



[PC-OC\Docs 2008\PC-OC (2008)08

<http://www.coe.int/tcj/>

Strasbourg 01/04/2008

PC-OC (2008) 08

**EUROPEAN COMMITTEE ON CRIME PROBLEMS**  
**COMITÉ EUROPÉEN POUR LES PROBLÈMES CRIMINELS**

(CDPC)

**COMMITTEE OF EXPERTS**  
**ON THE OPERATION OF EUROPEAN CONVENTIONS**  
**ON CO-OPERATION IN CRIMINAL MATTERS**

(PC-OC)

**COMITE D'EXPERTS**  
**SUR LE FONCTIONNEMENT DES CONVENTIONS EUROPEENNES**  
**SUR LA COOPERATION DANS LE DOMAINE PENAL**

(PC-OC)

Replies / Réponses

on/sur

**Mutual Legal Assistance in Computer-Related Cases**  
***L'entraide judiciaire dans les affaires liées à l'informatique***



**STATES/ ETATS**

<b>BACKGROUND INFORMATION:</b> .....	<b>4</b>
<b>INFORMATIONS GÉNÉRALES :</b> .....	<b>5</b>
<b>ARMENIA</b> .....	<b>6</b>
<b>BOSNIA AND HERZEGOVINA</b> .....	<b>7</b>
<b>HUNGARY</b> .....	<b>8</b>
<b>LATVIA</b> .....	<b>9</b>
<b>LUXEMBOURG</b> .....	<b>10</b>
<b>MALTA</b> .....	<b>11</b>
<b>POLAND</b> .....	<b>12</b>
<b>PORTUGAL</b> .....	<b>13</b>
<b>ROMANIA</b> .....	<b>14</b>
<b>SLOVAKIA</b> .....	<b>25</b>
<b>SLOVENIA</b> .....	<b>27</b>
<b>SUISSE</b> .....	<b>28</b>
<b>SWEDEN</b> .....	<b>29</b>

**BACKGROUND INFORMATION:**

The Cybercrime Convention Committee (T-CY) at its last meeting in Strasbourg from 13 to 14 June 2007 underlined current difficulties in relation to mutual legal assistance under the Convention on Cybercrime. The T-CY agreed that timeliness of co-operation between the states Parties is a crucial factor for combating cybercrime successfully. Among other matters, it was stressed that the Convention is applicable to offences committed with terrorist intent and in this respect the short period for data retention creates serious practical problems for responsible authorities.

The T-CY noted that offenders use all possibilities of cyberspace, which makes work of law enforcement authorities more difficult as cybercrime cases often involve more than two States. It was emphasized that when investigating crimes committed through the Internet the traditional methods of mutual legal assistance, in particular its time-limits, could not always serve the purpose of this Convention. In computer related crimes computer data, intended to be used as evidence, can be destroyed/lost instantly and therefore the period of 90 days seems to be inadequate.

Following the request from T-CY for guidance concerning best practices for mutual legal assistance in computer-related cases (in particular in urgent cases) the CDPC, at its last plenary meeting on 18-22 June 2007, instructed the PC-OC to provide the requested practical guidance as well as to consider questions relating to operational matters such as Article 32b of the Convention. This Article provides that:

“A Party may, without the authorisation of another Party [...] access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.”

At its last plenary meeting on 21-23 November 2007, the PC-OC held preliminary discussions concerning this request. It decided to send a questionnaire, containing a description of the information sought and specific questions, to all States Parties to the Council of Europe conventions on international co-operation in the criminal field, including Member States and non-Member States of the Council of Europe. These questions were prepared by Mr Branislav Boháčik, Chair of the CDPC, representative of the CDPC to the T-CY and member of the PC-OC.

**Questions:**

1. Please describe methods, means and tools used by your competent authorities for rendering mutual legal assistance to authorities of other States in urgent cases (the channels of communication, translation etc.). Please provide examples of good practices or any guidelines for an effective mutual legal assistance in urgent cases, in particular computer-related cases (cybercrime).
2. If your State is a Party to Convention on Cybercrime, please describe how Article 32 b of the Cybercrime Convention is applied or is intended to be applied in practice within your jurisdiction. How do your competent authorities interpret the provisions of the mentioned Article in legislation and/or in practice?

The responding States are invited to reply to the present questionnaire by 1 April 2008 at the latest, and sooner if possible, in order for the replies to be transmitted to the T-CY before its plenary meeting on 3-4 April 2008.

\* \* \* \* \*

## INFORMATIONS GENERALES :

Le Comité de la Convention Cybercriminalité (T-CY) a évoqué, à sa dernière réunion tenue à Strasbourg les 13 et 14 juin 2007, les difficultés actuelles relatives à l'entraide judiciaire en vertu de la Convention sur la cybercriminalité. Il est convenu que les Etats parties devaient coopérer dans les délais impartis pour que la lutte contre la cybercriminalité soit efficace. Il a entre autres souligné que la Convention était applicable aux délits commis dans un but terroriste et qu'à cet égard la courte période de conservation des données entraînait des problèmes pratiques importants pour les autorités compétentes.

Le T-CY a noté que les délinquants avaient recours à toutes les possibilités offertes par le cyberspace, ce qui rend la mission des services répressifs plus difficile étant donné que les affaires de cybercriminalité impliquent souvent plus de deux Etats. Il a été souligné qu'au cours des enquêtes sur les délits commis par le biais de l'Internet, les méthodes classiques d'entraide judiciaire, et en particulier ses limites de temps, ne pouvaient pas toujours répondre aux objectifs de la Convention. Dans le contexte des crimes informatiques, les données informatiques censées servir d'éléments de preuve, peuvent être détruites/perdus instantanément, et dans ces conditions la période de 90 jours paraît inappropriée.

Le T-CY ayant demandé des conseils de bonnes pratiques en matière d'entraide judiciaire dans les affaires liées à l'informatique (notamment les affaires urgentes), le CDPC, à sa dernière réunion plénière tenue du 18 au 22 juin 2007, a chargé le PC-OC de fournir les conseils pratiques demandés et d'examiner les points relatifs aux questions opérationnelles comme l'article 32b de la Convention, qui énonce la disposition suivante :

« Une Partie peut, sans l'autorisation d'une autre Partie [...] accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique. »

A sa dernière réunion plénière tenue du 21 au 23 novembre 2007, le PC-OC a tenu des discussions préliminaires au sujet de cette requête. Il a décidé d'envoyer un questionnaire, qui indique les informations recherchées et pose des questions spécifiques, à tous les Etats Parties aux conventions du Conseil de l'Europe sur la coopération internationale dans le domaine pénal, y compris les Etats membres et les Etats non membres du Conseil de l'Europe. Ces questions ont été élaborées par M. Branislav Boháčik, président du CDPC, représentant du CDPC auprès du T-CY et membre du PC-OC.

### Questions :

1. Veuillez présenter les méthodes, les moyens et les outils utilisés par les autorités compétentes de votre pays pour fournir une assistance judiciaire aux autorités d'autres Etats dans les affaires urgentes (voies de communication, traduction, etc.). Veuillez donner des exemples de bonnes pratiques ou des indications qui visent à renforcer l'efficacité de cette entraide judiciaire dans les affaires urgentes, notamment dans les affaires liées à l'informatique (cybercriminalité).
2. Si votre Etat est partie à la Convention sur la cybercriminalité, veuillez indiquer comment l'article 32 b de cette Convention est appliqué ou est censé être appliqué dans la pratique dans le cadre de votre juridiction ? Comment les autorités compétentes de votre pays interprètent-elles les dispositions de l'article mentionné dans la législation et/ou dans la pratique ?

Les Etats interrogés sont invités à répondre au présent questionnaire avant le 1<sup>er</sup> avril 2008, et avant cette échéance si possible, afin que les réponses puissent être transmises au T-CY avant sa réunion plénière qui se tiendra les 3 et 4 avril 2008.

\* \* \* \* \*

## **ARMENIA**

Please be informed that the Cybercrime Convention for Armenia entered into force on 1st of February 2007. In this view Armenia has no experience related to the implementation of the point 32b of Convention. The exchanging of the experience in this field will be greeted.

## BOSNIA AND HERZEGOVINA

1. In Bosnia and Herzegovina, rendering international legal aid is regulated by the Criminal Procedure Code of Bosnia and Herzegovina ("Official Gazette BiH", number 3/03) in Chapter XXX – Procedure to Render International Legal Aid to Enforce International Agreements in Criminal Matters. Article 408 of this Law stipulates that appeals by Court or Prosecutor for legal aid in criminal matters shall be submitted to foreign bodies through diplomatic channels, in such a way that the Court or rather the Prosecutor submits appeals to the competent ministry of Bosnia and Herzegovina, which is in this case BiH Ministry of Foreign Affairs and BiH Ministry of Justice. Article 409 of this Law stipulates that a competent ministry, upon reception of a foreign body's appeal, shall submit the appeal to the Prosecutor in cases where rendering legal aid fall under the Court's competency, after which, the Court or rather the Prosecutor shall decide on permission and ways of implementation of the activity which is the subject of the foreign body's appeal, in accordance with the laws of Bosnia and Herzegovina and in compliance with its competencies.

When rendering legal aid, Bosnia and Herzegovina observes the international conventions which have been ratified by Bosnia and Herzegovina, and most of all the European Convention on Common Rendering of Legal Aid in Criminal Matters, with additional protocols.

Bosnia and Herzegovina is a signatory of a range of bilateral agreements on police cooperation, which is achieved through exchange of information and experience in the common field of interest, exchange of experiences in the use of technology, methods and means in investigations, prevention, combating and prosecuting criminal activities, data on individuals linked with these activities, exchange of legislative solutions, exchange of publications and results of scientific research. Bosnia and Herzegovina has also signed the Convention on Police Cooperation for South-East Europe.

Keeping in mind the fact that cyber crime is relatively new form of crime in Bosnia and Herzegovina, Bosnia and Herzegovina has not had a large scale of international cooperation for prevention of this form of crime. We shall distinguish one of the examples of cooperation in this field, achieved in the year 2006 with the INTERPOL Office Wiesbaden. Namely, based on data received from the INTERPOL Office in Wiesbaden, we have discovered and trialed two persons in BiH who had committed internet frauds of many citizens from Western Europe, especially the citizens of FR Germany.

Police agencies, competent for combating cyber crime and perpetrators, have also performed inspection of some IP addresses of certain individuals in BiH, as well as other relevant measures and activities, based on requests from other countries delivered through Office for Cooperation with INTERPOL in BiH.

2. On May 19, 2006 Bosnia and Herzegovina ratified the Convention of the Council of Europe on Cyber Crime, with additional protocol. As regards to Article 32 paragraph b of the stated Convention, Bosnia and Herzegovina shall legally arrange this issue in the future.

## HUNGARY

Regarding the requests delivered before a criminal procedure has been started, the designated central authority is the ***Hungarian National Police International Implementing Co-operation Centre*** and, regarding the requests delivered after a criminal procedure has been initiated, the designated central authority is the ***General Prosecutor's Office of the Republic of Hungary***.

The General Prosecutor's Office of the Republic of Hungary could not provide us with relevant answers to your questionnaire, as it has not received any request based on Article 32 point b) of the Cybercrime Convention yet. Interpretation problem in connection with Article 32 of the Cybercrime Convention has not occurred neither at the General Prosecutor's Office of the Republic of Hungary nor at the investigating authorities.

The Hungarian National Police International Implementing Co-operation Centre gave the following answers:

1. Currently we use liaison officer's network in the different countries for an urgent information acquisition because this way it brings result within a few days (sometimes within 1-2 weeks) in our experience.

In connection with question 2, the Hungarian National Police International Implementing Co-operation Centre could not provide us with relevant answers, as it has not received any urgent request in connection with Article 32 of the Cybercrime Convention since it is in effect in Hungary.

According to the Hungarian legal regulations, official requests shall be made to the above-mentioned designated authorities in the frame of a mutual legal assistance. (The designated point of contact available on a twenty-four hour, seven-day-a-week basis is the Hungarian National Police International Implementing Co-operation Centre.) These requests shall be sent via special and secured channels, so the competent Hungarian authorities can receive them shortly after they have been sent.

However, there is a barrier to information service, according to the relevant Hungarian legal regulations, that data, which is processed in a database exclusively maintained for EU member states, is not permitted to be provided to those states which are not members of the European Union.



## LATVIA

1. Since June 1 of 2007, when the Convention Cybercrime and its Additional Protocol took effect in the Republic of Latvia, the International Cooperation Department of the Central Criminal Police Department as responsible institution within the scope of Article 35 of the Convention has not received from other contact points of the Member States to the Convention any requests of assistance aimed at ensuring immediate assistance for the purposes of investigation or court proceedings in relation to criminal offences associated with computer systems and data (for example, saving of computer data on the bases of Article 29 and 30 of the Convention).

In its turn, as regards to criminal proceedings instituted in the Republic of Latvia, the International Cooperation Department has twice requested through the US Interpol Bureau assistance of the competent authorities within the scope of Article 35 of the Convention to save computer data (in both cases the investigating authorities acted as the initiator of the requests). Requests were executed and the said data saved.

We believe that usage of communication system I-24/7 of the International Criminal Police Organization – Interpol, as communication channel for transmitting requests for urgent assistance to contact point of another party is an optimal solution and should be applied in the Member States to the Convention.

Similarly it is possible in urgent cases to send a request of assistance through Europol.

2. The competent authorities of a foreign state can request stored computer data from an owner or operator of a computer system and the above data can be provided if written consent of the user or subscriber has been received.

## LUXEMBOURG

Les affaires d'entraide judiciaire en matière pénale sont, en vertu de l'article 7 de la loi du 8 août 2000 applicable à cette matière, traitées comme affaires « *urgentes et prioritaires* » à toutes autres affaires et cela même si aucun caractère d'urgence n'a été spécifié à la demande d'assistance.

De même, bien que la même loi prévoie en son article 2 que toute demande n'est exécutée qu'après avoir reçu l'avis favorable du Procureur général d'Etat, il pourra être fait exception à cette règle si « *l'affaire à la base de la demande d'entraide paraît grave et s'il y a urgence consistant en particulier en un risque de dépérissement des preuves* » (art. 2, 5. de la loi du 8 août 2000). Dans ce cas, les devoirs d'instruction requis d'urgence peuvent être pris dès réception de la demande et avant d'avoir reçu l'avis du Procureur général d'Etat. Cet avis devra cependant être sollicité au plus vite.

Enfin, dernier cas d'urgence prévu à la loi du 8 août 2000, si en principe les pièces d'exécution de la demande ne peuvent être transmises à l'autorité requérant qu'au vu d'une ordonnance rendue sur demande du parquet par la chambre du conseil du tribunal d'arrondissement, une procédure simplifiée est prévue à l'article 11 de la loi « *s'il existe des indices graves et concordants que le déroulement de la procédure prévue (à la loi) risque de mettre en danger la santé physique ou psychique d'une personne* ».

En pratique, l'ensemble de la Justice est pourvue des moyens de communication – y compris électroniques - les plus modernes et performants. La réception d'une demande d'entraide par ces moyens, bien que non prévue à loi, est cependant admise par la pratique dans un premier stade et cela tout particulièrement s'il y a urgence, à la seule condition, évidente, que le moyen choisi permette d'avoir une trace écrite. La demande en bonne et due forme devra être en possession de la Justice au plus tard au moment du retour des pièces d'exécution.

Les demandes sont admises dans les langues déclarées comme admissibles par le Grand-Duché de Luxembourg dans le cadre des différentes conventions internationales régissant l'entraide, à savoir le Français, l'Allemand ou l'Anglais.

En outre, le Grand-Duché de Luxembourg, compte tenu de sa taille réduite, a des voies de communication internes extrêmement courtes, et qui se raccourciront encore plus après le déménagement de la Justice dans les locaux de la Cité judiciaire, où tous les services seront réunis sur un seul site.

De ce chef, une demande d'une urgence avérée peut être traitée par la Justice quasiment dès réception, quelle que soit la matière concernée, et donc également en matière de criminalité informatique.

L'exécution des mesures prises suite à la réception d'une commission rogatoire est du ressort de la police grand-ducale, qui dispose en matière de « *cybercriminalité* » de services spécialisés.

\* \* \* \* \*

## MALTA

The Reply hereunder treats requests for assistance in general and thus although not specifically addressing computer-related crimes, the generality of the foregoing would apply to such offences.

1. The Attorney General's Office which is the designated central authority in all Conventions, Treaties and Agreements providing for mutual legal assistance to which Malta is a party, has a specialised unit which deals with such matters, the International Co-Operation in Criminal Matters Unit. Within the Unit are the officers responsible for assisting in the execution and/or transmission of requests for assistance and extradition and EAW procedures. Moreover the National Member for Eurojust and European Judicial Network contact points form part of the Unit. As such the Attorney General's Chambers has relied on the centralised and specialised role of its Unit to deal with incoming and outgoing requests for assistance in a professional, expedited and efficient manner. Request vary from issuing freezing orders to service of documents, from notification of judicial records to the taking of witness testimonials, from the gathering of evidence to extradition requests.

The centralised function of the Unit wherein the officials involved are also prosecutors before the Criminal Courts and participate in international and EU fora in relation to mutual legal assistance matters, has ensured specialisation but more importantly efficiency. Requests for assistance are received by any means capable of producing written records and this aids the execution of requests whilst ensuring that the legal formalities prescribed by domestic law are complied with. For purposes of initial hearings or preliminary inquiries and investigations, so as to avoid unnecessary delays, a faxed or scanned copy is permissible provided that the original request would be received by the Attorney General's Office prior to any material or evidence gathered upon execution of the request being physically forwarded to the requesting authorities.

2. Malta is not yet a State Party to the Cybercrime Convention.

**POLAND**Question 1.

The requests for mutual legal assistance are transmitted between countries of the Council of Europe and executed pursuant to the provisions of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959, the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters of 17 March 1978 and the Second Additional Protocol to European Convention on Mutual Assistance in Criminal Matters of 8 November 2001.

In relation to all kinds of request, including requests in computer-related cases, the provisions of the Article 15 of the Convention are applied.

In relation to the countries which are both the members of the Council of Europe and the European Union, the provisions of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 29 May 2000 may also be applied.

According to Article 6 of the EU - Convention, any request for mutual assistance may, in case of urgency, be made via Interpol or any body competent under provisions adopted pursuant to the Treaty on European Union. In practice, urgent requests are transmitted between competent authorities with translation using means of modern communication.

Polish judicial authorities are encouraged to transmit the MLA – requests directly to the judicial authorities of the requested party in cases where direct transmission is permitted under the treaties and if the competent requested authority is known.

If the requesting judicial authority does not know the competent executing judicial authority or if it is necessary, transmission of the request may be effected through the Europol, Eurojust or the contact points of the European Judicial Network.

Question 2.

Poland is not a party to the Convention on Cybercrime.

**PORTUGAL**

- 1a. Portugal is not listed in G824/8 contact point network and, on the other hand, did not ratify the Convention yet. Thus, all international cooperation is provided by classic means and channels: outside European Union, according international treaties and at police level through Interpol channels; within European Union, according to Schengen and MLA framework.
- b. In urgent cases, Policia Judiciária is able to cooperate, even if it is not yet a contact point of the 24/7 network, by its special unit with national jurisdiction, on computer and telecommunications crime, based in Lisbon.

\* \* \* \* \*

**ROMANIA****CONTENTS:**

1. Introduction
2. Methodology
3. Tools
  - 3.1 Convention on Cybercrime, Budapest, 2001
  - 3.2 European Convention on Mutual Legal Assistance in Criminal Matters, Strasbourg, 1959
  - 3.3 Convention of 19 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union
  - 3.4 United Nations Convention against Transnational Organized Crime, Palermo 2000
  - 3.5 The Treaty on Mutual Legal Assistance in Criminal Matters between Romania and Canada(Ottawa 1998)
  - 3.6 The Treaty between Romania and the United States of America on the Mutual Legal Assistance in Criminal Matters(Washington, 1999)
4. Practical issues and case studies related to MLA requests in cybercrime cases
  - a. Requests during the pre-trial investigation
  - b. Requests during the trial
5. Good practices of the Ministry of Justice as central authority for MLA requests in cybercrime cases. Means used for communications.
6. Possible future steps to be taken
  - 6.1 Traditional means of mutual assistance are not effective when referring to cyber offences
  - 6.2. The necessity to create a global network for victims support
  - 6.3. Setting up a database with the central authorities responsible for receiving/transmitting the MLA request
  - 6.4. The necessity of updated statistics related to MLA requests in computer crime cases
  - 6.5. The problem of the prejudice
7. Conclusions

**1. INTRODUCTION**

Cybercrime is by its nature transnational, therefore establishing a legal framework for cooperation between states in this matter is fundamental. Instruments like extradition, mutual legal assistance requests and more recently, at the E.U level, the European Arrest Warrant are constantly being used in the fight against cybercriminals. The importance of this type of criminality has been acknowledged by the European and international organizations that are trying to find legal and technical solutions for combating it.

The fact that cybercrime is on the rise is reflected in the intense cooperation between states in this respect, the Romanian Ministry of Justice as central authority in the matter of judicial cooperation in criminal matters facing a significant number of mutual legal assistance requests , as well as European Arrest Warrants related to high –tech crime.

Computer related crime was included among the 32 offences mentioned in the *Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States* which are excluded from the double criminality requirement. Since January 1<sup>st</sup> 2007, the European Arrest Warrant became applicable in Romania as well. Taking into account the passive European Arrest warrants received by the Ministry of Justice as a central authority, it emerged the fact that those referring to cybercrimes played an important part, being among the most often encountered offences. For example, from the total amount of the European Arrest Warrants transmitted by the

Italian judicial authorities in 2007, around 40% was referring to skimming or phishing committed in an organized manner. Other countries which have transmitted European Arrest Warrants related to cybercrime cases in respect of the Romanian nationals in 2007 and the beginnings of 2008 were Netherlands, Germany, Belgium, Spain and France. These concrete examples are showing that in Romania computer crimes are more and more visible than in the past, being coordinated with the exponential growth of the Internet connectivity.

## **2. METHODOLOGY**

In order to offer an accurate overview of the problems encountered by the judicial authorities, the Division of International Judicial Cooperation in Criminal Matters within the Directorate International Law and Treaties of the Romanian Ministry of Justice, which is responsible with the transmittal of letters rogatory, service of documents and any other acts involving requests of mutual assistance in criminal matters, kindly required to the courts to provide useful information relative to the issues that were the object of point 1 of the questionnaire. Also available information was obtained from consulting the Ministry of Justice own records related to requests of mutual legal assistance during the pre-trial and trial stage.

As the competences of the Ministry of Justice are related mainly to the requests submitted/transmitted during the trial and the execution of the punishment, we tried to concentrate on these aspects, since the Service of Combating Cybercrime within the Section for Combating Organized Crime and Drugs Trafficking to the High Court of Cassation and Justice has already offered to the Council of Europe valuable data relative to the good practices and also difficulties that arise during the prosecutorial phase.

We are aware that the provisions of the Convention take into account especially the requests of mutual legal assistance during the criminal investigation phase, where the speedy communication is essential in preserving the evidence and catching the offenders. Nevertheless, it is our believe that all the efforts undertaken during the investigation phase are in vane unless the trial is taking place in an expedited manner.

The impact that a speedy trial has for the public in general can be lost if the procedures are prolonging for years. The deterrent effect of the punishment will not be effective anymore, neither the general prevention which is one of the main purposes of applying a punishment. Moreover, there are situations even during the actual trial when urgent requests have to be communicated to other states.

The data gathered from the courts revealed to us not only aspects related to the mutual assistance but also to the type of cybercrime offences, duration of the trials and type of punishment applied. The cases brought to our attention pointed the fact that the punishment imposed by the Romanian judge in a cybercrime case is, most of the times, the conditional suspension of the execution of the punishment. Corroborated with the long periods of time the trial is actually taking place, this might create the impression to the general public and to the offenders that this kind of crimes are susceptible of impunity.

## **3. TOOLS**

**The international instruments** applicable in cases related to cybercrime, in accordance with the Romanian legislation implementing the European and international instruments in force are:

### **3.1. Convention on Cybercrime, Budapest, 2001**

According to the declaration contained in the instrument of ratification deposited by Romania and bearing in mind the provisions of art. 27 paragraph 2.c of the Convention, there are two

central authorities responsible for sending and answering requests for mutual legal assistance:

- the Prosecutor's Office to the High Court of Cassation and Justice- for request of mutual legal assistance formulated in the pre-trial investigation and prosecution;
- the Ministry of Justice - for the requests of mutual legal assistance during the trial or the enforcement of judgments .

The 24/7 point of contact is, in accordance with art. 35, paragraph 1 of the Cybercrime Convention, the Service of Combating Cybercrime within the Section for Combatting Organized Crime and Drugs Trafficking within the High Court of Cassation and Justice.

From the very beginning, it has to be mentioned that from the study of the archives of the Ministry of Justice as well as from the data gathered from the courts, the Cybercrime Convention has never been invoked as a legal background for the MLA requests neither by Romania, nor by the states that forwarded the MLA requests to Romania. Art. 25 of the Cybercrime Convention stipulates in paragraph 4 that mutual assistance *shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties*. Art 27 of the Cybercrime Convention states in the first paragraph that the provisions of this article will apply only if there is no mutual treaty or arrangement in force between the requesting and requested state or if the *parties concerned agree to apply any or all of the remainder of this article in lieu thereof*. Art. 39 of the Convention, when referring to the effects of the Convention, recites that the purpose of the convention is *to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties*. Taking into account all these provisions, it is well understandable why the Convention was never used as legal instrument for the requests.

### **3.2. European Convention on Mutual Legal Assistance in Criminal Matters, Strasbourg, 1959**

As it is well known, the mutual legal assistance requests formulated on the basis of this Convention are to be made from central authority to central authority. In this respect, the two Romanian central authorities responsible for sending/receiving the MLA requests are the Ministry of Justice and the Prosecutor's Office of the High Court of Cassation and Justice, taking into account the phase of the trial in which the request was made (for the first during the proceedings, for the second during the investigation and prosecution). The major problem when applying this convention was related to the terms required, which were very difficult to comply with in urgent cases.

Romania still applies the Convention in relation with EU countries that are not parties to the Convention of 29 May 2000, such as Italy or Ireland.

### **3.3. Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union**

The Convention and its Additional Protocol (2001) entered into force for Romania on the 1<sup>st</sup> of December 2007. The Convention facilitates the direct contact between the Romanian judicial authorities (Prosecutor's offices during the pre/trial phase and courts, during the trial phase) and their foreign counterparts. Again, the Convention is allowing the service of documents directly to the addressee, through post and not by central authorities as before. The central authority is to be used only in specific/complicated cases, such as the temporary transfer of sentenced persons.



### **3.4. United Nations Convention against Transnational Organized Crime, Palermo 2000**

This Convention includes reference to mutual legal assistance in art. 18 and can be successfully used as long as *the offence involves an organized criminal group*. The provisions become applicable when the parties in question are not bound by a treaty of mutual legal assistance. *The provisions of this article shall not affect the obligations under any other treaty, bilateral or multilateral, that governs or will govern, in whole or part, mutual legal assistance* (art. 18 paragraph 6). From the situations the Romanian authorities confronted with, it came out that the Palermo Convention is a valuable tool, mostly for contacts with non-European countries that have no bilateral treaties with Romania.

The disadvantage is that the provision of the Convention are related strictly to offences committed in an organized manner and if the cybercrime is committed by a single individual, then again no instrument would be applicable, as the Council of Europe Cybercrime Convention has been signed only by few non-European countries and for the moment, it represents the only binding international instrument in this field.

### **3.5. The Treaty on the mutual legal assistance in criminal matters between Romania and Canada (Ottawa 1998)**

According to article 16 of the Treaty, all the requests and the subsequent replies shall be sent/received through the central authorities who will communicate directly, the central authority for Romania being the Ministry of Justice.

### **3.6. The Treaty between Romanian and the United States of America on the mutual legal assistance in criminal matters (Washington, 1999)**

Article 2 of the Treaty establishes that the communication of MLA requests will be done through central authorities, the central authority for Romania being the Ministry of Justice. Of course, Romania has also other bilateral instruments with other countries which could become applicable in case of a MLA request in a computer-related case, but we enumerated only those that, from our experience, were actually used in such circumstances.

## **4. PRACTICAL ISSUES AND CASE STUDIES RELATED TO MLA REQUESTS IN CYBERCRIME CASES**

### **a. Requests during the pre-trial investigation**

The Ministry of Justice is not the central authority in cases related to the pre-trial investigation, as previously stated. There are some exceptions from this rule, such as those above-mentioned (e.g the Bilateral Treaty between the USA and Romania which establishes the exclusive competence of the Ministry of Justice regarding any type of mutual assistance request. There are foreign though, that are forwarding their requests to the Ministry of Justice even if the request concerns the pre-trial investigation. Due to this, we are able to present some aspects that were observed by our Division, and which are aimed at completing the input offered by the Prosecutor's Office by the High Court of Cassation and Justice.

The rogatory letters that are transmitted to the Romanian authorities come mostly from Germany, Holland, France, Spain and USA. Romania has sent requests mostly to Germany, Spain, France, Holland, Belgium, Italy, UK, Austria, but also to countries such as Turkey and Cyprus. From outside Europe, Romania has asked the assistance of USA, Canada, China, Singapore, Australia, Israel. The response rate of the foreign authorities is different from country to country. For example, Germany, Austria and France have very high and rapid response rates. Some other countries are offering intermediary responses after 4, 5 months

and it takes several reminders until they are offering a response, whether negative or positive.

The MLA requests of the foreign authorities are processed by the Romanian prosecutors in a period of time that varies on average between 2 and 4 months. Of course, the duration of processing depends on the complexity of the request and the concrete elements. For example, the response to a request in a case of fake Internet auctions on the Internet coming from Cyprus came after 11 months since, due to the fact that the suspect that needed to be heard was not in Romania. In another situation, the German authorities have asked the Romanian prosecutors to hear the authors of a computer-related fraud but they did not know who exactly the defendants were. The response of the Romanian authorities came after 5 months. As regards the type of offences for which the requests are submitted, the majority are related to computer-related fraud and computer-related forgery, illegal access and skimming.

**Case study.** We would like to present a case that required the assistance of several countries from three continents. The request of the Romanian authorities referred to the pre-trial investigation phase and concerned multiple offences of computer related fraud and computer related forgery committed in an organized manner. The total amount of the prejudice was estimated to more than 700 000 euros. Consequently, there were submitted MLA requests for the following countries: Italy, France, Germany, Austria, UK, Russia, Denmark, Belgium, Holland, Poland, Australia and the United States. The requests consisted mainly in hearing the injured parties and asking them if they want to become civil parties in the criminal trial and to choose a legal representative in Romania where they could be subsequently summoned during the trial. The request has been transmitted simultaneously to the above-mentioned countries in September 2007. According to the files which are in the possession of the Directorate International Law and Treaties, the situation is as follows:

- intermediary responses were received from Italy, Australia, Belgium;
- no responses from USA, Russia, Poland;
- Austria responded in two months after the initial request;
- France sent the responses from three courts of appeal in the period January-February 2008;
- Germany had to forward the request to 12 Land Ministries of Justice and up to now 9 Land judicial authorities had replied to the Romanian authorities, some of the responses were received in November and December 2007, others in January, February and March 2008;
- Denmark answered to the request of the Romanian authorities after two months;
- UK transmitted a partial response encountering difficulties in identifying the victims.

This example shows that the practices of different countries differ when relating to assistance in cybercrime cases and so does the terms in which they respond to the request. While for some of them these cases are considered urgent and treated accordingly, others follow different guidelines for determining the priority of each case.

#### **b. Requests of mutual assistance during the trial.**

The following examples of cybercrime cases were presented to us by the Courts of Appeal. It has to be underlined from the very beginning that only some of the Courts of Appeal actually had under their subordination district courts or first instance courts that were discussing cases related to this type of criminality. The references will be related to service of documents which is the most often type of MLA request related to cybercrime that occurred during a trial. According to the rules of the Romanian Criminal Procedural Code,

the effective trial cannot take place unless the parties are legally summoned and the procedure is fulfilled (art.291). Therefore, it is very important for the continuance of the trial to receive the proof of service or a letter stating the impossibility of serving the documents.

1. Cases referring to offences related to infringement of copyright and related rights. There were several cases which had as an object this type of offence. The injured parties were legal persons but summoning the victims did not pose any special problem due to the fact that they have chosen legal representatives in Romania here and the service of documents took place in Romania. It has to be mentioned also that in these cases there was one defendant and only one or two injured parties.
2. Case of illegal access and misuse of devices. The victim was an American citizen and no problems occurred with reference to the mutual legal assistance.
3. Case related to computer related fraud. The injured party was represented by the US Secret Service representative in Romania, so there was no need to follow the whole procedure for summoning the victims through the Department of Justice.
4. Case related to computer-related fraud the service of documents has been solicited to the following states: USA, Canada, , Brazil, Ireland and the Dominican Republic. There were 122 injured parties in the United States, 1 in Ireland, 1 in Brazil, 1 in Canada, 1 in the Dominican Republic. Several international and bilateral treaties were invoked (the European Convention on Mutual Assistance in Criminal Matters, Strasbourg 1959, the bilateral treaties between Romania and the U.S.A and between Romania and Canada, the United Nations Convention Against Transnational Organized Crime). Due to the fact that there were no previous contacts with the Dominican Republic and obviously no bilateral treaty, the request had to be transmitted through diplomatic channels and unfortunately to another South-American Country where Romania had diplomatic representatives. Up to now, only one response was received, from Ireland that returned the documents due to the fact that, being part of Strasbourg 1959, was bound to its provisions, subsequently to the 40 days term which was not respected by the Romanian authorities because of the urgency of the request (the suspects were under provisional arrest, therefore the terms set for the court have to be short so that the procedural provisions related to the duration of the provisional arrest could be complied with). The main problem consists in the fact that because of the provisions of our domestic law if only one proof of service does not return for the specified date, the court has to set another term for the trial.
5. Case related to computer-crime fraud. There are 26 injured parties from Romania (1), United States (18), Netherlands (1), Canada (4), China (2). The file is pending since 2002. Due to the fact that the proof of service of some of the summoning documents never returned, the court was forced to adjourn the case several times, the terms granted being of 6, 7 months each time. This caused a remarkable delay. Special reference was made to the USA in the matter of the long terms for getting the proof the service.

We said before that we will refer to the service of documents, because this is the most often encountered MLA request during the trial. One cannot leave behind though the letters rogatory. Another Court made use of such a request for hearing some witnesses in France. The legal instrument invoked was the EU 2000 Convention, the request had an urgent character and the answer of the French authorities was received in record time that is in 20 days from the initial request.

We wanted to present these examples in order to prove the complexity of such cases and the numerous procedural acts that the Romanian courts and the Ministry of Justice have to transmit/receive as well as the problems that arise from these cases. In those situations when legal persons had to be summoned no special problems occurred. Difficulties interfere related to individuals, especially if in great number.

##### **5. GOOD PRACTICES OF THE MINISTRY OF JUSTICE AS CENTRAL AUTHORITY FOR MLA REQUESTS IN CYBERCRIME CASES. MEANS USED FOR COMMUNICATION.**

As previously said, the last years showed a continued increase of the MLA requests related to cybercrime. Taking into account these developments, the Division for International Judicial Cooperation in Criminal Matters might consider in the near future the necessity to create guidelines for the Romanian courts in this respect. For the time being, there are no such guidelines which refer especially to cybercrime cases. Nevertheless, the Ministry of Justice made available on its website some good practice related to EU Convention 2000 which comprises articles that have direct applicability in computer crime cases.

It has to be mentioned also that the requests related to **pre/trial phases** that are received by the Ministry of Justice are considered urgent requests and are transmitted firstly through expedited means of communication such as fax and email and then send by post.

Referring to the request during the **main proceedings (trial)**, the common procedure is to transmit the request from central authority to central authority by post (namely the Romanian Ministry of Justice to central authority of the requesting/requested state). In case the UE Convention is applicable, the competent Romanian court sends the documentation directly to the competent foreign authority or person (in case of service of documents).

The Ministry made use of expedited means of communication on several occasions when the term established by the competent court was short. The feed/back from the foreign authorities was not always positive. Bounded by the classical conventions and bilateral treaties, many countries refuse to execute the request if the certified copies are not received.

Romania has a national member to EUROJUST and several contact points to the European Judicial Network, among judges and prosecutors and legal advisers from the Ministry of Justice. After the legislative changes that occurred at the end of 2007<sup>1</sup>, it was also introduced the liaison magistrate institution. For the time being Romania, in order to enhance the legal cooperation with Italy, has sent two liaison magistrates there. In the near future several other liaison magistrates will be appointed in other UE member states that have intensive legal cooperation with Romania. All these persons are facilitating the contacts between the Romanian judicial authorities and other states and these channels of communication can be used in cybercrime and we should make full use of them. Human contacts are vital in matters of urgency and experience has showed that appropriate answers can be offered within minutes and not weeks or even months, when there are people involved.

---

<sup>1</sup> See for details the Emergency Ordinance no. 123/2007 regarding some measures for the consolidation of the judicial cooperation with the member-states of the UE.

## 6. POSSIBLE FUTURE STEPS TO BE TAKEN

Our study led to the identification of the following issues:

### 6.1. Traditional means of mutual assistance are not quite effective when referring to cyber offences

From our experience it emerged the fact that authorities from different countries are appealing to different means of communication while waiting for the original documents (that is the requesting state might first send by email or fax the request of mutual assistance and then transmit the certified documentation). Still the arrival of the documents from the requesting state to the executing state might take a long time, even months if we are speaking about service of documents between two countries from two different continents, or as the practical examples showed here countries from 4 continents.

Sometimes the bilateral treaty or the convention is bounding the solicited state to wait for the original documents in order to actually do something about it. Therefore, in our opinion and bearing in mind the good practices offered in the framework of the European Arrest Warrant where email and fax transmissions are considered sufficient and are taken into consideration<sup>2</sup> by the executing member states in the surrender procedure, as a valid and sufficient way to transmit requests of mutual legal assistance, in cybercrime cases could represent a possible solution for sparing a lot of time in cases of service of documents (this situation being encountered mostly during the trial phase) but also during the pre-trial investigation when getting a prompt response to a request of letter rogatory is essential when dealing with sensitive data, as it is happening in computer crime investigations.

Adopting such a solution would follow the provisions of the Convention which states in article 25 paragraph 3 that in urgent circumstances the parties may make use of expedited means of communication such as fax or email, with formal confirmation to follow, where required by the solicited state. The provision refers to urgent cases and as we have seen the urgency could occur not only during the criminal investigations but also during the trial phase. When such a thing happens, transmitting the request by fax or a scanned version of it by email could be the best solution for getting an answer in due time. The principle of mutual trust that stays at the very base of the European Arrest Warrant could be successfully applied in this case as well.

In fact, the Convention of 29 May 2000 is a good step toward this direction as in art. 6 which states that *requests for mutual assistance (...) shall be made in writing, or by any means capable of producing a written record under conditions allowing the receiving Member State to establish its authenticity.*

The Ministry had encountered situations when the rogatory letter and the supplement to the rogatory letter were transmitted by email to the Prosecutor's Office, Cybercrime Unit, still, following the provisions of the bilateral treaty, the certified documents should have been transmitted through the Ministry of Justice and the Ministry had received only the supplement not the original request. Should the email/fax communication have been sufficient, such a delay would have been avoided. Again, the situation of the service of documents to around 130 persons would have been solved in a much easier way if the email/fax would have been accepted in all the countries involved.

---

<sup>2</sup> Art. 10 paragraph 4 of the Framework Decision states that "The issuing judicial authority may forward the European arrest warrant by any secure means capable of producing written records under conditions allowing the executing member state to establish its authenticity

## **6.2. The necessity to create a global network for victims support**

The role of this kind of institution would be to represent the injured parties from country A in country B, circumventing the time consuming and most of the time unsuccessful procedure of service of documents.

It came out from the answers of the courts actually involved in cybercrime cases that in several occasions the foreign victims, in this case American citizens were represented by the US Embassy or the US Secret Service, so there was no need for these persons to be summoned in the United States and a lot of time was saved (we are talking about months, even a year).

Unfortunately the majority of the cases meant victims from more than three countries, sometimes even from three continents, so a unique body having headquarters in as much countries as possible, representing the interests of the injured parties during the trial and keeping them informed about the stage of the proceedings could represent a valid and recommendable solution for the midterm future. This idea is not new as experts have already mentioned the necessity of creating an independent body that would provide advice and assistance to victims<sup>3</sup>, although they were not bearing in mind the problem of the victims' representation during the trials.

## **6.3. Setting up a database with the central authorities responsible for receiving/transmitting the MLA requests.**

From the caseload of the Ministry of Justice, it emerged the fact that many foreign authorities do not know the actual division of competence between the Ministry of Justice (trial and execution of the punishment except as otherwise stipulated in bilateral treaties- e.g the Bilateral Treaty with the United States) and the Prosecutor' Office by the High Court of Cassation and Justice (pre-trial phase).

Also, the Ministry of Justice itself encountered difficulties in identifying ministries from other countries with whom had no cooperation previous to these requests related to cybercrime. It would be quite useful in our opinion if the Council of Europe could provide a database not only with the states that are parties to the Cybercrime Convention, but also with the members of the G8 24/7 contact network.

The contact details should not be reduced to postal address (as mentioned in the declarations to the Conventions applicable) but also the fax, email, and phone of the institutions involved. Following the example of the EJN, there should be nominated judges/prosecutors/policemen/officials from the ministries of justice so that they could facilitate the contact. States that are not parties to the Convention or the 24/7 network should be encouraged to join them in order to assure a greater coverage.

## **6.4. The necessity of updated statistics related to MLA requests in computer crime cases.**

The Division for Judicial Cooperation in criminal matters, due to the increased number of requests related to cybercrime could take into consideration the possibility of keeping records of such cases. For the time being, there are no separate records related to computer crime due to the fact that the Ministry of Justice is not an authority specialized in high-tech crime, consequently receives numerous requests of mutual assistance in criminal matters for a variety of offences.

Still, bearing in mind this type of criminality which has known the last few years such a boom, statistical data would be of utmost importance in establishing with what countries has

---

3

See for example the United Nations Manual on the prevention and control of computer related crime

Romania an enhanced cooperation, what are the difficulties that arise and what solutions might be identified in order to surpass these difficulties.

Additionally, important information about cybercrime cases in general could be obtained from the courts such as the duration of the trial, type of computer crime, the offences committed on regular basis, problems which occur during the instrumentation of the case. These data could be a valuable tool in drawing up specific criminal tools in the field, a step quite foreseeable in the near future. It would be interesting to see if in other countries the courts already have such statistics and if affirmative, to learn from their experience.

The importance of statistics in this field has already been ascertained by the Cybercrime Convention Committee<sup>4</sup> but our little survey comes to strengthen that, showing that courts actually felt in a negative way the lack of such statistics, being very difficult for them to identify the actual number of cases related to cybercrime. The real extent of cybercrime cannot be revealed by the courts caseload, as long as it is well known that the black figure of crime rates very high percentages in this field. But having a glimpse on the legal criminality, on the substantial and procedural issues that the courts have to face when dealing with computer-related crimes, represents at least a starting point in identifying the problems and finding the subsequent solutions.

**6.5. The problem of the prejudice** - Some countries when processing a MLA request are taking into account the value of the prejudice and bearing in mind this criterion they are refusing to execute the MLA requests that are not complying to the rules established in this sense. Unfortunately, this leads to the practical impossibility for the Romanian authorities to complete their investigation/main proceedings in due time.

## 7. CONCLUSIONS

It is obvious that the nature of this type of criminality raises some issues that could not have been foresaw by the persons who actually drafted the applicable Conventions in the matter of mutual legal assistance. Who might have imagined that a single court would have to summon more than 130 persons from four continents in a single case?

It would be advisable for the countries which are parties to the Convention or which are in any case parties of the 24/7 network to reach a consensus or at least agree to some common principles that need to be applied in the matter of mutual legal assistance in cybercrime cases, otherwise the prompt replies offered by some countries in urgent cases (in one of the cases presented the suspects were provisionally arrested, which according to the Romanian law confers an urgent character to the request) are losing their real efficiency due to the *sine die* prolongation of the criminal investigations.

As previously said, when presenting the practical cases, some countries consider the MLA requests related to computer crime as urgent, others do not. The lack of harmonization in this respect is very prejudicial to the trial itself, as our concrete examples had shown. Our internal policy was to consider these kind of requests as having a character of urgency because, although it cannot be compared to terrorism or drug trafficking, cybercrime is a serious offence, especially if committed in an organized manner. The urgency should be considered not only by the country where the offenders are physically located, but also by the country where the victims reside. The damage caused to the victim remains a damage whether of 500 euros or 10 000 euros. Moreover, due to phishing, pharming, Internet fraud, a multitude of victims can be affected, the total prejudice getting to very high figures. These aspects should not be neglected if the slogan *no safe havens for cybercriminals* should

---

<sup>4</sup> See for details the Report undertaken during the 2<sup>nd</sup> Multilateral Consultation of the Parties, Strasbourg 13 and 14 June 2007 available at [www.coe.int/cybercrime](http://www.coe.int/cybercrime)

prove true to life. In this sense, it is not sufficient to harmonize the legislation in the field, but also the procedural aspects referring to the mutual legal assistance.

Our conclusion would be that the need for speeding up the mutual assistance is felt not only during the prosecutorial phase, but also during the actual trial and that states should get to a compromise as regards the requirements, practical aspects and legal issues related to mutual legal assistance related to cybercrime, no matter the legal system they are coming from.



## **SLOVAKIA**

1. It should be noted, that methods, means and tools used by the competent authorities for rendering mutual legal assistance are described in applicable international treaties. In general, the use of direct contacts between the competent authorities as described for instance in the Second Additional Protocol to the European Convention on Mutual Legal Assistance improved the co-operation in urgent cases.

The Slovak Code of Criminal Procedure states following:

### **Article 478**

International treaties

Provisions of this Chapter shall be applied unless an international treaty provides otherwise.

### **Article 479**

#### **Reciprocity**

- (1) If the requesting State is not bound by an international treaty, its request shall only be executed by the Slovak authorities if the requesting State guarantees that it would execute a comparable request submitted by the Slovak authority and it is a kind of a request whose execution is not made in this Chapter conditional upon the existence of an international treaty. If a foreign authority requests the service of documents to a person at the territory of the Slovak Republic the condition laid down in the first sentence is not taken into account.
- (2) If the requested State, which is not bound by an international treaty, makes the execution of the request made by the Slovak authority conditional upon reciprocity, the Ministry of Justice of the Slovak Republic may guarantee reciprocity to the requested State for the purposes of execution of a comparable request should it be made by the requested State provided it is a kind of a request whose execution is not made in this Chapter conditional upon the existence of an international treaty.

### **Article 481**

Protection of the State's interests (Ordre Public)

A request by a foreign authority may not be executed if its execution would be incompatible with the Constitution of the Slovak Republic or a mandatory rule of the law of the Slovak Republic or if by the execution of the request an important protected interest of the Slovak Republic would be violated.

### **Article 483**

Commencement of procedure

Slovak authorities may start acting under this Chapter on the basis of a request by a foreign authority which was transmitted by facsimile or other electronic means, if they have no doubt about its authenticity and if the matter is urgent. The original of the request must be submitted subsequently within the deadline imposed by the requested authority.

### **Article 484**

Communication through INTERPOL and SIRENE

- (1) Incoming or outgoing requests under this Chapter can also be sent through the International Criminal Police Organisation (hereinafter referred to as "INTERPOL"); where such requests concern the states which use the Schengen information system, such communication can also be done through a Sirene Bureau.

- (2) Information on the dates and other modalities of surrender or transit of persons or things under Article 485 may also be exchanged through INTERPOL or Sirene.

In urgent cases 24/7 service of the Interpol Bureau is used (the Interpol, Sirene Bureau and Europol Bureaus created the SPOC –single point of contact). The Interpol Bureau Bratislava has been notified as the contact point for the purposes of the application of Article 35 of the Convention on Cybercrime. It should be noted that the Slovak Republic applies a system of judges and prosecutors on duty. The contact details of judges and prosecutors on duty are available through the Regional Directorates of the Police Corps. Therefore the order or approval from prosecutor or judge, where applicable, can be obtained very quickly. The combination of 24/7 service of the Interpol Bureau and the existence of a mechanism of prosecutors and judges on duty are considered as a very effective way of dealing with urgent cases. The involvement of the European Judicial Network and PC-OC contact points as well as the national members of Eurojust, where applicable, can contribute to the effective and prompt responses and actions in urgent cases if there is a need of any form of judicial co-operation.

There are no particular guidelines available for cyber-crime cases since the Slovak Republic will become the Party to the Convention only from 1 May 2008. No cases of urgent MLA were reported in cybercrime cases so far.

For more details see also declarations of the Slovak Republic to the Convention on Cybercrime.

2. Slovakia has no experience with this particular provision yet. We consider it as one of the most progressive and most difficult provisions. In any case the approval of a competent judicial authority of a “quasi-requested state” shall be obtained.

**SLOVENIA**

1. According to the Slovenian criminal legislation in emergency cases and on condition of reciprocity, requests for legal assistance may be sent through the ministry responsible for internal affairs. If reciprocity applies or if so determined by an international agreement, mutual legal assistance may be exchanged directly between the domestic and foreign bodies participating in the pre-trial procedure and criminal proceedings. In this, modern technical facilities, in particular computer networks and devices for the transmission of pictures, speech and electronic impulses may be used. Translation is needed if provisions of the international agreement used as a legal basis for the request for mutual legal assistance determinate so, taking into the consideration also possible declarations regarding translation of documents.

The Republic of Slovenia has not yet received or sent any request for mutual legal assistance based on the Convention on Cybercrime or based on any other international treaty that would have to be treated as an urgent computer-related case.

2. Considering the fact that the Convention on Cybercrime has not yet been applied in practice within our competent authorities Slovenia can not provide any concrete answer about the application of the Article 32 b.

Referring to the general principle of the Slovenian Constitution that ratified and published treaties shall be applied directly and considering the fact that there are no special provisions in the Slovenian criminal legislation about the content mentioned in Article 32 b of the Convention on Cybercrime Slovenia at this point has no doubt that Article 32 b could be within our jurisdiction/competent authorities applied directly, taking into the consideration also the national and international law on data protection.

## SUISSE

1. D'une manière générale, le droit suisse permet aux autorités de prendre les mesures provisoires nécessaires à garantir la bonne exécution d'une demande d'entraide à venir. Dans la pratique, les mesures provisoires peuvent être ordonnées extrêmement rapidement (quelques heures ou jours), dès l'annonce d'une demande d'entraide. Aucune forme particulière ni voie de transmission particulière n'est exigée à ce stade. La demande de mesures provisoires peut être présentée en français, allemand, italien, voire en anglais. L'autorité suisse qui prononce les mesures provisoires fixe ensuite un délai à l'autorité requérante pour présenter une demande en bonne et due forme, à défaut de quoi les mesures provisoires prononcées deviendront caduques.

S'agissant de l'accès aux données, le droit suisse prévoit qu'un certain nombre d'informations sont accessibles par la voie de police. Il en est ainsi en particulier de l'identification de l'abonné utilisant une adresse IP suisse. Pour d'autres types de données, il est conseillé de s'adresser à l'OFJ.

2. La Suisse n'a pas encore ratifié la Convention.

\* \* \*

**SWEDEN**

1. The Swedish Act on International Legal Assistance in Criminal Matters states that;

- A request from a state that is a Member of the European Union or from Iceland, Norway or Switzerland may be made directly to a competent prosecutor or court. This also applies if it in an international agreement that is binding on Sweden has been agreed that a request may be made directly.
- If the foreign authority so requests, the prosecutor or district court that is handling the matter shall acknowledge receipt of the request, unless the measure requested can be taken immediately.
- Requests for legal assistance shall be executed promptly
- If a measure requested can not be taken within the time limit stated in the request and if it can be assumed that this will impair the proceedings in the requesting state, the prosecutor or the district court that is handling the matter shall, promptly, notify the foreign authority of when it will be possible to take the measure requested.
- If the request contains a request of a particular procedure, this shall be applied, if it does not conflict with the fundamental principles of the Swedish legal system.
- In particular cases the instance responsible for executing a request can decide not to apply the main rule that a request for legal assistance and enclosed documents shall be written in Swedish, Danish or Norwegian or be accompanied by a translation into one of these languages.

2. Sweden is not a Party to the Convention on Cybercrime.