ECPAT International

Council of Europe Octopus Conference on Cybercrime

December 2013

Background information about ECPAT International

ECPAT International is the leading global network of organisations dedicated to stopping the commercial sexual exploitation of children (CSEC). Today, the network is comprised of an International Secretariat based in Thailand, together with 81 local member organisations in 74 countries.

ECPAT works closely with the ECPAT member organizations and other stakeholders (the Committee on the Rights of the Child, the Human Rights Council, Special rapporteurs, Council of Europe, EU and other regional HR monitoring mechanisms (e.g. SAARC, African Union) UN agencies, INGOs, NGOs, private sector, law enforcement agencies and national governments) to lobby for the ratification of relevant international and regional legal standards (international: CRC, OPSC, Trafficking Protocol, ILO Convention 182 – regional standards : CoE Conventions addressing CSEC and trafficking), for the harmonization of national laws according to international standards, and for the effective implementation and enforcement of existing laws.

Website: www.ecpat.net

The commercial sexual exploitation of children

ECPAT International focuses on four major manifestations of CSEC: prostitution, trafficking, exploitation in travel and tourism, as well as child pornography and exploitation on-line. There are significant interrelations between these major CSEC manifestations, for example some children are trafficked to tourist destinations where they are provided for prostitution to travelling sex offenders who in turn may make images or videos of their abuse. In addition to previously undertaken research on these linkages identifying appropriate prevention strategies[1], ECPAT maintains an awareness not only of how they are evolving, but also of emerging manifestations and areas of vulnerability, for example in situations of humanitarian crisis and natural disasters.

[1] Pimonsaengsuriya, K. (2008), Understanding the linkages between child sex tourism and other forms of commercial sexual exploitation of children in East Asia and the Pacific, ECPAT International,

Status of harmonisation of domestic legal frameworks with Budapest and Lanzarote Conventions

INTRODUCTION

The Council of Europe has played a key role with regard to the development of comprehensive regional legal standards aimed at protecting children against all forms of commercial sexual exploitation and which complements standards set forth in the Convention on the Rights of the Child and the Optional Protocol on the sale of children, child prostitution and child pornography (OPSC).

In 2007, the Council of Europe adopted the Convention on the Protection of Children against Sexual Exploitation and Abuse (Lanzarote Convention), which entered into force in 2010.[2] This Convention provides a robust legal framework against CSEC which address new trends in CSEC such as the online real-time viewing of child pornography, or the intentional access to child pornography materials through the use of information and communication technologies and the solicitation of children through the use of information and communication technologies for sexual purposes (*grooming*).

Such manifestations of CSEC are not included in the OPSC which was adopted in 2000, at a time when information and communication technologies were less developed than today and when the risk of children being sexually exploited through the use of information and communication technologies, although not non-existent, was minimal.

The Lanzarote Convention focuses on substantive criminal law which means that it defines all CSEC related crimes, criminalises all conducts related to CSEC crimes and provides for specific measures for the care and protection of child victims.

The Lanzarote Convention has been ratified by 29 Council of Europe member States[3] and is open for accession by non-member states.

In 2001, the Council of Europe adopted the Convention on Cybercrime (Budapest Convention) which contains specific provisions addressing child pornography. However, the main focus of this Convention is procedural criminal law which means that it establishes legal measures which ensure that investigations and criminal proceedings are carried out in the best interests and respecting the rights of the child.

The Budapest Convention has been ratified by **36** CoE member states[4] and **5** non-CoE member states[5]:

[2] Council of Europe (2007). Convention on the Protection of Children against Sexual Exploitation and Abuse. Accessible at: http://conventions.coe.int/Treaty/EN/treaties/Html/201.htm

[3] Chart of signatures and ratifications – Budapest Convention: http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=22/11/2013&CL=ENG

[4] Chart of signatures and ratifications – Lanzarote Convention: http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=201&CM=8&DF=22/11/2013&CL=ENG

[5] Australia, Dominican Republic, Japan, Mauritius and the USA

By ratifying those two Conventions, State parties have committed to harmonise their legal framework with the provisions of the Conventions and to implement revised legislation effectively. In countries which are not member states of the Council of Europe, the Convention can be used as a benchmark legal framework for strengthening national laws addressing CSEC.

The Octopus Interface conference is organized by the Council of Europe under the Global Project on Cybercrime and aims at building capacity of law makers, implementation of the Budapest Convention, and sharing of good practices and information related to key trends and threats related to cybercrime. It also helps in developing strategies and policies to combat this evolving form of cybercrime and provides important information to member states not only belonging to the Council of Europe but from non member states including those outside of Europe. Protecting children from sexual exploitation and abuse forms a key part of the theme of the conference each year and targeted workshops are arranged to address this issue.

The Council of Europe also organsied a workshop on *Protecting children against online sexual violence in South-East Asia* which took place in May 2013 in Manila and was co-organized by the Department of Justice of the Philippines.

The objective of the conference was to to promote the implementation of the criminal law benchmarks of the Budapest and Lanzarote Conventions as a basis for enhanced law enforcement cooperation to protect children against sexual violence.

The workshop targeted the 10 ASEAN member states and expected to produce analysis of legislation of participating countries in terms of their consistency with the Budapest Convention on Cybercrime and Lanzarote Conventions; and also better exchange of experience based on case studies, on procedures, and legal and other conditions for enhanced law enforcement operations.

As a follow up to this Council of Europe regional workshop, ECPAT International will provide an updated analysis of the harmonization of domestic legislation addressing child pornography and the sexual exploitation of children online with standards set forth in the Lanzarote and Budapest Conventions.
This analysis is mainly based on information contained in ECPAT International 2nd Edition monitoring reports on the status of action against commercial sexual exploitation of children which were presented to the Lanzarote Committee during its 4th meeting (March 2013) as a key resource in relation to the development of the Committee discussion paper on "*Protecting children against sexual violence: the criminal law benchmarks of the Lanzarote and Budapest Conventions*".

For the purpose of this presentation we have not restricted the analysis of the harmonisation of domestic legislation with the Budapest and Lanzarote Conventions to CoE Member States which have ratified the Conventions. The scope of the analysis covers 21 Council of Europe Member States where ECPAT has a presence. Both Conventions should be considered by States which have not ratified them yet as model laws for improving their national laws addressing child pornography and child sexual exploitation online.

As a specific follow up to Recommendation Number 3[6] of the Manila Regional Workshop, ECPAT will provide an analysis of the consistency of the 10 ASEAN Member States'[7] national laws addressing child pornography and child sexual exploitation online with the provisions of the Lanzarote and Budapest Conventions.

1. Status of harmonization of domestic legal frameworks with the Lanzarote Convention

ECPAT International has conducted a mapping on the compliance of domestic laws in 21 Council of Europe Member States[8] where ECPAT has a presence. This mapping is mainly based on the 2nd edition of ECPAT International's monitoring report on the status of action against commercial sexual exploitation of children[9].

This mapping exercise focused on the definition of each manifestation of CSEC and the criminalization of conduct relating to those CSEC manifestations. For the purpose of this presentation ECPAT will focus on information relating to child pornography and child sexual exploitation online.

In Council of Europe Member States

- Definition

A clear and comprehensive legal definition of child pornography, consistent with standards set forth in relevant international and regional legal instruments, is the cornerstone of substantive criminal law aimed at protecting children from sexual offenders willing to sexually exploit them online or through the production and dissemination of child pornography.

Article 20-2 of the Lanzarote Convention defines child pornography as: "*Any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes.*"

The study conducted by ECPAT revealed that out of the 21 reviewed countries, only 8 Council of Europe Member States[10] have enacted legal provisions which define child pornography in compliance with Article 20-2 of the Lanzarote Convention.

Some countries like Albania, Belgium, and Poland do not have any definition of child pornography.

---

[6] Rec. 3: *CoE to complement benchmark study with information on legislation of ASEAN countries (for discussion at Octopus Conference 4-6 December 2013).*

[7] ASEAN (Association of Southeast Nations) Member States: Brunei; Cambodia; Indonesia; Laos; Malaysia; Myanmar; Philippines; Thailand; Singapore; Vietnam.

[8] Albania; Austria; Belgium; Bulgaria; Czech Republic; Estonia; France; Germany; Italy; Luxembourg; Moldova; Netherlands; Poland; Romania; Spain ; Sweden; Switzerland; Russia; Turkey; Ukraine and the UK.

[9] ECPAT International, 2nd Edition Monitoring reports on the status of action against commercial sexual exploitation of children. Accessible at: http://resources.ecpat.net/EI/index_A4A.asp

[10] Bulgaria; Luxembourg; Moldova; Netherlands; Switzerland; Sweden; Ukraine and UK.

- Criminalisation of conduct relating to child pornography

Those types of conduct are listed by Article 20-1 of the Lanzarote Convention:

- producing
- offering
- distributing or transmitting
- procuring
- possessing
- knowingly obtaining access, through information and communication technologies, to child pornography.

Compared to the Optional Protocol, the CoE Convention extends the legal protection framework of children from exploitation in pornography by providing for a number of additional conducts that Member States should consider punishing including knowingly obtaining access, through information and communication technologies, to child pornography.

The mapping conducted by ECPAT International shows that out of the 21 reviewed states, only 7[11] have established comprehensive legal provisions which criminalise all of the above mentioned forms of conduct.

However, Bulgarian, Italian, Romanian and Ukrainian legislations are quite robust as they only fail to criminalise knowingly obtaining access, through information and communication technologies, to child pornography.
Knowingly obtaining access, through information and communication technologies, to child pornography is not yet criminalised in 11 out of the 21 reviewed Council of Europe Member States [12].
Those countries should make efforts in criminalising knowingly obtaining access, through information and communication technologies,
to child pornography as such a legal gaps encourages child sex offenders to sexually exploit children online in total impunity.

Children are increasingly using the online platforms and being lured through the different social media and chat services that allow the offenders to interact with them. In this context lack of laws criminialising grooming offences is an urgent gap that needs to be addressed.
Compared to the OPSC, the Lanzarote Convention extends the legal protection framework of children by criminalising the solicitation of the solicitation of children fro sexual purposes (grooming).

Article 23 of the Lanzarote Convention criminalises the online solicitation of children online for sexual purposes (child grooming).

[11] Belgium; France; Germany; Luxembourg; Netherlands; Sweden; and UK.
[12] Albania; Austria; Bulgaria; Czech Republic; Estonia; Italy; Moldova; Poland; Russia; Spain; Switzerland; Turkey; and Ukraine.

According to the ECPAT mapping, out of the 16 reviewed states, 11 CoE Member States[13] have enacted legal provisions criminalizing child grooming.

In ASEAN (Association of Southeast Asian Nations) Member States[14]

- Definition of child pornography

Among the 10 ASEAN member states, the Philippines is the only state that has adopted a definition of child pornography which is compliant with Article 20-2 of the Lanzarote Convention:

The Philippines Anti Child Pornography Act Section 3 defines child pornography as: "*any representation, whether visual, audio or written or a combination thereof, by electronic, magnetic, optical or any other means of a child engaged or involved in real or simulated sexual activities*"

The definition contained in the Cambodian Penal Code is only partially compliant as it does not cover the depiction of a child's sexual organs for primarily sexual purposes:

Article 40 of the Cambodian penal Code: "*Child pornography' in this law shall mean a visible material such as a photograph or videotape, including a material in electronic form, depicting a minor's naked figure which excites or stimulates sexual desire*".

Brunei, Indonesia, Malaysia, Myanmar, Singapore and Thailand still use "obscenity laws" to prosecute cases of child pornography. This means that none of these states have an adequate definition of child pornography in their legislation.

The terms "obscene" or "indecent" materials which are mentioned in the provisions of the criminal codes of the above mentioned countries are very broad and subject to various interpretations by law enforcement officials and may result in inadequate sentencing.

- criminalisation of conduct relating to child pornography

With regard to the criminalization of conduct relating to child pornography, none of the ASEAN member states fully comply with the requirements of the Lanzarote Convention.

However, The Philippines has strong laws which encompass knowingly accessing child pornography through the use of ICTs and child grooming. The only gap is the prohibition of mere possession of child pornography.

[13] Austria, Bulgaria, France, Germany, Netherlands, Poland, Romania, Spain, Sweden, UK.
[14] Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Thailand, Singapore, Vietnam

The Philippines is the only country in the ASEAN region to criminalise knowingly accessing child pornography through the use of ICTs

The online solicitation of children for sexual purposes (child grooming) is criminalised only in 2 countries: The Philippines and Singapore.

Recommendations in relation to the Lanzarote Convention

- Council of Europe Member States should make more efforts in ratifying the Lanzarote Convention and accelerate the harmonisation process of their domestic legal frameworks with the provisions of the Convention.

- The emergence of phenomenon such as live streaming of child sexual abuse based on demand, where an offender can direct and view live steams of child sexual abuse online without having to download or store the material in their computers, raises the need for adequate legislation criminalizing knowingly accessing child pornography through the use of ICTs.

- With an increase in the use of ICTs by children and young people, legal provisions should be in place in an increased number of States to prohibit the solicitation of children online for sexual purposes.

2. Status of harmonization of domestic legal frameworks with the Budapest Convention

ECPAT's mapping exercise was limited to an analysis of the substantive criminal laws as indicated within the Lanzarote Convention section above. However, it is important to highlight the need for suitable procedural laws to address investigations related to child pornography, as much of this revolves around investigating digital content that is distributed through computer networks.

While Article 9 of the Budapest Convention covers the substantive criminal laws related to child pornography, sections 16-21 provide clear guidance and practical measures to law enforcement officers in carrying out investigations.

Procedural laws are needed for:

- Handling digital evidence in a way that can be presented in the courts and accepted as evidence by the court;
- Defining the role of relevant law enforcement authorities who can investigate cybercrime cases. Without proper assignment of roles and responsibilities and identifying competent officers for such roles, it might create confusion amongst different law enforcement agencies as to who should take charge in the online investigations. Often the State defines a specific division or technical branch within the law enforcement to carry out such investigations;
- Defining rules regarding search & seizure of such digital evidence;

- Addressing rapidness of communication and trans-border issues. Unless clear procedures are defined for cross border collaboration, the methods and procedures for such exchange of information cannot take place systematically and with consistency. Moreover countries should harmonise practices and adopt standard international practices for such information exchanges.

These procedural laws enable consistency in global law enforcement and create a framework for cooperation on digital investigative methods.

Key considerations as outlined by the Council of Europe Cybercrime Convention

The Council of Europe Cybercrime Convention sets out some key criteria related to investigation of cybercrimes that are relevant to dealing with child pornography.

These are crucial elements that need to be incorporated into national procedural laws for cybercrime related investigations:

- To ensure that the technical nature of cybercrime and its prevention is given focus and considering the procedures involved for international cooperation, law enforcement authorities specifically the computer or technology crime divisions or units responsible for the investigation of cybercrimes are required to be clearly identified and assigned clear roles.

- Data collection, recording, preservation, and disclosure, play a crucial role in digital forensic and online investigation. Search, seizure and examination of computer data are also important elements of the investigation process. Procedural laws guide law enforcement officers in carrying out such tasks and are an integral part of any cybercrime legal framework.

The CoE Cybercrime Convention provides guidelines and a framework for devising such laws and procedural measures.

Important elements for carrying out cybercrime investigations, particularly those involving digital child pornography and related criminal activities online are:

- Admissibility of electronic evidence
- Need for identifying relevant authorities for carrying out expeditious preservation of specified computer data

Defining duties of law enforcement authorities to carry out :

- Expedited preservation
- Search and seizure
- Interception
- International co-operation

Article 14.2.C of the Budapest Convention requires State Parties to adopt legislative and other measures related to the admissibility of the collection of evidence in electronic form of a criminal offence and

Articles 16 through 21 requires legislative measures to enable competent authorities to carry out specific tasks related to the provisions referred in each of the articles.

It is important that the procedural law of a country captures and gives specific responsibility to the designated competent authorities as will be illustrated in the case example of the Philippines.

Article 16.1 says that "Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification."

It is very important that once identified, electronic data pointing to criminal content or criminal activity should be safeguarded from modifications and intentional tampering and hence expedited preservation of suspect data is crucial.

Relevant provisions of the Budapest Convention for procedural law implementation: [15]

- Article 14 – Scope of procedural provisions
- Article 16 – Expedited preservation of stored computer data
- Article 17 – Expedited preservation and partial disclosure of traffic data
- Article 18 – Production order
- Article 19 – Search and seizure of stored computer data
- Article 20 – Real-time collection of traffic data
- Article 21 – Interception of content data

Articles 14-21 of the Budapest Convention provide guidelines for various procedural matters in relation to dealing with computer data. These are key to carrying out digital forensic investigations and also for making sure that data is not tampered with or wrongfully presented to the judges.

It Is extremely important that the prosecutors and the judges are able to interpret digital evidence that is produced in the courtroom, and that they understand the various different tools and electronic devices that can serve as evidence such as chat and email logs; images stored on mobile phones; subscriber information; and traffic data that can be obtained from ISPs giving detailed information about source and destination of IP packets that can be used to identify the offenders.

Moreover expedited preservation is important to make sure that data is not tampered with, or lost due to inappropriate handling, and is handled safely by the concerned competent authorities during the investigations.

Articles 23-35 of the Budapest Convention provide guidelines for international cooperation to secure e-evidence.

[15] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Some country specific examples in the ASEAN region.

While ECPAT's mapping exercise did not cover the procedural law elements, the Council of Europe workshop in Manila in May 2013 allowed examination of the procedural law of some countries , which were presented during the event. The examples of Singapore and the Philippines are used here to show how specific elements of the Council of Europe Cybercrime Conventions are applied in local legislation.

Singapore:

- In Singapore, admissibility of all evidence (electronic or otherwise) is governed by the Evidence Act.
- Recent amendments were made to the Evidence Act in 2012 relating to the admissibility of electronic evidence. [16]

For example under section 3 of the Evidence Act, that deals with interpretation of electronic evidence, modifications were made so that definition of 'computer output' was deleted to accommodate wider forms of digital evidence including SMS, mobile phone data etc.

- Definition of 'document' was amended to include multimedia (audio, video, etc.) and magnetic media
- Definitions of 'copy of document' and 'electronic record' were introduced. This is crucial as electronic data can be copied easily and retain all the characteristic of orginial data. In cases where data is susceptible to tampering or modification or data loss is encountered, the procedural law should guide the enforcers to make mirror images.
- Electronic evidence will be treated like all other forms of evidence [17]

The Philippines: Cybercrime Prevention Act of 2012 (Republic Act No. 10175)

For the purpose of this presentation we are using *the Philippines : Cybercrime Prevention Act of 2012 (Republic Act No. 10175)* as a good practice example in terms of legislative drafting related to procedural criminal law. However, please note that the implementation of this ACT has been suspended by the Supreme Court of the Philippines due to a constitutional debate about unrelated provisions regarding libel.

This specific example shows how the sections within the RA 10175 of the Philippines address cybercrime in line with the guidance provided by the Council of Europe convention on cybercrime.

CHAPTER IV ENFORCEMENT AND IMPLEMENTATION [18]

The following sections provide necessary procedural powers and guidance to the authorities in alignment with the Council of Europe Budapest convention.

[16] http://www.mlaw.gov.sg/news/press-releases/proposed-amendments-to-the-evidence-act.html
[17] Ibid
[18] http://www.gov.ph/2012/09/12/republic-act-no-10175/

SEC. 10. **Defining the relevant agencies :** Identifies the The National Bureau of Investigation (NBI) and the Philippine National Police (PNP) as being responsible for the efficient and effective law enforcement of the provisions of this Act.

SEC 11: **Define the duties :** Law enforcement authorities specifically the computer or technology crime divisions or units responsible for the investigation of cybercrime are required to submit timely and regular reports including pre-operation, post-operation and investigation results and such other documents as may be required to the Department of Justice (DOJ) for review and monitoring.

SEC. 12. **Collection and recording of traffic data :** Law enforcement authorities, with due cause, shall be authorized to collect or record by technical or electronic means traffic data in real-time associated with specified communications transmitted by means of a computer system.

Traffic data refers only to the communication's origin, destination, route, time, date, size, duration, or type of underlying service, but not content, nor identities.

All other data to be collected or seized or disclosed will require a court warrant.

Service providers are required to cooperate and assist law enforcement authorities in the collection or recording of the above-stated information

SEC. 13. **Preservation of Computer Data** : The integrity of traffic data and subscriber information relating to communication services provided by a service provider shall be preserved for a minimum period of six (6) months from the date of the transaction. Content data shall be similarly preserved for six (6) months from the date of receipt of the order from law enforcement authorities requiring its preservation.

SEC. 14. **Disclosure of Computer Data :** Law enforcement authorities, upon securing a court warrant, shall issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic data or relevant data in his/its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation.

SEC. 15. **Search, Seizure and Examination of Computer Data**

The key provisions are :

(a) To secure a computer system or a computer data storage medium;

(b) To make and retain a copy of those computer data secured;

(c) To maintain the integrity of the relevant stored computer data;

(d) To conduct forensic analysis or examination of the computer data storage medium; and

(e) To render inaccessible or remove those computer data in the accessed computer or computer and communications network.

SEC. 16. **Custody of Computer Data** *:* All computer data, including content and traffic data, examined under a proper warrant shall, within forty-eight (48) hours after the expiration of the period fixed therein, be deposited with the court in a sealed package, and shall be accompanied by an affidavit of the law enforcement authority executing it stating the dates and times covered by the examination, and the law enforcement authority who may access the deposit, among other relevant data

Recommendations in relation to the Budapest Convention:

- All Member States of the Council of Europe should ratify the Budapest Conventions. Non Council of Europe Member States should consider the Convention as model laws for improving their national laws addressing cybercrime, including online sexual crimes against children.

- Domestic legislation should provide for the admissibility of electronic evidence and provide detailed procedural measures in relation to: expedited preservation ; search and seizure mechanisms ; and data interception methods.

- To allow better international collaboration, the laws should incorporate elements of : extradition; mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data; and for the collection of evidence in electronic form of a criminal offence.

- States should create a centralized authority or authorities responsible for sending and answering requests for mutual assistance, which can coordinate information exchanges with corresponding authorities of other countries.