NATIONAL SCHOOL OF JUDGES

THEMIS Competition 2018
Semi Final A - International Cooperation in Criminal Matters

CHILD PORNOGRAPHY IN A CLOUD ERA

Cloud Security Alliance cautions on the safety of Qantum Computing!

A. INTRODUCTION
- i. The case scenario

B. ISSUES TO BE ADDRESSED
- i. Legal framework on child protection
- ii. An insight to Budapest Convention
- iii. Who is a Child?
- iv. The Budapest Convention from human rights' perspective
- v. Jurisdictional issues of the case – scenario

C. LEGAL FRAMEWORK ON PROCEDURAL LAW AND INTERNATIONAL COOPERATION
- i. International cooperation
  - a. Between the EU and the US
  - b. Within EU Member States
- ii. Introducing JITs
- iii. Operation of JITs
- iv. The European Investigation Order Directive

D. AN OVERALL REVIEW OF THE ISSUES DISCUSSED
- i. Admissibility of evidence shared by the parties within a JIT
- ii. The need for harmonisation in a digital era

TEAM GREECE:

VASILIS DIMOULAS, TRAINEE PUBLIC PROSECUTOR
MARIA KARAGIANNI, TRAINEE PUBLIC PROSECUTOR,
EUGENIA PATRONI, TRAINEE JUDGE
LAMPROS TSOGKAS - PUBLIC PROSECUTOR
HEAD OF PUBLIC PROSECUTOR'S OFFICE IN THESSALONIKI COURT OF FIRST INSTANCE

A. INTRODUCTION

Developments in information technology have a conspicuous effect on all aspects of society. The ease of accessibility of information contained in computer systems, combined with the practically unlimited possibilities for its exchange and dissemination, regardless of geographical or national limitations, has led to an explosive growth in the amount of information available and the knowledge that can be drawn there from[1]. Inevitably, rapid expansion of the internet has created new opportunities for criminals to exploit[2]. New types of crimes have been emerged and traditional crimes are now committed easily by means of new technologies[3].

In this context, child pornography, a rather old phenomenon, has turned out to be the second, after drug trafficking, most profitable globalised illegal activity. A major factor contributing to this outcome is that nowadays the distribution of illicit material no longer conducted via traditional electronic methods, such as visiting ordinary web sites or sharing email attachments, but through newly introduced "hidden" services such as Tor Network, Freenet, Dark Web, or even through Cloud computing, a new way of storing, managing and distributing data.

Users of Cloud do not download material or install applications on their own device or personal computers, as all processing is done through the internet and storage is maintained by the Cloud server. They may permit, though, to other designated users to have shared access to their files. Thus, the Cloud allows practically anyone, to use publicly accessible software from anywhere. As a result, cybercrime investigators must deal with potentially thousands of Cloud users associated to a sole public address. This fact renders the investigations considerably time-consuming and generates privacy and data protection issues for many innocent customers not connected to the illegal activities.

Subsequently, the fact that perpetrators use Cloud's remote access to remain untraceable challenges traditional methods of acquiring and collecting electronic evidence. The increased implementation of encryption, the development of remote and multi-layered storage and the use of decentralised virtual currencies, such as Bitcoin – so that no one "follows the money"- stand

[1] Explanatory Report to the Convention on Cybercrime, Council of Europe, recitals 2, 4 and 5
[2] Decker, C. (2008) Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the changing Nature of Cyber Crime, Southern California Law Review, 81, 959 – 1016
[3] Explanatory Report to the Convention on Cybercrime, Council of Europe, recital 5

in the way of law enforcement agencies that cannot easily associate criminal activity back to the end-user.

According to inhope.org statistics, 21% of trafficked material depicts teenage minors, 72% pre-minors and 7% infants. As for the origin of reports, 40% comes from Europe, 44% from the US and 18% from the rest of the world[4]. The fact that child abuse cases increase exponentially on a global scale due to the unprecedented information technology development, justifies fully the intense effort that has been made by international institutions to equip the armory of judicial authorities with more efficient tools to combat child sexual abuse and exploitation.

In this study, a case scenario will be used as a vehicle to explore the relative legislative provisions and how the existing range of instruments on international cooperation, can be applied in order to ensure that e-evidence will be collected and preserved properly, as well as to reveal the criminal activity of involved persons and to hold them accountable for their actions under criminal Law. The attempted analysis will include a critical review of current international treaties and will end up proposing certain ways to face future challenges provided by the rapid evolution of internet technology.

i. Case Scenario

In the late afternoon of 21st of November 2017, the Cyber Crime Division in Greece receives a SIENA[5] message from Interpol, containing information about a case of production and distribution of child pornographic material. A group of people in Texas, USA (hereinafter Group A), produces video and images of (1) real child sexual abuse, (2) material depicting persons over eighteen years, appearing to be minors though, engaged in sexually explicit conduct, as well as (3) computer generated material of virtual children, which in turn uploads to the Cloud. Another group of people in Greece (hereinafter Group B) has been granted access to the Cloud by using passwords, in return for a large amount of money. Group B downloads pornographic material and distributes it for profit, both through the Internet and by other means to individual users. As soon as they received the information,, Greek police authorities launched an investigation, which resulted in the exposure of a third group (hereinafter Group C) consisting of Italian

[4]Christaki, I., (2017) Online assault of minors at 19th chapter of Greek Penal Code, available in Greek at: http://ikee.lib.auth.gr/record/289490/files/GRI-2017-19256.pdf

[5]Secure Information Exchange Network Application, managed by Europol. Over the course of 2017, more than one million SIENA messages were exchanged among Europol, Member States and third parties.

nationals, who were implicated in further distribution. However, some other findings came to surface, since individuals in France and in Germany have paid money to Group B and C in order to download child pornographic material.

B. ISSUES TO BE ADDRESSED

i. Legal Framework on cyber crime and child protection

Greek legislation on cybercrime and on child protection[6] stems from international framework documents and reports of the European Union and the Council of Europe. Recent amendments of the Greek Penal Code (hereinafter GPC) have been founded on Directives 2011/93/EU and on 2013/40/EU, which in turn, built onthe 2001 Council of Europe Convention on Cybercrime, also known as Budapest Convention, that constitutes a historic milestone in the combat against cybercrime. Beyond the Budapest Convention, at European level, one can also point out as of great significance the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, also known as Lanzarote Convention.

At UN level, two significant legal instruments has been introduced; the United Nations Convention on the Rights of the Child (UNCRC) and the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography, that came into force on 18 January 2002. The UNCRC acknowledges that every child has basic fundamental rights, one of which is protection from violence, abuse or neglect. In Art 34 UNCRC lies the first and direct reference at an international level, on the topic of child pornography, long before this phenomenon escalated dramatically.

ii. An insight to Budapest Convention

Ratification of the Budapest Convention by all Member States of the Council of Europe and accession to it by major other States[7], has contributed, accordingly to what was principally aimed, to harmonising the domestic substantive criminal law elements of offences and associated provisions in the area of cybercrime. The Budapest Convention also includes domestic criminal procedural law powers that States must implement to facilitate the investigation and prosecution of offences and provides for specific mechanisms of mutual assistance, to setup a fast and

[6] Applicable articles: 348A , 348B and 348C GPC

[7] To date fifty six countries have ratified or accessed the Budapest Convention, whereas four more countries have signed but not ratified it yet.

effective regime of international cooperation[8]. However, its provisions on international cooperation do not supersede other international legal instruments and especially international agreements on Mutual Legal Assistance, which will be later on analysed in detail[9]. Similar to that, the Lanzarote Convention provides that the Convention shall consist a free standing legal base for mutual assistance between parties in cases where there are no special agreements applicable[10].

In accordance with Art 9(1) of the Budapest Convention, GPC criminalises any conduct committed intentionally which involves (a) producing for purposes of distribution, (b) offering or making available, (c) distributing or transmitting, (d) procuring for oneself or for another person and (e) possessing child pornography in a computer system or on a computer-data storage medium. In view of Art 9(2), the term "child pornography" includes pornographic material that visually depicts (a) a minor engaged in sexually explicit conduct, (b) a person appearing to be a minor engaged in sexually explicit conduct and (c) realistic images representing a minor engaged in sexually explicit conduct. The Explanatory Report to the Convention gives also a detailed and clear definition of a "sexually explicit conduct". It is the conduct that encompasses real or simulated sexual intercourse, bestiality, masturbation, sadistic or masochistic abuse in a sexual context or lascivious exhibition of the genitals or the pubic area of a minor[11].

iii. Who is a Child?

With respect to the case scenario, perpetrators in the US produced both real and computer created child sexual abuse material. This distinction stimulates further discussion on who is perceived to be a child victim in relation to child pornography offences.

Definition of "child" is socially and temporally situated as are views about appropriateness of adult interest in children and what constitutes pornography[12]. Law definitions are pragmatic, oriented to ensure that there is a certainty as to who is a child[13]. Art 9(3) of the Budapest Convention defines the term "minor" in relation to child pornography in general as all persons younger than eighteen years, in accordance with the definition of a "child" in the UN Convention on the Rights of the Child (Art 1). Nevertheless, recognising that certain States

[8] Explanatory Report to the Convention on Cybercrime, Council of Europe, recital 4
[9] Without prejudice to the exceptions of Art. 25(4) and 27 (4) of the Budapest Convention
[10] Art 38(4)
[11] Explanatory Report to the Convention on Cybercrime, Council of Europe, recital 100
[12] Taylor, M., Quayele, E., (2003) Child Pornography, an Internet Crime, New York: Routledge, p. 3
[13] Gillespie, A., (2011) Child Pornography, Law and Policy, NYQ Routledge, p. 17

require a lower age-limit in national legislation regarding child pornography, the last phrase of Art 9(3) allows the parties to provide a different age-limit, provided it is not less than sixteen years[14]. This flexibility constitutes a point of difference between the Budapest Convention and the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, known as The Lanzarote Convention. The latter, which was signed on 25 October 2007, defines a child as any person under the age of 18 years and does not allow reservations to be made.

Beyond the age dimension, the answer to the formerly addressed question is also affected by stimuli provided by new technologies and so is the corresponding legislative response. Indeed, pornographic images of virtual children can be computer created from scratch, even if an original image of a real child never existed in the first place or in other cases an original photo depicting an adult could be morphed into child pornography[15].

Art 9(4) of the Budapest Convention gives States the discretion not to adopt legislation combating child pornography when the person depicted is not a child, either because a) the person is older than eighteen years (or sixteen in certain countries) or because b) it is a virtual child. The differentiation in the handling of cases involving real and not real children is justified by the legal interests aimed to be protected. Criminalisation of child pornography when a minor is involved focuses directly on the protection against child abuse. On the other hand, criminalisation of non-real child pornography aims at providing protection against behaviour that, while not necessarily creating harm to a "child", might encourage or seduce children into participating in such acts (grooming), and hence form part of a subculture favouring child abuse[16]. The scheme of prohibiting virtual images but allowing a reservation to be made is followed into the Lanzarote Convention[17]. Art 20(1) clearly covers virtual child pornography although Art 20(3) provides signatory States with the opportunity to opt out of criminalizsing the possession or production of material that consist exclusively of simulated representations or realistic images of non-existent child.

A glaring example that underlines the importance of including or not virtual child in the definition of child is sexual ageplay. Sexual ageplay refers to adults engaging in sexual activity

[14] Explanatory report to the Convention on Cybercrime, recital 104
[15] Gillespie, A., (2011) Child Pornography, Law and Policy, NYQ Routledge, p. 100
[16] Explanatory Report to the Convention on Cybercrime, paragraph 102
[17] Gillespie, A., ibid p. 104

with one or more of them role-playing as a child[18]. In real life, such behaviours between consenting adults may be considered as unusual, fetish or even deviant, but they are not in any case illegal[19]. However, although virtual sexual ageplay is essentially the same behaviour conducted online, it is regarded as much more problematic; it is regarded as the simulated sexual abuse of children in online environments[20]. Online sexual ageplay is, therefore considered to suggest a sexual interest in children by the adult players who use child computer characters (known as avatars) to act out scenes of child sexual abuse[21].

The Budapest Convention sets the foundation for a common legal background on a national level for all States participating in the case scenario. However, the US has reserved the right not to apply provisions for child pornography if the person involved appears to be minor or if the pornographic material is computer created[22]. France has also reserved the right to apply Art 9(1) to any pornographic material that visually depicts a person appearing to be a minor engaged in sexually explicit conduct, in so far as it is not proved that the said person was eighteen years old on the day of the fixing or the registering of his or her image[23].

iv. The Budapest Convention from human rights' perspective

It is undoubtable that the Budapest Convention took great steps towards the protection of children from exploitation and abuse through Internet. However, certain weaknesses of the Convention have also been identified. Art 9(4) permits States not to criminalise, in whole or in part, procurement and possession of child pornography[24,25]. This flexibility, which was added to the Member States' right to determine different age limits when introducing criminal provisions on child pornography, could lead to disparities in criminal legislation of the ratifying States. Such legal diversity could then hinder cross-border law enforcement operations, in case that the

[18]Reeves, C., (2018) The virtual simulation of child sexual abuse: online gameworld users' views, understanding and responses to sexual ageplay, Ethics and Information Technology, available at: https://doi.org/10.1007/s10676-018-9449-5

[19]Richards, C. (2015). Further sexualities. In C. Richards & M. J. Barker (Eds.) The palgrave handbook of the psychology of sexuality and gender. Palgrave MacMillan, Basingstoke, pp 60–76.

[20]Reeves, C. (2013) Fantasy depictions of child sexual abuse: The problem of ageplay in Second Life. Journal of Sexual Aggression19, p. 236–246

[21]Reeves, C., (2018) Ibid

[22] Reservation contained in the instrument of ratification deposited on 29 September 2006

[23] Reservation contained in the instrument of approval deposited on 10 January 2006

[24]The term "procuring of child pornography" refers to the active obtaining of such material, such as downloading it

[25]In the light of recital 98 of the Explanatory Report, the Convention appears to acknowledge that possession of child pornography may stimulate production and demand for such material. However, the Convention does not establish an actual obligation on States to attach criminal consequences to the last link of the production chain, namely the possessor.

States involved do not criminalise the same conduct or content[26]. Jurisdictions that have promoted criminalisation of virtual child pornography have based their stance on the nexus between virtual and real child pornography. This nexus implies that such imagery contributes to the normalisation of child sexuality, exploitation and abuse and it is correlated with other criminal activity, such as grooming of children and possession of real life child abuse images[27]. Moreover, the existence of virtual child pornography makes it difficult to eliminate the market for real child pornography and to prosecute those who produce material using real children[28].

The Budapest Convention has been subject to criticism on a human rights protection basis and especially regarding the right to free speech, on the right to privacy and on the right to data protection. In Ashcroft v Free Speech Coalition,[29] US Supreme Court accepted that Child Pornography Prevention Act of 1996, which extends prohibition against child pornography to sexually explicit images that *appear* to depict minors but were produced *without using any real children*, abridges the freedom to engage in a substantial amount of lawful speech.

Concerns have also been voiced as regards the difficulty of the Convention to meet data protection principles that the Council of Europe itself has established in the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the 1999 Recommendation R(99)5 in relation to privacy on the Internet. These legal instruments are not directly referred to either within Art 15 (Conditions and Safeguards) of the Convention or within the Preamble of the Cybercrime Convention, to ensure that the Council of Europe, its member States, and future signing States are also committed to data protection and fair privacy practices as set out by the Council of Europe[30].

Another objection to the Convention refers to the compromising of the right to privacy due to certain powers and procedures. According to the Convention, possible infringements of rights in the case of interception of communications and surveillance practices are subjected to the conditions and safeguards that are provided by the domestic law of each Party. However, those standards and safeguards vary among the States, even within the Council of Europe region

[26]Akdeniz, Y., (2008) Internet Child Pornography and the Law, Brookfiled: Ashgate
[27] Reeves, Ibid
[28] Gillespie, A., Ibid, p. 107. From (2) to (4): arguments of the US Attorney General in Ashcrof v Free Speech Coalition, 122S.Ct. 1389 (2002)
[29]Ashcroft v Free Speech Coalition 122S.Ct. 1389 (2002)
[30]Center for Democracy & Technology (CDT), An Advocacy Handbook for the Non Governmental Organizations, Available at: http://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf

despite the existence of the European Convention on Human Rights. Rather than leaving the decision making to the parties, common safeguards based upon the ECHR and the jurisprudence of the Strasbourg Court should have been provided within the 2001 Convention. If individuals are to be protected from arbitrary interference by the authorities, then a legal framework and very strict limits on such powers are called for. Therefore, the implementation of Art 15 of the Convention by parties needs to be sharper and more explicit in terms of guaranteeing rights to citizens[31].

v. Jurisdictional issues of the case – scenario

In the given cross-border case scenario, several jurisdictional issues emerge regarding both the competence of the national Prosecutor to initiate criminal proceedings against all involved persons, regardless of their residence or nationality and the so-called "investigative jurisdiction", namely the right of national authorities to carry out investigations within the territory of other states.

According to Art 5(1) of the GPC "Greek criminal Law is applicable regarding all offences committed in Greek territory", while according to Art 5(3) GPC "offences committed through the Internet or other means of communication, are considered to have been committed in the Greek territory too, as long as access is granted to those means in Greek territory, regardless of their place of hosting". Furthermore, by virtue of Art 8 GPC which establishes the principle of universal jurisdiction, "Greek criminal Laws are applicable against Greek citizens or foreigners for the prescribed[32] offences committed abroad, regardless of the laws applicable in the place where they were committed". Greek Penal Code, including Art 8, has been amended by a special law (L 4267/2014) to meet provisions of Art 17(1), 17(2), 17(3) and 17(4) of Directive 2011/93 of the European Parliament and Council. Art 8 of GPC illustrates the general principle of universality, in which international security, as one of the universal legal rights, has led to fostering a worldwide prosecuting web that aims to eliminate national "paradises" and to trap the perpetrators across the globe[33].

[31] Ibid, p. 11
[32] Child pornography and child sexual abuse is included (Art 8h)
[33] Anagnostopoulos, I., (2008), Ne bis in idem: European and International Aspects, P.N.SAKKOULAS publ. p. 5

Pursuant to those articles the Greek Public Prosecutor has jurisdiction to investigate the case and prosecute the perpetrators of online child pornography and child sexual abuse[34] committed in both the US and Italy.

C. LEGAL FRAMEWORK ON PROCEDURAL LAW AND INTERNATIONAL COOPERATION

Cybercrime investigation may involve some form of invasive or coercive measures including search, surveillance, or monitoring activity by law enforcement or intelligence agencies[35]. Search and seizure is an active mode of investigation, which involves discovering evidence, identifying suspects, apprehending offenders, and interviewing witnesses. Legal authority and best practices for executing search and seizure warrants varies considerably between jurisdictions and criminal justice systems, including rules governing handling electronic evidence[36]. In this context, several international instruments were introduced tominimise potential procedural obstacles towards protection of child victims of such crimes.

i. International cooperation

a. Between the EU and the US

When it comes to acquisition of e-evidence within an international environment, the applicable legal instruments are the Mutual Legal Assistance Treaties (MLATs), which constitute a mechanism for establishing international legal assistance through bilateral or multilateral agreements between States.

In the present case-scenario, the applicable instruments for establishing international cooperation between Greek and American competent authorities are (1) the MLA Agreement of 26 May 1999 between USA and Greece[37], (2) the MLA Agreement of 25 June 2003 signed between EU and USA in 25 June 2003[38] and (3) the Protocol supplementing the original GR-US MLA Agreement of 1999 which was signed in 18.01.2016[39].

[34] 187, 348A and 348C GPC
[35] Brown, C., (2015), Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice, International Journal of Cyber Criminology, vol. 9, issue 1, p. 55-119
[36] Jarrett, H. M., & Hagen, E. (2009), Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, United States Department of Justice, Office of Legal Education Executive Office for United States Attorneys. Available at: http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf
[37] Ratified by Greek Law 2804/2000
[38] OJ L 181/34
[39] Ratified by Greek Law 2804/2000. This Protocol was signed pursuant to Art 3(2) of the EU –US MLA Agreement

According to Art 1(3) of the GR-US 1999 MLA Agreement "the assistance shall be provided *without regard* to whether the conduct that is the subject of the investigation, prosecution, or proceeding in the Requesting State would constitute an offense under the laws of the Requested State." Given the above provision, the request of assistance made by the Greek Prosecutor concerned both real and virtual child pornography material, even though the latter is not an offence under US Law. Executing the request, the US authorities issued a local subpoena or search warrant and the gathered evidence[40]was handed over to Greek authorities. At the same time, the competent Judicial Council in Greece issued a decision that allowed the lift of the suspects' secrecy of communications[41], so that their identity and the details of their criminal activities would be revealed.

b. Within EU Member States

The judicial cooperation in criminal matters among EU Member States has always been considered as of paramount significance. The first Convention that governed this area was the European Convention on Mutual Assistance in Criminal Matters of the Council of Europe of 1959[42] (hereinafter CoE Convention) with its two additional protocols of 1978[43] and 2001[44]. It as ratified by Greece with Decree-Law 4218/1961[45]. In its provisions, it introduced the locus regit actum principle by providing in Art 3 that "the requested party shall execute in the manner provided for *by its law* any Letters Rogatory […] addressed to it by the judicial authorities of the requesting party". Furthermore, in accordance with the mutual assistance principle, a broad scope of grounds for reasoned[46] refusal was provided in cases where a) the request concerned an offence related to or constituting itself a political offence or a fiscal offence and b) the requested party considered that the execution of the request was likely to prejudice the sovereignty, security, ordre public or other essential interests of its country[47].

---

[40] i.e. IP addresses, contact information of users associated with the IP addresses, IP logs, data and metadata, the length of service, the types of service utilized by the users and sources of payments associated with the service, including credit cards and bank account numbers

[41] Pursuant to Art 4 of Law 2225/1994 and Art 253 and 253A of Greek Criminal Procedural Law (GCRC)

[42]CETS No 30

[43]CETS No 99

[44]CETS No 182

[45]With reservations regarding Art 4 of the Convention which is incompatible with Art 97 of GCCP and Art 11 which is incompatible with Art 459 of GCCP. The Additional Protocol of 1978 was also ratified by Greece by Law 1129/1981

[46]Art. 19 CETS No 30 "Reasons shall be given for any refusal of mutual assistance"

[47]Art 2 CETS No 30

In the meantime, the signing of the European Treaties of Maastricht, Amsterdam and Nice as well as the establishment of the Schengen acquis,[48] introduced the idea of a European area of freedom, security and justice, which, in turn, should be safeguarded in the internationally organised crime by an advanced international cooperation in criminal matters. Hence, in 2000 the European Council established in accordance with Art 34 of the Treaty on European Union, the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 29.05.2000[49] (hereinafter EU MLA Convention). The EU MLA Convention, even though it was meant to supplement the relevant pre-existing instruments on international cooperation[50], it adopted itself the forum regit actum principle, in contrast to the locus regit actum principle introduced in CoE Convention of 1959. It therefore prescribed that "the requested Member State *shall comply* with the formalities and procedures expressly indicated by the requesting Member State"[51], unless otherwise provided in the Convention and given that these formalities and procedures are not contrary to the fundamental principles of law in the requested MS.

ii. Introducing JITs

In an effort to promote the international cooperation procedures, it should not be neglected the fact that the efficiency of a legal instrument is analogous to the efficiency of the tools through which it is applied. Thus, the EU MLA Convention of 2000, apart from providing several investigative measures, has also regulated the conditions under which a Joint Investigation Team could be established and operate between Member States[52].

According to the definition given in the Joint Investigation Teams Practical Guide of the Council,[53] these teams constitute an international cooperation tool based on an agreement between competent authorities (both judicial and law enforcement) of two or more States.

[48]OJ L 176, 10.7.1999
[49]OJ C 197, 12.07.2000
[50]Art 1 of the Convention OJ C 197, 12.07.2000
[51]Art 4 OJ C 197, 12.07.2000
[52]The idea of establishing common teams for the facilitation of the international cooperation was already proposed in the Council Action Plan to Combat Organised Crime of 28 April 1997, OJ 97/C 251/2001, Political Guideline 8 (10) and in Art 30 of the Treaty on EU OJ 321/1, Art 32 where it is stated that the Council shall promote cooperation through Europol to the goal of "operational actions of joint teams", while in Conclusion no 43 of European Council in Tampere the set up of joint investigative teams was considered to be " the first step to combat trafficking in drugs and human beings as well as terrorism"
[53]OJ C 18, 19.1.2017

However, the slow rate of its ratification[54] and the large scale terrorist attacks of 11th September 2001[55]led to the decision that the instrument of JITs should be established separately, on the basis of Art 34(2b) of the Treaty on EU, though a Framework Decision. Accordingly, Framework Decision 2002/465/JHA[56]repeated the already existing provisions on JIT, but through its binding effect regarding the result to be achieved[57], led the Member States to take action for its transposition into national law. In Greece it was transposed by Art 13 of Greek Law 3663/2008, whilst the Convention of 29 May 2000 has not been yet ratified by the Greek Parliament.

JITs were also established within the regulatory scope of several bilateral or multilateral international instruments, such as (1) the Second Additional Protocol of 2001[58] to the Council of Europe Convention of 1959, (2) the Mutual Legal Assistance Agreement between EU and the USA of 6 June 2003[59], (3) the agreement on the application of provisions of the EU MLA Convention of 2000 to Norway and Iceland[60], (4) Police Cooperation Convention for South East Europe (PCC-SEE of 2006)[61], (5) United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances[62] and (6) United Nations Convention against Transnational Organized Crime (UNTOC)[63] and against Corruption (UNCAC)[64].

iii. Operation of JITs

In the case scenario under discussion, the fact that the investigation from Greek law enforcement agencies linked to Italian Group C, which was also distributing the illicit material, had led the Greek authorities to communicate with the Italian ones and consider the possibilities of judicial cooperation under EU legislation. Regarding the relevant applicable instruments, Greece have not ratified the EU MLA Convention[65] whilst Italy did not ratify it until 22 February 2018. As a result, the remaining applicable framework was fragmented with

[54]The Convention entered into force only in 2005 while it has not still been ratified by Croatia, Greece and Ireland. Italy ratified it on 22/2/2018
[55]As considered in the extraordinary Council Meeting on JHA and Civil Protection of 20 September 2001
[56]Framework Decision 465/JHA of 13 June 2002, OJ L162/1, 20.06.2002
[57] Art. 34 (2)(b) TEU
[58]CETS No 182
[59]Art.5 of EU-US MLA Agreement, OJ L 181, 19.07.2003 pp 34-42. Ratified by Greece with Law 3771/2009.
[60]OJ L 26, 29.01.2004. pp. 3-9
[61]Art 27. Registration with the Secretariat of the UN : Albania, 3 june 2009, No 46240
[62]Art 9 UN Treaty Series, vol 1582, p.95
[63]Art 19 UN Treaty Series vol 2225, p.209
[64]Art 49 UN Treaty Series vol 2349, p.41
[65]Along with Croatia and Ireland

insufficient regulation of cooperation issues. It was therefore contemplated that in lieu of a broad-scope Legal Assistance under CoE MLA Convention, there was another and probably more efficient tool available; the establishment of a Joint Investigation Team.

JITs are not a generic form of police or judicial cooperation but they are set to serve a specific purpose within a limited duration. More specifically, there are two situations where a JIT can be established i) in demanding cross-border investigations and ii) in cases where connected investigations require coordinated, concerted action in more than on Member States.[66]

In the operation of JITs the locus regit actum principle is established in the relevant instruments,[67] prescribing that the team operates in accordance with the Law of the MS in which it operates. The organisation of the team is also conducted by the MS in which it operates, whilst members from other parties are referred to as "seconded members".

One of the advantages of a JIT is the fact that all the information that a MS holds can be provided to the Team according to Art 13(9) of MLA Convention[68] without the need to recur to mutual assistance or mutual recognition instruments, while all the information gathered by the team is immediately available to all its members[69] within the purposes for which the team was set up. However, use of such evidence in the prosecution of other offences depends on the prior consent of the MS that rendered the information available according to Art 13(10)[70], whilst grounds for withholding its consent are found in Art 13(10b-d)[71].

Regarding the investigative measures that might be necessary, it is provided in Art 13(7)[72] that when the investigative measure needs to be executed in one of the Member States, the seconded member originating from that State can request its competent authorities to take those measures, under the conditions of their national legislation. This is considered to be one of the biggest advantages of JITs, because in these cases a formal request is not required and thus a check for refusal will not take place, since this request is "as if it were a request in a national

[66] Art 13 (1) EU MLA Convention of 2000
[67] Art 13 (3)(b) EU MLA Convention, Art 1 (3)(b) FD 2002/465/JHA, Art 19(1) Greek Law 3663/2008
[68] Same provision under Art 9 FD 2002/465/JHA
[69] Art 13(10a)
[70] Same provision under Art 10 FD 2002/465/JHA
[71] It could be agreed otherwise between the MSs when setting up the JIT pursuant to art. 11.
[72] Same provision under Art 7 FD 2002/465/JHA

case"[73]. In cases where the assistance of a third party, apart from those consisting the JIT, is necessary, the Art 13(8)[74] provides that relevant instruments should be applied.

During the last years, the establishment of JITs has become more common[75] and there has been a remarkable effort to make this tool more familiar to competent authorities and to clarify the relevant legal regime. A Spanish proposal, known as the project "fiches espagnoles," that was submitted in the Ninth Annual Meeting of National Experts on Joint Investigation Teams, contributed highly to that cause, urging for the concentration of the national legislation of all Member States regarding the establishment of JITs. Furthermore, the facilitation of the establishment of JITs was promoted by the publication of the Model Agreement of 2017[76] and the JIT Practical Guide of 2017[77] where several aspects and problematic areas of everyday JIT operation were addressed in an efficient way.

iv. The European Investigation Order Directive

In fact, the establishment of the JIT between Greek and Italian competent authorities,[78]facilitated simultaneous investigations in both countries and real time exchange of evidence and information obtained. During the operation of the JIT, it was discovered that the material was further distributed to purchasers in Germany and in France. Therefore, in order to investigate the involvement of those persons as well as the full exposure of the Groups' B and C criminal activities, the Greek and Italian JIT members decided to request from German and French authorities information and evidence that would be later assessed by the JIT. Fortunately, after May 2017 a new tool, which redefined the field of international cooperation among the EU Member States, the European Investigative Order, was already available. .

In an effort to maximise the efficiency of mutual assistance and enhance the procedure of harmonisation of national criminal law provisions, the European Council attempted a shift towards the adoption of the principle of mutual recognition which, particularly after the Tampere European Council, is perceived to be the cornerstone of judicial cooperation[79]. For that cause and

[73] Rijken, C., (2006), Joint Investigation Teams: principles, practice, and problems Lessons learnt from the first efforts to establish a JIT, Utrecht Law Review, volume 2, Issue 2
[74] Same provision under Art 8 FD 2002/465/JHA
[75] 69 JITs were established in 2016 out of 148 totally operating (Eurojust Annual Report 2016, p.20)
[76] 2017/C18/01, OJ C18
[77] Council of the European Union 6128/1/17/REV 1, of 14 February 2017
[78] Pursuant to Art 13 Greek Law 3663/2008 by which FD 2002/465/JHA was transposed
[79] European Council of 15-16 October 1999, Conclusions of the Presidency - SN 200/1/99 REV 1.

considering the fragmented and inapplicable existing framework[80,81], seven Member States (Belgium, Bulgaria, Estonia, Spain, Austria, Slovenia, Sweden) took an initiative that lead to the issuance of the 2014/14 Directive[82] on European Investigative Order (EIO).

According to Art 1 of the Directive, the EIO constitutes *a judicial decision* issued or validated by a judicial authority of a MS to have one or several measures carried out in another MS (the executing state) to obtain evidence. It is designed to have a horizontal scope[83] and thus it covers every investigative measure, except from the setting up of a JIT and the gathering of evidence within such team. The EIO can be issued by a MS that participates in a JIT for the purposes of requesting assistance from a third MS or from a third State, other than those which have set up the JIT, according to Art 13(8) of EU MLA Convention 2000[84].

Furthermore, as from 22 May 2017, the EIO Directive have replaced the corresponding provisions of Conventions[85] that governed international cooperation in criminal matters and gathering of evidence which were applicable among the Member States bound by the Directive[86]. EIO Directive also introduced[87] time limits for recognition or execution, which are no later than 30 days to deliver the decision on the recognition and 90 days after that to execute the measure[88].

[80]Council Framework Decision 2003/577JHA of 22 July 2003 for issuing a "freezing order" while the transfer of the evidence would follow regular MLA provisions. and Council Framework Decision 2008/978/JHA of 18 December 2008 "European Evidence Warrant"

[81]Council Framework Decision 2008/978/JHA of 18 December 2008 "European Evidence Warrant" applying solely on pre-existing evidence

[82]Directive 2014/14/EU of 3 April 2014, OJ L130,

[83]2014/14 paragraph 8

[84]This conclusion is expressly supported by the Greek Law 4489/2017, which states that "exceptionally, the MS in which the JIT operates can issue an EIO when the JIT needs assistance from another MS apart from those constituting the team".

[85]Referred to Art 34 of 2014/21/EU Directive

[86]Council Framework Decision 2008/978/JHA was expressly repealed later under the provisions of Directive 2016/95

[87] Art 12

[88] Under Art 14 it is also provisioned that MSs shall ensure legal remedies equivalent to those available in a similar domestic case. The substantive reasons for issuing the EIO may be challenged only in an action brought in the issuing State without prejudice to the guarantees of fundamental rights in the executing State. This article has considered lacking clarity and has already been the ground for a reference for a preliminary ruling (with four questions) from a Bulgarian Court (Spetsializiran nakazatelen sad) on 31 May 2017 in a case against Ivan Gavanozov. The first two questions considered the case that the national law does not provide any legal remedies in similar domestic cases and whether Art 14(2) of the directive could stand as autonomous legal base that would grant "in an immediate and direct manner" to the concerned party the right to challenge a court decision issuing an EIO. The other two questions referred to the meaning of the "concerned party" and more specifically whether the person against whom a criminal charge was brought is considered as such, if the measures for collection of evidence are directed to a third party, as well as if the person who occupies the property in which the search and seizure was carried out is also considered a concerned party. The Court has not reached a decision yet but these

The EIO Directive establishes the mutual recognition principle in judicial cooperation by providing that an EIO shall be recognised by the executing authority "without any further formality being required". In Art 9(1) it echoes the locus regitactum principle, stating that the investigative measure is being executed as if it had been ordered by an authority of the executing State. Nevertheless, Art 9(2) introduces the forum regitactum principle, since it provides that "the executing authority shall comply with the formalities and procedures expressly indicated by the issuing authority unless otherwise provided in the Directive and unless such formalities are not contrary to the fundamental principles of law of the executing state".

This provision can play a crucial role towards the minimisation of admissibility limitations of evidence gathered within international cooperation. However, its efficiency depends on the Directive's transposition on national legislation of Member States. For instance, Greek Law 4489/2017 provides that formalities indicated by the issuing State shall not be contrary to Greek Law *in general* and not just contrary to its fundamental principles. Consequently, if Greek laws are opposed to the indicated formalities, the latter cannot be followed. This provision, reinstitutes the locus regit principle.

In the studied case, Greece as the MS where the JIT was mainly operating, issued[89] an EIO towards the French authorities and another one towards the German authorities, requesting the identity of the persons that bought the material. Based upon all the evidence the Greek Public Prosecutor, collaborated with the Prosecutors of US, Italy, France and Germany and each of them decided that they would prosecute their own nationals, in view of the principal of procedural economy and so as to avoid a breach of the ne bis in idem principal.

D. AN OVERALL REVIEW OF THE ISSUES DISCUSSED

i. Admissibility of evidence shared by the parties within a JIT

Regarding procedural law, it is evident that the international judicial cooperation is a field where different jurisdictions and procedural rules are applied during the preliminary stage of criminal proceedings. However, the trial will usually be held only in one State whose procedural law may not be the one governing every procedural stage. It is therefore possible that issues

questions might be of special interest regarding the execution of an EIO order including investigative measures on data stored in cloud in cases of child pornography and whether the cloud storage companies could be considered as concerned parties able to challenge the execution of such orders.

[89] Pursuant to art. 21 Law No. 3663/2008 (art. 8 FD 2002/465/JHA)

regarding the admissibility of evidence shared by the parties may emerge. This problem was for example addressed in the ECHR case Stojkovic v France and Belgium[90]. The applicant was questioned by the Belgian police under a letter of request issued by a French judge, in which it was stated that the applicant is considered as "legally assisted witness" ("temoin assisté") under French Law and should have access to a lawyer. However, such option was not available in Belgian Law and the applicant was thus interviewed without legal assistance. The Court held that there had been a violation of Art 6(3) taken together with Art 6(1) of ECHR as concerned the application in respect of France, considering that the primarily responsibility for implementing and enforcing the rights guaranteed by the Convention was laid on the national authorities.

Within the scope of a JIT's operation the solution recommended in the conclusions of the 9th Annual Meeting of JIT Experts regarding the admissibility of evidence[91] is that "a general clause" should be included in the JIT agreement, providing that the evidence should be gathered according to the laws of the different MS of the JIT, where the evidence will eventually be used.

Apart from that, two other proposals could be made to address this problem. Firstly, the Member States could benefit from the experience gained through the "fiches espagnoles"[92] project and pursue a new equivalent: the "fiches d' admissibilité". This new project would aim at the collection of summaries of MS's national legislation, regarding the procedural requirements for each investigative measure, described in relevant international instruments of cooperation, e.g EU MLA Convention 2000. In this way the Member States, when considering the establishment of a JIT, will be able to foresee their operational and organisational needs concerning the required future investigating procedures.

Secondly, based on the observation that JITs are usually established amongst the same, more or less, groups of Member States depending on the nature and the characteristics of the regional cross-border criminality, several models of agreements could be construed in a way that will fulfill the admissibility of evidence requirements of the specific Member States. This would give these Member States an advantage regarding the establishment of future JITs[93].

[90] ECHR 2014/211 of 27.10.2011
[91] P 13
[92] Collection of the JIT set-up national rules
[93] E.g the French Ministry of Justice has signed bilateral agreements with Spain, Germany, Slovenia, Romania, the Netherlands, Belgium, Bulgaria and Cyprus, Conclusions of the 11th Meeting of JIT National Experts of 11-12 June 2015, Council of the European Union 11992/15 of 17 September 2015, p.5

ii. The need for harmonization in a digital era

There are, admittedly, two major factors that can lead to a successful prosecution that involves electronic evidence. The first refers to human and technical resources, and the second to a harmonised legal framework that establishes international cooperation, thus makingit easier for authorities to gather e-evidence in a safely and timely manner, regulating at the same time jurisdictional issues over the cyberspace.

As far as the human and technical resources factor are concerned, anyone can agree to the fact that the volatile and fragile nature of electronic evidence, which requires agility in its collection, maintenance of the chain of custody and protection of its integrity, since they can easily be altered, damaged or destroyed either by improper handling of law enforcement agencies or intentionally by the perpetrators, demand for the law enforcement agencies and judicial authorities to have the expertise, tools and both legislative and regulatory means at their disposal.

Furthermore, the need for an international harmonised and concrete legal framework has already been recognised originating from the borderless nature of this crime and the conflicting national laws that may affect it.

This is why, the beginning of this year is indicative of the efforts taking place at international level in order to shape data's cross-border future in a more consistent way. More specifically, European Commission is said to be preparing a Draft Directive in order to force companies to turn over customers' personal data when requested even if it is stored on servers outside the bloc.

On the other side of the Atlantic, where many of the Internet Service Providers reside, US Congress is advancing new legal and policy regimes that seek to overcome challenges that have - for the first time - come to the surface after Microsoft's ongoing dispute with the Government over Irish- held data. Actually, the question that the commonly known as Microsoft Ireland case posed was whether a US company must comply with a court order to turn over emails even if they are held abroad. In this case, US law enforcement agencies served Microsoft a search warrant for emails, as part of US drug trafficking investigation. Microsoft produced responsive metadata held in American data centers but challenged the order and refused to produce those in Ireland, on the basis of SCAS'[94] argued lack of extraterritorial application. The Federal Judge of

[94]Stored Communications Act that gives law enforcement with a warrant the authority to compel companies to hand over e-mails stored on U.S. soil that are relevant to an investigation

the Southern District of New York, ruled against Microsoft, but this decision was reversed by the Second Circuit, after the company's appeal. In response, the United States Department of Justice appealed to the Supreme Court. The case was heard on 27th February of present year and a ruling is expected by the end of the Court's term in June 2018.

When US Congress came across this case and realised the great importance of an up-to-date legislation that will help legal practitioners to keep pace with technology and at the same time reinforce and establish its national sovereignty, introduced on 6th of February 2018, a new set of internet regulations, namely as CLOUD ACT (Cloud is an acronym for Clarifying Lawful Overseas Use of Data).

This bill creates an explicit provision for U.S. law enforcement (from a local police department to federal agents in Immigration and Customs Enforcement) to access "the contents of a wire or electronic communication and any record or other information" about a person regardless of where they live or where that information is located on the globe. In other words, U.S. police could compel a service provider—like Google, Facebook, or Snapchat—to hand over a user's content and metadata, even if it is stored in a foreign country, without following that foreign country's privacy laws. Apart from that, the bill would allow the President to enter into "executive agreements" with foreign governments that would allow each government to acquire users' data stored in the other country, without following each other's privacy laws.

We should underline that European Courts and specifically the Supreme Court of Belgium at the relevant question of whether a Belgian public prosecutor validly sent a request to cooperate and provide personal user and communication data to a foreign provider of electronic communication service, which had no presence in Belgium, has ruled twice against Yahoo!

The case was brought before the Supreme Court and concerned a fraudulent purchase of, and subsequent failure to pay for, electronic equipment from a shop in Dendermonde, Belgium. Yahoo! Inc, a company registered in California, USA, received a request from the public prosecutor in Belgium to hand over the IP addresses associated with e-mail accounts of alleged criminals registered to Yahoo!'s e-mail service. However, it refused to comply because the request was sent directly by the Belgian prosecutor to its office in the USA, and not through the regular international procedure under MLAT.

The Supreme Court started by recalling that, as a general rule, a state can only take coercive measures to enforce its laws in its own territory. A State is considered as taking a

coercive measure in its own territory when there is a sufficient connecting factor between its territory and the measure in question. What qualifies as a sufficient territorial connecting factor is determined by, inter alia, the nature and scope of the coercive measure. The Supreme Court further concluded that Yahoo! is territorially present in Belgium, hereby voluntarily submitting itself to the jurisdiction of the Belgian authorities, since it takes an active part in economic life in Belgium, amongst others by use of the domain name http://www.yahoo.be, the use of the local language(s) on that website, pop-up advertisements based on the location of the users, and accessibility in Belgium of Belgium-focused customer services. The Court of Appeal had suggested that the accusations of extraterritoriality could only be accepted had there been a request for the handover of data or objects which are located in the USA, with which there is no Belgian territorial link whatsoever, and if the holder of these objects or data is not accessible in Belgium (either physically or virtually). To conclude, the need for an harmonised legal environment is illustrated by the above mentioned decisions that reached to diametrically opposed verdicts regarding the cornerstone of criminal investigation and imposed by the nature of crime of child pornography when is committed online due to irreversible trauma that one of the most vulnerable social group, minors, could suffer.

The aforementioned analysis, based on the study of the child pornography case scenario, intended to highlight the contemporary issues regarding substantive and procedural law, as well as international cooperation through the application of the existing legal instruments. The special nature of cybercrime, including online child pornography, demands for an effective international cooperation on multiple levels. The present study concluded that harmonisation of substantive legislation is of crucial importance in order to achieve this objective. However, in that process, human rights' concerns must not be neglected. Furthermore, in the field of procedural law, certain proposals were made aiming at the discovery of a minimum common ground amongst national laws. Under these proposals, the emergence of potential differences will increase the friction between the criminal procedural laws of the States, so as they ultimately soften their rough edges. Within the European Union, the above mentioned proposals will contribute to the fulfillment of the European goal of harmonisation, which stands as a prerequisite for the creation of an area of freedom, justice and security.