COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

T-ES(2018)19_bil rev.1

01/04/2019

LANZAROTE COMMITTEE / COMITE DE LANZAROTE

Compilation of Replies to Question 14 (Challenges in the prosecution phase)

of the Thematic Questionnaire on the protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTs)

Compilation des réponses à la Question 14 (Défis rencontrés dans la phase des poursuites pénales)

du Questionnaire Thématique sur la protection des enfants contre l'exploitation et les abus sexuels facilités par les technologies de l'information et de la communication (TIC)

Question 14. Challenges in the prosecution phase

What challenges do law enforcement, prosecution and courts face during the prosecution of ICT facilitated sexual offences against children involving the sharing of:

a. self-generated sexually explicit images and/or videos?
b. self-generated sexual content?

Question 14. Défis rencontrés dans la phase des poursuites pénales

Quels problèmes les forces de l'ordre, les autorités de poursuites et les tribunaux rencontrent-ils lorsqu'ils sont amenés à engager des poursuites en cas d'infraction sexuelle contre des d'enfants facilitées par les TIC et impliquant le partage :

a. d'images et/ou de vidéos sexuellement implicites autoproduites ?
b. de contenus à caractère sexuel autoproduits ?

TABLE OF CONTENTS / TABLE DES MATIERES

COMPILATION
of replies / des réponses[1]

States to be assessed / Etats devant faire l'objet du suivi

ALBANIA / ALBANIE
State replies / Réponses de l'Etat

Question 14.

What challenges do law enforcement, prosecution and courts face during the prosecution of ICT facilitated sexual offences against children involving the sharing of:

a. self-generated sexually explicit images and/or videos?
   Yes
b. self-generated sexual content?
   Yes

Comments sent by / Commentaires envoyés par ECPAT, CRCA, ALO 116 and / et ANYN

Question 14.

In our opinion the law enforcement etc. lack financial and technological support, knowledge (know-how), training, expertise and focus on such crimes. There is no policy on place yet on how to protect children, how to raise awareness and better cooperate to identify and criminalise such acts. The Albanian law enforcement and justice institutions are still living on 20th century, while the technology and the risk faced by children and young people are immense.

ANDORRA / ANDORRE
State replies / Réponses de l'Etat

Question 14.

Le problème principal que rencontre l'Unité de Délits technologiques lorsqu'ils doivent poursuivre des cas d'infractions sexuelles contre des enfants facilitées par des TIC, concerne les délais de réponse dans les demandes de coopération judiciaire internationale. Les affaires que l'Unité de Délits Technologiques doit traiter au niveau spécifiquement interne ne posent pas de problèmes, les autorités judiciaires et policières collaborent efficacement lorsque le délit est entièrement basé en Andorre. Mais lorsque des images/et ou vidéos sexuellement implicites sont par exemple liées à un compte d'un important fournisseur (Google, FB, etc..), l'identification de l'IP, si elle est conditionnée à une Commission Rogatoire internationale, délivrée par une autorité judiciaire andorrane vers l'autorité judiciaire qui possède juridiction sur ces fournisseurs, prend parfois jusqu'à 10 mois, et la réponse n'est pas toujours positive. Il arrive que l'autorité judiciaire étrangère informe qu'elle ne peut pas fournir l'information requise.

[1] The full replies submitted by States and other stakeholders are available at / Les réponses intégrales des Etats et autres parties prenantes sont disponibles ici : www.coe.int/lanzarote

AUSTRIA / AUTRICHE
State replies / Réponses de l'Etat

Question 14.
Concerning punishable crimes see answer to question 9.

Question 9 Criminalisation

9.1.a to c:
The replies of Austria to the General Overview Questionnaire as regards the implementation of Article 20 of the Lanzarote Convention (see replies to question 16) are still valid. However with the Criminal Law Amendment Act 2017, Federal Law Gazette.vol. I no. 117/2017, para. 5 was amended. A person is not liable under para. 1 and 3 of Art. 207a CC if the person produces or possesses a pornographic image of a person between the age of 14 and 18 with the consent of and for the private use by the minor or him/herself.

9.2.:
According to Arts. 198ff CCP, the Office of the Public Prosecutor and the court have to offer the suspect a so called "diversion measure" if the following prerequisites are met:

- the facts of the case are sufficiently clarified;
- a penalty does not seem indicated with a view to special or general prevention;
- the maximum penalty of the offence does not exceed five years of imprisonment;
- no serious fault is assumed;
- the act did not result in loss of life (with the exception of certain cases where a relative is killed as a result of the suspect's negligent behaviour).

There are four forms of diversion measures: payment of a sum of money (Art. 200), community service (Arts. 201 and 202 CCP), probation with the assistance of a probation officer and obligations (Art. 203 CCP), and victim-offender mediation.

(Art. 204 CCP). Diversion measures require the consent of the suspect. If the diversion measure was completed successfully, the charges are dropped with final effect.

9.3.:
In cases of crimes mentioned in 9.1.a the penalty is up to one year imprisonment or a fine up to 720 penalty units. In cases falling under 9.1.b and c the penalty is up to three years of imprisonment. Also see answer to question 9.2.

9.4.a and b:
Other sexual content does not fall under the provision of Art. 207a CC.

9.4.c to 9.6:
See answer to question 9.4.a and b.

9.7. a and d:
With the Criminal Law Amendment Act 2017, Federal Law Gazette.vol. I no. 117/2017, which entered into force on the first of September 2017, a new para. 6 was introduced in Art. 207a CC to decriminalise such cases. This exception is applicable if a minor of or above the age of 14 produces or possesses a pornographic image of himself/herself or if the minor offers, provides, relinquishes, displays, or otherwise makes such an image available to others in the sense of para. 1, para. 2 first alternatives or para. 3 of Art. 207a CC. The distribution is still punishable if it is done commercially (see Art. 70 CC).

9.7. e and f:
There is no exception for those cases. Children over the age of 14 are punishable under Art 207a para. 1 CC.

9.8. and 9.9.:
Criminal acts committed by a minor under the age of fourteen years are exempt from all forms of criminal prosecution. In reaction to such acts, only measures to ensure and foster the personal development of the minor can be taken by a tutelage court/family court.

A juvenile (i.e. a person between the age of 14 and the age of 18) who commits an offence shall furthermore not be liable to punishment, if

1. he/she is for certain reasons not mature enough to be aware of the unlawfulness of the offence or to act accordingly;

2. he/she commits an offence while still under the age of sixteen, if there is not gross fault on his/her part and there are no specific reasons requiring the application of the criminal law relating to young offenders to prevent the young person from committing criminal acts.

The public prosecutor shall refrain from prosecuting a juvenile offender, if the offence carries merely a fine or a prison sentence not exceeding five years and if additional measures do not seem to be necessary in order to prevent the young offender from committing further criminal acts. But the alleged offender must in any event be prosecuted, if the offence has resulted in the death of a human being. On the same conditions the court shall by decision discontinue proceedings for a punishable act after initiation of a preliminary investigation or indictment until closing of the trial.

Where it seems necessary to formally inform the alleged offender of the wrongful character of certain acts such as the one in respect of which information was laid, and of any possible consequences thereof, the guardianship court shall do so upon a request by the public prosecutor.

In the Austrian legal system, there is no principal distinction in substantive law between offences committed by adults and those committed by juveniles. There are however important differences in the gravity of punishment that can be applied and the criminal procedure. As a general rule, in case of juvenile offenders the maximum term of a prison sentence and the maximum amount of fines to be determined on the basis of daily rates, shall be halved.

There is no minimum sentence.

See also the answer to 9.2.

9.10. to 9.12:
These cases do not fall under Art. 207a CC.

Law enforcement bodies and prosecutors face the difficulty of identifying the owner of a web page providing ICT, e.g. Facebook, who shares sexual content.

Sexual content can be spread easily and quickly by ICT; often, at the time, an offence is being reported, the content has already been passed on several times, which again can be difficult to trace.

By law, internet communication such as provided for instance by WhatsApp cannot be observed. In order to obtain information about the content of previous internet communication and to stop the sharing of sexual content, law enforcement bodies have to seize the mobile devices or other data carriers of the involved persons (accused/victims/witnesses). Often, data are already erased; in these cases, IT-experts have to restore the data, which generally delays the investigation proceedings, especially in default of sufficient skilled personnel.

BELGIUM / BELGIQUE
State replies / Réponses de l'Etat

Question 14.
In Belgium, the police is not involved in the prosecution phase.

When they report to the magistrate they emphasize in their report the exact role of everybody involved.

Purely on procedure there is no challenge, but it is important to clearly explain the exact circumstances.

The main challenges law enforcement are facing are:

+ getting the right prevention message through to young people. They often see that the exchange of self-generated content makes young people vulnerable for crimes like sexual coercion.

+ finding partners outside the police to reach the right people in time with a for them acceptable message. This is being handled on a national level in the framework of the national security plan.

Comments sent by / Commentaires envoyés par ECPAT-Belgium

Question 14.
The answer is quite one-sided. There are so many problems that victims, police, judiciary face in the prosecution phase. First of all, there is the problem of under-reporting because victims blame themselves for what happened, especially when the material is self-produced. Secondly, child victims and their parents are encouraged by Child Focus/ECPAT Belgium to report the abuse to the authorities but they are not taken seriously because of a lack of knowledge among the "first reporting police instance" with the new realities that kids face online. Then comes the problem of prioritization of case-load within the judiciary. It is highly unlikely that a magistrate would bring a "sexting gone wrong"-case before a juvenile court, because the seriousness of the case is often underestimated.

In most sexting cases, Child Focus would not recommend bringing juvenile offenders to court: such cases should be handled between parents, schools, victim and offender, etc. When it comes to grooming, sextortion, and all other forms of online sexual abuse which involves a minor victim and an adult offender, the recommendation is obviously different. However, because police and judiciary are lagging behind in investigative techniques, victim identification techniques and overall knowledge on how to deal with such cases, the detection, prosecution and conviction rate for these offences is very low. Moreover, the current data collection system of criminal offences does not allow to have an overview on the different categories of child sexual abuse online such as grooming, sexting, sextortion, etc.

For more information, please contact:

Ariane Couvreur, Project manager, ECPAT Belgium, +3225222.63.23
arianecouvreur@ecpat.be

Yasmin Van Damme, Policy officer, Child Focus, +322475.44.29
yasmin.vandamme@childfocus.org

Nel Broothaerts, Chief Prevention & Development Officer, Child Focus, +322475.44.47
nel.broothaerts@childfocus.org

BOSNIA AND HERZEGOVINA / BOSNIE-HERZEGOVINE
State replies / Réponses de l'Etat

Question 14.
There is no available information

BULGARIA / BULGARIE
State replies / Réponses de l'Etat

Question 14.
No reply to this question / Pas de réponse à cette question

CROATIA / CROATIE
State replies / Réponses de l'Etat

Question 14.a.
The Ministry of the Interior of the Republic of Croatia has stated that there are issues in practice concerning the speed of development of modern technologies and the internet in the sense of how new forms of criminal offences are manifested as well as in the sense of how criminal offences are committed, of finding new and adequate modalities of providing evidence, as well as in the fact that the development of a criminal law system is a process that requires time to synchronise with new forms in which criminal offences are manifested and committed.

Question 14.b.
The above is not defined as a criminal offence by the Croatian criminal legislation, which renders us unable to provide an answer concerning the challenges which the law enforcement, prosecutors and courts face in the course of criminal proceedings with respect to the behaviours described under 14.b.

CYPRUS / CHYPRE
State replies / Réponses de l'Etat

Question 14.a.
No special challenges

Question 14.b.
No special challenges

CZECH REPUBLIC / REPUBLIQUE TCHEQUE
State replies / Réponses de l'Etat

Question 14.
The application practice of law enforcement authorities in the Czech Republic includes cases of illegal sharing of photos / videos with sexual content [a)] as well as cases of illegal sharing of other sexual content. Often, this is done through social networks, especially on Facebook or on ICQ, on e-mail, etc. Most often these cases are legally classified as a crime of blackmail under Section 175 of the Penal Code. The offender passes off as someone else, contacts the child (a person under the age of 18), requests photos (videos) with sexual content. Often, it is the image of the child's own body. It could concern girl but a boy too. Getting the photos, videos, or sharing the sexual content goes on in several phases. It is often accompanied by flattery, abuse of the child's inexperience, ignorance of the functioning of the social network, etc. The next step is to verify the identity of the child. Eventually, there is an increase of

the intimacy, the photos, videos, or sexual content are becoming more daring. The blackmailing manifests either as a threat of intimate content being disclosed to the parents of the child, or as a threat of publication of such content directly on the social network, to friends, classmates, etc.

A similar blackmailing mechanism may include the offender presenting him/herself as the representative of model agency. It may occur that there is a creation of virtual friendship between the victim and the offender. The criminal act of blackmailing consists in the fact that the offender forces the victim to do something, to omit or to tolerate. It is not necessarily part of the factum to require financial performance, counter-service, etc.

Other qualified facts of the crime that may occur:

Section 181 Infringement of Stranger's Rights of the Penal Code defined as "whoever causes serious harm to the rights of someone else by bringing another person into error, or taking advantage of another person's error, shall be punished by a prison sentence of up to two years or punishment by disqualification." For example, there has been a case where the offender has published intimate photos / videos of the child without his/her knowledge and consent, but it could target other intimate communications (correspondence) as well. It can often be a display of vengeance, hostility, a reaction to the breakup of a friendship. Often, the content is published on Facebook, or on other various social networks (such as www.spolužáci.cz, www.libimseti.cz), the content is used as false offer of sexual service.

Section 184 Slander of the Penal Code defined as "whoever shall bear a false statement about another person that is capable of substantially jeopardising their esteem among their countrymen, especially in their employment, disruption to their family, or to cause them any serious damage, shall be punished by a prison sentence of up to one year." The child will be particularly concerned with family relationships and relationships at school, with friends, etc. The qualified facts of the crime will then more severely affect acts committed by the press, film, radio, television, publicly accessible network or other similarly effective way. Most often, it may concern sending out (email) or publishing (on social networks) false statements about intimate life of the victim. These messages may be accompanied by photographs or videos. These actions can be the expression of the so called cyberbullying.

Section 353 Dangerous Threats of the Penal Code defined as "Whoever threatens another with death, grievous bodily harm, or other grievous harm in such a way that it raises legitimate concerns, shall be punished by a prison sentence of up to one year or punishment by disqualification." It may concern (in relation to the child) the mentioned other grievous harm which is assessed in consideration of every aspect of the case.

Section 354 Dangerous Persecution of the Penal Code defined as "Whoever persecutes another person long term by threatening them with bodily harm or another bodily harm to them or a person close to them, seeking out their personal closeness or watching them, persistently contacting them via means of electronic communications, written or otherwise, restricting them in their usual way of life, or abusing their personal data in order to obtain personal or other contact, and such conduct is capable of raising substantial concerns in them for their life or health or the life or health of persons close to them, shall be punished by a prison sentence of up to one year or punishment by disqualification. The concerned form of persecution is called cyber-stalking (unsolicited emails, distributing negative news via chat, blog or other way of virtual distribution of photos, videos, etc. Often it is so-called virtual or telephone terror.

Other facts of the crime may occur, such as **Section 186 Sexual Coercion** of the Penal Code ("whoever forces another person into masturbation, indecent exposure, or other comparable conduct by threat of violence or the threat of other grievous harm, or who exploits the person's vulnerability for such behaviour, **Section 193 Abuse of a Child for the Production of Pornography** of the Penal Code ("whoever

persuades, arranges, hires, allures, entices, or exploits a child for the production of pornographic works and exploits the child's participation in such pornographic works), **Section 193a Participation in pornographic performance** of the Penal Code ("whoever participates in a pornographic or any other similar performance in which a child performs shall be punished by a prison sentence of up to two years."), **Section 193b Establishment of unauthorised contacts with a child** of the Penal Code ("whoever proposes a meeting to a child below fifteen years of age with the intention to commit a criminal offence referred to in Section 187 Subsection 1, Section 192, 193, Section 202 Subsection 2 or any other sexually motivated criminal offence"), **Section 201 Endangering a Child's Care** of the Penal Code ("whoever, even out of negligence, endangers the intellectual, emotional, or moral development of a child by enticing them to an indolent or immoral life, allowing them to lead an indolent or immoral life, allowing them to procure means for themselves or others through criminal activity or by another condemnable manner, or seriously breaching their obligation to care for them or any important obligation under parental obligations") or **Section 202 Enticement to Sexual Intercourse** of the Penal Code ("whoever offers, promises, or provides monetary reward, benefits or advantages for the child or another person for sexual intercourse with a child, masturbation of a child, their indecent exposure, or other comparable conduct for the purpose of sexual satisfaction).

All these crimes can be committed through the internet and social networks. They also occur in the "non-internet" form.

DENMARK / DANEMARK
State replies / Réponses de l'Etat

Question 14.a.

One of the main challenges concerning prosecution of ICT facilitated offences in general is the presentation in court of the technical examination of the devices used for the ICT facilitated offence. This applies for instance when explaining to the court the technical details regarding the sharing of files.

Consequently, the Danish National Police, the Director of Public Prosecutions and the Police Academy in 2015 launched a cooperation on the development of a new national cybercrime education. The education consists of two courses, Cybercrime I and Cybercrime II, and aims to strengthen the basic knowledge of IT and IT related crime among the police staff and the prosecutors. Cyber Crime I is an E-learning course and is mandatory for all prosecutors.

The education contains IT-related crime in broad terms, including crimes committed on the internet and where the Internet acts as a communication platform between criminals and crimes targeted at IT systems or committed by using IT systems. The education also focuses on how to handle and investigate digital tracks.

It aims to ensure that the participants can handle IT-related crime professionally and accurately. A part of the course accounts how the IT statements forms a part of the criminal case among the investigation. It explains how you read the IT statement, what type of information the sections in the statement contain and the different types of data.

Cyber Crime II is addressed to specialists in crimes committed on the internet. It is a 4-day training course where the participants, among other things, are trained in how to use the IT statement as an evidence in court.

Question 14.b.

Please see answer to question 14(a)

ESTONIA / ESTONIE
State replies / Réponses de l'Etat

Question 14.
Individuals who are using mobile phones to connect to the internet to facilitate criminal activities cannot be identified because globally 90% of mobile internet access providers have adopted CGN technology, which prevents them from complying with their legal obligations to identify individual subscribers.

FINLAND / FINLANDE
State replies / Réponses de l'Etat

Question 14.
The police and the prosecutor work in close cooperation in accordance with mandatory legislation relating to criminal and pre-trial investigation. The cooperation aims at enhancing the criminal procedure. The stability and limited number of qualified personnel is a challenge. It is naturally also a challenge that the threshold for the victims to report a crime is decidedly high in cases where self-generated material falls in the wrong hands and is distributed or if it is used for extortion as the victim is often ashamed and considers that he himself has contributed to his difficult situation.

Furthermore, it may be problematic to define the material and the evidence to be presented in a case as there can be a lot of material, for example pictures, in an individual case. It is also time consuming to go through the material.

FRANCE
State replies / Réponses de l'Etat

Question 14.a.
Aucune en particulier pour ce type d'enquête. D'une manière générale, les difficultés rencontrées relèvent de l'identification des personnes qui ont mis en ligne les images (qu'elles soient autoproduites ou non).

Question 14.b.
Les principaux problèmes rencontrés dans ces enquêtes sont liés à l'environnement numérique qui ne permet pas toujours une identification aisée des consommateurs et divulgateurs de contenus. Les fournisseurs d'accès ou GAFAM (géants du web) répondent avec difficultés aux réquisitions en l'absence de protocoles d'accord partenarial. La durée de conservation des données est trop réduite à l'étranger (notamment dans les pays anglo-saxons) par rapport aux besoins d'investigation. Enfin, les partages de fichiers sur cette thématique sont aujourd'hui de plus en plus réalisés à l'aide de systèmes de chiffrement difficilement décryptables.

Comments sent by / Commentaires envoyés par Stop Aux Violences Sexuelles

Question 14.
Pas d'information sur le sujet

GEORGIA / GEORGIE
State replies / Réponses de l'Etat

Question 14.
During the investigation of child pornography cases the following difficulties take place:

1. Lack of awareness of children concerning the risks related to "sexting" and sharing self-generated sexual images;

2. Complications and expenses of expert examination leads to the investigation delay;

3. Child pornography appears as a transnational crime and often requires inspection information with other states, which is a time-consuming process itself;

4. Growing tendency to use ICTs for sexual abuse and exploitation.

GERMANY / ALLEMAGNE
State replies / Réponses de l'Etat

Question 14.
The Federal *Länder* report that the dissemination of self-generated sexually explicit images and/or videos by children and adolescents using the internet and mobile telephones is a widespread phenomenon. In this context, the images or videos will be generated on the children's or adolescents' own initiative, who fail to consider the risk of these files being forwarded or disseminated via social networks. In **Saxony**, the impression is that neither children not adolescents are sufficiently aware of the dangers and consequences of using and forwarding sexual content. In the view taken by the Federal *Länder*, many adolescents are not aware that sending images and/or videos constituting child pornography or juvenile pornography is an act liable to punishment under criminal law.

Lower Saxony, Bavaria, and **Saxony** all take the view that the willingness of children, respectively adolescents and adults, to file a report concerning the corresponding acts needs to be improved. To this end, the parties affected must be made aware that the authorities will be able to provide assistance and support. Besides stepping up efforts at awareness-raising and prevention, the cases involving the corresponding facts and circumstances that are brought to the attention of the law enforcement authorities must be processed consistently. As reported by the above *Länder*, the police, respectively the public prosecutor's offices, face the following challenges occasioned by the dissemination of images and/or videos of child pornography, respectively juvenile pornography, using ICT.

The increasing number of new files containing child pornography and juvenile pornography often will require comprehensive and time-consuming investigations in order to identify the victims. Thus, **Hesse, Saarland**, and the **Rhineland-Palatinate** all state that the identification of the corresponding perpetrators who use ICT in order to commit the offence represents a significant challenge since it is not possible to trace back the usage data obtained from the internet communications services (so-called IP addresses) to the contractual partners of the parties providing access to the internet, since the latter do not store such data; accordingly, it is not possible to trace the data back to the potential suspects. At present, it is impossible to assess whether the obligation to store traffic data, which the telecommunications enterprises are to comply with since 1 July 2017, will lead to an improvement in this regard. **Lower Saxony, Bavaria, North Rhine-Westphalia**, and **Saxony** already would want to see the providers of telecommunications services be obligated to store such data for a longer period of time.

By way of supplementation, the **Rhineland-Palatinate** has stated that the internet increasingly is being used by mobile end devices and mobile telecommunications. However, the technology used in mobile communications is such that a large number of users (which may be as large as 64,000) share one and the same IP. Drawing conclusions from the IP to the actual user will be possible in these cases only if, in addition to the IP and the time stamp, the corresponding port has also been stored. However, the law currently does not provide for a corresponding obligation to store such information.

As concerns the work done in their investigations, **Saxony** and **Hamburg** see a problem in that data are fleeting and in many cases must be restored, a process requiring significant amounts of time and effort. Often, perpetrators delete the relevant chat records. In many cases, the victims themselves also will delete them out of fear or shame. Another aspect is that the hash values of data will be changed in order to make the task of identifying the digital material more difficult.

Lower Saxony, Hamburg, Bavaria, and **Saarland** have highlighted the issue, moreover, that in many cases, it is impossible to prove that the perpetrators intentionally obtained or disseminated the images and/or videos constituting child pornography, respectively juvenile pornography. This is the result in particular of the darknet being used. In increasing numbers, perpetrators sharing self-generated images and/or videos will use a TOR browser or some other anonymization service in order to obfuscate their identity. Once a range of different TOR servers are involved, from the starting point of a message up to its end point, the physical connection (IP address) of the sender will be impossible to ascertain, as a general rule, or would be possible to ascertain only by means that are contravened by legal obstacles.

The Federal *Länder* all agree that the amounts of data that must be dealt with in these investigations are immense. In many cases, because the image and video files have been shared and disseminated in several instances, the investigations are very comprehensive and require significant manpower (and sometimes need to be done repetitiously). **Baden-Württemberg** regards offences to be particularly problematic that are committed in the context of group chats (e.g. via WhatsApp). Often, these groups will count large numbers of members who live outside the jurisdiction of the respective investigating authority; furthermore, because it is possible to use these services anonymously, the groups are very difficult to investigate and identify. **Hesse** reports that in many cases, the parties involved live abroad. This makes the collection of physical evidence, in particular storage media of all types, all the more difficult while on the other hand increasing the amount of data that need to be dealt with. **Hesse, Lower Saxony, Saarland**, and the **Rhineland-Palatinate** mention “literally terrabytes” of images and/or videos needing to be analysed. The increasing amounts of data stored on web-enabled computers and mobile telephones mean that it is well-nigh impossible for the technical and staffing resources of the specialised police stations to clear up the facts and circumstances promptly. Also in cases in which private service providers are involved because the police lack the corresponding capacities, it is to be noted that because of the increased amounts of data, the analysis takes longer and entails higher costs. **Lower Saxony** has reported that the long analysis periods will lead to delays (which may be quite significant in some instances) in processing the cases. In spite of significant organisational measures having been taken in order to accelerate processing by the police authorities, the analysis performed in complex proceedings entailing a large amount of data to be analysed may take between 1.5 and 2 years; in some proceedings, it may even last for 2 years. As a consequence, it is not a rare occurrence to see the sentences reduced due to the excessively long duration of the proceedings.

Furthermore, many Federal *Länder* highlight the fact that storage media, and in particular mobile phones, are password-protected and data carriers encrypted. Finding solutions for decoding passwords or encryptions, respectively for accessing the media/mobile telephones prior to protection is difficult or even impossible in light of data protection exigencies. As a rule, modern means of encryption can be unlocked only by the person creating the password or encryption; at any rate, they make the analysis of mobile end devices, tablets, etc. significantly more difficult.

Lower Saxony has underscored the fact that the speed at which digital media evolve and the ephemeral nature of the offerings and services for receiving and sending data often make the task of identifying perpetrators a difficult one. This view is supplemented by **Brandenburg** by the note that the law enforcement authorities must continually ensure that the technology and the investigation processes they use are abreast of the dynamic developments in digital technology.

Hesse, Bavaria, and the **Rhineland-Palatinate** all report that the locations of the servers on which the data are stored, respectively that are used to process the data flows, often will be selected such that access by German law enforcement authorities is obstructed to the greatest possible degree or in fact rendered impossible. In some cases, **Mecklenburg-Western Pomerania** has stated, the perpetrators will intentionally select providers who are located in countries that do not react to requests for legal assistance. Moreover, the work to identify the parties is complicated by the fact that in many cases, both the perpetrator and the victim will use internet communications services whose operators have their registered seat outside of Europe, meaning that investigative starting points such as current usage data can be obtained only by way of formal judicial assistance – because this process is lengthy, the data obtained can then no longer be assigned to the customer of the telecommunications provider because the mandatory storage period that this enterprise must comply with has lapsed. In this context, **Lower Saxony** notes that many foreign providers are unwilling to provide information.

A further challenge, according to the Federal *Länder* **Baden-Württemberg, Saarland**, and **Saxony**, is to be seen in the interviews held with children and adolescents, especially since in some cases, they will be injured parties and accused parties all at the same time. In light of the sensitive topic, it is not a rare occurrence for children and adolescents to deny that they have generated the corresponding images, or to remain entirely silent, in each case out of fear or shame. **Hamburg** notes that resorting to video interviews with these children, involving criminal psychologists, and obtaining reports from credibility experts requires the expenditure of significant amounts of time and effort.

As concerns the main trial before the court, **Hesse** addresses the problem that the children or adolescents who are the victims of such offences are supposed to appear as witnesses in the proceedings on the one hand, while on the other hand, certain scenarios may require them to begin therapy at the earliest possible opportunity. This leads to the conundrum of the witnesses being influenced as part of the approach taken in their therapy, while the defence of the perpetrator raises the concern that the testimony by the witness is being influenced. The decisive factor in this regard is that the first interview with the child or adolescent meets high standards in terms of its quality and that it has been documented well.

Finally, **Hesse, Bavaria**, and **Lower Saxony** highlight the special strain that the officers are under who must inspect the contents shown in the images and/or videos. Where this is concerned, the officers affected are given the opportunity in **Hesse** to avail themselves of assistance by seeking supervision.

GREECE / GRECE

State replies / Réponses de l'Etat

Question 14.

No reply to this question / Pas de réponse à cette question

HUNGARY / HONGRIE
State replies / Réponses de l'Etat

Question 14.

The National Office for the Judiciary contacted all Criminal Chambers of the county and regional courts for answering this question. The courts could identify certain challenges upon their experiences during cases involving children affected by criminal offences facilitated by ICTs.

The most relevant challenge is the tackle the difficulties during evidentiary procedure, this includes the identification of the perpetrator, the precise determination of the place, time, method (the exact wrongful conduct) and object of the perpetration.

- Challenges when determining the identification of the perpetrator: certain ICT tools and data carriers are not only used by the perpetrator, but by the people living in the same environment, or they already bought it used. Furthermore, the perpetrators use open servers and fake names. When sharing a certain content multiple times, it is difficult to identify the person who shared it. Sophisticated perpetrators use VPNs, TOR and other software that hide their identity. Also the ISPs who use NAT networks can't provide useful information without port numbers, but in most cases they are not in the possession of police.
- Challenges when determining the place of perpetration: most of the ICT tolls are portable. Many times the hosting service provider cannot give appropriate answer regarding the exact place and time of upload, or identifying the person who did the upload (e.g. servers of Facebook, Google and Skype are in the USA, they most likely do not comply with requests of the Hungarian authorities, thus the identification of the perpetrator for the lack of any other digital trace is difficult.)
- Challenges when determining the time of perpetration: the exact time of upload and download can sometimes only be determined with the help of an IT expert. The use of a certain IP address has to be connected to an exact time, in case of foreign partner servers, then attention must be paid on what zone the clock was set on, was the daylight/winter saving time applied.
- Challenges when determining the method of perpetration: the seizure/sequestration does not include all IT tools and data carriers of the perpetrator and the recovery of such further evidence at the time of the court procedure is usually pointless.

Further challenges include:

- that it is difficult to determine and prove whether a recording is real or not. Also, the deleted sexual contents are not restored during the procedure.

- the "exhibitionism" of a child – thus the real questions of this questionnaire – is also difficult to prove.

- the problem of the identification of the victims and their age. The latter one usually requires the involvement of a forensic doctor or anthropologist expert, but it still can happen that the expert opinion only determines a probable age.

- that sometimes it can be difficult to determine whether the person depicted is real or not.

- the difficulty to fully unravel the real knowledge of the perpetrator regarding the real age of the victim.

- the protection of personal rights of victims and the avoidance of their secondary victimization.

- the transnational nature of these crimes, the time-consuming compliance with legal assistance requests, which can lead to excessive duration of the evidentiary procedure and might not end successfully.

Further challenges, regarding online defamation: The Hungarian Criminal Code stipulates a crime if someone shares even a non-sexual depiction of a person under 18 y.o.a., when there is no approval of the depicted person thereof, or otherwise if someone misuses the personal data of the depicted person in defamatory ways, typically by posting and linking defamatory comments to the depiction. In such cases, taking into consideration all aspects of a certain case, the following crimes might be established: misuse of personal data (CC 219. §), harassment (CC 222. §), degrading treatment of vulnerable persons (CC 225. §), defamation (CC 226. §), or slander (CC 227. §). In these cases, the police may ask the service provider of the social networking site where the misuse of personal data was committed to deliver offender identification data. The police order can be smoothly completed if the social networking site brought effort to establish a special police "hotline" where the law enforcement agencies can directly reach the service provider with such requests; Facebook can be an example (facebook.com/records). However, there might be no such network for police orders with other social network providers, such as Snapchat or Ask.fm. In the latter cases, the police, in order to obtain the suspects' personal data (IP address, logs etc.) should utilize open source data gathering techniques which might not be successful.

Ideally, users should be able to connect the social networking site service provider in the above mentioned, petty crimes or misdemeanours, asking for terminating the profile of the harasser or the incriminated group's activity directly. There are however cases where the service provider does not react to the users' reports. In this case the user, whose rights have been violated could report the harmful activity to the National Authority for Data Protection and Freedom of Information. But because the latter is not a law enforcement agency, the social networking site likely turns down their requests. Hence, the only opportunity for the user (victim) is to report it to the police and undergo a criminal investigation. But because of the nature of the acts (petty crimes or misdemeanours, yet pretty personal in their nature) online defamation victims might be reluctant to pursue a criminal case, the acts remain unreported and uninvestigated, increasing the latency. When and whether the defamatory act so severely discounts the reputation of the victim, as it overcomes the burden of a criminal procedure, only then the victim turns to the police.

ICELAND / ISLANDE
State replies / Réponses de l'Etat

Question 14.

Regarding both questions, there is a certain problem how to handle a case when a child (aged 15-18 years old) takes a picture / produces material and sends / shares. Particularly this is a problem when both the offender and the victim are children in the legal sense.

ITALY / ITALIE
State replies / Réponses de l'Etat

Question 14.

Children's self-produced child pornography is widespread among young people and this poses various challenges for governments. There is a need to better regulate the phenomenon, since a specific legislation on this issues is still missing - as we said answering to Q 8 and Q 9 - whether or not directing to criminalization, and aiming to guide the prevention, counteraction (also as investigation) and assistance to the victims. Italy (see above answers to Q.1, Q. 2, Q. 4, Q.4, Q. 6, Q. 7) has been for years committed to protecting children from the risks associated with the use of new technologies (child

pornography, also grooming, cyberbullying, etc. included), but the interventions locally undertaken by public authorities and NGOs often lack coordination within an overall framework.

At the level of criminal investigation and prosecution, most problems lie in the identification of the persons legally involved and other difficulties connected to the use of computer and telematic technologies.

Another aspect on which action is needed is prevention: while several initiatives have been carried out for the children - often with the involvement of the schools, - the many actors in these initiatives report a dramatic lack of awareness in the children themselves of the risks and serious dangers connected with the self-production and / or dissemination of material through the internet.

In this perspective, an awareness-raising activity involving the education sector (from early childhood services to the secondary school) lead with continuity rather than episodic measures would be helpful in producing effective and generalized results.

Another challenge is the involvement of the parents, which is often problematic, not only on issues related to the use of the internet by minors but, more generally, on those related to abuse and sexual exploitation, as well as violence: it would be important to identify strategies to enhance effective collaboration of the families not only in prevention and counter-action of such phenomena as the self-production of pedopornographic material by children, but in an earlier stage in education activities to obtain the widest protection against the risks that these behaviours may cause.

Other issues concerning the protection of children from abuse and sexual exploitation, to which Italy intends to respond through the actions included in the National Plan for Prevention and Fight of Child Abuse and Sexual Exploitation 2015-2017 are:

- the training of the operators dealing with the protection of minors in the various sectors (Police, Courts, Social and Health services);

- the implementation and development of coordination among the many police corps engaged in activities against minor offenses (in particular those related to the use of information and communication technologies);

- implementation and development of coordination between police corps, magistrates, health services, through multidisciplinary training, protocols, notes, etc. including finding the way to reconcile the investigations with the needs and timing of criminal justice, and with the needs of prompt care and assistance to the minor victims;

- the identification of appropriate ways and times for hearing a minor victim of crime (and also involved in self-production / dissemination of paedophile material through ICT) in the criminal proceedings, both during the investigation and during the trial (according to what provided for in the Guidelines identifying the essential levels of protection and support for minors who are victims of sexual abuse and exploitation);

- strengthening the protection of minors in criminal proceedings against minors (in front of the Juvenile Court), now mainly focused on re-education of the perpetrator.

Comments sent by / Commentaires envoyés par Independent Authority for Children and Adolescents

Question 14.
A further challenge concerning the prosecution phase is the use of restorative justice programmes. As the events often involve minors – not only with regard to victims but also to offenders – and considered that all of them are almost fully unaware about the consequences of their actions, restorative justice could represent an appropriate means in order for children and adolescents to become really aware of the consequences of their actions through the "experience" of the other person.

LATVIA / LETTONIE
State replies / Réponses de l'Etat

Question 14.
One of the main problem, when investigating crimes connected with information and communication technologies is the lack of human resources. Frequently acquired data and materials are large volume and requires a considerable amount of time and work resources to test them. An expert-examination in these cases is also very time-consuming and sometimes exceeds the limitation period for a criminal offence. This problem is being solved by making changes to existing list of positions and creating new positions to the Criminal Police Offices of the State police in order to provide support in the field of ICT to the Criminal Police departments.

In additions, it should be noted that the majority of such offenses are committed through foreign servers and websites, and therefore request for criminal-legal assistance are written, but the time in which the request is fulfilled also significantly delays the investigation.

LIECHTENSTEIN
State replies / Réponses de l'Etat

Question 14.
For the Liechtenstein National Police, it is a challenge to examine and visualise the large volumes of relevant images and videos, to assess the ages of the persons depicted (<> 18 years), to identify the depicted persons on the basis of the image recordings, to prove that the materials are being offered to other internet users (e.g. via P2P file-sharing exchanges), and to deal with the psychological burden on investigators and forensic experts when looking at the data on an extended basis. Furthermore, access to protected internet environments (closed chats, darknet, etc.) is often only possible under special access conditions (personal recommendation, contribution of own material, etc.).

The Office of the Public Prosecutor is well equipped to prosecute both types (14.a and 14.b) of cases. There are no serious challenges in this regard. The prosecutors in Liechtenstein try to address the specifics of every case. While adult offenders are systematically prosecuted, there is a policy to react in a differentiated manner when the offenders are juveniles between the age of 14 and 18. Sometimes alternative measures are considered the more appropriate reaction. The protection of victims is taken seriously at all stages of the proceedings.

Courts do not consider there to be any special circumstances or specific challenges in dealing with cases of sexual offences. Rather, the same questions and difficulties arise in the course of the investigation as they do every time a crime is committed with the help of IT resources. In this respect, a special challenge for Liechtenstein is that, due to its small size, it is often necessary to obtain data from foreign providers by way of mutual legal assistance, which is time-consuming and can be problematic especially with

regard to the retention periods for peripheral data. Otherwise, however, criminal prosecution has the necessary legal bases and other resources to be able to proceed adequately.

LITHUANIA / LITUANIE
State replies / Réponses de l'Etat

Question 14.

During the prosecution of ICT facilitated sexual offences against children, the court shall take into account all the relevant circumstances. For example, the evaluation of the purpose of the production, acquisition, possession or distribution of the self-generated sexually explicit images and/or videos/self-generated sexual content, the evaluation of the nature of the relationship between victim and offender (e.g., if they are 15 and 16 years old, etc.), the evaluation of the sexual maturity and consciousness level of persons can lead to difficulties.

The key challenges for the successful prosecution and, in particular, investigation of cybercrimes, are limited opportunities for obtaining information form Internet service providers registered and operating abroad, especially from smaller companies as these companies do not provide the possibility for law enforcement authorities to obtain the information directly though dedicated platforms and systems.

LUXEMBOURG
State replies / Réponses de l'Etat

Question 14.

Dans le cadre de la poursuite pénale des infractions visées au questionnaire, des difficultés de nature variable peuvent effectivement se présenter. La liste des exemples cités ci-dessous n'a pas pour prétention d'être exhaustive.

1. Une première difficulté peut tenir au délai limité de conservation des données électroniques nécessaires à l'élucidation de l'affaire.

Au Luxembourg, la législation sur la protection des données limite la durée de conservation des données à six mois. Si une plainte est déposée tardivement, les autorités de poursuite risquent de s'y heurter, en ce qu'il n'est par exemple plus possible de faire identifier le détenteur d'un numéro IP qui a téléchargé des images sexuelles autoproduites par un enfant ou bien qui a exercé de la pression sur un enfant afin d'en obtenir.

2. Le caractère transfrontalier d'une affaire peut rendre l'exercice des poursuites plus compliqué.

En effet, si des images incriminées proviennent d'un serveur informatique se trouvant localisé à l'étranger ou bien si l'auteur identifié y réside, les autorités luxembourgeoises doivent procéder par voie de commissions rogatoires internationales, qui mettent parfois beaucoup de temps à être exécutées. Le même problème se pose lorsque le siège de la société qui détient les données requises se trouve à l'étranger.

Dans certaines hypothèses, il peut également s'avérer nécessaire de dénoncer l'affaire à une autorité étrangère, lorsque les faits peuvent y être poursuivis plus utilement.

3. Dans certains dossiers, les autorités se retrouvent face à des données cryptées.

L'exploitation du matériel informatique saisi, qui nécessite de toute façon un temps plus ou moins long selon le volume des données à analyser, se révèle alors comme particulièrement fastidieuse. Il peut même arriver que le cryptage soit tellement efficace que les spécialistes des forces de l'ordre n'arrivent pas à décoder l'intégralité des données saisies. Les infractions en relation avec ces données cryptées restent dès lors impunies.

4. Utilisation du matériel informatique ayant servi à commettre l'infraction par une pluralité de personnes.

Lorsque l'ordinateur à l'aide duquel une infraction telle que celles visées par le questionnaire a été commise, a été utilisé par plusieurs personnes (p.ex. ordinateur d'une entreprise auquel de nombreuses personnes ont accès à des fins professionnelles), il peut s'avérer très compliqué, sinon impossible, de démontrer laquelle de ces personnes est celle qui est l'auteur de l'infraction.

5. La technologie mise en œuvre ne permet pas la conservation des données.

On peut citer ici l'exemple du réseau de communication SNAPCHAT qui a comme particularité que les images transmises ne sont pas conservées et qu'elles ne peuvent pas être récupérées, lors d'une enquête pénale éventuelle ultérieure. Les données incriminées sont ainsi perdues à jamais et la poursuite de l'auteur s'avère vaine.

Le grand volume de données constitue un des défis majeurs dans la lutte contre l'exploitation et les abus sexuels facilités par les technologies de l'information.

Au Grand-Duché, les ordinateurs ou appareils saisis par la Police sont tout d'abord analysés du point de vue technique par le Service de police judiciaire. L'extraction de toutes les données informatiques d'un ordinateur prend 4 à 6 mois.

La période d'investissement de travail varie selon le volume des données trouvées sur les appareils et selon le nombre d'enquêteurs en charge de ces missions. Sachant qu'aujourd'hui il devient de plus en plus normal d'utiliser l'Internet au quotidien, il est clair que les enquêteurs se trouvent de plus en plus confrontés à un très grand volume de données à exploiter. Ceci engendre des temps d'exploitation et d'enquête de plus en plus longs.

En ce qui concerne les logiciels utilisés pour détecter du matériel pédopornographique sur des ordinateurs des auteurs présumés, le Service de police judiciaire est doté d'un programme informatique performant pour isoler les images à caractère pédopornographique, mais, comme mentionné ci-dessus, une adaptation à l'évolution constante des technologies s'impose.

MALTA / MALTE
State replies / Réponses de l'Etat

Question 14.

There are practically no challenges that are faced during the prosecution of such offences. Technical experts are invariably appointed by the Court to establish the details of the subscriber and / or user of the (device) corpus delicti.

Even though for a person to be convicted of a similar offence the identification of the victim is not a legal prerequisite, for preventive measures the victim's identification may lead to practical challenges.

REPUBLIC OF MOLDOVA / REPUBLIQUE DE MOLDOVA
State replies / Réponses de l'Etat

Question 14.

Child pornography offense is qualified, according to the legislation of the Republic of Moldova, as a less serious crime, thus preventive measures can only be applied under certain conditions. Taking these issues into account, the estimated challenges are:

Criminal Code:

- **Art. 208/1** "Child Pornography" does not criminalize the wittingly obtaining of access to child pornography through information and communication technologies, although this is established in the Lanzarote Convention.

Criminal Procedure Code:

1) The computer search procedure is not regulated, including on the storage media of the computer data used by remote access. Thus, the sampling procedure is not regulated when using cloud, remote server, computer data hosting technologies (Dropbox, etc.);

2) There is a lack of special measures of cyber data interception investigations;

3) There is no provision for obtaining communications by electronic means - text messaging through computer systems other than telephone services and other electronic communications - from the providers of e-mail services, chat etc.;

Psychological services are delivered only by non-governmental organizations, and the law enforcement bodies resort to their assistance. At present, there are no psychologists from law institutions trained in this field.

The expertise and research procedures (in the field of criminology and forensics) can be attributed to the challenges component, including the responsibility of the IT sector in the process of preventing these types of crimes.

The draft Law no. 161 (2016) for amending and completing some legislative acts with the following amendments:

- Implementation of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote, 2007) and the Council of Europe Convention on Cybercrime, in order to guarantee the effective investigation and prosecution of child sexual offenders.

- Implementation of the provisions of the Council of Europe Convention on Cybercrime, Computer Viruses, Quick Data Retrieval and Interception of Computer Data.

- Implementation of Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse, sexual exploitation of children and child pornography.

- Completion of the Law on preventing and fighting cybercrime, with a view to adopting a National Plan for Prevention and Fight against Cybercrime.

- Implementation of Council Directive 2008/114/EC of 8 December 2008 "Identifying and designating European Critical Infrastructures and assessing the need to improve their protection" by defining a number of relevant notions and defining the obligations of critical infrastructure owners and operators.

Comments sent by / Commentaires envoyés par La Strada - Moldova

Question 14.

The challenge faced during investigation phase relates to the intention of producing, possessing, and distributing self-generated sexual explicit images depicting children. The national law is ambiguous and unclear with regard to the intention of such actions. Consequently, a child of age 16 (in some cases a child of age 14) can be prosecuted for these kinds of behaviour.

Another challenge faced in the prosecution phase relates to classifying the content that is not sexually explicit. As the Lanzarote Committee is very specific in defining differences between sexually explicit images/videos and sexual content, on the national level, there is no content classification (including online).

One of the main challenge remain to be the capacities of professionals in investigating and prosecuting ICT facilitated child sexual abuse online and sexual exploitation online, as there is a lack of specialized trainings on the subject for law enforcement, prosecution and courts.

MONACO

State replies / Réponses de l'Etat

Question 14.

A ce jour, les forces de l'ordre n'ont pas constaté de difficultés particulières dans le cadre de la poursuite de ce type d'infraction.

MONTENEGRO

State replies / Réponses de l'Etat

Question 14.

The Prosecutor's Office is a body for prosecuting perpetrators of criminal offenses. We believe that in all cases in which the perpetrator has been identified, the prosecution effectively conducts criminal proceedings. The biggest challenge that arises in this issue is the revealing of perpetrators of these crimes.

NETHERLANDS / PAYS-BAS

State replies / Réponses de l'Etat

Question 14.

There are all kind of challenges, like combatting online sexual child abuse on the Dark web, the growing reports of online sexual child abuse (child pornography, sexting) mostly form NMEC.

NORTH MACEDONIA / MACEDOINE DU NORD

State replies / Réponses de l'Etat

Question 14.

There is no sufficient information for an adequate response.

NORWAY / NORVEGE
State replies / Réponses de l'Etat

Question 14.
On a general note, the Norwegian Prosecuting Authority describes increased priority of cases involving children and sexual offences with an online element. The handling of criminal cases, investigation, decisions on whether to prosecute, as well as the prosecution of cases in court has been impacted by cybercrime-related cases. Such cases are often complicated and may require substantial resource use. E.g. cases involving the sharing of sexually explicit material can involve many victims and offenders, have cross-jurisdictional aspects and require extensive international judicial cooperation.

POLAND / POLOGNE
State replies / Réponses de l'Etat

Question 14.
The issues of the origin of the content (self-generated or made by other person), victim's consent, and means employed by perpetrator (e.g. use of ICT) do not affect the criminal evaluation of the production (recording, performing), and possession of, as well as the obtaining access to the content involving children.

The main challenge is a proper and adequate assessment of such content in order to distinguish whether its character is sexually explicit but legal or pornographic content. The latter allows the prosecution of the offenders while the former may only result in family court and social services based on minor demoralization.

PORTUGAL
State replies / Réponses de l'Etat

Question 14.a.
High and fast evolution of information and communication technologies that the legislative creation can't follow immediately.

Age victim assessment is also a problem especially in relation to children between 16-14 years or under 14 years old.

Difficulties arise in the identification of the perpetrator of the crime due to problems in collecting valid electronic evidence - due to time limits for preserving data traffic (short and different from country to country) and access to them, namely when collecting data from the data holders, especially technologic companies with headquarters abroad. Connecting a particular person to the computer system is also difficult.

Most of the time it takes too long to obtain an answer.

Difficulties appear in retaining the dissemination of the images / videos and consequent continuous victimization of the child.

Related to the same issue, there are difficulties on international police and judicial cooperation, (in particular outside European Union).

Question 14.b.
See answer to previous question.

ROMANIA / ROUMANIE
State replies / Réponses de l'Etat

Question 14.
Generally, with regard to cybercrime - including in the case of child pornography - there are common problems identified at European level:

- the cross-border nature of the criminal activity requiring the obtaining of evidence through international judicial assistance, whether it is victim-related complaints or that it is about identifying IP addresses or other data;

- legislative differences between countries;

- encryption and anonymisation (generally the specialization of suspects in the technical field);

- lack of virtual currency regulation (currently preferred as a means of payment, including when it comes to blackmailing victims);

- lack of solutions for accessing data storage in the cloud;

- the lack of unitary data retention.

Also a challenge is sometimes the difficulty of obtaining testimonies from victims, as a consequence of trauma suffered during abuses. Instances of sexual abuse of minors usually involve specialists, such as psychologists and social workers within the Social Assistance and Child Protection Services, by providing consultations and introducing dedicated programs, making specialized reports, or even actually presenting places in home searches are carried out if urgent takeover of children is required. Subsequently, they continue to provide support to overcome the trauma suffered by providing specialist treatment.

RUSSIAN FEDERATION / FEDERATION DE RUSSIE
State replies / Réponses de l'Etat

Question 14.
The surveyed agencies have not got any information from the ground divisions

SAN MARINO / SAINT-MARIN
State replies / Réponses de l'Etat

Question 14.
Regarding San Marino law enforcement authorities, the lack of specific cases has so far prevented authorities from considering this a critical issue. In the past, also investigations regarding adults entailed serious difficulties when images were located in servers based in poorly collaborative countries.

SERBIA / SERBIE
State replies / Réponses de l'Etat

Question 14.
Public Prosecutor Answers:

Anonymity offered by the Internet, and closed nature of groups/networks within which such contents are shared are main challenges that Service for Cybercrime of the Ministry of Interior of the Republic of Serbia is faced with as a body in charge to detect crime offences and perpetrators and the Special Prosecution Office for Cybercrime that manages pre-investigation and investigation proceedings.

Comments sent by / Commentaires envoyés par Coalition for Monitoring Child Rights

Question 14.
The major problem is lack of licenced IT court expert witnesses that play a key role in criminal court proceedings who need additional specialized knowledge on child online sexual exploitation.

SLOVAK REPUBLIC / REPUBLIQUE SLOVAQUE
State replies / Réponses de l'Etat

Question 14.
In the area of legislation, there are challenges related to legislative regulation of data storage of telecommunications and stating of unified and reasonable term until the data are stored by the telecommunications service providers. Within the status quo, after the derogation of an EU Directive[2] and subsequent step on the national level and change of the acts concerned[3], providing with the information of user IP address is exclusively dependent on the decision of telecommunications service provider. Before mentioned could cause problem in the application practise and prevent from possibility to act quickly and effectively with regard to severity of this type of criminal activity.

While investigating this type of criminal activity, the law enforcement authorities also face to several technical challenges- the continuous development in the area of ICTs sets up high requirements on the amount of employees, their structure and specialisation within individual areas of ICTS, but mostly on their continuous lifelong learning. Regarding rapid development of technologies, it is primarily difficult to obtain evidence. Significant demands are also imposed on obtaining computer data throughout court orders, expert evidence, legal aid (when contact and "sharing" pornography material through Facebook, the evidence is ensured throughout the legal aid to the US). These operations are time-consuming, but necessary for offender identification as well as to prove guilt of committing the criminal offence.

SLOVENIA / SLOVENIE
State replies / Réponses de l'Etat

Question 14.
State prosecutors face numerous challenges in pre-trial and criminal proceedings concerning these crimes. It is best necessary to highlight the quantitative extent of the seized evidence (electronic and

[2] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC was declared invalid by the Court of Justice of the European Union ruling on 8th April 2014.
[3] Finding of the Constitutional Court no. 10/2014-78.

communication technologies containing such content), which makes the evidence procedure extremely complex and demanding. These circumstances effect on the length of the procedure. In practice, it has also accrued a difficulty with proving the age of the victim (whether the pornographic or other sexual material includes minors or not) — in respect to the criminal offence of Presentation, Manufacture, Possession and Distribution of Pornographic Material (Criminal Code, Article 176/3 paragraph).

The Police reports that the biggest problem is underreporting of criminal offences of this type, furthermore lack of technical and human investigative resources, furthermore lack of understanding by the lay public of extensive and demanding police work in this field.

Comments sent by / Commentaires envoyés par Association Against Sexual Abuse

Question 14.
In our opinion, with a lack of specialized staff.

SPAIN / ESPAGNE
State replies / Réponses de l'Etat

Question 14.
Main challenges come from the difficulties for identifying the IP directions with the real users in case of finding sexual abuse materials by internet. Once the user is identified, his material shows underage victims that most times can not been identified at all, because only images but not personal data are found.

SWEDEN / SUEDE
State replies / Réponses de l'Etat

Question 14.a.
Evidence and other contents of the case file of sexually explicit nature are considered classified and are subject to a confidentiality assessment if someone requests access to the case file. In the same way, evidence and other information of sexually explicit nature are assessed beforehand and presented in a part of the trial open only to the parties.

Question 14.b.
Prosecution: One of the biggest difficulties that can be encountered during the preliminary investigation is if the prosecutor does not have a known offender and it's hard to track them. To succeed you need IP numbers, subscriber data, etc. from the telecommunications companies. It is very different from different telecommunications companies what tasks can be obtained but generally it has become more difficult since the verdict regarding data retention.

The prosecutor can also encounter difficulties with obtaining material from servers located in other countries, as mutual legal aid may in some cases take a long time. Another problem is how to legitimately consider and handle cloud services (images are often saved in different types of cloud services and how to access what's in the cloud, and to get the material deleted if it's child pornographic).

Evidence and other contents of the case file of sexual nature are often considered classified and are subject to a confidentiality assessment if someone requests access to the case file. In the same way, evidence and other information of sexual nature are assessed beforehand and often presented in a part of the trial open only to the parties.

SWITZERLAND / SUISSE
State replies / Réponses de l'Etat

Question 14.

- Apparition régulière de nouveaux phénomènes (par ex. sextorsion, live streaming, etc.) et de nouveaux modes opératoires.
- Les grandes quantités de données et le cryptage nécessitent beaucoup de temps.
- Anonymisation / Darknet.

TURKEY / TURQUIE
State replies / Réponses de l'Etat

Question 14.

Main challenge that all authorities deal with regarding online sexual abuse of children is its international dimension and the difficulty arising from this particularity in regard to collection of evidence. In order to collect evidence of an ICT facilitated sexual offence, law enforcement and prosecution offices have to address international police or judicial cooperation, which should be faster and prompt.

UKRAINE
State replies / Réponses de l'Etat

Question 14.

The problems are common to all sexual crimes through information and communication technologies.

Comments sent by / Commentaires envoyés par Parliament Commissioner for Human Rights

Question 14.

Among the difficulties, it should be indicated the following: the difficulty of proving guilt, distrust of law enforcement officers to the testimony of a child, repeated interrogation of a child, and delaying pre-trial investigation. The absence of specially trained specialists for interrogation of a child, taking into account his/her vulnerable state, age and best interests.