Deliverable Report

D7.7 Policy Briefs

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant

Document Information and contributors

Deliverable No.	7.7	Work Package No.	WP7	Task/s No.	Task 7.3
Work Package Title		COMMUNICATION, DISSEMINATION & TRAINING FOR CYBERCRIME PREVENTION & AWARENESS			
Linked Task/s Title					
Status		Final version	(Draft/Draft Final/Final)		
Dissemination level		PU	(PU-Public, PP, RE-Restricted, CO-Confidential)		
Due date deliverable		30/09/2023	Submission date		18/10/2023
Deliverable version		4			

Deliverable responsible	ZABALA		
Contributors	Organization	Reviewers	Organization
Viera Zuborova	BPI	Lynne Henderson	PSNI
Mario Castro Ponce	COMILLAS	Susana Sola	PLV
Gregorio López	COMILLAS	Ruben Bleda	PLV
Jaime Pérez	COMILLAS	Violeta Vázquez	ZABALA
Gabriel Valverde	COMILLAS	Abel Muñiz	ZABALA
María Reneses	COMILLAS		
Pieter Gryffroy	TIMELEX		
Mari-Liisa Parder	TARTU		
Gregory Milopoulos	EA		

Document History

Version	Date	Comment
1	15/09/23	All policy briefs except WP6 (data analysis)
2	30/09/23	Including reviewers' comments and suggestions
3	15/10/23	Final draft including WP6 inputs
4	18/10/23	Final document including second review

Table of contents

Contenido

List of Abbreviations

Abbreviation	Description
CaaS	Cybercrime-as-a-Service
LGBTQIA+	Lesbian, Gay, Bisexual, Transgender, Queer, Intersex, and Asexual.
AI	Artificial intelligence
CSAM	Child Sexual Abuse Material

Executive Summary

Cybercrime poses threats to the safety and well-being of people across Europe. To tackle this pressing issue, we have prepared 10 policy briefs that analyse the problems affecting minors online worldwide from the different perspectives addressed in the project (i.e., human perspective, technological perspective, legal and ethical perspective, educational perspective, communications perspective, and data analysis perspective) , providing recommendations for solutions. These briefs cover online grooming, cyberbullying, human trafficking, misinformation, security and privacy concerns, problematic technology use, legal issues, education through gamification, effective awareness campaigns, and the insights on the considered cybercrimes coming from the analysis of the data gathered through the videogame. We identify factors that make minors vulnerable to these risks, such as isolation, weak family connections, and excessive internet usage. Furthermore, we examine offenders' tactics, such as manipulation, coercion, and deceit. The briefs also shed light on the consequences of victims, including trauma, social challenges, and reluctance to report crimes. We highlight gaps in existing frameworks and prevention efforts while offering recommendations focusing on raising awareness through campaigns promoting literacy programs for young people's safety online. We also emphasize the importance of stakeholders' cooperation and nurturing critical thinking skills and resilience in minors. Additionally, we discuss how emerging technologies like AI can be harnessed while ensuring design standards and oversight.

1. Introduction

Collectively, these policy briefs present an overview of cybercrimes' impact on minors. They offer insights to guide advocacy efforts and inform education initiatives, legislation development, enforcement measures, and technological advancements in this field. By working, stakeholders from different sectors can collaborate to establish a safer online environment. This will ensure that young individuals can take advantage of technology's benefits while being shielded from harm.

1.1. Target groups

The primary objective of the policy briefs is to communicate with and educate important groups involved in combating cybercrime that affects minors in Europe. One crucial target audience includes policymakers, at both the European Union and national government levels. The briefs aim to provide insights and recommendations to shape legislation, regulations and policies that can better address cybercrime against minors. It is crucial to establish policy frameworks and legal measures to safeguard children online.

Law enforcement agencies represent another group. The briefs offer information on emerging cybercrime trends, preventive strategies and recommendations that can assist law enforcement in strengthening their efforts against threats affecting minors. Their frontline role is of capital importance.

Academics and researchers who study issues related to minors, such as grooming, cyberbullying, human trafficking as the impacts of technology and social media, also form a significant audience. The briefs can support their work by providing up to date data for analysis. Their research plays a role in informing evidence-based policies.

Digital platforms like Facebook, Instagram or TikTok have an influence on people today. These briefs act as a guide for these companies in developing strategies and tools to enhance safety features and content moderation on their platforms. Their contribution towards protection is invaluable.

Civil society organisations, child protection agencies and youth advocacy groups have also a role in supporting and safeguarding minors. The efforts of these briefs are supported by insights showcasing their dedication to protecting children.

To ensure the safety of minors online, schools, educators and parents play a role in equipping them with knowledge. These briefs can empower these individuals by engaging in informed conversations about threats.

Additionally, the briefs directly target minors themselves, educating them about avoiding behaviours that could make them vulnerable to victimization. They emphasize the importance of reporting incidents of abuse and being responsible while navigating the world. The smart actions taken by minors are key to ensuring their safety.

In conclusion, the main objective of this policy brief is to inform and support all stakeholders involved in the mission of combatting cybercrime that affects European minors. As it has just been said, each stakeholder has an important role to play in this effort.

1.2. Objectives and aim

The safety and well-being of people in Europe are significantly threatened by cybercrime. To address these concerns, the RAYUELA project has developed 10 policy briefs that analyse various issues affecting minors in the online world. These briefs provide recommendations for solutions.

These briefs cover online grooming, cyberbullying, human trafficking, misinformation, security and privacy concerns, problematic technology use, legal issues, education through gamification, effective awareness campaigns, and the insights on the considered cybercrimes coming from the analysis of the data gathered through the videogame. They closely examine the factors that make minors vulnerable to these risks, such as isolation, weak family connections and excessive time spent online. Moreover, they delve into the tactics and strategies employed by offenders like manipulation, coercion, and deceit.

Furthermore, the briefs shed light on the distressing consequences experienced by victims of cybercrime. These consequences can include health difficulties, social challenges and a hesitance to report these hidden crimes. Throughout the briefs gaps in existing frameworks and prevention efforts are highlighted while offering recommendations with a focus on raising awareness. This is achieved through promoting literacy programs and educational campaigns aimed at enhancing people's safety and resilience online.

A key theme emphasized throughout the briefs is the importance of collaboration among stakeholders such as civil society organisations, law enforcement agencies, policymakers, academia and technology industry representatives.

The briefings emphasize the promise of new technologies, such as artificial intelligence, in tackling cyber risks for individuals if these technologies are designed and deployed in an ethical manner with human oversight (Hasse, 2019).

As shown in Table 1, RAYUELA team developed 10 policy briefs.They provide evidence-based insights to support the advocacy work of NGOs and guide the development of initiatives, legislation, law enforcement strategies and technological advancements in this field. By collaborating across sectors, stakeholders can create an online environment for young users in Europe. This ensures that minors can fully benefit from technology while being protected from exploitation and harm.

Table 1. RAYUELA POLICY BRIEFS

NO	Title	Number of policy brief
1	Review and Analysis of Online Grooming in Europe	1
2	Review and Analysis of Cyberbullying in Europe	2
3	Review and Analysis of Human Trafficking in Europe	3
4	Review and Analysis of Fake News, Deception, and Cyberhate	4
5	Role of Technology and AI to Improve the Online Experience of Minors	5
6	Cybersecurity and Privacy Threats of IoT Devices Widely Used by Minors	6
7	The Legal Landscape for tackling cybercrime offenses by Minors in Europe	7
8	Enhancing Cybersecurity Education Through Gamification - Insights from the Rayuela Project Pilots	8
9	Effective Awareness Campaigns and Social Media Strategies to Combat Cybercrime and Engage Minors and Children	9
10	General Policy Brief related to the Analysis of the Data gathered through the Videogame	10

These policy briefs consolidate research findings from projects focused on these issues to guide evidence-based policies while encouraging collaboration across sectors to combat cybercrime, targeting minors throughout Europe effectively.

The primary goals of these policy briefs are as follows:

1. Thoroughly examine the pressing challenges faced by minors, in Europe regarding cybercrime including issues like grooming, bullying, trafficking, spreading information threats to privacy and problematic use of technology.
2. Conduct an analysis of the factors contributing to risks and offender strategies well as the impact on victims. Identify any gaps in existing frameworks or prevention efforts.
3. Provide tailor-made recommendations and insights to stakeholders such as policymakers, law enforcement agencies, academics, technology companies, child protection groups, schools, parents and minors themselves.
4. Inform advocacy initiatives and educational programs while raising awareness about cybercrime affecting minors. Additionally propose solutions and improved policing alongside legislation.
5. Emphasize the significance of approaches based on evidence involving stakeholders. This includes promoting literacy and awareness campaigns while developing safety tools and standards with an emphasis on thinking skills.
6. Recognize the potential of emerging technologies like AI and gaming in addressing these issues while emphasizing considerations, oversight mechanisms and human involvement.
7. Empower minors with knowledge on navigating the internet by avoiding victimization, detecting manipulation promptly and reporting abuse incidents, all while fostering online communities.
8. Finally, synthesize insights from projects that tackle these topics to facilitate knowledge sharing, among stakeholders working towards safeguarding children

2. Policy Brief 01

2.1. Executive Summary

The policy brief analyses minors' online grooming in Europe, focusing on risk factors, strategies used by offenders, and recommendations for prevention. It finds that factors making minors vulnerable include isolation, mental health issues, and poor family communication. Most victims spent over 6 hours daily online. Offender risk factors include loneliness driving excessive internet use and grooming behaviours. Many offenders are unemployed, while some already work with children. In terms of strategies, implication by offenders was most dangerous as it enabled physical encounters. Deception about identity was not that common compared to other tactics. Corruption occurred through gifts and money. Coercion via blackmail was sometimes used. Significantly, 20% of offenders already knew the minor prior to grooming[1]. Sexual contact occurred in nearly half the analysed cases. Consequences for victims include guilt and shame. A lack of communication prevents minors from disclosing grooming. Most cases are discovered by police or families rather than the minor voluntarily disclosing.
Recommendations focus on reducing loneliness and improving family communication. Educating minors on online risks, healthy relationships, and sexuality is advised. Working with families can facilitate disclosure without blaming victims. Normal adolescent sexual curiosity should be distinguished from illegal exploitation. Prevention efforts should target both "fast" and "slow" grooming types.

2.2. Review and Analysis of Online Grooming in Europe

For whom?
This policy brief focuses on various issues such as risk factors, modules operandi, and offender strategies on online grooming from both practical and theoretical point of view. It is addressed to law enforcement agencies, academic organisations, and experts focusing on online grooming.

Highlights and key observations[2]

- The online grooming process is not long, the time between conversation and action around sex has minimized.
- Online grooming is not necessarily circumscribed to adults but could include minors too.
- Notable increase of up to 70% in the number of cases of this cybercrime.
- Offenders tend to be younger than what people think, something to consider in prevention, as they have easier access to minors (for instance, do not have to lie about their age or identity).

Findings: Online grooming risk factors from the victim's perspective

[1] D1.7 OPEN REPORT ON VICTIM AND OFFENDER PROFILE DESCRIPTION REPORT, RAYUELA project, available online at / https://www.rayuela-h2020.eu/docs/d1-7-open-report-on-victim-and-offender-profile-description-report-2-2//

[2] as above, D1.7 Open report on Victim and offender profile description report

The study sample consisted of eight victims, who were difficult to contact due to data protection protocols and the consent of the parents or therapists. The study also included the analysis of 15 offenders' interviews – who gave information about the victim, the analysis of 23 experts interviews, and the study of 50 European court sentences. Risk factors included isolation, previous history of abuse, poor mental health, low self-esteem, and poor family communication. Almost 63% of the subjects did not find it easy to interact with others face-to-face, preferring online interface interactions. Six of the eight victims stated they would have liked to have more friends when the grooming situation occurred and that the search for attention also played a role in the case. The effect of the Internet on social interactions is not restricted to those with low social skills, as one of the children with no social relationship problems and with plenty of friends pointed out that despite being the same as in real life, on the Internet, he could be a little different, bolder[3].

The online disinhibition effect (Suler, 2004) also plays a role in young people's interactions as they specifically tend to consider that their online identity is different from the one they have in face-to-face interactions. The most critical details are that some subjects indicated that their mood was fine when the first contact with the offender occurred. Still, most recognized that they had been dealing with issues, such as having recently moved to a new city, having no friends around, not being popular at school, or being “shut off.”
Experts pointed out that having previous difficulties socializing is a dangerous factor for becoming more involved in technology. It is seen as a refuge for those who do not have such a rich scenario in their face-to-face world. The most critical details are that Instagram was the most used social network within the sample, followed by Facebook (one child) and banned sites like OMEGLE (another child). The time spent on social networks was high, with an average of 6 hours per day (with a minimum of 4 hours). Previous research has suggested that the more time the children spend online, the more likely they are to become victims of online grooming.[4]

Key recommendations:

- Focus on how to minimize feelings of loneliness, which is the driving force to become a victim of online grooming.
- The average age is in adolescence mainly for two reasons: the search for experience and sexual curiosity. It is necessary to understand the active role of the victims in order to better prevent the phenomenon.
- The average age is in adolescence mainly for two reasons: the search for experience and sexual curiosity. It is necessary to understand the active role of the victims in order to prevent the phenomenon better.
- Most of the children had their profile public when the contact took place, so prevention should focus on this too.
- Gender was a key aspect to consider in interventions: boys take more risks and see less danger and girls are coerced to a greater extent (through violence and/or threat of abandonment)

Findings: Online grooming risk factors from an offender perspective

Loneliness is the most repeated reason to explain both spending plenty of time on the Internet and ending up in a grooming situation, with 73% believing it is one of the main reasons. 80% of offenders admitted having

[3] as above

[4] D1.7 Open report on Victim and offender profile description report, RAYUELA project, available on onine / https://www.rayuela-h2020.eu/wp-content/uploads/2022/10/Attachment_0-2.pdf /

lied on the Internet, and the lack of vulnerability and disinhibition are critical aspects for committing the crime. Experts agree that other conditions, such as having time and being unemployed, can lead to grooming. The unemployment rate suggests that many offenders start grooming in difficult situations. Most offenders admitted to having maintained online contact with victims, having had a relationship, and exchanging audiovisual material with sexual content.[5]

Our study showed two types of abusers: pedophile abusers and diverse abusers. Offenders often refer to themselves as "deviants" and begin to consume child pornography online. Narcissistic traits are common in these offenders, and several of them worked with minors. The online disinhibition effect implies that online criminals tend to separate the online and offline worlds.[6]

Key recommendations:

- Focus on how to minimize feelings of loneliness, which is the driving force to become an online grooming offender.
- In one quarter of cases the offender was known and belonged to the victim's environment, which implies targeting prevention to these cases as well. The family and the school environment are usually the main focuses. These cases are especially severe as the manipulation is ever stronger when the offender is socially recognized, and the probability of having a physical sexual encounter increases.
- In most cases, the offenders did not create a fake profile or lie about their age. It is important to not focus prevention only on impersonation but also on the risks of starting a relationship with an adult, even though he/she is a young one.
- Although some offenders look for attractive photos and the age in their victims' social network profiles, there does not seem to be a clear-cut patron of choosing, as they usually contact many teenagers and minors.

Findings: Modus Operandi

One of the most important findings was that around 20% of the analysed cases concerned offenders that had known their victims before the grooming process started. In one case, the offender was not close to the victim before the grooming situation but was a manager of a candy store in the neighbourhood. In two cases, the offender was the teacher of the victim(s). Some of the perpetrator stated that they clearly informed the students from the beginning that they were looking for sex but admitted that they also talked to them about their problems at school, not just the explicit content.

The study also found that one offender pretended to be a teenage girl working for a fan club of a TV show popular with the 14-year-old daughter of his partner and her best friend. By posing as this fictional girl, he was able to manipulate and threaten the two teens, claiming he would "help" them if they had sex with him. He used this deception and coercion to sexually exploit the young teens.

[5] as above, open D1.7, plus compare with the D1.5 Open Report on Case Study Results, RAYUELA projecta, available online / https://www.rayuela-h2020.eu/wp-content/uploads/2022/10/Attachment_0-1.pdf /

[6] as above

Three minors in court sentence sample had their first interaction through a dating website, which means that although not majoritarian, these apps must be considered a place for risk as well. Most of the profiles were public, with pictures, ages, names, and locations on them. 71.4 % of the victims[7] suspected that the offender lied when specifying things, but not about their age. These findings show how important it is not only to focus on the possibility of deception, but also on the risks of starting a relationship with an adult.

Regarding the first interaction, many started with general questions to first get to know each other. Later they started establishing a relationship, showing interest in the victims' topics, and talking about them. Finally, the sexual topic arises. Nevertheless, some offenders go directly to the sexual topic and quickly change their objective if finding no interest.

Key recommendations:
Both, the slow and the fast grooming dynamics must be prevented, as they both take place. Attention should be paid the to slow types and opportunistic offenders, as although the first ones would be more dangerous, the second ones are more frequent.

Findings: Persuasive Strategies
Online grooming involves exploiting naivety and vulnerability of victims with several types of grooming, opportunistic ones being more common but less dangerous. The manipulation strategies offenders employ in the sample are multiple, changing from one offender to another, and from one victim to another with the same offender.

Deception: The most important details are that none of the offenders in the sample of the interviewed victims used a fake profile to contact the minor and that most of the victims suspected that the offender lied about their status, skills, or romantic feelings. Only four offenders from the other sample admitted using fake profiles and/or photos. One of the offenders created many fake profiles in advance to be able to contact many and sell their images to different buyers later. Another one created several profiles to interact to him. Through these fictional personas, he was able to portray himself as having desirable qualities, status, and power in order to gain influence and control over potential victims. A thirdinterviewed offender contacted the minor telling her he had seen a video online of her showing her breasts and that he could delete it if she agreed to perform different sexual behaviours in his presence. Thus, offenders use fake accounts, fake profiles, and identity theft to deceive potential victims. They can create fake accounts with phone numbers, addresses, and pictures of a girl to give them confidence. They can also create parallel accounts with the victim's images and impersonate them without hacking or advanced computer knowledge.

Implication: Offenders used implication as a strategy to gain attachment to the child. Offenders admitted to talking with minors about their problems, while some felt excluded and looked for elders. Implication was the most dangerous strategy as it was more likely to end up with a physical encounter and because it was frequently followed by different types of coercion.

Corruption: Offenders often ask victims for photos in exchange for money, which can be dangerous if the minor is dealing with economic problems. Other times, instead of money they offer (and the victims accept)

[7] D1.7 Open report on Victim and offender profile description report, RAYUELA project, available online / https://www.rayuela-h2020.eu/wp-content/uploads/2022/10/Attachment_0-2.pdf /

gifts or mobile recharges. In another cases, they promise creating a model book or giving improvements in videogames. A Youtuber manipulated a young boy pressuring the boy to send explicit pictures, threatening to end their friendship if the boy did not comply. The boy felt compelled to maintain the friendship in order to continue learning about a videogame from him.

Coercion and blackmail: Offenders often take pleasure in the power imbalance and attention they get from victims and may use emotional manipulation or threats. Most offenders did not openly admit to using coercion or blackmail, however one offender stated that he blackmailed a girl by threatening not to meet with her in person if she did not comply. Two other offenders threatened girls by saying they would spread explicit images they had already obtained from them. In the case of the stepfather offender, he used a combination of building trust and calculated manipulation strategies.

Sex: The most important findings are that almost all offenders obtained images from their victims, and nearly half of them had a sexual physical encounter. The severity of the content varied from semi-naked pictures to sadistic/bestiality. Most offenders admitted diverse strategies, the most extreme of which was coercion through fear of abandonment or threats. Offenders use various strategies to gain victims' trust, such as taking advantage of their lack of knowledge and explaining sex through descriptions and/or sending diverse material. Experts agree that sex education should be included in the curriculum. .

Key recommendations:

- It should be considered that the deception strategy is not limited to the age of the profile. Offenders often lie about their feelings and to get more information~~, they have~~ about the victims.
- Special focus should be put in the implication strategy as it is the most dangerous one.
- Considering that sexual curiosity is exploited by offenders who take advantage of the lack of knowledge, sexual education would be a key tool to face online grooming.
- Strategies must also be careful not to blame the victims, since a fear of being blamed or punished leads many victims not to disclose the crime.

Consequences. Prevention

The sample of teens reported receiving the support they needed to complete the process, but some interviewees insisted they did not have the help they would have required earlier. Two victims who ended in physical and sexual contact described how they tried to deal with the situation back in the past and how, although they have recovered, it is still difficult to overcome it. Feelings of guilt and shame are typical and must be considered when prevention strategies are designed. It is crucial, for schools and sexual education programs to offer education on the dangers of the internet to help prevent people from being exploited. In our study, law enforcement or families discovered the crime more frequently than victims themselves.. This emphasizes the need for measures through education and awareness to safeguard children of solely relying on them to report abusive situations where they may feel manipulated or threatened by predators. It is essential to implement initiatives, beyond depending on youth self-reporting in order to effectively detect and put a stop to sexual exploitation.

Experts agree that the most crucial factor is guaranteeing good family communication. Communication should mean neither threatening to cut off from social networks nor understanding that no topic is a taboo. Victims may change groups of friends, lock themselves at home, or panic about going out of the house.

Recommendations

- Work with families should be included to facilitate disclosure. This work should emphasise the importance of encouraging communication so that children are not afraid to disclose the situation.
- Include sexual and gender equality education when approaching online grooming prevention programs. It is important to highlight that gender socialization appears as a risk factor in both boys and girls. In girls, the pressure of being desired and low self-esteem would make them more vulnerable. In boys, the traditional male role would make them more likely to underestimate risk and engage in more unsafe behaviours.

3. Policy Brief 02

3.1. Executive Summary

The policy brief focuses on cyberbullying in Europe, approaching risk factors, strategies, and recommendations. It finds victims seem vulnerable due to low mood or problems at school/home when bullied. Negative impacts include mental health issues, low self-esteem, and loneliness. Risk factors are difficult to profile but include eccentricity, minority status, and relationship issues. Offenders often have negative self-image, family issues, low self-control, and past victimization. Strategies like flaming, harassment, denigration, impersonation, outing/trickery, exclusion and cyberstalking are used. Intentional victim selection occurs in most cases. Cyberbullying typically extends from offline bullying. Sexual content is common (Wachs - Wright - Vazsonyi, 2019). Consequences include reluctance to report, with only one third coming forward. Prevention should encourage face-to-face interaction, educate on prosecutable actions, teach evidence collection, and involve peers/parents. Recommendations include implementing an "online shield" to prevent misunderstandings. Boredom, stress, isolation, and excessive digital media use during the pandemic increased cyberbullying. Supporting peers to shape behaviour and teaching bystanders to take a stance are advised. Parental supervision of online use should be promoted. Schools can create information points for reporting.

3.2. Review and Analysis of Cyberbullying in Europe

For whom?
This policy brief focuses on various issues such as risk factors, modus operandi, and offender strategies on cyberbullying from both practical and theoretical point of view. It is addressed to law enforcement agencies, academic organisations, and experts focusing on cyberbullying.

Highlights and key observations

- The research shows that there are no specific victims' profiles, but rather a certain vulnerability at the time of perpetration, feelings of sadness and helplessness. Social structure and inequalities derived from gender, sexual orientation and migratory status also play a role in victimization.
- Cyberbullying was observed predominantly in the connection of concrete social media networks, such as Instagram, Tik Tok, Snapchat, and Facebook.

Findings: Cyberbullying risk factors from the victim's perspective
The victims interviewed seemed vulnerable due to low mood or not feeling good at school or at home. At the time of bullying, they often felt sad, helpless, scared, or humiliated. Consequently, the cyberbullying incident had a negative impact on their lives. According to experts, a feeling of helplessness returns frequently. Victims are more likely to suffer from mental health issues, lower self-esteem, and loneliness, while they are more sensitive to social anxiety.

Setting up risk factors or characteristics of a victim might be contradictory, as these might be consequences for the bullying rather than the actual cause. It is difficult to profile potential victims or make assumptions, as cyberbullying is more unpredictable than bullying. Risk factors include eccentricity, deviating from the

group in any way, insecurity, a desire for attention and approval, being cautious or anxious, sensitive, quiet, withdrawn, and shy.

Minorities are more likely to be targeted due to their gender, sexual orientation, origin, religion, lack of proficiency in sports, school, etc. Lack of support or acceptance, unreasonable expectations, tolerance towards bad attitudes, and misbehaviour - they all have negative fallout.

Another risk factors to consider are that it is possible to be bullied by your romantic partner, and that *many cases were related to **sharing passwords** or having **weak passwords** online.*

Key recommendations:

- Focus on how to minimize feelings of loneliness, which is the driving force to becoming a victim of cyberbullying,
- Educate young people to externalize their feelings and, if they are being bullied, encourage them to tell their friends, family, teachers or someone they trust.
- Promoting family communication, or person of trust, reinforce children's self-esteem.
- The ability to report anonymously to all the authorities active in criminal proceedings to verify the profile.

Findings: Cyberbullying risk factors from the offender's perspective

It is important to mention that there is no specific profile of the cyberbullying offender, but there are risk factors. The risk factors identified in the research on the profile of offenders were: displaying a negative self-image in the school and family environment; having perceived a disturbance in their family environment; having lower self-control and higher levels of anger; having suffered other stressors during childhood and having previously been a victim.

Instagram is the most widely used social network, but other social networks, such as Facebook, TikTok, and WhatsApp are also mentioned. The time they spend online varies from person to person.One of the offenders declared that before the COVID-19 pandemic, he/she had to wait a long time for somebody else to connect to an online game, while during the pandemic, he/she sometimes only had to wait 5 minutes. Only three offenders declared to have more than one profile, two of them having two profiles, five offenders having public profiles, and two having private profiles. [8]

Key recommendations:

- Encourage empathy in young people and show them that their actions towards other people have consequences.

Findings: Modus Operandi

Cyberbullying intentionally misuses power exerted by a single person or group of individuals through cybertechnology. It is limited to the abuse of visuals (e.g., videos and memes) and verbal use. The potential of repetition is automatic, and the online world is not limited to school, work, or any other place. Once you

[8]D1.7 Open report on Victim and offender profile description report, RAYUEAL project, available online /https://www.rayuela-h2020.eu/wp-content/uploads/2022/10/Attachment_0-2.pdf/, see also the open public report D.1.5 Open Report on Case Study Results

switch on your device, you might become vulnerable to attack at anytime, anywhere. This is because the material might be online forever, and the potential risk of being attacked repeatedly is obvious. Eventually, the victim is never fully safe from cyberbullying.

In terms of modus operandi, the behaviours of the offenders involved in the dynamics of cyberbullying are (Willard; 2007):

- **Flaming**: online "fights" using electronic messages with angry and vulgar language.
- **Harassment:** repeatedly sending offensive, rude, and insulting messages.
- **Denigration:** Sending or posting cruel gossip or rumours about a person to damage his or her his/her/their reputation or friendships "Dissing" someone online.
- **Impersonation:** Breaking into someone's account, posing as that person and sending messages to make the person look bad, get that person in trouble or danger, or damage that person's reputation or friendships.
- **Outing and Trickery:** Sharing someone's secrets or embarrassing information or images online. Tricking someone into revealing secrets or embarrassing information, which is then shared.
- **Exclusion:** Intentionally excluding someone from an online group, like a "buddy list"
- **Cyberstalking:** Repeatedly sending messages that include threats of harm or are highly intimidating. Engaging in other online activities that make a person afraid for her or her his/her/their safety.
- Use of technology, usually cell phones, to control a partner.

In addition, the research revealed that in 79.9% of the cases the selection of the victim is intentional.[i]

Cyberbullying is an extension of offline bullying, with limited cases where the bully and victim do not know each other or are not connected in any way in real life. It is challenging to escape online harassment, as it happens almost 24/7, and the offenders are shielded behind the screen. However, it is more common to go from bullying to cyberbullying; the other way around is rare. The Internet is the perfect place for an encouraged aggressor, an ideal victim, and the lack of an efficient guardian to be found easily. It is difficult to remove the material completely. Obtaining proof of cyberbullying is more accessible when the necessity of this is emphasized. Ugly comments or rage are quickly deleted to avoid it. Confronting the offender with conclusive proof tends to be more effective.

According to our findings, *the usage of sexual content in situations of cyberbullying was pretty common.*

Key recommendations:
Disseminate information on the modus operandi of cyberbullying in order to detect it quickly.

Consequences, Reporting

It is believed that around one third of victims never come forward. Thresholds to do so need to be lowered.

Face-to-face interaction should be encouraged to foster social bonds in real life. Prevention days are organised in schools with games, cases, and videos where people talk about their experiences. The research suggests that using social media influencers who have personally gone through and overcome cyberbullying could be advocates, for raising awareness among people. By sharing the stories and insights of influencers whom adolescents admire educational messages about risks like cyberbullying can become more relatable

and meaningful. By highlighting influencers who have experience dealing with cyberbullying young individuals may be more open, to receiving and applying advice to combat online harassment. Utilizing the voices of role models who have faced real life struggles can help capture the attention of youth and address emerging threats more effectively[9].
Offenders and victims should know that insults with images and text, racism, discrimination, and sexism are all prosecutable. Educating how to respond as a victim, but also as bystanders, encouraging them to take a clear position, making it safe to report such cases at school or with trustees, learning to collect evidence, teaching children how to behave in the online space, and working on an individual level, if necessary, involving the parents.

Recommendations

- The "online shield" should be implemented from all points of view to prevent cyberbullying. Recognizing that the inability to see the other person's reactions is a significant part of cyberbullying and the possibility of misunderstandings is essential.
- Significant projections of cyberbullying have increased during the pandemic, such as boredom, frustration, stress, mental health issues, lack of social interaction, and digital media use.
- Support and develop peers to shape social behaviour by discussing and analysing different situations in a group, allowing them to adapt and question their norms. This has a higher impact on social behaviour. Teach bystanders to take a stance, even in private, not to remain indifferent.
- Disseminate the importance of parental supervision when young people use the Internet and limit their time of use.
- Create information or help points in schools to which young people experiencing cyberbullying can report it.

[9] D1.7 Open report on Victim and offender profile description report, RAYUEAL project, available online /https://www.rayuela-h2020.eu/wp-content/uploads/2022/10/Attachment_0-2.pdf/, see also the open public report D.1.5 Open Report on Case Study Results

4. Policy Brief 03

4.1. Executive Summary

The policy brief focuses on human trafficking, specifically the "loverboy" phenomenon, in Europe. It looks at risk factors, strategies, and prevention recommendations. It finds the loverboy method involves isolating and controlling victims through emotional and financial dependency. Fast-track offenders exploit quickly while slow-track offending takes time. Trends are hard to discern as it's a hidden crime. Victims are mainly girls but boys and LGBTQIA persons are also targeted. Risk factors include poor family ties, running away, and attachment problems that offenders exploit through compliments and gifts. Offenders are often attractive young men aged 20-30 seeking illegal means to achieve social goals. The internet facilitates selecting and grooming victims. Strategies include groomingvictims to address their needs, gather personal information, isolate them and move to exploitation. Victims have strong bonds with offenders. Consequences are difficulty leaving due to the emotional bond formed. Prevention should build resilience, set boundaries, and raise awareness of indicators like isolation, provocative clothing, and exhaustion. Focus should be on reporting and training. Cultures preventing recognition must be addressed.

4.2. Review and Analysis of Human Trafficking in Europe

For whom?
This policy brief focuses on various issues such as risk factors, modus operandi, and offender strategies on online human trafficking from both practical and theoretical point of view. It is addressed to law enforcement agencies, academic organisations, and experts.

Highlights
The "loverboy phenomenon" is a specific form of human trafficking for sexual exploitation in the European Union. Data were obtained from 10 experts[10] on the phenomenon, including law enforcement agencies, victim services, and the judiciary. The text outlines how experts define the phenomenon, describe typical victims, offender characteristics, the process of sexual exploitation of victims, and provides experts' views on prevention. The "loverboy" phenomenon in the Netherlands and Belgium is a well-known problem, but no specific legal definition exists. Experts agree that the problem is more concrete than the legal definition of human trafficking of minors for sexual exploitation, with the main central element being the social isolation of the victim in combination with the exercise of control through (emotional and financial) dependency. This dependency can be generated in many ways: giving gifts, shelter, romance, money, or anything else the victim is missing (Smeaton, 2013).

The "loverboys" phenomenon is difficult to discern, as the strategy and behaviour are adapted to the victim's unique needs. However, some respondents indicate a difference in the time a "loverboy" takes to initiate contact and move to the exploitation stage. In the fast-track approach, "loverboys" may start to exploit the

[10] D1.7 Open report on Victim and offender profile description report, RAYUEAL project, available online /https://www.rayuela-h2020.eu/wp-content/uploads/2022/10/Attachment_0-2.pdf/, see also the open public report D.1.5 Open Report on Case Study Results

victim within a number of hours, whereas, in the slow-track approach, exploitation only takes place after a prolonged period. It was also indicated that in the fast-track approach, coercive approaches, such as violence or threats are more predominant than in the slow-track approach. When respondents are asked about the trends in the phenomenon, there is general agreement that this is almost impossible to evaluate for various reasons. It is a generally hidden form of crime, and it is not easy to detect potential cases of "loverboys." [11] The report discovered that several European countries do not have any registered instances of online human traffickingamong adolescents. This is likely due to taboos surrounding the issue and a lack of recognition as there is no established definition for the phenomenom..

Outreach efforts should focus both on sensitizing law enforcement agencies to recognize and respond to the crime, and encouraging victims to speak out, given the possibility of prosecution under various charges.

Findings: Human trafficking risk factors from the victim's perspective[12]

- Experts agree that "loverboys'' target specific vulnerabilities of the victim, but some common elements can be found. Gender is an important characteristic, as most reported cases of human trafficking of minors for sexual exploitation concern girls.
- Victims of human trafficking for sexual exploitation can have any nationality and come from different cultural identities such as Romany or Islamic. Cultural differences in sexual behaviour or identity may be exploited by the abuser.
- Young people can become victims of human trafficking at any age, and socio-economic status can be attractive, especially for those from deprived social classes.
- Socio-economic status may indicate risk, but poor family ties or lack of family/social support can also lead to human trafficking.
- Socio-economic status is a proxy for attachment problems in a potential victim's family and broader social circle, which other risk factors can exacerbate.
- Attachment problems are the core of human trafficking, and institutional history can reinforce it. People who leave or run away from an institution are especially vulnerable to "loverboys" as they are socially isolated and find it difficult to foster meaningful social bonds.
- According to experts, the following can be considered risk factors: neglect (emotional, cognitive, material), dysfunctional family, exposure to violence in the family, past abuse or violence, and violent peers. According to the experts, the factors that play less of a role are forced marriage, witnessing violence in the community, and exposure to war or collective violence.
- Other factors, such as non-belonging, missing something, and being misunderstood can lead to attachment problems. "Loverboys" exploit these feelings by seducing victims, complimenting them, and buying them gifts. Impaired cognitive development can further put people at risk, as they are more prone to accept false promises.

[11] as above

[12] D1.7 Open report on Victim and offender profile description report, RAYUEAL project, available online /https://www.rayuela-h2020.eu/wp-content/uploads/2022/10/Attachment_0-2.pdf/, see also the open public report D.1.5 Open Report on Case Study Results

Key recommendation:

- Develop clear legal definitions and categorization of "loverboy" phenomena and human trafficking of minors for sexual exploitation to facilitate reporting and data collection.

Findings: Human trafficking risk factors from the offender's perspective [13]

- The master narrative of human trafficking often portrays the offender as a creepy professional criminal, but respondents agree that the offender is most likely to be an attractive young man.
- The offender is often a young man ranging from 20-30 years old on average when the victim is a minor.
- Ethnic origin and cultural/religious differences can impact a potential offender's susceptibility to human trafficking, usually influenced by how they perceive women.
- Offenders are often young men, but girls can be involved by recruiting other girls for the "loverboy."
- The main driver behind "loverboys" is similar to society's goals, but they choose illegal means to achieve it. This mismatch between the goals and the standards to achieve it is identical to strain theoretical approaches, where individuals aspire to the same goals but choose illegal means to achieve them. Identifying "loverboys" is difficult due to the broad and general risk factors for unhealthy or antisocial behaviours.

Key recommendations:

- Develop profiles of common exploiter characteristics and grooming techniques to enhance early identification.
- Implement sting operations and monitoring of online platforms to identify and apprehend perpetrators.
- Establish specialized police units focused on investigating loverboy crimes and disrupting trafficking networks.

Findings: Modus Operandi

"Loverboys" are adaptive to the individual situation of the victim and have a "sixth sense" to select victims in a targeted way. This stage is facilitated by the emergence of the Internet, where offenders have more access to potential victims. The Internet has made it easier for likely offenders to select victims, making the process more visible to the victim's neighbourhood and potential loved ones. However, the internet renders this process hidden and diminishes the social control that can be exerted on potential victims. Additionally, young people are often vulnerable to their online image, as they often present themselves positively, post much information online, and accept friend requests from anyone who looks good as a proxy of individual success.

The offender grooms the victim by generating mutual interest and addressing their emotional needs. The Internet facilitates this process, as potential victims often post what is on their minds online. Furthermore, the likely offenders can gather information about the victims based on their photos, which often portray their interests and hobbies.

[13] D1.7 Open report on Victim and offender profile description report, RAYUEAL project, available online /https://www.rayuela-h2020.eu/wp-content/uploads/2022/10/Attachment_0-2.pdf/, see also the open public report D.1.5 Open Report on Case Study Results

Victims of "loverboys" have a strong bond with their aggressor, and it is difficult to convince them to leave their prostitution life. A prosecutor told a story of a court case in which a "loverboy" was being tried, and the victims cheered the "loverboy" when the accusations were read out. This shows the depth of the problem with "loverboys" and suggests that prevention or sensitization of this crime will be a difficult task.

Key recommendations:

- Analyse patterns in offenders' interactions to identify common strategies for manipulating victims. Incorporate findings into police training.
- Provide schools with research-based educational programs on healthy relationships and resisting manipulation.
- Establish mentorship programs to provide positive role models and guidance to deter boys from becoming loverboys.

Consequences, Prevention

The experts discussed the difficulty of preventing human trafficking for sexual exploitation using the "loverboy" technique due to its romantic and emotional nature. Offenders control victims through emotional and material dependence, and victims often lack the will to leave due to their intimate connection with the offender. Victims often have specific personal histories that may be conducive to seek attention and success outside of the legal sphere, making prevention more difficult.

Experts suggest that prevention strategies should focus on resilience and setting boundaries to prevent human trafficking for sexual exploitation. They also agree that not only the victim, but the society at large should be addressed to prevent this form of crime. It is a hidden crime, which is often overlooked by local authorities and victim services. Any efficient program should start with rising awareness of the crime and discarding possible cultural barriers that impede recognition.

Experts were sceptical of preventing "loverboy" crime due to its specific life choices and intimate relationship with the offender. To educate people about the crime and equip them to identify potential cases, they asked respondents about common indicators or "red flags." This could be a solid social preventive tool.

Visualization of a set of indicators of victimization by the Loverboy:[14]

- Having a “secret lover”
- Isolation from friends
- Engaging in a new social network that they shield from other friends
- Suddenly showing up with expensive things
- Wearing sexy and provocative clothes
- Having business cards from hotels
- Permanently getting calls or going to make calls outside
- Visible signs of exhaustion and/or drug use
- Running away (e.g., skipping school, running away from an institution)
- Psychosomatic complaints, such as abdominal pain without any medical grounds

[14] D1.7 Open report on Victim and offender profile description report, RAYUEAL project, available online /https://www.rayuela-h2020.eu/wp-content/uploads/2022/10/Attachment_0-2.pdf/, see also the open public report D.1.5 Open Report on Case Study Results

Recommendations

- Implement training programs for law enforcement, child protection agencies, schools, and community organisations to raise awareness of signs of grooming and exploitation.
- Establish multidisciplinary teams involving law enforcement, social workers, psychologists, and victim advocates to provide comprehensive support for identified victims.
- Develop outreach and education campaigns targeting vulnerable youth on healthy relationships, self-worth, boundaries, and warning signs of exploitation.
- Enhance regulation of online platforms and messaging apps to reduce opportunities for grooming.
- Promote resilience programs, life skills training, and mental health support in schools and community centres.
- Engage religious and community leaders to address cultural taboos that may prevent reporting.
- Increase penalties for human traffickers while providing protections and rehabilitation support for victims.

5. Policy Brief 04

5.1. Executive Summary

This policy brief focuses on online issues for youth in Europe. Even though European teenagers are considered digital natives they still need guidance to cultivate digital literacy skills. These skills are essential for them to critically evaluate the accuracy and truthfulness of content. Without training young people can be easily manipulated by malicious individuals who take advantage of their limited ability to verify sources, fact check information and recognize techniques used to spread misinformation. They trust traditional media but share false info for popularity, althoughlinguistic factors and quick sharing without verifying exacerbate fake news as well. Another form of online deception is commercial deception, which is increasing, especially around events. In addition, fake accounts enable bullying and misinformation.
One last relevant phenomenom is cyberhate, which targets groups while cyberbullying targets individuals, but both overlap around gender and discrimination (Shu, at all., 2017Parental engagement, educating on verifying information, and simplifying reporting processes are recommended. Teaching the consequences of sharing fake news or cyber hash and offering in-app report buttons can help prevent these crimes.

5.2. Review and Analysis of Fake News, Deception, and Cyberhate

For whom?
This policy brief focuses on various issues related to online deception such as fake news, online interaction with strangers, and cyberhate, from both practical and theoretical points of view. It is addressed to law enforcement agencies, academic organisations, and experts.

Highlights and key observations[15]

- Young people are more likely to believe in fake news because their digital and literacy skills are developing.
- Young teens are more conservative in their criteria for adding strangers to their lists of followers than older ones. While girls tend to only add good friends of people they know, boys frequently ask for more information and follow them if they have a private account.
- Fake news and cyberhate are linked to polarization, spreading negative stereotypes against vulnerable groups.
- Young people tend to share and look up information quickly, making it easier not to pay attention to the characteristics of disinformation, fake news, and misinformation.

Eight focus groups were conducted in five countries (Spain, Portugal, Greece, Estonia, and Slovakia) with 47 young people of different ages. In a secondary school in Belgium, three workshops were conducted with 12-year-old students about misinformation and deception on the Internet[16]. The main objective was to collect

[15] D1.3 OPEN REPORT ON INTERVIEW RESULTS (PER COUNTRY/ FINAL) [2/2] + OPEN REPORT ON MISINFORMATION AND DECEPTION, RAYUELA project, available online / https://www.rayuela-h2020.eu/wp-content/uploads/2022/10/Attachment_0.pdf /

[16] as above

data for developing RAYUELA's game and to help young people learn about the forms of deception and disinformation on the Internet. The activities were organised using the focus group template and included practical exercises, discussions, and questionnaires about fake news, misinformation, and cyber hate. A survey was also implemented in a representative sample in Madrid (Spain) and Estonia to contrast some of the findings in the focus groups.

Findings: Fake News[17]

- Although young people are vulnerable to fake news, according to our results, most of them do not mistrust traditional media. In our sample, only some regional sensationalist tabloid portals or yellow press were pointed out as the first sources of misinformation, while more traditional media were stated as credible. Participants trust information in the news more than those on social networks.
- Young people share false information to gain popularity/virality on social networks, show a desired identity, develop and reaffirm their identity, gain more likes, and be part of the trend.
- Young people often share false information without verifying it, leading to the spread of "click bait" designed to attract attention.
- Fake news can be used as a form of entertainment or as a way of accepting reality, such as COVID-19.
- Experts have identified two main reasons why young people share fake news: access to news and linguistic level. Access to news is a major factor, as it allows young people to access a large amount of content and information quickly. The linguistic level is another factor since those with less linguistic knowledge may need help understanding the article's content when they read it. (Mendiguren, at, 2020). Participants shared fake news related to health issues (mainly COVID-19) and restrictions measures but also liked the news about mobile radiation and other kinds of news that appeal to their interests, such as famous gossip and music events
- One relevant aspect is that even knowing that it is not true, it still has an impact on the person.
- Most participants were aware and familiar with the term fake news.
- They associated the presence of fake news with certain social media channels, such as TikTok and YouTube.

Key recommendations:

- Young people still rarely check and verify the news. We should focus on the awareness campaign and education that explain to them the need for and importance of the verification process, adding special series of workshops in school curriculums.
- Prevention should focus on the consequences of disseminating fake news,
- Topics selected for the interventions should appeal to their interests and emotions, as they are the most frequently shared fake news.

Findings: Deception[18]

[17] D1.3 OPEN REPORT ON INTERVIEW RESULTS (PER COUNTRY/ FINAL) [2/2] + OPEN REPORT ON MISINFORMATION AND DECEPTION, RAYUELA project, available online / https://www.rayuela-h2020.eu/wp-content/uploads/2022/10/Attachment_0.pdf /

[18] D1.3 OPEN REPORT ON INTERVIEW RESULTS (PER COUNTRY/ FINAL) [2/2] + OPEN REPORT ON MISINFORMATION AND DECEPTION, RAYUELA project, available online / https://www.rayuela-h2020.eu/wp-content/uploads/2022/10/Attachment_0.pdf /

- Commercial deception increases during calendar dates and events when commercial activity is high - as Christmas holidays, Summar holiday, etc., and some teenagers have been victims of fake sellers. They also remember seeing fake offers and product commercials on Instagram and online games.
- Adult groomers are a common threat to online deception, and many participants have stories of being approached by older men.
- Fake accounts can break up relationships or make people mock others, leading to online bullying and spreading misinformation.
- When children are asked if grooming incidents affect more girls than boys, they responded unanimously that girls.
- Participants in the sample interacted with strangers, which is the main danger of the frequent practice of considering that a friend of a friend is a safe and known person.
- Participants found more deception on Instagram and TikTok, with TikTok allowing users to be themselves and follow strangers, while Facebook and Snapchat are more conservative.
- Deception can play a role in cyberbullying, such as making fake accounts and spreading nude photos. It is common among teenagers to manipulate people into responding with comments and secretly record them.

Key recommendations:

- Deception is a key element in all cybercrimes, so prevention aimed at safer and more responsible use of the Internet should include the development of critical thinking around the most common deception situations.
- Prevention should also focus on the interactions/acceptance of friendship requests of strangers.

Findings: Cyberhate[19]

- Cyberbullying and cyberhate are mixed topics, with cyberhate referring to attacking ethnic, social, etc. groups and cyberbullying referring to attacking individuals. Both phenomena overlap in some cases, but not always. Together with the common forms of discrimination, physical appearance is repeatedly highlighted in various states of cyberhate.
- Cyberbullying and cyberhate are connected, among other issues, due to gender roles and sexism. The main victimization factors for receiving online hate speech are also the main factors for suffering cyberbullying: being a woman, a migrant and/or having a non-heterosexual sexual orientation. On the contrary, being a heterosexual man seems more related to being the perpetrator of aggression.
- Cyberbullying is often masked as humour. Discourses of cyberhate overlap with those of cyberbullying, as some of the target groups are the same and it is also dressed up as humour.
- This masking through humour is relevant in two ways. On the one hand, sexist jokes might potentially exclude women from virtual social spaces by silencing them. On the other hand, the association between sexism and humour has been broadly studied as related with the construction of men's in-group cohesion, but also with victim blaming.

Key recommendations:

- One may wonder why cyberhate receives much less attention than cyberbullying, both in academia and especially in prevention programmes. As we have shown, cyberbullying is inseparable from the

[19] D1.3 OPEN REPORT ON INTERVIEW RESULTS (PER COUNTRY/ FINAL) [2/2] + OPEN REPORT ON MISINFORMATION AND DECEPTION, RAYUELA project, available online / https://www.rayuela-h2020.eu/wp-content/uploads/2022/10/Attachment_0.pdf /

social structure and different forms of discrimination, so it is essential to incorporate a critique of LGBTQIA phobia, sexism and racism into prevention.

- Furthermore, how these discourses are tolerated and maintained must be explicit. To this end, two key mechanisms must be explicit: trivialization through humour and victim-blaming.

Findings: Reporting the crime [20]

For some focus group participants (especially the younger ones) it was easy to report an online incident to a friend than to an adult, so this alternative should be also promoted.

- Parents should be engaged with their children to understand how online activities work and help them make better decisions without parental supervision. More actors like school, teachers, and peers or friends should be involved. Experts agree that long-term programs should be structured to increase media knowledge among young people, teach them to read the full article in the case of fake news and encourage them to "pause and think before sharing" when dealing with online content.
- Regarding suspicious accounts that contact minors, participants usually block those accounts if they are insistent, otherwise, they simply ignore them or ask more questions to know who the person is, but they do not generally report the incident.
- Unlike cyberbullying, where participants report intervening to prevent it, in the case of cyberhate they tend to take no further action.
- Experts suggest developing reaction strategies to prevent cybercrimes like cyberhate by offering buttons to report content for infringing social network rules. This would be convenient for users as only one of the reasons must be alleged, and no further reason is requested.

Key recommendations:

- According to our results, we should encourage minors to act when facing fake news, cyberhate, or online deception by explaining the negative consequences of actively sharing or ignoring false information or cyberhate.
- Offering buttons in apps and simplifying the reporting process is also important, together with involving family and people of trust.

[20] D1.3 OPEN REPORT ON INTERVIEW RESULTS (PER COUNTRY/ FINAL) [2/2] + OPEN REPORT ON MISINFORMATION AND DECEPTION, RAYUELA project, available online / https://www.rayuela-h2020.eu/wp-content/uploads/2022/10/Attachment_0.pdf /

6. Policy Brief 05

6.1. Executive Summary

The brief reveals that minors spend an amount of time online each day often using apps like Instagram and TikTok on their smartphones. Among minors' game consoles, smartwatches and speakers are regarded as the devices. To tackle this issue, AI and technology can play a role by offering moderation tools, parental controls, educational resources for cyberbullying prevention, safety programs, reporting mechanisms and age verification measures. However, it is essential to adopt an approach that combines guidance, education initiatives, regulations enforcement along with collaboration among stakeholders.

The key recommendations put forth include investing in research and development (R&D) to identify solutions for threat detection purposes; implementing age verification protocols; establishing AI standards for businesses catering specifically to childrens, minors needs; fostering collaboration between stakeholders; empowering users through AI assistants. It is also crucial to ensure design practices for AI systems while maintaining monitoring efforts. Emphasizing the role in tandem with AI adoption is highly advised well.

6.2. Role of Technology and AI to Improve the Online Experience of Minors

For whom?
This policy brief focuses on (human) vulnerabilities connected to technology and social networks used by European minors and the role of technology and AI in improving the way they experience them online. It is addressed to technology companies, law enforcement agencies, and child protection organisations.

Highlights and key observations[21]
The use of technology by minors can expose them to vulnerabilities such as literacy gaps, online grooming, cyberbullying, exposure to content, privacy concerns, addiction issues and excessive screen time. To mitigate these risks of cybercrime it is crucial for parents, educators and policymakers to promote literacy programs along with online safety education among minors. Collaboration between technology companies, law enforcement agencies and child protection groups is indispensable, in combating cybercrime while creating an online environment.
By leveraging technology and AI capabilities we can significantly enhance the experience of minors by ensuring their safety through improved security measures while providing educational resources and fostering positive interactions.
This includes things like filtering and moderating content, setting controls using platforms, preventing cyberbullying, providing safety education, implementing reporting and response mechanisms, and verifying

[21] D2.1 ANALYSIS OF SECURITY AND PRIVACY OF CONNECTED DEVICES, D2.2 METHODOLOGY, TOOLS, AND RESULTS OF TESTING SECURITY AND PRIVACY RISKS OF CONNECTED DEVICES, and D2.4 TECHNOLOGICAL THREATS ASSOCIATED WITH THE CYBERCRIMES CONSIDERED, RAYUELA project, these reports are confidential, executive summary is available on the official project website

age. However, ensuring the safety of minors requires an approach that involves parental guidance, education and collaboration among different stakeholders.
The purpose of this policy brief is to gather information about how minors use technology and how AI can be used to improve their online experience.

Findings: the use of technology by children and the human/demographic factors affecting online victimization in cybercrimes[22]

According to the RAYUELA survey findings most minors spend 1 to 2 hours online each day during weekdays and over 4 hours daily on weekends. The survey also reveals that minors consider game consoles, smartwatches and smart speakers as their devices.

- When it comes to fighting cybercrime, technology plays a role alongside AI. AI powered content filtering can. Block harmful information such, as explicit material or hate speech. When combined with human moderation efforts this approach can create an environment.
- Parental controls enable parents to supervise and regulate their children's activities by limiting access, to websites setting time limits for screen usage and receiving alerts about potentially risky interactions.
- Thanks to technology educational platforms, online courses and interactive learning tools personalized with the help of AI can adapt to each child's needs. Learning pace.
- AI algorithms specifically designed to identify signs of cyberbullying such as language can provide information to relevant parties. Additionally, AI powered chatbots can offer assistance and counselling for victims.
- Technology plays a role in promoting safety education. Through platforms, movies and games children can learn about behaviour, privacy settings and how to recognize potential threats.
- Reporting content, cyberbullying incidents or suspicious online behaviours becomes more streamlined with the help of technology. AI systems can assist in analyzing and prioritizing these reports for action.
- To ensure age content consumption and protect minors from information or activities online AI age verification systems prove beneficial. Moreover, AI technologies contribute towards identifying profiles and suspicious behaviours.

[22] D2.1 ANALYSIS OF SECURITY AND PRIVACY OF CONNECTED DEVICES, D2.2 METHODOLOGY, TOOLS, AND RESULTS OF TESTING SECURITY AND PRIVACY RISKS OF CONNECTED DEVICES, and D2.4 TECHNOLOGICAL THREATS ASSOCIATED WITH THE CYBERCRIMES CONSIDERED, RAYUELA project, these reports are confidential, executive summary is available on the official project website

Key recommendations to technology usage:

- Investing in assistants that guide minors in configuring security settings while safeguarding their privacy is highly recommended. These assistants also educate them on avoiding sharing information.
- Deep learning techniques should be employed to analyze patterns of behaviour effectively so as to detect instances of abuse promptly.
- Involving minors in reporting cybercrime incidents through AI systems that they interact with would not empower them but also provide necessary support during such situation.

General recommendations

- Encourage research and development efforts aimed at creating solutions that effectively detect and prevent cyber threats targeting minors such, as grooming practices, cyberbullying incidents and exploitative activities.
- Collaborate with technology companies to enhance AI moderation systems specifically designed for children ensuring the filtration of content.
- Advocate, for the implementation of AI age verification methods to effectively enforce age restrictions on content consumption.
- Establish guidelines and regulations for businesses catering to children that employ AI technologies prioritizing the protection of minor's privacy and security.
- Promote collaboration among stakeholders in developing AI tools capable of detecting and reporting cybercrime incidents.
- Facilitate the creation of AI driven products that empower children to navigate spaces safely such as tools, platforms and virtual assistants.
- Prioritize considerations in AI design to ensure protection for minors across all digital platforms.
- Continuously. Evaluate the performance of AI systems in combating cybercrime while encouraging knowledge sharing, between policymakers, researchers and technology companies.

7. Policy Brief 06

7.1. Executive Summary

This policy brief addresses the issue of cybersecurity and privacy risks associated with Internet of Things (IoT) devices that are commonly used by minors. The aim is to provide insights that can assist policymakers in safeguarding minors and enhancing their experience with these devices. It also aims to raise user awareness and encourage manufacturers to improve security features.
The research methodology that has been applied in the RAYUELA project to address this issue is as follows. First the state-of-the-art was reviewed[23] and it was decided to focus the analysis specially on wearables (e.g., activity bands, smart watches) and smart personal assistants, since they are widely used by minors. Then, a set of relevant commercial devices from these categories were selected and acquired. Next, a testing procedure was proposed for both types of devices for the sake of replicability and a set of tests were defined. This policy briefs highlight the main findings of performing such set of tests on the acquired commercial wearables and smart personal assistants, which resulted into two scientific publications [24] [25].

7.2. Cybersecurity and privacy threats of IoT devices widely used by minors

For whom?

This policy brief focuses on cybersecurity and privacy threats of IoT devices widely used by minors. The main goal is to provide insights to policymakers that help them to develop policies and measures to protect minors and improve their experience when using such devices. In addition, the policy briefs also aim to increase transparency and user awareness on the security and privacy of this kind of devices, as well as to encourage manufacturers to improve their security and privacy features, paying special attention to the protection of the most vulnerable groups, like children.

Highlights and key observations

1. The analysed commercial smart personal assistants are not resilient to voice replay attacks. The voice authentication mechanism can be cheated with a recording of the activation message so that the attacker may get access to sensitive information stored in the device (depending on the users' configuration). Nevertheless, one of the the analysed devices include a two-factor authentication (2FA) mechanism to avoid that sensitive information gets compromised.

[23] S. Solera-Cotanilla, M. Vega-Barbas, J. Pérez, G. López, J. Matanza, M. Álvarez-Campana. Security and privacy analysis of youth-oriented connected devices. Sensors. Vol. 22, nº. 11, pp. 3967-1 - 3967-25, June 2022.

[24] C. Valero, J. Pérez, S. Solera-Cotanilla, M. Vega-Barbas, G. Suárez, M. Álvarez-Campana, G. López. Analysis of security and data control in smart personal assistants from the user's perspective. *Future Generation Computer Systems*. Vol. 144, pp. 12 - 23, July 2023.

[25] J. Fúster de la Fuente, S. Solera-Cotanilla, J. Pérez, M. Vega-Barbas, R. Palacios, M. Álvarez-Campana, G. López. Analysis of security and privacy issues in wearables for minors. *Wireless Networks*

2. The analysed commercial smart personal assistants do not offer reliable mechanisms to activate skills in multi-users households. As a result, minors may activate skills that give them access inappropriate content.
3. The analysed commercial smart personal assistants lack of default configurations adapted to minors, on the contrary to other widely used applications such as streaming media services. This represents an example of a security and privacy problem due to poor usability and makes minors whose parents are not tech-saavy or very familiar with technology more expose to accessing inappropriate content or to share sensitive information without consent.
4. The research carried out for commercial wearables targeting minors (and their associated applications) show that the low-end devices present more security and privacy issues than the high-end devices. This makes low income families more exposed to security and privacy risks and threats.

Recommendations

1. Regulation, such as the cyberresilient act or the GDPR, is needed to avoid that IoT devices that do not meet minimum privacy and security requirements are commercialized in the EU, putting especial emphasis in the case of devices that target minors. As Bruce Scheneir explained in his keynote in RSA2017 "Regulating the Internet of Things"[26], there is no other way to ensure this, since device manufacturers do not have any incentive to include security (on the contraty, it may make their devices more expensive). However, regulation is not the end of the road, but just the beginning. The greatest challenge is indeed related to law enforcement once the required regulation is in place, especially in such a huge market as the IoT.
2. This problem could be mitigated not only punishing but also rewarding. Ensuring security and privacy during the entire lifecycle of an IoT device is impossible; new breaches may always appear. Some kind of incentive to manufacturers with active responsible vulnerability disclosure programmes that quickly patches the reported problems may dramatically improve the security and privacy features of such devices.
3. When it comes to security and privacy for this kind of devices used by minors, usability and training are especially important. Effort should be made to ensure that security and privacy feasures are easily configurable (or available by default). Campaigns to increase the awareness on possible security and privacy problems associated to these devices and training programmes to improve digital skills are also very important to make minors' security and privacy more egalitarian.

[26] https://www.youtube.com/watch?v=b05ksqy9F7k

8. Policy Brief 07

8.1. Executive Summary

The policy brief examines approaches in the EU for addressing cybercrime committed by minors and teenagers. It finds minors/ teenager may unknowingly commit crimes or spread harmful content online, thinking it's a joke. Clarity on legality is needed. Cybercrime by minors is significant for offenses like grooming, bullying, and hacking. Comprehensive, coordinated approaches are required, including more research on drivers and prevention. Gaps exist in legal definitions of grooming, leaving potential for minors to exploit minors. Broadening definitions to cover power imbalances regardless of age would help. Minor and teenagers offenders need different responses like education. Human trafficking grooming laws have gaps when intent falls short of trafficking.

Bridging divides with online grooming laws could help address this. Cyberbullying laws are fragmented, relying on existing crimes like stalking. Quantifying behaviours could inform comprehensive regulations. Education is also key. Misinformation rules balance freedom of speech and public harm. Social and educational initiatives could supplement laws. Hacking and cybercrime-as-a-service rules are clear, but awareness is needed that these acts have consequences. Education can redirect technical skills. Recommendations include legislative and policy approaches for minor offenders, explicit grooming laws, incorporated prevention education, and awareness creation.

8.2. The Legal Landscape for tackling cybercrime offenses by Minors in Europe

For whom?
This policy brief focuses on the current landscape in the EU on dealing with cybercrime offences committed by minors. It is addressed to lawmakers and policymakers, civil society, law enforcement agencies, educational institutions, policy makers and stakeholders and child protection organisations.

Challenges and key observations
Handling cybercrime among minors in Europe is not an easy task. Children may commit crimes online without realizing the real-life impact of their actions online, thinking that something is “a joke” or “just for fun”, while they may effectively be **exposing themselves to criminal liability**. Hacking offences by curious and tech-savvy teenagers and minors could be an example of that kind of behaviour or spreading fake news as a joke. For certain cybercrimes, e.g., cyberbullying, there is the additional difficulty of having **unclear legal definitions** and limits that may aid to the confusion of what is permissible online and what is not. More clarity on these topics and better education in these matters would help show children where the line is that they must not cross in an online context. Right now, this line is often blurred by the online disinhibition effect, leading minors to say and do things online they might not do in an offline context (Herrero-Diz, 2020).

Cybercrime by minors is not just a trivial element. In fact, for certain crimes, youngsters are a significant part of the offender population, e.g., for online grooming and the production of Child Sex Abuse Materials, (CSAM), for cyber bullying and for hacking and Rules on Hacking and Cybercrime as a Service. This reality

must be accepted and better understood to define the best responses. Therefore, in order to keep children safe online, we must also consider the harm other children may do to their peers in particular.

While creating awareness about what is legal and what is not is an important measure, teenagers and minors must not be discounted as competent actors in their own right. Youngsters do not just commit criminal offences because they are unaware of the impact and severity, **some minors will knowingly and willingly aim to create harm**. This must also be countered through various prevention and education strategies, social measures, etc.

Therefore, a comprehensive and coordinated approach is needed to tackle this challenge. This should include more research on the drivers of cybercrime by minors, risk factors and prevention strategies, and the education, prevention and social measures to match those risks. In addition, policy and legislative changes are needed to adequately address the current challenges and shortcoming of various legal systems in the EU and beyond that were reviewed. Because preventing cybercrime by minors and dissuading cybercrime by minors is another important avenue to keep minors safe online.

Findings[27]

Due to international and European Union instruments, there are often similar wordings used in the regulations. However, interpretation issues can lead to different understandings of online grooming and which behaviours are punishable. This can result in gaps in protection for victims. Legislators and policymakers should consider whether their legal system has such gaps and how to close them.

One key aspect to consider is that **online grooming is typically seen as involving an adult** older than 18. However, a 17-year-old with a sexual attraction to children can groom a younger individual, such as a 10-year-old, for sexual interaction or the production of Child Sexual Abuse Material (CSAM). Thinking of grooming only in terms of adult offenders ignores a reality of minor offenders that is very significant.

This raises the need for legislators and policymakers to recognize that **minors can also be offenders**. The offense of online grooming should encompass any situation with an imbalance in power, maturity, or the ability to consent to sexual relations legally. To address this issue, it is suggested that **clear intent and an attempt to groom should be sufficient to establish criminal liability**. This means that even if a prosecution may not always follow. In addition, minor offenders are treated differently by most legal systems, acknowledging that they may need more educational and other measures to prevent reoffending rather than purely repressive measures and punishment. However, despite that reality, the legal framework should acknowledge the seriousness of the act also when committed by youngsters. By broadening the definition of online grooming to include any situation where there is an imbalance in power or maturity, lawmakers can ensure more comprehensive protection for potential victims.

In addition, legislators and policymakers must consider the complexities of online grooming and the potential involvement of minors as offenders not only from a purely legislative point of view (“can minors be offenders and be prosecuted?”) but also from a prevention, social and educational angle, in order to fully safeguard vulnerable individuals better and close any gaps in protection.

[27] D4.5 Legal landscape for tackling cybercrime offenses by minors in Europe and beyond, RAYUELA project, available online / https://www.rayuela-h2020.eu/wp-content/uploads/2022/09/RAYUELA-D4.5_Final.pdf /

Recommendations:

- Legislators and policymakers should consider whether their legal system has gaps in protection and how to close them.
- Legislators and policymakers should ensure that minor offenders of online grooming are punishable by law, albeit where appropriate under a milder juvenile system.
- Legislators and policymakers should make sure that good laws are coupled with good prevention, social and educational strategies.

Findings: Rules on Online grooming for Human Trafficking[28]

The regulation of online grooming for human trafficking presents a significant challenge as **no specific legislation targets this issue**. In some cases, offenses related to human trafficking may be captured by existing online grooming laws. Still, these provisions are typically limited to adult offenders and require intent to engage in sexual interactions directly with the victim or to produce child sexual abuse material (CSAM). Additionally, human trafficking rules may come into play, including attempts at human trafficking, even if unsuccessful. However, **a concerning issue arises when interactions fall into a grey area, where the intent is aimed at human trafficking but does not meet the criteria to be considered an attempt at trafficking**. These interactions may not be covered by online grooming regulations, mainly when there is no direct intention for sexual interactions with a minor or the creation of CSAM, and especially when the offender is not an adult. This creates potential gaps in the legal framework. To address these gaps, it may be necessary to develop specific regulations that target online grooming for human trafficking. This would involve considering scenarios where the intention is to exploit individuals but falls short of meeting the threshold for human trafficking charges. By closing these loopholes, the law can provide better protection for potential victims and hold offenders accountable for their actions.

Efforts should be made to bridge the divide between online grooming and human trafficking laws, ensuring that the legislation encompasses a broader range of interactions and intentions. This may involve revisiting the definition of online grooming to include situations where there is an intent to exploit individuals for trafficking purposes, even if there is no direct intention for sexual interactions or CSAM creation. By doing so, we can provide better protection for potential victims and combat the insidious nature of online grooming for human trafficking.

Recommendation:

Legislators and policymakers should consider whether their legal system has gaps in protection and how to close them.

Findings: Rules on Cyberbullying[29]

Cyberbullying regulation varies significantly across different countries, with **many countries lacking specific legislation** addressing this issue directly. Instead, **they rely on existing qualifications such as threats, slander, and stalking** to handle cyberbullying cases. However, this approach could create gaps in protection,

[28] D4.5 Legal landscape for tackling cybercrime offenses by minors in Europe and beyond, RAYUELA project, available online / https://www.rayuela-h2020.eu/wp-content/uploads/2022/09/RAYUELA-D4.5_Final.pdf /

[29] D4.5 Legal landscape for tackling cybercrime offenses by minors in Europe and beyond, RAYUELA project, available online / https://www.rayuela-h2020.eu/wp-content/uploads/2022/09/RAYUELA-D4.5_Final.pdf /

particularly when the threshold or specific conditions for these existing qualifications are set at a high standard.

To effectively tackle cyberbullying and ensure adequate protection for victims, assessing the existing legal qualifications and identifying any shortcomings or gaps that may leave individuals vulnerable is crucial. However, cyberbullying as a phenomenon is often not very well understood and therefore reduced to existing main categories of offences such as threats, slander, and stalking.

In order to analyse the effectiveness of current legislation, lawmakers and policy makers should obtain a better understanding of the various cyberbullying behaviours and should attempt to quantify and assess the prevalence and impact of such behaviour. This is needed to make informed decisions regarding the necessity for comprehensive cyberbullying regulations.

In addition to a clear legal framework, cyberbullying in particular also requires further education of minors, as this is a crime where confusion may exist about which behaviours constitute a crime and which do not. This is of particular importance as certain unpleasant but innocent behaviours may, if unchecked, escalate into criminal offences.

Recommendations:

- Legislators and policymakers should obtain a deeper understanding of the various cyberbullying behaviours and their impact.
- Based on this understanding, legislators and policymakers should consider whether their legal system has gaps in protection and how to close them.
- Legislators and policymakers should consider how they can use social and educational measures to reduce the prevalence of cyberbullying (of minors) by minors.

Findings: Rules on Misinformation and Deception [30]

Regulating misinformation and deception presents a complex challenge, trying to balance the right to freedom of speech (and freedom of information) with the need in society to stop the spread of harmful misinformation and deception of large groups or populations, especially where the information is harmful.

This may be challenging for minor offenders as they may easily share information as a joke or to provoke reactions, but consequences may be serious. Because of this precarious balance, existing regulation tends to be fragmented and piecemeal. In many cases, misinformation is only covered by other qualifications, such as slander, when it involves false statements that harm someone's reputation. Some countries have specific crimes targeting misinformation or "fake news", typically with a very high threshold for the harm produced, such as the potential to affect public security or mislead a substantial portion of the population. This becomes particularly relevant in situations like the COVID pandemic.

In an ever-increasing digital society, there may be a need to further regulate misinformation and deception. However, striking the right balance between protecting the public and respecting fundamental rights such as freedom of speech and information is crucial. Simple instances of disinformation should not be outright forbidden or subject to censorship, as this could infringe upon these rights. However, intentional

[30] D4.5 Legal landscape for tackling cybercrime offenses by minors in Europe and beyond, RAYUELA project, available online / https://www.rayuela-h2020.eu/wp-content/uploads/2022/09/RAYUELA-D4.5_Final.pdf /

disinformation meant to harm individuals, or the public should be addressed through appropriate regulations and legal measures.
In order to maintain full respect for fundamental rights, policymakers and lawmakers should also consider social and educational measures. Such measures may be used in addition to legislative measures or may even replace them entirely.

Recommendations:

- Legislators and policymakers should consider how they can use social and educational measures to reduce the prevalence of misinformation/disinformation and deception by minors.
- Legislators and policymakers should consider whether additional regulation is necessary to address the issue of disinformation and deception and if so, must take due care to strike the right balance between protecting the public and respecting fundamental rights such as freedom of speech and information.

Findings: Rules on Hacking and Cybercrime as a Service (CaaS)
The regulation of Hacking and Cybercrime as a Service (CaaS) raises essential considerations, with some differences in legal opinions that could benefit from clarification. Surprisingly, many respondents in the RAYUELA did not view this as a crime concerning young offenders, except for the UK and the USA, which recognized minors as very significant risk sources. It is essential to acknowledge that children engage in such criminal activities, and the accessibility of CaaS to young individuals is a concerning aspect that requires policy attention.

While hacking, creating hacking tools, providing or using CaaS are clear offenses punishable by law, they may not always be perceived as such by minors, childrens. There may be instances where individuals attempt to defend their actions as jokes or pranks that were not intended to cause real-world harm. This is in particular imaginable where a youngster used a CaaS service which may somewhat resemble an innocent commercial experience. However, such a defence is not a viable legal strategy, as hacking or providing CaaS is sufficient to establish criminal liability.
Hacking and CaaS is regulated quite clearly and is relatively harmonized, thanks in particular to the Budapest convention on Cybercrime.

Therefore, the focus in this context should primarily be on creating awareness. Educating minors about the serious legal consequences of hacking and the provision or use of CaaS is crucial. By raising awareness about the potential harms and potential criminal liability involved, minors can be deterred from engaging in these activities and to redirect their technical skills and interests in other directions, within the confines of the law, including e.g., ethical hacking. It is essential to emphasise through education that hacking and providing or using CaaS are severe offenses with significant legal implications. In addition, awareness-raising may be needed within government, law enforcement and policy-making bodies. For example, in the RAYUELA consortium, Intervention campaigns were done by LEAs with good results: warning messages or honey pots in forums, as well as in google searches of CaaS tools have been proven to be useful in combatting it.

Recommendations:

- Policymakers should consider whether this issue is adequately recognized within the governmental bodies and agencies, law enforcement agencies and policy-making bodies and agencies, and if not create further awareness.
- Policymakers should focus on social and educational measures to raise awareness and educate minors about the serious legal consequences of hacking and the provision or use of CaaS.

General Recommendations

Based on the research findings of the RAYUELA project, the following general recommendations can be made in addition to the specific recommendations above based on the different cybercrimes studied:

- Focus on the development of comprehensive legislative and policy approaches that addresses cybercrime committed by children, acknowledging their significance in the offender population while focusing on prevention and education.
- Establish explicit and comprehensive criminal charges expressly targeting child exploitation in cyberspace by other minors, such as online grooming.
- Incorporate cybercrime prevention education into school curricula, focusing on improving knowledge of possible hazards, safe online habits, and responsible digital citizenship. Include law enforcement in prevention actions. Encourage efforts that provide children, parents, and educators with the information and resources they need to navigate the digital environment appropriately.

9. Policy Brief 08

9.1. Executive Summary

The RAYUELA Project developed a serious game focused on cybercrime to enhance students' cybersecurity knowledge. Through extensive pilot testing with students aged 11-16 across Europe, the project provided valuable insights into implementing gamification for cybersecurity education. Key recommendations include introducing the purpose of the game and research to students, ensuring they play honestly while protecting their data privacy, monitoring emotional responses to sensitive content, and engaging them in discussions afterwards. The pilots revealed gamification's effectiveness in making learning more impactful and enjoyable. Simulating real-life threats builds practical skills. However, educators must be attentive to potential emotional responses. Upholding data privacy and informed consent is also crucial. For broader implementation, educators should integrate such games into curriculums after understanding the mechanics. Parents should encourage open communication about cyber threats. Policymakers should recognize the value of simulation-based learning and enforce data regulations. Administrators should provide resources and training for educators. Overall, the RAYUELA Project demonstrated gamification's potential for engaging students in cybersecurity education. Following the recommendations can help policymakers, educators and parents create effective and ethical gamified learning experiences. As we advance digitally, such innovative methods are vital for empowering the next generation of cyber-aware citizens.

This policy brief offers practical recommendations for implementing gamification approaches in cybersecurity education based on the insights gained from the RAYUELA Project's three pilot phases. The RAYUELA Project, a European research initiative, aimed to develop innovative educational interventions using a serious game on cybercrime. The findings and experiences from these pilots provide valuable guidance for educators and policymakers seeking to engage students in cybersecurity education effectively.

9.2. Enhancing Cybersecurity Education Through Gamification - Insights from the RAYUELA Project Pilots

The RAYUELA Project developed a serious game with interactive storylines focused on cybercrime to enhance students' knowledge of cybersecurity and technological research. The project's three pilot phases aimed to test the game's effectiveness, usability, and impact on students' understanding of cyber threats. The success of the RAYUELA Project in engaging students in a gamified cybersecurity curriculum offers several key takeaways for educators and policymakers.

RAYUELA Playing Recommendations:

- At the beginning of the session, provide students with a brief introduction to the RAYUELA Project and the purpose of the game.
- Use the initial adventure as a tutorial to familiarize students with the game mechanics subtly. Ensure students understand that their choices matter and that they should act as they would in real-life situations.
- During gameplay, remain attentive to signs of discomfort in students, especially when encountering scenarios that may remind them of personal experiences. Reiterate the importance of reporting such events to trusted adults.

- After students complete each adventure, engage in open discussions about their experiences.
- Engage students in a post-game discussion. Ask for their opinions on the game and encourage them to share any relevant insights.

Key Insights and Implications:
The RAYUELA Project's pilot phases revealed essential insights into gamifying cybersecurity education:

- Gamification can effectively engage students in cybersecurity education, making learning more enjoyable and impactful.
- Simulating real-life cyber threats within the game allows students to develop practical skills and knowledge.
- Educators must be attentive to students' emotional responses when handling sensitive content related to cybercrime.

Recommendations for various Stakeholders for wider implementation of RAYUELA Educators play a pivotal role in shaping students' learning experiences. To effectively incorporate gamification into cybersecurity education they should consider integrating serious games, such as the one developed in the RAYUELA Project, into the standard curriculum subjects. These games provide students with hands-on experiences of cyber threats, making learning more engaging and practical. Before playing the game with their students, they need to spend time into understanding the game's mechanics and user interface. Then it is essential to monitor student progress during the pilot and after the end of the game initiate meaningful discussions with the students.

Parents or guardians are constant partners in a student's educational journey. They should frequently foster open communication with their children about their online experiences. They should encourage their children to share what they learn from the serious game and discuss any concerns or questions they may have about cyber threats. It is also very important that they are aware of any emotional reactions their children may have when engaging with sensitive content. Concurrently they need to offer emotional support and create a safe space for them to express their feelings.

Policymakers can influence the adoption of gamified cybersecurity education at a broader level. They should recognize the value of practical learning experiences that simulate real-life cyber threats and advocate for the inclusion of these elements in national or regional educational standards. It’s also crucial that they enforce data privacy regulations in all educational initiatives and ensure that informed consent is obtained from participants, emphasizing the importance of data confidentiality.

School administrators play a crucial role in implementing cybersecurity education programs. They should work with educators to seamlessly integrate serious games into the cybersecurity curriculum. They should also allocate resources and technology to support these initiatives and provide motives and training to educators to help them address emotional responses from students when engaging with sensitive content.

Conclusion
The RAYUELA Project's three pilot phases demonstrated the potential of gamification in cybersecurity education. By following the recommendations outlined in this policy brief, educators and policymakers can create engaging, effective, and ethical gamified learning experiences that prepare students to navigate the complex landscape of cybersecurity with confidence. As we continue to advance in the digital age, innovative educational methods like gamification are vital in empowering the next generation of cyber-aware citizens.

10. Policy Brief 09

10.1. Executive Summary

This policy brief aims to provide insights on developing impactful awareness campaigns and social media strategies to educate and empower minors and children to protect themselves from cybercrime risks. It synthesizes key findings from previous policy briefs and inputs from project teams to inform recommendations. Cyberthreats like grooming, bullying, trafficking, misinformation, privacy issues and inappropriate content disproportionately impact minors across Europe due to excessive Internet use, isolation, and home/school problems. Tactics used by offenders include impersonation, flattery, gifts and emotional manipulation. Anonymity facilitates cyberbullying and hate. Smartphones and apps enable threats despite their popularity. Targeted messaging and content tailored to groups' online presence and preferred platforms is advised. Facebook, Instagram and TikTok can effectively engage minors and children. Twitter and LinkedIn suit stakeholders like law enforcement, academia, industry and policymakers. Raising awareness should focus on promoting critical thinking to identify manipulation, avoiding oversharing personal information, securing social media settings, building resilience against grooming, reporting abuse, distinguishing curiosity from exploitation, increasing reporting mechanisms, and cross-sectoral collaboration. With collaborative efforts on multichannel, youth-centred campaigns and social media strategies, stakeholders can prevent cybercrime, empower minors to use the internet safely, avoid victimization and shape positive online spaces. But sustained engagement is essential to match evolving threats.

10.2. Effective Awareness Campaigns and Social Media Strategies to Combat Cybercrime and Engage Minors and Children

For whom?

This policy brief uses social media networks, and gamification approaches to design an effective communication and awareness campaign. It looks at various social media and their ability to generate social impact with various combinations of infographics, videos, music, and engagement formats such as quizzes. With the rapid proliferation of the Internet and digital technologies, the risks associated with cybercrime have increased significantly, particularly for minors and children. Designing an effective awareness campaign and utilizing social media platforms to educate, engage, and empower young individuals to protect themselves online is crucial. This policy brief outlines key considerations for developing an impactful awareness campaign and creating engaging social media posts to raise awareness about cybercrime among minors and children.

Targeted messaging and content

The awareness campaign of the RAYUELA project focuses on targeted groups, and according to their online presence, the consortium chose particular social media to design an individual communication channel with them.

No	Target Group	Social Media Type
1	Minors and Children	Facebook, Instagram, TikTok
2	Civic society organisation	Facebook, Instagram
3	Educational and VET institutions	Facebook, Instagram
4	LEAs	Twitter, Linkedin
5	Academia	Twitter, Linkedin, Facebook
6	Business sector	Twitter, Linkedin
7	Policymakers and public officials	Twitter, Linkedin

Cybercrime poses serious risks to minors across Europe, including grooming, bullying, trafficking, misinformation, privacy breaches, and inappropriate content exposure. Developing effective awareness campaigns and social media strategies is crucial to educate minors on these cyber threats, prevent victimization, and engage them as partners in combatting cybercrime. This policy brief gathers insights from previous policy briefs and inputs from all project teams under working groups 1-6 to provide key insights.

Key Insights:

- Minors are vulnerable to "fast track" cybercrime due to excessive internet use, isolation, and problems at home/school. Slow grooming also occurs.
- Impersonation, deception about identity, flattery, and gifts are used to manipulate minors by offenders.
- Trafficking of minors often involves "loverboys" who build dependency through emotional manipulation.
- Anonymity enables cyberbullying and cyberhate. Reporting is challenging for minors.
- Smartphones and apps like Instagram, WhatsApp and TikTok are very popular but also enable threats.
- Age limits and parental controls need better enforcement on social media.
- Awareness must cover fake news, verifying information, consequences of sharing, and misinterpreting humour/sarcasm.

Key considerations for the use of social media

- Promote critical thinking on social media and teach minors to collect evidence of abuse.
- Advise minors to avoid oversharing personal information and secure settings.
- Encourage minors to build resilience, set boundaries, and identify grooming indicators.
- Distinguish adolescent sexual curiosity from illegal exploitation in messaging.
- Increase social media reporting mechanisms and information points in schools.
- Foster collaboration between tech firms, police, and child protection organisations.
- Implement prevention education and training, focused on healthy relationships and sexuality.

11. Policy Brief 10

11.1. Executive Summary

We aim to define policy briefs based on RAYUELA's analytical results, complemented by an interpretation from a multidisciplinary perspective of specialised knowledge (including law enforcement agencies, psychologists, sociologists, educators, and more). This multidisciplinary approach is essential to clarify and refine the knowledge acquired.

In Deliverable D6.6, we discuss the impact of the analysed human and technological factors on cybercrimes affecting minors. We combined the quantitative results obtained in task 6.3 (data analysis based on causality and Bayesian statistics) with the results of WP1 (involving literature review, surveys to minors, focus groups, analysis of sentences, and interviews). All these results were critically discussed in a workshop with the other members of the RAYUELA consortium in Zagreb (Croatia) on September 28, 2023. During this workshop, participants responded to interactive questionnaires, shared their views on risk factors and intervention strategies, addressed discrepancies between the data analysis and WP1, and expressed their degree of agreement with certain conclusions. Building on this work, we will define specific recommendations and guidelines that may be useful for law enforcement agencies and policymakers.

Our results suggest that considering the available data and the technical limitations of the methodologies employed, the RAYUELA serious game represents a valuable tool in the field of social sciences for studying the analysed cybercrimes. These findings confirm the suitability of our chosen methodology, not only for predictive purposes but also for its prescriptive capability, which has been validated with expert input. However, it is imperative to reiterate the methodological limitations and emphasise the need to interpret these results cautiously.

It should be noted that Cyber bullying, (CB) is the only cybercrime for which we have a psychological test of cyber victimisation and cyber aggression, with which to validate the results obtained. For the rest of the cybercrimes, there is no such guarantee that the groupings of players identified correspond to those with a greater or lesser risk of suffering the cybercrime under consideration. Consequently, values obtained in the experiments could be exaggerated or distorted, and conclusions should be taken with greater caution. For this reason, we also held the workshop mentioned above, where we discussed the possible conclusions that could be drawn for each cybercrime.

11.2. General Policy Brief related to the Analysis of the Data gathered through the Videogame

Our analysis indicates that variables derived from the serious game are highly relevant for understanding and predicting most cybercrimes under consideration. This suggests that the RAYUELA game is well-suited for this purpose. In comparison, demographic and psychological factors are generally negligible, except for the case of cyberbullying (CB). In summary, creating risk profiles based on personal traits is ineffective; instead, risk appetite is better explained by behaviour in specific situations. Serious games are a valuable tool to assess how players react to complex situations without taking a real risk. These results validate the game design and show its potential to study and educate about the considered cybercrimes, although further research and data are needed for more robust validation.

Recommendations:

0. Prioritise Serious Game Integration: These findings confirm that the developed serious game is a valuable tool for understanding and addressing various cybercrimes affecting minors.
    - Policymakers should consider integrating serious games, like the one developed in RAYUELA, into educational and intervention programs to study and prevent cybercrimes effectively.
1. Focus on Behaviour, Not Profiling: There seems to be no specific profile of victims or perpetrators in the cybercrimes considered. We suggest focusing detection and prevention strategies more on behavioural patterns or responses to specific situations.
2. Cyberbullying Prevention: Given the significant impact of prior cyberbullying victimisation on the propensity to engage in cyberbullying, policymakers should prioritise targeted interventions and support for individuals who have experienced cyberbullying in the past. This approach may help break the cycle of victimisation and aggression.
    - Interventions should focus on understanding and addressing the behaviours exhibited by individuals in specific cybercrime scenarios.
    - Tailoring prevention efforts to behaviours in real-life situations is crucial.
    - We emphasise that individuals should not be stigmatised based on their socio-demographic conditions.
    - To enhance behaviour in specific situations, we propose providing education on information and communication technology usage by simulating or presenting complex scenarios. Serious video games have proven to be effective in this regard.
3. Ethical Serious Game Design: Ethical considerations must be upheld during game design and implementation, including privacy protection, informed consent, and age-appropriate content.
4. Validation and Further Research: Policymakers should support further research and data collection to validate and generalise the presented findings.
    - Expanding the scope of research and including a more extensive and diverse dataset will enhance the accuracy of policy recommendations.
    - Even within the same project, work on obtaining more samples to reach a more representative sample of the general population.

11.3. Cyberbullying insights from data analysis

The results indicate that the game and players' decisions are very relevant in explaining the CB offending and victimisation. It also seems that identifying CB offenders is easier from the available data. The most relevant variable related to demographic or psychological data is having been a previous victim of CB. There does not seem to be a unique profile for either perpetrators or victims.

For whom?

This policy brief focuses on various issues, such as risk factors of cyberbullying, from both practical and theoretical points of view. It is aimed at law enforcement agencies, academic organisations, educators, and experts focusing on cyberbullying.

Highlights and key observations

5. The research shows no specific victims' profiles but rather a particular vulnerability during perpetration, feelings of sadness and helplessness. Social structure and exclusion based on gender, sexual orientation and migration status may also play a role in victimisation.
6. Previous victimisation is the most relevant risk factor in CB offenders and victimisation.
7. Family Support seems to be a relevant risk factor for CB victimisation.
8. Self-esteem appears to be fundamental to CB offending and victimisation, although it may also be a consequence of the aggression in the victim's case.
9. Many hours spent on the Internet seem to be a relevant risk factor for CB offenders.

Key recommendations:

4. Raise awareness about the importance of parental supervision when young people go online and monitor their use time.
1. Establish information hubs where learners are confronted with complex real-life situations, explaining and facilitating the appropriate actions to be taken.
2. Concentrate on strategies to reduce feelings of isolation and social exclusion, which serve as the primary catalyst for becoming a cyberbullying victim.
3. Strengthen children's self-esteem by fostering family communication or relationships with trusted individuals.

11.4. Online Grooming insights from data analysis

We have no validated questionnaire to verify the results obtained in this cybercrime. Online Grooming (OG) is a very sensitive cybercrime to measure, especially considering the ethical restrictions of working with minors. According to the literature, there are two types of victims: vulnerable and risky appetite. In the game, we would be measuring, indirectly, only the risky-apetite victim. So, we do not have an excellent direct measure of the risk of suffering from this cybercrime.

The results indicate that the game and players' decisions are more relevant in explaining the risk of suffering OG than demographics or psychological variables. There does not seem to be a unique profile for OG victims.

For whom?

This policy brief focuses on various issues, such as risk factors in online grooming, from both practical and theoretical points of view. It is addressed to law enforcement agencies, academic organisations, and experts focusing on online grooming.

Highlights and key observations[1]

1. Gender is a relevant risk factor in OG. For instance, males appear to accept more friend requests from strangers.
2. Age also appears to be a risk factor in OG, primarily due to a quest for new experiences and sexual curiosity.
3. Social support is a relevant risk factor for correctly identifying dangerous new relationships or suspicious situations.

Key recommendations:

1. The fact that many children had public online profiles during initial contact highlights the importance of addressing proactive education about online risks and good online practices.
2. A comprehensive understanding of the victims' active involvement is essential for more effective prevention.
3. Emphasise strategies to reduce feelings of isolation and social exclusion.
4. Collaboration with families should be integrated to facilitate the disclosure of problematic situations.

11.4. Cyberthreats insights from data analysis

We have no validated questionnaire to verify the results obtained in this cybercrime. The results indicate that the game and players' decisions are more relevant in explaining the risk of suffering cyberthreats (CT) than demographics or psychological variables. There does not seem to be a unique profile for CT victims.

For whom?
This policy brief focuses on various issues, such as risk factors on technological risks, from both practical and theoretical points of view. It is addressed to law enforcement agencies, academic organisations, and experts focusing on cyberbullying.

Highlights and key observations

1. Demographic Factors: General agreement between WP2 and WP6 analyses regarding certain demographic factors, such as male gender, age, and limited family support, associated with a higher risk of cyberthreats.
2. Internet Usage Hours: The amount of time teenagers spend online was identified as a relevant factor in assessing the risk of experiencing cyberthreats, underscoring the importance of online time management.
3. Behaviour: Results suggest that teenagers' online behaviour is a better indicator of susceptibility to cyberthreats than demographic traits.
4. Unlike other cybercrimes, we observe alignment with WP2 regarding the Big Five; however, we do not emphasise it, as the measures are considered inadequate, and the conclusions in WP2 are somewhat speculative.

Key recommendations:

- We recommend using serious games or workshops to measure adolescents' online behaviour in real-life situations and, at the same time, teach them good online practices.
- Provide ongoing cybersecurity training and awareness, emphasising secure practices such as regular password updates and ensuring strong password security.
- Provide guidance on the procedures to follow if they detect a security breach.
- Parental Control and Supervision: Promote parental involvement and communication with their children about online activity.
- Mental Health Support: Offer resources for teens facing emotional challenges that may affect their online safety.

- Promote responsible internet usage, tailoring recommendations to their specific online activities and needs.

11.5. Fake News insights from data analysis

We have no validated questionnaire to verify the results obtained in this cybercrime. The results indicate that the game and the player's decisions are relevant in explaining the risk of falling for Fake News (FN). There does not seem to be a unique profile for CT victims.

For whom?
This policy brief focuses on various issues, such as risk factors of FN, from both practical and theoretical points of view. It is addressed to law enforcement agencies, academic organisations, educators and experts specialising in combating the proliferation of fake news.

Highlights and key observations

1. We have not observed the relevance of demographic or psychological factors.
2. Teenagers are heavy users of social media platforms, which can be breeding grounds for spreading FN.
3. It seems that internet usage hours (on social networks) may influence the risk of falling for FN.
4. Media literacy is a crucial skill for discerning credible sources from unreliable ones. Many teenagers lack formal education in media literacy, making them more prone to falling for FN.
5. Teenagers may feel pressured to conform to the opinions of their peers. This can lead them to accept and share fake news to fit in or avoid social isolation.
6. FN often relies on emotional or sensational content to attract attention. Teenagers, who may be more emotionally driven, can be particularly susceptible to such tactics.
7. Educators and parents play a crucial role in helping teenagers become more discerning information consumers by teaching them critical thinking skills, media literacy, and the importance of fact-checking.

Key recommendations:

1. We recommend using serious games or workshops to measure adolescents' online behaviour in real-life situations and, at the same time, teach them good online practices.
2. Introduce media literacy education as a part of the school curriculum. Ensure that students learn critical thinking skills, source evaluation, and fact-checking techniques.
3. Familiarise students with fact-checking tools and resources and encourage them to fact-check information before accepting it as accurate.
4. Educate adolescents on the consequences of disseminating fake news. Highlight the legal consequences, potential harms and negative impacts on individuals and society.
5. Promote responsible online behaviour, emphasising the importance of ethical and respectful online communication.
6. Engage parents and guardians in conversations about media literacy and online safety, providing them with resources to support their children's digital literacy education at home.

12. Conclusions

In summary, these 10 policy briefs offer an overview of the cybercrime issues that impact young people in Europe. They cover online grooming, cyberbullying, human trafficking, misinformation, security and privacy concerns, problematic technology use, legal issues, education through gamification, effective awareness campaigns, and the insights on the considered cybercrimes coming from the analysis of the data gathered through the videogame. The briefs shed light on concerning patterns, identifying gaps in existing policy frameworks, propose prevention strategies and provide recommendations to strengthen safeguards and empower individuals to navigate the online world safely.

The key takeaways include the necessity for definitions that criminalize online grooming and cyberbullying. It is essential to implement programs focused on prevention while improving reporting mechanisms and fostering collaboration among stakeholders. Targeted awareness campaigns are also crucial. The briefs emphasize the promotion of resilience critical thinking skills and digital literacy among minors while advocating for oversight when leveraging technology and AI based solutions.

Overall, these policy briefs highlight the significance of approaches that are based on evidence. Collaborative initiatives involving minors themselves, families, schools, industry players, law enforcement agencies, researchers and policymakers are vital. Sustained efforts are paramount to strengthen safety frameworks and foster a culture that can adapt to evolving threats.

Looking ahead the continuous research, education advocacy and development of policies will be crucial in combating cybercrimes affecting minors. Stakeholders must remain vigilant towards emerging threats and new platforms. It is imperative to prioritize promoting literacy, resilience and empowerment, among youth.

These policy briefs play a role in combating cybercrime by providing guidance for evidence-based decision-making, informing advocacy campaigns, raising awareness and promoting collaboration between sectors. They condense insights into a roadmap that can drive actions in legislation, law enforcement, education, technology regulation and social initiatives aimed at safeguarding the online experiences of young Europeans.

References

- Balakrishnan, Vimala, Shahzaib Khan, and Hamid R. Arabnia. "Improving cyberbullying detection using Twitter users' psychological features and machine learning." Computers & Security 90 (2020): 101710.
- Facebook. "Here's how we're using AI to help detect misinformation." Facebook AI (blog), November 19, 2020. https://ai.facebook.com/blog/heres-how-were-using-ai-to-help-detect-misinformation/.
- Hasse, Alexa, Sandra Clio Cortesi, Andres Lombana, and Urs Gasser. "Youth and Artificial Intelligence: Where We Stand." SSRN Electronic Journal, 2019. https://doi.org/10.2139/ssrn.3385718.
- Herrero-Diz, P., Conde-Jiménez, J., & Reyes de Cózar, S. (2020). Teens' Motivations to Spread Fake News on WhatsApp. Social Media and Society, 6(3).
- Mendiguren, T., Pérez Dasilva, J., & Meso Ayerdi, K. (2020). Actitud ante las Fake News: Estudio del caso de los estudiantes de la Universidad del País Vasco. Revista de Comunicación.
- Shu, K., Sliva, A., Wang, S., Tang, J., & Liu, H. (2017). Fake news detection on social media: A data mining perspective. ACM SIGKDD explorations newsletter, 19(1), 22-36.
- Smeaton, E. (2013). Working with children and young people who experience running away and child sexual exploitation: an evidence-based guide for practitioners. Essex: Barnardo's.
- Suler, J. (2004). Online disinhibition effect. CyberPsychology and Behavior, 7, 321-326.
- Willard, Nancy E. Cyberbullying and cyberthreats: Responding to the challenge of online social aggression, threats, and distress. Research press, 2007.
- Wachs, S., Wright, M. F. & Vazsonyi, A. T. (2019). Understanding the overlap between cyberbullying and cyberhate perpetration: Moderating effects of toxic online disinhibition, Criminal Behaviour and Mental Health, 29(3), 179–188. doi: 10.1002/cbm.2116.

Further Readings

- D1.3 Open report on interview results: Building A Knowledge Base On Cybercrime Drivers For Children & Young Adults
- D1.5 Open Report on Case Study Results
- D1.7 Victim and offender profile description report: Building A Knowledge Base On Cybercrime Drivers For Children & Young Adults
- D2.5 RAYUELA Open report on Technological threats associated to the cybercrimes considered
- D2.1 ANALYSIS OF SECURITY AND PRIVACY OF CONNECTED DEVICES
- D2.2 METHODOLOGY, TOOLS, AND RESULTS OF TESTING SECURITY AND PRIVACY RISKS OF CONNECTED DEVICES
- D2.4 TECHNOLOGICAL THREATS ASSOCIATED WITH THE CYBERCRIMES CONSIDERED
- D2.5 Open Report on Technological Threats Associated with the Cybercrimes Considered