QUESTIONNAIRE

GREECE

Dr Leonidas KANELLOS

Attorney-at law,

lkanellos@telecomexperts.eu

1. Introduction

Please read carefully before answering the questionnaire

The RAYUELA project is aimed at protecting children in their online interactions. For this purpose, the project will develop a "game", which will present the children with realistic scenarios relating to the following cybercrimes/cyber-facilitated crimes:

- ***Online grooming*** (further: OG) is the crime where the perpetrator (usually an adult) uses electronic communication services, including social media, to contact a minor and build rapport with the aim of eventually meeting in person for the purposes of sexual activity. The perpetrator may employ various strategies (deception, romantic/emotional attachment, promise of material or other benefits, blackmail, coercion, etc.) to lower a child's inhibitions, heighten their curiosity about sexual experiences, or otherwise convince them to meet up.
- ***Cyber bullying*** (further: CB) is a broad term that includes all types of bullying behaviour online. This includes cyber stalking and cyber harassment, and any other type of behaviour online aimed at hurting the victim. Cyber bullying may also have a sexual component.
- ***Misinformation and deception*** (further: MD) is a behaviour that may or may not be punishable by law depending on the context. It involves all kinds of information sharing that is fake, or deceptive. For a criminal qualification to apply, typically the behaviour will need to be intentional and there will need to be material consequences to this intention.
- ***Human trafficking with a cyber component*** (further: HT) is the online facilitation of human trafficking by grooming and attracting potential victims for human trafficking.

The purpose of the game is to teach children how to remain safe online, while the obtained insights will be used to provide policy recommendations and educational tools.

The game does not focus solely on the threats of potentially falling victim to one of these four crimes. It also aims to raise awareness about the general threats of using IT, such as the Internet and connected devices, and minors' capacity to make responsible choices in this regard.

A particular point of interest is understanding whether minors are aware of when they, or someone else, is crossing the line in becoming offenders themselves, as this an important aspect of protecting children online. Due to the nature of online communication, inhibitions may be lowered, and certain actions may feel more innocent or less "real" than in real life. In addition, a perception may exist that what happens on the Internet has little or no impact beyond the digital world. This creates situations where minors engage in what they perceive to be relatively innocent behaviour ("everyone does this on the internet"), that may however have serious legal consequences.

One of the goals in RAYUELA is to ensure that minors realize when their behaviour may turn into actions that are punishable by law.

The present study and questionnaire are set up in the context of the RAYUELA project in order to provide an overview of the **legislative framework and relevant policies** in a number of countries, both in the EU and beyond, in relation to:

- How the main crimes of OG, CB, MD and HT are dealt with by the legal system i.e., which behaviours are punishable and under which conditions?
- How cybercrime and cyber-facilitated crime perpetrated by minors is dealt with in the legal system (both in general and specifically in relation to the crimes in focus)?
- What international instruments and cooperation mechanisms are available in dealing with cybercrime perpetrated by minors?

Importantly, we want to know both the legal rules and policies which are implemented in practice, and their effect on the **real enforcement situation**. If you have knowledge about the effects of current policies on crime rates by minors and on the crime rates for OG, CB, MD and HT, this would be of interest.

We are specifically interested in **case law** that illustrates the "why and how" of certain legal rules, principles and policies in practice. Case law will help us illustrate the similarities and differences between jurisdictions and is therefore *essential***.** Please ensure to have a good amount of case law processed in your answers.

In addition, we want input on **international legal instruments and international cooperation** relevant for cybercrime, and in particular for cybercrime perpetrated by minors. What happens when cybercrimes is perpetrated in a cross-border context? What are the legal rules in place for cooperation with authorities from other countries, and how does this work out in practice (issues, problems, etc.)?

Lastly, we are interested in some **statistical information on cybercrime** in your country and cybercrime by minors specifically.

The purpose of this questionnaire is to help you provide this information for your jurisdiction.

Introduction

The Greek legal framework concerning the protection of minors from online grooming, child prostitution, seduction of minors and sexual abuse combines several international, EU and national provisions. Greece has signed and ratified, inter alia, the International Convention on the Rights of the Child, the Geneva Convention on Refugees, the EU Charter of Fundamental Rights, as well as the Council of Europe Budapest Convention on Cybercrime (2004), the Warsaw Convention on Action against Trafficking in Human Beings (2005) and the Lanzarote Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (2007). Their provisions largely cover the protective framework around child exploitation and abuse,[1] as enhanced by various EU legislative measures, such as Directive 2011/93 on combating the sexual abuse and sexual exploitation of children and child pornography and Directive 2016/800 on procedural safeguards for children who are suspects or accused persons in criminal proceedings.

Moreover, the Greek Constitution includes special provisions on the respect for human dignity (art. 2), on the prohibition of torture, psychological violence, and insults to human dignity (art. 7), as well as on the protection of childhood (art. 21). National ministries (Justice, Education) together with administrative, judicial and police authorities (such as the Cybercrime Division of the Hellenic Police)[2] and a few NGOs, Greek and international (The Child's smile, ARSIS, Greek Cyber Crime Centre, Safer internet for Kids, INHOPE, ECPAT etc.) are also active in the country trying to raise awareness, prevent and combat crimes committed against children.

The Greek criminal justice system is based on the Continental tradition. Therefore, the stages of the criminal justice process in Greece are prosecution, preliminary examination, trial, and implementation/execution of the penal decision. The Prosecutor supervises the whole process as well as the actions of the rest of the authorities (police, prisons, and the officers in the justice system). During these stages the prosecutor acts as an independent judicial authority in the name of the State to ensure both the Constitutional Rules and the proper operation of the application of the Law. Moreover, the Prosecutor conducts the penal prosecution and the preliminary investigation and is responsible for checking the imposition of the decisions of the court.

Question 1: Is online grooming punishable by law in your country?

Answer:

The term online grooming reflects the process of socialization during which an offender interacts with a child by getting to know and befriend him/her, to prepare him/her for sexual abuse. Except for the application of Greek civil law legislation protecting the right to the name and the personality, specific penal law provisions apply on online grooming[3].

In fact, Greek law 3727/2008 (article 3) refers to online grooming, which amended several articles) of the Criminal Code (337, 338, 339, 342, 344 of Law 4623/2019, as subsequently amended by Laws 4637/2019 and 4689/2020). Said article punishes with a minimum two years' imprisonment the adult

[1] https://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=4bcbf8aa2

[2] A campaign "CYBERKID" has been developed by the Police in order to inform parents, teachers and children about the internet safety, https://eucpn.org/sites/default/files/document/files/GP_EL_Cybercrime%20Division%20and%20Cyberkid%20Campaign.pdf

[3] Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review, 2017, International Centre for Missing & Exploited Children, https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf

who, through the Internet or other means of electronic communications, establishes contacts with a minor under the age of fifteen and indulges his/her sexual dignity with proposals or gestures or indecent request (art. 337 paragraph 3 of Criminal code). If a meeting follows this contact, a minimum imprisonment of three years is imposed. Whoever commits a sexual act with a person under the age of fifteen or misleads as a result of committing or suffering such an act shall be punished, if there is no case to be punished more severely with Articles 342 and 351A, as follows: a) if the victim has not completed twelve (12) years, with imprisonment of at least ten (10) years, b) if the victim has reached twelve (12) years, with imprisonment.

It is worth mentioning that in the Greek legal order the age of the offender does affect the legal characterisation of the act committed, which will be considered either as a petty offence or a misdemeanour. More precisely, in Greek penal law criminal offences are grouped into three major categories, petty offences, misdemeanours and felonies. According to article 18 of Penal Code, any act punishable with confinement in a penitentiary is a felony. Any act punishable with imprisonment or with pecuniary penalty or detention in a correctional institution is a misdemeanour. Any act punishable with jailing or a fine is a petty offence. Consequently, every offence, which may be punished with detention in a correctional institution, regardless of its duration, such as online grooming, is a misdemeanour.

Furthermore, Article 348A of the Greek Penal Code incriminates the dissemination of child pornography and Child Sexual Abuse Material (CSAM),[4] as well as the access to relevant illicit and harmful content (Supreme Court 709/2015, 291/2015, 735/2014, 63/2013). Greece has also implemented Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography. In this regard, the implementing Law 4267/2014 has amended several articles of the Criminal code (5, 8, 67, 113, 187B, 339, 348A etc). On several occasions, the Greek courts have incriminated various online grooming practices, usually activated via fake social media profiles used by pedophiles to attract minors on purposes of their seduction and sexual exploitation (Supreme Court 317/2021, 715/2020, 686/2020, 279/2020, 3/2018, 931/2012, Thessaloniki Criminal court 157/2020, Athens Criminal Court 3277/2018).

Question 2: Is cyberbullying punishable by law in your country? Please take into account a broad understanding of cyberbullying (cyber/online stalking, harassment, sexual harassment)?

Answer:

The term "cyberbullying" is not to be found as such in the Greek penal law. Article 312 of the Penal Code, as amended by Law 4322/2015 (art. 8) incriminates bullying, as the act of an adult causing physical injury or damage and/or mental injury (such as denigration, constant criticism, threats, "happyslapping", "textwars" or rejection) to minors or "weak" persons (ill, elderly, drug addict etc), incapable of defending themselves (such as employees, husbands etc.) through continuous cruel behaviour (Piraeus First instance Court 1780/2021 on interim measures by the parents to protect their child's personality, Patras Public Prosecutor order 315/2020 on work mobbing etc)5. If the bullying act is committed between minors, it remains without punishment, unless there is an age difference between

[4] The term "Child Sexual Abuse Material" defines any image or depiction that portrays a child engaging in sexual activity, appearing as being engaged or forced to sexual activity, or a child the genitalia of which are depicted on an item for primarily sexual purpose. The term "Child Sexual Abuse Material" is being used more frequently as more appropriate than the term "Child Pornography"

[5] A famous bullying case in 2015 against an Ioannina Agricultural School student, Manolis Giakoumakis, caused his death via suicide http://www.newsbomb.gr/ellada/news/story/563927/thyma-agrioy-bullying-ovaggelis-giakoymakis-symfona-me-to-porisma-tis-ede#ixzz3h1qBwoOT, http://www.fthis.gr/article/394120/baggelis-giakoymakis-to-bullying-i-exafanisi-i-zoi-kai-toadoxo-telos-toy

them which is bigger than 3 years, in which case only curative measures are imposed against the perpetrator.

Imprisonment sentences range between at least one year up to ten years, depending on the gravity of the act and the injury caused to the victim. In case bullying of children is committed through the internet, via any offensive act, such as cyber/online stalking (sending emails, text messages, social media posts etc.) or any type of harassment, there might be a case of cyberbullying[6].

As components of the same crime, traditional bullying and cyberbullying present some common characteristics (defamation, verbal violence or threat for physical violence, stress of the victim, character of the bully, purpose of the harassment) but also notable differences (degree of exposure, variety of ways to harm the victim). The effects of cyberbullying may include anxiety, depression, fear, low self-esteem, self-isolation, aggressiveness, cyber-bullying back and suicidal ideation.

Several studies and empirical research[7] conducted on cyberbullying in Greece[8] conclude that it appears to be as less common than the act of "traditional" bullying[9]. According to a November 2021 survey by the NGO "Actionaid", 85% of female respondents said they have experienced sexual harassment at work. Another poll by the organisation "ProRata" found more than 90% of those who said they had been harassed or abused did not believe they could get any legal redress[10]. In the first half of 2021 alone, the NGO "The Smile of the Child" received 30,000 calls for incidents of child abuse, including sexual crimes, bullying and psychological violence. According to statistical data from the Hellenic Police, a complaint of child rape occurred on average almost every week in Greece in 2020, while one out of 30 children is reported to have had some experience of rape or attempted rape. More specifically, in 2020, well in excess of 300 cases of sexual abuse and pornography involving children were reported[11] to bodies involved with safe ICT use and hotlines for reporting illegal online content in Greece (Safeline, Greek Safer Internet etc).

Question 3: When would misinformation and deception online constitute a criminal offence in your country? In other words, what potential qualifications could apply?

Answer:

A recent amendment (replacement of art. 191 of the Criminal code by law 4855/2021), makes a criminal offense the act of spreading "fake news" capable of causing concern or fear to the public or undermining public confidence in the national economy, the country's defense capacity or public health. Notably, this seems to require a showing of specific actions (e.g., cancellations), rather than influencing beliefs or opinions. Said article is restricted to specific misinformation online offenses and does not specifically

[6]G. Floros et alii, Adolescent online cyberbullying in Greece: the impact of parental online security practices, bonding, and online impulsiveness, https://pubmed.ncbi.nlm.nih.gov/23586890/

[7] https://cyberbullying.org/research/map/greece

[8] Nafsika Antoniadou & Constantinos M. Kokkinos (2015) A review of research on cyber-bullying in Greece, International Journal of Adolescence and Youth, 20:2, 185-201, https://doi.org/10.1080/02673843.2013.778207

[9] Cyberbullying and Traditional Bullying in Greece: An Empirical Study, October 2020, ETLTC2020-Virtual ACM Chapter Workshop on Professional and Social Media Communication, https://www.researchgate.net/publication/344651261_Cyberbullying_and_Traditional_Bullying_in_Greece_An_Empirical_Study

[10] Greece to toughen laws on sex crimes after wave of abuse allegations, https://www.reuters.com/article/us-greece-abuse-idUSKBN2AP1HX

[11] Child abuse 'constantly multiplying' in Greece, https://www.ekathimerini.com/news/1169941/child-abuse-constantly-multiplying-in-greece/

refer to minors. The law provides that offenders "shall be punished by imprisonment of at least three months and a fine. If the act was repeatedly committed through the press or online, the perpetrator shall be punished by imprisonment of at least six months and a fine". This provision has been criticized by journalistic unions as very broad thus potentially violating freedom of speech in the country.

Question 4: What constitutes human trafficking and how is human trafficking facilitated by electronic means punished in your country? Are online grooming activities to find victims (e.g. lover boys) before the actual human trafficking punishable in itself? In addition, are these activities punishable as a separate crime if human trafficking does take place afterward?

Answer:

Human trafficking, otherwise known as modern slavery, involves the use of force, fraud, or coercion to obtain some type of labor or commercial sex act against the will of the person trafficked. Traffickers may use violence, manipulation, or false promises of well-paying jobs or romantic relationships to lure victims into being trafficked. Trafficking victims include men, women, and children of all ages, races, and nationalities.

Greece has signed and ratified the three fundamental international legal instruments against THB:

1. The UN Convention against Transnational Organized Crime and its Protocols – the "Palermo Protocol" by Law 3875/2010

2. The national transposition of the 2011/36/EU Directive on preventing and combating trafficking in human beings and protecting its victims took place via law 4198/2013. Such law established the Office of the National Rapporteur (MFA) and gave an official mandate of accountability to the informal Coordination Mechanism of competent Ministries, International Organizations and accredited NGOs.

3. The Council of Europe Convention on Action against Trafficking in Human Beings (Warsaw, 16.V.2005) was implemented via law 4216/2013.

From a national law perspective, two separate provisions of the Criminal Code, namely Articles 323A and 351 incriminate trafficking in human beings. Under Greek law, THB includes three components:

a) an action ("the recruitment, transportation, transfer, harboring or receipt of persons");

b) the use of certain means ("threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person") and

c) the purpose of exploitation ("at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labor or services, slavery or practices similar to slavery, servitude or the removal of organs"). In the case of children, it is irrelevant whether the electronic means referred to above have been used.

By virtue of article 323A of the Penal Code, offenders shall be punished by a maximum penalty of 10 years' imprisonment and by a fine of 10.000 to 50.000 Euros, if the act: (a) is against a minor or a physically or mentally disabled person, (b) is carried out in a repetitive manner, (c) is committed by an official who during the performance of their duty or by abuse of power commits or participates in any

manner in the act, or (d) had as a result a particularly grave injury or exposed the life of the victim to great danger. The perpetrator shall be punishable according to the above penalties if, to achieve the same goal, he/she achieves the consent of a person by fraudulent means or deceives this person by exploiting his/her position of vulnerability by making promises, gifts, payments or giving other benefits. Any person who knowingly accepts the labor of a person who is under the conditions described above. The perpetrator shall be punished by life imprisonment if the offence resulted in the person's death.

In the same direction, Article 351 of the Hellenic Criminal Code provides that: "1. A person who, by the use of force, threat of force or other coercive means, or by imposition or abuse of power, or by abduction, recruits, transports or transfers within or outside the country's territory, retains, harbors, delivers with or without benefit a person to another person or receives a person from another person with the purpose of sexual exploitation either by himself or by another person, shall be punished by a maximum penalty of 10 years' imprisonment and a fine of 10.000 to 50.000 Euros. In the meaning of the previous paragraphs, sexual exploitation consists in committing sexual acts for profit or using the body, voice, or image of a person for the actual or virtual commission of such acts or for the supply of labor or services for sexual arousal[12].

Greece is predominantly a country of destination and transit of victims of trafficking in human beings, usually arriving from Eastern Europe, post-Soviet Union countries and/or third countries. Since 2015, it has been a host country for thousands of refugees and migrants, coming mainly from countries in the Middle East and Sub-Saharan Africa. Among the people who enter the country, half of them represent minor children and most are unaccompanied[13]. The migration of these children is a high-risk experience, not only during their migration travel, but also during their stay in a refugee camp, where they may face all forms of abuse and exploitation, including sexual abuse. To a certain degree, Greece is also a country of origin, since a significant number of identified victims, such as the Roma children, are of Greek citizenship (domestic trafficking)[14]. Although the existing legal framework regarding the protection of unaccompanied children from any kind of violence and abuse is complete, this phenomenon continues to exist in the country.

Much of Greece's efforts to address the problem has been implemented in the context of anti-trafficking. The Office of the National Rapporteur on Trafficking in Human Beings,[i] situated within the Hellenic Republic Ministry of Foreign Affairs has been particularly active in this respect, despite lack of adequate resources. A permanent consultation has been created as a framework for exchange between the Office of the National Rapporteur and representatives of 11 NGOs specialized in the field of combatting human trafficking by preparing a National Action Plan on Trafficking in Human Beings, in cooperation with public agencies, NGOs, civil society and grassroots organizations (2019-2023).

[12] Council of Europe, Committee of the Parties to the Council of Europe Convention on Action against Trafficking in Human Beings, Report submitted by the authorities of Greece on measures taken to comply with Committee of the Parties Recommendation CP(2018)3 on the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings

[13] According to Article 1 (f) of Presidential Decree 220/2007, an unaccompanied minor is defined as '*a third-country national or stateless person under the age of 18 who arrives in Greece without being accompanied by an adult responsible for his or her care, by law or custom, for as long as he has not been placed under the substantial care of such a person, or the minor who was left unaccompanied after entering Greece*'.

[14] Greek policy on trafficking in human beings, https://eucpn.org/document/greek-policy-on-trafficking-in-human-beings.

2. Questions regarding cybercrime or cyber-facilitated crime committed by minors

Question 5: How is crime committed by minors dealt with in your country, in general? Is there a specific juvenile justice system? If yes, please explain in detail how this works.

Answer:

In Greece, the institutional framework relevant to children involved in judicial proceedings is a mix of criminal and private law provisions. The institutions involved, as well as relevant laws and policies vary depending on whether the child is a suspect/defendant or a victim. For the most part, witnesses are treated in the same way as victims though victims' rights are more extensive if they acquire the status of civil claimant. In this case, they are equipped with greater enforcement powers. Prevention of relapse is one of the key principles of the Greek juvenile justice[15] system with respect to child suspects/offenders; in order to achieve this goal, the Greek legislator clearly promotes child suspects'/offenders' therapy and social integration through their education.

In fact, the criminal law provisions applicable to minors (persons having completed 12 years but having not reached 18 years of age) are integrated within chapter eight of the Penal Code (Articles 121-133 of law 4619/2019 as amended). Moreover, several provisions of various laws apply on the protection of minors (e.g. Law 4689/2020, articles 4-16 and 41-45, Law 4267/2014, Law 3189/2003 etc). The age is defined with reference to the time where a criminal act was committed, irrespectively from the date where the offensive result arose or when the victim obtained knowledge. In case no sufficient identification of the offender's age exists, the applicable "*in dubio pro reo*" principle imposes milder treatment of the perpetrator, who is considered as a minor (see also art. 3 of the United Nations Convention on the Rights of the Child and Greek implementing law 2101/1992).

The victim of a criminal act committed by a minor may also participate in the trial before the juvenile court as a litigant bringing his civil claims for any damage that has suffered (compensation and restoration of damage, financial redress for moral damage or mental anguish). Finally, the victim can also request reparation before the juvenile court even if the minor is considered criminally irresponsible. Moreover, the victim can initiate a civil action before the civil courts against the minor offender and/or against his parents, alleging negligent behavior and lack of proper supervision, under the limitations of articles 915-918 of the Civil Code. Namely, article 915 of the Greek Civil Code, as replaced by Law 2447/1996, stipulates that anyone who harmed another without being aware of his actions or while he was in a mental or intellectual disorder that decisively limited the operation of his judgment and will, is not responsible. In the same direction, article 916 of the Civil Code provides that "whoever has not reached the age of ten is not liable for the damage caused." Furthermore, the provision of Article 918 of the Civil Code stipulates that the person who caused the damage, if he is not liable, according to the provisions of Articles 915 to 917 of the Civil Code (due to lack of capacity to be charged) is sentenced by the Court, after assessing the situation of the parties, in reasonable compensation, if the damage cannot be covered otherwise.

Question 6: Are there specific rules or is there a specific policy that deals with cybercrime by minors as a special topic, acknowledging the special characteristics of crime by minors in the cyber environment, and the fact that minors may not knowingly or intentionally break rules (issues with criminal intent)? Even absent a written policy, are minors prosecuted for cybercrime in practice?

[15] Calliope D. Spinellis, Aglaia Tsitsoura, Juvenile Justice in Greece, https://www.oijj.org/sites/default/files/documentos/documental_2094_en.pdf

Answer:

In general, penal law provisions in Greece do not deal with cybercrime by minors as a special topic. If a crime of any kind is committed by minors, a tiered approach applies, depending on the age of the minor offender. The Greek Penal Code recognises different levels of criminal responsibility of minors (from 12 up to below 18 years old). Any crimes committed by children under 12 remain without any prosecution, since children are considered as being not 'criminally responsible'. Minors between 12-15 years may be subject (art. 127 of Penal Code) only to reformatory and therapeutic measures (under parental control as per art. 1518 of the Civil Code) when they commit criminal acts. Crimes committed by minors having completed 15 years of age may be subject to reformatory and therapeutic measures, unless criminal correction measures are deemed necessary, which entail the deprivation of their liberty in special penitentiary departments. However, imprisonment of minors (between 15-18 years old) appears to be an exceptional measure in Greece. Statistical data of the Anti-Crime Secretariat of the Ministry of Justice, reveal that on 1.1.2022 out of 11.030 adult prisoners in total in Greek prisons only 32 were minors, as compared to 2021 (11379 prisoners with 33 minors) and 2020 (10.891 prisoners with 30 minors)[16].

To protect minors in cyberspace, several awareness raising campaigns by the Greek State, the Greek Police and NGOs. Besides, the Code of Penal Procedure (Articles 1, 4, 7, 27, 130, 239, 305, 316, 489, and 549) together with special Acts, presidential decrees and ministerial decisions have set up special institutions, such as, Juvenile courts, probation services for juveniles, Societies for the Protection of Minors, Centres for the re-education of juvenile delinquents and their compulsory primary education, preceded or supplemented the provisions of the Codes. Juvenile justice competent authorities include juvenile judges serving in the juvenile courts, juvenile public prosecutors, investigating judges and probation officers, youth protection associations and the police. Child victims and witnesses on the other hand must go through the ordinary criminal justice system if the offender is an adult. This means that child victims are often dealt by officials who have not received specific child-focussed education and training.

Furthermore, Greece has implemented, via law 4689/2020, Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings (right to information, right to have the holder of parental responsibility informed, right to legal assistance, medical examination, limitation of deprivation of liberty etc). There is no special mention for crimes committed by minors in the cyber-environment, such as hacking (punishable under articles 370 A, B, C, D of Penal Code), violation of online privacy (incriminated by art. 38 of GDPR implementing Law 4624/2019), copyright infringements (punished by article 66 of Copyright Act, law 2121/1993 etc).

Question 7: Can minors be punished for online grooming in your country? I.e., the situation of a minor capable of providing sexual consent (e.g. 17 year-old) grooming a minor who has not reached the age of sexual consent (e.g. 13 years old) to meet up with the intent to perform sexual activities? Please focus not only on the specific crime of online grooming (which, if present as a separate crime in your jurisdiction, often requires an adult perpetrator), but also on other crimes that would punish the activities that constitute online grooming (i.e. the use of different strategies to force a meeting with the minor victim with the intent to perform sexual activities). If criminal sanctions could apply, are minors prosecuted in practice?

[16] Ministry of Justice, Anti-Crime Secretariat
http://www.mopocp.gov.gr/index.php?option=ozo_content&perform=view&id=7055&Itemid=696&lang=GR

Answer:

Greece recognizes the concept of the age of criminal responsibility for young persons in conformity with the terms of article 40 (3) (a) of the Convention on the Rights of the Child (CRC)[17]. Whether minors may be punished for online grooming in Greece depends on various factors, such as the age of consent and the circumstances of the offense. The age of consent is the minimum age at which an individual is legally considered old enough to consent to participation in sexual activity. As per Greek law (Article 339 of Penal code), the age of consent in Greece is 15 years old. Individuals aged 14 or younger in Greece are not legally able to consent to sexual activity, and such activity may result in prosecution for statutory rape (as per article 336 para 1 of Penal Code) or the equivalent local law. However, there is also a close-in-age exemption of 3 years in the country. Should a minor having completed 15 years of age rapes another minor, he will be prosecuted before the Juvenile Courts, under the applicable penal law provisions (Thessaloniki Misdemeanor Council 253/2020, Supreme court 1680/2008, 58/2010, 1156/2010).

Question 8: Can minors be punished for purely online behaviour with a sexual intent when other minors are the victim? E.g. the situation where a minor perpetrator obtains sexually explicit material from the minor victim in order to sell this or to force the victim to do something. If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

As per the Penal code (Article 339 paragraph 2), sexual intercourse between minors under the age of fifteen (15) years is not punishable, unless the age difference between them is greater than three (3) years, in which case only remedial or therapeutic measures can be imposed. Purely online behavior with a sexual intent when other minors are the victim falls under the above rule. Commonly known as "Romeo and Juliet law" in USA, this provision is designed to prevent the prosecution of underage couples who engage in consensual sex when both participants are significantly close in age to each other and one or both are below the age of consent. Depending on the situation, such exemption may completely exempt qualifying close-in-age couples from the age of consent law or merely provide a legal defense that can be used in the event of prosecution.

Question 9: Can minors be punished for cyberbullying behaviour, without there being a physical component to the crime? This includes behaviours such as cyberstalking and cyberharassment. If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

Cyber-bullying is the situation in which a child, preteen or teen is continuously threatened, harassed, humiliated, embarrassed, or otherwise targeted by another minor using the Internet, interactive and digital technologies, or mobile phones (handy-mobbing, Internet-mobbing). Cyber bullying, cyber harassment or online bullying is the evolution of traditional bullying, which takes place over electronic means and therefore may constitute an attempt of a crime. Such act is punishable, depending on their age, via remedial and curator measures, under the aforementioned article 312 of the Penal Code, as amended by Law 4322/2015 (art. 8) which incriminates bullying.

Cyberbullying can take many forms, including: a) posting a mean or unflattering picture or video of a classmate b) posting rumors (or starting rumors) on a social media platform c) threatening people via

[17] https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

text messages c) outing someone for their sexual orientation or gender identity d) sending messages telling someone to kill themselves e) pretending to be someone else online in order to friend, and then expose someone.

Several studies have tried to explore the extent of cyber bulling in Greece[18]. Although there is a lack of nationwide data, the main research findings, although fragmented, could be summarized as follows: a) Cyber bullying seems to have a small extent in Greece, when compared to more common traditional bullying although there is an overlap between them b) Girls are likely to be more vulnerable to cyber bullying and are more victimised than boys c) there is a statistical dependence between cyber bullying and traditional bullying victims d) there is a correlation between cyber bullying victims and family relations e) cyber-bullying may be more prevalent during high school and decline in University years, though more research is needed to this direction.

Question 10: Can minors be punished for wilful misinformation or deception online (sharing false news, false information, pretending to be someone else, pretending to be an expert, etc.)? Which crimes/qualifications could possibly apply? If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

Under the Council of Europe Budapest Cybercrime Convention, ratified by Greece by law 4411/2016[19], fraud and forgery are considered part of the computer-related offences (i.e., computer-related forgery and computer-related fraud). Article 7 of the Council of Europe Cybercrime Convention defines *computer-related forgery* as "intentional… and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible." Computer-related forgery involves impersonation of legitimate individuals, authorities, agencies, and other entities online for fraudulent purposes.

However, the Budapest Convention has specific technical limitations[20] and does not adequately address several issues, such as the stealing of digital identities, cyberbullying or cyberterrorism[21]. In practice, cybercriminals can impersonate people from legitimate organizations and agencies so as to trick them into revealing personal information and providing the offenders with money, goods and/or services. Should those actions be engaged by minors having completed 15 years of age, they would most likely be sanctioned by juvenile courts with educational and curative measures, depending on the age of the offender, unless criminal correction measures are considered necessary, which entail the deprivation of their liberty.

Furthermore, there are no dispositions in Greek criminal law which favor the responsibility of parents for the delinquent behavior of their children based on the notion of objective responsibility. Parents of

[18] Maria Papatsimouli and alii, Cyberbullying and Traditional Bullying in Greece: An Empirical Study (2021), SHS Web of Conferences 102, 04012 (2021), https://www.shs-conferences.org/articles/shsconf/pdf/2021/13/shsconf_etltc2021_04012.pdf

[19] https://www.e-nomothesia.gr/nomikes-plirofories/n44112016-kyrosi-tis-symvasis-gia-to-egklima-ston-yvernochoro.html

[20] Clough, Jonathan, A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation (2014). (2014) 40(3) Monash University Law Review 698-736, Monash University Faculty of Law Legal Studies Research Paper No. 2015/06, Available at SSRN: https://ssrn.com/abstract=2615789.

[21] Dominioni S. Multilateral tracks tackling cybercrime, overview, 18 July 2018, https://www.ispionline.it/en/pubblicazione/multilateral-tracks-tackling-cybercrime-overview-20962

a minor offender cannot incur any criminal liability with respect to offences committed by their child, unless they act with intent to promote or allow the delinquent conduct, or with negligence. Article 360 of the Penal Code (law 4619/2019) renders liable to imprisonment for up to one year, unless any aggravating circumstances exist, any person who, having the supervision of a minor, neglects his or her duty and fails to prevent the minor from committing a criminal act or engaging in prostitution, provided that the case does not involve harsher punishment under another provision. Should this act be committed by the parents or by a custodian, imprisonment penalty may reach two years.

Question 11: Can minors be punished for online actions facilitating human trafficking? Typically this includes the selection and grooming of victims (e.g. lover boy phenomenon). If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

If teenagers act as lover boys (or romeo pimps), using social media or chat rooms to attract young girls or boys to fall in love with them, so as to push them towards human traffickers with the purpose of exploiting them through the sex industry, they may be considered as accomplices to a crime. Should they engaging in online actions (e.g. use of social media) facilitating human trafficking, punishable under articles 323A and 351 of Criminal Code, minors may be punished, but mostly via educational and curative measures.

Question 12: Can minors be punished for acts of online piracy in your jurisdiction, i.e. the illegal use and/or distribution of content protected by intellectual property rights? Please focus on the elements of criminal nature. If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

Any act of criminality engaged by minors has a special treatment, as mentioned on several occasions above. When the perpetrator is an adult, the law provides for imprisonment of at least one year and pecuniary fines ranging from 2.900 to 15.000 euro, by virtue of article 66 of the Hellenic Copyright Act (law 2121/1993). Greek civil law (articles 915-918) also provides for means of redress, as explained under question 5 above. Under articles 134-136 of the Civil Law code, minors do not bear any civil liability for damages caused to others, but they only may conclude some acts beneficial for them or sign labour agreements, under their parents' consent.

Question 13: Can minors be punished for acts of hacking (i.e. unauthorized access to a computer system)? In particular, would this also apply to various scenarios exploiting vulnerabilities in IoT and connected devices? If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

Criminal treatment of minors is similar under Greek law and does not involve any differentiation per type of crime. As already explained, Article 370D of Greek Criminal Code aims to punish and suppress any unlawful interference in computer systems and its peripheral memories, any unlawful use or copying of computer programs and any unlawful access to data transmitted through telecommunications systems. It is established as a crime of endangerment and several court precedents exist in Greece (Supreme Court 1087/2019,367/2017, 1414/2017). It is therefore not necessary to harm the owner's right, if this behavior has created a danger that threatens it. The introduction of the provisions of article 370D extended the scope of protection for data in motion, as this does not fall under the provision of article 370A, B and C of Greek Criminal Code, whose criminal protection extends to telephone and oral conversations. The protected right is the power of the legal owner of the data to exclude others from accessing them (right of sovereignty).

In other words, it is a right over the intellectual content of the data, and it is independent of any ownership in relation to the material or digital carrier. Moreover, this right is not necessarily linked to any economic benefit from the data. The legal owner, who is the only one who can allow third parties to have access to the programs, systems, or data, is not necessarily the same person with the one to whom the information relates. Minors may exceptionally be prosecuted for such offenses, if they are between 15-18 years old, via therapeutic and educational measures and, exceptionally, via deprivation of their liberty. The Greek police regularly publishes press releases on such cases although no official data on minors' cybercriminality exist [22].

Question 14: Can minors be punished for acts of using any instance of Cybercrime as a Service? If yes, under what qualification? If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

Cybercrime-as-a-Service (attacks-as-a-service/ malware-as-a-service/fraud-as-a-Service) is the provision of services to others to facilitate their commission of cybercrimes. Such felonies involve the use of computer systems and the internet to illegally access computer memories, copy confidential data (articles 370A, B, C. D) or commit fraud (art 386 of Criminal code). The criminal provisions on cybercrime cover any related act while minors have the adequate milder treatment, based in their age. The Cyber Crime Division of the Hellenic Police HQ is responsible, according to the Presidential Decree 178/2014, for Internet issues that involve minors. Its mission includes awareness raising activities (e.g. Cyberkid), lectures in schools, provision of advice via websites, as well as the prevention and prosecution of crimes or antisocial behaviours that are committed via the Internet against minors.

3. General questions regarding cross border cybercrime, international legal instruments applicable to fighting cybercrime and regarding international cooperation

Question 15: How does your country deal with the cross-border nature of many cybercrimes? When is jurisdiction established? Can judgements have extra-territorial effect?

Answer:

Although most cybercrimes, committed through the internet, are cross-border by nature, the territoriality principle is a fundamental principle of Greek and international law. As such, it effectively limits the Greek police powers to act within the Greek territory. Nationally, the mandate of the Hellenic Police, under the auspices of the Ministry of Citizen Protection, includes enforcing laws on the trafficking of children for sexual purposes and other forms of SEC. The Cyber Crime Division also cooperates internationally with EUROPOL and INTERPOL. Furthermore, they also receive complaints related to Greek jurisdiction from organizations such as the NCMEC (National Centre for Missing and Exploited Children) in the USA, and the NCEEC (National Centre for Missing and Exploitation Coordination Center) in Canada, that are responsible for the collection and distribution of complaints on the sexual abuse of children from technology companies and social media platforms, amongst others.[ii]

Notably, according to the established principle of jurisdiction to enforce, also known as the Lotus principle, established by the International Court of Justice (ICJ), states are prohibited to "exercise its power in any form in the territory of another state" unless there are specific grounds to do so deriving

[22] http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=107264=

from international custom or agreements. However, the legal boundaries of the principle of territoriality become especially blurred is when the Greek police needs, for investigation purposes, to access data that is located extraterritorially.

The consequence of the territoriality principle has been that a state who required intelligence or evidence stored abroad in the context of criminal investigations or prosecutions would have to use recognized international co-operation procedures, such as letters rogatory or Mutual Legal Assistance (MLA), the latter of which is based on bi-lateral or multi-lateral treaties. To this end, the Greek police officials closely cooperate with EUROPOL and INTERPOL to fight various types of cybercrime.[23] However, all measures used and employed by Law Enforcement Agencies' (LEAs') to access data extraterritorially must be in accordance with the legal limits as set in both Greek, EU (Police Directive 2016/680 as implemented by law 4624/2019) and international law. Notwithstanding efforts to negotiate a new cybercrime convention at the level of the United Nations, the Council of Europe Budapest Convention (2004) remains the main multilateral Convention for the fight against cybercrime aiming at setting up a fast and effective regime of international cooperation.

Question 16: What international legal instruments (bi-lateral, multi-lateral) apply in your country to the fight against (cross-border) cybercrime and how have they been implemented in national law (if implementation is necessary)?

Answer:

In the Greek legal system, ratified international conventions constitute an integral part of the legal order and prevail over any contrary provision of the law. Greece signed the United Nations Convention on the Rights of the Child (CRC) in 1990. The country has also ratified the Optional Protocol on the sale of children, child prostitution and child pornography (OPSC), thereby explicitly committing itself to combatting the sexual exploitation of children. Furthermore, Greece has also ratified the Council of Europe's Budapest Convention on Cybercrime and its Protocol on Xenophobia and Racism.[24] It has also signed and ratified (via law 3727/2008[25]) the Lanzarote Convention[26], officially titled as the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. The Convention requires parties to align their national laws to enable them to prosecute the offences referred to in the Convention, by ensuring jurisdiction based not only on the traditional principles of "territoriality" and the "nationality" of the perpetrator, and even in some cases the victim, but uniquely establishing jurisdiction based on the habitual residence of the perpetrator or the victim.

While subject to reservation of the parties, this additional ground for jurisdiction was seen as important to make it possible to make it possible to effectively step-up against sex tourism. Furthermore, the removal of dual criminality in prosecuting such serious offences abroad is an exceptional move in international criminal law instruments. As it was shown above in the context of the EU, this is no longer an issue due to the mutual recognition principle. However, in the non-EU context this is certainly a bold move. The Convention further provides for corporate liability, types and levels of sanctions, aggravating

[23] Council of Europe Cybercrime Convention Committee (T-CY), The mutual legal assistance provisions of the Budapest Convention on Cybercrime. Adopted by the T-CY at its 12th Plenary (2-3 December 2014) e.g. p 123. For further views on Mutual Legal Assistance and cooperation provisions in international and regional cybercrime instruments, see UNODC, Comprehensive Study on Cybercrime, Op. cit. 13. pp. 197-208

[24] https://www.coe.int/en/web/cybercrime/-/ratification-by-greece-to-the-budapest-convention-on-cybercrime-and-its-protocol-on-xenophobia-and-racism

[25] Available in Greek at http://www.dsanet.gr/Epikairothta/Nomothesia/n3727_08.htm

[26] https://www.coe.int/en/web/children/lanzarote-convention

circumstances, the taking into account of prior convictions and an array of judicial cooperation tools, also applicable for Greece.

Question 17: What forms of international cooperation exist in your country to the fight against cross-border cybercrime? Please describe different routes/options/procedures and the measures that can be requested (e.g. asking for investigative actions, exchange of information/evidence, etc.)?

Answer:

The Budapest convention is considered the most relevant instrument for fighting cybercrime to date. It allows for the harmonisation of laws, supports improvement of investigation techniques, and facilitate international cooperation. It is noteworthy that the Cybercrime Convention Committee of the Council of Europe adopted several recommendations to address, including through the negotiation of a Second Additional Protocol to the Convention on Cybercrime on enhanced international cooperation, the challenge that electronic evidence relating to cybercrime and other offences is increasingly held by service providers in foreign jurisdictions, while the powers of law enforcement remain limited by territorial boundaries[27]. Chapter II of the Protocol provides for measures to enhance cooperation in relation to existing mutual assistance treaties or arrangements, practices, or domestic law as well as for the disclosure of computer data in emergency situations and mutual legal assistance in emergency situations (by video conference, joint investigations etc).

The second additional Protocol will enter into force once five Parties have expressed their consent to be bound by the Protocol in accordance with Article 16, paragraphs 1 and 2. EU Member States should take the necessary steps to ensure swift entry into force of the Protocol, which is important in view of a number of factors (law enforcement and judicial authorities will obtain electronic evidence necessary for criminal investigations by respecting fundamental rights, including criminal procedural rights, the right to privacy and the right to the protection of personal data, in view of legal certainty, transparency, accountability and respect of fundamental rights and procedural guarantees of the suspects in criminal investigations (as per the "Police directive 2016/680").

Moreover, the Protocol will resolve and prevent conflicts of law, affecting both authorities and private sector service providers and other entities, by providing compatible rules at international level for cross-border access to electronic evidence. Finally, the Protocol will demonstrate the continued importance of the Convention as the main multilateral framework for the fight against cybercrime. This will be of key importance in the process following the United Nations General Assembly (UNGA) Resolution 74/247 of December 2019 on 'Countering the use of information and communications technologies for criminal purposes' that established an open-ended ad hoc intergovernmental committee of experts to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.

[27] Proposal for a COUNCIL DECISION, authorising Member States to sign, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, Brussels, 25.11.2021, COM (2021) 718 final, 2021/0382(NLE), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0718&from=EN

Question 18: Do the rules (national, international) and policies mentioned in your answers in this section have any particular effect or impact on cybercrime committed by minors?

Answer:

There are no sufficient data available to substantiate any response that question. Some reports[28] suggest that migrants often act as intermediaries between children and perpetrators, facilitating their transaction. Mobile phones allow for plans to be made efficiently and undetected and dating apps have made the process easier for children to engage in their own exploitation through prostitution. Perpetrators are often older men or sex tourists who visit Athens with the intent of meeting young boys, having already connected with them through the Internet. According with the 2021 US State Department's Trafficking in Persons report (TIP), Greece is a Tier 2 country, which means the country does not fully meet the minimum standards for the elimination of trafficking, Nevertheless, the Greek government, despite heavy pressure by illegal migration and trafficking emanating from Turkey, is making significant efforts to do so via coordination efforts of all co-competent bodies (Ministries, judiciary, police)[29].

4. Other

Question 19: Do you have any information on the rates/statistics of cybercrime in your country and their recent evolution? Of particular interest would be statistics related specifically to the crimes covered in this questionnaire and statistics on cybercrime by minors (ideally also specifically for the crimes covered above)? If there were any (relatively) recent legislative or policy changes, please try to find statistical information on how this has impacted the incidence of cybercrime in practice, and in particular cybercrime by minors.

Answer:

Official statistics from the Cybercrime Division of the Hellenic Police[30] regarding cybercrime show that the total number of new criminal cases handled during the year 2020 rose to 5,148. More specifically, the annual increase from 2019 to 2020 reached 14%. In 2020, the Cyber Crime Division of Hellenic Police handled about 300 cases of Online Child Sexual Abuse. During the Covid-19 lockdown, children turned into an online virtual life. They were mostly occupied with video calls with family and friends, social media, online gaming, remote education etc. According to Europol, sex offenders have found in this development a tempting opportunity to access a broader group of potential victims. there is also noticed an increase of distribution of child sexual exploitation material (CSAM) online, since offenders were unable to travel for sexual purposes. Moreover, there has been an increase in detection and reporting of CSAM on the surface web, which indicates "the level of re-victimisation of children through the distribution of images and videos depicting them".

However, a large amount reaching up to 40% of the total crimes, is related to online fraud, which increased by 13.66% from 2019 to 2020. Most of the cases were related to illegal money transfers

[28] Report submitted by the authorities of Greece on measures taken to comply with Committee of the Parties Recommendation CP(2018)3 on the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings First evaluation round, https://rm.coe.int/cp-2020-02-greece/16809eb4db, Supplementary report on "Sexual Exploitation of Children in Greece", submitted by ARSIS and ECPAT International, Bangkok, Thailand on 1 November 2019, to the Committee on the Rights of the Child, for the 85th Pre-session, (10 February – 14 February 2020).

[29] https://www.state.gov/reports/2021-trafficking-in-persons-report/greece/

[30] https://www.h2020-infinity.eu/sites/default/files/2022-02/pb_cybercrime_hellenicpolice_final.pdf

through banking systems and fraud related to products purchase. New modus operandi, in addition to phishing scams via e-mail, SMS or messaging also came up, such as scams committed through "sim swap", by replacement/change of mobile phone SIM cards and the scams with the promise of investment services.

Additionally, the latest data show that cyber-attacks in Europe are doubling. The number of serious cyberattacks against critical targets in Europe in 2020 has risen and Covid-19 pandemic has contributed to this. According to the EU Agency for Cyber Security (ENISA)[31], in 2020 there were 304 significant, malicious attacks against "critical targets", i.e. more than doubled from the 146 recorded in 2019. The agency also recorded a 47% increase in attacks on the critical sector of hospitals. This depicts the growing impact of cyber-attacks. Europol also reported that criminals have used the Covid-19 scam to launch pandemic-themed social engineering attacks to distribute various malware packages. Cybercriminals have also taken advantage of the growing number of businesses that offered the possibility of remote connection to their organizations' systems to assist remote working.

Question 20: Do you have any other comments to make that may be relevant to your jurisdiction?

Answer:

The existence of a strong legislative framework does not necessarily signal the elimination of the phenomenon of criminal behavior of any form engaged by minors and by adults against minors. The Greek Anti-Crime Policy Program must continue focusing on some specific goals concerning cybercrime and ICT-facilitated crimes (child pornography, cyber bullying, Internet fraud, victim solicitation via the Internet, intrusions, and cyber-attacks). The EU and the Greek state should allocate sufficient resources to implement the national action plan for combating trafficking. They should develop policies for victim-centered prosecutions and implement witness protection provisions already incorporated into law. It is also important to provide extensive training to judges, prosecutors, and law enforcement on trafficking investigations and prosecutions, particularly in rural areas and for non-specialized staff, standardize data collection and produce accurate data on anti-trafficking efforts. Finally, it is important to strengthen cooperation with foreign competent prosecuting Authorities via the legal communication channels (INTERPOL, EUROPOL, EUROJUST, etc.), to make possible the tracing down and the solution of cybercrimes with international nature.

Finally, children and teenagers should be considered as holders of rights who are entitled to protection from privacy violations and deserve an internet without manipulative and exploitative practices, as UNICEF has been repeatedly stating. Therefore, they should be empowered to recognize, understand, and abstain from the tactics and forms of digital abuse. Parents and caregivers, school and civil society should inform children about the new ways of sexual abuse, support them to develop critical thinking and protect their rights.

[31] ENISA Threat Landscape 2021, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021