QUESTIONNAIRE

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.

2. Questions relating to OG, CB, HT and MD with minors as victims

In this section, we will ask questions to understand how to main 4 crimes in focus in RAYUELA are regulated in your jurisdiction. In this section, the focus is on adult perpetrators with victims that are minors. We are interested in both the general rules, and whether the fact that the victim is a minor has an influence on the application of the law. We are also in particular interested in your thoughts on whether the scope of the law affects the number of cases that are brought before the courts, in other words, are the current provisions sufficient to prosecute the diverse forms of crime present in reality? And are cases effectively prosecuted in practice or are there obstacles (e.g., lack of resources)?

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

Answer:

Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.

Any person who, using an electronic communication service, proposes a personal meeting to a child below fifteen years of age with the intention to commit a criminal offence of sexual abuse or a criminal offence of production of child pornography against him and is not a child himself, shall be punished by a prison sentence of six months to three years.

The above provision was added to the Slovak Criminal Code with effect from 1 August 2013. This was due to the transposition of the Directive of the European Parliament and of the Council of 13 December 2011 on combating sexual abuse and sexual abuse. exploitation of children and against child pornography. Pursuant to Article 6(1) of the Directive, Member States have undertaken to prosecute an adult proposal made using information and communication technologies to meet a child who has not reached the age at which he or she is competent to give consent to sexual intercourse, with a view to sexually abusing or producing child pornography, and will, after that proposal, take concrete steps towards that meeting (incitement of children for sexual purposes). Article 3(2) and (3) of the Directive obliged Member States to prosecute the cause of a child who has not yet reached the age of sexual consent to witness sexual activities or sexual abuse for sexual purposes, even though that child may not participate directly in them.

Conditions for application:

- *object of the offence: the protection of the kids against online grooming activities,*

- *subject of the offence: this offence can only be committed by an offender who has reached the age of 18, this is an exception to general criminal liability from the age of 14,*

- *subjective aspect of the offence: intentional causation,*

- *objective aspect of the offence: a proposal for a child under the age of 15 to have a face-to-face meeting with a view to committing an offence of sexual abuse or the offence of producing child pornography.*

Punishments:

Because it is a criminal offence for which the law sets out a prison sentence with an upper penalty limit not exceeding five years, it is minor offence. If there is a minor offence, it is obligatory to examine the seriousness of minor offence, because it is not a minor offence if it is of lesser seriousness in view of the mode of its commission and consequences, the circumstances of its commission, the degree of causation, and the motivation of the offender. Under these conditions, the offender would not be punished.

Under other conditions, an offence involves the imposition of a suspended prison sentence, a sentence of house arrest or a compulsory work sentence. At the same time as the sentence imposed, the court may impose appropriate obligations and limitations on the offender, in this case especially a ban to contact the specified person in any form, including contact through an electronic communication service or other similar means. In the case of a recidivist or an offender whose stay at large would not serve the purpose of the sentence, the court imposes an unconditional custodial sentence on the offender at the statutory rate.

Please provide case law to illustrate the application of the rules in practice.

The defendant has been found guilty because at an undetected time on 28 March 2014, at approximately 00.25 am, through the internet portal www.pokec.sk, acting under the username "W.", made contact with the minor S. M., acting under the username "S.", who, when communicating with each other via the internet portals www.pokec.sk and www.facebook.com, repeatedly proposed and arranged a face-to-face meeting with him, first in the afternoon of 28.09.2014 and then in the afternoon of 29.09. 2014 at the department store, with the intention of personal acquaintance and sexual intercourse with the minor, asking him questions about his sexual orientation and sexual experience in the communication, confiding in him about his own sexual experiences, asking him for "bare" photos of him and requiring him never to disclose it under any circumstances, despite the knowledge that minor S. M. was not 15 years old at the time and he himself reached the age of majority at the time.

Please provide details on known issues of application.

Application problems are not known for this offence. However, the general problem may be the detection of this type of criminality, unless the minor is confided with the problem to some adult. In private conversations, it is almost impossible for police authorities to act and detect such crimes on the basis of their own activities, without initiative. Also, in court, it would be difficult to prove the act if there was no preserved or legally obtained written conversation.

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:

Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.

Who intentionally, through an electronic communications service, a computer system or a computer network, substantially impairs the quality of life of another by

a) it has long humiliated, intimidated, unlawfully acted on its behalf or harassed him for a long time, or

b) unlawfully publishes or makes available to a third party a video, sound or video-sound recording of his personal expression, obtained with his consent, capable of substantially endangering his seriousness or causing him any other serious harm to rights,

he faces up to three years in prison.

If the offender commits the offence in question against a victim who is a child, he or she is punished with a prison sentence of between one year and four years. A child means a person under the age of eighteen.

Conditions for application:

- object of the offence: the protection of the person against cyberbullying including all unwanted activities on the Internet interfering with the victim's personal rights, dignity, life as well as recordings of expressions of a personal nature

- subject of the offence: this offence can be committed by an offender who has reached the age of 14

- subjective aspect of the offence: intentional causation

- objective aspect of the offence: impairing the quality of life of another by humiliation, intimidation, unlawfully action on other behalf or harassed somebody for a long time or unlawfully publishing or making available to a third party a video, sound or video-sound recording of other personal expression with cause of serious harm to other rights.

This offence was added to the Slovak Criminal Code with effect from 1 July 2021. The impetus for the new legislation is the increasing transfer of work and private activities of the population to the digital world. It offers plenty of room for cyber harassment or "cyberbullying." The term expresses harassment, harm, intimidation, mockery or threats with the intention of gaining superiority over the victim. The main features of cyberbullying are: long-term or repetition, intrusiveness, demonstrable impact on the victim.

Punishments:

Because it is a criminal offence for which the law sets out a prison sentence with an upper penalty limit not exceeding five years, it is minor offence. If there is a minor offence, it is obligatory to examine the seriousness of minor offence, because it is not a minor offence if it is of lesser seriousness in view of the mode of its commission and consequences, the circumstances of its commission, the degree of causation, and the motivation of the offender. Under these conditions, the offender would not be punished.

Under other conditions, an offence involves the imposition of a suspended prison sentence, a sentence of house arrest or a compulsory work sentence. At the same time as the sentence imposed, the court may impose appropriate obligations and limitations on the offender, in this case especially a ban to contact the specified person in any form, including contact through an electronic communication service or other similar means. In the case of a recedivist or an offender whose stay at large would not serve the purpose of the sentence, the court imposes an unconditional custodial sentence on the offender at the statutory rate.

Please provide case law to illustrate the application of the rules in practice.

Due to the short period of time since the adoption of this offence, the decision-making activities of the courts and case law on this issue are not yet known.

Please provide details on known issues of application.

Application problems to this offence are not yet known. However, the adoption of this offence removed the application problems from the previous legislation, when cyberbullying could not be penalised due to the absence of legislation.

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

Answer:

Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.

The crime of spreading misinformation is not enshrined in the current Slovak criminal law. More recently, mainly due to the spread of false information concerning to Covid situation, this offence has been proposed in the legislative proposal, but has not met with the consent of the professionals. It would be difficult for law enforcement and courts to distinguish the line between freedom of expression and disinformation in this crime, as well as to assess the veracity of a particular information. In criminal proceedings, this would mean the need to recruit an expert to assess the veracity of the information. At present, it is not possible to punish the spread of disinformation in Slovakia.

On the other hand, it is possible in Slovakia to punish a person who deliberately causes a risk of serious concern to at least part of the population of a place by spreading an alarm message that is untrue or committing another similar act capable of causing such a danger, such a perpetrator will be punished with a custodial sentence of up to two years. This offence requires the effect of causing serious concern to at least part of the population, so spreading disinformation alone will not be enough.

Furthermore, a criminal offence could occur if the perpetrator, through his misinformation, intervenes in the victim's personal sphere. Anyone who reports a false statement about another who is capable of significantly endangering his seriousness with fellow citizens, harming him in employment, in business, disrupting his family relations or causing other serious harm to him shall be punishable by up to two years' imprisonment. That offence of defamation requires that false information causes more serious harm to the injured party in various important areas of his or her life.

It is also worth mentioning in particular the false dissemination of information concerning holocaust denial and approval, the crimes of political regimes and crimes against humanity, since the legislature has responded in criminal law to this problem, which also occurs in the online space. Whoever publicly denies, disputes, approves or tries to justify the holocaust, the crimes of a regime based on a fascist ideology, the crimes of a regime based on a communist ideology or crimes of a similar movement which through violence, threat of violence or threat of other grievous harm leads to the suppression of fundamental rights and freedoms of persons shall be liable to a term of imprisonment of six months to three years.

Please provide case law to illustrate the application of the rules in practice.

The defendant on 21.10.2018 at 13:08 h in an precisely undetected place using a computer network via the internet service www.azet.sk created a fake account in the name of X. Q., on which he published an album with photos of the naked body of X. Q. and the text that X.Q. provides various erotic services, while also indicating her phone number, which was called by various persons interested in the services on offer, at the same time, he posted a link to this account via the internet service www.facebook.com on the account "Confessions of V. employees", which is set up for employees of the company in which X.Q. was employed, thereby reporting on another false figure, which is capable of significantly endangering his seriousness with fellow citizens, damaging him at work, disrupting his family relations, causing him other serious harm and committing the act publicly.

Please provide details on known issues of application.

As mentioned above, an application problem may occur when assessing the veracity of a particular information as well as in the assessment of injury to the rights of the injured party. This must therefore be properly established in the context of the taking of evidence. It is easier for acts committed in the online space, as the text in the online space remains recorded in full form.

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:

Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.

Trafficking of people by electronic means is not specifically regulated in Slovakia before human trafficking take place.

Any person who, by using fraudulent practices, a trick, restriction of personal freedom, violence, threatened violence, threat of grievous bodily harm or other forms of coercion, by accepting or offering monetary payment or other benefits in order to get approval of a person on whom another person depends, or by misusing his position, or abusing of defencelessness or other vulnerable position, entices, transports, harbours, hands over or takes over another person, even upon his consent, for the purposes of his prostitution or another form of sexual exploitation, including pornography, forced labour and services including beggary, slavery or practices similar to slavery, servitude, forced marriage, misuse for committing criminal activities, removal of organs, tissues or cells or other forms of exploitation, shall be liable to a term of imprisonment of four to ten years.

The same sentence shall be imposed on any person who entices, transports, harbours, hands over or takes over a child, even with his consent, for the purposes of his prostitution or other form of sexual exploitation, including child pornography, forced labour or forced services including beggary, slavery or practices similar to slavery, servitude, forced marriage, misuse for committing criminal activities, illegal adoption, removal of organs, tissues or cells or other forms of exploitation.

However, since the Slovak Criminal Code does not specifically penalise online grooming activities for the search of the victims, these kind of activities could be punished as preparation for the crime of trafficking in human, which was mentioned above. Preparation for committing a crime means wilful organisation of a criminal act, procurement or adaptation of means or instruments for its commission, associating, grouping, instigating, contracting, abetting or aiding in such crime, or other deliberate actions designed to create conditions for its commission, where a crime has been neither attempted nor completed. Preparation for committing a felony shall carry the same punishment as the crime, for which it has been intended.

Please provide case law to illustrate the application of the rules in practice.

The defendants, from the undetermined time on 30.12.2019 to the undetected time of 04.01.2020 via the Messenger application, communicated with the injured I. U., which she was trying to lure to the meeting, giving the injured party the mistaken impression that they would meet as friends during that period, but the accused lured the injured person to the meeting for purpose that the injured person will be taken to the car during the meeting and transported to the apartment and there they will use it to provide sexual services for them for financial reward, which on 04.01.2020 they managed to do together, so that the accused at the exact undetected time of 04.01.2020 in the premises of the train station, forcibly removed her mobile phone, ID card and wallet and when the injured party asked for her belongings back, the accused told her that if she did not get in the car and went for coffee together, she would not return her phone, then the victim, believed to be going with the accused for coffee and returning her phone, got into a passenger car, and after she got in the car, the accused disassembled her mobile phone and threw him out the window, she hid her ID card in her pocket and told her she was going to be taken to the person who beat her up, for which the victim cried and begged them not to drive her there so they told her they were going to the accused's apartment, and as they arrived, the accused created a profile of her against her will and without her consent with nick "Barbiel 111" and under the threat of beating and bodily harm, she was held in this apartment and did not allow her to leave the apartment, the apartment locked and hid the keys, and so damaged between 04.01.2020 and 30.01.2020 for fear for her life and health performed sexual services in the village of Nová Dubnica in the parking lot next to the swimming

pool in the cars of customers, which she received for their provision to the accused, when during that period the victim provided sexual services to at least 30 customers, where she collected at least 20,-€ for one service, and in this way the perpetrators enriched themselves by at least 600,- €, while on 30.01.2020 she managed to escape from the apartment with the help of one of the customers.

Please provide details on known issues of application.

Because the problem of trafficking of people by electronic means committed by juveniles in Slovakia is unknown, application problems cannot be mentioned.

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

This section is aimed at understanding how cybercrime or cyber-facilitated crime committed by minors is dealt with in your jurisdiction. In particular, we are trying to assess to what extent the rules and policies in place create leeway for minors who may not always be aware of when their behaviour is crossing a line. We are also interested to know the real enforcement situation. In addition to the general rules on the juvenile justice system and the punishment of minors, the 4 crimes of focus of RAYUELA are addressed, as well as two particularly relevant crimes committed by minors online: online piracy and hacking.

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:

Please explain the applicable rules, the conditions for application (general age limit, limits for certain crimes), the range and types of punishment that may be imposed on minors, rules about mitigating/attenuating circumstances, and jurisdictional aspects in cross-border cases) and applicable policy.

In Slovakia, juvenile crimes are dealt with by the same authorities, which also deal with the criminal activities of adults. The Criminal Code distinguishes between several categories within adolescence:

- The person who has not reached the age of fourteen at the time of commission of the criminal offence may not be held criminally liable. Prosecutions against him or her are inadmissible and, even if prosecutions against such a person have already been initiated, it must be stopped without delay.

- A young offender shall mean a natural person who, at the time of commission of the criminal offence, is over fourteen and under eighteen years of age. A young offender under fifteen years of age who, at the time of commission of the criminal offence, has not reached such a mental and moral state so as to be able to recognise its unlawfulness, or to exercise self-restraint, shall not be held criminally liable for committing this criminal offence. For juveniles, the Criminal Code specifically regulates the provisions relating to the punishment of juveniles. For juveniles, criminal rates are halved compared to adults. Also, the Criminal Code emphasizes the prevention and re-education of a juvenile offender outside the execution of a custodial sentence. A juvenile offender should be placed in an institution for the execution of a custodial sentence only in the most extreme case, priority is given to sentences not connected with imprisonment.

A court may impose on the young offender only

a) community service work,

b) pecuniary penalty,

c) forfeiture of a thing,

d) prohibition to undertake certain activities,

e) expulsion,

f) imprisonment.

- A young adult shall mean a person who has reached eighteen and has not yet reached twenty-one years of age. Although a person of this age is punished in the same way as an adult offender, in certain cases this age is considered an attenuating circumstance.

Please provide case law to illustrate the application of the rules in practice.

The juvenile offender drove a car without driving licence, causing a traffic accident. After the accident, he was inspected by a police and underwent a breath test for the detection of alcohol in his breath, and the measured value was 0.93 mg/l of alcohol in the breath. Thus, in a condition excluding ability to drive, the juvenile carried out, under the influence of an addictive substance, an activity in which it could endanger the life or health of humans or cause significant damage to property, for which he was given a three-month prison sentence with a suspended sentence of twelve months.

Please provide details on known issues of application.

The Criminal Code gives sufficient thought to juveniles and gives juveniles a special part in the context of inference of criminal liability and the imposition of sentences. However, taking into account the legislation of the surrounding states, consideration should be given to the need to adopt a special law on juvenile criminal regulation or a special judiciary specialised in the punishment of juveniles.

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?

Answer:

Please explain the applicable rules or policies, if any, and their impact in practice.

There are no specific rules or a specific policy in Slovakia dealing with cybercrime of minors as a specific topic. Minors can be punished for the same crimes committed in cyberspace as adult offenders. The difference between the juvenile offender and the adult offender shall be reflected in the amount and type of the sentence.

Please provide details on known issues of application.

In view of the above, application problems on this issue are not known.

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?

Answer:

Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.

Any person who, using an electronic communication service, proposes a personal meeting to a child below fifteen years of age with the intention to commit a criminal offence of sexual abuse or a criminal offence of production of child pornography against him and is not a child himself, shall be punished by a prison sentence of six months to three years. – This crime cannot be committed by minors, only adult person.

Slovakia does not regulate other crimes in which a juvenile would be punished for online grooming, i.e. luring a minor to sexual encounters.

A 17-year-old offender would not be criminally liable if he proposed to a 13-year-old person for sexual activity if these activities had not actually taken place.

Please provide case law to illustrate the application of the rules in practice.

Please provide details on known issues of application.

Because it is not possible to hold a juvenile liable for this offence, neither application problems nor court decisions are known.

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:

Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.

If a minor who has reached the age of 14 receives sexually explicit content from a child (a person under the age of 18), he/she will commit the offence of manufacturing of child pornography.

Any person who exploits, elicits, offers or otherwise abuses a child for manufacturing child pornography or manufacturing child pornographic performance, or enables such abuse of a child, or otherwise participates in such manufacturing, shall be liable to a term of imprisonment of four to ten years.

The offender shall be liable to a term of imprisonment of seven to twelve years if he commits this offence

a) against a child under twelve years of age,

b) acting in a more serious manner, or

c) in public.

Child pornography shall mean pornographic material that visually depicts sexual intercourse, different act of sexual intercourse, or other conduct similar to sexual intercourse with a child, or naked parts of the child's body, and that is designed to gratify sexual desire of another.

A child pornographic performance is a live performance intended for the audience, including by informational and technical means, in which the child is engaged in actual or feigned sexual acts or in which the parts of the child's body are exposed to inciting the sexual gratification of another person.

Conditions for application:

- *object of the crime: protection of morality against the manufacturing of child pornography and protection of the moral growing-up of children,*

- *subject of the crime: this offence can only be committed by an offender who has reached the age of 14,*

- *subjective aspect of the crime: intentional causation,*

- *objective aspect of the crime: exploiting, eliciting, offering or otherwise abusing a child for manufacturing child pornography.*

Another offence that a juvenile offender may also commit in connection with child pornography is the dissemination of child pornography or possession of child pornography.

Any person who disseminates, transports, procures, makes accessible or otherwise puts into distribution child pornography shall be liable to a term of imprisonment of one to five years.

Any person who has in his possession child pornography shall be liable to a term of imprisonment of up to two years.

Punishments:

If these offences are committed by a juvenile, the sentence will also depend on the age difference between the offender and the victim. Situations where, for example, a 17-year-old offender receives sexually explicit photographs from his 16-year-old partner as when a 17-year-old offender with a 10-year-old victim commits this. In such cases, the sexual deviance of the offender would be expertly examined and a protective measure would be imposed within the sentence – sexological treatment.

In the case of a juvenile offender, those penalty rates will be halved. In accordance with the principle of the primacy of imposing a non-custodial sentence, a juvenile offender will first be given a suspended prison sentence.

Statistics:

In 2021, a total of 26 people were prosecuted for manufacturing of child pornography, 10 of them were juveniles. A total of 99 people were prosecuted for dissemination of child pornography, 41 of them were juveniles. A total of 55 people were prosecuted for possession of child pornography, 13 of them were juveniles.

In 2022, a total of 12 people were prosecuted for manufacturing of child pornography, 2 of them were juveniles. A total of 29 people were prosecuted for dissemination of child pornography, 49 of them were juveniles. A total of 17 people were prosecuted for possession of child pornography, 5 of them were juveniles.

Please provide case law to illustrate the application of the rules in practice.

From an undetected time to 22.06.2020, the accused kept in a phone, as well as in a laptop, a child pornography in the form of images of a minor, in the photographs the minor is in a challenging position kneeling completely naked, clearly showing her bust, then there are photographs where the shot is directly on the genitals, while the accused knew that the minor V. P. was not 18 years old. The accused was given a 32-month prison sentence with a suspended sentence. At the same time, the accused was ordered to undergo probationary psychotherapy and to participate in psychological counselling.

Please provide details on known issues of application.

Application problems could occur in the event of a low age difference between the juvenile offender and the victim. It is common for adolescents (15-18 years of age) to send sexual content to each other

as part of their adolescence or create it together. However, such a case cannot be punished in the same way as cases where the offender has sexual deviance. Since the crime of producing child pornography is a crime, it is not possible to apply the material side of the crime and the act because of its slightness does not punish, as could be the case with an offence.

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:

Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.

Offences such as cyberstalking or cyberharassment, crimes committed in the online space, can be punishable by the crime of dangerous electronic harassment. This offence may also be committed by a juvenile. The conditions for committing this offence were discussed in question 2.

Who intentionally, through an electronic communications service, a computer system or a computer network, substantially impairs the quality of life of another by

a) it has long humiliated, intimidated, unlawfully acted on its behalf or harassed him for a long time, or

b) unlawfully publishes or makes available to a third party a video, sound or video-sound recording of his personal expression, obtained with his consent, capable of substantially endangering his seriousness or causing him any other serious harm to rights,

he faces up to three years in prison.

Please provide case law to illustrate the application of the rules in practice.

Please provide details on known issues of application.

Since this crime is regulated by Slovak law only from 2021, there is currently no judicial practice available to it and therefore it is not even expected that juveniles have been punished for it so far.

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:

Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.

As has already been stated in the answer to question 3, sharing false news or false information cannot be currently punished by criminal law.

If a person on the Internet pretends to be someone else, it does not constitute a crime. In this case, the protection of personal rights in civil proceedings is considered.

Pretending to be an expert is not a criminal offence unless the perpetrator shows a profit in the area. Any person who unlawfully carries out small-scale business activities shall be liable to a term of imprisonment of up to one year. The offender shall be liable to a term of imprisonment of between six months and three years if he commits this offence by providing, without professional qualifications, services or other professional activities which, by law, can only be carried out by a person with professional competence.

Please provide case law to illustrate the application of the rules in practice.

Please provide details on known issues of application.

As wilful misinformation or deception online is not a criminal offence, the case law and issues of application are not known.

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:

Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases).

Juveniles are as criminally responsible for the crime of trafficking in human beings as adult offenders. The Criminal Code does not specifically regulate the crime of trafficking in human beings committed on the basis of online space. If the offender searches the victim on the Internet, communicates with them and creates the conditions for committing it, it may be a preparation for the crime of trafficking in human beings.

Any person who, by using fraudulent practices, a trick, restriction of personal freedom, violence, threatened violence, threat of grievous bodily harm or other forms of coercion, by accepting or offering monetary payment or other benefits in order to get approval of a person on whom another person depends, or by misusing his position, or abusing of defencelessness or other vulnerable position, entices, transports, harbours, hands over or takes over another person, even upon his consent, for the purposes of his prostitution or another form of sexual exploitation, including pornography, forced labour and services including beggary, slavery or practices similar to slavery, servitude, forced marriage, misuse for committing criminal activities, removal of organs, tissues or cells or other forms of exploitation, shall be liable to a term of imprisonment of four to ten years.

The same sentence shall be imposed on any person who entices, transports, harbours, hands over or takes over a child, even with his consent, for the purposes of his prostitution or other form of sexual exploitation, including child pornography, forced labour or forced services including beggary, slavery or practices similar to slavery, servitude, forced marriage, misuse for committing criminal activities, illegal adoption, removal of organs, tissues or cells or other forms of exploitation.

Preparation for committing a crime means wilful organisation of a criminal act, procurement or adaptation of means or instruments for its commission, associating, grouping, instigating, contracting, abetting or aiding in such crime, or other deliberate actions designed to create conditions for its commission, where a crime has been neither attempted nor completed. Preparation for committing a felony shall carry the same punishment as the crime, for which it has been intended. The court may also reduce the term of imprisonment below the minimum rate set out for this crime also when sentencing an offender for preparing a felony or for an attempted criminal offence if it believes that, considering

the nature and gravity of preparation or attempt, a custodial sentence pursuant to law would be inappropriately harsh, and that a shorter-term punishment would be sufficient to protect the society.

Please provide case law to illustrate the application of the rules in practice.

Please provide details on known issues of application.

Given the nature of this crime, it is not common in Slovakia for this crime to be committed by juvenile offenders, and judicial practice is not known to do so. In 2021, a total of 39 people were prosecuted for this crime, one of them was juveniles. Also, one juvenile has been prosecuted for this crime in 2022 yet.

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:

Please explain the applicable rules (all applicable legal qualifications/ articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.

Protection against the illegal use or dissemination of content protected by intellectual property rights is provided through the infringement of copyright offence.

Any person who unlawfully infringes the protected copyright to a work, performance by a performing artist, an audio recording or audio-video recording, radio or television programme or database shall be liable to a term of imprisonment of up to two years.

Conditions for application:

- *object of the offence: the protection of the work and copyright in works from unauthorised disposal in connection with its creation, use and dissemination,*

- *subject of the offence: this offence can only be committed by an offender who has reached the age of 14,*

- *subjective aspect of the offence: intentional causation,*

- *objective aspect of the offence: unlawfully infringes the protected copyright to a work.*

Punishments:

Since it is an offence where there is not even a lower limit of the penalty, it is expected to impose a conditional sentence with compensation for the damage suffered. If the proceedings were not so serious, the act would not have to be prosecuted at all as a criminal offence.

Statistics:

In 2021, a total of 15 people were prosecuted for this offence, none of them juveniles. Also, no juvenile has been prosecuted for this offence in 2022 yet.

Please provide case law to illustrate the application of the rules in practice.

Please provide details on known issues of application.

As this is an offence that is not committed by juveniles, there is no known case law or application problems in this area.

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:

Please explain the applicable rules (all applicable legal qualifications/articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.

Anyone who overcomes a security measure and thereby obtains unauthorised access to the computer system or part thereof shall be punishable by up to two years imprisonment.

Conditions for application:

- *object of the offence: the protection of the computerised system as a whole or part thereof,*

- *subject of the offence: this offence can only be committed by an offender who has reached the age of 14,*

- *subjective aspect of the offence: intentional causation,*

- *objective aspect of the offence: unauthorised intrusion into the computer system or part thereof by overcoming the security measure.*

Juveniles can also be punished for hacking, but it is not a common crime. Since it is an offence where there is not even a lower limit of the penalty, it is expected to impose a conditional sentence with compensation for the damage suffered. If the proceedings were not so serious, the act would not have to be prosecuted at all as a criminal offence.

Statistics:

In 2021, a total of 2 people were prosecuted for this offence, none of them juveniles. Also, no juvenile has been prosecuted for this offence in 2022 yet.

Other cybercrime offences:

- Who restricts or interrupts the functioning of a computer system or part thereof by unauthorised insertion, transmission, damage, erasure, deterioration, alteration, suppression or inaccessibility of computer data, or by making unauthorised interference with the technical or software of the computer and unlawfully destroys, damages, erases, alters or reduces the quality of the information obtained shall be punishable by a custodial sentence of between six months and three years.

- Anyone who intentionally damages, erases, alters, suppresses or disables computer data or impairs its quality within or part of a computer system shall be punishable by a custodial sentence of between six months and three years.

- Anyone who unlawfully intercepts computer data by means of technical means of non-public transmission of computer data to, from or within a computerised system, including electromagnetic emissions from a computerised system containing such computer data, shall be punishable by a custodial sentence of between six months and three years.

Please provide case law to illustrate the application of the rules in practice.

Please provide details on known issues of application.

As this is an offence that is not committed by juveniles, there is no known case law or application problems in this area.

Question 14: Can minors be punished for acts of using Cybercrime as a Service? If yes, under what qualification? In particular, how would this apply to using such services for exploiting vulnerabilities in IoT and connected devices e.g., the device of a friend or acquaintance? Does it matter if the intent is somewhat innocent (i.e., the minor thinks it's a joke or a prank)? If criminal sanctions could apply, are minors prosecuted in practice?

Answer:

Please explain the applicable rules (all applicable legal qualifications/articles, conditions for application, prescriptive period, and the range and types of punishment that may be imposed and jurisdictional aspects in cross-border cases) and applicable policy.

The Criminal Code does not include a criminal offence that would punish the use of a service served illegally. Passive conduct which does not involve unauthorised interference with the computerised system or data or a violation of copyright, does not constitute a criminal offence.

Please provide case law to illustrate the application of the rules in practice.

Please provide details on known issues of application.

Because of the absence of criminality of the act, the case law or issues of application are not known.

4. 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:

Please explain the applicable rules or policies, if any, and their impact in practice.

The Slovak Criminal Code shall be applied to determine the criminal liability for an act committed on the territory of the Slovak Republic.

The criminal offence is considered as having been committed on the territory of the Slovak Republic even if the offender

a) committed the act, at least in part, on its territory, if the actual breach of or threat to an interest protected under this Act took place or was intended to take place, in whole or in part, outside of its territory, or

b) committed the act outside of the territory of the Slovak Republic, if the actual breach of or threat to an interest protected under this Act was intended to take place on its territory, or such a consequence should have taken place, at least in part, on its territory.

The Slovak Criminal Code shall also be applied to determine the criminal liability for an act committed outside of the territory of the Slovak Republic aboard a vessel navigating under the State flag of the Slovak Republic, or aboard an aircraft entered in the aircraft register of the Slovak Republic.

The Slovak Criminal Code also be applied to determine the criminal liability for an act committed outside of the territory of the Slovak Republic by a Slovak national or a foreign national with permanent residency status in the Slovak Republic.

The Slovak Criminal Code also be applied to determine the criminal liability for a particularly serious felony if the act was committed outside of the territory of the Slovak Republic against a Slovak national, and if the act gives rise to criminal liability under the legislation effective in the place of its commission, or if the place of its commission does not fall under any criminal jurisdiction.

The question of whether judgments have extraterritorial effect depends on the legal order of individual countries. The decision of the court of another State in a criminal matter by which a punishment was imposed may be performed in the territory of the Slovak Republic only if it is recognised by the Slovak court.

If there is a specific impact on cybercrime committed by minors, please explain this as well.

Please provide details on known issues of application.

Related to this question there is no specific impact on cybercrime committed by minors or issues of application.

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:

Please explain the applicable legal instruments (Budapest Convention, bilateral treaties), if any, their implementation in national law (if necessary) and their impact in practice.

Slovakia implemented Budapest Convetion by announcement in The collection of law in 2008. Furthermore, Slovakia has transposed Directive 2013/40/EU of the European Parliament and of the Council on attacks on information systems by Act No. 398/2015 Coll. on the European Protection Order in Criminal Matters in Art. II.

With effect from 1 January 2016, Slovakia has adopted new offences:

▪ Unauthorized access to the computer system

▪ Unauthorised interference with the computer system

▪ Unauthorized interference with computer data

▪ Unauthorized interception of computer data

▪ Manufacture and possession of access equipment, computer system password or other data

The purpose of the Convention is to harmonise national legislation, to provide investigative bodies with appropriate procedural tools for investigating this type of crime, to strengthen and streamline cross-border cooperation. This Convention is the most comprehensive instrument for combating cybercrime, containing both substantive provisions and procedural provisions and provisions on international cooperation.

If there is a specific impact on cybercrime committed by minors, please explain this as well.

Please provide details on known issues of application.

Related to this question there is no specific impact on cybercrime committed by minors or issues of application.

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:

Please explain the applicable rules or policies, if any, and their impact in practice. E.g. Mutual Legal Assistance (based on a specific bi-lateral treaty, or on the Budapest Convention and national law or purely on the basis of national law), EU instruments, participation in INTERPOL Cybercrime Information Sharing, etc.

CERT

At national and EU level, CERT teams work in the fight against cybercrime. They work together to deal with each other in dealing with attacks and then provide information to providers so that they can defend themselves against attacks. They also serve as primary entities for early warning and monitoring of cyber danger. They respond to incidents and attacks in a coordinated manner with other Member States.

With designation of the National Security Authority as the National Authority for Cyber Security since January 1st, 2016, the Authority has established the Slovak Computer Emergency Response Team (SK-CERT), which was transformed to National Cyber Security Centre SK-CERT on September 1st, 2019. It provides national and strategic activities in the field of cyber security management, threat analysis as well as coordination of national security incident resolution. National Cyber Security Centre also aids governance, development, management and support of cyber security competence centres, including training, educational activities, and research.

Creating and distributing security bulletins and alerts containing current information on cyber threats, product vulnerabilities, cyber-security incidents, or other cyber-related information, Monitoring, detecting and evaluating cyber-related incidents and threats at national level, Resolving cyber-security incidents and their coordination at national level, eliminating their impact, and then restoring the operation of information systems in cooperation with the owners and operators of the systems concerned, Strategic analysis of incidents, vulnerabilities and threats at national level, Creating background for strategic decision-making on cyber security, Security and operational monitoring services, Forensic analysis, malware analysis, Keeping track of trends in cyber security and new opportunities, Increasing cyber security awareness by publishing of articles, knowledge standards, advice and recommendations, Sharing information with national and international partners, Cyber-security education and training, Research into the field of cyber security, Applying the invented techniques including and AI and machine learning towards the goal of increasing the level of national cyber security.

On April 1, 2018, went into force The Act No. 69/2018 on Cyber security and on the amendment of certain laws defining the roles, rights and obligations in the field of cyber security. At the same time, this law determines the role of the National Security Authority as the National CSIRT Unit, with this task being performed by the independent unit National Unit SK-CERT.

The National CSIRT Unit, SK-CERT performs various tasks under the law in the Slovak cyberspace:

- fulfils the notification and reporting obligations towards the competent authorities of the European Union and the North Atlantic Treaty Organization, and participates in and supports the development of national and international partnerships in the field of cyber security,

- ensures the membership of the Slovak Republic in the cooperation group and in the network of CSIRT units,

- cooperates with central authorities, other state administration bodies and CSIRT units, basic service providers and digital service providers in the performance of their tasks under this Act,

- systematically acquires, gathers, analyses and evaluates information on the state of cyber security in the Slovak Republic,

- provides and is responsible for coordinated cyber security incident resolution at national level,

- resolves cyber security incidents, announces a warnings and issues a warning of a major cyber security incident, imposes an obligation to take a reactive action, and approves a security measure,

- announces early warnings,

- receives national reports on cyber-security incidents,

- receives reports on cyber security incidents from abroad and ensures cooperation with international organizations and authorities of other states in dealing with cyber security incidents with a cross-border nature.

EUROJUST

In the context of investigations and prosecutions involving two or more EU Member States, EUROJUST shall operate with the objectives of which are to::

• to stimulate and improve the coordination of investigations and prosecutions in the Member States between the competent authorities of a Member State, taking into account any request from the competent authority of a Member State and any information provided by any authority competent under provisions adopted within the framework of the Treaties.

• improve cooperation between the competent authorities of the Member States, in particular by facilitating the processing of requests for judicial cooperation and the implementation of decisions on judicial cooperation, including applications and decisions relating to instruments conferring effect on the principle of mutual recognition

• otherwise, encourage the competent authorities of the Member States to make their investigations and prosecutions more effective.

European Cybercrime Centre

European Cybercrime Centre has 5 strategies:

• dismantle international criminal networks

• prevent terrorism, radicalisation and recruitment of new members

• increase the level of security of citizens and the business public in cyberspace

• increase security through border management

• increase Europe's resilience to crises and disasters.

As a liaison information department, the Centre should ensure the collection of information on cybercrime from the widest possible range of public, private and open sources. It should gradually fill existing gaps in the information provided by those responsible for cybersecurity and the fight against cybercrime. The information collected concern activities, methods and suspects in the field of cybercrime. They serve to improve knowledge of and prevent, detect and prosecute cybercrime, as well as to promote relevant links between law enforcement authorities, the computer emergency response team and private sector information and communication technology security experts. The European Cybercrime Centre helps EU Member States reduce cybercrime through expertise and training. The

Centre provides operational support in the investigation of cybercrime cases, for example by supporting the setting up of joint investigation teams and promoting the exchange of operational information in ongoing investigations. In the context of cybercrime investigations, it also provides forensic assistance and coding expertise.

If there is a specific impact on cybercrime committed by minors, please explain this as well.

Please provide details on known issues of application.

Related to this question there is no specific impact on cybercrime committed by minors or issues of application.

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:

Please indicate relevant rules or policies, if any, and their impact on cybercrime committed by minors in practice.

Cybercrimes committed by young people is not a serious problem in Slovakia, as evidenced by the above statistics. Hacking is not perpetrated by juveniles, as this crime requires better computer skills. A more common problem is electronic harassment or bullying through social networks. In most cases, this kind of criminality is latent. However, even if it appears, it should be dealt with in the first place by families and schools, not by criminal law. However, a bigger problem are sexually motivated crimes through electronic services aimed to children. At this point, the Criminal Code sufficiently regulates offences relating to the protection of minors from sexual predators.

5. 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:

Please provide us with any information from official sources you may have and, if possible, of the impact of any changes in legislation or policy.

1. The offence of sexual abuse by using an electronic communication service:

2020 – a total of 11 prosecuted people,

2021 – a total of 9 prosecuted people,

2022 – a total of 1 prosecuted person.

2. The offence of dangerous electronic harassment (cyberbullying):

2020 – not in Criminal code in that year,

2021 – no one prosecuted,

2022 – no one prosecuted.

3. The crimes connected to child pornography:

-2020 - a total of 20 people were prosecuted for manufacturing of child pornography, 2 of them were juveniles. A total of 85 people were prosecuted for dissemination of child pornography, 27 of them were juveniles. A total of 58 people were prosecuted for possession of child pornography, 8 of them were juveniles,

- 2021, a total of 26 people were prosecuted for manufacturing of child pornography, 10 of them were juveniles. A total of 99 people were prosecuted for dissemination of child pornography, 41 of them were juveniles. A total of 55 people were prosecuted for possession of child pornography, 13 of them were juveniles,

-2022, a total of 12 people were prosecuted for manufacturing of child pornography, 2 of them were juveniles. A total of 29 people were prosecuted for dissemination of child pornography, 49 of them were juveniles. A total of 17 people were prosecuted for possession of child pornography, 5 of them were juveniles.

4. Infringement of copyright:

- 2020 - a total of 21 people were prosecuted for this offence, none of them juveniles,

- 2021- a total of 15 people were prosecuted for this offence, none of them juveniles,

- 2022 – 0 prosecuted people.

5. Unauthorized access to the computer system:

- 2020 - a total of 2 people were prosecuted for this offence, none of them juveniles,

- 2021- a total of 15 people were prosecuted for this offence, none of them juveniles,

- 2022 – 0 prosecuted people.

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

Answer:

Please provide us with any other comments you think are relevant for us to understand the legal and policy situation in your country.

The one of the main issue of criminal legislation in Slovakia is that it is not progressive and regulates high penalties. The Cod Law and The Code of Criminal Procedure have been in force in Slovakia since 2005, and their recodification is currently necessary in accordance with modern times. The Criminal Code regulates a number of outdated or non-novelized crimes. It is also necessary to adjust the penalty rates, as it is scientifically proven that too high repression does not act preventively.