

Online Investigations: darknet and online sexual violence against children

Overview of current practices on obtaining evidence from other countries and the role of the 24/7 PoC

Rajka VLAHOVIC and Christian AGHROUM

Council of Europe Expert

30th September – 1st October 2019
The Hague, The Netherlands

2. Obtaining evidence from other countries & the role of the 24/7 PoC

- This presentation considers and comments provisions of the Budapest Convention which support the obtaining of evidence from other jurisdictions other than through the use of MLA
 - Convention Article 32 – Transborder access to data,
 - an extra-territorial provision which operates independently of MLA.
 - Convention Article 35 – 24/7 Network
 - provision of immediate assistance in relation to computer related offences and in the obtaining of e evidence.
 - Convention Article 26 – Spontaneous information
 - supports sharing of information and can facilitate investigations and stimulate MLA requests

3. Obtaining evidence from other countries & the role of the 24/7 PoC

- Article 32 Budapest Convention – Trans-border access to stored computer data or where publicly available:
 - A Party may without the authorisation of another Party:
 - (a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
 - (b) access or receive, through a computer system in its territory, stored computer data located in another Party if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.
- Background, purpose of A 32 – Explanatory Report;
 - A compromise provision based on agreement of drafters of the Convention that there may be instances where it may be acceptable for Parties to act unilaterally,
 - Insufficient concrete experience at the time to prepare a comprehensive legally binding regime,
 - understanding that the solution often depended on the precise circumstances of the individual case,
 - drafters therefore agreed to set out situations in A 32 situations in which there was agreement that unilateral action was permissible,
 - agreed not to regulate other situations until further experience gathered,
 - therefore other situations are neither authorised nor precluded (A39 (3)).

4. Obtaining evidence from other countries & the role of the 24/7 PoC

- Two permissible situations in A 32
 - (a) that LE officials may access any data that the public may access understanding that if a portion of the website is closed to the public it is not publicly available ,
 - (b) is considered more controversial and raises a number of issues in particular the question of lawful authority to disclose data.
- Article 32 (b) was re-visited in Guidance Note #3 (endorsed by T-CY in 2013) and envisaged two concrete situations where Article 32(b) might apply:
 - (1) a person's email may be stored in another country by a service provider or a person may store, perhaps intentionally data in another country. These persons may retrieve the data and provided they have lawful authority, may disclose or allow access to LE.
 - (2) a suspected drug trafficker is arrested in possession of his device which may contain evidence of a crime. If the suspect consents to allow access to LE and LE believe the data is located in another Party to the Convention, then LE may access data under para (b).

5. Obtaining evidence from other countries & the role of the 24/7 PoC

- It is assumed that A 32 (b) operates as between the Parties based on common understandings that:
 - Article 32 (b) is to be applied to specific investigations in line with A 14,
 - Parties to the Convention form a community of trust respecting human rights and rule of law,
 - measure applies as between the Parties, if data is not stored in another Party or there is uncertainty about this, the circumstances do not fall within A 32 (b),
 - A 32(b) neither authorises nor precludes other situations – Parties may need to evaluate the legitimacy of search or access in line with international law principles,
 - notification is not required, Parties may notify each other if appropriate,
 - consent given must be lawful and voluntary (note restrictions in national law e.g. relating to minors, explicit consent for cooperation in criminal investigation) ,
 - domestic standards apply,
 - who is lawfully authorised? – an individual providing access to own data stored abroad or an individual, SPs may not be able to consent in the absence of an MLA request and subsequent order to produce the data,
 - A 32(b) is not relevant to domestic production orders,
 - where is the person giving access located? assumed that person is in requesting Party but may also be in a third country and represented in requesting Party. Some Parties may object to persons in their territory being approached directly by foreign LE.

6. Obtaining evidence from other countries & the role of the 24/7 PoC

- In practice;
 - little evidence of successful use of A 32 (b),
 - Instead national solutions formulated to deal with the 2nd situation envisaged in Guidance Note #3 e.g arrested person can commit an additional offence by not providing LE with a password enabling access to data stored on a device in his possession,
 - more recently other unilateral initiatives including the issuance of extra territorial warrants or, the issuance of technical assistance order on extra-territorially located service providers (Australia)
- The Cloud Evidence Group (CEG) final report endorsed by T-CY in 2017;
 - CEG concluded that A 32 (b) currently offers only very limited possibilities,
 - It does not address situations involving multiple SPs and jurisdictions or where it is not feasible to identify the location of a criminal act,
 - CEG noted that states would increasingly pursue unilateral solutions,
 - but that a re-negotiation of the trans-border cooperation provision would not be realistic in the then current climate,
 - however, an international framework relating to the exercise of the existing A 32 with safeguards was both desirable and necessary to prevent possible rogue assertions of jurisdiction,
 - such framework currently being discussed within the framework of 2nd Additional Protocol

7. Obtaining evidence from other countries and the role of the 24/7 PoC

- Article 35 Budapest Convention – 24/7 Network
 - (1) requires Parties to designate a 24/7 PoC to ensure the provision of **immediate assistance** for the purposes of investigations or proceedings concerning criminal offences relating to computer systems and data or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include **facilitating** or, if permitted by domestic law and practice, **directly carrying out** the following measures:
 - (a) the **provision** of technical advice ,
 - (b) the **preservation** of data pursuant to A 29 and 30,
 - (c) the **collection of evidence**, the provision of legal information and locating of suspects,
 - 2(a) A Party's PoC shall have the capacity to **communicate** with the PoC of another Party on an expedited basis,
 - (b) if a Party's PoC is not part of that Party's authority for MLA or extradition then that Party should ensure that it is able to **co-ordinate** with such authorities on an expedited basis,
 - 3. each Party shall ensure that **trained equipped personnel** are available to facilitate the operation of the Network.

8. Obtaining evidence from other countries & the role of the 24/7 PoC

– Purpose of the Network;

- Network considered amongst the most important means provided by the Convention ensuring that Parties can respond effectively to challenges posed by computer (related crime),
- PoC responsibilities are set out in para 1 (a) – (c),
- for Party to decide where the PoC should be located (MLA authorities, police or other),
- PoC tasks are set out in para 2 and essentially consist of coordination with ones own authorities and communicating with other Party's PoCs on an expedited basis,
- para 3 requires that PoCs have appropriate resources and training.

– Relevant reviews of the Network

- The functioning of 24/7 PoCs for cybercrime – CoE Economic Crime Division 2009,
- T-CY Assessment Report on International Cooperation, 2014,
- Concept note on 24/7 PoCs Project Cybercrime@EAPII, 2016.

– Issues arising

- accepted that most PoCs are able to provide technical advice (A 35 1 (a)) and to communicate directly with other PoCs on an expedited basis (A35 2 (a)) but issues identified in relation to other responsibilities;
- A 35 1 (b) responsibility for requesting or acting on preservation requests – sometimes compromised through either lack of legislation or lack of power.

9. Obtaining evidence from other countries and the role of the 24/7 PoC

- response has been to amend national arrangements so that this can work or, alternatively appointing additional PoCs in prosecution services who do have the requisite powers,
 - preservation template developed to assist the process.
- A35 1 (c) collection of evidence - sometimes compromised by PoCs lack of capacity or power to do this,
 - response has been to appoint additional contact points with investigative responsibilities or in some cases security services,
- A35 2 (b) coordination with MLA authorities – in some cases suggestions that PoCs are not well known to their own authorities and cooperation with MLA authorities is limited,
 - these suggestions have given rise to the call for better integration between MLA authorities and PoCs in combination with a greater role for PoCs in MLA and for better links to be established between preservation requests and MLA requests.
- A 35 (3) training and resources – ongoing issue (training provided by C-Proc through various projects).
- Strengthening of the Network – discussions on providing a national legal basis have given rise to different views. On the other hand Network is now better organised since regular meetings started in 2017.

24/7 Network

Christian AGHROUM



You are here: Cybercrime > Resources

International Cooperation against Cybercrime



Cybercrime is very much transnational crime. **Urgent measures** that are needed to preserve data at the national level are also necessary within the framework of international co-operation.

Chapter III of the **Convention on Cybercrime** provides a legal framework for international cooperation with general and specific measures, including the obligation of countries to cooperate to the widest extent possible, urgent measures to preserve data and efficient mutual legal assistance.

- ▶ [Overview of the international cooperation provisions of the Convention](#)
- ▶ List of competent authorities for judicial cooperation and 24/7 points of contact
- ▶ About 24/7 points of contact

The Convention on Cybercrime is complemented by a wide range of other treaties of the Council of Europe on international cooperation in criminal matters (see Transnational Criminal Justice).

m.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304352



Protecting You and Your Rights in Cyberspace

CONTACT US

10. Obtaining evidence from other countries and the role of the 24/7 PoC

- Article 26 Budapest Convention – spontaneous information;
 - enables a Party to forward to another Party, within limits of domestic law, information from own investigations when it considers that such information may assist the receiving Party in initiating or carrying out relevant investigations,
 - the Party providing the information may make the provision of the information subject to confidentiality and other conditions, the receiving Party is to notify the providing Party if it can comply with these, the providing Party then takes the decision whether or not to provide the information.
- Background and purpose;
 - provision derives from earlier CoE instruments and enables a Party in possession of valuable information to provide it to another Party which is not aware of its existence,
 - Included because in some states a positive legal basis is required to disclose such information.
- T-CY Assessment Report;
 - found that this is a useful provision which can stimulate investigations and MLA requests,
 - but noted little use of the provision.



Eurojust – CoE / Glacy +

- Necessity
- To act quickly
- To research evidences
- To keep evidences
- During a small part of time
- Issues
- Evidences around the world
- Difficulty to maintain them on darknet websites
- Many countries do not response
 - Lack of legislation
 - Lac of willing
 - Lack of knowledge
 - Corruption



Eurojust – CoE / Glacy +

Official



- Border exchanges :
commissariats
transfrontaliers (EU)
- Regional level : EU / West
Africa / ASEAN
- International level : Interpol

Non-official

- Same levels
- Associations (IPA / Francopol
/ Gendarmeries ...)
- Friendship networks
- Direct access

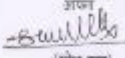
Cybercrime : new context : PPP
More and more NGO or private organisations

Making cooperation more efficient - standardization of Police requests



सुरेश लाड
 असपर, अहमदनगर

श्री,
 प्रा. मिलिंद सोहनो
 आय आय टी, मुंबई

अभिनंदन पत्र !
 आय आय टी ने गैरकायदा वसाहत करणे, वि-गणित वास्तुविकास
 मता प्रमोदपत्रात विषयाव्वा धरण्या वान सोडवणेव्वा अनुभवने विशिष्ट व
 दिग्दर्शने कार्यरत घाला सहकार्यने फलदायक प्रत्यय लया केला आहे हे खूप
 कौतुकामय आहे.
 आम्ही मनापूर्वक आभारदा

अणन

 (सुरेश लाड)
 विधानसभे माया
 कलता

*सोहो अख्यत विद्या, जे-५५, मुंबई, मः २२८५४१५५
 विद्याः मु.पं. वलिकरी, ता. वलिकरी, जि. तालुक, वि.प. ४१० २०१. मः ०२५४८-२२२३१५


深圳市人民政府外事办公室

邀请确认函
 Confirmation Letter of Invitation

编号/ No.: 1501-1103-0906
 中华人民共和国驻 三都县总领事馆 (总领馆 / 领事馆 / 总) 或
 中华人民共和国外交部驻 三都县总领事馆 (总领馆 / 领事馆 / 总)
 The Embassy (Consulate General) (Consular Office) of the P.R. of China, PAKISTAN, in the
 Consulate's Office of the Foreign Ministry of the P.R. of China (总领馆 / 领事馆 / 总)

兹确认 深圳市登田五金制品有限公司 (邀请单位名称)
 邀请的 AHMAD NAFFEM NASIR (姓名) 等 1 人将于
 2015.04.14 (入境时间) 来华, 停留 25 天, 从事 商务考察学
 习 等活动, 留申请 1 个月有效 1 次入境签证,
 邀请人员名单附后。

At this certified and certified confirm that AHMAD NAFFEM NASIR
 (AHMAD NAFFEM NASIR) (NAME) (NAME) (NAME) (NAME) (NAME)
 will come to China on 2015.04.14, and stay for 25 days for Business
 and study activities, and will apply 1 time for valid visa for 1 month. Name list of the
 invitee enclosed.

邀请单位联系人: 王瑞霞 联系电话: 17691355
 Contact Person of the Company Tel.

被邀请单位名称: 深圳市人民政府外事办公室
 Name of the Invited Unit:

联系人: 陈泽斌 联系电话: 0755-82135509
 Contact Person Tel.

被邀请单位名称及负责人签署
 Name of the Invited Unit and Signature

(深圳市人民政府外事办公室)
 2015年03月28日
 Date of Issue

注: 1. 邀请单位须提供邀请单位盖章或一起盖章。
 2. 邀请单位负责人或邀请单位负责人须亲笔签名。
 Note: 1. Please present this letter together with the invitation letter and the company's official seal.
 2. Please present the name list of the invitee on separate paper with seal of the invitee.


PREFECTURE DE POLICE
 DIRECTION DE LA POLICE JUDICIAIRE

Brigade de Répression de la Délinquance contre la Personne
 100-126 rue du Château des Renards 75013 PARIS
 Tél. : 01 56 79 24 56 / Fax : 01 56 79 22 04

2015/01006 PARIS (19), le 7 janvier 2015

REQUISITION JUDICIAIRE

Nous, _____
 Chef de la 1^{ère} Division de Police Judiciaire
 en fonction à la P.J.P.

Agissant en vertu et pour l'attribution de la Commission Régionale n° _____ créée le 23
 novembre 2015 par Monsieur Yves MADRE, Premier Juge d'instruction au Tribunal de Grande
 Instance de PARIS, dans le cadre d'une information contre X, cas d'atteinte de diffusion publique
 envers un particulier, et de diffusion d'un contenu nuisible, suite à une plainte avec
 constitution de partie civile déposée par le social COCO DESIGN DDA (CNRS) par le procureur
 GUYARD, par Monsieur Damien GUYOT, et par Monsieur Rudy HAI (CNRS).

Vu les articles 51, 15° et suivants du Code de Procédure Pénale,

Présenter au dossier réquisitoire :
Monsieur Alain DONNET de SONAL
Président de l'association « Egalité et Réconciliation »
 2 rue du Ton de la Biche 93200 SAINT DENIS
 et toute personne par lui désignée.

A l'effet de passer aux actes suivants :

- Vous fournir la date de publication de l'article initial et une copie actualisée de la dernière
 écopartie sur une feuille A4 (voir 150° de la loi) - URL: <http://www.egalite-reconciliation.fr> (voir 100° de la loi) (voir 98/91/111).
- Vous communiquer l'identité complète du directeur de votre site internet
 (personnel les commentaires) ainsi que les chiffres de diffusion du contenu nuisible.
- Vous communiquer l'identité complète de l'auteur de l'article visé ci-dessus, nom,
 prénom, date et lieu de naissance, filiation, nationalité, adresse personnelle.
- Vous me transmettre le principe de modération que en vigueur sur votre site internet
 (personnel les commentaires) ainsi que les chiffres de diffusion du contenu nuisible.
- Vous communiquer tous les éléments permettant l'identification des internautes utilisant
 les fonctionnalités sociales (e-mail, ip, url, adresse, cookie, adresse personnelle, etc.)
 (selon l'Age et l'Opinionnaire). C'est-à-dire, sans le tenir, Chèque d'ITV, etc., lorsque
 possible, avec inscription. Références.



Law Enforcement



Request Access



Email

Enter your email address to receive a unique link to the Law Enforcement Online Request System. The link will give you access to the system for one hour.

Cancel

Submit

Request Secure Access to the Law Enforcement Online Request System

We disclose account records solely in accordance with our terms of service and applicable law.

If you are a law enforcement agent who is authorized to gather evidence in connection with an official investigation, you may request records from Facebook through this system.

I am an authorized law enforcement agent and this is an official request

Request Access

Warning: Requests to Facebook through this system may be made only by governmental entities authorized to obtain evidence in connection with official legal proceedings pursuant to Title 18, United States Code, Sections 2703 and 2711. Unauthorized requests will be subject to prosecution. By requesting access you are acknowledging that you are a government official making a request in official capacity. For further information please review the [Law Enforcement Guidelines](#).

An opportunity for investigators

24/7 network



Article 35

- **Obligation to create a permanently available contact point**
 - a so called *24/7 network* of contact points
- **General objectives of these contact points**
 - to facilitate international co-operation
 - giving technical advisory to other contact points
 - activating the proper mechanism to expedited preservation of data
 - urgently collecting evidence
 - identifying and discovering suspects



24/7 Contact Points

- Operational network of experts on high-tech criminality
- Provide help and cooperation very quickly even if a formal cooperation request must follow this informal way
- One single point of contact for each country, available 24 hours a day, 7 days a week
- Direct communications between the points
- Mainly planned to provide the possibility to immediately preserve traffic data and other stored data worldwide



24/7 Contact Points

- Most of the contact points are police based contact points
- Some of them are Prosecution Services contact points
- Budapest Convention provided a legal basis to the 24/7 network of contact points, that are recognised as one of the most useful tools regarding international cooperation



24/7 Contact Points

- Interest for countries
 - To live inquiries at the same or practically same speed than internet
 - To “clean their own garden”
 - To have a national overview of their inquiries and to avoid doubles
 - To get reciprocity



GLACY+

Global Action on Cybercrime Extended
Action globale sur la cybercriminalité élargie

Funded
by the European Union
and the Council of Europe



Implemented
by the Council of Europe

THANK YOU

questions and comments

Cybercrime Programme Office (C-PROC)
Bucharest - Romania