Deliverable Report

D4.5

Legal landscape for tackling cybercrime offenses by minors in Europe and beyond

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 882828. The sole responsibility for the content of this document lies with the author and in no way reflects the views of the European

Document Contributors

Deliverable No.	D4.5	Work Package No.	4	Task/s No.	T4.2
Work Package Title		Online Privacy, Data Security and Ethics			
Linked Task/s Title		Task 4.2. Legal landscape for tackling cybercrime offenses by minors in the EU and beyond			
Status		Final	(Draft/Draft Final/Final)		
Dissemination level		PU	(PU-Public, PP, RE-Restricted, CO-Confidential)		
Due date deliverable		30/09/2022	Submission date		30/09/2022
Deliverable version		V1.0			
Copyright information and disclaimer		The copyright is reserved by the authors. Reproduction in whole or in part of the current report or of the country reports is subject to express written permission by the respective authors. Please contact the authors of the current report or the RAYUELA project through the RAYUELA website for more information and in any case prior to any reproduction or re-use of the current report or the country reports. The information in the report and country reports is provided “as is” and not declared to be fit for any specific purpose.			
Deliverable responsible		Timelex			

Contributors	Organization	Reviewers	Organization
Siyanna Lilova	Timelex	Ben Heylen	UGent
Pieter Gryffroy	Timelex	Jelle Janssens	UGent
		Geert Somers	Timelex
		Ingrid Borarosova	BPI
		Viera Zuborova	BPI
		Violeta Vázquez	ZABALA
		Abel Muñiz	ZABALA
		Gregorio López	COMILLAS
		María Reneses	COMILLAS

Document History

Version	Date	Comment
0.1	08/08/2022	Table of contents and first draft
0.2	16/08/2022	First interim draft
0.3.	25/08/2022	Second interim draft
0.4	07/09/2022	First complete draft for submission to internal reviewers
1.0	23/09/2022	Final version after review

Table of contents

List of Abbreviations

Abbreviation	Description
ACM	Age of criminal majority
BC	Council of Europe Convention on Cybercrime, also known as Budapest Convention
CB	Cyberbullying
CRC	United Nations Convention on the Rights of the Child
EU	European Union
HT	Human trafficking
LC	Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse, also known as Lanzarote Convention
MACR	Minimum age of criminal responsibility
MD	Misinformation and Deception
OG	Online grooming
UK	United Kingdom
UN	United Nations
USA	United States of America

Executive Summary

This report provides an overview of the rules applicable to minor offenders, in particular in relation to the following behaviours:

- **Online grooming** (Section 2);
- **Online grooming for the purposes of human trafficking** (Section 3);
- **Cyberbullying** (Section 4);
- **Misinformation and Deception** (Section 5);
- **Online piracy**, e.g., online copyright offences (Section 6);
- **Hacking and the use or creation of Cybercrime as a Service** (Section 7).

Both **international and national perspectives** are presented, covering the following jurisdictions:

  - Belgium;
  - Bulgaria;
  - Czech Republic;
  - Estonia;
  - Germany;
  - Greece;
  - Latvia;
  - Portugal;
  - Romania;
  - Slovakia;
  - Spain;
  - The Netherlands;
  - Brazil;
  - China;
  - Mexico;
  - Russia;
  - South Africa;
  - The United Kingdom (UK);
  - The United States of America (USA).

The report also presents the **general juvenile justice systems** of all these countries and international perspectives on **criminal responsibility of minors** (Section 1).

The purpose of the study and this report is to provide **recommendations for the RAYUELA serious game**. Recommendations are presented in this report in light blue boxes, and all recommendations are grouped at the end of each section.

As it can be seen in the recommendation subsection of each section and in the conclusions, the general outcome of the study is that **criminal liability may indeed attach for minors who execute any of the abovementioned behaviours**. Sanctions (sometimes including custodial sentences), reformation and education measures, fines, civil liability and other consequences may apply depending on the specific circumstances and the severity of the behaviour in question. In some countries minors may at times

even be tried as adults and tackled with full force of the law, in particular when they are older adolescents.

The game should therefore aim to provide guidance, based on the recommendations provide in this report, to explain to the young players at what point certain behaviour crosses the line from innocent into potentially criminal behaviour and to reinforce the importance of staying on the right side of the dividing line.

Introduction

This deliverable on the legal landscape for tackling cybercrime offenses by minors in Europe and beyond was made part of RAYUELA's legal and ethical WP4 in order to complement the interviews and case studies in WP1 and to provide the game with some legal perspectives in terms of how cybercrime by minors is treated on the international level, as well as on the national level in various countries, including not only EU jurisdictions, but also a number of third countries.

The goal of this task is to inform the game design with some relevant insights that may help correctly frame the potential for criminal sanctions in the diverse scenario's that are envisioned in the game in relation to the crimes in focus in RAYUELA, namely online grooming (OG), Cyber Bullying (CB), grooming for human trafficking (HT) and misinformation and deception online (MD). While the game is focused in the first place on protecting young people from becoming the victim of online interactions, it will also aim to prevent minors from becoming perpetrators themselves. Hence, this study sought to explore how minors as perpetrators are dealt with in relation to the aforementioned crimes. Can they commit these crimes or related crimes and what are the sanctions that may apply? From what age can minors be responsible and is this full criminal responsibility or does as system of juvenile justice, focused on reformation apply? Are minors effectively prosecuted in practice? These are some of the questions that the study sought to answer in order to inform the scenarios in the game.

In addition to the aforementioned crimes in focus, two other offences were added to this report. First, online piracy, i.e., the online infraction of copyright of movies, pictures, music etc. through downloading and sharing of protected content without permission. This was added in particular because it may seem like a particularly low threshold offence, with no direct victim and little damage. Nonetheless, making copyright protected content available to the public may, without the minor realizing, make criminal liability attach. Even absent prosecution, serious consequences could still apply through a civil suit by the rightsholder or their representatives. Because of its potentially low threshold this potentially criminal behaviour was added to the study.

Second, the offences of hacking and creating/using Cybercrime as a Service were added. From an offender point of view, it is relevant to the game to realize that certain minors may possess significant interest and/or skills in IT and may be tempted to test these skills, misuse them or commit acts that may have serious consequences. Minors may be capable of serious criminal intent, but acts could also be committed as a joke or prank, as a result of peer pressure, to challenge themselves or out of curiosity, etc. Therefore, it is important to inform the game of the red lines as to when behaviour becomes a potential criminal offence.

Last but not least, the study also seeks to inform the game about the general approach to juvenile justice in the different countries and issues of civil liability of minors and parents in general, as this may also be relevant to give the scenarios further context.

In what follows, these topics are explored in depth:

- Section 1 provides general insights related to the interactions of minors with the criminal justice system;
- Section 2 deals with online grooming, both in general and from the perspective of minors offenders;
- Section 3 deals with online grooming for the purposes of human trafficking, both in general and from the perspective of minors offenders;
- Section 4 covers Cyberbullying, both in general and from the perspective of minors offenders;
- Section 5 addresses Misinformation and Deception, both in general and from the perspective of minors offenders;
- Section 6 covers online piracy by minors in particular; and
- Section 7 covers hacking and CaaS by minors in particular.

Every section presents not only the national perspectives, but also the international elements that are relevant to the topic at hand.

The intention of the study is to provide legal perspectives and insights, translated in recommendations. These recommendations are provided in light blue text boxes throughout the present report and grouped at the end of each section. The recommendations are by no means hard requirements for the game and are consequently not formulated as such. They are meant as suggestions for the game designers who can decide, with the feedback of the RAYUELA ethical experts and the whole consortium to implement them, if and where appropriate. The recommendations are intentionally formulated in a general way and will necessarily require further discussion within the consortium to implement them appropriately in the game scenarios.

Methodology and disclaimer

In order to write this report, the following methodology was followed:

- First, a questionnaire was drafted and consulted with the consortium to define some of the relevant topics and questions that needed to be addressed. The questionnaire can be found in Annex 1.
- Second, a number of countries in focus to get relevant legal perspectives from were selected in consultation with the consortium partners. The aim was to cover a reasonable geographic spread of countries, with diverse legal traditions and different backgrounds relating to cybercrime and the crimes and focus. Because RAYUELA is an EU-focused project and because the game will be focused on the EU as well, 12 EU countries were covered. In addition, to provide international perspectives 7 non-EU countries were covered as well. The countries that were chosen are:
    - Belgium;
    - Bulgaria;
    - Czech Republic;
    - Estonia;
    - Germany;
    - Greece;
    - Latvia;
    - Portugal;
    - Romania;
    - Slovakia;
    - Spain;
    - The Netherlands;
    - Brazil;
    - China;
    - Mexico;
    - Russia;
    - South Africa;
    - The United Kingdom (UK);
    - The United States of America (USA).
- After deciding on the countries in focusing, legal partner Timelex used its international network to find best value for money national experts on the topic to act as respondents and fill out the questionnaire. Respondents all have appropriate legal knowledge and are either cybercrime practitioners, lawyers or from academia, or a mix of profiles. The full text questionnaires containing the answers of the national respondents will be published on the Timelex (www.timelex.eu) or RAYUELA website (https://www.rayuela-h2020.eu/) , or both.
- After receiving a questionnaire, a follow-up interview was planned with the respondent to make sure that all answers were understood correctly and to ask additional questions or

clarifications. At times this led to questionnaires being adapted and completed further. The version that will be published is the final adapted version.

- For Greece and Portugal, it was decided to duplicate the questionnaires by having both a more practice-oriented and a more academia-oriented profile answer the questionnaire, in an effort to unearth different perspectives and angles relating to the same jurisdiction, which provided insights relating to specific follow-up questions to be asked in all interviews (in as far as not already answered in the questionnaire). This means that there are in fact 21 country reports (19 countries, but 1 extra report each for Greece and Portugal).
- Finally, all answers were processed and completed where necessary with desktop research to produce this report.

It is important to understand that while additional desktop research was performed, the Timelex team did not consistently check the answers provided by the national legal experts. Equally, there is no guarantee that questionnaires answer the questions exhaustively. In fact, given the sometimes broad topics such as cyber bullying and misinformation and deception, it may be assumed that reports often do not exhaustively cover all potential criminal law qualifications that could apply in the variety of scenarios that may be covered under these broad terms. This is acknowledged in the sections below as well, but nonetheless allows to describe relevant trends, issues and findings.

The reader should note that the information provided in the national country reports and in this report is provided "as is" and without any claims of being accurate, complete or fit for the purposes of the reader.

1. Minors and the criminal justice system

1.1. Minimum age of criminal responsibility

1.1.1. International standards

Under a certain age, children are considered to lack the emotional and intellectual maturity to understand the meaning of their actions and thus to be held criminally responsible. The minimum age of criminal responsibility (MACR) introduces an irrefutable presumption that children below that age cannot be held responsible in a penal law procedure. A MACR exists in nearly all countries throughout the world and is encouraged by Article 40(3) of the **United Nations Convention on the Rights of the Child** (CRC).[1] Determining the age under which minors are not mature enough to be penalised, however, is a controversial topic, heavily influenced by culture and history. Accordingly, the CRC does not introduce a universal international standard regarding the minimum age of criminal responsibility.

Some guidance can be found in Rule 4 of the Beijing Rules which recommends that the beginning of MACR is not fixed at too low an age level, bearing in mind the facts of emotional, mental and intellectual maturity.[2] This rule, however, still remains too broad and open to interpretation. A specific recommendation about the minimum age of criminal responsibility can be found in General Comment No. 10 to the CRC, in which the Committee on the Rights of the Child concludes that a MACR below the age of 12 years is considered 'not to be internationally acceptable'.[3] In addition, the Committee stresses that States should not lower their age of criminal responsibility to 12 where it has already been set higher and strongly encourages States to introduce a higher MACR, preferably 14 or 16 years of age. There are no restrictions of course in raising the minimum age up to 18 years of age and some countries, such as **Brazil,**[4] have taken advantage of that possibility.

[1] All eligible nation states are parties to the CRC, save for the USA which is only a signatory. See UN Treaty Collection, Status of Treaties, Convention on the Rights of the Child. Available at: https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-11&chapter=4&clang=_en (last accessed 09/08/2022).
[2] UN Standard Minimum Rules for the Administration of Juvenile Justice ('The Beijing Rules'), adopted by General Assembly resolution 40/33 of 29 November 1985, Rule 4.
[3] UN Committee on the Rights of the Child, CRC General Comment No. 10 (2007): Children's Rights in Juvenile Justice, 25 April 2007, CRC/C/GC/10, p. 11, para 32.
[4] Minors in Brazil under the age of 18, however, can commit 'acts of infraction' even though they are not criminally liable. See Section 1.1.2.

Overall, the mere encouragement of the CRC and the lack of clear international standards in this regard have led to diverging range of MACR throughout the world. Minimum ages range from a very low level of age 7 or 8 to the commendable high level of age 14 or 16 (see *Figure 1*). The age of 14 is the most common MACR internationally. The **USA**, on the other hand, remain an outlier by not having minimum age of criminal responsibility on a federal level. Different minimum age thresholds are introduced in some states but in 27 of them there is still no MACR specified.[5] An additional factor complicating the international framework is the fact that quite a few countries use two minimum ages of criminal responsibility. In these cases, children in conflict with the law who at the time of the commission of the crime are at or above the lower minimum age but below the higher minimum age are assumed to be criminally responsible only if they have the required maturity in that regard. The assessment of this maturity is left to the court, with or without a requirement of involving a psychological expert.[6] Given this varying international landscape, efforts to agree on a reasonable lowest age limit to be applicable internationally are recommended.

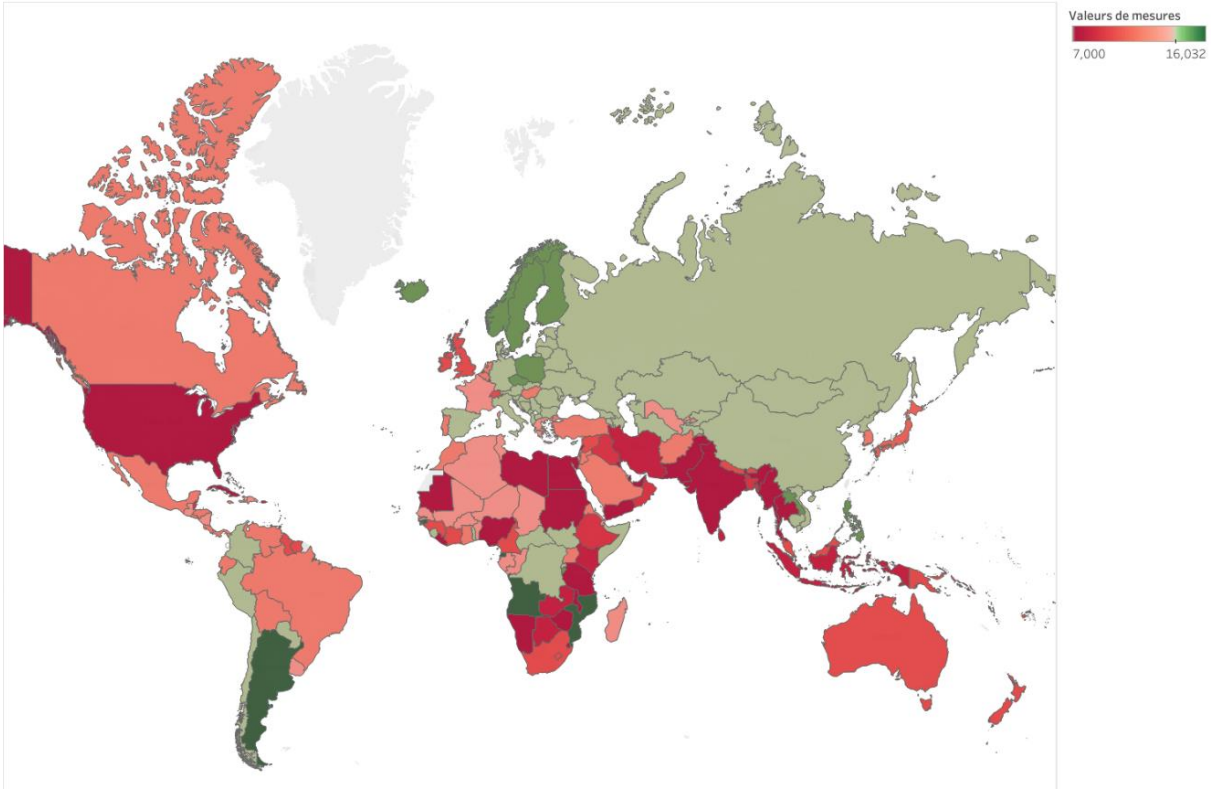

Figure 1: Minimum age of criminal responibility. Source: Child Rights International Network.[7]

[5] National Governonrs Assosiaction, Age of Boundaries in Juvenile Justice Systems (2021). Online. Available at: https://www.nga.org/wp-content/uploads/2021/08/Raise-the-Age-Brief_5Aug2021.pdf (last accessed on 10/08/2022). For an interactive map, although not as up to date, see Juvenile Justice Geography, Policy, Practice & Statistics. Online. Available at: http://www.jjgps.org/jurisdictional-boundaries#delinquency-age-boundaries?year=2018&ageGroup=1 (last accessed on 10/08/2022).

[6] UN Committee on the Rights of the Child, CRC General Comment No. 10 (2007): Children's Rights in Juvenile Justice, 25 April 2007, CRC/C/GC/10, p. 10, para 30.

[7] Child Rights International Network (CRIN), The minimum age of criminal responsibility, Interactive map. Available at: https://home.crin.org/issues/deprivation-of-liberty/minimum-age-of-criminal-responsibility (last

1.1.2. MACR in the interviewed countries

The lack of international uniformity in terms of the minimum age of criminal responsibility can be observed in the interviewed countries as well (see *Figure 2*). In Europe, the most common MACR is 14.

A typical example is **Latvia** where a person who has not attained fourteen years of age, may not be held criminally liable. If a child has reached the age of 14, a forensic psychiatric and psychological examination takes place to determine whether the minor was able to fully understand or manage his or her activities at the time of the commission of the offense.[8] Many European countries have opted to introduce two minimum ages of responsibility. In **Romania**, for example, there is an absolute presumption of lack of discernment i.e., the ability to discern, understand and appreciate things at their fair value, for minors under the age of 14, and a relative presumption of lack of discernment regarding minors between the ages of 14 and 16, which may be overturned by evidence. Commendable examples of countries going beyond the average age of MACR in Europe (14) are **Portugal** (16) and the **Czech Republic** (15). On the contrary, the **United Kingdom** stands out with the lowest age of criminal responsibility in Europe (10).

The Child Justice Act in **South Africa**[9] also provides that children up to 10 years of age lack criminal capacity. A dual system of MACR kicks in for children between 10 and 14 years of age who are considered to have criminal capacity, but onus rests on the State to prove beyond reasonable doubt that the child had such capacity when committing the crime. Minors older than 14 years are considered to have reached the age of criminal majority in South Africa (see Section 1.1.3). In **China**, a person who has reached the age of 16 and commits a crime bears criminal responsibility for all crimes, while minors between 14 and 16 are responsible only for certain serious crimes. Exceptionally, 12-year-olds can also be criminally liable when they commit intentional homicide or intentional injury, causing death or serious injury by particularly cruel means.[10]

At first glance, **Brazil** seems to have gone in the opposite direction and introduced the most generous regime in terms of minimum age of criminal responsibility. According to Art. 228 of the Brazilian Federal Constitution, all minors under 18 years old are not criminally liable, regardless of whether they are emancipated under civil law. Nonetheless, children under 12 and adolescents between 12 and 18 years of age can commit 'acts of infraction'. These acts are regulated under a special Statute of Children and Adolescents which establishes that for acts of infraction committed by children, protective measures are applied, while for those committed by adolescents, social-educational measures are applied.[11] Even though minors don't have criminal responsibility in Brazil, the regime of social-educational measures for 'acts of infraction' closely resembles the regime of criminal sanctions usually applicable to minors in other countries (see Section 1.3). Therefore, Brazil's legislation taken as a whole, resembles regimes where the MACR is 12 years, despite the prohibition of criminal liability for under-18-year-olds in the Constitution.

accessed on 10/08/2022). Please note that the map is not updated regularly and some discrepancies might exist between the image and the current regulatory landscape.

[8] Section 11 of Criminal Law of Latvia.

[9] The Child Justice Act, 2008 (Act 75 of 2008).

[10] Article 17 of the Criminal Law of the People's Republic of China.

[11] See Article 101 and Article 112 of Estatuto da Criança e Adolescente (Federal Law No. 8,069 of 1990).

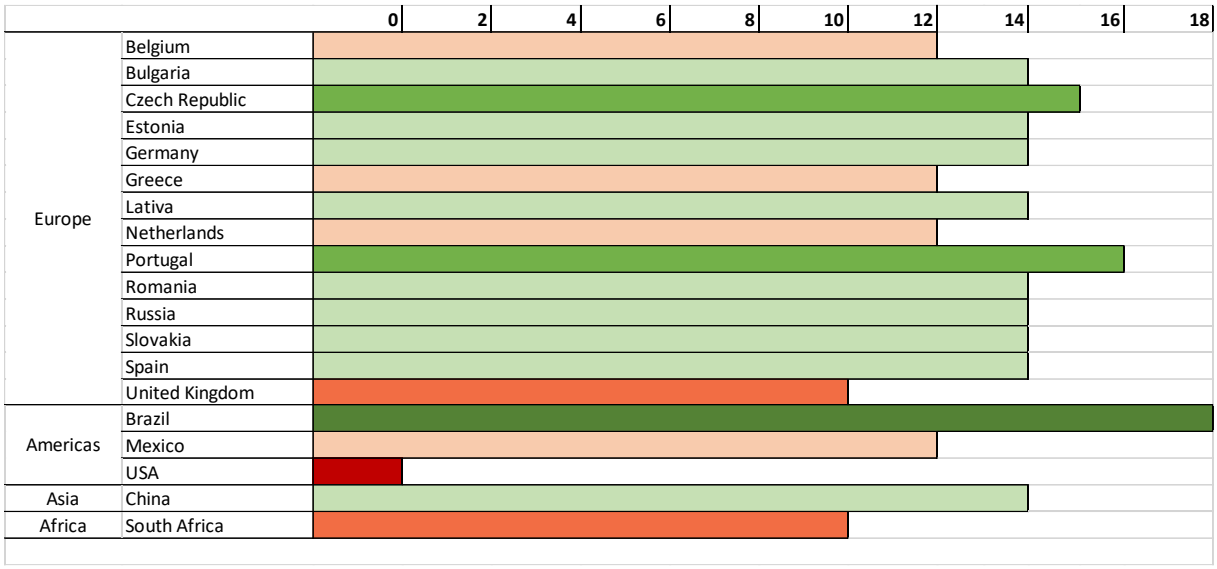

Figure 2: Minimum age of criminal responibility in RAYUELA interviewed countries.

The biggest outlier of all interviewed countries is the **USA** – it is the only country that hasn't ratified the CRC and that doesn't have a MACR neither on a federal level, nor in most individual states. In 15 of the 23 states with MACR, that age is 10 and only in 3 it becomes as high as 12 years.[12] Hence, even the states that do have a minimum age of criminal responsibility do not meet the internationally acceptable standard of 12 years recommended by the Committee on the Rights of the Child. What's more, most states allow for discretionary prosecution of minors in adult criminal courts which further diminishes the protection offered to minors in conflict with the law (see Section 1.1.3).

1.1.3. Age of criminal majority

The other relevant age for the rights and treatment of minors in the criminal justice system is the upper age limit for juvenile justice, or the age of criminal majority (ACM). ACM is the age at which a person is considered fully criminally liable and is no longer subject to the youth justice provisions but is rather automatically held accountable under the adult criminal justice system. Unlike with MACR, regarding ACM there is an international consensus that the appropriate age is 18 years. This is universally the case in all interviewed European countries. In **South Africa**, for example, where all minors above the age of 14 are considered criminally capable, the ACM is also 18 years because until that age all minors are subject to the additional protections under the Child Justice Act. In **China** too, even though anyone above the age of 16 bears criminal responsibility, the safeguards under the Chinese Law on the Protection of Minors apply to everyone under the age of 18.

In many countries, however, there are certain measures can effectively lower the ACM. Some countries allow minors' cases to be transferred to adult courts because a crime is considered 'too serious' to be dealt with in the juvenile justice system. For example, in the **Netherlands** and **Belgium** minors can be transferred to adult courts from the age of 16. This, however, is the exception and can happen only regards to very serious crimes and if the circumstances of the case and the perpetrator warrant

[12] Ibid 5.

prosecution under adult criminal law.[13] In both countries, the decision to transfer a minor to the criminal justice system is at the discretion of the youth judge, except in the case of traffic offences in Belgium, where the transfer takes place automatically.[14]

The juvenile court judge has the discretion to transfer the prosecution of minors to adult criminal court also in 46 states in the **USA**.[15] In these situations, the US respondent notes that the case proceeds as any criminal case would, with the exception that a juvenile under 18 transferred to adult status may never be housed with adults, either pre-trial or to serve a sentence. Worryingly, in 2018 there were 22 States that had at least one provision for transferring minors to criminal court for which no minimum age was specified. Even in the States that do specify a minimum transfer age, it is usually as low as age 14.[16] Research from the USA suggests that transferring children to adult courts results in high rates of pre-trial detention, more severe sentences, placement of children in adult facilities and overall, has led to increased rates of recidivism.[17] This is a central reason why the Committee on the Rights of the Child recommends that those countries which limit the applicability of their juvenile justice rules to children under the age of 16 (or lower) years, or which allow by way of exception that 16 or 17-year-old children are treated as adult criminals, change their laws with a view to achieving a non-discriminatory full application of their juvenile justice rules to all persons under the age of 18 years.[18]

In the other hand, some countries lead by a positive example in effectively extending the age of criminal majority above 18 by treating people aged between 18 and 21 differently from adults. This is usually done in particular with relation to the sentences they receive and the type of detention facilities to which they are sent. In **Germany**, there are rules for the opposite transfer, e.g., offenders who are over 18 but under 21 can be transferred from adult to youth courts. A differentiated regime which extends some of the benefits of juvenile justice to young adults can be found in **Portugal** (21), **Estonia** (21) and the **Netherlands** (23).

1.1.4. Relevance of point in time to determine responsibility

The relevant point in time to determine if the offender has reached either the minimum age of criminal responsibility or the age of criminal majority, is generally the moment the criminal act was committed. This is universally the case in all interviewed countries. The moment in time is relevant because if a child commits an otherwise criminal offence before they have reached the respective MACR, they will not be prosecuted and instead only protective measures could apply. When a minor commits a criminally prosecuted act between the MACR and ACM, the state may impose not only protective, but also different socio-educational or therapeutic measures, as well as more invasive criminal sanctions. As a rule, the opportunity to apply such protective and educational measures ceases when the minor

[13] See art. 77b Dutch Criminal Code.
[14] Leenknecht, J., Put, J. and Veeckmans, K. (2020) Age Limits in Youth Justice: A Comparative and Conceptual Analysis, Erasmus Law Review, 1 , pp. 13-30.
[15] Juvenile Justice Geography, Policy, Practice & Statistics. Online. Available at: http://www.jjgps.org/jurisdictional-boundaries#delinquency-age-boundaries?year=2018&ageGroup=1 (last accessed on 10/08/2022).
[16] See https://www.juvenilecompact.org/age-matrix.
[17] Bishop, D. (2000) Juvenile Offenders in the Adult Criminal Justice System, Crime and Justice, 27, pp.81–168.
[18] UN Committee on the Rights of the Child, CRC General Comment No. 10 (2007): Children's Rights in Juvenile Justice, 25 April 2007, CRC/C/GC/10, p. 12, para 38.

reaches the ACM. Then only the normal sanctions under the respective criminal system apply (see Section 1.3.2).

Recommendation for the game: The game should, if possible, inform children about the applicable minimum age of criminal responsibility and highlight that being a minor does not entail that you cannot be criminally prosecuted and sanctioned.

1.2. Special treatment of minors in the criminal justice system

1.2.1. General principles

The CRC requires all States parties to develop a comprehensive juvenile justice policy which implements not only the specific provisions related to the administration of juvenile justice in articles 37 and 40 of CRC, but also takes into account the general principles enshrined in articles 2, 3, 6 and 12 of CRC.[19] Most of these general principles reflect the fundamental human rights in the International Covenant on Civil and Political Rights (ICCPR) but some deserve to be highlighted with respect to their significance to the treatment of minors in the criminal justice system.

Article 3 CRC is of particular importance as it sets out that the best interests of the child should be a primary consideration in the he administration of juvenile justice. The UN Committee on the Rights of the Child clarifies that, pursuant to this principle, the traditional objectives of criminal justice, such as repression/retribution, must give way to rehabilitation and restorative justice objectives in dealing with child offenders.[20] The Beijing Rules also reiterate in Rule 5 that the main objective of the juvenile justice system is to promote the well-being of the minor. All forms of violence in the treatment of children in conflict with the law are therefore be prohibited and must be prevented. Additionally, according to Article 40(1) of CRC, treatment in the juvenile justice should promote the child's reintegration and assuming of a constructive role in society, and should develop in the child respect for human rights and freedoms. In order to avoid harm being caused to minors by undue publicity or labelling, Rule 8 of the Beijing Rules proclaims the principle of protection of children's privacy in all stages of the criminal procedure. This principle prohibits the publication of any information that may lead to the identification of a juvenile.

In line with these international standards, most of the interviewed countries have also developed their juvenile justice systems by focusing on the rehabilitation, protection, and education of minors. Some countries have comprehensive laws that regulate their juvenile justice system (e.g., **Czech Republic,**[21] **Spain,**[22] **Germany,**[23] **Mexico,**[24] **South Africa**[25]), while others have included special norms for the treatment of minors in their general penal legislation (e.g., **Bulgaria**, **Greece**, **Slovakia**). Usually, these

[19] Ibid, para 4.
[20] Ibid, para 10.
[21] Act No. 218/2003 Coll. on Liability of Youth for Unlawful Acts and on Juvenile Justice (Juvenile Justice Act)
[22] Organic Law on the Criminal Responsibility of Minors.
[23] Juvenile Court Act (Jugendgerichtsgesetz, JGG).
[24] National Law of the Comprehensive Criminal Justice System for Adolescents.
[25] Child Justice Act 75 of 2008.

special laws or norms proclaim that their objective is not the punishment, but the rehabilitation and treatment of juvenile offenders in order to achieve their social reintegration.[26] **Bulgaria** succinctly states that the objective of juvenile justice is to "re-educate minors and prepare them for socially useful work".[27] Noteworthy in this respect are efforts in **Estonia** to speed up the investigation of juvenile delinquency, which aims to ensure that the objectives of juvenile justice are achieved in practice. The idea is that if a juvenile offender spends less time as a suspect, they can more quickly rectify and learn from their actions.[28] So far, the **Russian Federation** has been the only country where respondents indicated that no specific rules on the special treatment of minors in the criminal system exist, apart from norms regarding the determination of criminal sanctions.

1.2.2. Investigation and prosecution

Part two of the Beijing Rules includes specific guidance on the rules that should be applicable in investigation and prosecution of minors. In line with the general principles, their main focus is on respecting the legal status of the juvenile, promoting their well-being and avoiding harm. The juvenile's parents or legal guardians should be immediately notified upon apprehension (Rule 10), while any detention pending trial should be used only as a measure of last resort and for the shortest possible period of time (Rule 13). Essential is Rule 11 on diversion, according to which cases should be dealt with, whenever appropriate, without resorting to formal trial. To achieve this, the police and prosecution dealing with juvenile cases are usually empowered to dispose of such cases at their discretion. The Beijing Rules also advise that these organs be specially instructed and trained to deal with juveniles (Rule 12).

Most of the interviewed countries have implemented all of the abovementioned rules on juvenile investigation and prosecution. They often have either specialized organs dealing with juveniles or organise professional trainings in the field. **Mexico**, for example, has a public prosecutor specialized in justice for adolescents with specific mandate for crimes committed by teenagers and juveniles.[29] In **China** public security organs and people's procuratorates are obliged to take care of the physical and mental characteristics of juveniles and may set up special agencies or designate professional handling.[30] In **Portugal,** the policy is to involve the police as little as possible, hence investigations are conducted directly by the prosecutor, rather than the police under their instructions.

Due to the principle of diversion in the prosecution of minors, the interviewed countries report that many cases of juvenile crime don't reach trial (which explains the limited data on cybercrime committed by minors in Section 1.6). Prosecutors usually have the discretion whether to continue investigation or to drop the case. In **Bulgaria** for example, the prosecutor may decide to abstain from instigating pre-trial proceedings or to terminate the instigated proceedings. In such cases educational measures are imposed instead.[31] Similar provisions can be found for instance in **Estonia**, **Germany,** and

[26] Chapter 8 of the General part of the Greek Criminal Code.
[27] Article 60 of the Bulgarian Penal Code.
[28] In 2018 the Estonian government repealed the Juvenile Sanctions Act which led to the abolition of the Juvenile Commission as an intermediate step in the proceedings in order to speeded up the criminal process.
[29] Article 66 of the National Law of the Comprehensive Criminal Justice System for Adolescents.
[30] Article 40 of the Law of the People's Republic of China on the Protection of Minors.
[31] Article 61 of the Bulgarian Penal Code.

South Africa. In this respect, it is interesting to note that the **Dutch** criminal procedure applies the opportunity principle, i.e., the public prosecutor decides whether or not to prosecute in all cases, regardless of whether they pertain to juvenile crime. As a result, particularly where it concerns relatively light instances of cybercrimes committed by minors, it is uncommon for juveniles to be prosecuted in practice. The Dutch respondent, however, noted that if the crime has serious consequences, such as causing substantial damage or societal uproar, minors are more likely to be prosecuted for the general prevention purpose of showing other minors that such behaviour is illegal.

Recommendation for the game: The game should, if possible, make it clear that minors can be prosecuted for cybercrimes, even though preferential treatment would be applicable. This is especially true for more serious crimes where state organs could decide to prosecute a minor in order to dissuade other juveniles from this behaviour.

1.2.3. Court proceedings

Article 40(2) of CRC contains an important list of rights and guarantees that are meant to ensure minors in conflict with the law receive fair treatment and trial. As most of these guarantees are universal and overlap with Article 14 of ICCPR, this section will focus on the principles specific for the juvenile justice system. The CRC sets out that the minor's parents or legal guardians should be informed about the raised charges, while according to Rule 15 of the Beijing Rules, the parents or the guardian are entitled to participate in the proceedings. These legal instruments also set out that children have the right to legal assistance, including the right to apply for free legal aid, in the preparation and presentation of their defence. According to international standards, it is especially important that cases are handled expeditiously, without unnecessary delay, and with consideration of the age and situation of the minor and their parents/legal guardians.[32] The Beijing Rules add in specific that proceedings should be conducive to the best interests of the juvenile and be held in an atmosphere of understanding (Rule 15). In addition, Rule 17.4 sets out that judges should have the power to discontinue the proceedings at any time. Another specificity of juvenile justice is that due to the principle of full respect of children privacy, hearings are normally behind closed doors and records of juvenile offenders are kept strictly confidential and closed to third parties.

While the above safeguards have been implemented in different ways and to various extents, they can all be found in the national legislation of most interviewed countries. The countries that don't have a juvenile court - **Bulgaria, Brazil, China, Estonia, Latvia,** the **Russian Federation, Slovakia**, usually have in place a special procedure for juvenile cases and organise trainings for judges. The majority of interviewed countries, however, have set up special tribunals due to the significant difference in treatment of juveniles**: Belgium, Czech Republic, Germany, Greece, Mexico, Portugal, Romania, Spain, South Africa, The Netherlands,** the **United Kingdom,** and the **USA**. In the **UK**, for example, minors between the age of 10-18 are tried in Youth Courts where proceedings less formal, with defendants addressed by their first name. The public cannot attend Youth Courts and if the victim wants to observe, they must specially request this with the court. If the accused are 16 or under, their parents, guardians or carers must attend court.

[32] Article 40(2)(iii) of CRC, Rules 16 and 20 of Beijing Rules;

In the **USA** the Juvenile Justice and Delinquency Prevention Act creates a unique federal procedure for delinquency proceedings against juveniles -- a process with quasi-criminal and quasi-civil nature which seeks to take account not only of the special protections provided to minors but also of the fact that even persons under 18 can commit "adult" crimes.[33] The juvenile proceeding is different from a criminal prosecution as they determine whether the minor is a "juvenile delinquent" not whether he or she is guilty of committing a crime (i.e. it does not result in a criminal conviction). It is specifically designed to lessen the amount of stigma that attaches to the act of delinquency compared to a criminal conviction, and to emphasize the rehabilitation, rather than punishment.[34]

The **Czech Republic** is another interesting case with respect to juvenile justice. When a child under the age of 15 (the MACR) commits an act with the characteristics of a criminal offence, this is considered an '*act otherwise punishable'*. The Juvenile Justice Act regulates special proceedings in these cases, which are not criminal but a special type of civil uncontested proceedings. The difference in the nature of the proceedings, however, brings its own problems due to the lack of safeguards normally mandated in criminal juvenile justice. Some of the issues flagged by the Czech respondent include suppression of the principle of restorative justice in proceedings involving children under 15; lack of the institution of the necessary defence (i.e, children are not automatically entitled to legal aid); not enough restrictions regarding the admissibility of evidence in court hearings. This leads to the peculiar situation where children under MACR are not criminally liable but at the same time are deprived from many of the guarantees for juvenile justice during trial. Given the universality of the CRC and the Beijing Rules, it is paramount that all children receive the same protection when being accused of committing a criminal offence.

1.3. Sanctioning minors and young people in the criminal justice system

1.3.1. International standard

After a fair and just trial in full compliance with Article 40 of CRC, a decision is made regarding the measures which should be imposed on a minor who is found guilty. When it comes to determining the appropriate sanction, the principle of proportionality should be takin into account (Rule 5 of the Beijing Rules). This principle is an instrument for curbing punitive sanctions and is expressed by taking into consideration not only of the gravity of the offence but also the personal circumstances of the young offender.

In this respect, Article 40(4) of CRC provides that national courts should be able to choose from a variety of dispositions, such as care, guidance and supervision orders; counselling; probation; foster care; education and vocational training programmes and other alternatives to institutional care. Such measures aim to assure that deprivation of liberty is used only as a measure of last resort and for the shortest possible period of time (Article 37(b) of CRC). The CRC also prohibits the sanctioning of minors with the death penalty and imprisonment without parole. In exception cases where children are deprived of liberty, they should be separated from adults and be able to maintain contact with their

[33] https://ipmall.law.unh.edu/sites/default/files/hosted_resources/CyberCrime/usamay2001_7.pdf
[34] Ibid. See also United States v. Hill, 538 F.2d 1072, 1074 (4th Cir. 1976)

family.[35] Additional guarantees for the rights of children in such cases are set out in the UN Rules for the Protection of Juveniles Deprived of their Liberty (the "Havana Rules").

1.3.2. Measures applicable to minors below MACR

No criminal sanctions can be imposed to minors below MACR. Nonetheless, most countries envision the applicability of a set of child protection (and sometimes educational) measures in cases where minors commit acts that would otherwise be treated as criminal offences. In the **UK**, children under 10 can be given local child curfews (ban for children to be in public places between 9pm and 6 am, unless accompanied by an adult). If they break the curfew, they can be given a Child Safety Order which places them under the supervision of a youth offending team.[36] Often measures are directed toward the parents, rather than the children themselves. In **Spain**, the parents or guardians of minors under 14 years of age are obliged to pay a financial penalty. In **China**, the parents or guardians are ordered to discipline children who are not subject to criminal punishment because they are below MACR. Special correctional education can also be conducted.

In **Portugal**, where MACR is 16, the measures for children below the age of 12 are only within the child protection system. Young people between 12-16, can also be subject to educational guardianship measures. In these cases, the Portuguese youth justice system gives utmost importance to educating juveniles on the fundamental community values that have been violated by the illicit act. For that reason, in this age range a transfer of the juvenile to adult's courts is totally inadmissible, whatever the nature of the offences committed, and the Family and Minors court can only impose educational measures (see Table 1).

Similarly, in **Brazil** where minors under 18 are not criminally liable, protective measures are taken vis-à-vis children under 12 who commit 'acts of infraction' and social-educational measures are applied for adolescents between 12-18. It should be noted, however, that some of the social-educational measures in Brazil (e.g., provision of services to the community, insertion in a semi-liberty regime, institutional reception) and the educational measures in Portugal (e.g., admonition, restriction of the right to drive, economic compensation or community work) overlap with the criminal sanctions applicable in other countries for juvenile offenders. Therefore, even though the MACR in these countries is relatively high, in practice the regime applicable to over 12-year-olds is not too different from the one for criminally responsible minors elsewhere.

Table 1 . Educational measures provided by the Portuguese Educational Guardianship Law

MEASURE		DURATION
Admonition (Article 9, LTE)	A lenient warning that, alone or cumulatively with other measures, may be imposed by a court to a young person juvenile subject to youth justice. It consists of a formal reproach or warning given by the court at a public hearing to a young person found guilty of minor facts qualified by the penal law as crime.	---
Restriction of the right to	The young person's right to drive or to obtain a driver's permit for mopeds is subject to restriction.	Applicable for a period

[35] Article 37(c) of CRC.
[36] See https://www.gov.uk/youth-offending-team.

drive or obtain a driver's permit for mopeds (Article 10, LTE)		ranging between one moth and one year.
Reparation to the victim (Article 11, LTE)	Presenting apologies or undertaking any activities related to the inflicted damage which may benefit the victim.	---
Economic compensation or work for the benefit of the community (Article 12, LTE)	The young person must (i) make a payment of a specified amount or (ii) perform a specific activity that benefits a public or private non-profit organization. Activities could be carried out on weekends and bank holidays. Financial compensation could also be paid in instalments, as long this option does not distort the meaning and content of the educational measure. Before establishing the amount of the payment, the judge must take into consideration the young person's ability to pay.	Maximum duration of 60 hours and cannot exceed a total period of three months.
Imposition of rules of conduct (Article 13, LTE)	The imposed rules cannot put abusive or unreasonable constraints to the young person's liberty to make decisions or lead his/her life. The rules should be of preventive nature and are meant to adjust the young person's behaviour to the rules and values essential to life as a member of society.	Maximum duration of two years.
Imposition of obligations (Article 14)	This measure seeks to address young people whose educational needs for the law could be satisfied by attending programmes and activities of educational, formative or therapeutic nature and that are organized and accessible for the population in general. This measure means the young person is obliged to attend controlled activities and programmes, which can include training, school, counselling sessions in psycho-pedagogical institution, activities in clubs or youth associations or undergo medical, psychiatric, psychological treatment or equivalent at a public or private institution, as an outpatient or as hospitalised patient, to treat alcoholism, drug addiction, contagious or sexually transmitted diseases or mental illness. The judge should always seek the young person's agreement for the treatment programmes and over the age of 16 the consent is compulsory.	Maximum duration of two years.
Attendance of training programs (Article 15, LTE)	The legislator intended the intense participation of the young person in certain formative and training programmes specifically adapted for young offenders. The imposition of the obligation of attendance would, therefore, restrict the young person's liberty. In exceptionally situations, this measure can include an obligation to the young person to live with a competent person or institution that provides accommodation, in all cases, in open facilities.	Maximum duration of one year
Educational supervision (Article 16, LTE)	This measure consists of the adjudication to an individualised educational plan (PEP) that covers the areas of intervention defined by the court and involves a combination of measures and educational intervention. The content of the measure is wide-ranging and it can be imposed rules of conduct or obligations as well as attending formative, training or school programmes. The PEP is executed by the services of the Ministry of Justice (currently, the Directorate General of Reintegration and Prison's Services), which has the task to supervise, guide, follow and support the young person throughout its implementation. In case of repeated non-compliance of the PEP, the measure can be extinguished and the	From the minimum of three months to the maximum of two years.

	young person may be sentenced up to four weeks ends in custody in an educational centre.	
Placement in custody (Articles 17 and 145, LTE)	Liberty depriving educational measures could be enforced in four ways: pre-trial detention (Article 146, LTE, up to 3 months, eventually plus 3 months maximum), custodial measure to perform psychological assessment in forensic context (Article 147, LTE, up to 2 months, eventually plus 1 month maximum), for compliance of detention following the young person have been caught in 'flagrant offense' (Articles 51 and 146, LTE), detention measure (Article 148, LTE).	From three months to two years, exceptionally three years in the closed regime.

Source: LTE (1999, 2015), Maria João Carvalho Questionnaire

1.3.3. Measures and sanctions applicable to minors above MACR

Measures for minors above MACR are not only protective but also educational and sometimes punitive. National governments have different approaches towards the system of sanctions applicable to juveniles. In countries such as the **Russian Federation**, **The Netherlands**, **China** and **Latvia**, the same measures are applicable both to minors and adults. The difference in the regime lies in the severity of the sanction and its execution. In the **Russian Federation**, for example, the execution of punishments is done in special prisons or special education and training institutions of a closed type. Additionally, there are reduced fines and imprisonment terms, reduced prescriptive periods (in a half) and reduced time limits for expunging a criminal record. At the same time, the Russian respondent remarked that criminal fines may only be imposed in relation to minors if they have some income or other property.

Other interviewed countries have a special system of sanctions applicable to minors. Some of the measures often overlap with the sanctions for adults (with reductions), while others are targeted only at children. This is the case in **Bulgaria, Belgium, Czech Republic, Greece, Germany, Estonia, Romania, Slovakia, South Africa, Spain**, **UK, USA**. In **Estonia**, for example, measures include: admonition; social program; indemnification and remedy for damage caused by the criminal offence; addiction treatment or another treatment; conciliation service; subjection to supervision of conduct; community service; restriction of freedom of movement with submission to electronic surveillance; placement in closed children's institutions. In **Romania**, only educational measures can be imposed on juveniles. These measures are non-custodial as a rule, although in serious cases minors can be sanctioned with imprisonment in an educational or a detention centre.

The **German** juvenile justice system is remarkable in the extent of its flexibility. It includes three major categories of sanctions: 1. educational measures, e.g., the instruction to attend certain courses like a social skills training course or supervisory assistance (§§ 9-12 JGG); 2. disciplinary measures, e.g., the imposition of conditions or youth detention of up to 4 weeks (§§ 13-16a JGG) and, as a last resort, 3. youth penalty (§ 17 JGG). However, there is no specific range of punishment for each offence and the judge can choose quite freely and individually from the set of sanctions above. When it comes to cybercrime, the German respondent shared that this results in judges imposing measures such as restriction of access to smartphone, the Internet, or social media.

The main issue with this approach, however, remains the enforceability of such measures and whether they will indeed have a dissuading and educational effect on the minor. Indeed, in all interviewed countries the juvenile sanction system is lighter, more flexible and with a focus on re-education and

prevention. Nonetheless, in serious cases measures can also include imprisonment and other forms of restriction of movement. In addition, minors are often obliged to remedy the damage caused by the offensive act. This is especially relevant in cases of hacking and online fraud where the damages could potentially be thousands or even millions of euros.

Recommendation for the game: The game should, if possible, inform minors about the potential sanctions for more serious cybercrimes such as online grooming for human trafficking. It should also make it clear that children and/or their parents could be obliged to remedy any damages caused, which is especially relevant in cases of hacking, using cybercrime as a service and copyright infringements.

1.3.4. Sanctions applicable to young adults over ACM.

Reaching ACM has a great impact in the criminal system because, as clarified in Section 1.1.3, if a child reaches 18 before criminal proceedings are commenced, they will become an adult in the eyes of the law. Young people, however, obviously do not gain maturity from the moment they turn 18 and criminal justice systems worldwide are increasingly recognising this fact.

A situation which is not always clearly regulated is under which system are young adults above the age of 18 prosecuted, tried, and sanctioned when they have committed an offence under ACM. In other words, if a minor commits a crime at 17 but charges are raised when they are 18 or 19, which system applies – the juvenile or the adult one? Many criminal justice systems are notorious for their delays, especially recently in the context of the global pandemic. The issue of juvenile offenders reaching ACM before or during criminal proceedings is therefore quite widespread in practice. The CRC makes it clear that "child justice systems should also extend protection to children who were below the age of 18 at the time of the commission of the offence but who turn 18 during the trial or sentencing process."[37] Nonetheless, turning 18 still has serious consequences for defendants in criminal proceedings in many countries.

Some of the countries in focus have extended the applicability of the juvenile system or provide for lighter sanctions for young adults over 18, even though they have reached the age of criminal majority. In the **Czech Republic** young people between 18-25 are not sent to 'adult prisons' but rather to special institutions for young adult offenders. **Brazilian** law also provides special provisions for crimes committed by people between 18-21, such as compulsory release in case of internment and assistance from parents/guardians.

In **Germany** and the **Netherlands**, the approach is different. The court makes an overall assessment of the offender's personality and the circumstances of the case and afterwards decides whether it would be more appropriate to prosecute them under the juvenile system, rather than the adult one.[38]

Under **USA** federal law, a "juvenile" is a person who has not yet reached the age of 18 at the time of the commission of the offense and is under 21 as of the time of the filing of formal juvenile

[37] UN Committee on the Rights of the Child (2019) *General Comment No. 24 on children's rights in the child justice system*, para 31.
[38] For Germany, the age bracket for this special regime is 18-21 (§ 105 JGG), while for the Netherlands it's 18-23 (Article 77c DCC).

charges.[39]Thus, a person who committed the offense before their 18th birthday but is over 21 on the date formal charges are filed, is prosecuted as an adult. This is true even where the government *could have* charged the juvenile prior to his twenty-first birthday but did not.[40] The situation is different when it comes to state prosecution. As of 2021, 46 states and the District of Columbia automatically prosecute 18-year-olds as adults and 3 states automatically prosecute 17-year-olds as adults.[41] Vermont is the only state that expanded the age of juvenile court jurisdiction to include 19-year-olds in 2022.[42]

Turning 18 has serious consequences for young adults in the **UK**. Reaching ACM during criminal proceedings can affect the procedure in two main ways depending on the timing of the child' birthday:

- If a child is convicted but turns 18 *prior to sentence*, they are entitled to receive youth sentences if specified compulsory conditions are met.
- If a child turns 18 *before, they are convicted*, they can no longer receive youth sentences, regardless of the date of the offence.

Therefore, over-18-year-olds they have not been yet convicted become automatically subject to adult sentences. This has a great impact because the purposes of adult sentences include deterrence, punishment of the offender and protection of the public. This is a significant shift from the purposes of child sentences, which have the prevention and welfare of the child as their central considerations.[43] Although the length or severity of any sentence should always reflect the age a defendant was at the time they committed the offence, the Youth Justice Legal Centre in the UK notes that in practice defendants are sentenced according to their age at the date of conviction, rather than the date of offence.[44] Another highlighted issue is that males who commit offences as children but turn 18 prior to receiving a custodial sentence serve their sentence in Young Offender Institutions. Such institutions, however, do not exist for females, meaning that young women convicted at 18 have to serve their custodial sentence in adult women's prisons.[45]

Therefore, an important aspect of juvenile justice that should be highlighted by RAYUELA is that the protections given to minors during criminal proceedings and the respective milder sanctions regime apply only until the juvenile reaches the age of criminal majority. One can be convicted as an adult for

[39] See 18 U.S.C. § 5031.

[40] See In re Jack Glenn Martin, 788 F.2d 696, 698 (11th Cir. 1986) (determinative date is date of filing of formal indictment or information, fact that Government could have brought charges against defendant prior to his twenty-first birthday held to be "irrelevant").

[41] Children's Defense Fund, *State of America's Children – Youth Justice* (2021). Available at: https://www.childrensdefense.org/wp-content/uploads/2021/04/The-State-of-Americas-Children-2021.pdf

[42] National Governors Association, Age Boundaries in Juvenile Justice Systems (2021). Available at: https://www.nga.org/center/publications/age-boundaries-in-juvenile-justice-systems/

[43] Youth Justice Legal Centre, *Timely Justice: Turning 18 A briefing on the impact of turning 18 in the criminal justice system* (2020). Available at: https://www.justforkidslaw.org/sites/default/files/upload/YJLC%20Turning%2018%20briefing%20(June%202020).pdf

[44] Ibid. See also R v Danga (1992) 13 Cr App R (S) 408 (CA), R v Cassidy (2000) Times 13 October, R v Robinson (1993) 14 Cr App R (S) 448.

[45] Ibid, 39.

crimes they have committed as a minor which could have serious consequences for the future of the young adult.

Recommendation for the game: The game should, if possible, stress that young adults can be prosecuted under the adult criminal system for crimes they have committed as children, oftentimes as soon as they reach 18 years of age.

1.4. Civil liability of minors for their actions

The criminal acts reviewed in this report often can result not only in criminal prosecution but also in civil liability. Even though the civil law consequences of cybercrime are not the central focus of RAYUELA or this report, the applicable regime to minors is important to clarify as the possibility of paying civil damages can play an important role in dissuading minors from committing certain crimes. Civil damages in cases such as online piracy and hacking, for instance, can amount to thousands, which can have a strong preventative influence over minors. In the civil law doctrine, the general principle is that that minors above a certain age of maturity (often 14 years of age), are civilly liable so long as they are able to control their actions and assess their consequences. In addition, their parents are presumed to be jointly liable for the damages caused, unless they were unable to prevent the child's act.

The **Netherlands** is a typical example in this respect. Our respondent noted that under Dutch civil law, children can commit a tort when they are 14 years or older, while parents are solely liable for acts of children under 14. Parents are liable for acts of children aged 14-15 unless they cannot be reproached with not having prevented the child's conduct. Children aged 16-17 are generally liable for damages themselves although their parents might (also) be held liable if they committed a tort by not preventing their child to commit the offence.

Our **Czech Republic** respondent noted that a minor will be held liable for the damage caused if they are able to control their actions and understand their consequences. The minor would be jointly and severally liable with the adult who is obliged to supervise him. The **German** respondent also mentioned that German law has special provisions concerning the civil liability of minors. The lower limit for civil liability in Germany, however, is considerably lower, beginning at age of 7. Nonetheless, the respondent noted that the rule is flexible, and the court would need to assess in each case whether the child was aware and able to understand the consequences of their actions. In **Greece**, the same principle applies, but the minimum age of civil liability is 10 years.

In **Russia**, minors from the age of 14 to 18, can be held liable independently. However, if the juvenile has no income or other assets sufficient to compensate for the harm, the damages are to be paid in full or in part by a legal representative, unless they can prove that they had no fault of their own. In Brazil, the respondent noted that parents are generally responsible for the acts of their children. If they cannot afford to repair the damage or do not have an obligation to pay for the compensation, the minor will repair the damage if he has assets. Minors, however, are liable in a subsidiary and equitable manner, without depriving themselves of their livelihood.

Historically, under the common law doctrine parents were not liable for their children's tort solely on the basis of their relationship. The law has since evolved and the respondents from **South Africa**, **UK** and **USA** noted that parents can be vicariously liable for the actions of their children under 18 years of

age. Vicarious liability may be imposed in cases involving civil wrongs for acts done by others without proof of bad intent on the part of the individual held liable. In other words, parents can be held liable for damages caused by the child's negligent or wrongful actions, regardless of their lack of knowledge of the child's conduct.

Generally, the respondents from the countries in focus confirmed that minors can be held civilly liable under certain circumstances and usually their parents will be obliged to pay the damages because the law considers them either jointly or vicariously liable for their children's unlawful actions.

Recommendation for the game: The game should, if possible, highlight that minors can be held civilly liable even in cases where they are not criminally prosecuted. If possible, it should also clarify that their parents would have to carry the responsibility and pay for any damages caused by them.

1.5. International instruments for cooperation (tackling cybercrime by minors across borders)

In the questionnaire, respondents were also asked about international cooperation mechanisms used to tackle cybercrime by minors across borders. Unsurprisingly, these are the same as are used for tacking (cyber)-crime across borders in general.

This part of the questionnaire does not have direct impact on the game, other than the fact that criminal prosecution does not stop at borders, so that behaviour committed on the internet, with the use of location and identity masking services, or from abroad, do not prevent that criminal liability may attach. This could be a useful element to include in one of the scenarios, to present a united European/global law enforcement front against potential offenders.

Recommendation for the game: The game should, if possible, introduce the fact that criminal prosecution does not stop at borders, highlighting that behaviour committed on the internet, even with the use of location and identity masking services, or from abroad, do not prevent that criminal liability may attach and prosecution may follow, presenting a united European/global law enforcement front against potential offenders.

Since this part does not present a lot of details that have direct influence on the game, this section will not present a detailed analysis of the respondent's answers. Please refer to the national questionnaires for details on the answers for a given country. For the purposes of this report is suffices that the following were mentioned as relevant by the different respondents:

- In general, the possibility on the basis of various international conventions of:
    - extradition of a person for criminal prosecution;
    - transfer of criminal proceedings;
    - cross-border execution of a security measure;
    - cross-border recognition and execution of a judgment;
    - and other measures provided for in international treaties;
- Between the parties to the Budapest Convention on cybercrime (Council of Europe), under the convention the following measures provided for by the convention:
    - Extradition (Art. 24);

  - The general obligation to provide mutual assistance to the widest extent possible (Art. 25);
  - Spontaneous information exchanges (Art. 26);
  - Expedited preservation of stored computer data in another country (Art. 29);
  - Expedited disclosure of preserved traffic data in another country (Art. 30);
  - Mutual assistance regarding accessing of stored computer data in another country (Art. 31);
  - Trans-border access to stored computer data with consent or where publicly available (Art. 32);
  - Mutual assistance regarding the real-time collection of traffic data in another country (Art. 33);
  - Mutual assistance regarding the interception of content data in another country (Art. 34);
  - 24/7 Network to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence (Art.35);

- Cooperation based on the Budapest Convention is also extended to hate speech for the parties to the Additional Protocol on Xenophobia and Racism Committed through Computer System;
- In the future, the second additional protocol to the Budapest Convention, which "provides a legal basis for disclosure of domain name registration information and for direct co-operation with service providers for subscriber information, effective means to obtain subscriber information and traffic data, immediate co-operation in emergencies, mutual assistance tools, as well as personal data protection safeguards". The protocol was opened for signature on 12 May 2022 and will enter into force once it has been ratified by five states;
- European Convention on Mutual Assistance in Criminal Matters and its protocols (Council of Europe);
- The European Convention on Extradition;
- The Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime of the Council of Europe and its update, the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism;
- The Palermo convention (the United Nations Convention against Transnational Organized Crime);
- The Lanzarote Convention;

- Other multilateral mutual assistances treaties than the Budapest Convention and de facto cooperation between several parties, e.g., the mutual assistance treaty between the EU and the US and including regional treaties such as:
    - For Russia, the regional Agreement on cooperation of member state of the Commonwealth of Independent States in combating crimes in the sphere of computer information is mentioned;
    - For South Africa, the African Union Convention on Cyber Security and Personal Data Protection (AUCCSPDP) also known as the "Malabo Convention "is mentioned as relevant.
    - For the USA, the Inter-American Convention on Mutual Legal Assistance of the Organization of American States is mentioned in particular.
    - For China, a number of regional initiatives are mentioned, in particular cooperation with ASEAN states;
- Bilateral mutual assistance treaties and de facto cooperation between two parties;
- For EU countries: the convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union and its protocol, European legal instruments such as the European Arrest Warrant,[46] European Investigation order (Directive 2014/41/EU), European freezing order,[47] and in the future the proposed European Production Order and the European Preservation Order, the Schengen Information System (Regulation 2018/1862) and other justice and home affairs information systems managed by eu-LISA such as the European Criminal Records Information System – Third Country Nationals (ECRIS-TCN), and information sharing instruments such as the Prüm decisions (if relevant),[48] the Swedish Framework decision;[49]
- For EU countries: cooperation with or information from EC3 (the European Cybercrime centre) at Europol, ENISA. Cooperation between national CERTs/CSIRTs and authorities based on the NIS Directive[50] may also affect cybercrime;
- Cooperation and information exchange through Interpol and Europol (including the Joint Cybercrime Action Taskforce), and Eurojust for EU countries,[51] as fora for cooperation, providing various tools and services;
- Various other forms of cooperation that may have an impact on international cooperation in cybercrime, such as the United Nations Commission on Crime Prevention and Criminal Justice (CCPCJ), the Organization for Security and Co-operation in Europe (OSCE), European Judicial Network on Cybercrime), The Global Prosecutors E-Crime Network (GPEN), the Iberoamerican Network of Specialized Cybercrime Magistrates (CiberRede/CiberRed), the Lusophone Forum on Cybercrime and Digital Evidence, the Anglophone intelligence alliance, the Organization of

[46] Council framework decision 2002/584/JHA.
[47] Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence.
[48] Council Decision 2008/615/JHA and 2008/616 JHA.
[49] Council framework Decision 2006/960/JHA.
[50] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
[51] Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust).

American States (OAS) Inter-American Cooperation Portal on Cyber-Crime and Working Group, the Group of Seven (G7)'s 24/7 Cybercrime Network, the Global Forum on Cyber Expertise, the Internet Crime Complaint Center (IC3), cooperation with NGO's (e.g., NCMEC) and international organizations, etc.;

It is worth noting that most respondents have also dealt in detail with the question of territorial jurisdiction and sometimes of extra-territorial application of laws. This is equally not of direct relevance to the RAYUELA game, but readers may wish to consult national questionnaires on this topic.

1.6. Data on cybercrime by minors

While the main intention of the questionnaire and this report was to get more detailed information on the applicable legislation in the countries in focus, it was decided include a request for statistics on cybercrime committed by minors in the questionnaire. The hope was that this would help indicate which are the most problematic areas and could have given guidance to the game in determining which crimes to focus on. Sadly, however, data provided by respondents was in most cases sparse and in most cases where some data could be obtained, there was some information for some crimes, but not for others. Respondents often did not only perform desktop research but also reached out to contacts at competent authorities, with varying degrees of success.

Generally, there is a clear finding that there is a serious lack of publicly available data on cybercrime by minors and in particular on specific crimes. If data is available, it is typically on a higher level and not specific to a given cybercrime.

In a couple of cases where data was found the number of minors offenders were very low or even zero. Several respondents mentioned that they believe that cybercrime by minors is (severely) underreported compared to more obvious crimes by minors, such as theft, vandalism, verbal or physical aggression etc. Part of the reason for underreporting may be that even when a crime is committed and reported to the police, it will only be recorded in statistics if the case is prosecuted and/or brought to trail, with many cases involving minors either being dismissed or never reaching formal trail. Despite that, it may be important to highlight in the RAYUELA game that is important to report online crimes to teachers, parents/guardians and/or the appropriate authorities.

Recommendation for the game: Because of the problem of underreporting in cybercrime (by minors), the game should, if possible, reinforce the importance of reporting online crimes to teachers, parents/guardians and/or the appropriate authorities if a child notices something that they think may constitute criminal behaviour.

Because the data is sporadic it is more anecdotal than anything else. The only trend that could be clearly identified is that several countries reported specific numbers of juvenile offenders in relation to child pornography and related sexual offences against minors and that these were consistently high. In other words, such offences were often committed by other minors or peers. For Germany, the respondent mentioned that 54% of child pornography offences committed through the internet were committed by minor offenders, and 44% of online grooming offences. In both cases the number became smaller when looking at convicted offenders (12% and 16,9% respectively). For Greece, the respondent pointed out that 17% of offenders for crimes of child pornography and online child sexual

exploitation were minors themselves, aged between 12 and 17, compared to 2.6% looking at a broader sample of online crimes). In Slovakia, the respondent reports high numbers from 2020, 2021 and 2022 ranging from around 10% to around 40% for juvenile offenders in several crimes related to child pornography. In addition, the respondent for the UK mentioned that two thirds of contact sexual experienced by children aged 17 or under was committed by someone who was also aged 17 or under and that peer-on-peer abuse is one of the most common forms of abuse affecting children in the UK.

This supports findings from WP1 that also younger offenders are important to focus on in the game, in relation to online grooming and related sexual offences against minors. In the interview sample of D1.3, 33% of offenders were 25 or younger.

Recommendation for the game: The game should, if possible, incorporate the fact that in relation to sexual offences, e.g., online grooming, online sexual abuse, creation and dissemination of child sexual abuse material, including through threat or coercion, etc. other minors or peers may also be a potential offender.

1.7. Recommendations for the RAYUELA serious game

The recommendations of this section are the following:

- The game should, if possible, inform children about the applicable minimum age of criminal responsibility and highlight that being a minor does not entail that you cannot be criminally prosecuted and sanctioned;
- The game should, if possible, make it clear that minors can be prosecuted for cybercrimes, even though preferential treatment would be applicable. This is especially true for more serious crimes where state organs could decide to prosecute a minor in order to dissuade other juveniles from this behaviour;
- The game should, if possible, inform minors about the potential sanctions for more serious cybercrimes such as online grooming for human trafficking. It should also make it clear that children and/or their parents could be obliged to remedy any damages caused, which is especially relevant in cases of hacking, using cybercrime as a service and copyright infringements;
- The game should, if possible, stress that young adults can be prosecuted under the adult criminal system for crimes they have committed as children, oftentimes as soon as they reach 18 years of age;
- The game should, if possible, highlight that minors can be held civilly liable even in cases where they are not criminally prosecuted. If possible, it should also clarify that their parents would have to carry the responsibility and pay for any damages caused by them;
- The game should, if possible, introduce the fact that criminal prosecution does not stop at borders, highlighting that behaviour committed on the internet, even with the use of location and identity masking services, or from abroad, do not prevent that criminal liability may attach and prosecution may follow, presenting a united European/global law enforcement front against potential offenders;
- Because of the problem of underreporting in cybercrime (by minors), the game should, if possible, reinforce the importance of reporting crimes online to teachers, parents/guardians and/or the appropriate authorities if a child notices something that they think may constitute criminal behaviour;
- The game should, if possible, incorporate the fact that in relation to sexual offences, e.g. online grooming, online sexual abuse, creation and dissemination of child sexual abuse material, including through threat or coercion, etc. other minors or peers may also be a potential offender.

2. Online grooming and minors

2.1. Introduction: what is online grooming?

Online grooming (further also referred to as: OG) is a part of the broad category of online enticement crimes which involve an individual communicating with someone believed to be a child via the internet with the intent to commit a sexual offense or abduction.[52] Online grooming, also known as solicitation, takes place when an adult uses electronic communication in a predatory fashion to try to lower a child's inhibitions, or heighten their curiosity by sending pornographic material or talking about sexual matters. OG is usually a preliminary step with the aim of the predator being to eventually meet the child in person for the purposes of sexual activity. The process often starts with the offender sending pornographic images of themselves so as to normalise the requests, and then moves to requesting from the child to send naked photos or perform sexual acts on a web cam.[53]

Offenders can use different tactics to gain children's trust – pretending to be their peers, creating fictional personas to develop a sense of kinship with victims, or portraying themselves as a trustworthy adult in a place where other adults are largely absent. To achieve their aims, online predators use all types of platforms: social media, messaging apps, video games, online chats, etc.[54]

Recommendation for the game: The game should, if possible, include many different platforms where minors could become victims of online grooming - social media, messaging apps, video games, online chats, etc.

In recent years, OG has become and increasing growing concern, presumably due to the Covid-19 pandemic, when both children and offenders spent more time online and at home. The number of **grooming cases reported globally increased by 98% in 2020** compared to the previous year (37 872 in 2020 vs 19 147 in 2019).[55] What's more, in a survey conducted by Thorn in 2020, 50% of children aged 9 to 17 said that they had sent nudes to someone they had never met in real life, and 41% believed they were sending the images to an adult. That represents a significant increase year-over-year, up

[52] NCMEC, Online enticement, see https://www.missingkids.org/theissues/onlineenticement.

[53] Susan McLean, Presentations at John XXIII College, September 2014. Available at https://www.johnxxiii.edu.au/view/parent-resources/susan-mclean-cybersafety.

[54] Thorn, Online grooming: What it is, how it happens, and how to defend children, June 15, 2020. Available at: https://www.thorn.org/blog/online-grooming-what-it-is-how-it-happens-and-how-to-defend-children/. See also NELLIE BOWLES and MICHAEL H. KELLER, Video Games and Online Chats Are 'Hunting Grounds' for Sexual Predators, The New York Times, DEC. 7, 2019. Available at: https://www.nytimes.com/interactive/2019/12/07/us/video-games-child-sex-abuse.html

[55] NCMEC, Online Enticement Reports Skyrocket in 2020, 21 January 2021. Available at https://www.missingkids.org/content/ncmec/en/blog/2021/online-enticement-reports-skyrocket-in-2020.html

from 37% in 2019.[56] This worrying trend has resulted in renewed efforts to regulate the field, including by automated detection and prevention of grooming activities online.[57]

2.2. International standards

OG is regulated internationally in the Council of Europe Convention on the **Protection of Children against Sexual Exploitation and Sexual Abuse**, also known as the Lanzarote Convention (LC), which requires criminalization of all forms of sexual offences against children. All 46 Member States of the Council of Europe have signed and ratified the Lanzarote Convention. The Russian Federation has also signed and ratified it. In addition, Tunisia has also acceded to it has thus become the first non-European State Party to the Convention. In particular, OG is regulated in Article 23 of LC – Solicitation of children for sexual purposes, which states:

> Each Party shall take the necessary legislative or other measures to criminalise the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the age set in application of Article 18, paragraph 2 [the age below which it is prohibited to engage in sexual activities with a child], for the purpose of committing any of the offences established in accordance with Article 18, paragraph 1.a [engaging in sexual activities with a child], or Article 20, paragraph 1.a [producing child pornography], against him or her, where this proposal has been followed by material acts leading to such a meeting.

Therefore, the crime of OG includes the following elements:

1. intentional proposal through ICT to meet,
2. followed by material acts leading to such a meeting
3. of an adult
4. to a child of an age below which the law prohibits engagement in sexual activities
5. for the purpose of engaging in sexual activities with the child or producing child pornography.

In it important to note that the LC sets the minimum standard for criminalizing OG and most countries have gone beyond it in their national legislation. First, the Convention does not mandate for its State Parties to criminalize this activity when committed by minors, although many countries have opted to do so. In addition, the act needs to be performed with the purpose to further commit two specific crimes: 1) performance of sexual activities with a child i.e., statutory rape, and/or the production of child pornography. Once again, as observed in Section 2.3 in further detail, State Parties usually refer to additional crimes of sexual nature as well in their national laws. Furthermore, some countries do not include an obligation for further material acts to take place after the proposal for a meeting.

[56] Thorn, Self-Generated Child Sexual Abuse Material: Youth Attitudes and Experiences in 2020, 2020. Available at: https://www.thorn.org/blog/thorn-research-trends-confirm-need-for-parents-to-talk-about-online-safety-with-kids-earlier-more-often/?utm_source=organic+social&utm_medium=twitter&utm_campaign=SG_monitoring_2021&utm_content=thread

[57] See European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse, May 2022.

The EU also sets minimum standards with regards to the criminalization of child sexual abuse, including online grooming. Article 6 of **Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography** [58] (CSA Directive) has almost the same wording as Article 23 Lanzarote Convention with only two key differences. The first is that the relevant age of the victim is harmonized throughout the EU as the age of sexual consent. The second difference is that the CSA Directive regulates that the maximum term of imprisonment for OG in EU Member States should be at least 1 year. In addition to the CSA Directive, the in May 2022 the European Commission published a Proposal for a Regulation laying down rules to prevent and combat child sexual abuse.[59] Unlike the Directive, which harmonizes the types of child sexual abuse acts to be criminalized in the Union, the proposed regulation introduces new rules and obligations for online service providers to detect and remove online grooming and child sexual abuse material in the EU. The new regulation will therefore not change the definition of OG but will rather attempt to facilitate law enforcement in the field.[60]

2.3. How is online grooming regulated in the countries in focus?

Most of the interviewed countries have introduced national legislation which follows the structure of the Lanzarote convention. EU Member States, in particular, have kept their regulation close to the text of the CSA Directive with deviations in different parts of the qualification, often aiming to offer greater protection for victims of OG. The interviewed countries which are not State Parties to the Lanzarote Convention also criminalize OG but usually under the more general crime of [online] child enticement. From interviewed countries, China has the most specific approach to OG, as the responded indicated that this offence is covered under the provision that criminalizes abducting and trafficking women or children.

It should be noted that if the online groomer reaches their desired aim and commits child sexual assault, production of child pornography or another crime against the minor, then the national rules about cumulation and concurrency of offences apply. Often the perpetrator would be punished only for the more serious crime to which the grooming leads up to. A noteworthy example in this respect is **Spain** where the Spanish Supreme Court has made a distinction between the offences that can concur with child grooming. When the offences of sexual abuse or sexual assault are involved, there is actual concurrence – that is, the penalties for both offences will be applied independently. On the other hand, when it comes to the crime of prostitution, the Spanish Supreme Court considers that this crime protects the same legal right as the crime of child grooming, i.e., sexual indemnity. Consequently, in

[58] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

[59] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse. See also the Commission's Impact Assessment: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0209.

[60] For more information see European Commission, Press Release, Fighting child sexual abuse: Commission proposes new rules to protect children (2022). Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2976

cases of concurrence between a prostitution offence and a child grooming offence, the penalty applied is the one corresponding to the more serious offence.

In European countries, national legislation reflects the structure, and often the wording, of the Lanzarote Convention. An intentional proposal to meet with a child through ICT, followed by material acts which aim to lead to such meeting, are the main objective elements of the crime in **Belgium, Estonia, Greece**, **Spain,** and **The Netherlands**. The *material acts leading to the meeting* could be any acts that aim to facilitate the meeting and ensure it takes place, e.g., arranging for the victim's transport, arranging a space for this purpose, etc. In **The Netherlands** the respondent highlighted that it is sufficient for the perpetrator to pressure the victim to meet soon and to give his phone number to the child.[61]

Another set of European countries considers the act of making a proposal to meet a child with the intention of carrying out a sexual offence as sufficient for committing OG. This is the case in the **Czech Republic, Bulgaria, Latvia** (what the law criminalizes, however, is 'encouragement' of a minor to meet, not mere proposal), **Portugal**, **Romania,** and **Slovakia.** In **Portugal**, if the grooming is followed by material acts leading to the meeting, the offender is punished with a more severe penalty. If the encounter takes place and sexual crimes are committed, the offender is punished for them.[62]

In the case Acórdão do Tribunal da Relação de Lisboa 117/17.2PHLRS-3, the judge notes that online grooming "*is a formal crime or a mere activity, which is therefore consummated with the mere attempt to arrange a meeting with a minor with such illicit desiderata (it is not required that the meeting actually takes place), and it is also a crime of abstract danger*". The judge continues to find the offender guilty by explaining exactly what parts of the perpetrator's actions demonstrate their criminal intent – "*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*."[63]

Recommendation for the game: The game should, if possible, include scenarios with growing levels of inappropriate grooming behaviour in order to determine when children realise that the person, they are communicating with is crossing the line (i.e., from making compliments in a messaging app, to sending revealing photos, to sexting, to asking for revealing photos and child sexual abuse material, to proposing a meeting in person and arranging a place to meet).

Interestingly, **Bulgaria** criminalizes an act that could be considered as preparatory to OG (which is itself a preparatory activity), namely disclosure or collection information about a person under 18 for the purpose of establishing contact with that person to perform sexual abuse.[64] In other words, if law enforcement authorities are successful in finding evidence that a predator is collecting information

[61] HR [Dutch Supreme Court] 11 November 2014, ECLI:NL:HR:2014:3140.
[62] See Portuguese Questionnaire.
[63] Acórdão do Tribunal da Relação de Lisboa 117/17.2PHLRS-3 (Decision of the Court of Appeal of Lisboa). Judge: João Lee Ferreira. Date: 12-11-2019.
[64] Article 155a(1) of the Bulgarian Criminal Code.

about a minor with the aim of committing sexual abuse, even before the actual grooming began, the offender could be found guilty. This brings the moment in time where a crime is committed even earlier than the proposal of a meeting, or even the establishment of contact with the child.

In the **UK**, there are several crimes under which the offender can be prosecuted for online grooming, depending on the discretion of the prosecutor:

- Section 14 of the Sexual Offences Act (2003) makes it an offence to arrange or facilitate a meeting with any child under the age of 16 where there is an intention by an individual to sexually abuse the child or there is an intention for another person to sexually abusing them.
- Section 15 of the Sexual Offences Act (2003) makes it a criminal offence to *meet* a child under 16 (or if the offender does not reasonably believe that the victim is 16 or over) following the process of grooming.
- Section 67 of the Serious Crime Act (2015) defines *any* repeated sexual communication with a child under 16 as a criminal offence thus outlawing the actions of any groomer who uses mobile phones, SMS texts, social media, or emails to communicate sexually with children or with the intention of eliciting a sexual response.

The UK respondent summarised a case that demonstrates the various means predators can use to groom minors and gain their trust is *R v Scarrott*.[65] Scarrott had begun by contacting children over the internet and had built up a very significant following from a messages and other material he posted or uploaded. With an online profile which attracted over 70,000 followers, Scarrott was a "social media influencer". He travelled significant distances throughout England and Wales to meet children he had contacted and even booked a hotel room in which to abuse a victim. Scarrott was sentenced in 2020 for multiple offences against young females aged 14 or 15 years, including for 3 offences of arranging or facilitating a meeting with a child, contrary to Section 14 of the 2003 Act.

Recommendation for the game: The game should, if possible, include a reference to a situation where the grooming is done by a person who is considered famous or admirable for children (e.g., Tik Tok or Instagram influencer, well-known gamer). That would demonstrate that famous people are not necessarily trustworthy, and children should still be conscious of possible predatory behaviour.

Germany also has a slightly more different regulation when it comes to online grooming. § 176b StGB requires that the offender acts on a child under the age of 14 by making use of a content according to § 11 section 3 StGB in order to prepare a type of sexual abuse, either by making the child carry out a sexual act on or in front of the offender or a third person or to allow the offender or a third person to carry out a sexual act on the child. The German respondent pointed out that one of the problems of application is the question what *acting on a child* („auf ein Kind einwirken“) actually means.[66] In a case that was decided in 2015 by the German Federal High Court,[67] the offender sent a pornographic picture via WhatsApp to a girl that was 11 years old. On the same day, in other messages, he told her that he wanted to make her have an orgasm. The court stated that sending the picture alone did not fall under § 176 StGB, because acting on the victim would require a deeper psychological influence on the victim;

[65] R v Scarrott, [2020] EWCA Crim 1435.
[66] See also Stoiber, Cyber-Grooming aus strafrechtlicher und kriminologischer Sicht, 2018, 157 et seq.
[67] BGH, Beschl. v. 22.01.2015, NStZ-RR 2015, 139.

the mere display of pornography would not suffice for that. Sending the picture in combination with the following messages, however, was considered sufficient.

Legislation like the one in **Germany** and the **UK** (i.e., Section 67 of the Serious Crime Act) highlights the issue with online grooming and abuse that take place entirely online, where the predator may not intend to meet in person with the child. Our respondent from **Estonia** highlighted this issue by noting that the online grooming crime in Section 178 of the Estonian Penal Code (Agreement of sexual purpose for meeting with child) does not include online meetings and hence does not address one of the most pressing concerns – when the crime takes place fully online. Nonetheless, usually other offences such as enticement, extortion, online harassment and child pornography could be used to prosecute abusive behaviour that takes place entirely online. In fact, nearly all interviewed respondents confirmed that purely online behaviour with sexual intent is punished under one form or another, and that minors can be prosecuted and punished for such actions as well.

Recommendation for the game: The game should, if possible, include a scenario with purely online predatory behaviour with sexual intent (e.g., requesting intimate photos, sexting) where the offender does not necessarily aim to meet the victim in person. The game should make it clear that such behaviour is also criminalized.

After a failed legislative attempt, the **Russian Federation** does not have a legislation specifically targeting online grooming. Nonetheless, there are three crimes which cover not only online grooming but also other online acts of sexual nature against a minor. The first one is 'depraved actions'[68] which is applicable to any actions without violence which are intended to satisfy the sexual desire of the perpetrator, or to arouse sexual arousal in the victim, or to arouse his interest in sexual relations. This article includes cases where the groomer has engaged the minor by means of emotional or romantic attachments. On the other hand, if the perpetrator uses non-physical violence (e.g., blackmail, threats), the act would be qualified as a ''coercion to acts of a sexual nature'.[69] Where the grooming is committed against children under the age of 12, another article applies which envisions more serious criminal sanctions.[70] The Russian respondents gave examples where individuals were convicted under these crimes for engaging in sexual correspondence over *Vkontakte* social media, sending sexualised text messages and pornographic imagery to minors, and requesting intimate images of the victims.

Contacting minors online and requesting "images, audio or video of explicit sexual activities, acts of sexual connotation, or a sexual encounter" is also criminalized in **Mexico**. According to our respondent, as long as the victim provides sufficient and convincing evidence to the *Ministerio Público* (Public Prosecutor) through data, screenshots that he or she is being contacted for sexual purposes, the case will be investigated. A similar legislative approach which criminalizes in general any enticing, inducing, persuading or encouraging of a child to engage in illegal sexual activities is undertaken in **Brazil**, **South Africa** and the **USA**. In addition, 42 states in the USA have their own anti-grooming legislation. In **China** there is no explicit legislation on online grooming but our respondent notes that the act is directly included in the broad constituent element of 'abducting', which covers the use of deception, inducement, or other means to take away minors under the age of fourteen.[71]

[68] Article 135 of the Russian Criminal Code.
[69] Article 133 (2) of the Russian Criminal Code.
[70] Article 132 (4)(b) of the Russian Criminal Code (Violent actions of a sexual nature in relation to a minor).
[71] Article 240 of the Criminal Law of the People's Republic of China (Abducting and trafficking women or children).

For the act of online grooming to be punishable, it needs to be intentional. What is characteristic of online grooming, however, especially as it is regulated under the Lanzarote Convention, is that the offender needs to act with the specific intent commit another crime. The crimes that the groomer aims to further commit are specified in national legislation.

All State Parties to the Lanzarote Convention set out that the crimes the perpetrator should have in mind are engaging in sexual acts with a minor (sexual abuse) and/or the production of child pornography. Countries like **Greece, Portugal, Slovakia,** and **Spain** limit online grooming only to these two crimes. Many countries, however, have widened the spectrum (e.g., **Czech Republic, Estonia, Bulgaria**) and have included in their OG provisions grooming for the purposes of seduction to sexual intercourse, prostitution, molestation. Another approach, such as the one in **Belgium** for example, is to generally refer to all sexual offences against minors.

Proving specific intent, however, can be especially difficult in cases of online child sexual grooming. The **Belgian** respondent notes that the judge will look into the content of the conversation in order to determine if there is sufficient proof for the intent of the offender. For example, the Court of Appeal in Gent did not consider the offence of grooming to be present in a case where a 46-year-old man repeatedly had sent declarations of love and virtual kisses to a 12-year-old girl, without any explicit sexual insinuations.[72]

The **USA** respondent highlighted that indeed some offenders may seek to engage in sexualized online chats with minors with no intention of moving the online interactions to criminal acts such as sending or receiving sexual material or in-person sexual contact.[73] The respondent noted that some authors argue that fantasy-driven sexualized conversation online may not constitute a preparatory action for in-person sexual contact, and therefore shouldn't be prosecuted under sexual grooming legislation. There also examples in practice where the jury agreed with the "fantasy defence". In a case summarised by the US respondent, a 34-year-old man had sexual online correspondence for over nine months with KRISLA (an undercover FBI agent). At some point he travelled from Seattle to Santa Monica to meet KRISLA. The offender was arrested for using the Internet to try to arrange to have sex with a minor. During trial the defendant argued that he thought the person he was about to meet was a grown woman who shared his "daddy/daughter" fantasy and was "playing the part" of a young girl. The jury believed his "fantasy defence" and acquitted him.[74]

Recommendation for the game: The game should, if possible, make it clear that it is not illegal to have romantic or even intimate conversations with a peer. It should, however, if possible, informed children of the dangers when they engage in such communication with adults.

Age is relevant with regards to online grooming in two ways. First, national legislation could include threshold for the age of the offender. Second, many countries specify different ages under which a person can be victim to the crime.

As the LC and the CSA Directive set only the minimum standards for criminalising online grooming, they envision the prosecution of only adult offenders. This approach is followed in **Latvia, Portugal,**

[72] Gent 19 October 2018, RW 2019-20, alf. 17, 670.
[73] Gilden, A. (2016). Punishing sexual fantasy. *Wm. & Mary L. Rev.*, *58*, 41
[74] Yamagami, D. (2000). Comment, Prosecuting Cyber-Pedophiles: How Can Intent Be Shown in a Virtual World in Light of the Fantasy Defense?, 41 Santa Clara L. Rev. 547.

Romania, Russia, Slovakia, and the **UK**, where only adults can commit the crime of online grooming. In most of the interviewed countries, however, minors can be punished for grooming activities as well. This is the case in **Belgium, Brazil, Bulgaria, China** (minors above 14 are criminally responsible for Article 240 abducting and trafficking women or children), **Czech Republic, Estonia** (if the difference between the minors is more than 5 years), **Germany**, **Greece, Mexico, Spain, South Africa**, **The Netherlands**, **USA** (for the federal crime).

Recommendations for the game: The game should, if possible:

Include a scenario where the offender is a minor (a peer of the victim) as most of the interviewed countries criminalise OG committed by minors. It should, however, try to highlight the difference between predatory behaviour and innocent romantic conversations between peers.

Include a scenario where the offender is adult who is either open about their age or is pretending to be the victim's peer by using a fake account.

Educate children about ways the fact that accounts may be fake and help them to learn how to spot fake and suspicious accounts by providing them with concrete examples in the game where accounts are likely fake or clearly present suspicious elements.

Rules also exist about the age of the victim below which grooming can exist (see Table 2). They are determined by national legislation but in the EU the CSA Directive harmonises as relevant the age of sexual consent in the respective Member State (Article 6).

Table 2. Relevant age of the victim of online grooming

Country	Maximum age of the victim	Comments by the respondents
Belgium	16	There will be no offence if the minor is 14, consents to the act, and the age difference between them and the other person is no more than 3 years.
Brazil	18	
Bulgaria	14	But offenders can be punished for disclosure or collection of information about a person under 18 for the purpose of establishing contact and performing certain prohibited acts.[75]
China	14	
Czech Republic	15	
Estonia	14	To be raised to 16 with a legislative reform in 2022.
Germany	14	
Greece	15	
Latvia	16	
Mexico	18	

[75] Article 155a (1) Anyone who, by using information or communication technology or otherwise, discloses or collects information about a person under 18 years of age for the purpose of establishing contact with that person so as to perform molestation, copulation, sexual intercourse, or prostitution, or to create pornographic material, or for the purpose of involvement in a pornographic show shall be punished by imprisonment from one to six years and a fine from BGN 5,000 to BGN 10,000.

Portugal	18	However, the age of sexual consent is 14 and some of the crimes for the purpose of which OG is committed only apply to sexual abuse of children under 14.[76]
Romania	13	
Russian Federation	16	
Slovakia	15	
Spain	16	
South Africa	18	
The Netherlands	16	
United Kingdom	16	
USA	18	For the federal enticement statute under 18 U.S.C. § 2422 of the U.S. Criminal Code. Different ages could be applicable in state OG legislation.

Source : information from the questionnaires.

What is important, however, is that the age of the victim could be regulated as both an objective and subjective element of the crime. If age is an objective element, i.e., not only is the offender convinced that they are communicating with a minor, but the victim is in fact a child, that could create issues in efforts to identify and catch predators. The **German** respondent gave an example with a case in 2016 where the mother of a 9-year-old that was messaged by a groomer took her daughter's phone and decided to continue the conversation in her daughter's name. The court held that a relevant urging or convincing had not taken place as the messages to the actual victim did not have a sufficient sexual content and the later messages were not received by the child itself. The fact that the later messages were only received by the mother of the victim excluded criminal liability.[77] The German legislator later filled this gap in the law by including § 176b section 3 StGB with its special regulation of a punishable attempt in cases where the offenders only think they are communicating with a child. In other words, the new provision considers the subjective belief of the perpetrator with regards to the age of the victim as the relevant factor.

There was a similar issue in **The Netherlands** where under previous law, in 2013, a man was acquitted of grooming because it turned out that the person he was grooming, whom he thought to be a minor, was in fact an adult policewoman.[78] Therefore, he had not actually proposed a meeting to a minor. As a result, the law was changed to include '*someone who pretends to be below 16, with or without the help of a technical tool, including a virtual of someone below 16*.'[79] The latter part – using a technical tool – was added due to the publicity given to Terre des Homme's campaign against webcam sexual abuse using an avatar of a young Philippine girl called Sweetie.[80] The Dutch lawmaker considered it important that law enforcement might also use such an avatar in OG investigations. These examples should be taken into consideration by countries that consider the age of the victim solely as an objective element of the crime. The approach in Germany and The Netherlands opens grater

[76] It was acknowledged in the report "Sexual Exploitation of Children in Portugal, that the OG provision does not give an equal protection to all children against grooming for the purpose of sexual relations, as articles 171-1 and 171-2 only apply to sexual abuse of children under 14. Available at: https://gddc.ministeriopublico.pt/sites/default/files/documentos/pdf/3ciclo-cc1.pdf

[77] OLG Hamm, Beschl. v. 14.1.2016, MMR 2016, 425. See German questionnaire.

[78] Hof [Court of Appeal] Den Haag, 25 June 2013, ECLI:NL:GHDHA:2013:2302.

[79] *Kamerstukken II* [Parliamentary Documents Second Chamber] 2016/17, 34 372, 15.

[80] See https://www.terredeshommes.nl/en/programs/sweetie.

possibilities for law enforcement to identify predators and for parents to protect their children, without the risk of that leaving the offender unpunished.

Recommendation for the game: The game should, if possible, outline the possible actions a child that realises it is being groomed can undertake (e.g., immediately talking to a parent, teacher or informing the police). It should, if possible, be made clear that there would be negative consequences for the offender in each of those cases.

Another aspect in which both the age of the offender and the age of the victim could be relevant is with regards to the so-called "Romeo and Juliet laws" in some countries (e.g., **Belgium, Estonia, Germany, The Netherlands**). The goal of these laws is to prevent behaviour between people who are close in age from being considered sexual abuse. They set acceptable age limits for minors and persons close in age who can engage in sexual activities. The relevance of these provisions therefore is that if the proposal for a meeting to a minor close in age is done with a view to engaging in sexual activities and Romeo and Juliet laws are applicable, then the purpose for the meeting would not be to commit a crime. This element would be absent from the act and the crime of online grooming would not be committed as well.

In **Belgium**, for example, a minor who has reached the age of 14 years but is not yet 16 is capable of giving sexual consent if the age difference with the other person is not more than 3 years. The Belgian respondent summarised the applicability of these rules in the following way: a 20-year-old who proposes a 15-year-old to meet with a view to perform sexual acts, will be committing a grooming offence if this proposal is followed by material acts which may lead to such a meeting since a 15-year-old is never capable of giving sexual consent to a 20-year-old. A 17-year-old who proposes a 15-year-old to meet with the same intentions will not necessarily commit a grooming offence, since in those circumstances the meeting up and sexual acts may be performed with mutual consent. It should be noted, however, that Romeo and Juliet laws usually apply with regards to engagement in sexual activities and are not relevant in cases of creation of child sexual abuse material, i.e., crimes related to production of child pornography.

The applicability of Romeo and Juliet laws to online grooming, however, is not straightforward as it is usually not explicitly noted in the law. The respondents from both Germany and The Netherlands noted that this leads to inconsistency in national legislation and its application. In **Germany** there is an explicit possibility to refrain from punishment in cases where there is no big difference in age and maturity between victim and offender performing a sexual act (see § 176 section 3 StGB) but such a provision does not exist regarding online grooming (§ 176b StGB). In **The Netherlands**, on the other hand, the closeness of age matters in the context of sexting and child pornography but no reference to the relevance of age is made in the online grooming provision. As the exact rules as to the applicability of Romeo and Juliet laws to OG are still unclear in many countries, the closeness in age between the victim and the offender would not necessarily exclude the criminal liability of the offender even in countries where such laws exist.

2.4. Recommendations for the RAYUELA serious game

The recommendations of this section are the following:

- The game should, if possible, include many different platforms where minors could become victims of online grooming - social media, messaging apps, video games, online chats, etc.;
- The game should, if possible, include scenarios with growing levels of inappropriate grooming behaviour in order to determine when children realise that the person, they are communicating with, is crossing the line (i.e., from making compliments in a messaging app, to sending revealing photos, to sexting, to asking for revealing photos and child sexual abuse material, to proposing a meeting in person and arranging a place to meet);
- The game should, if possible, include a reference to a situation where the grooming is done by a person who is considered famous or admirable for children (e.g., Tik Tok or Instagram influencer, well-known gamer). The game should highlight that famous people are not necessarily trustworthy and children should still be conscious of possible predatory behaviour;
- The game should, if possible, include a scenario with purely online predatory behaviour with sexual intent (e.g., requesting intimate photos, sexting) where the offender does not necessarily aim to meet the victim in person. The game should make it clear that such behaviour is also criminalized;
- The game should, if possible, make it clear that it is not illegal to have romantic or even intimate conversations with a peer. It should, however, if possible, informed children of the dangers when they engage in such communication with adults;
- The game should, if possible, include a scenario where the offender is a minor (a peer of the victim) as most of the interviewed countries criminalise OG committed by minors. It should, however, try to highlight the difference between predatory behaviour and innocent romantic conversations between peers;
- The game should, if possible, include a scenario where the offender is adult who is either open about their age or is pretending to be the victim's peer by using a fake account;
- The game should, if possible, educate children about ways the fact that accounts may be fake and help them to learn how to spot fake and suspicious accounts by providing them with concrete examples in the game where accounts are likely fake or clearly present suspicious elements;
- The game should, if possible, outline the possible actions a child that realises it is being groomed can undertake (e.g., immediately talking to a parent, teacher or informing the police). It should, if possible, be made clear that there would be negative consequences for the offender in each of those cases.

3. Online grooming for purposes of human trafficking and minors

3.1. Introduction: what is online grooming for human trafficking?

Online grooming is the act using social media, online platforms, or other ICT to lower a child's inhibitions and gain their trust. As observed in the previous section, however, the purpose for which the grooming is carried out is relevant for the qualification of the crime. Solicitation of children can be carried out not only to fulfil the sexual desires of the predator, but also to "recruit" minors for human trafficking. ***Human trafficking*** (further also referred to as: HT) involves the use of force, fraud, or coercion for the purpose of sexual or labour exploitation. Traffickers are experts at finding vulnerable victims and manipulating their feelings and reality to leverage fear and induce submission.[81] Grooming for human trafficking is not a new phenomenon but the Internet has introduced ever more possibilities for traffickers to directly contact and entrap their victims. Similarly, to the observed trend with respect to the crime of OG, the Covid-19 pandemic has led to growth in recruitment for sexual exploitation online and technology-facilitated child trafficking for the purpose of sexual exploitation.[82]

A 2021 Polaris report using data from the National Human Trafficking Hotline in the **USA** demonstrates the troubling recent trends regarding the recruitment locations used by traffickers. Between 2019 and 2020, 'traditional' recruitment locations such as bus stations, schools, mental health facilities, and private foster homes all experienced significant declines. At the same time, Facebook experienced a 125% increase in trafficking recruitment rivalled only by Instagram, which had a 95% increase. The total number of victims groomed on both social media platforms has increased by 120% for the same period.[83] Similar trends are observed worldwide in the UNODC Global Report on Trafficking in Persons for 2020, which observes how the Internet in recent years has served to better connect perpetrators, victims and consumers at multiple locations.[84] The report demonstrates that traffickers use different types of platforms to connect with victims:

- Social media, including *Facebook*, *Instagram*, *WhatsApp* and *Vkontakte*;
- Classified webpages for advertisement, i.e., generic websites where individuals post advertisements or browse for items or services to buy or sell;

[81] Polaris Project, Love and Trafficking: How Traffickers Groom & Control Their Victims, Online, 2021. Available at: https://polarisproject.org/blog/2021/02/love-and-trafficking-how-traffickers-groom-control-their-victims/.
[82] Committee on the Elimination of Discrimination against Women, General Recommendation No. 38 (2020) on trafficking in women and girls in the context of global migration, UN Doc. CEDAW/C/GC/38, 6 November 2020.
[83] Polaris Project, Typology of Modern Slavery: Defining Sex and Labor Trafficking in the United States. Available at: https://polarisproject.org/wp-content/uploads/2022/01/Polaris-Analysis-of-2020-Data-from-the-National-Human-Trafficking-Hotline.pdf
[84] UNODC, Global Report on Trafficking in Persons 2020 (United Nations publication, Sales No. E.20.IV.3).

- Free-standing webpages, i.e., websites created by traffickers that do not form part of larger domains.

Among them, social media is ever more increasingly used by traffickers, which is especially dangerous for minors. Two main types of recruitment can be observed on social media – online relationship recruitment and online fake/deceptive job recruitment.[85] In the first case, traffickers usually create a fake online profile to appear to be approximately the same age as the victim. They comment on photos and send direct messages, building rapport and intimacy to entice their victims into a false sense of trust. The next phase is often "boyfriending" – showing romantic interest, extreme flattery, promises of gifts or other financial assistance. Once they've gained the victim's trust, traffickers may ask the child for intimate pictures or to participate in sexually explicit acts via live stream. This part of the process largely resembles online sexual solicitation. However, traffickers often use the explicit material they obtain to blackmail or extort the young person into commercial sexual exploitation. They create feelings of fear, anger, and hopelessness in their victims in order to convince them to engage in sexual acts with/for other people.[86]

The other main type of recruitment is with fake or deceptive online job advertisements. Some sex traffickers recruit victims through illegitimate job offers for modelling or dancing, sometimes by using ugh fake business profiles, event pages on Facebook, or on specialised websites for job offers. Traffickers may also contact the potential victim directly, claiming to be a recruiter for a modelling agency or the owner of another kind of legitimate business seeking staff.[87] This type of recruitment is different from the more typical forms of online grooming but is also quite common on social media websites and can be used as a means to entice minors in a vulnerable situation.

Recommendations for the game: The game should, if possible:

Include scenarios that include the two main types of online grooming for the purposes of human trafficking used by predators on social media: online relationship recruitment ("boyfriending"/"lover boys"/"Romeo pimps") and online fake or deceptive job recruitment (e.g., someone is looking for models for an advertising agency, or proposing an easy way to make money).

Demonstrate the ways traffickers operate to gain the trust of their victims and entrap them (i.e., from engaging in intimate conversations, making compliments, or pretending to be friends, to then asking the victim for intimate photos or participation in live streams, to blackmail and creation of feelings of isolation and hopelessness).

Inform minors about ways to stop communication with the groomer and signal parents/authorities.

[85] Polaris Project, On-Ramps, Intersections, and Exit Routes: A Roadmap for Systems and Industries to Prevent and Disrupt Human Trafficking, Social Media. Available at: https://polarisproject.org/wp-content/uploads/2018/08/A-Roadmap-for-Systems-and-Industries-to-Prevent-and-Disrupt-Human-Trafficking-Social-Media.pdf

[86] Valentin Luz, Social media grooming for sex trafficking, 2020, The Canadian Centre To End Human Trafficking. Available at: https://www.canadiancentretoendhumantrafficking.ca/social-media-grooming-for-sex-trafficking/

[87] Ibid at 81.

3.2. International standards

The criminalization of human trafficking is mandated on an international level by the **UN Convention against Transnational Organized Crime** (2000) and the **Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime** (also known as the Palermo Protocol). All RAYUELA interviewed countries have ratified both the convention and the Palermo Protocol, meaning that the national regulation in the field of human trafficking is harmonised to a large extent.

The international definition of human trafficking is included in Article 3 of the Palermo Protocol:

> (a) "Trafficking in persons" shall mean the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs;
>
> (c) The recruitment, transportation, transfer, harbouring or receipt of a child for the purpose of exploitation shall be considered "trafficking in persons" even if this does not involve any of the means set forth in subparagraph (a) of this article;
>
> (d) "Child" shall mean any person under eighteen years of age.

What's notable in that definition is that 'trafficking' does not refer just to the process of moving a victim into situations of exploitation. It also includes acts such as recruitment and maintenance of a victim in a situation of exploitation. It is also important to highlight that while consent plays an important role in determining whether a sexual act with minors above the age of consent is criminal or not, it is not possible to 'consent' to HT. International human rights law has always recognized that personal freedoms cannot be alienated and therefore even if the minor has reached the age of sexual consent according to national legislation, their 'consent' to the trafficking is irrelevant. This is also underlined by the drafters of the Palermo Protocol: "once it is established that deception, coercion, force or other prohibited means were used, consent is irrelevant and cannot be used as a defence."[88] The same definitions are used in the 2005 Council of Europe **Convention on Action against Trafficking in Human Beings** as well as in the EU's **Directive 2011/36/EU of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims**. Both instruments go beyond the minimum standards in the UN Convention and Protocols and strengthen the protection afforded to victims.

An important principle with respect to the treatment of victims of HT that has become an international standard, is the *principle of non-punishment*. It is not included in the Palermo Protocol but Article 26 of the CoE Convention on Action against Trafficking in Human Beings states:

[88] Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime and the Protocols Thereto (United Nations publication, Sales No. E.05.V.2), p. 270.

> Each Party shall, in accordance with the basic principles of its legal system, provide for the possibility of not imposing penalties on victims for their involvement in unlawful activities, to the extent that they have been compelled to do so.

Directive 2011/36/EU also has a non-punishment provision in Article 8, which reads:

> Member States shall, in accordance with the basic principles of their legal systems, take the necessary measures to ensure that competent national authorities are entitled not to prosecute or impose penalties on victims of trafficking in human beings for their involvement in criminal activities which they have been compelled to commit as a direct consequence of being subjected to any of the acts referred to in Article 2.

Unlike the CoE Convention, which applies only with regards to the imposing of penalties, the Directive also envisions the option for national authorities not to prosecute the victim in the first place. The principle of non-punishment is especially important to ensure victims are not afraid to seek help from authorities out for fear of prosecution for crimes they have been compelled to commit as a direct consequence of their trafficking situation.

Recommendation for the game: The game should, if possible, highlight that victims of human trafficking, who have been compelled to commit crimes due to their situation, will not be punished for their actions (at least in Europe).

With regards to child trafficking in particular, the Palermo Protocol sets a lower standard for what could qualify as the crime by removing the requirement for the act to be executed "by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits". In addition, there are international instruments that include some specific provisions concerning the HT of children.

The CRC and the **Optional Protocol on the Sale of Children, Child Prostitution, and Child Pornography**, prohibit trafficking in children for any purpose, including for exploitive and forced labour. Article 39 of the CRC requires State Parties to "take all appropriate measures to promote physical and psychological recovery and social reintegration of a child victim of: any form of neglect, exploitation, or abuse", while the Optional Protocol specifies particular forms of protection and assistance to be made available to child victims. All of these international instruments contribute to the relatively uniform regulation of HT, and child trafficking in particular, around the world. This unification in regulation is necessary due to the transnational character of human trafficking which requires coordinated response from national law enforcement (see Section 1.5).

Recommendation for the game: The game should, if possible, highlight that human trafficking is criminalised in the same way throughout the world and that international cooperation efforts exist to ensure offenders from abroad are brought to justice.

3.3. How is online grooming for human trafficking regulated in the countries in focus?

National legislation on human trafficking in the interviewed countries is based on the international standard set by the Palermo Protocol. Provisions usually envision more severe punishment for child trafficking and do not require that it be committed through forceful or deceitful means. With respect to online grooming for the purposes of human trafficking, almost all respondents replied that it is punishable under their criminal system. Only the respondent from **Mexico** highlighted that the *General Law to Prevent, Punish and to Eradicate Crimes of Human Trafficking and the Protection and Support for Victims of said Crimes* does not include any reference to the facilitation of human trafficking crimes through electronic means, which creates problems for the prosecution of such acts in practice.

Nonetheless, there are different approaches as to the qualification of online grooming for the purposes of human trafficking. In most of the countries in focus, such acts are not regulated separately from human trafficking. This is the case in **Brazil, Bulgaria, China, Czech Republic, Germany, Greece, Latvia, Portugal, Romania, Russia, Slovakia, Spain, South Africa, The Netherlands, United Kingdom**. Respondents from these countries most often replied that online grooming for the purposes of HT would be qualified as "recruitment". Depending on the case, the perpetrator could also be prosecuted for attempt for human trafficking, or as an accomplice to the crime.

Recommendation for the game: The game should, if possible, clarify that even acts that seem 'less serious' than transporting and holding people hostage for human trafficking, such as helping in the online recruitment process, can be punished as human trafficking.

Most countries also highlighted that the online grooming provisions in national legislation cover only grooming for the purposes of engaging in certain types of sexual offences. Therefore, if the purpose of the grooming is to recruit the victim for HT and exploit them sexually with or for other people, the act would be qualified as human trafficking not online grooming. Naturally, however, the qualification of the crime would depend on the evidence on the case regarding the purpose of the grooming. Several of the respondents noted that it would be up to the prosecutor to determine under which crime to prosecute the groomer, but whenever possible, HT would be preferred as the more serious crime.

Some countries have special legislation that makes online grooming of minors for the purposes for human trafficking punishable as a separate crime, even if does not have the necessary elements to be qualified for human trafficking. This is the case in **Estonia**, which has one general provision for human trafficking and one with respect to minors:

- *§ 133. Trafficking in human beings* (1) Placing a person, for the purpose of gaining economic benefits or without it, in a situation where he or she is forced to marry, work under unusual conditions, engage in prostitution, beg, commit a criminal offence or perform other disagreeable duties, and keeping a person in such situation, if such act is performed through deprivation of liberty, violence, deceit, threatening to cause damage, by taking advantage of dependence on another person, helpless or vulnerable situation of the person, is punishable by one to seven years' imprisonment. (2) The same act if: 2) committed against a person of less than eighteen years of age; is punishable by three to fifteen years' imprisonment.

- *§ 175. Human trafficking with respect to minors* (1) Influencing of a person of less than eighteen years of age, for the purpose of gaining economic benefits or without it, in order to cause him or her to commence or continue engagement in prostitution or commission of criminal offences, work under unusual conditions, beg or marry against his or her will or appear in pornographic or erotic performances or works *if it does not contain the necessary elements of an offence provided for in § 133 of this Code*, and aiding in other manner in the activities specified in this section of a person of less than eighteen years of age, is punishable by two to ten years' imprisonment.

The Estonian respondent clarifies that under § 175 Estonian criminal code, the act is considered committed with the act of *influencing*, not when the minor is actually proceeding with any acts mentioned under § 175. The provision itself clarifies that it is applicable only if the act "does not contain the necessary elements of an offence provided for in § 133".

In **Belgium**, online grooming for the purpose of HT could also fall under the qualification of "cyber luring" if it does not meet the criteria of the human trafficking crime. Cyber luring criminalises any communication of an adult with an apparent or probable minor by means of ICT to facilitate the commission of a crime or misdemeanour against this minor while (i) concealing or lying about his identity, age, or capacity; (ii) emphasizing the confidential nature of the conversation; (iii) offering or holding up the prospect of a gift or other advantage or (iv) tricking the minor in any other way. [89] These acts could cover the beginning stages of human trafficking recruitment as described in Section 3.1.

Therefore, in **Belgium** and **Estonia** online grooming for the purposes of human trafficking can be punished as a standalone crime, even if it cannot be qualified under the human trafficking, or the general online grooming provisions.

Recommendation for the game: The game should, if possible, make it clear that the online grooming for the purpose of human trafficking is punishable in itself, even if the human trafficking does not take place.

In the **USA**, 18 U.S.C. § 2422 (b) of the U.S. Criminal Code is the federal enticement statute that criminalizes online grooming. It reads:

> (b) Whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title and imprisoned not less than 10 years or for life.

The USA gave an example of the applicability of Statue 18 U.S.C. § 2422 with a case where a man was prosecuted for his role in recruiting minors online and enticing them to engage in prostitution. The defendants in the case arranged dates for underage girls and supplied them with condoms to use on the dates.[90] The USA respondent noted that such cases demonstrate that online grooming of minors for the purpose of sex trafficking is punishable under Statue 18 U.S.C. § 2422, regardless of whether human trafficking was followed. This approach is different than the one in most European countries,

[89] Article 433bis/1 of the Belgian Criminal Code.
[90] UNITED STATES of America, v. Justin EVANS, 06-10907.

where a stricter distinction is made between the crime of online grooming and online recruitment for human trafficking.

On a state level, the USA respondent noted that some jurisdictions have recently expanded their definitions of trafficking to specifically include facilitation (both online and offline). For example, Hawaii's Sex Trafficking Law criminalizes the act of aiding or facilitating sex trafficking of a child. In Missouri and Oklahoma there are laws that include in the definition of trafficking for the purposes of sexual exploitation the act of "advertising the availability." That means that people who advertise on posters, websites and apps can be prosecuted in the same manner as those perpetrators actually trafficking. In other words, offenders could be punished for passive recruitment, even without proactively contacting and grooming their victim.

With respect to the relevance of age, the HT provisions in national legislation are more uniform and straightforward than the online grooming ones. The Palermo Protocol sets the standard by defining as a child for the purposes of human trafficking anyone under 18. If the victim is a child, then normally more severe sanctions apply and the threshold for committing the act is lower.

There are no specific rules in the interviewed countries that limit the criminal responsibility online actions facilitating HT of minors. The respondents clarified that the normal rules under the juvenile justice system would apply (see Section 1.1. and Section 1.2.). In countries like **Russia** and **China**, which have different ages of minimum criminal responsibility depending on the crime, the age of MACR for human trafficking offences is lowered from 16 to 14 years of age. Several respondents, including those from **Bulgaria, Estonia, Latvia, Germany, Portugal**, and **Romania**, however, highlighted that minors are either never or very rarely prosecuted for this crime in practice. The respondent from **Latvia** confirmed that even though the country prosecutes persons for trafficking in human beings every year, national experts could not cite any examples where minors were involved or punished for this offense. In **Romania**, minors can in theory be punished under the general human trafficking crime but only adults can commit the specialised crime under Article 222 of the Romanian Criminal Code, *Recruitment of minors for sexual purposes.*

Even though most respondents replied that their countries do not prosecute minors for acts of facilitating human trafficking, that does not imply that there are not minor offenders in practice. The respondents from **Brazil** highlighted that while they did not find instances of minors being effectively convicted of these charges, that could be due to the fact that the court proceedings in such cases usually occur in secrecy to protect the minor offender and victim (minor groomers are more likely to target other minors). Given that protection of privacy is a main principle of juvenile justice, this is an important observation that brings attention to the fact that many of the cases regarding cybercrime by minors remain out of the public eye. This fact therefore can create a false sense that such crimes do not occur at all. The respondent from **China,** for instance, confirmed that human traffickers in his country are usually middle-aged or older persons. Nonetheless, he reported of a recent case in which young females were involved in facilitating human trafficking by recruiting their young female friends for prostitution. The respondent from the **UK** also gave an example of a girl below the age of 18 who became affiliated with a gang which recruited, trained, and transported teenage girls around the UK in order to engage in refund frauds by using fake barcodes and receipts. She was charged under the Modern Slavery Act with the HT offence "conspiracy to arrange or facilitate travel or another person with a view to exploitation."

Recommendation for the game: The game should, if possible, include a scenario where a minor victim is being targeted or recruited by another minor, including a friend or a schoolmate.

Our respondents from **Spain** highlighted that in most cases where HT networks use a minor as a "hook" for the recruitment of another minor, he or she has usually been recruited before. This is an important remark because of the non-punishment principle for victims of human trafficking. As explained above, the principle states that victims cannot be detained, charged, or prosecuted as perpetrators of crimes as long as they are a direct consequence of their trafficking situation. In other words, minors that are above MACR who become involved in online grooming for the purposes of human trafficking because they are compelled to do so by their trafficker, are offered additional protection to ensure they will not be prosecuted for their actions.

3.4. Recommendations for the RAYUELA serious game:

The recommendations of this section are the following:

- Include scenarios that include the two main types of online grooming for the purposes of human trafficking used by predators on social media: online relationship recruitment ("boyfriending"/"lover boys"/"Romeo pimps") and online fake or deceptive job recruitment (e.g., someone is looking for models for an advertising agency, or proposing an easy way to make money);
- The game should, if possible, demonstrate the ways traffickers operate to gain the trust of their victims and entrap them (i.e., from engaging in intimate conversations, making compliments, or pretending to be friends, to then asking the victim for intimate photos or participation in live streams, to blackmail and creation of feelings of isolation and hopelessness);
- The game should, if possible, inform minors about ways to stop communication with the groomer and signal parents/authorities;
- The game should, if possible, highlight that victims of human trafficking, who have been compelled to commit crimes due to their situation, will not be punished for their actions (at least in Europe);
- The game should, if possible, highlight that human trafficking is criminalised in the same way throughout the world and that international cooperation efforts exist to ensure offenders from abroad are brought to justice;
- The game should, if possible, clarify that even acts that seem less serious than transporting and holding people hostage for human trafficking, such as helping in the online recruitment process, can be punished as human trafficking;
- The game should, if possible, make it clear that the online grooming for the purpose of human trafficking is punishable in itself even if the human trafficking does not take place;
- The game should, if possible, include a scenario where a minor victim is being targeted or recruited by another minor, including a friend or a schoolmate.

4. Cyberbullying and minors

4.1. Introduction: what is cyberbullying?

Cyberbullying (further also referred to as: CB) is a broad term that may include a variety of behaviour of bullying behaviours online. This includes but is not limited to cyber stalking and cyber harassment. Cyberbullying may also have a sexual component.

A 2016 study for LIBE Committee on "Cyberbullying among young people" [1] provides an interesting overview of all the behaviours that may be caught under the CB umbrella:[91]

Behaviour	Definition
Exclusion	The rejection of a person from an online group provoking his/her social marginalization and exclusion
Online harassment	The repetition of harassment behaviours on the net, including insults, mocking, slander, menacing chain messages, denigrations, name calling, gossiping, abusive or hate-related behaviours. Harassment differs from nuisance in light of its frequency. It can also be featured as sexual harassment if it includes the spreading of sexual rumours, or the commenting of the body, appearance, sex, gender of an individual
Griefing	The harassment of someone in a cyber-game or virtual word
Flaming	The online sending of violent or vulgar messages. It is different from harassment because flaming is an online fight featured by anger and violence (e.g., use of capital letter or images to make their point)
Trolling	The persistent abusive comments on a website
Cyberstalking	Involves continual threatening and sending of rude messages
Cyber-persecution	Continuous and repetitive harassment, denigration, insulting, and threats

[91] Cyberbullying among young people (study for the LIBE committee), available at https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf

Masquerade	A situation where a bully creates a fake identity to harass someone else
Impersonation	The impersonation of someone else to send malicious messages, as well as the breaking into someone's account to send messages, or like posts that will cause embarrassment or damage to the person's reputation and affect his/her social life
Fraping	The changing of details on someone's social network page when they leave it open (e.g., changing the person's political views into something extreme).
Catfishing	Occurs when someone steals you're the child's online identity to recreate social networking profiles for deceptive purposes
Outing	Occurs when personal and private information, pictures, or videos about someone are shared publicly without permission
Dissing	Occurs when someone uploads cruel information, photos or videos of children online
Tricking	Occurs when someone tricks someone else into revealing secrets or embarrassing information, which is then shared online
Grooming	Befriending and establishing an emotional connection with a child, and sometimes the family, to lower the child's inhibitions for child sexual abuse.
Sexting	The circulation of sexualized images via mobile phones or the internet without a person's consent
Sexcasting	Is similar to sexting but it involves high-definition videos of sexually explicit content
Happy slapping	Aggressive or degrading behaviour conducted and recorded by a bystander and the video is then forwarded to other people's phones or posted on a website
Threats	To damage existing relationships, threats to family, threats to home environment, threat of physical violence; death threats

The above list illustrates how broad the concept of cyberbullying may be and how many behaviours may be linked to it.

Generally, the following characterizing elements emerge when looking at the literature and the above behaviours:[92]

- **The use of electronic or digital means;**
- **To cause intentional harm;**
- Often with **an imbalance of power** (difficulty for the victim to defend itself);
- Of a **repetitive** nature, however including the fact that sharing something once online may lead to resharing, and re-use, causing repetitive harm, even without repetition of the harmful act;
- With a **sense of anonymity/lack of accountability** (e.g., the feeling of an online world where the consequences are not the same as in the 'real' world; and
- An added measure of **publicity,** e.g., the fact that online bullying is after very visible to others and may reach a much larger audience.

In particular the public nature of the internet and the related possibility for a single act to cause repetitive effects, combined with the sense of anonymity and lack of accountability present a dangerous environment for minors to become victim of CB, but also to become an offender. Cyberbullying is moreover something that can easily multiply (offenders from anywhere may join in) and can happen 24/7 (as opposed to traditional bullying in a school environment). In addition, the inability to see the victim's reaction and the immediate damage of the bully's actions may be another stimulant towards CB behaviours. D1.3 describes this as the "online shield". See also D1.3 for more details on CB behaviour and takeaways for the RAYUELA game.

In D1.5, the following behaviours were mentioned as included in the analysed sample of cyberbullying cases, mostly focused on cases where the offenders were minors:

- Flaming
- Online harassment
- Social exclusion
- Stalking
- Denigration
- Masquerading
- Outing
- Happy slapping
- Trickery

By far the most common behaviours were flaming and outing. Online harassment was also common. It was also found in D1.5 that in particular CB tended to no include false information or coercion, but does often include sexually explicit content. Another interesting point made in D1.5 is that cyberbullying often happens in group.

[92] See also Cyberbullying among young people (study for the LIBE committee), p. 23-24 and references, available at https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf

There is no single accepted definition of cyberbullying, let alone a common legal definition.[93] While some EU countries have an official definition of cyberbullying as a phenomenon, cyberbullying is not caught by a specific provision in criminal codes. This is because its encompasses such a broad range of potential behaviours that it would be difficult to regulate the phenomenon as such, in all its diversity.

For that reason, from a legal point of view, cyberbullying is regulated through specific behaviours that are punishable in a given country.

Typical criminal qualifications that may apply are:

- Harassment/bullying;
- Violence/fear of violence;
- Threats;
- Insults;
- Defamation & Slander;
- Stalking/ Online stalking / Cyber Stalking;
- Blackmail, extortion;
- Coercion;
- CSAM provisions, when sexually explicit content depicting a minor is involved.

This approach leaves the opportunity for gaps, as new cyberbullying behaviours may not be caught by existing qualifications under national criminal law, especially when applicable provisions are decades old and aimed at a pre-internet reality. Some respondents have argued that such gaps in protection exist.

A specific issue in terms of protection is the scenario where the cumulative effects of many acts of bullying by different bullies in itself may not amount to something that is sufficient to be caught under the existing qualifications of the criminal code, but may lead to serious damage for the victim. Moreover, even if some behaviours would meet the threshold of a qualification under the criminal code, having to prosecute many offenders, which would often also be minors, is not an evident undertaking. Both the respondents for **China** and **Estonia** mentioned severe cases of cyberbullying where the victim ended up committing suicide, yet no charges were ever brought against any of the bullies.

The game should, if possible, highlight the cumulative effect of online bullying behaviour, even if the individual contribution is small (and too small to meet the threshold of constituting an offence).

Because CB is such a broad phenomenon, it must be understood that the answers of the respondents are not to be regarded as exhaustive. Because CB is such a broad phenomenon it is easy to overlook a possible qualification. Hence, it is not because, for example, a respondent fails to highlight sexual offences as part of CB, that these are not covered in the country in focus, but this may perhaps rather mean that these sexual offences were not considered by the respondent as cyberbullying, but rather as self-standing sexual offences. The same goes for other qualifications. Threat for example, is a commonly found crime, but it may be considered that a serious one-off threat is not a form of bullying,

[93] For more details on existing definitions, please see: Cyberbullying among young people (study for the LIBE committee), p. 21 and further, available at https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf

which tends to require a continuous pattern of behaviour intended to annoy, hurt or otherwise harm the victim, but rather simply a punishable threat. However, in what follows, the answers of the different respondents and the interesting trends that could be identified will be discussed.

4.2. How is Cyberbullying regulated in the countries in focus?

The respondent for **Belgium** noted that under Belgian law both the classical offence of stalking and a specific online stalking offence could apply to the situation of CB.

Classical stalking (Art. 442bis Criminal Code), on the one hand, exists when the perpetrator knew or should have known that their behaviour would seriously disturb the victim's peace and quiet and affect their privacy. Usually, persistent and recurring behaviour is required to establish such an offence, but the Belgian supreme court has accepted in a case concerning the online publication of a video, that also a single act of conduct which has unwavering or recurrent consequences which seriously affects someone's privacy, may constitute the criminal offence of stalking.

Online stalking (Art. 145 §3bis Act on Electronic Communication), on the other hand, is the use of electronic communication network or service or other electronic communication means to cause nuisance to his correspondent or to cause damage. In this case once act may expressly suffice, and repetition of the behaviour is not typically required. A case is mentioned where the online stalking offence was committed by a psychologist who copied a telephone number of a minor from his file and used it to incite the minor to perform sexual acts.

In addition, for bullying that takes place in a public forum, the respondent mentioned the following relevant offences:

- Hate speech;
- Sexism;
- Slander and defamation (Art. 443);
- Insult (Art. 448, when the accusation affecting the dignity of the person is vague in nature);

In addition, other offences that may apply depending on the circumstances are:

- Threatening behaviour;
- Violence, harassment and sexual harassment in a professional context;
- Other specific sexual offences, depending on the harassment strategy.

Minors may be prosecuted for these offences in Belgium, applying the general regime for juvenile offenders.

The respondent for **Bulgaria** mentioned in particular the offences of threat (Art. 144), stalking (Art. 144a) and coercion/blackmail (Art. 214). For threat and stalking, there is a need to create a well-founded fear in the victim. Coercion exists when someone is compelled to do something by force or threat and this inflicts material damage.

Minors may be prosecuted in Bulgaria under the general rules applicable to juvenile offenders, despite a lack of actual prosecution in practice.

For the **Czech Republic**, the mentioned offences were:

- Extortion (Section 175)
- Infringement of Rights of Another (Section 181)
- Defamation (Section 184)
- Dangerous Threatening (Section 353; threat, creating reasonable fear)
- Dangerous Pursuing (Section 354)

The extortion, defamation and threat offences are rather straightforward and typical offences cited in the context of CB. The dangerous pursuing offence is a stalking offence. One of the possible scenarios includes seeking persistent contact through electronic means or abusing personal data for the purpose of gaining contact. When this behaviour is capable of raising reasonable fear for the victim's life or health or lives or health of persons close to them this is punishable.

Of particular interest is the mention of an offence in section 181 of the Czech Criminal Code relating to the infringement of rights of another. If someone misleads another person or uses their mistakes against them causing serious detriment to the victim's rights, this person is punishable by law. The respondent mentioned the relevance of this in a CB context. Another interesting example mentioned is section 183, which punishes the making available of files and private documents of a person to third parties, which is of obvious relevance to the CB context where photos or videos may be shared without the consent of the person depicted.

Minors may be prosecuted in the Czech Republic under the general rules applicable to juvenile offenders, meaning they cannot be punished but various forms of measures can be imposed.

The respondent for **Estonia** mentioned that most forms of CB were civil in nature and not criminalized and that these are not really prosecuted in practice. Mentioned as potentially relevant however were:

- §217 Illegal obtaining of access to computer systems (e.g., hacking to obtain access to another's computer and/or accounts);
- §153.1 Sexual harassment;
- §157.3 Harassing pursuit (a stalking offence, punishable if the intent or effect of the repeated or consistent stalking is to intimidate, humiliate or disturb the person);
- §157.2 Illegal use of another's identity (fake accounts for example).

An important note was that the sexual harassment crime in Estonia focuses on physical contact, which may mean that online sexual harassment in the context of CB would be potentially difficult. As stated above, the respondent for Estonia also mentioned two cases about CB, committed in particular by minors, which lead to the suicide of the victim (in one case a middle-aged man, in the other a 19-year-old), which were not able to be addressed, despite the horrifying results.

Minors may be prosecuted in Estonia under the general rules applicable to juvenile offenders, despite a lack of actual prosecution in practice.

For **Germany**, our respondent mentioned in particular the following crimes as relevant to the CB context:

- Stalking (§ 238 StGB including online stalking);
- Threat (§ 241StG, threatening the victim with a serious offence against them);
- Insult (§ 185 StGB, verbal harassment);
- Malicious gossip and defamation (§ 186 and 187 StGB)

- Sexual abuse of children without physical contact with the child (§ 176a StGB, e.g., sending pornographic photos).
- Violation of intimate privacy/personality rights by taking photos or other images (§201a StGB)

Stalking is understood in Germany as the crime where the offender seriously restricts the victim's lifestyle by stalking that person, e.g., by contracting that person by electronic means, improperly using the victim's personal data, threating the person, stealing their data, spreading pictures, sharing content that is apt to degrade the victim or negatively affect public opinion about the victim or by committing comparable acts.

In relation to the crime of insult/verbal harassment the respondent makes note of the particular challenge of balancing the right to freedom of speech with the personality and honour rights.

The respondent mentions two interesting cases. In one case, the offender started stalking his former employer and landlord after the latter had terminated tenancy and the working contract. Inter alia, the offender regularly wrote degrading and threatening posts on a website. The court found the offender guilty of insult (§ 185 StGB), threat (§ 241StG) and stalking (§ 238 StGB) at the same time.

In another case, a juvenile offender had insulted and threatened his (minor) victims via Facebook and WhatsApp and had even urged one of them to produce a video while masturbating, which the perpetrator posted on Facebook afterwards. The court made use of the full spectrum of juvenile criminal law sanctions. It not only imposed a youth prison sentence of two years (which was suspended on probation), but also a youth detention of 4 weeks and the obligation to start a sexual therapy, to pay a compensation for pain and suffering of 1500 Euro to two of his victims and –especially interesting – to delete his accounts on Facebook, WhatsApp and Instagram and to refrain from using these services for six months.

Minors may generally be prosecuted in Germany for CB offences, under the rules applicable to juvenile offenders.

In **Greece**, our respondents mentioned in particular the crime of bullying (of minors) (Art. 308-312 criminal code, Art. 308 "Bodily Injury", Art. 309 "Dangerous Bodily Injury", Art. 310 "Severe Bodily Injury", Art. 311 "Fatal Bodily Injury", Art. 312 "Bodily Injury of Weak Individuals"). The crimes covered by these Articles exist when mental or physical injury is administered through continuous cruel behaviour. The crime exists against adults (Art. 308) and against minors or weak persons in particular (Art. 312) and with different aggravating circumstances/escalations The crime seems to refer initially to bodily injury but according to respondents also clearly covers mental injury, although the threshold would be high, requiring serious mental harm. Respondents explain that this can be the case where there is continuous harassment, embarrassment, humiliation, threats or other forms of serious cyberbullying or cyber harassment. One respondent notes that prior to July 1st, 2019 the then article 312 of the Penal Code titled "Causing damage with constant harsh behaviour" essentially concerned the criminal act of "Bullying" with certain provisions, however, the lawmaker in the amended article 312 changed the title to include not only minors but weak individuals in general as well, and also to include acts of domestic violence (law no 3500/2006). The current Article 312 hence covers situations of CB but also other situations. The pervious Article 312 state that if the act is committed between minors, it remains without punishment unless the age difference is more than 3 years. This is no longer applicable to the current Art. 312, which hence covers CB more comprehensively.

Other qualifications that are mentioned by the respondents are:

- Threat (Art. 333)
- Insult (Art. 361)
- Defamation (Articles 362-363)
- Criminal penalties under data protection law (Art. 38 of Law No 4624/2019 "Privacy - Protection of Personal Data")

This last mention is of particular interest, as the Greek respondents were the only ones to mention data protection law applicable to an individual acting in a household-exception-like situation. Art. 38 of the Greek implementation of EU data protection law punishes anyone who without legal ground interferes in filing systems and becomes aware of data, processes data in any way without legal ground or shares it with third parties/publishes data. This Article could come into play easily in CB scenarios, e.g. where personal details or images/videos containing such details are processed and shared without legal ground and against the will of the data subject/the person depicted. One respondent mentioned a case in which a female minor was prosecuted and convicted for continuous violation of article 38§2 L.4624/2019 (Personal Data Protection) and serial and continuous Insult through Internet with Racist Characteristics in violation of articles 1, 12, 14, 16, 17, 18, 19, 26, 27 par. 1, 79, 82A, 94 par. 1, 98 par. 1, 121-126, **361** par. 1 (Insult), and 368 par. 1 of the new Greek Penal Code. The court decided to impose the reformation measure of being supervised under Juvenile Curator.

Minors may be prosecuted in Greece under the general rules applicable to juvenile offenders.

The respondent for **Latvia** mentioned in particular section 132 of the Latvian Criminal Code (persecution), which is a stalking offence where repeated or lasting tracking and surveillance of another person, expressing threats to such person, or unsolicited communication with such person is punished if that person has had reasonable grounds to fear for his or her safety or the safety of his or her relatives.

The respondent also mentions administrative sanctions that can be imposed in the context of CB on the basis of the law on protection on children rights in Latvia. Sanctions can be imposed for emotional abuse or violence against a child and sanctions may also apply to minors if they have reached the age of fourteen (14).

Minors may be prosecuted in Latvia under the general rules applicable to juvenile offenders, despite a lack of cases in practice. Administrative sanctions may also apply to juvenile offenders.

The respondents for **Portugal** mentioned a number of offences that may apply in a CB context, namely:

- Threat (Article 153)
- Coercion (Article 154)
- Persecution/stalking (Article 154A), if the behaviour directly or indirectly is adequate to provoke fear or uneasiness or to harm the victim's freedom of determination
- Defamation (Article 180)
- Injury (Article 181)
- Publicity and Slander (Art. 183)
- Devastation of private life/invasion of privacy (Article 192)
- Devastation by means of information technology (Article 193)
- Breach of correspondence or telecommunications (Article 194)

- Illegal recordings and photographs (Article 199, concerns the making and use of photo or recordings without consent)
- Discrimination and incitement to hatred and violence (Article 240)
- Computer forgery (Art. 3 of the Cybercrime law 109/2019)
- Illegal access (Art. 6 of the Cybercrime law 109/2019)

The devastation crimes are worth highlighting and relate to constitutional protection of privacy. Article 192 of the criminal law punishes anyone who records or transmits conversations, captures images, or discloses facts relating to the private life of other people. This is a common provision to be found in the law of EU countries, as is the protection of secrecy of correspondence and communications (Article 194). More unique is Article 193, which relates to the creation and use of files of sensitive personal data, e.g., relating to political, religious or philosophical beliefs, party or trade union affiliation, private life, or ethnic origin. Creating databases of such data is in itself an offence that may be punishable.

One respondent notes that there is ongoing discussion as to whether a specific cyberbullying offence needs to be added to the criminal code to adequately cover the phenomenon.

Minors may be prosecuted in Portugal under the general rules applicable to juvenile offenders.

For **Romania** the correspondent mentioned harassment (Art. 208 of the criminal code), a type of stalking offence, as the main Article of relevance. In the context of CB, harassment may exist in particular when someone causes a state of fear to an individual through the frequency or content of the online communication (attempts).

Minors may be prosecuted for harassment in Romania under the general rules applicable to juvenile offenders.

The respondent for **Slovakia** mentioned a specific online stalking crime. The online stalking crime fits the CB scenario very well. It punishes anyone who for a long time online humiliates or intimidates someone (impairing their quality of life), or otherwise acts unlawfully or unlawfully publishes pictures, sound, video etc. without the consent of the person depicted, if this seriously endangers the victim or causes other serious harm to rights. The offence can be committed by people over 14 years old and has stricter sentences if committed against a minor. The respondent also mentioned in the interview that other qualifications may apply such as extortion, slander and threat.

Minors may be prosecuted in Slovakia under the general rules applicable to juvenile offenders.

The respondent for **Spain** mentioned the following qualifications as relevant to CB:

- Inducement to suicide (Article 143);
- Injury (Articles 147 to 156);
- Threats or coercion (Articles 169 to 172);
- Stalking or harassment (Article 172 ter), for this offence it is required that the stalking seriously impairs the daily life of the victim;
- Offence against moral integrity (Article 173.1), an offence that punishes degrading treatment;
- Sexual assault and sexual abuse (Article 178 to 183);
- Sexual harassment (Article 184);
- Offences against the privacy (of minors) (Article 197), a provision on privacy and secrecy of communications;

- Knowingly possessing or accessing material or child pornography (Article 189.5);
- Slander and libel (Article 205 to 210).

Under Spanish law, minors may be prosecuted for CB offences, under the Spanish juvenile regime. The Respondent indicates that this could mainly happen for Article 173.1 (against moral integrity) or the cyberstalking behaviour in Article 172 ter of Criminal Code.

The respondent mentions that the main characteristics of this type of crime are the following:

- It can be proven that, because of the acts, a serious impairment of the victim's moral integrity had occurred (which can take the form of a worsening of schooling, psychological assistance, unjustified absences from class, etc.);
- That there is a reiterated action through different forms of bullying or harassment. There is no minimum number of actions but there is a requirement that the acts must be spread over time. This excludes isolated behaviour;
- This behaviour causes a serious disruption of the victim´s daily life.

For CB to be punishes, there is no need for a physical component.

Regarding the **Netherlands**, our respondent mentioned in particular:

- Stalking (which includes both physical and cyberstalking (art. 285b Dutch Criminal Code) this offence covers the systematic intentional infringement of someone's privacy, with the aim to force the person to do (or not do) or undergo something or to induce fear. The offence can be prosecuted only upon complaint of the victim. The infringement of privacy does not have to be particularly serious; it suffices if there is an infringement, but behaviour must be systematic;
- Harassment (Art. 284 DCC): without right forcing someone to do (or not do) or undergo something, using violence or some other factual circumstance, or the threat of violence or of another factual circumstance, against the victim or a third person, or by threatening with defamation;
- Sexual harassment (Art. 246 DCC);
- Discrimination (Art. 137c and following DCC); e.g., publicly offending a group (art. 137c) or making public a statement that offends a group (art. 137e) because of their race, religion, physical or mental impairment, or sexual orientation;
- Doxing: proposed art. 285d DCC: doxing is not yet criminalized as such, but a Bill is being prepared to make doxing as a specific criminal offence. A draft published for consultation mid-2021 defined this offence as procuring, spreading, or making available personal data about someone with the aim of inducing fear in that person or seriously hindering him or her. This is a specific form of CB.

In the interview the respondent also mentioned Articles 240 para. 2 or 240a Criminal Code (sending indecent images and sending indecent images to minors) and Article 139h para 2 b (revenge porn, making images public with a broad definition of what public means).

Under Dutch law, minors may be prosecuted for acts of CB, applying the juvenile system.

Regarding CB in **Brazil**, the respondent explained the country's Program to Combat Systematic Intimidation (Bullying), which includes and defines cyberbullying as "systematic intimidation on the world wide web, when using its own instruments to disparage, incite violence, adulterate photos and

personal data in order to create means of psychosocial embarrassment." The respondent indicates that bullying, if in the form of a threat, constitutes a crime provided for in Article 147 of the Brazilian Criminal Code.

Also mentioned in the context of CB are in particular the following:

- Stalking (Article 147-A), this may include cyberstalking and is present when there is a conduct of persecuting someone, repeatedly and by any means, threatening their physical or psychological integrity, restricting their ability to move around or, in any way, invading or disturbing their sphere of freedom or privacy;
- Slander (Article 138);
- Defamation (Article 139);
- Insult (Article 140).

Under Brazilian law, minors may be prosecuted for these offences, however applying the different provisions applicable to the prosecution of minors. The respondent also noted that The Superior Court of Justice in Brazil recognizes that schools have a duty to guard and preserve the integrity of its students and must take preventive action to avoid damage or offenses to students, including cyberbullying.

For **China** our respondent mentioned that CB could be punished under many laws and regulations, depending on the circumstances.

The Chinese respondent also mentioned in particular the following case, showing gaps in protection in terms of CB, especially when many bullies operate at the same time, without one being clearly identified as an instigator or main bully:

The case concerns a minor who was the victim of human trafficking (he was sold as a child) and was from December 14, 2021 to January 24, 2022 searching for his biological parents. Having found them he subsequently broke out in conflict with them as he had asked them if he could live with them, or to buy or rent a home for him as he did not have one of his own. The minor alleged that his parents cut him off instead, with his mother even blocking him on messaging platform WeChat. His parents disputed this, with his mother saying he tried to force her into buying him a home, which she could not afford. News sources at the time wrote articles implying that the minor was a "human tragedy" and destroyed his biological mother's "normal life", was a "White Eyed Wolf" (i.e. a vicious person), etc. The teenager was then reportedly cyberbullied, with many saying that he had only wanted a house from his parents and that he was trying to gain sympathy. In the end the minor committed suicide. The incident has attracted official attention and prompted Chinese online platforms to advance measures to prevent cyberbullying However, no person has ever been investigated or punished for the wrongdoing.

Important to note in this context is the respondent's mention of the fact that in the State Internet Information Office is drafting "Regulations on the Protection of Minors on the Internet" as a comprehensive document to motivate fellow minors, families, and diverse institutions (educational, telecommunications, public security, civil affairs, culture and tourism, health, market supervision and management, radio and television institutions) to protect minors. It is the extension of the Chinese idea of the so-called "comprehensive governance of social order" into cyberspace.

In terms of criminal liability then, the respondent mentioned in particular the crime of defamation and the crime of "picking troubles and provoking trouble" as being of main relevance to the CB context.

This last crime is of particular interest. It is crime that punishes 1) those who use information networks to abuse or intimidate others, when the circumstances are vile, and the social order is disrupted or 2) those who fabricate false information, or knowingly fabricating false information, spread it on the information network, or organize or instigate others to spread it on the information network, causing trouble and causing serious public disorder. Our respondent explained that in general the threshold is relatively low to find that a malicious act as threatens the social order. Social influence is considered when an act is committed to find whether the threshold is reached or not. For cyberbullying of ordinary classmates to reach the threshold of this crime, the situation would have to be rather extreme, e.g., if the victim were to become mentally ill, commit suicide, or the bullying would reach a nation-wide public (e.g., by coming into the press or stories going viral).

The respondent indicated that under Chinese law, minors between 14 and 18 can be prosecuted and held accountable.

For **Mexico** our respondent explained that CB situations in particular with a sexual component are covered by the crimes of sexual harassment and sexual abuse (Arts. 259 Bis, 260, 261 of the Federal Criminal Code). It was noted that issues may exist with proving damage if only online, because the provisions are not particularly adapted to the digital reality.

Concerning violence against women, and the regulation of distribution of non-consented sexual images, the Mexican government published in June 2021 a decree that reforms the *Federal Criminal Code* and the *General Law of Access for Women to a Life Free of Violence* in the Official Gazzete (Diario Oficial de la Federacion). These legal reforms arise as a result of a wide campaign of national activism from Olimpia Coral, whose former boyfriend shared and distributed sexual images and videos of her through social media when she was only 18 years old. This law is also known as the "Ley Olimpia" in honour and reference to said national female activist.

Following this a new chapter was introduced in the criminal code containing articles 199 Octies, 199 Nonies and 199 Decies of the Federal Criminal Code. These articles criminalize the conduct of sharing and distribution of sexual content without the consent of an individual and provide for specific punishments and aggravated circumstances.

In turn, the General Law of Access for Women to a Life Free of Violence punishes digital and media violence committed against women. The following should be understood under digital and media violence:

- *Digital violence is any fraudulent action carried out through the use of information and communication technologies, by which images, audio, or real or simulated videos of intimate sexual content of a person without his consent, without his approval or without his authorization are exposed, distributed, disseminated, exhibited, transmitted, commercialized and offered and that cause psychological, emotional damage, in the sphere of his private life or in his own image. As well as those malicious acts that cause damage to the intimacy, privacy and/or dignity of women, which are committed through information and communication technologies."*

- *Media violence is any act through any means of communication, which directly or indirectly promotes sexual stereotypes, makes reference to violence against women and girls, produces or allows the production and dissemination of hate speech, sexist hatred, gender discrimination or inequality between women and men, which causes psychological, sexual, physical, economic, patrimonial or femicide harm to women and girls. Media violence is exercised by any natural or legal person who uses a*

communication medium to produce and disseminate content that threatens against the self-esteem, health, integrity, freedom and security of women and girls, that prevents their development and that threatens the equality."

It should be noted that the above provisions cover most in particular sexual offences and offences against women or girls. The respondent stated that there are no particular provisions on the cybercrime of CB in Mexico, but that some other laws may apply, e.g., the law on the protection of children, although these rules are not particularly aimed at the digital realm.

The respondent indicated that minors could be prosecuted for such offences (sexual harassment and abuse), that that there is no sufficient evidence to confirm that this would happen in practice.

With regards to **Russia** our respondent mention that CB was not in particular regulate in Russia.

However, Article 110 of the criminal code could apply, which punishes the inducement to suicide (attempted suicide included) a result of threats, ill-treatment or systematic humiliation of the victim's dignity by the other person. CB may qualify as a form of such ill-treatment and systematic humiliation of the victim's dignity as the Criminal Code does not specify the particular ways and methods of inducement. Only individuals in the age over 16 years old may be subject to criminal liability under article 110 of the Criminal Code.

If the CB has sexual components, other crimes may come into play:

- Violent actions of a sexual nature in relation to a minor (article 132 (4 (b)) of the Criminal Code), some forms of sexual harassment online may be covered by this Article. Nevertheless, some actions that are practically constitute sexual cyberbullying are not punishable under the Criminal Code. This Article does not cover "jokes" of a sexual nature, rating minor users on attractiveness/sexual activity, body shaming, 'outing' someone where their individual's sexuality or gender identity, offensive or discriminatory sexual language and name calling online and other similar actions;

- Depraved Actions (article 135 of the Criminal Code), this crime may be applicable to some forms of cyberbullying in relation to minors over the age of 12 and under the age 16. For instance, it may include sending someone sexual content (images, emojis, messages), unwelcome sexual advances or requests for sexual favours and etc.;

- Violation of privacy (article 137 of the Criminal Code), this covers revenge porn and other forms of sharing of images/videos without consent.

The respondent noted that Russian law enforcement authorities pay more careful attention to crimes committed in relation to minors, especially of sexual nature.

And interesting case is mentioned in relation to the application of article 137 of the Criminal Code in regarding "revenge porn", namely on of the landmark decisions of the European Court of Human Rights ('ECtHR') Volodina v. Russia. The applicant in this case tried to break off the relationship with her partner, who had previously beaten her repeatedly, abducted her and threatened to kill her. At the same time, the applicant's account was hacked in 2016 and fake pages later appeared. A former suitor listed her real details and posted intimate photos for several years. In connection with this, a case for violation of privacy (Article 137 of the Criminal Code) was initiated in 2018, but two years later the police closed the case due to the end of the two-year limitation period. The ECtHR stated that the

Russian authorities had failed to meet their obligation to conduct an effective investigation when an arguable claim of ill-treatment had been raised not only in relation to cyberbullying, but also to more serious physical harm.

The respondent also mentioned that administrative offences may exist for insult or slander-like offences.

Under Russian law, minors may be prosecuted in practice, depending on a case-by-case assessment. Because the mentioned qualifications have a strong sexual component, the respondent mentions that this would in particular be the case when the offender is over 14 years of age and the victim is younger than 12. It can be deducted that in such cases the age difference is relevant.

For **South Africa** our respondent mentioned in particular harassment and bullying punishable under the harassment Act. It was explained that the harassment act is of a more civil nature and serves to provide relief to bullying situations. If the court order is not respected then criminal sanctions may apply, in particular for a continuous infringement under contempt of court.

Of particular relevance is also the Cybercrimes Act, which punishes the sending of malicious communications to incite damage to property or violence, to threaten persons with damage to property or violence or to unlawfully disclose intimate images.

Minors may be prosecuted for these offences. A protection from harassment order may even be issued irrespective of age.

In the **UK**, the respondent mentioned the following as key legal tools in combatting CB:

- The Public Order Act (1986), which punishes causing a person harassment, alarm or distress with intent by using: '... threatening, abusive or insulting words or behaviour, or disorderly behaviour, or displaying any writing, sign or other visible representation which is threatening, abusive or insulting. Offences under this act can be committed in both a private place and a public place and include written threats so this could in theory be extended to online harassment, but in practice the Act has tended to be applied more in offline contexts;
- The Protection from Harassment Act (1997), which defines that a criminal offence occurs where the perpetrator engages in repeated and unwarranted behaviour to the victim, causing them 'alarm or distress'. Section 1 of the Act specifically prohibits '... a course of conduct which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.' In the online context, typical behaviours could include repeated texts, voicemails, direct messages, emails, online comments or threats. For an offence to occur there must be contact on more than two occasions - though the law makes it clear that this does not have to involve the same kind of behaviour on both occasions. This would mean that if 100 people were each to send a single abusive tweet to one person, an offence would not have been committed under the 1997 Act, highlighting the issue described above already, where CB may more easily present situations where the victim is bullied by many perpetrators, each only providing a small contribution to the total damage suffered by the victim;
- The Crime and Disorder Act (1998) applies if the offences are racially or religiously aggravated;

- The Malicious Communications Act (1988) punishes communications sent with the intention of causing distress or anxiety;
- The Communications Act (2003). In turn Section 127 of the more recent Communications Act (2003) also prohibits the sending of any electronic message which is grossly offensive, indecent, obscene or has a menacing character. This includes messages sent across social media platforms like Facebook or Twitter and indeed practically any other communications medium;
- The Defamation Act (2013)

The respondent noted that online harassment and cyberstalking are criminal offences under these acts, even if bullying or cyberbullying as such is not a specific offence in the UK and most bullying incidents are not treated as crimes. Both for minors and adults, a threshold is crossed where bullying involves violence or assault; theft; harassment and intimidation over a period of time including calling someone names or threatening them, making abusive phone calls, sending abusive emails or text messages, and anything involving hate crimes. As the respondent explained, there generally is an expectation that there is a repeated harassment. Usually one instance is not enough, but two or more instances are required, normally over a long period of time. There may be issues in practice to identify such behaviour if different accounts are used by the same bully.

In addition, for minors The Education and Inspections Act (2006) is also relevant. This act provides for staff and teachers to confiscate items from pupils who may be involved in bullying, such as mobile phones. Under this legislation "All UK schools are now required to have an anti-bullying policy either under the School Standards and Framework Act 1998 or the Education (Independent Schools Standards) Regulations 2003."

In principle minors can be prosecuted for these offences and while prosecutions of minors are rare, they have occurred. The first UK case of a minor being given a custodial sentence came in 2009, when a teenage girl was jailed for cyberbullying. The girl was 18 when sentenced but had conducted a campaign of abuse against her victim for nearly four years, one which culminated in her posting a series of death threats on Facebook. As a result, she was sentenced under the Protection from Harassment Act to 3 months in a young offender's institution. This unprecedented sentence was a direct result of previous convictions against the perpetrator, one for assault when the victim was walking home, another for criminal damage when she kicked the victim's front door.

The difficulties and ambiguities in securing cyberbullying related convictions for minor was seen in another case where a 16 years old girl was arrested at school, in the middle of a lesson. Police also raided her home and confiscated her laptop and tablet. She had been accused by another girl who said she was targeting her online, making threats to 'get her' and hacking into her family's webcam. These allegations turned out to be untrue and police were forced to issue an apology for their heavy-handed (and mistaken) attempt to enforce harassment laws.

For the **USA**, our respondent explained that there is no specific law on CB on a federal level, although several federal laws prohibit sending abusive or harassing messages and other behaviours that are closely related to the CB context, such as:

- 18 U.S.C § 875 (Interstate Communications) prohibits the use of communication devices to threaten a person with injury or damage to property;

- Title 47 U.S.C § 223 (Obscene or Harassing Telephone Calls in the District of Columbia or in Interstate or Foreign Communications) forbids the use of telecommunication devices to carry out harassing behaviour, such as making, creating, soliciting, initiating requests that are obscene or that involve child sexual exploitation materials with the intent to annoy, threaten, abuse, or harass others. It is also prohibited to withhold one's identity and use these devices to annoy, abuse, threaten, or harass someone;
- 18 U.S.C. § 2261A details how interactive computer services cannot be used for any activities that cause a person to feel substantial emotional distress or places that person or their family in reasonable fear of death or serious bodily injury.

The respondent explained that although there are no specific Federal Cyber bullying laws, almost every state has legislation addressing cyberbullying, including legislation on the roles of schools to prevent bullying among minors (https://www.stopbullying.gov/resources/laws). In addition, most states have legislation on related behaviors such as cyberstalking or online harassment, or both.

Usually, such rules require to prove that a credible threat has been made, creating an actual fear or concern for safety. Another major challenge to the application of these laws, is that their enforcement must comply with the First Amendment, which imposes two key limitations on threats and harassment law: First, the "true threat" doctrine teaches that the government cannot punish threats that in context are mere advocacy or political hyperbole, as these are protected speech under the First Amendment, meaning threats can be punished only if they are "true threats." Second, another First Amendment limit on these laws may be that only incitement of illegal conduct- speech that encourages other to act, rather than suggest the speaker's intent to take action – may be punishable.

As was stated at the outset of this chapter as an expectation, the answers of the respondents were indeed varying in nature. Even assuming they were non-exhaustive it was interesting to see how certain respondents confidently presented a broad range of behaviours that may form part of the CB phenomenon, where other respondents presented a rather light legal framework.

In general, minors can be prosecuted for these CB related offences under the juvenile justice regime applicable in the given country. It is important to keep in mind that while these regimes tend to have a more reformative goal rather than mainly punitive, the fact that minors could be prosecuted should still be considered as an important deterrent. This holds true despite several respondents indicating that prosecution in practice was rare or did not happen. The RAYUELA game could protect children from becoming CB offenders, and thereby protect other children from becoming victims of CB, by teaching the player that, in general, there are legal consequences to their actions if crossing the line into a criminal behaviour, and that they may be prosecuted for such offences, which could have serious consequences (including having a (juvenile) criminal record, fines, community work, educational measures, being institutionalized), while keeping in mind ethical rules and principles to not unduly scare the players. This can only be done if appropriate examples are given of what is criminal behaviour and what is not.

Recommendation for the game: the game should, if possible, touch upon the fact that in general, the player's actions in reality have legal consequences if they cross the line into a criminal behaviour, and that they may be prosecuted for such offences, which could have serious consequences (including having a (juvenile) criminal record, fines, community work, educational measures, being

institutionalized), while keeping in mind ethical rules and principles to not unduly scare the players. It is important in this context to give appropriate examples of what is criminal behaviour and what is not.

Knowing that in the RAYUELA game, there will be a focus on online harassment, flaming and outing, it is interesting in particular to consider that these may take place in a public forum. Many respondents mentioned that in that case freedom of speech guarantees must be balanced against the protection of personality rights. This is something that could perhaps integrated in the game, as not every negative interaction or opinion is or should be punishable. Only when the statement is fundamentally untrue and can seriously affect the victim should this be punishable.

Recommendation for the game: the game should, if possible, touch upon the distinction between a negative or angry opinion or hyperbole and defamation/slander.

Similarly, the game could make a distinction between negative interactions and credible threats, which incite real fear in the victim, one being innocent and part of life, the other being a punishable behaviour.

Recommendation for the game: the game should, if possible, touch upon the distinction between negative interactions and credible threats.

Regarding online harassment and online stalking (despite both outing and flaming potentially being a part of that), most countries who mentioned stalking or online harassment offences indicated the requirement for some kind of continuity, behaviour that is repeated and of a given intensity with a continued conscious aim to hurt. Concerning stalking offences, which were one of the most repeated offences to cover the CB context, such a continued behaviour is needed. Some countries seem to require credible threats to safety or a real fear to have taken hold of the victim, where other put the bar at a serious disruption of peace & quiet or a disruption of the victim's life(style). Despite these differences the common ground seems to be that the victim's daily life must be substantially impact by the CB behaviour. It would be good if the game could distinguish between negative interactions and disagreements, dislike of one another etc. and the type of continued (almost obsessed) behaviour of persecuting someone that is stalking and continued online harassment, which goes beyond merely annoying the victim or giving them an unpleasant experience, but amounts to a continued significant disruption of their daily life.

Recommendation for the game: The game should, if possible, highlight the distinction between "normal" negative interactions or disagreements between people/minors, and the type of continued (almost obsessed) behaviour of persecuting someone constituting stalking or online harassment. The latter goes beyond merely annoying the victim or giving them an unpleasant experience but amounts to a continued significant disruption of their daily life.

Another issue that was mentioned by several respondents, but in particular the cases presented by the respondents for **Estonia** and **China**, is the issue of collective cyberbullying, where a victim is simultaneously bullied by many bullies, each contributing only a small part of the damage inflicted on the victim. This may present a real issue for persecutors and it could be interesting for the game to highlight not necessarily this issue of enforcement, but rather the issue as such, teaching the players that despite small one-off behaviours like that perhaps not amounting to a crime in itself, it may nonetheless create very real damage and is therefore not innocent.

Recommendation for the game: The game should, if possible, highlight the cumulative effect of online bullying behaviours, even if the individual contribution is small (and too small to meet the threshold of constituting an offence).

A last issue, which was mentioned by several respondents, both in relation to crime by minors in general and in relation to CB is the issue of underreporting of crimes by victims, which leads to the conclusion that lots of CB goes unpunished. This could also be introduced in the game as a specific aspect of relevance.

Recommendation for the game: The game should, if possible, highlight the issue of underreporting of CB offences, which causes bullies to get away unpunished, victims to not get the help and support they need, and the phenomenon to persist.

4.3. Recommendations for the RAYUELA serious game

The recommendations of this section are the following:

- The game should, if possible, touch upon the fact that in general, the player's actions in reality have legal consequences if they cross the line into a criminal behaviour, and that they may be prosecuted for such offences, which could have serious consequences (including having a (juvenile) criminal record, fines, community work, educational measures, being institutionalized), while keeping in mind ethical rules and principles to not unduly scare the players. It is important in this context to give appropriate examples of what is criminal behaviour and what is not;
- The game should, if possible, touch upon the distinction between a negative or angry opinion or hyperbole and defamation/slander;
- The game should, if possible, touch upon the distinction between negative interactions and credible threats;
- The game should, if possible, highlight the distinction between "normal" negative interactions or disagreements between people/minors, and the type of continued (almost obsessed) behaviour of persecuting someone constituting stalking or online harassment. The latter goes beyond merely annoying the victim or giving them an unpleasant experience but amounts to a continued significant disruption of their daily life;
- The game should, if possible, highlight the cumulative effect of online bullying behaviour, even if the individual contribution is small (and too small to meet the threshold of constituting an offence);
- The game should, if possible, highlight the issue of underreporting of CB offences, which causes bullies to get away unpunished, victims to not get the help and support they need, and the phenomenon to persist.

5. Misinformation and deception and minors

5.1. Introduction: what is misinformation and deception?

Misinformation and deception (further also referred to as: MD) is not a well-established crime or legal concept, but rather an area of interest that was defined as relevant to the protection of children through the game in the duration of the RAYUELA project. The concept refers to various elements that children may encounter online and which may be directly or indirectly harmful to them, categorized in two parts: misinformation and deception.

First, misinformation refers to fake news and any type of intentional (e.g., disinformation) or non-intentional incorrect information, as was rampant on social media during the COVID-19 pandemic for example. To make matters worse, once children are exposed to misinformation and engage with it, social media algorithms may lead to cementing that type of information reaching them, potentially negatively altering the children's views or confirming factually incorrect points of view. Misinformation may come from diverse sources. During the early COVID-19 pandemic, the International Centre for Journalists conducted a survey of 1,406 journalists and media workers, covering 125 countries, asking them to identify their main perceived sources of disinformation. With 49%; the main source identified was regular citizens, but an impressive 46% of respondents also named political leaders and elected officials as a source of misinformation; 34% of the answer listed biased or State media; 25% indicated that they had experienced misinformation coming from government agencies or their spokespeople; and 23% referred to government-sponsored troll networks.[94]

That misinformation is a worldwide problem that is spreading is widely acknowledged on the international forum, where states are looking how to combat fake news, trying to respect the freedom of speech and avoid censorship while trying to curb rampant misinformation.[95] On 1 April 2022, the UN Human Rights Council adopted a new resolution to combat disinformation. The resolution rejects measures that rely on censorship but instead reaffirms the importance of the right to freedom of expression and the linked right to have the freedom to seek, receive and impart information. Rather than censoring information, states should support media freedom, ensure the safety of journalists, and enable access to information held by public bodies.

[94] Julie Posetti, Emily Bell and Pete Brown, Journalism and the Pandemic: A Global Snapshot of Impacts (2020, ICJF and Tow Center for Digital Journalism), p. 14, https://www.icfj.org/sites/default/files/2020-10/Journalism%20and%20the%20Pandemic%20Project%20Report%201%202020_FINAL.pdf.

[95] See for example the 2021 OSCE paper on "International law and policy on disinformation in the context of freedom of the media" (available at: https://www.osce.org/files/f/documents/8/a/485606.pdf); UN special rapporteur for Freedom of Expression, Submission on an Annual Thematic Report on Disinformation (2021), available at https://www.ohchr.org/sites/default/files/Documents/Issues/Expression/disinformation/2-Civil-society-organisations/UN-SR-on-FOE-CLD-Submission-Disinformation-Mar21-final.pdf.

Indeed, balancing the freedom of expression with the fight against harmful disinformation is not an easy exercise. A recent study on "The fight against disinformation and the right to freedom of expression" (2021) for the LIBE committee at the European Parliament explains the topic in detail.[96] There as well it is mentioned that media literacy rather than censorship is the way forward.

Taking a step back from the larger debate, the question around misinformation covered in the context of this study for the RAYUELA project is whether, and at what point, misinformation by a private individual/citizen becomes a punishable offence under criminal law, if at all.

Second, the Misinformation and Deception concept also covers deception online, which can manifest in a number of ways, such as intentionally lying online (e.g., on social media, on forums, in email messages), in particular to obtain an unlawful result, using fake identities, profiles and accounts, committing fraud, etc. Deception may also be an important part of online grooming (e.g., the counterparty pretending to be minor themselves or otherwise lying about their identity).

Misinformation and deception may also exist together, e.g., where someone spreading fake news is doing so from a fake account that seems to be from a government agency, NGO or other trustworthy source to more easily spread the misinformation. Both misinformation and deception online may be harmful to minors, either directly or indirectly and minors should know how to identify red flags in order to be safe online. This why the concept was onboarded by the project and will be represented in the game. At the same time, minors should not only learn about how to prevent becoming a victim, but also how to not become a perpetrator. Minors may view spreading misinformation or using deception (in a light form) as a joke or prank, which may in many cases be harmless. However, this is not always the case and it is important that children learn to consider the potential harm, especially in the digital environment where something can go viral and reach wide audiences much more quickly than anticipated and intended. Moreover, certain behaviours are definitely harmful in itself, such as impersonating another person or an entity (in particular a governmental entity).

Because the project has onboarded this concept, misinformation and deception is also covered in this report both from a general perspective (e.g., assuming an adult offender, minors may be victims) and from the perspective of minors as offenders, despite being quite broad and relatively vague. This means that, as with CB, many legal qualifications may apply. As was the case for CB, the reports must not be regarded as exhaustive, e.g., it is possible that qualifications apply that were not mentioned because the concept is quite broad and was interpreted by the respondent in a specific manner. However, in what follows, the answers of the different respondents and the interesting trends that could be identified will be discussed.

5.2. How is MD regulated in the countries in focus?

The respondent for **Belgium** mentioned in relation to MD the crime of IT forgery (Art. 210bis of the Criminal Code). IT-forgery under Belgian law consist of "entering into a computer system, altering, deleting or by any other technological means changing the legal meaning of such data which are

[96] "The fight against disinformation and the right to freedom of expression" (2021), study for the LIBE committee, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/695445/IPOL_STU(2021)695445_EN.pdf.

stored, processed or transferred by means of a computer system". The constituent elements of the crime of forgery being the following:

- a disguise of the truth;
- by entering, altering or deleting data;
- which led to an alteration of the legal scope of said data, meaning that misuse had been made of "the reasonable and credible appearance" of said data;
- with a potential damage;
- and with fraudulent intent or the intention to harm.

As such, the crime seems to cover both fraud as well as broadly any other intent to harm (which could include the commission of other specific offences). The threshold for this crime is rather low, and several relevant case law examples are mentioned. IT-forgery was found to exist:

- In a case concerning a person who created a Netlog and Hotmail profile under a false name, who had used these profiles to contact a minor and who proposed to this minor during a chat session to have sex with him in return for payment;
- In a case where a person created a fake Facebook-account and was fraudulently posting messages on behalf of another person;
- In the case of the creation of a fake Facebook-, Twitter- and blog-account to fraudulently spread information on behalf of an association;
- In a case of creation of a fake dating profile while using the phone number and contact details of another person.

The respondent notes that the simple use of a fake account does not in itself constitute a crime, rather it must be proved that the account was created with a fraudulent intent or intent to harm and should allow to abuse the credible appearance of the profile.

In addition, the respondent notes that the use of a fake surname is punishable under Belgian law, as well as the public use of titles one is not authorized to use.

There is no specific mention of disinformation as an offence.

In general, all offences may be committed by minors, minors will be prosecuted under the Belgian Juvenile system.

The respondent for **Bulgaria** mentioned in particular fraud/deceit (Article 209) and computer fraud (Article 212a) as relevant. These crimes are relevant because they imply false information and misleading (deception), often also using fake profiles. For the crimes to apply there has to be a (material) benefit for the perpetrator.

The respondent also notes that sending a message through media that reaches the level of bringing turmoil to society (e.g., false bomb alarm) may be punishable as well, but notes that this qualification would not be used against minors, only against adults. If children would commit such actions, educational measures would be applied.

The respondent also mentions the importance of insult and defamation in case the misinformation is targeted at a specific person. In this case perpetrators may often use fake accounts or post things anonymously. This seems to be an issue in Bulgarian practice, in particular because court orders for computer data (aimed at the website administrator for example), is only available for serious crimes, which is not applicable to insult or slander. The respondent mentions however that legislative changes are pending to solve this challenge.

In general, provisions apply to minors, and minors may be prosecuted under the Bulgarian juvenile system (as of 14), despite a lack of prosecution in practice.

With regards to the **Czech Republic,** our respondent noted a number of potential offences that could apply. One angle that was followed was clearly the situation of spreading of misinformation related to a person of a group, mentioning the following qualifications:

- § 184 Defamation;
- § 345 False accusations (falsely accusing someone of a criminal act);
- § 355 Defamation of a nation, race, ethnic or other group of persons;
- § 356 Instigation of hatred towards a group of persons or suppression their rights and freedoms.

From another angle, using misinformation and deception was considered as potential tool for inciting criminal behaviour with the following offences being cited:

- § 364 Incitement to a criminal offense;
- § 365 Approval of a criminal offense;
- § 404 Expression of sympathy for a movement aimed at suppressing human rights and freedoms.

The respondent also mentioned § 181 “Infringement of Rights of Another”, which punishes generally the causing of serious detriment to the right of another by misleading that person or using other people’s errors (against them).

Of particular interest is also the mentioned § 357 “Spreading of alarming news”. This section of the criminal code punishes “whoever intentionally causes a threat of serious concernment of at least a portion of population of a certain area by spreading alarming news that is untrue”, as well as communicating this news to stakeholders like the police, companies, authorities or the media for example.

Prosecution of minors for such offences would be possible under the juvenile system.

In **Estonia**, the respondent explained that misinformation is not usually punished, as this is usually an accidental act. Even if the situation concerns disinformation (e.g., intentional misinformation) or intentional deception this is only punishable in the context of sexual grooming acts (discussed above) or in the context of fraud (§ 209 of the Penal Code). Other than that, deception and disinformation is not criminalized in Estonia. In certain cases civil consequences may apply, but in most cases, statements are protected under freedom of speech and expression.

Minors may in principle be prosecuted for such offences, even though this is rare in practice. Repeat offences for fraud or identity theft would however likely be prosecuted. The Estonian juvenile system applies.

Regarding the situation in **Germany**, the respondent highlighted that the is no specific offence that relates to „fake news“, e.g., misinformation and deceit, no matter if it happens online or offline.

However, misinformation and deception can constitute a criminal offence, if certain special individual interests or legally protected goods are at stake, such as:

- The spreading of false facts that are apt to degrade that person or to negatively affect public opinion about that person can be a punishable as “malicious gossip” (§ 186 StGB) or – if the offender intently or knowingly spreads false facts about a person – “defamation” (§ 187 StGB);
- Intentionally deceiving another person and damaging his or her financial interests in order to gain monetary advantages for oneself or a third person can constitute the criminal offence of fraud (§ 263 StGB). This includes online fraud. If the deceptive behaviour is not aimed at a human being, but is rather used in an interaction with a computer system, the offence of computer fraud (§ 263a StGB) becomes relevant.

Minors may be prosecuted for such offences under the juvenile system.

For **Greece,** the respondents mentioned in particular Article 191 of the Greek Penal Code aimed at punishing the dissemination of fake news.

This Article punishes anyone who publicly or via the internet spreads or disseminates in any way fake news that are capable of causing concern or fear to the public or undermining public confidence in the national economy, the country's defence capacity or public health. The way this Article is interpreted has changed over the years and it is no longer sufficient to cause fear or to disturb or destroy the public confidence in the national economy, the country’s defence capacity or public health, but notably, it is required that it influences an indefinite number of people or a certain circle or category of persons, to either carry out unplanned acts or to cancel planned acts, i.e. to reach the level of changing their behaviour, with the risk of damaging the economy, tourism, public health, the defence capacity of the country or disturbing its international relationships.

One respondent mentions a 2022 case where a minor was convicted of committing this offence and reformation measures were imposed, making clear that this offence can be committed by minors and that such offences are prosecuted under the Greek juvenile system.

Other relevant offences that were mentioned are:

- Fraud (Article 386 of the Greek Penal Code);
- Computer related fraud and forgery;
- Article 38 of the Law 4624/2019 on “Protection of Personal Data” in case the minor perpetrator without legal grounds obtains personal order to impersonate another person for any reason whether it is legal or illegal.

In **Latvia**, our respondent indicated that while there is no specific regulation on the subject of false news or misinformation, there are instances where the dissemination of false information which could cause significant harm to society or endanger public safety will be penalized. In those cases. it will be important to establish the intent of the dissemination. Examples include:

- Hate speech: Article 74.1 on Acquittal of Genocide, Crime against Humanity, Crime against Peace and War Crime and Section 78. Triggering of National, Ethnic and Racial Hatred punish misinformation that amounts to hate speech against certain groups or glorifies genocides or crimes against humanity and war crimes;
- Article 150 punishes Incitement of Social Hatred and Enmity, which punishes the act of inciting hatred or enmity depending on the gender, age, disability of a person or any other characteristics, if substantial harm has been caused thereby;
- If the dissemination amounts to defamation Article 157 of the Criminal Law will apply;
- If information is disseminated without special intent to harm a specific person, the conduct may be qualified as hooliganism under Article 231 of the Criminal Law, however there is no consensus on the degree of harm required in this case to amount to the "gross disturbance of the public order" required by that Article and that proving intent is often difficult;
- If the situation includes the unlawful processing of personal data, the person may be held liable under Article 145 of the Criminal Law;
- Article 194.1 punishes Dissemination of False Data or Information Regarding the Condition of the Finance System of the Republic of Latvia, if committed knowingly;
- Article 231.1 punishes any "person who knowingly commits making a false report on placing of explosive, poisonous, radioactive or bacteriological substances or materials or explosive devices in an institution, undertaking or other object, or locating outside of an institution, undertaking or other object". The Article seems to cover an array of false reports and the respondent mentions a case where the defendant was sentenced to three years in prison for disseminating false COVID-19 news that caused public concern.

Offences can be committed by minors and could be prosecuted under the juvenile system, despite a lack of practice.

For **Portugal,** respondents note that online misinformation and deception are not in themselves a crime, but can easily be part of a criminal qualification.

Mentioned first and foremost is fraud (Art. 217 of the penal code). This Article punishes "whoever, with the intent to obtain for himself/herself or a third-party illegitimate enriching, by means of mistake or deceit about facts which he/she has caused with astuteness, determines another person to the commission of acts which causes to such person, or causes to another person, a property loss".

Defamation is also mentioned as relevant, depending on the circumstances. One respondent mentions a case where it was decided that "The creation, on a social network, of a profile in the name of another person, with the inclusion of user characteristics offensive to the honour and consideration of the "owner" of the profile, constitutes a crime of defamation".

In addition, the following are mentioned:

- Online identity theft (not in itself a qualification but potentially encompasses several crimes);
- Illegal recordings (Art. 199 of the Penal Code) as a form of deception.

It is also noted that misinformation and deception can be an instrumental part of other crimes, such as online grooming, and other online sexual offences against children.

Minors can in principle be prosecuted for such offences in accordance with the Portuguese juvenile system.

Regarding the legal system in **Romania**, the respondent mentioned in particular fraud/deceit (§ 244 Penal Code. This crime presupposes material gains. Also mentioned was computer fraud. The respondent provides a number of cases and details on application that illustrate the problem. Hence, misinformation and deception are not punished as such in Romania, even though it can be part of other crimes.

In principle, minors may be prosecuted for such offences under the juvenile system of Romania.

For **Slovakia**, the respondent explains that MD is not a crime as such. Following the COVID-19 crisis, this offence has been proposed in a legislative proposal, but was met with a lot of critique because it would be difficult for law enforcement and courts to distinguish between freedom of expression and disinformation, as well as to assess the veracity of particular information.

However, the respondent mentions that it is possible in Slovakia to punish any 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". It is explained that this offence requires that the act causes serious concern to at least part of the population. The bar is therefore set high and the mere spreading of disinformation alone will not typically meet this standard.

Also mentioned are:

- The crime of defamation; this however requires that the false information causes serious harm to the victim in various important areas of their life;
- Denial/approval of holocaust, crimes of political regimes, crimes against humanity, etc.

The respondent mentions a particular case that highlight the type of defamation that could lead to criminal liability:

> *The defendant 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 X. Q.'s 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 account, which is capable of significantly endangering X. Q.'s seriousness with fellow citizens, damaging X. Q. at work, disrupting their family relations, causing them other serious harm and committing this act in a clearly public manner.*

In addition, the respondent mentions that pretending to be an expert is not a criminal offence until the perpetrator makes a profit from this. This is understood as relating to scenarios of fraud, as mentioned by several other respondents.

Minors can in principle be prosecuted for such offences under the rules applicable to juveniles in Slovakia.

For **Spain** the respondent mentioned in particular fraud/swindling (Article 248). Also mentioned are slander/libel, hate crime and crimes against moral integrity of a person (as covered under CB).

In principle, if such offences apply, a minor could be prosecuted for it under the general juvenile system applicable in Spain.

Concerning the situation in **the Netherlands**, the respondent indicated that misinformation or fake news is not criminalised as such. Interestingly, if the misinformation serves to induce others to commit an offence, the perpetrator of the deception can also be held responsible for that crime having committed intentional provocation according to art. 47 of the Dutch Criminal Code (containing the definition of the perpetrator of an offence).

Depending on the circumstances, some other qualifications may apply as well:

- In special circumstances, if the misinformation consists of spreading a false message to influence the price of goods or stocks, this could be qualified as manipulating stock prices (Art. 334 DCC);
- In theory, forgery (Art. 225 DCC) could apply, if the information has a purpose of falsely proving a legally relevant fact; but this will not often be the case with deceptive information spread by minors;
- If the deception includes the use of someone else's identity, the behaviour could fall under identity fraud (Art. 231b DCC). This is applicable if the abuse of someone else's identity is aimed at hiding one's own identity or to abuse the other's identity, and if such abuse causes any harm.

The respondent notes that the interpretation of the term "spreading a false message" to influence stock prices in Art. 334 DCC may be relevant if fake news were to be regulated in the future. Under the current interpretation of that Article, falsely stating an expectation (so not only falsely stating facts), is also covered, as well as providing facts that are in themselves true but at the same time holding back other facts that are essential for interpreting the facts. However, while the issue is debated, there are no pending proposals to regulate fake news. It is acknowledged that this may be in part due to the position of Dutch legal literature that criminalizing fake news is complicated because it is such a broad term encompassing a wide variety of statements, and because a prohibition is very difficult to enforce.

In as far as specific offences apply, minors can be prosecuted for these under the general rules of the Dutch juvenile system.

For **Brazil**, our respondent noted that there is no express provisions regulating MD. However, bills have been proposed with the aim to fight the dissemination of false content on social networks and private messaging services. While it is by no means ready to be signed into law (and this may not even happen), it can be envisioned that in the future there will be specific rules on misinformation.

The respondent notes that regarding online deception the following crimes may in particular apply:

- Swindling (Article 171, Criminal Code), including fraud and electronic fraud;
- False Identity (Article 307, Criminal Code).

Depending on the situation, the following may also apply:

- Slander (Article 138, Criminal Code);
- Defamation (Article 139, Criminal Code);
- False Alarm (Article 41, Law of Misdemeanours), this offence consists of causing alarm, announcing disaster or non-existent danger, or performing any act capable of producing panic or turmoil. For the characterization of the misdemeanour, it is necessary for the agent to be aware that the information he is spreading is not true;
- Pretending to be a Public Official (Article 45, Law of Misdemeanours);
- Illegal Exercise of a Profession (Article 47, Criminal Misdemeanours Act).

In general, minors can commit these offences and be prosecuted for them, under the juvenile system applicable to minors in Brazil.

For **China,** our respondent mentioned several laws that could apply to MD:

First up, under the crime of picking quarrels and provoking trouble (Article 293 of the criminal law), Item (4) of paragraph 4, punishes whoever fabricates false information, or clearly knows that it is fabricated false information, spreads it on the information network, or organizes or instructs personnel to spread it on the information network, causing trouble and causing serious chaos in the public order. Potentially also relevant to MD is paragraph 1 (2) of the same Article, which punishes those who use information networks to abuse or intimidate others, with vile circumstances and disrupt social order.

Another Article related directly to false information is Article 291-1 of the Criminal Law. Paragraph 1 of that Article punishes fabricating and intentionally disseminating false terrorist information, such as explosion threats, biological threats, and radiological threats, or deliberately spreading terrorist information knowing that it is fabricated, and seriously disrupting social order. Paragraph 2 of that same Article punishes fabricating or intentionally disseminating false information referring to false dangers, epidemics, disasters, and police situations, and disseminating them on information networks or other media, or knowing that the information is false, deliberately spreading it on the information network or other media, and seriously disrupting the social order.

A related administrative sanction can be found in Article 25 of the Public Security Administration Punishment Law, which punishes with smaller sanctions:

- Spreading rumours and falsely reporting dangerous situations, epidemic situations, police situations, or intentionally disrupting public order by other means;
- Disrupting public order by throwing false explosive, toxic, radioactive, corrosive substances or infectious disease pathogens and other dangerous substances;

- Threatening to commit arson, explosion, or throwing dangerous substances to disrupt public order.

A second administrative provision that is mentioned is paragraph 6 of Article 14 of the 2019 "Regulations on the Administration of Business Sites for Internet Access Services", which states that Internet access service business premises operators and online consumers shall not use the Internet access service business premises to produce, download, copy, consult, publish, disseminate or otherwise use information containing the following contents, which:

- (1) Oppose the basic principles established by the Constitution;
- (2) Endanger national unity, sovereignty and territorial integrity;
- (3) Divulge state secrets, endanger state security or damage state honour and interests;
- (4) Incite ethnic hatred, ethnic discrimination, undermine ethnic unity, or infringe upon ethnic customs and habits;
- (4) Undermine the state's religious policy and promoting cults and superstitions;
- (5) Consist of spreading rumours, disturbing social order, and undermining social stability;
- (6) Propagate obscenity, gambling, violence or instigate crimes;
- (7) Insult or slander others, infringing upon the lawful rights and interests of others;
- (8) Endanger social morality or excellent national cultural traditions;
- (9) Contain other content prohibited by laws and administrative regulations.

A third administrative regulation affecting spreading of online misinformation) is paragraph 5 of Article 5 of the 2011 "Administrative Measures for the Security Protection of International Networking of Computer Information Networks", which state that no unit or individual may use the international network to produce, copy, consult and disseminate the following information:

- (1) Incite to resist or undermine the implementation of the Constitution and laws and administrative regulations;
- (2) Incite subversion of state power and to overthrow the socialist system;
- (3) Incite to split the country and undermine national unity;
- (4) Incite ethnic hatred, ethnic discrimination, or undermine ethnic unity;
- (5) Fabricate or distort facts, spread rumours, and disrupt social order;
- (6) Advocate feudal superstition, obscenity, pornography, gambling, violence, murder, terror, or instigating crimes;
- (7) Openly insult others or fabricate facts to slander others;
- (8) Damage the credibility of state organs; (9) Other violations of the Constitution, laws and administrative regulations.

The respondent also mentions a number of other provisions relevant to MD scenarios:

- Insult and libel (Article 246 Criminal law);
- Personality rights related to reputation, to be free of insults and slander and right to name, portrait, reputation and honour (Article 101 and 120 of the General Principles of Civil Law);
- The crime of inciting subversion of state power, under this crime, whoever incites subversion of state power or the overthrow of the socialist system by spreading rumours, slander or other means is punished with serious sanctions (Paragraph 2 of Article 105 of the Criminal Law).

Lastly, the respondent mentioned some provisions applicable only in very specific cases:

- Manipulating stock prices by making false or seriously misleading statements or omitting material information in the process of stock issuance and trading or by conspiring or concentrating funds, or influencing stock issuance and trading by means such as spreading rumours (Article 74 of the 1998 Interim Regulations on the Administration of Stock Issuance and Trading) or fabricating and spreading false information that affects securities and futures trading, disrupts the securities and futures trading market, and causes serious consequences (Article 181 Criminal law);
- Article 15 of the 2011 "Destructive Earthquake Emergency Regulations" provide that no organization or individual may spread rumours about the earthquake and that when earthquake rumours occur, the competent department of earthquake prevention and disaster reduction work shall assist the people's government to quickly quell and clarify them;
- Article 52 of the 2011 Regulations on Public Health Emergencies provides that during the occurrence of emergencies, those who spread rumours, drive up prices, deceive consumers, and disrupt social order and market order shall be given administrative penalties by the public security organs or the administrative departments for industry and commerce; if a crime is constituted, criminal responsibility shall be investigated according to law;
- Article 48 of the 2017 "Emergency Regulations on Major Animal Epidemics" provides that during the occurrence of major animal epidemics, those who drive up prices, deceive consumers, spread rumours, and disrupt social and market order shall be subject to administrative penalties by the competent pricing department, industry and commerce administrative department or public security organ according to law; if a crime is constituted, criminal responsibility shall be investigated according to law.

It is quite clear that Chinese law includes both criminal and administrative law examples of the fight against (perceived) misinformation and deception, including MD online. For the various criminal law provisions, the general juvenile rules apply, and the age limit of 16 for criminal responsibility. The respondent indicated that administrative fines are in general applicable to minors as well. However, sanctions may be reduced and there is more focus on education that on punishment in case of minors.

For **Mexico**, the respondent noted that misinformation and deception in general are not specific crimes regulated under Mexico's Federal Criminal Code. The respondent however mentioned that:

- Misleading information for online purchases is punished only under consumer law;

- Defamation may apply;
- In some states, identity theft is criminalized.

In as far as one of these qualifications would apply, the juvenile system would apply to minor offenders. However, the respondent highlights that since MD is not a crime, it is in principle not possible for minors to commit this particular crime.

Regarding the law in **Russia**, the respondent explained that while misinformation and reception can be an important way to commit other offences, it is not punished separately as such, except for the following specific circumstances:

- If it reaches the level of slander (article 128.1 of the Criminal Code), meaning the dissemination of information that is knowingly false and of defamatory nature; or
- If it falls within the remit of Article 207 of the Criminal Code, which combats fake news.

Disseminating "fake news" qualifies as a criminal offence when:

- There is public dissemination of information on circumstances posing a threat to the life and security of citizens and (or) the measures taken to ensure the safety of the population and territories, methods and means of protection against such circumstances e.g., epidemic, pandemic, natural disaster etc. (article 207.1 of the Criminal Code); or
- Public dissemination of information that caused dire consequences (e.g., harm to health or death) (article 207.2 of the Criminal Code); or
- Public dissemination of information on Russian military forces and public authorities acting in their powers outside the territory of Russia (article 207.3 of the Criminal Code).

Fake news is only punished if the offender should be reliably aware that some information is not true from the outset.

The juvenile system in Russia applies to these offences as well.

For **South Africa** our respondent stated that MD has not been addressed by South African law specifically. The closest offence would be misrepresentation (of data), fraud and forgery under section 8 and 9 of the new Cybercrime Act. The juvenile regime applies to these offences, with the state having to prove beyond reasonable doubt that the minors understood the consequences of their actions.

Regarding the legal situation in the **UK**, the respondent explained that it is not an offence under existing legislation to post disinformation, fake news or false stories, unless other conditions are met, such as the conditions for defamation, slander or libel.

Posting misinformation over a public electronic communications network can also be an offence under the Communications Act 2003 if this is grossly offensive or of an indecent, obscene or menacing nature. However, if it does not fit these categories then, again, it remains legal to post false information, such as "fake news".

By contrast, deception can be a criminal offence, though convictions have been most commonly associated with fraud i.e. "making a dishonest representation for your own advantage or to cause another a loss". Deceptions of this kind can involve perpetrators hiding their identities behind websites and email addresses, or making false claims or promises with the intention of for gaining illicit profit

at the expense of a victim. Deceptions specifically associated with fraud and cyber-fraud are dealt with via The Fraud Act (2006). This requires there to also be an intention. Thus, the act of setting up a false social networking accounts or aliases could amount to criminal offences under the Fraud Act 2006 if there was a financial gain.

The respondent also explains that the following could also be relevant, depending on the circumstances:

- The Theft Acts (1968 &1978);
- Forgery and Counterfeiting Act (1981);
- Proceeds of Crime Act (2002) ('POCA').

The respondent indicates that a recent review by the UK Law Commission has attempted to address some of the gaps in managing misinformation online. They found that there were potential gaps in the existing legislation, under criminalising misleading or harmful communications. One example is that whilst the Malicious Communications Act makes it illegal to post abusive or false messages in a public forum, no offence is committed if the message has no "intended recipient". However, the same Commission also found that there can be a risk of overcriminalisation (criminalising innocent but silly behaviour). As a result of the Law Commission's recommendations following the review, the new Online Safety Bill has been created. The Bill, which is still to be fully ratified, would expand the legal powers against deception, by focusing more directly on situations where deception or providing false information results in harm, rather than financial loss alone. A new offence created in the Bill centres upon disinformation or false communications which are deliberately circulated to inflict harm - for example a hoax bomb threat. However, it does not criminalise misinformation when people are unaware what they are sending is false or genuinely believe it to be true. For example, if an individual posted a message on social media encouraging people to inject antiseptic to cure themselves of coronavirus, a court would have to prove that the individual knew this was not true before posting it.

Minors could be prosecuted for the mentioned offences under the UK's juvenile system, but since fake news and misinformation is generally not criminalized, this would not apply in this case. The most common MD related offence, in particular related to deception is fraud (under the 2006 Fraud Act). The respondent mentions a number of fraud cases for which minors were prosecuted and convicted.

Regarding the situation in the **USA** the respondent explains that the freedom of expression guaranteed by the first amendment poses a serious challenge in preventing the spread of fake news. One legal recourse that is mentioned is when misinformation reaches the level of defamation/libel/slander. However, the respondent notes some difficulties in the application of defamation online.

In addition, regarding deception in particular, the respondent notes that this could manifest as online fraud. In the absence of specific legislation, online fraud is punished in the USA on the basis of traditional mail and wire fraud statutes (18 U.S.C. § 1343). For this crime to apply it has to be proven that the offender had an intent to benefit from the actions. The respondent mentions that another relevant fraud statute is 18 U.S.C. § 1029. This statue makes it illegal to knowingly have the intent to defraud others using counterfeit or unauthorized access devices.

Minors are subjected to these statutes under the juvenile regime.

Looking at the total of responses, it is quite clear that in general, **misinformation** in particular is covered in large part by the freedom of speech, and is not punished in and of itself. Exceptions typically exist when the freedom of speech comes in conflict with other legally protected interests such as:

- Prohibition of defamation/slander/libel;
- Prohibition of hate speech, incitement of hatred and violence or crimes against certain groups, denial or approval of war crimes, crimes against humanity or holocaust.

Recommendation for the game: The game should, if possible, highlight the importance of free speech and sharing information, while indicating the limits that exist in the form of breaching personality rights and any information that amounts to hate speech or incitement of hatred, violence or crimes against certain groups.

Some countries also have specific crimes for spreading fake news in particular when this has a serious impact on society, public security/order or public health and safety. In our sample the respondents for Bulgaria, Czech Republic, Greece, Latvia, Slovakia, Brazil, China and Russia mention such provisions. Some of these provisions would for example be able to punish fake COVID-19 news if that news has a significant impact and the person sharing it did so knowing it was false (or should have known that the information was unreliable, see e.g., Russia). Latvia for example mentions a case where the defendant was sentenced to three years in prison for disseminating false COVID-19 news that caused public concern. Relevant aspects of whether disinformation reaches the impact required to be sanctioned may be the use of fake accounts of governmental agencies or other official source, abusing their credibility and trustworthiness to achieve impact.

Recommendations for the game: The game should, if possible:

Highlight the fact that fake news can spread rapidly and can be very damaging. The COVID-19 pandemic could be used as a clear example. It should be highlighted that before sharing information it is important to check the source and whether the information is true, because sharing information that is obviously wrong could in theory be punishable in certain countries;

Highlight that knowingly sharing information you know to be wrong is an offence in certain countries and is in any case harmful behaviour;

Highlight that creating fake profiles or attempting to seem like an official source is not a prank or funny but a criminal offence in certain countries and can have severe consequences, but for the offender and in terms of damage;

Explain that sharing information that is factually incorrect is not in itself a crime if you did not know and did not mean to harm anyone.

Deception is mentioned in several country reports as a relevant part of other crimes, but is not typically punished as such. Making fake accounts or other forms of deception are then only punishable if part of a specific crime, typically requiring an intent to harm, and, for fraud, an intent to obtain material or monetary benefits. Fraud is by far the most mentioned qualification related to deception. Also mentioned a number of times is that deception is also punished when it amounts to identity theft or to impersonation or involves falsely using a protected title. In addition, computer fraud and forgery is mentioned as well, depending on the form of deception. Creating fake accounts impersonating someone else or impersonating official instances is mentioned in several countries as a punishable

crime. If deception involves hacking or accessing accounts without permission, this is also typically punished (see also hacking further).

Recommendations for the game: The game should, if possible:

Highlight that making and using fake accounts is okay (fake Instagram, fake Facebook accounts for fun, e.g. of a non-existing person or using a second account for yourself), but that limits apply, in particular that it is not okay and may be a criminal act to impersonate someone else, use their name or otherwise steal parts of their (online) identity, or to use titles or pretend to be a person of authority (e.g. police, lawyer, etc.);

Highlight that deception of any kind with the intention to mislead someone is not acceptable behaviour and may amount to a criminal offence with serious consequences if any material gain is involved;

Highlight that accessing someone's account without permission or hacking into someone's account to use this account to pretend to be them, to gain access to their personal information or to mislead them is not acceptable behaviour and may amount to a criminal offense.

For both misinformation and deception, minors could be prosecuted under the applicable juvenile rules. Greece and the UK in particular provide some case examples.

Recommendation for the game: The game should, if possible, highlight that minors may be prosecuted for MD-related offences if they are serious, while taking care to not overly frighten the players who may already be prone to think that innocent behaviour is punishable.

5.3. Recommendations for the RAYUELA serious game

The recommendations of this section are the following:

- The game should, if possible, highlight the importance of free speech and sharing information, while indicating the limits that exist in the form of breaching personality rights and any information that amounts to hate speech or incitement of hatred, violence or crimes against certain groups;
- The game should, if possible, highlight the fact that fake news can spread rapidly and can be very damaging. The COVID-19 pandemic could be used as a clear example. It should be highlighted that before sharing information it is important to check the source and whether the information is true, because sharing information that is obviously wrong could in theory be punishable in certain countries;
- The game should, if possible, highlight that knowingly sharing information you know to be wrong is an offence in certain countries and is in any case harmful behaviour;
- The game should, if possible, highlight that creating fake profiles or attempting to seem like an official source is not a prank or funny but a criminal offence in certain countries and can have severe consequences, but for the offender and in terms of damage;

- The game should, if possible, explain that sharing information that is factually incorrect is not in itself a crime if you did not know and did not mean to harm anyone;
- The game should, if possible, highlight that making and using fake accounts is okay (fake Instagram, fake Facebook accounts for fun, e.g., of a non-existing person or using a second account for yourself), but that limits apply, in particular that it is not okay and may be a criminal act to impersonate someone else, use their name or otherwise steal parts of their (online) identity, or to use titles or pretend to be a person of authority (e.g., police, lawyer, etc.);
- The game should, if possible, highlight that deception of any kind with the intention to mislead someone is not acceptable behaviour and may amount to a criminal offence with serious consequences if any material gain is involved;
- The game should, if possible, highlight that accessing someone's account without permission or hacking into someone's account to use this account to pretend to be them, to gain access to their personal information or to mislead them is not acceptable behaviour and may amount to a criminal offense;
- The game should, if possible, highlight that minors may be prosecuted for MD-related offences if they are serious, while taking care to not overly frighten the players who may already be prone to think that innocent behaviour is punishable.

6. Online piracy (copyright offences) by minors

6.1. Introduction: what is online piracy and when is it criminalised?

Copyright protects the expression of ideas by granting a set of exclusive rights to authors of original creative works. In its essence, copyright is a limited monopoly granted to creators for certain a period of time (usually 70 years after their death) which allows authors to profit from the use of their works. The works covered by copyright range from films, books, music and paintings to computer programs, video games and databases. An important characteristic of copyright protection is that it is obtained automatically with the creation of the work and no registration or other formalities are necessary. This means that any original work (i.e., expression of ideas) is protected by copyright and if a person uses it without the authorisation of the author, they will infringe copyright.

The ease of sharing information online has created a challenge for copyright owners in the recent years to exercise their exclusive rights over their works. Media can easily be accessed, downloaded, and distributed over the Internet without the permission of rightsholders. Moreover, online piracy is popular with younger people, who often resort to using illegal sources mainly because they are cheaper or free, or because they offer better access to content.[97] Illegal sources are intentionally used most often for films, TV series, music, software or computer programs, games, e-books, and live sport events (see Table 3). The trend in this respect, however, has been positive in the recent years since the rise of streaming services which have made content both more accessible and cheaper.

Table 3. Use of only/mainly illegal sources for different types of content, by gender and age

Variable	Films	TV series / shows	Music	Live sport events	Software	E-books / audio books	Games	Concerts / events	Educational content	Photos
Gender										
Male	25 %	19 %	17 %	19 %	18 %	14 %	15 %	14 %	12 %	10 %
Female	18 %	14 %	13 %	9 %	9 %	12 %	8 %	6 %	6 %	5 %
Age										
15-17	24 %	14 %	15 %	14 %	11 %	12 %	10 %	8 %	7 %	6 %
18-21	22 %	17 %	14 %	14 %	14 %	12 %	11 %	10 %	8 %	7 %
22-24	21 %	18 %	17 %	17 %	16 %	15 %	13 %	12 %	12 %	10 %

Source: *EUIPO, Intellectual Property and Youth Scoreboard 2022*

Nonetheless, the portion of young people accessing media from illegal sources is still relatively high. One third of the respondents in the 2022 EUIPO Intellectual Property and Youth Scoreboard aged 15-

[97] EUIPO, Intellectual Property and Youth Scoreboard 2022. Available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/IP_youth_scoreboard_study_2022/IP_youth_scoreboard_study_2022_en.pdf

24 confirmed that they had played, downloaded, or streamed content from illegal sources over the previous 12 months. In addition, 26% of the respondents said they did not know if they accessed the content from an illegal source, which points to a need for better education on the ways to distinguish legitimate from illegitimate sources online. The percentage of respondents declaring that they intentionally use illegal sources of digital content is significantly lower for the age group of 15-17 (13%), than for 18–21-year-olds (25%). While this is a positive trend, much can still be done to better educate minors of the negative consequence of online pirating and the legitimate options that are available to them.

Another notable aspect of copyright is that not every use of copyrighted content without the authorisation of the author is illegal. Copyright should be balanced with the fundamental right of freedom of information. For that reason, national laws include exceptions and limitations to copyright in cases where the reproduction does not conflict with a normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the author. In countries like the US, the rule is that copyrighted materials can be used without permission if the use can be considered fair ("fair use doctrine"). A special four-factor analysis is then applied in each case to determine whether the use is fair. In other countries, such as the EU Member States, legislation provides for a specific list of exceptions and limitations for education, quotation, commentary, parody, and others.[98] If a use falls under these exceptions, then it is not an infringement of copyright.

Copyright is part of civil law, and it is generally up to the copyright holders to prevent copyright infringements and to ensure their rights are respected. Whenever their rights are infringed, copyright owners are entitled to a civil remedy, such as damages or injunctive relief. Nevertheless, infringers can in some cases be prosecuted criminally for copyright infringements. Infringements amount to a criminal offence in more serious cases and criminalised copyright penalties have always been the exception rather than the rule. In general, criminal sanctions to apply only to particularly serious cases (e.g., online piracy at a large scale), where the infringer knows their actions are wrong, they have attempted to circumvent technology that is used to prevent piracy, or the type of case renders civil enforcement by individual copyright owners especially difficult.

Recommendation for the game: The game should, if possible:

Distinguish between lawful use of copyrighted content without the permission of the author (e.g., in the context of education, parody, commentary) and unlawful copyright pirating;

Inform children about platforms that provide legal access to content and guide them on how to distinguish legal from illegal sources.

[98] See Article 5 of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSoc Directive).

6.2. International standards

The main international copyright treaty is the Berne Convention for the Protection of Literary and Artistic Works. It was the **TRIPS Agreement,**[99] however, that included provisions mandating its members to include not only civil but also criminal procedures for copyright infringement. One of the main reasons for the criminalisation is the fact that new technology has greatly improved the possibility to exploit works, made piracy activities very lucrative and linked them to all sorts of organised crime.[100]

Article 61 TRIPS mandates that its members provide for criminal procedures and penalties to be applied "at least" in cases of *wilful copyright piracy on a commercial scale*. What is important about this provision is that it sets a minimum standard which has two main consequences. First, it criminalises wilful infringements, but nonetheless member states "may" provide for criminal procedures and penalties also where the acts are committed not wilfully but with, for instance, gross negligence. Second, member states can also criminalise online piracy which is not only on a commercial scale.

As far as remedies are concerned, Article 61 TRIPS prescribes that they shall include *imprisonment and/or monetary fines* sufficient to provide a deterrent, consistently with the level of penalties applied for crimes of a corresponding nature. This provision not only makes it mandatory to include imprisonment and/or monetary fines as a sanction but also prescribes that the remedies must be severe enough to provide a deterrent against infringements. The fact that the penalties should correspond to crimes of a similar gravity is generally interpreted as meaning that they should correspond to that of theft or similar crimes.[101]

All members of the World Trade Organisation, and respectively all of the countries in focus, are members to the TRIPS Agreement and have legislation criminalising online piracy. The regime in the Member States of the EU, however, is not harmonized with regards to criminal enforcement of copyright infringements. The European Commission's Proposal for a Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights was withdrawn in 2010. Nevertheless, Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights sets the standards for harmonisation of civil enforcement throughout the Union.

6.3. How is online piracy regulated in the countries in focus?

All of the countries in focus are members of the TRIPS Agreement and criminalise certain cases of online piracy. When asked about the prosecution of minors for this crime, however, almost all respondents highlighted that this is only a theoretical possibility and usually minors are not prosecuted

[99] Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement). The TRIPS Agreements is an international legal agreement between all the member nations of the World Trade Organization signed in 1994.
[100] Henry Olsson, *Fighting Piracy In The Field Of Copyright And Related Rights: Actions And Remedies* (2005), WIPO/CR/KRT/05/5.
[101] Ibid.

for copyright infringements. The respondents from **Bulgaria, Brazil, China, Czech Republic, Estonia, Greece, Latvia, Netherlands, Romania, Russia, Slovakia, South Africa, Spain** all either did not mention any cases with minors or remarked that they are generally not prosecuted in practice.[102] The respondent from **Latvia** noted that so far, the police have not initiated any criminal proceedings against a minor for online piracy. The respondent from the **Netherlands**, on the other hand, concluded that copyright violations in his country are generally not combated through criminal law but only through private law.

Two main reasons were noted from the respondents for the lack of prosecution of minors for online piracy. First, as the **UK** respondent reported, governments "do not want to see teenagers prosecuted for file sharing in their bedrooms". Governments are generally disinclined to spend resources and lead a policy that prosecutes minors actively for individual copyright infringements. What's more, as mentioned in Section 6.1., copyright holders are responsible for the civil enforcement of their exclusive rights. Second, many countries have kept the minimum standard set out in the TRIPS Agreement and prosecute online piracy only when it is intentional and committed on a commercial scale. The requirement for infringement on a "commercial" or "large scale" is rarely met with regards to minors which makes the likelihood of criminal prosecution for minors even lower. It should be noted, however, that not all countries include such limitations to the act of criminal copyright infringement.

In **Russia** minors over the age 16 years old may be subject to criminal liability for online piracy but only if the actions are committed on the large scale or on the especially large scale, e.g., the value of the copies of the works or phonograms or the value of the rights to use the copyright and related rights objects exceeds 100,000 RUB (approx. 1,652 EUR), and on an especially large scale, 1,000,000 RUB (approx. 16,521 EUR). The Russian respondent noted that this crime is rarely applicable to minors s their acts usually do not meet the applicability conditions. Similarly, in **Mexico** online piracy is punished only when committed with intention to profit.

In **Brazil**, on the other hand, criminal law does not require the copyright infringement to be committed for profit. Nevertheless, the Brazilian respondent noted that there is a trend, identified in the jurisprudence, that the crime has been attributed only to agents who use the violation for profit, although this element is not required for its configuration.

The **Bulgarian** Criminal Law also criminalises any intentional distribution, broadcast, transmission or other use of a copyrighted work without the authorization of the rightsholder. The general part of the Criminal Code, however, stipulates that an act can be prosecuted as a crime only if it poses danger to society. Therefore, this requirement is still unlikely to be fulfilled with respect to minors torrenting films.

Other countries, however, have a stricter approach when it comes to criminalising online piracy. **Portugal,** for example, criminalises copyright infringements irrespective both intent and the commercial scale of the infringing act. The Portuguese respondent mentions that three main guidelines have emerged from case law with respect to criminal online piracy:

i. that it is unlawful, in relation to a computer program that has been lawfully purchased, to reproduce it in a number greater than that provided for in the contract;

[102] In China and Russia only minors above the age of 16 can be prosecuted for copyright infringements.

ii. that these type of crime does not require a profitable intention; and

iii. that it's typical core elements (reproduction, dissemination and communication to the public) are not cumulative, and it is sufficient that only one of them is committed.

In **Belgium**, pursuant to article XI. 293 BCEL, a person is guilty of the criminal offence of counterfeiting, which also includes online piracy, when he or she *maliciously or fraudulently infringes copyright. The* Belgian respondent explained that the criminal offence of counterfeiting is committed when two conditions are met:

- *Substantive element*: the act of "counterfeiting" in criminal law is equivalent to "infringement" of copyright under Belgian civil law. Therefore, any conduct prohibited under civil law would also entail the substantive element for the criminal offence of counterfeiting. The Belgian respondent noted, however, that this naturally implies that whenever a use is covered by a copyright exception or limitation, it would not constitute either an infringement, or an act out counterfeiting;
- *Intentional element:* the offence should be committed with either *malicious* or *fraudulent* intent. The Belgian respondent noted that *malicious* intent is very broadly interpreted, essentially covering any aim to provide an unlawful, even non-financial and indirect benefit to oneself or a third party. For example, any profit-based intent – even if no actual profits are gained – suffices to meet the threshold in article XI. 293 BCEL.

Therefore, similarly to Portugal, the threshold for an act to qualify as criminal online piracy in Belgium is rather low. The Belgian respondent gives the example that any form of illegal downloading could be considered as being committed with a malicious intent, i.e., granting oneself a (non-)financial benefit, and would constitute a criminal offence. Nonetheless, due to insufficient means of the prosecution to investigate all instances of online piracy, priority is given to cases where perpetrators engage in commercializing or spreading illegally obtained content on a large scale.

Recommendation for the game: The game should, if possible:
Inform children that copyright infringements not only cause damages to authors but can also lead to criminal prosecution, as in some countries the threshold for criminality is very low;
Highlight that online piracy is more likely to be prosecuted when committed on a larger scale or to make profit.

The respondents that noted that their countries are, or have been in the past, actively prosecuting minors for online piracy are **Germany**, the **United Kingdom**, and the **USA**.

Germany criminalizes the illegal use and distribution of copyrighted content not in the German Penal Code (StGB), but in a special intellectual property rights act (Urhebergesetz, UrhG). According § 106 UrhG, a person will be punished with a fine or a prison sentence of up to 3 years if they duplicate, distribute, or publicly display a copyright protected work without authorization. However, offences can only be prosecuted upon a request by the victim (the rightsholder), unless the public attorney confirms a public interest in law enforcement (§ 109 UrhG). The German respondent highlighted that law enforcement against juvenile offenders was particularly relevant in Germany with respect to illegal filesharing on platforms like Napster. He also noted that under German copyright law the exception for 'private use' (i.e., downloading a movie to watch at home) is not applicable if the content is shared

at the same time as is the case with filesharing platforms. This apparently came as a surprise to youths who were prosecuted criminally for using file sharing platforms. The respondent noted that a mistake of law is handled very strictly under German law and only excludes liability in exceptional cases (§ 17 StGB). In other words, even if juveniles are not aware that their actions are illegal, this is unlikely to be an obstacle for their prosecution.

Reporting of criminal offences to the public prosecution office used to be more widespread several years ago because the previous German Copyright Act obliged rightsholders to report a criminal offence in order to file a civil lawsuit against the alleged copyright infringer.[103] Many cases therefore were also brought against infringements committed minors, although often copyright holders address their claim directly against the parents.

For example, in 2007 a music company filed a criminal complaint against a parent of a 13-year-old child who used a peer-to-peer filesharing flatform to make 1147 musical works freely and publicly available. The defendant refused to pay damages which led to follow-up civil proceeding where the music company asserted the parent, who obliged to supervise his children, and had failed to instruct his child on the dangers of the internet in general and on copyright violation and filesharing in particular. The court held that parents are in general not required to monitor the children's Internet usage and *"in the case of a normally developed 13-year-old child the condition "fulfils the requirements of his duty to supervise" is met when the parents regularly advise and instruct their children on the fact that illegal activities such as file sharing shall not be permitted".*[104]

Recommendations for the game: The game should, if possible:

Inform children that file sharing is generally considered illegal if is used to download/upload copyright protected content such as films, music, video games, etc.

Illustrate that parents are often liable to pay damages and can even be prosecuted criminally for their children's copyright infringements.

In the **UK** it is also illegal to both upload and download copyrighted content without the permission of the rightsholder. The respondent notes that online piracy is usually treated as civil offence, although in certain circumstances (i.e., in cases of severe infringement) it can also be deemed a criminal offence with damages awarded by a court. If the action results in financial loss for the content creator, such as lost income from licensing the work, then the offender may also face claims for compensation. The respondent also remarked that public policy and enforcement efforts towards online piracy in the UK have been very uneven and but it is now extremely unusual for minors to be prosecuted for copyright offences.

Nonetheless, the music and film industry in the UK remain determined to pursue charges and seek damages for copyright infringements, regardless of the age of the age of the infringer. The UK respondent mentioned a couple of cases where the British Phonographic Industry (BPI) filed charges against minors for online piracy. In one of them, the home of a 17-year-old boy was raided by the

[103] Benjamin Schuetze, *BGH: Are parents liable for their children? (Germany)*, Kluwer Copyright Blog (2012). Available at: http://copyrightblog.kluweriplaw.com/2012/11/19/bgh-are-parents-liable-for-their-children-germany/.
[104] Ibid.

police, Trading Standards officers, members of the International Federation of the Phonographic Industry (IFPI) and the BPI. He was charged with illegal downloading for sharing three albums and one single. The defendant's solicitor argued that he was a "victim of a cynical attempt by the record industry to legitimise its heavy-handed tactics and dubious methods by using police resources and the public purse" and prosecutors eventually dropped the case noting it was not in the public interest to pursue it.

In another case in 2011, however, the BPI were successful in pursuing a case against a young adult for running the download site Dancing Jesus. The infringer was a minor when he had originally begun to engage in file sharing but was 22-years-old when arrested. He was given a prison sentence of over two years which was the longest ever sentence for music piracy in the UK.

In the **USA**, the approach towards copyright infringement is notably stricter in comparison to the other countries in focus. The US respondent illustrates this by noting that according to the Federal Bureau of Investigation, "theft is theft, and if you're going to wilfully steal another party's intellectual property, the FBI stands ready to step in and shut you down."

The primary statute that criminalizes copyright infringement is § 506 of the Copyright Act, which regulates three essential copyright crimes:

1. Wilful infringement "for purposes of commercial advantage or private financial gain," 17 U.S.C. § 506(a)(1)(A).
2. Wilful infringement by "the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000," 17 U.S.C. § 506(a)(1)(B). This infringement does not have a financial component.
3. Wilful infringement "by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution," 17 U.S.C. § 506(a)(1)(C) (enacted in 2005). This infringement (referred to as "pre-release" piracy) also does not have a financial component.

The statute also criminalizes other acts, such as removing a copyright notice from a protected work, fraudulently displaying a copyright notice. The US respondent highlighted that due to the general rule that ignorance/mistake of the law is no defence to a criminal prosecution, minors could be prosecuted for acts of online piracy in the USA. The conduct under § 506, however, needs to be "*wilful*", i.e, a voluntary, intentional violation of a known legal duty which is often a contentious issue in online piracy cases.

Recommendation for the game: The game should, if possible, make it clear that not knowing a certain act is illegal and infringing on other people's rights, does not exclude criminal responsibility.

The respondent also noted that criminal prosecutions of copyright infringement often involve schemes where people intentionally infringe thousands and millions of copyright-protected works and operate large-scale piracy rings in order to massively profit from them. Another often prosecuted act is where people create technology or devices that are primarily intended to enable copyright infringement.

Moreover, the US Copyright Act is not the only legislation that regulates illegal copyright infringement in the States.

The No Electronic Theft Act of 1997 further outlaws cases when the person who received or expected to receive copyrighted work did not profit through commercial or personal gain, i.e., it is illegal to even *attempt* to acquire pirated media through file sharing rather than paying for the intellectual property.[105] The penalty for piracy in the USA can be up to 5 years in prison and $250,000 in fines, together with statutory damages. In addition, the Digital Millennium Copyright Act (DMCA), further makes it illegal to circumvent any protective technologies placed on copyrighted materials, and to tamper with copyright management software or protections.

The fact that the USA actively prosecutes online piracy is especially relevant for the game because oftentimes copyright infringements in Europe have as their object content from the US. In this respect, it should be noted that the USA government has asserted, and courts have repeatedly held, that a foreigner's activities outside the States can infringe US copyright law, so long the activity has some nexus with the United States. Indeed, there is a number of cases where US copyright law is being used against online piracy occurring outside of American borders.[106] For instance, in 2012 a man was charged for US criminal copyright infringement for being the head of an extremely popular Hong Kong-based website, Megaupload, that enable the worldwide sharing of unauthorised copies of US movies, TV shows and other copyrighted works. The USA government arranged for his arrest in New Zealand, even though he was not a USA citizen, didn't reside in the USA, and the vast bulk of his allegedly infringing activities occurred outside the USA.[107]

Another notable case is *Shropshire v. Canning*. Canning is a Canadian who uploaded a homemade video that used a US copyrighted song to YouTube.ca. The video was uploaded from Canada and could be viewed by other Canadians. Nonetheless, the video was allegedly stored on YouTube's servers in California and could also be seen on YouTube.com, the company's USA-oriented website. That was enough for a US district court judge to hold that Canning could be sued for violating US copyright law. Canning didn't know his uploaded video would have any connection to the US, but his lack of knowledge was deemed irrelevant. According to the court, "*Direct infringement does not require intent or any particular state of mind*."[108]

An important aspect of copyright infringement is that even in cases that are not serious enough to be prosecuted criminally, or where the state is unwilling to take criminal action against juveniles, copyright holders can enforce their rights through civil law measures. As analysed in Section 1.4., damages can be claimed by private parties for infringements committed by juveniles either against the minors themselves, or more often, against their parents.

[105] Bossler, A. M. (2020). Cybercrime legislation in the United States. *The Palgrave handbook of international cybercrime and cyberdeviance*, 257-280.

[106] Steven Seidenberg, *More Foreigners Find Themselves Targets of US Copyright Law* (2012), Intellectual Property Watch. Available at: https://www.ip-watch.org/2012/03/15/more-foreigners-find-themselves-targets-of-us-copyright-law/.

[107] Ibid.

[108] Ibid.

This is certainly the case in the **USA** where claimants, usually record companies, can (and often do) bring claims against the parents of children who allegedly infringe copyright via either indirect copyright liability or state parental liability statutes.[109]

Recommendation for the game: The game should, if possible, highlight that the US has an active policy in prosecuting both minors and foreigners for copyright infringements. It should, if possible, inform children that foreign copyright holders may seek to enforce their rights even abroad.

6.4. Recommendations for the RAYUELA serious game

The recommendations of this section are the following:

- The game should, if possible, distinguish between lawful use of copyrighted content without the permission of the author (e.g., in the context of education, parody, commentary) and unlawful copyright pirating;
- The game should, if possible, inform children about platforms that provide legal access to content and guide them on how to distinguish legal from illegal sources;
- The game should, if possible, inform children that copyright infringements not only cause damages to authors but can also lead to criminal prosecution, as in some countries the threshold for criminality is very low;
- The game should, if possible, highlight that online piracy is more likely to be prosecuted when committed on a larger scale or to make profit;
- The game should, if possible, inform children that file sharing is generally considered illegal if is used to download/upload copyright protected content such as films, music, video games, etc.;
- The game should, if possible, illustrate that parents are often liable to pay damages and can even be prosecuted criminally for their children's copyright infringements;
- The game should, if possible, make it clear that not knowing a certain act is illegal and infringing on other people's rights, does not exclude criminal responsibility;
- The game should, if possible, highlight that the US has an active policy in prosecuting both minors and foreigners for copyright infringements. It should, if possible, inform children that foreign copyright holders may seek to enforce their rights even abroad.

[109] See EFF, Parental Liability for Copyright Infringement by Minor Children (2007). Available at: https://www.eff.org/document/parental-liability-copyright-infringement-minor-children

7. Hacking and Cybercrime as a Service (CaaS) by minors

7.1. Introduction: what is hacking and CaaS?

Hacking refers to the activity of seeking to compromise digital devices, such as computers, smartphones, tablets, and even entire networks through unauthorized access to an account or computer system. In the typical setting, hacking requires strong technical skills. Especially in countries such as the USA, hacking is often associated with young people with strong technical capabilities. While hacking can be done for a variety of reasons, not all of them inherently malicious or criminal, it is commonly associated with illegal activity (e.g., fraud, extortion, data theft). Depending on the applicable law, hacking tends indeed to be an illegal activity, unless covered by a specific setting that justifies the activity, e.g., a service contract between hacker and target or an ethical hacking policy defined by the target to allow hackers to do a penetration test on the system. In those cases, the access is no longer completely unauthorized, which should help alleviate the legal concerns.

Cybercrimes as a Service (CaaS) refers specifically to turnkey hacking tools that allow would-be criminals who lack the technical skills to nonetheless commit technical cybercrimes such as hacking.

Neither hacking nor the creation or use of Cybercrime as a service by minors are part of the main crimes in focus in the RAYUELA project, but they have been identified as fields of relevance since the inception of the project. While the game will focus in large part on the children's awareness surround technology risks, e.g., in relation to connected devices and wearables, it must not be forgotten that some children, especially in the older ranges targeted by RAYUELA (e.g., a 14-year-old or 15-year-old) may be quite tech-savvy. Hence, it may be very useful to cover both hacking and the creation of CaaS, as well as the use of CaaS. While many of the players will not be tech-savvy to the point of knowing how to hack or create technical CaaS services while playing the game, it seems prudent to treat children as capable actors, taking into account some of them may possess substantial technical expertise already or may develop this in the near future. In addition, some children may think hacking is cool or innocent ("just for fun"), which makes it all the more relevant to address it in the game as well. For this reason, the respondents were also asked to identify potential criminal qualifications that could apply specifically to these types of cybercrimes committed by minors.

With regards to this topic, it is relevant to make mention of the 2001 **Budapest Convention on Cybercrime**, before addressing the answers of the national correspondents. The Budapest Convention is an international treaty with the Council of Europe that seeks to deal with crimes committed via the Internet and computer networks, in particular dealing with copyright infringements, computer fraud and forgery, child sexual abuse materials and network security. It contains both provisions for substantial criminal law of the States that are a party to the convention, as well as a number of powers and procedural provisions that aim to enable that every State party to the convention has sufficient powers in its national procedural law to search computer networks, access and seize computer data, can collect real-time traffic data and intercept contents of communications, and can use these powers for international cooperation.

In particular the following crimes are required to be included in substantive criminal law of the signatories:

- Illegal access to whole or any part of a computer system without right. Parties may decide to impose the additional requirement that the access infringes security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system. (Article 2 Budapest Convention);

- Illegal interception, e.g., the intentional interception without right, by technical means of non-public transmissions of computer data to, from or within a computer system. Parties may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system (Article 3 Budapest Convention);
- Data interference, e.g., the intentional damaging, deletion, deterioration, alteration or suppression of computer data without right. Parties may require that the conduct results in serious harm for it to be punishable (Article 4 Budapest Convention);
- System interference, e.g., the intentional and serious hinder, without right, of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data (Article 5 Budapest Convention);
- Misuse of devices, e.g., the intentional production, sale, procurement for use, import, distribution or otherwise making available of devices, programs or other tools designed, adapted or intended to commit one of the crimes of illegal access, illegal interception, data interference of system interference, without right. Also covered is the possession of such items with intent to commit these offences. The Article should not be interpreted as imposing criminal liability in this regard if the production, sale, procurement for use, import, distribution or otherwise making available is for other purposes. Parties may require that a number of items are possessed before criminal liability attaches, and may even opt out, provided they at least make the sale, distribution or otherwise making available a punishable offence (Article 6 Budapest Convention);
- Computer-related forgery, e.g., the intentional input, alteration, deletion, or suppression of computer data, without right. The forgery should result in inauthentic data, with the intention that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible. Parties may require that there is an intent to defraud, or similar dishonest intent, before criminal liability attaches (Article 7 Budapest Convention);
- Computer-related fraud, e.g., the intentional causing of a loss of property to another person, without right, by any input, alteration, deletion or suppression of computer data or any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person (Article 8 Budapest Convention).

These offences directly relate to the hacking and CaaS questions in RAYUELA. Computer related forgery and fraud are also relevant to the deception part of MD above.

The Budapest Convention has been ratified and has entered into force in the following countries in our sample: **Belgium, Bulgaria, the Czech republic, Estonia, Germany, Greece, Latvia, Portugal, Romania, Slovakia, Spain, the Netherlands, the UK and the USA**. In these countries it can be expected that the provisions of the convention are implemented, even if not always mentioned by the respondents.

From our countries in focus, **Brazil and Mexico** are in the process of accession, but have not signed the convention, **South Africa** has signed but not ratified the convention, and **China and Russia** have neither signed nor are they in the process of accession.

As with the preceding sections, it is important to realize that respondents were given a rather specific question and may fail to exhaustively enumerate all provisions of their national law that may potentially apply in situation of hacking or the creation and use of CaaS. Moreover, the respondents were really only asked about the use of CaaS, and not specifically about creation of CaaS products by minors, so this angle therefore did not really receive attention in the answers. It may however be assumed that the creation of CaaS services will often be punishable under the rules applicable to hacking, even if not mentioned by the respondent, as many respondents pointed out that the creator of the CaaS solution would be punishable as a collaborator or co-perpetrator to the hacking behaviour in their answers to the question of potential criminal liability for CaaS users.

With these potential limitations in mind, the following section discusses the answers of the different respondents and the interesting trends that could be identified.

Moreover, since the Budapest Convention is in force in 14 of the countries in focus, the answers of the respondents for these countries are to be read in conjunction with the knowledge that for these countries all the crimes mentioned above are present in the national criminal law, even if not explicitly mentioned.

7.2. How is hacking and CaaS regulated in the countries in focus?

In relation to hacking and CaaS, our respondent for **Belgium** mentioned the following offences:

- Art. 550bis §1 of the Criminal Code defines the offence of external hacking: “A person who, while knowing that he is not entitled to do so, gains access to a computer system or maintains himself therein”;
- Art. 550bis §2 of the Criminal Code defines the offence of internal hacking: “A person who, with fraudulent intent or with the intent to harm, exceeds his access rights to a computer system”;
- Art. 550bis §5 of Criminal Code criminalises any person who, unlawfully possesses, produces, sells, obtains with a view to its use, imports, distributes or in any other way makes available any instrument, including computer data, designed or adapted to commit hacking offences;
- Art. 550bis §6 of the Criminal Code the ordering or incitement of a hacking offence constitutes a separate offence;
- Art. 550bis § 7 of Criminal code punishes any person who, knowing that data have been obtained through hacking, retains such data, discloses or disseminates them to another person, or makes any use of them;
- Art. 210bis of the Criminal Code: IT-forgery is a crime under Belgian law: "entering into a computer system, altering, deleting or by any other technological means changing the legal meaning of such data which are stored, processed or transferred by means of a computer system".

- Art. 550ter Criminal Code on IT sabotage punishes "directly or indirectly entering data into a computer system, modifying or deleting data or altering the normal use of computer data by any other technological means while knowing that he is not entitled to do so."

These qualifications punish instances of hacking and creation of CaaS but also potential scenarios of use of CaaS. Minors are in principle liable for such offences under the Belgian juvenile system.

The respondent notes that the required intent of the applicable offence will be relevant to determine whether an offence applies. Depending on the criminal offence in question a general intent may suffice. This is the case for instance for the general external hacking offence, which will apply irrespective of the motives, e.g., if the minor considers it to be a joke or prank. The same is true for IT sabotage, which is punishable both if committed with a general or fraudulent intent. Other crimes require more specific intent. For example, for IT-forgery, a fraudulent intent or intent to harm is required. Using a fake profile for the sole purpose of an innocent prank will therefore not qualify as IT-forgery. In a similar vein, IT-fraud presupposes intent to obtain illegal economic advantages for oneself or for another person. Effectively obtaining these advantages is not required to commit the crime, the intent suffices. However, without this intent there is no IT fraud.

For **Bulgaria**, the respondent mentions in particular the following Articles:

- Article 319a, which punishes anyone who copies, uses or obtains access to computer data in a computer system without permission, where such is required;
- Article 319b, which punishes anyone who, without consent by a person administering or using a computer system, installs, modifies, deletes or destroys a computer program or computer data, where the occurrence is not considered insignificant;
- Article 319c, which punishes anyone who commits the act under art. 319b with regard to data that are provided electronically or upon magnet, electronic, optic or other carriers;
- Article 319d, which punishes anyone who introduces a computer virus in a computer system or in a computer network, as well as the person who introduces another computer program which is intended to disrupt the work of a computer system or a computer network or to discover, erase, delete, modify or copy computer data without permission, where such is required, as long as this does not constitute a graver crime;
- Article 319e, which punishes anyone who discloses passwords or codes for access to a computer system or to computer data, and personal data or information which qualifies as secret of the State or another secret protected by the law are thus revealed.

The respondent notes that all these provisions apply to minors, who may in theory be prosecuted under the juvenile regime, but mentions that there is usually no prosecution of minors. Rather, if children would commit such crimes the outcome would tend to be that parents compensate the damages and undertake educational measures. The respondent explains further that there are to their knowledge no known cases of computer fraud committed by children that were serious. The focus should be on prevention of children committing more serious crimes in the future.

For the **Czech Republic**, the respondent notes only that minors cannot be punished for such offences but can only be prosecuted under the juvenile regime which is aimed at imposing measures of reformation, not punishment, moreover only as of 15 years old.

For **Estonia**, the respondent mentions the main hacking offence of §217 of the criminal code, which punishes "illegal obtaining of access to computer systems by elimination or avoidance of means of protection".

Regarding the use of CaaS, the respondent states that the use of CaaS services is not in itself punished, however if used to commit another crime (e.g., fraud, money laundering, extortion, etc.) this may be caught.

The respondent notes that hacking and CaaS offences may be committed by minors, but adds that minors are rarely prosecuted and only in case of severe or repeat offences. The respondent notes that the intent of the minor is relevant in the sense that it should be established that the minor knew that what they were doing is illegal and that there was at least an indirect intent to commit the crime. However, the most likely scenario for an offender is probably a warning from the police or prosecutor, but not real prosecution.

With regards to the legal situation in **Germany**, our respondent explains that minors can be punished for hacking especially in cases, where they obtain access to data, which were not intended for them and were specially protected against unauthorised access by circumventing the access protection (§ 202a StGB, data espionage). This can also apply to exploiting vulnerabilities in IoT and connected devices, as long as there was some kind of relevant access protection the offender circumvented.

Another relevant provision mentioned is § 202b StGB (phishing); offenders are criminally liable if they intercept data which are not intended for them, either for themselves or another party, by technical means from non-public data transmission or from an electromagnetic broadcast from a data processing facility.

In addition, the respondent mentions that preparatory acts to data espionage or phishing can be punished according to § 202c StGB, e.g., the producing, acquiring, selling, supplying to another, disseminating or making available in another way of passwords or other security codes which provide access to data or computer programs for the purpose of a commission of the before mentioned offences.

Other related offences that are mentioned are:

- § 202d StGB (handling of stolen data), which punishes anyone who procures, for themselves or for another person, supplies to another person, disseminates or otherwise provides access to data which are not generally accessible and which another person has obtained by an unlawful act for the purpose of personal enrichment or the enrichment of a third party or to harm another person;
- § 303a StGB (data manipulation), which punishes anyone who unlawfully deletes, suppresses, renders unusable or alters data;
- § 303b StGB (computer sabotage), which punishes anyone who interferes with data processing operations which are of substantial importance to another by committing an offence under §

303a (see above), by entering or transmitting data with the intention of adversely affecting another or by destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier.

The respondent notes that criminal liability for all these offences requires intentional behaviour; mere negligence is not sufficient. All offences are applicable to juvenile offenders as well, and juvenile offenders can be punished with the full range of special juvenile sanctions. In practice, however, courts will impose a non-custodial sanction in almost all cases due to the less severe character of the offence.

With regards to CaaS, the respondent explains that minors, like adults, can be punished for acts of using Cybercrime as a service. Two specific scenarios are mentioned:

- If the offender (e.g.) buys certain passwords or security codes on a darknet platform in order to commit data espionage (§ 202a StGB) or phishing (§ 202b StGB), this preparatory act itself is punishable according to § 202c StGB.
- If the offender "orders" the commission of a certain cybercrime (like e.g., data espionage or phishing) by other persons online, criminal liability depends on the question if this crime is actually committed. If this is the case, the offender would be liable for this offence in terms of incitement (§ 26 StGB), with the same range of punishment a perpetrator would have to face. If the cybercrime is not committed for whatever reason, the offender is only criminally liable for attempted incitement to this offence if the latter is a felony (Verbrechen) according to § 12 StGB, i.e. a severe crime like robbery or homicide with a minimum statutory punishment of at least one year of prison. Neither of the before mentioned cybercrime offences is a felony, however, so the attempt of incitement would not be punished in these cases.

Although not specifically mentioned by the respondent, in as far as CaaS is used purely as an enabling tool to commit a specific crime itself, the above discussed hacking crimes could likely apply.

The respondent also notes that a somewhat "innocent" intent would – as a rule – not exclude criminal liability, as long as the offender still acted with sufficient intent (Vorsatz) concerning the objective elements of the offence in question, e.g., willingly and knowingly fulfilled these elements. If the "innocent" intent leads to a mistake of law (Verbotsirrtum), where the offender lacks the awareness of acting unlawfully, punishment is legally excluded if this mistake was unavoidable (which is, however, only rarely assumed by the courts).

For **Greece**, the respondents note that minors can also be punished and be prosecuted as perpetrators for acts of hacking when gaining unauthorized access to any information and communications technology, including the cases in which they might also take advantage and exploit any vulnerabilities in IoT or connected devices, of course applying the Greek juvenile system.

Mentioned in particular are the following provisions:

- Article 370B "Illegal Access to Information System or Data" of the Greek Penal Code, (par. 1), which punishes whoever, in violation of protection measures and without right, gains access to part or to the whole of the information system or electronic data. In particular mild cases the act goes unpunished;

- Article 370B, Par. 2 (internal hacking), which mentions that if the perpetrator is in the service of the lawful holder of the information system or electronic data, the act referred to in the preceding paragraph shall be punished only if it is explicitly prohibited by an internal regulation or by a written decision of the holder or its competent official;
- Article 370C, which punishes whoever unlawfully copies, prints, uses, discloses to a third party or in any way infringes data or computer programs, which constitute state, scientific or professional secrets or secrets of a public or private sector enterprise. Confidentiality is also considered to be those which the legal owner, out of justified interest, treats as confidential, especially when he has taken measures to prevent third parties from gaining knowledge of them;
- Article 370D par. 2, which punishes whoever gains unauthorized access to all or part of the information system or data transmitted by telecommunication systems, and doing so by violating prohibitions or security measures taken by its rightful owner;
- Article 370E, which punishes whoever, unlawfully, using technical means, monitors or captures on a physical medium non-public data transmissions or electromagnetic emissions from, to or within an information system or interferes with them with the aim of informing himself or others of their content, as well as whoever makes use of information obtained in this manner;
- Article 292B "Obstruction of the Operation of Information Systems", which may apply if the hacking has seriously obstructed or interrupted the operation of an information system by entering, transmitting, deleting, destroying, altering digital data or by blocking access to such data;
- Article 15 of Law 3471/2006, which regulates privacy in the field of electronic communications and imposes a penalty fee if the offender gained unauthorized access to personal data of the subscribers or users of the information system.

With regards to Cybercrime-as-a-Service, respondents note that minors may be punished for CaaS, in particular taking into account that they may be punished not only as offenders, but also as collaborators (Art. 45 of the Greek penal Code), abettor or agent provocateur (Art. 46), or Associate (Art. 47) to the crime. In addition to the articles already mentioned, the following qualifications are noted as potentially relevant:

- Article 292C, which requires the perpetrator to make available, possess or use of hardware, software or other tools with the intent to commit cybercrime, otherwise it goes unsanctioned;
- Art 386 of Criminal code, which punishes fraud.

Respondents agree that for both hacking and CaaS minors may be prosecuted for such offences under the juvenile framework, which will take into account the offender's age and the seriousness of the offence, including the intent. This also happens in practice, as was illustrated by one respondent with a pending case where 4 male minors are standing trial for illegal access (Art. 370), and possession of and distribution of illegal material, infringement of protection of personal data and defamation. Moreover, this is just one example of pending cases.

For **Latvia**, the respondent mentioned the following relevant provisions concerning hacking and CaaS:

- Section 241 (Arbitrary Accessing Automated Data Processing Systems), which punishes anyone who "commits arbitrary accessing of an automated data processing system, if it is related to breaching of system protective means or if it is carried out without the relevant permission or using the rights granted to another person, and if substantial harm has been caused thereby";
- Section 243 (Interference in the Operation of Automated Data Processing Systems and Illegal Actions with the Information Included in Such Systems), which punishes anyone who "commits unauthorised modifying, damaging, destroying, impairing or hiding of information stored in an automated data processing system, or knowingly entering false information into an automated data processing system, if substantial harm has been caused thereby";
- Section 244 (Illegal Operations with Automated Data Processing System Resource Influencing Devices), which punishes anyone who "commits the illegal manufacture, adaptation for utilisation, disposal, distribution, obtaining, movement, or storage of such tool (device, software, computer password, access code or similar data), which is intended for the influencing of resources of an automated data processing system or with the aid of which access to an automated data processing system or a part thereof is possible for the purpose of committing a criminal offence";
- Section 244.1 (Acquisition, Development, Alterations, Storage and Distribution of Data, Programs and Equipment for Illegal Activities with Electronic Communications Network Terminal Equipment), which punishes anyone who "commits altering of the data necessary for identification of electronic communications network terminal equipment in an electronic communications network or acquisition, storage or distribution of data intended for such purposes, as well as acquisition, development, storage or distribution of programs or equipment intended for such purposes without the consent of the manufacturer or its authorised person, if such activities have been committed for the purpose of acquiring property or if it has been committed by a group of persons according to a prior agreement, or if substantial harm has been caused thereby".

The respondent notes that all above norms are also applicable to minors, who would be treated under the Latvian juvenile system. However, according to information provided by state police, so far, no criminal proceedings have been instituted against minors for these offenses.

For **Portugal**, the respondents indicated that 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.

Some relevant parts of this law are as follows:

- Art. 4 (damage to programs or other computer data) punishes "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", as well as "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 aforementioned unauthorised actions;

- Art. 5 (computer sabotage) punishes "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", as well as "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 aforementioned unauthorised actions;
- Article 6 (Illegitimate access) punishes "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", as well as "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 aforementioned unauthorised actions.

Crimes under this law may be committed by minors, under the juvenile system (and with full liability as of 16 under Portugal's general rules on this). The focus of the juvenile system is however, as is typical, focused on rehabilitation and education. In particular measures may be imposed to teach minors that such behaviour is serious and not "fun" or "a prank".

For **Romania**, the respondent mentioned in particular that Art. 360 of the Criminal Code criminalizes the illegal access to a computer system, e.g., the access, without right to a computer system. Minors may in theory be punished for such an act under the general juvenile rules. Regarding CaaS, the respondent mentioned that minors may be more likely to provide CaaS than to rely on it, as they do not typically have financial resources to squander on CaaS. The respondent notes that no information on CaaS cases or investigations was available to them.

For **Slovakia**, the main hacking offence mentioned by respondents punishes "anyone who overcomes a security measure and thereby obtains unauthorised access to the computer system or part thereof" The offence can under only be committed by an offender who has reached the age of 14 and requires the element of intentionally committing an unauthorised intrusion into the computer system or part thereof by overcoming the security measure. The respondent mentions that this is not a common crime, 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. In addition, it is noted that this is a minor offence and upon prosecution the expectation would be that only a conditional sentence is imposed with compensation for the damage suffered. If the situation at hand is not very serious, it may not be prosecuted as a criminal offence at all, what the respondent refers to as the "material corrective".

Other cybercrime offences that are mentioned are the following:

- Slovakian law punishes anyone 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;

- Slovakian law punishes anyone who intentionally damages, erases, alters, suppresses or disables computer data or impairs its quality within or part of a computer system;
- Slovakian law punishes 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.

Regarding CaaS, the respondent explains that the Slovakian 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. *A contrario*, if CaaS is used as a tool and amounts to e.g., hacking (illegal access to computer systems) or illegal changing of data, it could be punishable under those offences.

For **Spain**, the respondent notes that minors can be punished for hacking and that in fact, the technological environment in which the behaviour takes place means that those who commit it are usually young and, on many occasions, minors.

The respondent mentions as the main provision of relevance Art. 197 bis of the criminal code, which punishes anyone who, by means of software or any other device, infiltrates a computer system and accesses data without the owner's authorisation and in violation of the right to “computer privacy”. The respondent notes that the wording of the offence foresees a subjective element that requires the will to violate the victim's privacy in order to know his secrets, and furthermore emphasises that the real danger lies in the integrity of the computer system in which the data is stored.

Another provision that is mentioned is Article 264 of the criminal code, related to hacking when the aim is to exploit vulnerabilities. Article 264 punishes “anyone who, by any means, without authorisation and in a serious manner, deletes, damages, deteriorates, alters, suppresses or makes inaccessible computer data, computer programs or electronic documents of others”.

Regarding CaaS, the respondent notes that minors can be punished for this as well, but that it is common to downplay the facts when the offender is a minor, because of the (assumed) lack of knowledge that is often involved in the commission of the offence.

The respondent note that children can more easily commit such offences than ever before, given the amount of information available, as well as tools (including CaaS), especially taking into account the (perceived) anonymity and feeling of security present on the internet, leading to a feeling of greater permissiveness. In this regard, the respondent explains the relevance of the fact that an attempt to commit a crime (e.g., a hacking offence) is punishable as well, unless the subject voluntarily desists from the execution. Hence, the fact that the crime did not completely succeed does not mean it cannot be punished, however the mere gathering of information on how to do something or playing around with this without an actual attempt cannot be punished. The respondent also notes that the legislation is more focused on protection of the minor as a victim. There have been reports that show an increase in offences committed by minors but there is no legislative action or guidance for institutions yet.

In the **Netherlands**, hacking is punishable under art. 138ab of the Dutch Criminal Code. This also applies if IoT or connected devices are hacked, as long as these devices qualify as a "computer", which likely is the case because of the broad definition of "computer". Minors can be prosecuted for hacking under the general rules of youth criminal law.

With regards to CaaS, the respondent notes that:

- If CaaS is used for DDoS attacks, this constitutes the crime of blocking access to or hindering the use of a computer (art. 138b DCC);
- Depending on the specific activity, CaaS might also be punishable as computer sabotage (Art. 161sexies DCC) or as system interference (art. 350c DCC).

Interestingly, the respondent notes that if the behaviour is "somewhat innocent", i.e., if there is no criminal intent, the act might still be punishable under one of the negligence offences:

- Art. 161septies DCC (the negligent causing of computer sabotage, involving a computer used for the common good or delivery of services), or;
- Art. 350b DCC (negligent data interference).

For criminal negligence to apply, the non-intentional behaviour must be reproachable, against the yardstick of what can be normally expected in human interactions. To make this assessment, age will be a relevant indicator of what is normally expected, as well as the broader context.

Minors can be prosecuted for these offences under the general rules of youth criminal law. However, the mentioned negligence offences are not usually applied and certainly not with regard to minors.

In **Brazil**, Article 154-A of the criminal code punishes anyone who would "invade a computer device for use by others, whether connected or not to the computer network, in order to obtain, tamper with or destroy data or information without the express or tacit authorization of the user of the device or to install vulnerabilities to obtain an unlawful advantage". This means that both the action of accessing or invading another individual's computing device (including smartphones, tablets, or others), without due authorization is punishable, as well acts committed in preparation, trying to exploit vulnerability (e.g., malicious software that allows access to the content of the computer device as soon as it is connected to the network). It is required that the invasion of a computer device be done with the purpose of obtaining, altering, or destroying data or information, with conscious intent to do so. The crime is consummated the moment the agent invades the victim's computer device, by means of undue violation of security mechanisms, or installs vulnerabilities in it, regardless of the production of the result sought by the invader (such tampering with or destruction of the victim's data or information or obtaining an illicit advantage).

Minors can also commit this crime. The respondent mentions that there are reports of minors being apprehended by authorities for acts of hacking or correlated actions, but that they were unable to find case law to prove that minors are being convicted of such crimes.

This Article applies to hacking quite clearly, but may also apply to CaaS. The respondent notes that while using CaaS is not specifically criminalized the elements for the crime of Article 154-A may be present. Moreover, under Article 29 of the criminal code, several persons may be agents/perpetrators in the same crime, which could apply in the case of CaaS. Hence minors could be punished for CaaS

depending on the situation and in particular when they are essentially paying for another party to commit a crime, even if they think it is a joke or a prank. The respondent mentioned that they did not find instances where minors were effectively convicted of such charges. However, this could potentially be due to the fact that these processes usually occur under judicial secrecy to protect the minor (agent) and the victim.

For **China**, the respondent mentioned the following as relevant to hacking and CaaS:

The "Network Security Law" stipulates that no individual or organization shall engage in activities that endanger network security, such as illegally intruding into other people's networks, interfering with the normal functions of other people's networks, stealing network data, or using programs and tools that endanger network security activities.

- Article 285 of the Criminal Law punishes “Whoever violates state regulations and invades computer information systems in the fields of state affairs, national defence, construction, and advanced science and technology “. Violating state regulations by hacking into other systems than the aforementioned or “using other technical means to obtain data stored, processed or transmitted in the computer information system, or illegally controlling the computer information system” is punished only if the circumstances are serious;
- Article 285 of the criminal law also punishes “whoever provides programs or tools specially used to invade or illegally control computer information systems, or provides programs or tools for others knowingly committing illegal and criminal acts of invading or illegally controlling computer information systems, if the circumstances are serious”;
- Article 286 of the criminal law punishes “Whoever, in violation of state regulations, deletes, modifies, adds or interferes with the functions of a computer information system, causing the computer information system to fail to operate normally” if the consequences are serious;
- Article 286 also punishes whoever is “deliberately making or spreading destructive programs such as computer viruses that affect the normal operation of the computer system, with serious consequences”.

The respondents notes that the prerequisite for punishing minors for such crimes as fully criminally liable is that the suspect is beyond the age of 16 years old. Reduced sentences may still apply for offenders under 18.

In addition, the respondent mentions the Public Security Administration Punishment Law, Article 29 of which provides for administrative sanctions for similar offences, namely for:

- (1) Violating state regulations, intruding into computer information systems and causing harm;
- (2) Violating state regulations by deleting, modifying, adding, or interfering with the functions of the computer information system, causing the computer information system to fail to operate normally;
- (3) Deleting, modifying or adding data and application programs stored, processed or transmitted in the computer information system in violation of state regulations;

- (4) Deliberately creating or spreading destructive programs such as computer viruses that affect the normal operation of computer information systems.

For **Mexico** the respondent mentions that minors may be punished for hacking. The Federal Criminal Code contains a full chapter prohibiting and sanctioning illegal access to computer equipment and information technology systems. Crimes pertaining to unauthorized access to computer systems are prosecuted as the result of an individual petition by the victim to the federal authorities. Title Nine, Chapter II of the FCC titled Illegal Access to Systems and Informatics Equipment consists of seven articles (Articles 211bis 1–211bis 7) that are generally used to criminalize and investigate illegal access to computer systems pertaining to the State, including information systems of the national financial and banking entities. The respondent notes that there is no sufficient evidence to conclude that minors that commit these types of conducts are being prosecuted by the national law enforcement authorities in practice.

With regards to CaaS, the respondent notes that neither the Federal Criminal Code nor the National Law of the Comprehensive Criminal Justice System for Adolescents criminalize acts using any instance of cybercrime as a service by minors. However, aiding and abetting could potentially cover this behaviour, despite those provision not being intended for the digital age.

Our respondent for **Russia** stated that hacking usually qualifies as unauthorized access to a computer information system under article 272 of the Criminal Code. Minors may subject to criminal liability only if they are in the age over 16 years old. The same article would also apply to various scenarios exploiting vulnerabilities in IoT and connected devices if it results in obtaining authorized access to information which is protected by law, including confidential information, personal data, state, banking or tax secrecy etc. In those cases where IoT is part of critical information infrastructure, criminal liability for hacking this would attach under article 274.1 (2) of the Criminal Code which provides higher criminal sanctions.

With regards to CaaS, the respondent indicates that using CaaS would make one qualify as an accomplice to the (hacking) crime committed. Complicity is regarded as equal to committing a criminal offence under Russian criminal law and is punishable. The general rule that only minors in the age over 16 years old may be subject to full criminal liability also applies in this case. The respondent indicated however that minors may in fact also be prosecuted in practice.

For **South Africa**, the 2020 Cyber Crimes Act (CCA) applies. The main hacking offence can be found in section 2, which punishes any person who unlawfully and intentionally secures access to data, a computer programme, a computer data storage medium or a computer system.

Other qualifications that are relevant are:

- Section 3 on unlawful interception of data;
- Section 4 on unlawful acts in respect of software or hardware tools (misuse of devices);
- Section 5 on unlawful interference with data or computer program;
- Section 6 on unlawful interference with computer data storage medium or computer system;

- Section 7 on unlawful acquisition, possession, provision, receipt or use of password, access code or similar data or device, this section punishes whoever acquires, has or provides tools for committing the other hacking offences, such as CaaS;
- Section 8 on cyber fraud;
- Section 9 on cyber forgery and uttering.

Section 11 of the CCA provides for aggravated offences against restricted computer systems which would include banks and any organ of the state and the Courts and any organisation of the state, which specifically has security measures in place

All these crimes as subject to the general legal position in South Africa on the prosecution of minors.

In the **UK**, minors can and routinely are charged with hacking offences. A significant number have also been prosecuted and convicted. The prevailing attitude in the UK is that minors have a disproportionate role in hacking and therefore need to be tackled with the full force of the law. For example, the National Crime Agency have suggested that 61% of computer hackers identified in UK begin their activity before the age of 16.

The main legal tool used against hackers (whether above or below the age of 18) is the Computer Misuse Act (1990) which contains three key sections defining computer related offences:

- Section 1 effectively criminalises hacking by making it an offence to obtain "unauthorised access to computer material";
- Section 2 extends the remit against hacking by making it an offence to obtain unauthorised access (to a computer/digital network) with intent to commit or facilitate commission of further offences. For example, access obtained in order to transfer funds from one account to another It is not necessary to prove that any intended further offence has actually been committed. Heavier penalties apply;
- Section 3 contains the most stringent provisions and is directed at ways in which hackers can disrupt or damage computer functionality. This makes it an offence to commit unauthorised Acts with intent to impair, or with recklessness as to impairing the operation of a computer. This covers acts such as inserting malware or spyware, modifying or deleting data and suspending operations via a DDos attack. Even more substantial penalties apply in this case.

The respondent notes that any charge under section 2 or 3 automatically also includes a charge under section 1.

Alternative legal tools include:

- The Fraud Act (2006), which can be used against those involved in pharming (cloning false websites for fraud) or the installation of trojan malware, again for the purpose of fraud;
- The Investigatory Powers Act (2016), which can also be directed against hackers who have been involved in unauthorised interception of a public or private telecommunication systems.

The respondent mentions several cases that were brought against minors under the Computer Misuse Act:

- *In 2016, a 16-year-old boy associated with the 'Crackas with Attitude' hacking gang was arrested for hacking into the email account of the Director of the CIA. The offender was able to release over 40 sensitive documents into the public domain as well as resetting the Directors AOL email account. He was given a two-year prison sentence of which he spent 8 months in the high security Belmarsh prison with a one-year probation with no internet access;*
- *A lesser sentence under the Computer Misuse Act was imposed upon another boy who was 16 when he engaged in a series of DDos attacks on leading multinational corporations like Netflix, Amazon, BBC, Vodafone, Nat West and even the UK National Crime Agency. The offender, who worked in conjunction with a digital crime group called VDos was responsible for launching over 2,000 attacks. Though he was 19 when the case came to court, the sentencing judge decided that he had been taken advantage of by the gang and that imposing a custodial sentence would be make him extremely vulnerable. As a result, he was sentenced only to 16 months in a young offender's institution, suspended for two years;*
- *Also in 2016, another boy - who was 17 at the time - admitted to involvement in a DDos based cyber-attack on the TalkTalk website and the leaking of customer details. TalkTalk lost over £70 million and had a £400,000 fine imposed as a result of the huge data breach. Though the offender was one of 10 individuals believed to have been involved in the attack and it was accepted that he did not expose the vulnerability which led to the attack he was sentenced to 8 months imprisonment under the Computer Misuse Act as he was over 18 when the case was eventually heard.*

In relation to CaaS, the respondent explained that making, adapting, supplying or offering to supply any article which can be used to commit a cyber-dependent related offence is an offence under Section 3a of the Computer Misuse Act (1990). This clause specifically targets the market in "hacker tools"; commonly used for breaking into, or compromising, computer systems. It thus covers many activities related to the use of CaaS such as using it to acquire malware, hiring botnets, adapting ransomware or similar. Providing software or devices which permits the exploitation of IoT or other connected devices for the purpose of fraud can also be an offence under the Fraud Act.

Prosecution generally follows intention or demonstrable harm so where the minor is purely involved as a joke, or has been influenced heavily by adults, it is unlikely that there would be consequences. Using the Fraud Act to secure a conviction in this context involve rigorous conditions. The individual must be proved to have knowledge that the CaaS object can be used for fraud, has been adapted it to that end, or has explicit intentions to use it for that purpose.

Mere possession of these tools can also be grounds for prosecution, though again with the aforementioned conditions attached.

The respondent indicates that in general, prosecutions tend to occur more for using the tool than for merely obtaining it. Some cases are mentioned to illustrate how practice has evolved:

- *In one case from 2005, a minor was charged with obtaining a CaaS mail-bomber tool called Avalanche. He used this to overwhelm the mail server of the D&G insurance company with over 5 million e-mails. His defence was a technical one. It suggested that since every e-mail that is sent to an e-mail server is in fact "authorised" to modify it (otherwise e-mail would not work) there is no specific point at which a large quantity of such e-mails suddenly become "unauthorised". The Court rejected this argument but felt that the Computer Misuse Act remained sufficiently ambiguous at that point for the prosecution's case not to be proved. They argued it was not up to them but to Parliament to properly extend this law;*

- *By 2015, the interpretation of the Computer Misuse Law had tightened. Six teenagers, aged between 15 to 18 were arrested for accessing and using the CaaS tool called Lizard Stresser. They used this to attack a number of gaming sites such as Microsoft's Xbox Live and Sony's Playstation network. The youths were*

bailed and because of their age were not ultimately given a custodial sentence, but clear precedents had been set about the consequences of using CaaS tool, irrespective of age.

Minors who create or distribute tools used for CaaS are also routinely prosecuted, as well as minors who operate a cybercrime market themselves.

The respondents provide the following case to illustrate:

- *The boy who created and sold the Titanium Stresser CaaS tool when he was 15 was charged with two offences under the Computer Misuse Act following his arrest in 2016. The tool was used in over 1.7m cyberattacks and the offender was estimated to have made around £370,000 from its distribution. Though he was 20 when the case eventually came to court he was treated as a youth offender and sentenced to two years imprisonment in a youth offenders' institution;*
- *In 2011, three UK teenagers who created Ghostmarket, one of the largest online crime forums and markets were arrested but were not charged under the Computer Misuse Act, even though the site provided hacking 'tools' in the form of tutorials and tips. Because Ghostmarket also sold details of credit card numbers resulting in estimated losses of over £16 million they were charged with offences under the Fraud Act. Two of the youths were under 18 when the site was first created, but were handed substantial custodial sentences.*

For the **USA**, the respondent mentions that the Computer Fraud and Abuse Act (CFAA) is the most important piece of federal legislation in the United States that deals with cybercrime in general and computer hacking specifically. The CFAA is used to prosecute attacks against "protected computers," which can be defined as a computer "(a) exclusively for the use of a financial institution or the United States government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (b) which is used in or affecting interstate or foreign commerce or communication" (18 U.S.C § 1030 (e) (2))."

The CFAA specifies seven applications of hacking that violate federal law including:

- Obtaining national security information;
- Accessing a computer and obtaining information;
- Trespassing in a government computer;
- Accessing a computer to defraud and obtain value;
- Intentionally, recklessly or negligently damage a computer during by intentional access;
- Traffic passwords;
- Extorting using computers.

18 U.S.C. § 2701 (Unlawful Access to Stored Communications) is an additional Federal statute which could be used for the prosecution of hacking. This statute makes it illegal to either "intentionally access[es] without authorization a facility through which an electronic communication service is provided" or "intentionally exceed[s] authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." Punishments under this statute were increased under the Homeland Security Act of 2002 if the offense was committed for "purposes of commercial advantage, malicious destruction or

damage, or private commercial gain, or in furtherance of any criminal or tortuous act in violation of the Constitution or laws of the United States or any State".

Computer hacking and the use of code for unauthorized access are criminalized at the state level as well. All of the US states have passed computer crime legislation with most laws addressing computer hacking or unauthorized access. Most states use a two-tiered system to prohibit hacking behaviours with simple hacking (unauthorized access but no damage to the system or further criminal behaviour) being considered a misdemeanour and aggravated hacking, unauthorized access leading to further criminal behaviour in the form of copying or destroying of data, being treated as a felony. However, other states use a single statute to criminalize unauthorized access regardless of whether further criminal activity occurs. States also differ on whether they criminalized these behaviours under existing statutes relating to burglary and theft or whether new statutes were enacted to establish the unique characteristics of computer hacking more clearly.

Known issues in the application of these statues evolves around the court interpretation of the word "access", as well as the interpretation of "authorized access." In the context of "access," courts may interpret access to a computer as either virtual or physical. Under the "virtual access" interpretation, access hinges on whether the user has made a virtual entrance into the computer. Using this interpretation one can imagine a user trying to use a password-protected computer network and is confronted by a screen that requires a valid username and password to proceed. The screen requiring the logging credentials is akin to a lock on a front door, and entering a username and password is like using a key to open the lock. In contrast, under the "physical access" interpretation, we recognize that computers are simply machines that communicate with each other by sending and receiving information. Under this approach, one can interpret access by looking to whether a user has sent communications that have physically entered the computer. The respondent mentions the following cases to illustrate the different interpretations:

- *In State v. Riley, the court adopts the view that access can be pretty much anything that interacts with a computer. In this case, the defendant was accused of calling the general number of Northwest Telco Corporation (which provided long-distance telephone service) and entering random numbers every 40 seconds to try to discover access codes, which then could be used to place long distance calls. The defendant was convicted of three counts of computer trespass and four counts of possession of a stolen access device after he used his home computer to obtain long-distance telephone access codes from telephone company computers;*

- *In contrast, in State v. Allen, the court adopted more of a virtual view that the user has to virtually "enter" the machine to access it. In this case, the defendant used his computer to dial up access numbers of Southwestern Bell, and he then faced the prompts that asked him for a password that would enable him to make free long-distance telephone calls. The access numbers were only supposed to be known to Southwestern Bell employees. There was no direct evidence that the defendant had responded to the password prompt. The Kansas Supreme Court held that Allen had not accessed Southwestern Bell's computer.*

Another issue in the application of these computer access statues pertains to the question of what is authorization. The respondent mentions literature that suggests that there are three basic ways to set computer users privileges on a computer: by code, by contract, or by social norms.

When an owner regulates privileges by code, the owner or her agent designs and programs the computer's hardware and software so that the code limits each users' privileges. Perhaps every user

must have an account, and access to that account is protected by a password. For a user to exceed privileges imposed by code, the user must somehow "trick" the computer into giving the user greater privileges. The code creates a barrier designed to limit privileges. *United States v. Morris* is a classic case on code-based restrictions. In this case, the defendant was convicted under the Computer Fraud and Abuse Act for releasing a worm which caused computers at various educational and military sites to cease functioning. He appealed his conviction and argued the government had to prove not only that he intended the unauthorized access of a federal interest computer, but that he also intended to prevent others from using it. The Second Circuit concluded that the defendant could be convicted so long as the evidence showed that he intentionally accessed a federal interest computer without authorization and that damage was caused by this access. Since the worm was designed to invade computers at which he had no authority, express or implied, Morris's conviction was affirmed.

Alternatively, a computer owner or operator may regulate computer privileges by contract. Access to the computer can be conditioned on the user's promise to abide by a set of terms such as Terms of Service for an e-mail account or Terms of Use for a website. In *United States v. Nosal,* the defendant convinced some of his former colleagues who were working for an executive search firm the defendant used to work for as well to use their log-in credentials to the firm's computers and download source lists, names and contact information from a confidential database on the company's computer, and then transferred that information to the defendant. The employees were authorized to access the database, but the firm had a policy that prohibited disclosing confidential information. The government indicted the defendant on twenty counts, including trade secret theft, mail fraud, conspiracy and violations of the Computer Fraud and Abuse Act (CFAA). The defendant filed a motion to dismiss the CFAA counts, arguing that the statute only targeted hackers and not individuals who accessed a computer with authorization and then later misused information they obtained by means of such access. A federal appellate court affirmed the judgment arguing that a violation for exceeding authorized access occurs where initial access is permitted but the access of certain information is not permitted.

Finally, computer use might be unauthorized if it violates a social norm on computer use. Social norms are widely shared attitudes that specify what behaviours an actor ought to exhibit. In the context of computer misuse, access might violate a social norm if most computer users would understand that they are not supposed to access the computer in that way even if it does not circumvent a code-based restriction or breach an explicit contract-based restriction.

The respondent notes that since minors in the USA are subject to the same statutes as adults, they could be prosecuted for acts of hacking under the applicable rules for juveniles. The respondent mentions a 1997 case in which prosecutors brought Federal computer crime charges against a Massachusetts teenager whose modem mischief temporarily knocked out phone service to about 600 homes and a small airport's control tower. The teenager signed a plea barging in which he faced two years of probation, 250 hours of community service and $5,000 in restitution, which he needed to pay to Bell Atlantic, the telephone company he attacked. He was also forbidden to use a modem or other remote-access device for two years.

With regards to CaaS, the respondent notes that cybercrime-as-a-service is a broad concept and operations may involve many types of cybercrime, such as botnets, distributed denial of service attacks (DDoS), credit card fraud, malware, hacking, spam, and phishing attacks. These services are often sold through hacker forums, direct web sales, and on the dark web using cryptocurrency. Since many of the

crimes that fall under the definition of cybercrime-as -a-service may be prosecuted using the CFAA, subsection 1030(b) of the act, which makes it a crime to attempt or conspire to commit any of these offenses, could be used in this context. Since minors are subject to CFFA, they could be punished for these acts as well.

The foregoing shows that hacking is an offence known to every country in focus in one form or another. Similarities based on the Budapest convention are clear, but also the countries that are not signatories have laws that cover this behaviour. Minors are always capable of committing these offences, either under the juvenile system, or even under full criminal liability as an adult for minors of 16 or over (see e.g. **China, Russia, Portugal, Romania**) or even younger (**South Africa**, certain states in the **USA**). Interestingly, respondents had quite different views on whether minors are prosecuted in practice.

In the UK, this was mentioned as something that happens regularly, with minors and young people being a substantial part of offenders for technical offences such as hacking. The **USA, Russia and China** also noted this and the fact that prosecution will happen in practice. The other countries however, including nearly all EU countries either stated that there was little data or evidence of minors being prosecuted in practice or that prosecution would be unlikely, or were at the very least neutral on the topic, stating that it would be possible in theory, without providing case examples in practice. In fact, several respondents went further and noted that minors would not commit such crimes unless it's an innocent prank or similar, or would not likely have the necessary skills to commit such technical offences. This illustrates the stark contrast in legal traditions, with the **UK** respondent noting that "*The prevailing attitude in the UK, as elsewhere is that minors have a disproportionate role in hacking and therefore need to be tackled with the full force of the law. For example, the National Crime Agency have suggested that 61% of computer hackers identified in UK begin their activity before the age of 16".*

Despite any shortcomings that the sample may have, it is clear that legal traditions in the countries in focus approach the problem in quite divergent ways. While this may in part have to do with the fact that certain countries have more hackers and hence face the problem more often (China, the US, Romania being typically mentioned as countries that have the high numbers of hackers and high incidences of hacking offences and the UK respondent mentioning that 1 in 20 UK youths were involved in hacking offences in 2021) this is hardly the full story. Other countries in the sample also have reportedly high numbers of hackers and incidences and despite the various (online) data sources being at times of questionable reliability, it should be clear that hacking by minors does happen in practice and countries should not treat minors as not capable of such offences. As is explained in section 1.6, reliable crime statistics are clearly hard to come by and hence it is difficult to estimate numbers in practice, as well as to chart how many incidents with minor offenders never make it to the formal trial stage because they are considered not serious or because the country's juvenile justice system allows to impose educational and reformative measures, which are considered sufficient to deal with the problem.

Another relevant element is the intent of the minor. An element that may be relevant to the educational aspect of the game is that minors may see hacking as fun challenge or joke. However, only specific provisions mentioned by the respondents require a criminal or fraudulent intent. In the Netherlands, the respondent mentions that criminal intent is usually required, but that negligence offences exist as well (even though these are not usually relied on against minors). In most countries however, it is sufficient that the hacking was intentional, and it is of no relevance whether the intent

was somewhat innocent or even positive, as is the case with some ethical hackers. It is hard to argue that hacking is not intentional or that it does not constitute the intentional access to a system the hacker should know they are not allowed to access. Hence, minors may at times think hacking is a fun challenge or rather innocent, but the law in general does not agree with this.

Recommendation for the game: The game should, if possible, provide a hacking scenario which is meant quite innocently as a joke, prank or challenge, but turns out to lead to legal consequences, to illustrate that even in such scenarios, criminal liability may attach. Ethical hacking could be used as an example, where the ethical hacker is told by authorities to stop, without being prosecuted.

Regarding Cybercrime as a Service, the respondents who mentioned the creation of CaaS by minors tend to agree that this would constitute an offence, in particular the making available of tools for hacking offences and cybercrimes.

Recommendation for the game: The game should, if possible, introduce the element of creating, selling or distributing or otherwise making available of CaaS tools to others, to illustrate that this is behaviour that may incur criminal sanctions.

With regards to the use of CaaS, different opinions exist. Some respondents (e.g., the **UK**) mention that the mere possession is sufficient, whereas other respondents say that the procuring of a CaaS service is only punishable if it is in fact used to commit a crime (e.g., **Estonia, Slovakia**).

This is in line with Article 6 of the Budapest convention (misuse of devices), which in principle covers the intentional production, sale, procurement for use, import, distribution or otherwise making available of devices, programs or other tools designed, adapted or intended to commit one of the crimes of illegal access, illegal interception, data interference of system interference, without right. Article 6 does not cover situations where such tools are obtained for other intended purposes. Of course, this becomes a matter of proving the intent of obtaining certain tools. This may be different depending on the tool at issue and whether it has certain legitimate uses as well. Countries can also decide to require that in the case of mere possession, there must be a number of tools in possession of the suspect before criminal liability attaches. This also serves to prove that the tools were obtained for the purpose of committing a crime. However, the parties may opt out of the criminalization of possession altogether. Only the sale, distribution or otherwise making available must always be a punishable offence.

Recommendation for the game: The game should, if possible, provide introduce the element of procuring certain tools, but in a setting where the tool is perhaps not intended for criminal use (e.g., also has a far-fetched legitimate use or the tool/service is only bought under peer pressure without intent to use). The scenario or elements of a scenario are meant to illustrate that even the mere procuring such tools may in some countries be a punishable offence. It should also be illustrated that just looking up information out of curiosity does not constitute an offence anywhere.

In so far as the use of CaaS leads to the commission of a crime, hacking offences in particular included, all respondents agreed that minors would be punishable for that, either as a perpetrator or an accomplice (at least in theory, taking into account that some respondents noted that prosecution in practice is rare, non-existent or that they did not know of any cases).

Respondents noted again that in as far as hacking offences are committed, having innocent intent does not typically exclude prosecution. While it may be taken into account by prosecutors in practice, the law typically only requires that the actions were committed intentionally, not that the actions were intended to commit a crime, intend to harm or had fraudulent intent.

Recommendation for the game: The game should, if possible, introduce the element of using CaaS tools or a service to carry out a prank, take on a challenge by peers, to learn about how things work or to carry out ethical hacking without the skills (e.g., to use a tool to highlight weaknesses with the aim to disclose them afterwards), so as to illustrate that whenever tools are used for something that constitutes hacking, even with innocent or good intent is a punishable offence.

In the questionnaire, the link was made with WP2 and their work on the potential dangers of exploiting vulnerabilities in connected devices used by minors in their daily life. A couple of respondents picked up on this and mentioned that hacking and CaaS would be very relevant in this context as well. It could be considered to mix these perspectives and to set up a scenario including hacking or CaaS (perhaps ethical hacking or something of an innocent character) in the context of connected devices or wearables, which may present a scenario that minors playing the game can easily relate to.

7.3. Recommendations for the RAYUELA serious game

The recommendations of this section are the following:

- The game should, if possible, provide a hacking scenario which is meant quite innocently as a joke, prank or challenge, but turns out to lead to legal consequences, to illustrate that even in such scenarios, criminal liability may attach. Ethical hacking could be used as an example, where the ethical hacker is told by authorities to stop, without being prosecuted;
- The game should, if possible, introduce the element of creating, selling or distributing or otherwise making available of CaaS tools to others, to illustrate that this is behaviour that may incur criminal sanctions;
- The game should, if possible, provide introduce the element of procuring certain tools, but in a setting where the tool is perhaps not intended for criminal use (e.g., also has a far-fetched legitimate use or the tool/service is only bought under peer pressure without intent to use). The scenario or elements of a scenario are meant to illustrate that even the mere procuring such tools may in some countries be a punishable offence. It should also be illustrated that just looking up information out of curiosity does not constitute an offence anywhere;
- The game should, if possible, introduce the element of using CaaS tools or a service to carry out a prank, take on a challenge by peers, to learn about how things work or to carry out ethical hacking without the skills (e.g., to use a tool to highlight weaknesses with the aim to disclose them afterwards)., so as to illustrate that whenever tools are used for something that constitutes hacking, even with innocent or good intent is a punishable offence.

8. Conclusions

As can be seen in the recommendations' subsection of each section and in the conclusions, the general outcome of the study is that **criminal liability may indeed attach for minors who execute any of the abovementioned behaviours**. Sanctions (sometimes including custodial sentences), reformation and education measures, fines, civil liability and other consequences may apply depending on the specific circumstances and the severity of the behaviour in question. In some countries minors may at times even be tried as adults and tackled with full force of the law, in particular when they are older adolescents.

Crimes such as online grooming for sexual exploitation and online grooming for human trafficking are serious offences that have worryingly become more widespread post the Covid-19 pandemic. The game should, therefore, highlight the ways for minors to identify grooming behaviour and include scenarios with different types of perpetrators (e.g., adults with fake accounts, influencers, peers). One of the important findings of this report with respect to grooming-related crimes is that purely online predatory behaviour can be punishable in itself, even if the crime with a view to which the grooming is undertaken does not take place.

The answers from our respondents clarify that acts of cyberbullying and misinformation and deception are prosecuted worldwide under different crimes, depending on the relevant circumstances. The difference between legitimate and criminal behaviour online, however, is often difficult to determine, especially for minors. The game should, therefore, illustrate what type of communication online crosses the line of criminality and highlight the possible negative consequences of behaviour that amounts to criminal conduct.

Online piracy is another act that minors might commit without realising that it amounts to criminal activity. In this respect, the game should illustrate the difference between legitimate use of copyrighted content and illegal distribution. Another aspect that should be highlighted is the civil liability that is attached to online piracy even when it is not criminally prosecuted. Hacking and using cybercrime-as-a-service can be committed by minors as a joke, prank, or even as a result of peer pressure. It is important, therefore, that game includes scenarios that clarify that even 'innocent' hacking can constitute a punishable offence and even mere procuring of CaaS tools may be criminalised in some countries.

The game should therefore aim to provide guidance, based on the recommendations provide in this report, to explain to the young players at what point certain behaviour crosses the line from innocent into potentially criminal behaviour and to reinforce the importance of staying on the right side of the dividing line.

9. Annex 1

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) are 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.

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

Please provide details on known issues of application.

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.

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.

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.

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.

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.

Question 7: Can minors be punished for online grooming in your country? E.g., 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 (e.g., 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.

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.

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 cyberharrassment. 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.

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.

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

Please provide details on known issues of application.

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).

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

Please provide details on known issues of application.

Question 12: Can minors be punished for acts of online piracy in your jurisdiction, e.g., 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.

Question 13: Can minors be punished for acts of hacking (e.g., 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.

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.

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

Please provide details on known issues of application.

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.

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

Please provide details on known 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.

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

Please provide details on known 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.

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

Please provide details on known 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.

Please provide details on known issues of application.

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.

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.