QUESTIONNAIRE

PORTUGAL

Pedro VICENTE

Polícia Judiciária

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 amount 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.

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

Please provide details on known issues of application.

Article 176 - A - Solicitation of minors for sexual purposes was added to the Criminal Code by Law no. 103/2015, of 24 August. In this way, fulfilling the wishes of the Directive 2011/93/EU, new forms of sexual abuse and exploitation facilitated by the use of ICT have been criminalized, such as the solicitation of a minor through the internet[1]

Article 176a (Criminal Code)

Enticement of minors for sexual purposes

1 - Whoever, being of age, entices a minor, by means of information and communication technologies, to an encounter for the practice of any of the acts included in paragraphs 1 and 2 of article 171[2] and in paragraphs a), b) and c) of paragraph 1 of the previous article[3], shall be punished by a maximum imprisonment of one year.

2 - If such inducement is followed by material acts leading to the encounter, the agent shall be punished by imprisonment of up to 2 years.

---

[1] "Manual ROAR - da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas"

[2] Article 171 (Criminal Code)
Sexual abuse of children
1 - Whoever commits a relevant sexual act with or on a person under 14 years of age, or causes him or her to commit such an act with another person, shall be punished with a prison sentence of one to eight years.
2 - If the relevant sexual act consists of copulation, anal coitus, oral coitus or vaginal or anal introduction of body parts or objects, the agent shall be punished by imprisonment of three to ten years.

[3] Article 176 (Criminal Code)
Pornography of minors
1 - Who:
a) Using a minor in pornographic performances or inducing for such purposes;
b) Using a minor in pornographic photography, film or recording, whatever the medium, or to entice him/her to do so;
c) Produce, distribute, import, export, divulge, exhibit, cede or make available under any title or by any means, the materials foreseen in the previous sub-paragraph;

Article 118 (Criminal Code)

Statute of Limitation

1 - The criminal procedure is extinguished by statute of limitations as soon as the following periods of time have elapsed since the commission of the crime

…

c) Five years, in relation to crimes punishable by a prison sentence with a maximum limit of one year or more but less than five years;

…

2 - For the purpose of the provisions of the previous item, in determining the maximum sentence applicable to each crime, the elements pertaining to the type of crime shall be taken into account, but not aggravating or attenuating circumstances.

…

5 - In the case of crimes against sexual freedom and self-determination of minors, as well as the crime of female genital mutilation where the victim is a minor, the criminal procedure shall not be extinguished by statute of limitations before the victim turns 23 years of age.

Article 4 (Law 88/2017)

Scope of application

1 - The EIO shall cover any investigative measure with the exception of the setting up of joint investigation teams and the taking of evidence by such teams.

2 - The EIO shall also cover investigation measures intended for the achievement of the objectives of a joint investigation team, to be carried out in a Member State not participating in it, by decision of the competent judicial authority of one of the Member States participating in it.

3 - The EIO applies to the acquisition of new evidence and the transmission of evidence held by the competent authorities of the executing State, at all stages of the proceedings.

Article 5 (Law 88/2017)

Types of proceedings

An EIO may be issued

(a) in criminal proceedings which are initiated by a judicial authority, or which may be initiated before such an authority, in respect of a criminal offence under the national law of the issuing State;

(b) in proceedings brought by judicial authorities in respect of an offence which is punishable under the national law of the issuing State, provided that the decision may give rise to proceedings before a court having jurisdiction in particular in criminal matters

(c) in proceedings brought by administrative authorities in respect of offences which are punishable under the national law of the issuing State, including for offences which constitute an administrative

offence, and where the decision may give rise to proceedings before a court having jurisdiction in particular in criminal matters

(d) in connection with proceedings referred to in the previous sub-paragraphs which relate to offences or other illegal acts for which a legal person may be held liable or punished in the issuing State.

Article 2 (Law 65/2003)

Scope of application

1 - A European arrest warrant may be issued for acts punishable by the law of the issuing Member State by a custodial sentence or a detention order for a maximum period of at least 12 months or, where the aim is the enforcement of a sentence or detention order, provided that the sentence imposed is for a period of at least four months.

Article 11 (Law 109/2019 – Cybercrime Law)

Scope of application of the procedural provisions

1 - With the exception of the provisions of Articles 18 and 19, the procedural provisions set out in this Chapter shall apply to proceedings concerning crimes:[4]

(a) Provided for in this law;

b) Committed by means of a computer system; or

c) In relation to which it is necessary to collect evidence in electronic format.

2 - The procedural provisions provided for in this chapter shall not prejudice the regime of Law 32/2008, of 17 July.

Article 1 (Law 166/1999)

Scope of the law

The practice, by a minor between the ages of 12 and 16, of an act qualified by law as a crime shall give rise to the application of a tutel educational measure in accordance with the provisions of this law.

"Online grooming can be defined as a process of manipulation and a form of grooming of children. It usually starts through a non-sexual approach, namely through the Internet and ICT, including online games and social networks, in order to establish a relationship of trust with the child and convince the child to meet personally with another person, so that the latter may consummate the sexual abuse. The establishment of trust with the child, mediated by the internet and ICTs, may also aim at persuading the child to produce and share sexual content.

Online grooming allows perpetrators to select the type of victim they want to manipulate and and lure. Additionally, online grooming allows for the grooming of a large number of victims victims simultaneously, among other advantages for the perpetrator of the online grooming and anonymity, the

[4] Article 12 Expedited data preservation; Article 13 Expedited disclosure of traffic data; Article 14 Injunction to produce or grant access to data; Article 15 Search for computerised data; Article 16 Seizure of computer data

preservation of his/her real identity and the management of the other "identities" with which he/she presents with which he/she presents him/herself to the targets selected.

Following this form of sexual abuse and exploitation, the child may be subject to threats and blackmail to divulge or share the sexual contents produced by themselves, in order to obtain sexual favours sexual favours, money or other benefits."[5]

The Portuguese legislator has extended the scope of incrimination with reference to Directive 2011/93 by typifying as victim any person under 18 years of age.

Thus, in our understanding, besides the cases in which the victim does not have the legal age for legal self-determination - 14 years old in the case of Portugal - the legal provision should contain the enticement, whether by force of deceit, inexperience of the victim, fragility of the victim, power relationship that overshadows an already relevant will of the victim. A healthy relationship between adolescents who, for instance, already know each other in real life and whose wills are relevant and freely established, cannot be considered punishable.

Judgment of the Lisbon Court of Appeal n.º xxx

"The legal provision of the crime of enticement of minors for sexual purposes covers the typical hypotheses in which the agent uses means connected to the information and communication technologies to arrange meetings with minors in order to practice with them pornographic or relevant sexual acts.

It is a formal crime or a crime of mere activity, which is consummated, therefore, with the mere attempt of arranging a meeting with a minor with such illicit desiderata (it is not required that the meeting actually takes place), and it is also an abstract danger crime.

The doctrine and jurisprudence coincide in the understanding that a relevant sexual act will be the act endowed with objective sexual connotation identifiable by an external observer, which is abstractly suitable for the satisfaction of sexual instincts that constitute a serious and grave offence against the intimacy and sexual freedom of the passive subject.

The typical provision regarding solicitation does not require the use of any explicit formula in the invitation and in order to understand the purpose intended by the accused when writing and sending the messages, a joint interpretation of the common meaning of the expressions used must be made.

Taking into account the express references to various acts of copulation, followed by requests for a relationship in an intimate and affectionate atmosphere ("just the two of us alone, at ease" "to see you well and happy, so that you can relax and unwind with me and feel loved and cared for" "I love you and I like you a lot"), in a private place where the accused was available ("bring you to my house"), it is unequivocal for us that by sending messages through social networks, the accused not only had the purpose of arranging a mere meeting with the minor but also intended that in that meeting he would practice with her a sexual act as provided for in Article 171 no. 1 and no. 2 of the Penal Code."

Judgment of the Coimbra Court of Appeal n.º xxx

"I - Enticement of a minor for sexual purposes, a conduct typified in article 176-A of the Penal Code, presupposes an approach to the child by any technological means of information and communication, such as the Internet and the mobile phone.

[5] "Manual ROAR - da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas"

II - Enticement constitutes an aggravated form of the crime when it involves the performance of material acts leading to a meeting of the agent with the minor - e.g. travelling to the meeting place, helping to transport the victim and arranging a physical space for the purpose.

III - The type of crime in article 176-A of the Criminal Code contains an intention ("aiming") to achieve a result that is not part of it (the practice of acts provided for in article 171 (1) and (2) and article 176 (1) (a), (b) and (c)), but is provoked by a subsequent action by the perpetrator, thus providing for a crime of a severed act.

IV - The subjective type admits only the intentional form of malice, as is clear from the Lanzarote Convention and the word "aiming".

V - The said offence is a common crime of necessary accomplishment in the form of a crime of encounter, with the minor (necessary accomplice) not being punishable."

VI - The offence provided for in article 176-A, no. 1 of the Criminal Code is committed by the agent who, through various messages sent to a minor insinuating sexual acts to be practised with her, tries to meet her, offering to pay for her trip and suggesting that she give him a lift to a place where they could meet.

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.

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

Please provide details on known issues of application.

"Cyber-bullying emerges from the use of ICT and the Internet, with the aim of verbally and/or contribute to the victim's social exclusion and isolation. Some of the behaviours that operationalise this form of online aggression may include: the dissemination of negative/false information with the intention of defaming the victim (through the use of phone calls, text messages, video messages, e-mail messages, video messages, email, chat room, websites, social networks); harassment of the victim (by the use of the same means) (APAV, 2011; Jahankhani et al., 2014).

Cyber-bullying is distinguished from more conventional forms of bullying by the possibility at any time of the day, regardless of the need for direct contact between victim and aggressor, by the potential of anonymity that it guarantees to the aggressor, by the high potential of "publicity" and audience with which it is associated (it can be infinitely shared in the social networks or any other Internet communication platform where it was initiated/published and even published and even between platforms) and by the difficulty of removing the content created.

In what concerns the different forms of expression of cyber-bullying, we can highlight conducts of online aggression with a sexual nature, such as:

- The online sharing of rumours or lies about the victim's sexual behaviour;

- The use of offensive or discriminatory sexual language online directed against the victim;

- The theft of identity for the purpose of sharing sexual content and/or sexual harassment against other persons on behalf of the victim;

- The sharing of information online concerning the victim's intimacy, in a non-consensual manner, as a strategy to perpetuate aggression and harassment behaviours on a large scale.

We may also highlight body shaming through the Internet and ICTs, as the sharing of derogatory comments about the victim's physical appearance, and outing, when someone publicly reveals (or threatens to reveal) publicly, through the Internet and ICTs, information regarding the victim's sexual orientation or gender identity, without the victim's knowledge and authorisation.

Cyber-stalking may be defined as a form of stalking which, maintaining the intrusive, repetitive and persistent character that causes fear to the victim and characterises this form of persecution and persistent harassment, is practised using the Internet and ICTs, with the aim of threatening and harass the victim (Maran & Begotti, 2019).

Cyber-stalking practices may include, among different stalking behaviours:

making multiple and unwanted attempts to contact the victim, via telephone, email and social networks;

installing spyware in the victim's computer; accessing, without the victim's permission, the victim's e-mail and/or

social networks account, to monitor private information and the victim's daily life and/or to act on their behalf (Martellozzo & Jane, 2017)

Still in the scope of online violence in the context of interpersonal relationships, we may highlight, besides cyber-bullying and cyber-stalking, the non-consensual dissemination of images and videos, as the sharing of intimate images, including photographs, films and/or video recordings, without the consent of the person viewing their nudity, body parts, including sexual organs, and/or exposed sexual activity"[6]

There is no specific typification of the crime of cyber-bullying, having to signal and frame the concrete behaviours developed by the aggressor, namely:

Art.3 º Cibercrime Law – Law 109/2019

Computer forgery

1 - Whoever, with intent to cause deception in legal relations, enters, modifies, deletes or suppresses computer data or in any other way interferes with a computer processing of data, producing non-genuine data or documents with the intention that they be considered or used for legally relevant purposes as if they were, is punishable by a term of imprisonment of up to five years or a fine of 120 to 600 days.

Art. 6 º Cibercrime Law – Law 109/2019

Illegal access

[6] "Manual ROAR - da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas"

1 - Whoever, without legal permission or without being authorised by the owner or other right holder of the system or of part of it, in any way accesses a computer system, shall be punished with a prison sentence of up to one year or with a fine of up to 120 days.

Article 193 º Penal Code

Devastation by means of computer

1 - Whoever creates, maintains or uses an automated file of individually identifiable data concerning political, religious or philosophical beliefs, party or union membership, private life or ethnic origin, is punished with a prison sentence of up to two years or with a fine of up to 240 days.

Art 154-A Penal Code

Pursuit

1 - Whoever repeatedly pursues or harasses another person, by any means, directly or indirectly, in a manner likely to cause him fear or uneasiness or to impair his freedom of determination, shall be punished by imprisonment for up to three years or a fine, if a more serious penalty is not applicable under any other legal provision.

2 - Attempts are punishable.

3 - In the cases provided for in no. 1, the defendant may be charged with the accessory penalties of prohibition of contact with the victim for a period of between 6 months and 3 years and the obligation to attend specific programmes for the prevention of behaviour typical of stalking.

4 - The accessory penalty of prohibition of contact with the victim must include removal from the victim's residence or place of work and its compliance must be monitored by technical means of remote control.

5 - The criminal procedure depends on a complaint.

Article 192 º Penal Code

Invasion of privacy

1 - Whoever, without consent and with intent to intrude upon the private life of persons, namely the intimacy of family or sexual life:

(a) intercepts, records, uses, transmits or discloses conversation, telephone communication, electronic mail messages or detailed billing;

b) Capture, photograph, film, record or disclose images of people or intimate objects or spaces;

(c) secretly observing or eavesdropping on persons in a private place; or

(d) disclosing facts concerning another person's private life or serious illness;

shall be punished with imprisonment of up to one year or with a fine of up to 240 days.

2. The act provided for in sub-paragraph d) of the preceding paragraph shall not be punishable when committed as an appropriate means for the achievement of a legitimate and relevant public interest.

Art. 194º Penal Code

Breach of correspondence or telecommunications

1 - Whoever, without consent, opens a parcel, letter or any other closed writing that is not addressed to him/her, or learns of its contents by technical means, or prevents it from being received by the addressee in any way, is punished with a prison sentence of up to one year or with a fine of up to 240 days.

2 - The same penalty is applicable to anyone who, without consent, interferes with or becomes aware of the contents of a telecommunications program.

3 - Whoever, without consent, discloses the contents of letters, parcels, sealed documents or telecommunications referred to in the previous paragraphs, shall be punished by a prison sentence of up to one year or a fine of up to 240 days.

Art. 199 º Penal Code

Illegal recordings

1 - Whoever without consent:

(a) records words spoken by another person and not intended for the public, even if they are addressed to him; or

b) Uses or allows the use of the recordings referred to in the previous paragraph, even if they are lawfully produced;

is punished with a prison sentence of up to one year or with a fine of up to 240 days.

2 - The same penalty is incurred by anyone who, against their will:

(a) photographs or films another person, even at events in which he or she has legitimately participated; or

b) Use or allow the use of photographs or films referred to in the preceding paragraph, even if lawfully obtained.

Art. 240, par. 1, points (a) and (b) Penal Code

Discrimination and incitement hatred and violence

1 - Whoever:

(a) founds or forms an organization or engages in organized propaganda activities that incite or encourage discrimination, hatred or violence against a person or group of persons because of their race, color, ethnic or national origin, ancestry, religion, sex, sexual orientation, gender identity or physical or mental disability; or

b) Participating in or providing assistance to the organization or activities referred to in the previous paragraph, including financing them;

shall be punished with a prison sentence of one to eight years.

2 - Whoever publicly, by any means intended for dissemination, namely through apologia, denial or gross trivialization of crimes of genocide, war or against peace and humanity:

(a) provoke acts of violence against a person or group of persons because of their race, color, ethnic or national origin, ancestry, religion, sex, sexual orientation, gender identity or physical or mental disability;

b) Defaming or insulting a person or group of people because of their race, color, ethnic or national origin, ancestry, religion, sex, sexual orientation, gender identity or physical or mental disability

(c) threatening a person or a group of persons because of race, color, ethnic or national origin, ancestry, religion, sex, sexual orientation, gender identity or physical or mental disability; or

(d) inciting violence or hatred against any person or group of persons because of their race, color, ethnic or national origin, ancestry, religion, sex, sexual orientation, gender identity or physical or mental disability;

is punishable by imprisonment from 6 months to 5 years.

“Judgement of 14 March 2007 (Case nº 0644864) Purposes of the tutela educativa measure

According to article 1 of Law no. 166/99, of 14 September, hereafter referred to as the LTE, "the practice by a minor aged between 12 and 16 years of between the ages of 12 and 16 years, of an act qualified by law as a crime shall give rise to the application of a tutelary educational measure in accordance with the provisions of the present law".

On the other hand, article 1, no. 2 of the same law states that "the tutelary educational measures are aimed at educating minors to the law and their insertion, in a dignified and responsible way, in life in the community". However, the purpose of these measures is not at all to punish the practice of illicit committed, but rather to educate each one of the minors to the legal duty/being, in essence it is their socialization in the sense of incorporating the values and legal norms of a society which respectful of the most essential moral and ethical values. The minors, naturally some more than others others, have revealed a great contempt for such an important social value as the physical integrity of the human of the human person.”

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.

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

Please provide details on known issues of application.

Misinformation and on-line deception are not in themselves types of crime, but are part of some typical conduct relating to other crimes.

This circumstance may be because in Portugal Non-repudiation, meaning the trust that a certain communication may be attributed to an authentic and not disguised sender, is not yet being identified as a Legal Asset associated to computer systems, like security, confidentiality and integrity.

The most commonly associated criminal offence of misinformation and deception is perhaps that of:

Art. 199 º Penal Code

Illegal recordings

1 - Whoever without consent:

(a) records words spoken by another person and not intended for the public, even if they are addressed to him; or

b) Uses or allows the use of the recordings referred to in the previous paragraph, even if they are lawfully produced;

is punished with a prison sentence of up to one year or with a fine of up to 240 days.

2 - The same penalty is incurred by anyone who, against their will

(a) photographs or films another person, even at events in which he or she has legitimately participated; or

b) Use or allow to be used photographs or films referred to in the previous sub-paragraph, even if lawfully obtained.

…

Conduct that could be consummated by verifying its integration as mode of action in crime such as Grooming, online sexual abuse, coercion, insult, defamation etc.

And the most common phenomena are:

Fraud in intimate relationships

Fraud in intimate relationships occurs when the perpetrator seeks to establish a relationship of trust and intimacy, namely through the Internet and ICT, with a certain target, as a prelude to obtaining personal benefit, namely financial and patrimonial.

In this form of fraud, there is usually room for:

- Creation of a false profile on social networks, dating applications or other chat and social interaction platforms;

- Establishing contact with apparently more vulnerable targets;

- Creating an emotional bond with the previously identified target;

- Development of a narrative with the intention of extorting personal/financial assets from the target.

This process of seduction and creation of a relationship with the victim aims at accessing the victim's money or other assets, bank accounts, credit cards, passports, email accounts, and/or personal identification numbers. It may also aim at coercing the victim into committing crimes on behalf of the

the perpetrator's name.[7]

Online identity theft

Identity theft covers the non-consensual obtaining of personal and/or confidential data of a particular victim (such as, for example, the victim's e-mail account and/or personal identification numbers), their possession or transfer, and their use in committing crimes.

It includes, in this way and cumulatively, the following acts:

- Obtaining personal and/or confidential information about another person, without their knowledge;

- Possession or transfer of such data with the awareness that it will be used for illicit illicit purposes;

- Using the data initially obtained for the commission of crimes.

These acts correspond to online identity theft when the personal and/or confidential data of the victim are obtained through the Internet and/or when the data obtained, by any means, are transferred over the Internet and/or used for the commission of a crime over the Internet.

It usually has as its objectives the obtaining of financial advantage, credit and other benefits, the creating disadvantage or loss for the victim (Enisa, 2010, Harrell & Lagton, 2013, Tuli & Juneja, 2015 cited in Reep-van den Bergh & Junger, 2018), and even committing crimes on behalf of the victim. The victim whose identity has been used, in addition to financial losses, may thus be subject to legal consequences if they are held responsible for the perpetrator's actions.

Identity theft is not a crime in itself, but may encompass a multiplicity of crimes provided for and punishable under the Portuguese Criminal Code.[8]

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.

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

Please provide details on known issues of application.

The phenomenon of trafficking in human beings is fundamentally foreseen in Article:

Article 160º Penal Code

Human Trafficking

[7] "Manual ROAR - da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas"
[8] "Manual ROAR - da compreensão e prevenção do cibercrime ao apoio e empoderamento das vítimas"

1 - Whoever offers, delivers, recruits, entices, accepts, transports, harbors or receives a person for the purpose of exploitation, including sexual exploitation, labor exploitation, begging, slavery, organ extraction or the exploitation of other criminal activities:

(a) By means of violence, abduction, or serious threat;

b) Through ruse or fraudulent maneuver;

c) With abuse of authority resulting from a relationship of hierarchical, economic, work, or family dependence;

d) By taking advantage of a psychic incapacity or a situation of special vulnerability of the victim; or

e) By obtaining the consent of the person in control of the victim;

shall be punished with a prison sentence of between three and ten years.

2 - The same penalty is applied to whoever, by any means, recruits, entices, transports, harbours or receives a minor, or delivers, offers or accepts him/her for the purposes of exploitation, including sexual exploitation, labour exploitation, begging, slavery, organ extraction, adoption or the exploitation of other criminal activities.

3 - In the case provided for in the previous number, if the perpetrator uses any of the means provided for in paragraph 1 or acts professionally or with lucrative intent, he will be punished with a prison sentence of between three and twelve years.

4 - The penalties provided for in the previous numbers will be increased by one third, in their minimum and maximum limits, if the conduct referred to therein:

(a) Has endangered the life of the victim;

b) Has been committed with particular violence or has caused particularly serious harm to the victim;

(c) committed by an official in the performance of his/her duties;

(d) was committed within the framework of a criminal association; or

(e) resulted in the suicide of the victim.

5 - Whoever, for payment or other consideration, offers, delivers, solicits or accepts a minor, or obtains or consents to the adoption of a minor, is punished with a prison sentence of between one and five years.

6 - Whoever, having knowledge of the commission of a crime under paragraphs 1 and 2, uses the services or organs of a victim, is punished with a prison sentence of one to five years, if a more serious penalty is not applicable under any other legal provision.

7 - Whoever withholds, conceals, damages or destroys identification or travel documents of a person who is a victim of a crime as provided in paragraphs 1 and 2, shall be punished by a maximum imprisonment of three years, if a heavier penalty is not applicable under any other legal provision.

8 - The consent of the victim of the crimes under the previous numbers shall in no case exclude the illegality of the fact.

The provision of paragraph 1(b) of the criminal typification allows for the framing of phenomena of misinformation and deception being consumed in the evaluation of the conduct.

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.

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

Please provide details on known issues of application.

The signaling, evaluation, and punishment of serious delinquent behavior by minors is provided for in a special regime:

TUTELARY EDUCATION LAW

Article 1

Scope of the law

The practice, by a minor between the ages of 12 and 16, of an act qualified by law as a crime shall give rise to the application of a tutel educational measure in accordance with the provisions of this law.

Article 2

Purpose of the measures

1 - The educational guardianship measures, hereafter abbreviated as guardianship measures, aim at educating minors to the law and their insertion, in a dignified and responsible manner, in community life.

2 - The causes that exclude or diminish illicitness or guilt shall be considered for the assessment of the need and the type of the measure.

Article 6

Criteria for choosing the measures

1 - When choosing the applicable guardianship measure, the court will give preference, among the ones that are adequate and sufficient, to the measure that represents less intervention in the minor's autonomy of decision and life conduction, and that is likely to obtain his/ her greater adhesion and the adhesion of his/ her parents, legal representative or de facto guardian.

2 - The provisions of the previous number are correspondingly applicable to the establishment of the modality or the regime of execution of the guardianship measure.

3 - The choice of the applicable guardianship measure is guided by the interests of the minor.

4 - When the minor is considered to be the author of a plurality of facts qualified as crime, the court shall apply one or more guardianship measures, according to the concrete need for education of the minor regarding the law.

Article 28

Competence

1 - The family and minor sections of the central instance of the district court are responsible for:

a) Perform the jurisdictional acts related to educational guardianship inquiry;

b) Examine the facts qualified by law as crime, practiced by a minor between 12 and 16 years old, with the purpose of applying a tutelary measure

c) Execute and review tutelary measures;

d) Declare the termination or extinction of the tutelary measures;

e) Hear, under the terms foreseen in article 201, the appeal against decisions applying disciplinary measures to minors who have been interned.

2 - The competence of the family and juvenile sections of the central instance of the district court ceases when:

(a) an effective prison sentence is imposed, in criminal proceedings, for a crime committed by the minor between the ages of 16 and 18;

b) The minor turns 18 years old before the date of the decision in 1st instance.

3 - In the cases provided for in the previous number, the process will not be initiated or, if it has been initiated, it will be shelved.

Article 29

Sections of local instance

1 - Outside the areas covered by the jurisdiction of the family and juvenile courts, the criminal courts of local instance are responsible for hearing educational guardianship cases, by application, with the necessary adaptations, of the provisions of paragraph 5 of article 124, of Law no. 62/2013, of August 26.

2 - Without prejudice to the provisions of the previous number, in case of not occurring split, it is up to the sections of general jurisdiction of the local instance to know the tutelary educational processes, as provided in paragraph a) of paragraph 1 of Article 130, of Law No. 62/2013, of 26 August.

3 - In the cases provided for in the previous numbers, the court is constituted in family and minors section.

Article 30

Constitution

1 - The family and juvenile court works, as a rule, with only one judge.

2 - In the hearing where the application of a detention order is in question, the court is constituted by the judge of the case, who presides, and by two social judges.

Article 45

Minor's rights

1 - The minor's participation in any procedural steps, even if under detention or guardianship, is carried out in such a way that he/she feels free in his/her person and with the minimum of constraint.

2 - At any stage of the process, the minor has the special right to:

(a) to be heard, ex officio or when he requests it, by the judicial authority;

b) Not to answer questions asked by any entity about the facts that have been charged to him, or about the content of the statements he makes about them;

(c) Not to answer questions about his conduct, character or personality;

d) To be assisted by a psychiatric or psychology specialist whenever he/she requests it, for the purpose of assessing the need to apply a tutelary measure;

e) Be assisted by a legal counsel in all procedural acts in which they participate and, when detained, communicate, even privately, with him/her;

f) Be accompanied by their parents, legal representative or person having their de facto custody, except when there is a decision based on their interest or on the needs of the proceedings;

(g) To offer evidence and to request that any necessary steps be taken;

(h) To be informed of the rights to which he/she is entitled;

(i) appeal, under the terms of this law, against decisions that are unfavourable to them.

3 - The minor shall not under any circumstances take an oath.

4 - The rights referred to in sub-paragraphs f) and h) of paragraph 2 may be exercised on behalf of the minor by his parents, legal representative, de facto guardian or advocate.

Article 46

Public Defender

1 - The minor, his parents, legal representative or the person in his custody may appoint or request the appointment of a legal counsel at any stage of the proceedings.

2 - Having not been previously constituted or appointed, the judicial authority will provide for the appointment of the defense in the order in which it determines the hearing or the detention of the minor.

3 - The defender appointed ceases functions as soon as another one is constituted.

4 - The defender is a lawyer or, when this is not possible, a trainee lawyer.

5 - The appointment of a legal counsel should preferably be among lawyers with specialized training, according to a list to be prepared by the Bar Association.

Article 47

Hearing of the minor

1 - Hearing of the minor is always carried out by the judicial authority.

2 - The judicial authority may designate a social service technician or other specially qualified person to accompany the minor in the procedural act and, if applicable, provide the minor with the necessary psychological support by a specialized technician.

Article 71

Information and social report

1 - Information and a social report may be used as means of obtaining evidence.

2 - The information and the social report are intended to assist the judicial authority in knowing the personality of the minor, including his or her conduct and socio-economic, educational and family integration.

3 - The information is ordered by the judicial authority and may be requested from the social reintegration services or other public services or private entities, and must be presented within 15 days.

4 - The social report is ordered by the judicial authority and requested from the social rehabilitation services; it must be presented within 30 days. Its updating or complementary information may be requested and the technical experts who signed it may be heard, for clarification and without assistance.

5 - A social report with psychological evaluation is compulsory whenever an open or semi-open internment measure is to be applied.

Article 86

Modalities

The Public Prosecutor closes the inquiry, closing it or requesting the opening of the jurisdictional phase.

Article 87

Archiving

1 - The Public Prosecutor closes the inquiry as soon as it concludes

a) Inexistence of the fact;

b) Insufficient evidence of the commission of the fact

c) No need to apply a precautionary measure, if the fact is qualified as a crime punishable with a prison sentence of no more than three years.

2 - The Public Prosecutor's Office may also decide to close the investigation when, in the case of a fact qualified by law as a semi-public or private crime, the victim expresses opposition to its continuation, invoking particularly relevant grounds.

3 - The provisions of article 78(3) shall apply accordingly.

Article 89

Application to open the jurisdictional phase

Should the case proceed, the Public Prosecution Service requests the opening of the jurisdictional phase.

Ruling of the Coimbra Court of Appeal

I - The practice, by a minor between the ages of 12 and 16, of an act qualified by penal law as a crime, gives rise to the application of a tutelary educational measure, whenever at the time of delivering the decision, it is revealed to be necessary the state intervention aimed at his education for the law, with a view to the insertion, in a dignified and responsible way, in community life.

II - Through the practice of the aforementioned facts qualified by criminal law as a crime, particularly that of aggravated theft, whose degree of illegality is reflected in the (high) penalty that is abstractly applicable to him, allied to his previous deviant path, characterized by another conduct that also fits the crime of aggravated theft, and to the verified personal and socio-familiar context in which the incapacity of the parents to impose rules and limits on their son stands out, promoting changes in his behavior, which has fostered the repetition of antisocial conduct, without, on the other hand, the child revealing openness to intervention by the school and the protection system, with a view to achieving change at behavioral level, it is clear that the minor reveals a need for education for the law that demands the application of a tutelary educational measure, a need to which he has raised no objection in his appeal.

III - At the level of the criterion of choice of the measure to be applied, the law establishes that the court gives preference, among those that prove to be adequate and sufficient, to the measure that represents less intervention in the autonomy of decision and conduction of the minor's life and that is susceptible of obtaining his greatest adhesion and the adhesion of his parents, legal representative or person who has his de facto custody, the choice being guided by the minor's interest.

IV - In this context, preference should be given to the application of non-institutional measures.

V - The framework considered by the court, resulting from the proved facts, in conjugation with the elements provided by the technical evaluation carried out by the DGRSP, seen in the social report attached to the records and also taken to the list of matter verified, is clearly revealing that the institutional measure of internment in open regime is the only one that assures with adequacy and sufficiency the purposes of education of the minor for the right inherent to the educational tutelage intervention.

VI - The deviant path of the minor who, on xx-xx-xxxx, turns 16 years of age, together with the refined characteristics of his personality and the unstructured way of life he has been adopting, without rules or limits and in which the ineffectiveness of the family response, of the structures of protection and of the non-institutional tutelary educational intervention stand out, requires the adoption of a solution that provides an effective opportunity for change aimed at inverting a life trajectory translated into the unwanted practice of conducts that, at this stage, will already incur him in criminal responsibility.

VII - Solution that, in this case, will only be reached through the temporary removal from the environment that clearly reveals itself as an obstacle to the accomplishment of an educational intervention minimally adequate and effective, imposing, therefore, the needs of education for the right the application of an institutional measure.

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.

Please provide details on known issues of application.

There are no specific rules that frame cybercrime phenomena committed by minors, but only a CRIMINAL REGIME APPLICABLE TO DELINQUENT YOUNG PEOPLE, provided by Decree-Law No. 401/82, of September 23

Article 1

(Scope of application)

1 - The present law applies to young people who have committed an act qualified as a crime.

2 - For the purposes of this law, a juvenile is an agent who, on the date of commission of the crime, has reached the age of 16 without having yet reached the age of 21.

3 - The provisions of the present diploma are not applicable to young people who are criminally incapable by virtue of psychic anomaly.

Article 4

(Special mitigation regarding juveniles)

If a prison sentence is applicable, the judge shall specially mitigate the sentence in terms of articles 73 and 74 of the Penal Code, if he/she has serious reasons to believe that the mitigation will result in advantages for the social re-integration of the convicted juvenile.

Article 5

(Subsidiary application of legislation on minors)

1 - Whenever the case corresponds to a prison sentence of less than 2 years, the judge may, considering the personality and the circumstances of the fact, apply the measures outlined in article 18 of Decree-law no. 314/78, of 27th October, to a minor under the age of 18, individually or cumulatively.

2 - When the measures provided for in paragraphs i) to l) of article 18 of Decree-law no. 314/78, of 27 October are applied, the judge may, at the request of the young person and after hearing the management of the respective establishment, authorise them to remain there after they have turned 18 years of age, when there are unequivocal advantages for their training and education, and such permanence may not extend beyond the date on which the interested party turns 21 years of age.

Article 6

(Corrective measures)

1 - When the circumstances of the case and considering the personality of a juvenile over 18 years of age and under 21 years of age indicate that a prison sentence of up to 2 years is neither necessary nor convenient for his or her social reinsertion, the judge may impose corrective measures.

2 - For the purpose of the previous number, only the following are corrective measures:

a) Admonition

b) Imposition of certain obligations

c) fine

d) Internment in detention centers.

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.

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

Please provide details on known issues of application.

Portugal has transposed the substantive criminal law provision of Directive 2011/93 on Enticement of Minors for Sexual Purposes by considering only persons 18 years of age or older as perpetrators.

On the other hand, it considers and typifies as victims any persons under 18 years of age, even if above the age of sexual self-determination established in Portugal at 14 years of age.

The reason for the legal conformation has to do with the circumstance of providing a very distant and remote protection of the danger of effective violation of the sexual freedom and self-determination of minors.

Article 176-A

Enticement of minors for sexual purposes

1 - Whoever, being of age, by means of information and communication technologies, entices a minor to an encounter for the practice of any of the acts included in paragraphs 1 and 2 of article 171 and in paragraphs a), b) and c) of paragraph 1 of the previous article, is punished with a prison sentence of up to 1 year.

2 - If this inducement is followed by material acts leading to the encounter, the agent will be punished with a prison sentence of up to 2 years.

This is without prejudice to other more dangerous conducts obeying another framework, such as, for example, those foreseen in the following norms in which the perpetrator is only required to have the age of criminal responsibility of 16 years old:

Article 171

Sexual abuse of children

1 - Whoever commits an important sexual act with or on a person under 14 years of age, or causes him to commit such an act with another person, is punished with a prison sentence of between one and eight years.

2 - If the relevant sexual act consists of copulation, anal coitus, oral coitus or vaginal or anal introduction of body parts or objects, the agent shall be punished by imprisonment of three to ten years.

3 - Whoever:

(a) Harasses a minor under 14 years of age by performing an act provided for in Article 170; or

b) Acts upon a minor under 14 years of age by means of pornographic talk, writing, show or object;

c) Enticing a minor under 14 to witness sexual abuse or sexual activities;

is punished with a prison sentence of up to three years.

4 - Whoever commits the acts described in the previous number with the intent to profit is punished with a prison sentence of between six months and five years.

5 - Attempts are punishable.

Article 176

Pornography of minors

1 - Whoever:

(a) uses a minor in a pornographic show or entices him to do so;

b) Use a minor in pornographic photography, film or recording, regardless of its medium, or to entice him to do so;

c) Produce, distribute, import, export, disclose, exhibit, assign or make available in any way or by any means, the materials foreseen in the previous paragraph;

d) Acquire, possess or harbor the materials mentioned in paragraph b) with the purpose of distributing, importing, exporting, disseminating, exhibiting or assigning them;

will be punished with a prison sentence of one to five years.

2 - Whoever commits the acts described in the previous paragraph professionally or with lucrative intent is punished with a prison sentence of between one and eight years.

3 - Whoever commits the acts described in paragraphs a) and b) of no. 1 using violence or serious threat is punished with a prison sentence of between one and eight years.

4 - Whoever commits the acts described in paragraphs c) and d) of no. 1 using pornographic material with realistic representation of a minor is punished with a prison sentence of up to two years.

5 - Whoever intentionally acquires, holds, accesses, obtains or facilitates access through a computer system or any other means to the materials referred to in paragraph 1(b) will be punished by a maximum imprisonment of two years.

6 - Whoever, in person or through a computer system or by any other means, being of age, attends, facilitates or provides access to pornographic performances involving the participation of minors will be punished by a maximum imprisonment of 3 years.

7 - Whoever commits the acts described in paragraphs 5 and 6 with the intention of profit shall be punished by a maximum imprisonment of five years.

8 - For the purposes of this article, pornographic material is considered to be any material that, for sexual purposes, depicts minors engaged in real or simulated sexually explicit conduct, or contains any representation of their sexual organs or any other part of their body.

9 - Attempts are punishable.

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.

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

Please provide details on known issues of application.

In Portugal, it follows from the criminal law regime in force that any minor above the age of freedom and sexual self-determination set at 14 years of age can develop their sexual activity as long as they freely consent and are enlightened.

Any sexual behavior imposed on a minor under the age of 14; or a minor over the age of 14 without their free and informed consent will be typified as a crime by the types already provided for in the criminal regime that provides for an age of responsibility from 16 years old, with the exception of Enticement of minors for sexual purposes under the terms previously exposed.

The criminal liability of 16- to 21-year-olds is subject to special rules for evaluation.

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.

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

Please provide details on known issues of application.

The typification of the conduct associated with the phenomena mentioned is an open typification, allowing its integration by behaviors developed online.

The rules for the punishment of minors are the rules previously defined.

Article 154-A

Persecution

1 - Whoever repeatedly pursues or harasses another person, **by any means**, directly or indirectly, in a manner likely to cause him fear or uneasiness or to impair his freedom of determination, shall be punished by imprisonment for up to three years or a fine, if a more serious penalty is not applicable under any other legal provision.

2 - Attempts are punishable.

3 - In the cases provided for in no. 1, the defendant may be charged with the accessory penalties of prohibition of contact with the victim for a period of between 6 months and 3 years and the obligation to attend specific programmes for the prevention of behaviour typical of stalking.

4 - The accessory penalty of prohibition of contact with the victim must include removal from the victim's residence or place of work and its compliance must be monitored by technical means of remote control.

5 - The criminal procedure depends on a complaint.

Article 154

Coercion

1 - Whoever, **by means of violence or threat of great evil**, constrains another person to an action or omission, or to support an activity, is punished with a prison sentence of up to three years or with a fine.

2 - Attempt is punishable.

3 - The fact is not punishable

(a) if the use of the means to achieve the intended end is not objectionable; or

b) If it is aimed at avoiding suicide or the commission of a typical unlawful act.

4 - If the act takes place between spouses, ascendants and descendants, adopters and adopted persons, or between persons of the other or the same sex, who live in a situation analogous to that of the spouses, the criminal procedure depends on a complaint.

Question 9: 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.

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

Please provide details on known issues of application.

In Portugal, the conducts of deception and misinformation are not punishable autonomously, but only as part of a certain conduct provided for and punished under other types of crime as a means to achieve those results prohibited by law.

Question 10: 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).

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

Please provide details on known issues of application.

The typification of conduct that foresees the referred phenomenon is carried out in an open manner, allowing for the integration of online activities; on the other hand, no special characteristics are required of the perpetrator, namely in terms of age, with any person over the age of 16 being liable.

Article 160

Human Trafficking

1 - **Whoever** offers, delivers, recruits, entices, accepts, transports, harbors or receives a person for the purpose of exploitation, including sexual exploitation, labor exploitation, begging, slavery, organ extraction or the exploitation of other criminal activities

(a) By means of violence, abduction, or serious threat;

b) Through ruse or fraudulent maneuver;

c) With abuse of authority resulting from a relationship of hierarchical, economic, work, or family dependence;

d) By taking advantage of a psychic incapacity or a situation of special vulnerability of the victim; or

e) By obtaining the consent of the person in control of the victim;

shall be punished with a prison sentence of between three and ten years.

2 - The same penalty is applied to **whoever**, **by any means**, recruits, entices, transports, harbours or receives a minor, or delivers, offers or accepts him/her for the purposes of exploitation, including sexual exploitation, labour exploitation, begging, slavery, organ extraction, adoption or the exploitation of other criminal activities.

3 - In the case provided for in the previous number, if the perpetrator uses any of the means provided for in paragraph 1 or acts professionally or with lucrative intent, he will be punished with a prison sentence of between three and twelve years.

4 - The penalties provided in the previous numbers will be increased by one third, in their minimum and maximum limits, if the conduct referred to therein:

(a) Has endangered the life of the victim;

b) Has been committed with particular violence or has caused particularly serious harm to the victim;

(c) committed by an official in the performance of his/her duties;

(d) was committed within the framework of a criminal association; or

(e) resulted in suicide of the victim.

5 - **Whoever**, for payment or other consideration, offers, delivers, solicits or accepts a minor, or obtains or consents to the adoption of a minor, is punished with a prison sentence of between one and five years.

6 - Whoever, having knowledge of the commission of a crime under paragraphs 1 and 2, uses the services or organs of a victim, is punished with a prison sentence of one to five years, if a more serious penalty is not applicable under any other legal provision.

7 - Whoever withholds, conceals, damages or destroys identification or travel documents of a person who is a victim of a crime as provided in paragraphs 1 and 2, shall be punished by a maximum imprisonment of three years, if a heavier penalty is not applicable under any other legal provision.

8 - The consent of the victim of the crimes under the previous numbers shall in no case exclude the illegality of the fact.

Question 11: 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.

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

Please provide details on known issues of application.

Title III of Chapter III of Section II of the Intellectual Property Code - Decret of Law 110/2018 - defines a set of crimes against intellectual property whose formulation follows the general regime of the Penal Code, especially with regard to the age of criminal responsibility from 16 years old.

Likewise, in the cybercrime Law - Law 109/2019 - it is also typified in the general terms:

Article 8

Illegitimate reproduction of a protected programme

1 - Any person who illegitimately reproduces, discloses or communicates a legally protected computer program to the public shall be punished with a prison sentence of up to three years or with a fine.

2 - The same penalty shall apply to anyone who illegitimately reproduces a topography of a semiconductor product or commercially exploits or imports a topography or a semiconductor product manufactured from such a topography for these purposes.

3 - Attempt shall be punishable.

Question 12: 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.

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

Please provide details on known issues of application.

In Portugal, the transposition of the Budapest Cybercrime Convention was accomplished through Law 109/2009.

This law establishes a set of relevant definitions on what is understood by computer systems, as well as providing a set of provisions of substantive criminal law typifying conduct against the security, integrity and confidentiality of these systems.

Under the terms of the general criminal law, these types of offenses may be committed by minors over the age of 16.

Article 2

Definitions

For the purposes of this law

(a) "computer system" means any device or set of interconnected or associated devices, in which one or more of them develops, in execution of a program, the automated processing of computer data, as well as the network that supports the communication between them and the set of computer data stored, processed, retrieved or transmitted by that or those devices, with a view to its operation, use, protection and maintenance;

(b) "computer data" means any representation of facts, information or concepts in a form that can be processed in a computer system, including the programs suitable for causing a computer system to perform a function

Article 4

Damage to programs or other computer data

1 - **Whoever**, without legal permission or without being authorized by the owner or by another holder of the right to the system or part of it, erases, alters, destroys, in whole or in part, damages, suppresses or renders unusable or inaccessible programs or other computer data belonging to others, or in any way affects their usability, is punished with a prison sentence of up to 3 years or a fine.

2 - Attempt is punishable.

3 - The same penalty as in paragraph 1 applies **to anyone who** illegitimately produces, sells, distributes or in any other way disseminates or introduces into one or more computer systems devices, programs or other computer data intended to produce the unauthorised actions described in that paragraph.

4 - If the damage caused is of high value, the penalty is imprisonment for up to 5 years or a fine of up to 600 days.

5 - If the damage caused is of a considerably high value, the penalty is imprisonment for between 1 and 10 years.

6 - In the cases provided for in paragraphs 1, 2 and 4 the criminal procedure depends on a complaint.

Article 5

Computer sabotage

1 - **Whoever**, without legal permission or without being authorised by the owner or another person holding the right to the system or part of it, hinders, prevents, interrupts or seriously disturbs the functioning of a computer system by introducing, transmitting, deteriorating, damaging, altering, erasing, preventing access to or deleting programmes or other computer data, or by any other form of interference with a computer system, is punished with a prison sentence of up to five years or with a fine of up to 600 days.

2 - **Any person who** illegitimately produces, sells, distributes or in any other way disseminates or introduces into one or more computer systems, devices, programs or other computer data intended to produce the unauthorised actions described in the previous paragraph, shall also be punished.

3 - In the cases provided for in the previous number, the attempt is not punishable.

4 - The penalty is 1 to 5 years' imprisonment if the damage resulting from the disruption is of high value.

5 - The penalty is imprisonment for 1 to 10 years if

(a) the damage emerging from the disturbance is of a considerably high value;

b) the disruption caused seriously or lastingly affects an IT system that supports an activity aimed at ensuring critical social functions, namely supply chains, health, security and the economic well-being of people, or the regular functioning of public services.

Article 6

Illegitimate access

1 - **Whoever**, without legal permission or without being authorised by the owner or by another holder of the right to the system or part of it, in any way accesses a computer system, shall be punished by a prison sentence of up to one year or a fine of up to 120 days.

2 - **Any person who** illegitimately produces, sells, distributes or in any other way disseminates or introduces into one or more computer systems, devices, programmes, an executable set of instructions, a code or other computer data intended to produce the unauthorised actions described in the previous paragraph, shall also be punished.

3 - The penalty is imprisonment for up to two years or a fine of up to 240 days if the actions described in the preceding paragraph are intended for access to obtain data recorded, incorporated in or relating to a payment card or any other device, tangible or intangible, that allows access to a payment system or means of payment.

4 - The penalty is imprisonment for up to three years or a fine if:

(a) the access is achieved through violation of security rules; or

b) Through access, the agent obtains data recorded, incorporated in or concerning a payment card or any other device, tangible or intangible, that allows access to the payment system or means of payment.

5 - The penalty is imprisonment for one to five years when:

(a) through the access, the agent has gained knowledge of a commercial or industrial secret or confidential data, protected by law; or

b) The benefit or advantage obtained is of a considerably high value.

6 - Attempt is punishable, except in the cases provided for in paragraphs 2 and 3.

7 - In the cases provided for in paragraphs 1, 4 and 6 the criminal procedure depends on a complaint.

Question 13: 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:

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.

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

Please provide details on known issues of application.

Cybercrime Law No. 109/2009 establishes not only the legal types of direct damage to computer legal interests, but also accessory behaviors aimed at enhancing such criminal conduct, usually for profit.

Article 4

Damage to programs or other computer data

1 - Whoever, without legal permission or without being authorized by the owner or by another holder of the right to the system or part of it, erases, alters, destroys, in whole or in part, damages, suppresses or renders unusable or inaccessible programs or other computer data belonging to others, or in any way affects their usability, is punished with a prison sentence of up to 3 years or a fine.

2 - Attempt is punishable.

3 - **The same penalty as in paragraph 1 applies to anyone who illegitimately produces, sells, distributes or in any other way disseminates or introduces into one or more computer systems devices, programs or other computer data intended to produce the unauthorised actions described in that paragraph.**

4 - If the damage caused is of high value, the penalty is imprisonment for up to 5 years or a fine of up to 600 days.

5 - If the damage caused is of a considerably high value, the penalty is imprisonment for between 1 and 10 years.

6 - In the cases provided for in paragraphs 1, 2 and 4 the criminal procedure depends on a complaint.

Article 5

Computer sabotage

1 - Whoever, without legal permission or without being authorised by the owner or another person holding the right to the system or part of it, hinders, prevents, interrupts or seriously disturbs the

functioning of a computer system by introducing, transmitting, deteriorating, damaging, altering, erasing, preventing access to or deleting programmes or other computer data, or by any other form of interference with a computer system, is punished with a prison sentence of up to five years or with a fine of up to 600 days.

2 - **Any person who illegitimately produces, sells, distributes or in any other way disseminates or introduces into one or more computer systems, devices, programs or other computer data intended to produce the unauthorised actions described in the previous paragraph, shall also be punished.**

3 - In the cases provided for in the previous number, the attempt is not punishable.

4 - The penalty is 1 to 5 years' imprisonment if the damage resulting from the disruption is of high value.

5 - The penalty is imprisonment for 1 to 10 years if

(a) the damage emerging from the disturbance is of a considerably high value;

b) the disruption caused seriously or lastingly affects an IT system that supports an activity aimed at ensuring critical social functions, namely supply chains, health, security and the economic well-being of people, or the regular functioning of public services.

Article 6

Illegitimate access

1 - Whoever, without legal permission or without being authorised by the owner or by another holder of the right to the system or part of it, in any way accesses a computer system, shall be punished by a prison sentence of up to one year or a fine of up to 120 days.

2 - **Any person who illegitimately produces, sells, distributes or in any other way disseminates or introduces into one or more computer systems, devices, programmes, an executable set of instructions, a code or other computer data intended to produce the unauthorised actions described in the previous paragraph, shall also be punished.**

3 - The penalty is imprisonment for up to two years or a fine of up to 240 days if the actions described in the preceding paragraph are intended for access to obtain data recorded, incorporated in or relating to a payment card or any other device, tangible or intangible, that allows access to a payment system or means of payment.

4 - The penalty is imprisonment for up to three years or a fine if:

(a) the access is achieved through violation of security rules; or

b) Through access, the agent obtains data recorded, incorporated in or concerning a payment card or any other device, tangible or intangible, that allows access to the payment system or means of payment.

5 - The penalty is imprisonment for one to five years when:

(a) through the access, the agent has gained knowledge of a commercial or industrial secret or confidential data, protected by law; or

b) The benefit or advantage obtained is of a considerably high value.

6 - Attempt is punishable, except in the cases provided for in paragraphs 2 and 3.

7 - In the cases provided for in paragraphs 1, 4 and 6 the criminal procedure depends on a complaint.

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

Question 14: 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.

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

Please provide details on known issues of application.

Cybercrime Law No. 109/2009, when transposing the Budapest Convention, provided for the legal provision of international cooperation mechanisms.

At the same time, other European legislative instruments related to the protection of victims, European Investigation Order, European Investigation Order, Seizure and Recovery of Assets were also transposed, in order to consolidate the coherence of the Portuguese legal order with European legal orders.

Question 15: 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.

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

Please provide details on known issues of application.

Portugal proceeded to transpose all relevant international and European instruments in the matter, both those specifically relating to criminal phenomena and those relating to the production and collection of evidence.

Given the historical context, in addition to the instruments constituting the European acquis, some legislative instruments for cooperation in criminal matters concluded with Portuguese-speaking Countries are also highlighted.

These Instruments translate into special cooperation rules aimed at the production and obtaining of evidence, and are based on the usual rules and principles of international cooperation.

Question 16: 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.

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

Please provide details on known issues of application.

Law No. 88/2017, of August 21

EUROPEAN INVESTIGATION ORDER IN CRIMINAL MATTERS

Article 1

Object

This law establishes the legal regime for the issuance, transmission and recognition and enforcement of European investigation decisions, transposing into the domestic legal order Directive 2014/41/EU of the European Parliament and of the Council, of 3 April 2014, on the European Investigation Order (EIO) in criminal matters.

Article 2

Nature

1 - The EIO is a decision issued or validated by a judicial authority of a Member State of the European Union to carry out one or more specific investigative measures in another Member State, with a view to obtaining evidence in accordance with this law.

2 - The EIO is carried out on the basis of the principle of mutual recognition, under the terms of this law and in accordance with Directive 2014/41/EU of the European Parliament and of the Council, of 3 April 2014.

Cybercrime Law n.º 109/2009

Article 20

Scope of international cooperation

Competent national authorities cooperate with competent foreign authorities for the purposes of investigations or proceedings concerning crimes related to computer systems or data, as well as for the purpose of collecting electronic evidence of a crime, in accordance with the rules on transfer of personal data provided for in Law No. 59/2019, of 8 August.

Article 21

Permanent point of contact for international cooperation

1 - For the purposes of international cooperation, with a view to providing immediate assistance for the purposes referred to in the previous article, the Judiciary Police ensures the maintenance of a structure that guarantees a point of contact available at all times, twenty-four hours a day, seven days a week.

2 - This contact point may be contacted by other contact points, under the terms of agreements, treaties or conventions to which Portugal is bound, or in compliance with international cooperation protocols with judicial or police bodies.

3 - The immediate assistance provided by this permanent contact point includes:

a) The provision of technical advice to other contact points;

b) Expedited preservation of data in cases of urgency or danger in delay, in accordance with the provisions of the following article;

c) The collection of evidence for which it is competent in cases of urgency or danger in delay;

d) Locating suspects and providing information of a legal nature, in cases of urgency or danger in delay;

e) The immediate transmission to the Public Prosecutor's Office of requests relating to the measures referred to in paragraphs b) to d), outside the cases provided for therein, with a view to their rapid execution.

4 - Whenever acting under subparagraphs b) to d) of the previous number, the Judiciary Police immediately informs the Public Prosecutor of the fact and sends him the report provided for in article 253 of the Criminal Procedure Code.

5 - The Public Prosecutor's Office must, in order to respond promptly to requests for immediate assistance, ensure the availability of magistrates and technical means to carry out any urgent procedural interventions within its competence.

Question 17: 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.

Please provide details on known issues of application.

The rules and respective regimes above mentioned cover behaviors and phenomena related to minors from 12 years of age onwards.

They are naturally complemented with other preventive and pedagogical actions, with measures and institutions related to the safe internet centers programs being established and operational in Portugal.

5. Other

Question 18: 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.

Question 19: 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.