national law or for the reasons specified in Article 2 of the European Mutual Assistance Convention" /Paragraph 4 (a) (ii)/.

In our opinion the notified Member State has been provided a rather wide range of ground for refusal. The intercepting MS, for example, is not able to control the conditions which could be imposed by the other State.

Our study intends to elaborate upon this problem later; meanwhile it is worth mentioning that despite the presented difficulties, there is pertaining regulation on EU level for this scenario.

2. **The police had carried out the interception successfully, nevertheless, only after analyzing the evidence did they notice that the suspect had been abroad at the time of the recorded conversation.**

It should be pointed out that in our opinion this is the most probable scenario, since the majority of interceptions are recorded only by technical means. The content of the recorded conversations are analysed only later by the competent authority.

In this scenario, the Hungarian police notice only after the termination of the interception that the suspect was on his way abroad when this important conversation was recorded.

The first problem arising is that after the event it is very difficult to determine the exact whereabouts of the suspect at the time of the interception. In this case it is uncertain whether the suspect talking about the robbery was still on the Hungarian territory or had already crossed the Austrian border.

In this present case, the Hungarian law enforcement and judicial authorities would like to use this crucial intercept material in court proceedings. The question to be answered is whether the Austrian authorities should be informed about the interception or could the intercept material be used as evidence in the Hungarian criminal procedure without their approval.

As it was already mentioned in the first scenario, interception across borders without technical assistance is regulated in Article 20 (2) of 2000 MLA Convention.

The relevant part of this Act stipulates that the intercepting Member State shall notify the other Member State prior to the interception / Paragraph 2 (a) of Article 20/ or *immediately after it becomes aware that the* ***subject of the interception is on the territory*** *of another state* /Paragraph 2 (b) of Article 20/.

Attention should be drawn to the fact that the wording of the above mentioned provision is drafted in the simple present tense, which means that it does not cover acts having occured in the past.

Referring to our scenario, the suspect had been on the territory of the "notified" Member State at the time of the interception, but later, when the recorded conversations were analyzed, the subject was already in Hungary and not in the "notified" Member State.

With regard to these facts a very significant question should be raised: How authorities could use an intercept carried out on the territory of another Member State without its technical assistance as evidence, if the intercepted person is not abroad any more at the time of the analysis of the recorded conversations?

Different interpretations could be provided, nevertheless, in our opinion the literal interpretation already gives a clear answer.

According to the wording of this Article, the intercepting state shall inform the notified state about interceptions that are intended or pending.

In our scenario the interception has already been terminated, the suspect has returned to Hungary. Indeed, the suspect had been abroad at the time of the interception but when this fact was noticed, he/she was no longer on the territory of the other Member State. Following this logic it can be stated that the Hungarian authorities may use the recorded intercept as evidence without the approval of the Austrian authorities; consequently, provisions of the 2000 MLA Convention are not applicable for this situation.

In connection with that answer, which seems to be very simple, the following question should be considered:

What was the intention of the EU by drafting the above mentioned provision in the simple present tense? Did the EU intentionally differentiate interceptions carried out on the territory of other Member State on the basis of the whereabouts of the suspect at the time of the interception, or was this problem not foreseen?

There are several reasons to believe that this question was not carefully examined by EU legislators.

On the one hand, neither the 2000 MLA Convention, nor its explanatory report gives an adequate answer to this question. It should be pointed out that even this kind of cross-border interception falls under the scope of the international interception of telecommunications. It has the same effect towards the other Member State since it concerns its sovereignty.

On the other hand, the explanatory report itself explains that rules of the Convention "are provided for a situation where there is neither a requesting Member State nor a requested Member State (the intercepting Member State does not need technical assistance from the Member State on whose territory the subject is located)".[9]

[9] Explanatory Report on the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 379/02) Title III General introduction and technical data http://eur lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2000:379:0007:0029:EN:PDF

On the basis of the explanatory report, one has the impression that the 2000 Convention intended to regulate all kinds of cross-border interceptions carried out without technical assistance of another Member State.

As a conclusion, it may be stated that there is a loophole in the regulation of the 2000 MLA Convention.

To clarify this problem we are obliged to take a look at the European level; whether this uncertainty in the regulation is interpreted in the same way by MS, or different answers are given to the emerging problems.

According to Eurojust Annual Report 2010, even Eurojust raised a number of questions concerning this issue, "….whether informing another Member State on the concluded cross-border interception is necessary…". [10]

The Annual Report underlines that "the outcome showed that the opinions, legislation and practice of MS in this area of co-operation differ considerably and that this issue may need clarification at EU level." [11]

Upon these statements it has to be presumed that in some MS there is an obligation to inform the other Member State of the concluded cross-border interception, while there are countries where similar requirements do not exist.

The lack of common practice also means that some MS use the collected evidence in court proceedings without the approval of the concerned Member State, while other MS' legal systems do not allow the use of this kind of evidence without the consent of the other State.

It has to be accepted that MS' legal systems differ from each other and the same kind of evidence would be treated differently in each country (admissible or inadmissible); at the same time we believe that a European legal instrument should be sufficiently clear and give adequate solutions to the problems it intends to regulate.

[10] Eurojust Annual Report 2010, page 25
http://www.eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202010/Annual-Report-2010-EN.pdf

[11] Eurojust Annual Report 2010, page 25

Under the current circumstances, on the same legal basis there are countries which certainly refuse to provide their approval protecting their sovereignty, while others easily give green light for the use of interception – carried out by other State - as evidence. At the same time there are countries which do not even inform the other State on whose territory the interception is carried out.

3) **The third scenario deals with the situation when it was not identified either during the investigation or in the court proceeding that the suspect had been abroad during the surveillance.**

It is also very probable that the subject's whereabouts during the interception are overlooked by the investigators. If no contrary information is available, competent authorities may presume that the suspect was in the intercepting Member State all along the procedure.

As a result, it is evident that the whereabouts of the suspect play a very important role in cross-border interceptions.

The next part of our study will argue that due to rapid technical development it is more and more difficult to determine the exact whereabouts of the suspects who are using more and more as sophisticated telecommunication tools.

IV. Technical Challenges in Lawful Interception

Following the analysis of the legal difficulties of cross-border interception, we will now take a brief look at the new challenges faced by legislators, judicial and law enforcement authorities. Namely the challenges of the modern-day versions of interceptions related to the different types of new telecommunication possibilities.

The ways in which people communicate have always been changing. Technology, specifically over the internet has been opening even newer avenues in recent times. Each type of communication comes with its own challenges for law enforcement authorities in the field of interception.

From landline phones, which can be wire tapped, to mobile phones, whose location can be traced, the focus is now shifting towards communication over the internet. Emails in the beginning were easier to track since Internet Service Providers (ISP) provided the service and

thus kept information pertaining to the customer involved. This then changed to webmail services, which allowed users to have multiple email addresses with no means to verify the identity of the users creating accounts from different parts of the world.[12]

Communication over the internet has even further advanced to many forms of instant messaging, bulletin boards, social networking facilities, file-sharing and distribution services, voice messaging...etc. In fact, social networking sites only existed in primitive forms when communications surveillance laws were devised. Many online and console games allow users from around the world to meet up in their virtual space to interact, discuss issues, and exchange in goods and ideas with live voice communication.[13]

Each one of these forms of communication tends to follow their own technical rules/protocols to make the communication work with different companies and service providers customising their own techniques.[14]

Various service providers are present over the internet at the user's disposal offering various services. These services are often provided with minimal user information requirements and without the need for the user's information to be filled in accurately. The user could thus be able to create multiple accounts across service providers. This is true of many web-based email services but also of file-sharing, Voice Over Internet Protocol (hereafter: VOIP), instant messaging and social networking.[15]

Users are able to get even greater levels of anonymity with the wide-spread availability of pay as you go (PAYG) tariffs for mobile phones and the Internet cafes where online time can be purchased for cash and without any need to demonstrate identity. Wi-Fi networks are another case where such anonymity can be achieved by hijacking poorly secured Internet connections of others. Another dimension is also added by the fact that there may be multiple users sharing the same internet connection.[16]

---

[12] Romanidis Evripidis: Lawful Interception and countermeasures, School of Information and Communication Technology, Royal Institute of Technology Stockholm, Sweden, 2008 page http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/080922-Romanidis_Evripidis-with-cover.pdf (accessed: 30/03/2012)

[13] Briefing on the Interception Modernisation Programme, Policy Engagement Network, Information Systems and Innovation Group, LSE, Houghton Street, London, WC2A 2AE (accessed 30/03/2012) page 17

[14] Op at footnote no 3 page 17

[15] Op at footnote no 3 page 18

[16] Op at footnote no 3 page 18

Skilled cybercriminals are always on the lookout for new techniques they can use to achieve their goals. One such technique which is being used ever increasingly is the use of certain software applications that enable cybercriminals to change their internet address (IP address) on a frequent basis and, as a result, make it harder for the law enforcement agencies to trace them.[17]

Encryption is one of the sophisticated methods used to protect the confidentiality of messages and VOIP conversations over the Internet. By using encryption, information can be made unreadable for other people who might have access to it if they do not have a proper key to decipher it.[18] One of the major hurdles for interception techniques in recent times has been Skype. Although Skype interception is already possible, it is very rarely used due to the technical challenges.
The main problem caused by Skype's encryption is that the encryption occurs only between the Skype partners who create encryption keys and pass them to each other.[19]

V. Summary and solutions

In general, it can be concluded that the development of technology has given rise to new challenges for legislators especially in the field of interception. Our study has presented that due to the emergence of new ways of telecommunications, law enforcement authorities face challenges when intercepting these new kinds of communications, and locating the whereabouts of the suspects at the time of the interception.

Problems with the wording of Paragraph 2 of Article 20 of 2000 MLA Convention have been elaborated upon as well.

Our aim is to provide recommendations to solve the problems mentioned above.

The first possible solution is very simple. As it is written in Eurojust Annual Report 2010, it would be sufficient to amend the text of Paragraph 2(b) of Article 20 of the 2000 MLA Convention with a past simple distinction. According to this proposed amendment, the

[17] Op at footnote no 3 page 18
[18] Dominique Valiquet: Cybercrime: Issues, Publication No. 201-36E, 5 April 2011, page 8
[19] Robert Poe: Skype Secrecy Under Attack Again, February 24, 2009, http://www.voip-news.com/feature/skype-secrecy-attack-022409/ (accessed: 20/03/2012)

notified Member State shall be informed immediately after it becomes aware that the subject of the interception **is *or was*** on the territory of the notified Member State.

This kind of amendment would protect the sovereignty of MS since they could control all kinds of interceptions carried out on their territory.

This solution would impose the obligation on the intercepting Member State to ask for the approval of the competent foreign authority as soon as it learns that the suspect has crossed borders or was staying abroad at the time of the interception. If the consent has been declined, the interception cannot be continued or used as evidence in court proceedings. Consent of the concerned Member State should be given not only before but also after the interception.

Despite the fact that this solution would give an adequate answer to the presented problems, in our opinion, it would have a negative impact on the efficiency of the investigations.

Our case study has already presented a situation where the whereabouts of the suspect could not be determined exactly in connection with a recorded conversation which was intended to be used as evidence.

Would this uncertainty (the suspect was maybe in Austria at the time of the interception) constrain the Hungarian authorities to turn to the Austrian authorities for an approval in a criminal case which they have possibly nothing to do with?

What is the reason for this EU regulation according to which the approval of the concerned Member State should be requested in cross-border interceptions even if the State does not provide any assistance? In our opinion the principle of sovereignty should be the answer to this question.

Mutual legal assistance requests are usually submitted to the other MS with the aim to request execution of investigating measures with the help and on the territory of the requested Member State. Cross-border interceptions can be carried out without technical assistance; evoking sovereignty issues in these cases seems outdated.

We have pointed out in one scenario that the competent authorities (either the intercepting or the requested State) may not even notice that the suspect was abroad at the time of the interception.

Furthermore, different examples could be presented to indicate the contradiction of the present and proposed regulation as well.

It occurs more and more often that perpetrators are using the same email account (they have the same passwords). To facilitate their conversation they do not send emails to each other but leave only their messages in the draft folder providing the possibility for the others to check it easily.

Let us suppose that a similar email account used by two suspects is intercepted by an authority. One suspect leaves messages in the draft folder from abroad. Do we have to inform the concerned Member State on whose territory the message was written?

Furthermore, how should we proceed if we want to use data of GPS surveillance as evidence and we know that the suspect crossed the borders during the surveillance?

As the Treaty on the Functioning of the European Union sets forth, "judicial cooperation in criminal matters shall be based on the principle of mutual recognition of judgments and judicial decision and shall include the approximation of the laws and regulations of the Member States".

The principle of mutual recognition, which intends to ensure a quicker and more effective way of criminal cooperation, is based on the notion of mutual trust.

The principle of mutual trust presumes that MS accept the fact that interceptions carried out by other States on their territory have been ordered and executed in a lawful manner.

For this reason we believe that MS should give up the control of interceptions carried by other State on their territory. In our opinion MS should be entitled to carry out interceptions abroad without the approval (and the technical assistance) of the concerned MS.

On the one hand, this approach would solve the technical problems in the detection of the whereabouts of the suspect, since in this case the competent authorities would not be obliged to deal with this issue. This recommendation presumes that interceptions are always lawfully ordered and carried out. On the other hand, it would create a clear and transparent legal background in the field of cross-border interceptions and solve the legal problems concerning the admissibility of intercept as evidence in criminal proceedings.

Bibliography

- Briefing on the Interception Modernisation Programme, The London School of Econimics and Political Science
- Briefing on the Interception Modernisation Programme, Policy Engagement Network, Information Systems and Innovation Group
- Eurojust Annual Report 2010
- Romanidis Evripidis: Lawful Interception and countermeasures, School of Information and Communication Technology, Royal Institute of Technology
- Explanatory Report on the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000/C 379/02)
- History of the Morse Telegraph
- Robert Poe: Skype Secrecy Under Attack Again Reply to a questionnaire on special investigation techniques in relation to acts of terrorism, Denmark, Sweden, Ireland Council of Europe
- Technical aspects of Lawful Interception ITU-T Technology Watch Briefing Report Series
- Dominique Valiquet: Cybercrime: Issues, Publication No. 201-36E, 5 April 2011,

Legal Background

- The European Convention on Human Rights (4 November 1950 Rome)
- European Convention on Mutual Legal Assistance in Criminal Matters of 1959
- Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union
- Valenzuela Contreras v. Spain (application no.: 58/1997/842/1048)