Authors: Adriana Iordache, Ioana Cărtărescu-Petrică

Youth online behavior, risks and avenues for mitigating them

Transnational report

ISBN 978-973-0-38673-8

Bucharest
2023

Co-funded by the European Union

Authors: Adriana Iordache, Ioana Cărtărescu-Petrică

Youth online behavior, risks and avenues for mitigating them

Transnational report

Bucharest
2023

Project Title: **Action-Based Approach in Addressing and Mitigating Risks of Young People in Online Social Networks**

Agreement Number: **2021-1-RO01-KA220-YOU-000028688**

EU Programme: **KA2 – Cooperation partnerships in youth**

Contributors:

Damaris Frîncu
Octavian Rusu
Ioanna Athinodorou
Marja-Liisa Helenius
Eveliina Kauhanen
Myrto Siapardani
Dimitris Georgoulis
Stella Ioannou
Corso Giulia
Ursino Giuseppe Fabio

This document has been produced with the financial support of the 'ERASMUS+ KA220-YOU - Cooperation partnerships in youth' programme of the European Union. The content represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Table of contents

I. Introduction

This report looks into the risks associated to the use of internet and online social networks by young people. It explores aspects such as socio-demographics, social media use, risk perception, risky and preventive and behaviors, critical reading ability, incidence of the manifestation of risks as well as other relevant aspects in the context of the post-COVID-19 pandemic. The research aims to assess the current situation and the factors which hinder or encourage the manifestation of these risks, in order to identify the learning needs of young individuals so that they can prevent and combat these phenomena. The ultimate goal of this report is to gather pertinent information for the development of an online game that equips young people with the necessary tools to mitigate the identified risks.

The report will present an overview of the online behavior, attitudes and manifestation of the identified risks among young people in six European countries: Cyprus, Finland, Germany, Greece, Italy and Romania. The research reflects on the main online risks faced by young people (aged 16-30), the patterns in which these risks manifest and the relevant national strategies and legislation aimed at combating these risks. Specifically, the report will examine their socio-demographic characteristics such as age, gender, socioeconomic status, rural/urban residence, level of education and ethnicity. Additionally, it will explore their social media usage and online behavior, risk perception, existing preventive behaviors and attitudes in the post COVID-19 era.

Furthermore, the study will delve into the attitudes and behaviors of young people regarding global threats such as pandemics, international politics, armed conflicts, refugees, and will also identify risk factors among youth concerning fake news, disinformation, and other pertinent risks. The main risks identified by the research as being associated to the online presence of young people are the following: 1. fake news and disinformation, 2. cyberbullying, 3. identity theft, 4. image-based sexual abuse and online gambling and gaming. The report will describe each of these risks, along with their patterns of manifestation and effects upon young people. Moreover, the study also includes information on the regulations aimed to discourage these risks in the six countries, as well as relevant data regarding the manifestation of the risks.

The report is based on both qualitative and quantitative data, gathered from all six countries in the period of October- December 2022, namely by an online survey completed by 348 young people (16-30 years old) and 30 interviews with youth workers and trainers from the six countries. The data was collected by national experts contracted by Center for Not-for-Profit

Law Association in Romania, Institute of Entrepreneurship Development (Greece), Vitale Tecnologie Comunicazione - Viteco SRL (Italy), Learning for Integration ry (Finland), BK Consult GbR (Germany) and Synthesis Center for Research and Education (Cyprus).

This study has been elaborated within the RISE project: Action-Based Approach in Addressing and Mitigating Risks of Young People in Online Social Networks, financed by European Union's Erasmus+ Programme, Strategic Partnerships - Key Action 2, project number 2021-1-RO01-KA220-YOU-000028688.

II. Methodology

The present report reunites and comparatively presents the results of the research conducted in all six states included in this study (Germany, Greece, Cyprus, Finland, Italy and Romania) on the topic of online risks faced by young people.

Both quantitative and qualitative data were collected for the present research. The instruments used by every participant country was identical, for comparability purposes: an online survey filled in by participants on a non-probabilistic, voluntary basis. Since the survey employed a quantitative approach, using exclusively closed questions, semi-structured interviews with youth workers and trainers were also conducted in each state and used within the present analysis to illustrate the quantitative findings and provide more in-depth, qualitative insights meant to exemplify and explain the revealed state of affairs.

Data from a total of 348 online survey participants – aged 16 to 30 – who took part in this research was collected between October and November 2022. Since participation in the survey was voluntary, different countries received a different number of responses, as follows:

- Germany – 40 respondents
- Greece – 39 respondents
- Finland – 76 respondents
- Cyprus – 40 respondents
- Italy – 70 respondents
- Romania – 83 respondents

When it comes to the qualitative data, exerts from each country conducted a number of interviews with different types of professionals working with young people: youth workers, teachers/ trainers, social workers, activists for young people's rights, etc., as follows:

- Germany – 4 interviews conducted with teachers and non-formal educators.
- Greece – 4 interviews conducted with youth workers and teachers.
- Finland – 4 interviews conducted with social workers, a youth worker and a theatre director.
- Cyprus – 4 interviews conducted with teachers and non-formal educators.
- Italy – 4 interviews conducted with psychologists and teachers.
- Romania – 10 interviews conducted with formal educators, non-formal educators, youth counselors, advocates for young people's rights and a psychologist.

Given the fact that the participant samples from each of the six countries included in the study are quite low (most consisting of around 40 respondents) and that a significant portion of the data is categorical in nature, a simple analysis, based on frequency distribution was opted for instead of more complex statistical operations. For most categories of information presented, two major views were used to present the findings: a comparative approach, where the results of each country, for each tested variable, would be displayed side by side and an overall, big-picture chart which can provide the reader with a global perspective. This approach allows for the understanding of both the regional differences and the wider, overall European trends and patterns of online risks facing young people.

The limitations of the present research are primarily related to the small size, as well as the non-probabilistic nature of the research samples, which leave room for sampling bias to occur. Furthermore, minor differences in the way the different countries have conducted the survey and processed the data (question translation nuances, minor variations in question layout, minor data coding errors, etc.) may have contributed to some decrease in data accuracy.

Further research is encouraged in order to go into further depth studying issues out of the scope of the present study, but very relevant to it, such as a comparative analysis of the educational frameworks existing in all 6 countries meant to support online safety and critical thinking and to actively combat online risks for children and young people.

III. Literature review

1. Fake news and disinformation

The first online risk addressed by this report is that of online misinformation, disinformation and fake news. According to the European Commission, these can be defined as two different phenomena, based on whether the spreading of false information is intentional or not. Thus, according to the European Commission, disinformation is false or misleading content that is spread with an intention to deceive or secure economic or political gain, and which may cause public harm. Misinformation is false or misleading content shared without harmful intent though the effects can be still harmful. Both disinformation and misinformation can have a range of harmful consequences, such as threatening the quality of democratic debate, increasing polarization and putting the health, security and environment at risk (European Commission 2022). Disinformation has been closely linked with the development of echo chambers, that is online spaces in which people tend to talk only with one another and reinforce already held beliefs, thus not coming in contact and not being able to accept arguments from those who hold a different opinion.

The research conducted for this report has focused on several issues regarding disinformation: the extent to which it creates a feeling of alienation among young people, the polarizing effect it has on democratic debate, several conspiracy theories shared widely, especially during the COVID-19 pandemic, the psychological factors which favor its spread and the legal responses to it in the countries represented in the project.

One of the most prominent issues examined in the literature is the extent to which some psychological factors increase one’s probability to believing and sharing fake news. Several theories have been proposed and tested by researchers in psychology. These debates are examined in the report on Romania. Some of these hypotheses include: 1. the political hypothesis - people tend to believe and share news that confirm their beliefs; 2. the "cognitive laziness" hypothesis - people do not pay enough attention to what news they read and simply share news items without consideration; 3. The heuristics hypothesis - people tend to think in shortcuts and accept information which is closer to what they already know and reject information which does not conform to it; 4. The in-group/ out-group hypothesis - conspiracy theories/ disinformation is believed if it increases the solidarity of a particular in-group, especially if it includes negative stereotypes about an out-group perceived as hostile.

Among the findings of researchers were that those who had a "conspiracy mentality", were the most likely to believe in conspiracy theories (Mahl, Scheffer and Zeng, 2022; Petrovic and Zezelj 2021). Alternatively, Pennycook and Rand (2021) supported the heuristic hypothesis according to which people tend to share fake news and disinformation because they do not take the time to evaluate the information that they have been presented with. Prooijen and van

Vugt (2018) claim that the tendency to believe conspiracy theories could be grounded in evolutionary psychology, given that it might be triggered by mechanisms which might have been crucially useful in hunter-gatherer societies in which inter-group aggression was high and the losses from such conflict were significant.

With regard to the strategies useful to combat fake news, two distinct approaches have been identified in the literature: the retroactive approach, or de-bunking, which involves publicly sharing a disclaimer to counter false information that has been already spread. This has the disadvantage that false information tends to spread much faster than statements aimed at disputing it, and that people tend to believe information that confirms what they already know. Alternatively, Pennycook and Rand (2021) recommend preemptive strategies, such as pre-bunking, for example through education and online games. In their view, this is more effective, given that it forewarns people to stop and consider the veracity of a news item that they encounter, rather than attempting to reach all those convinced by a previous piece of disinformation.

Increasing media literacy skills has also been seen as highly effective, for example in Finland, which tops the media literacy index, an annual index of European countries measuring resistance to fake news. Media literacy is the “ability to critically engage with media in all aspects of life”. Media literacy skills include differentiating facts from opinion and analysis, verifying sources, and understanding how the media works. Finland has been credited with its success given the early age at which it begins teaching media literacy for students. In Finnish schools, information literacy and critical thinking are taught to children in kindergarten as well and media literacy classes for older people are provided. The aim is to make sure that everyone (from students to politicians) can spot various forms of misinformation, disinformation and mal-information (Quicke 2020). Alternatively, the Italian Ministry of Health has run several public awareness campaigns on disinformation in the context of COVID-19. Similarly, the Greek government has launched awareness campaigns to educate the public on how to identify and avoid false information, and it has also worked with social media platforms to remove fake news and misinformation from their sites. Conversely, Germany has undertaken a tougher approach, allowing courts of law to suspend false information based on reports from citizens (Lovari and Righetti 2020, Donato 2022).

Finally, the national reports of countries included in the project describe specific conspiracy theories which have been spread during recent times. These include fake news about the negative effects of Covid-19 vaccines, the association of COVID-19 with malignant entities

which have, allegedly, created and spread it and the idea that 5G towers are used to control the vaccinated (Moscadelli et al, 2020).

2. Cyberbullying

Another important online risk encountered by young people is that of cyberbullying. According to Younan (2018), this phenomenon can be defined as *unprovoked aggressive or violent behavior which implies repetitiveness, the express intent to cause distress to the victim, as well as a power imbalance on the part of the perpetrator.* The aim of cyberbullying is to prevent the victim from expressing their opinion, by using ad hominem attacks, denigratory language and other forms of humiliation with the express goal of making the person experience feelings of humiliation and shame.

The specific characteristics of the bullying carried out online is that it grants significantly more power to the aggressor, due the his or her ability to conceal his or her identity. According to the literature consulted for this report, online bullying deepens the power imbalance between the aggressor and the victim, causing significantly more harm, despite the absence of physical interaction between the two (Ansary, 2019; Bartlett et al, 2020; Vaillancourt et al., 2017 apud Ansary, 2019). Scientific studies have identified several types of online bullying such as online harassment (trolling, threats, mobbing), cyberstalking, doxxing, impersonation or exclusion (Scheitauer et al, 2021; Runcan, 2020).

According to the literature consulted for this study, online harassment can include behavior such as trolling (purposefully contradicting or insulting someone online in order to cause them anger or distress), denigration (posting hurtful or offensive statements about someone else online), visual violence (exposing someone to violent multimedia content against their wishes, such as sending them unsolicited graphic videos or imagery), online threats (directly or indirectly threatening someone's physical integrity, psychological wellbeing or livelihood online, through private messages or public posts) or mobbing (encouraging others to join up in harassing someone, either in person or online, through digital means (Runcan, 2020). Alternatively, cyberstalking is defined as "repetitive and unwanted communication or contact that is directed toward an individual through electronic means (e.g., Internet, social media, email or other forms of technology)" (Kaur et al, 2021) while doxxing is defined as "the practice of publishing private, proprietary, or personally identifying information on the internet, usually with malicious intent" (Andersen and Wood, 2021).

Other forms of cyberbullying identified in the literature include impersonation, a situation in which a person posts content online while pretending to be the victim, with the explicit goal of humiliating or denigrating him or her. Further, exclusion involves arbitrarily withdrawing or denying the victim's access to internet places which she/ he wishes to visit, such as chat groups, online gaming servers, mass blocking them on social media, etc. Studies analyzed in this report have identified the common online environments that online harassment can take place, include social media (66 percent), comments section of a website (22 percent), online gaming (16 percent), personal emails (16 percent), discussion sites (e.g., reddit) (10 percent), dating sites or apps (6 percent) (Sammons, 2017).

Regarding cyberbullying, several topics are approached by the national reports elaborated under the framework of the RISE project. These include the increase in time spent online by young people during the pandemic and the association of this increase with an increase in cyberbullying. Secondly, the fact that opportunities for online access are distributed unevenly between developed, urban areas and sparsely populated, rural areas is mentioned in the report on Greece. Thirdly, the reports discuss the way that states have reacted to this new phenomenon, by regulating, although imperfectly, this behavior.

The COVID-19 pandemic has led to a considerable increase in the time spent online by young people. However, this was associated with an increase of the phenomenon of cyberbullying and the consequent rise in mental health issues associated with it. According to a study, adolescents who experience cyberbullying both as victims and as offenders have higher rates of depression, lower self-esteem, school and academic problems, more delinquent behaviors and higher rates of suicide (Hinduja et al 2010). Another study, carried out in Finland, has revealed that almost 34% of survey respondents have been a victim of some kind of online bullying. A comparison of the survey data between 2016-2022, has revealed that online bullying has increased by 20% (Ebrand 2022), while in Italy, according to a survey conducted in 2019 by ISTAT – the Italian National Statistics Institute – around 7.1% girls and 4.6% of boys who own a smartphone or can access an Internet connection have been subjected to continuous harassment via the Internet or cell phone (Commissione parlamentare per l'infanzia e l'adolescenza (2019). Results in Greece have shown that between 3 and 20 % of young people have been the victims of cyberbullying, while 3 to 25% have committed acts of cyberbullying, depending on the type and frequency of cyberbullying and cybervictimization (Athanasiades et al. 2015; Kapatzia 2008; Tsorbatzoudis and Aggelakopoulos 2012).

Regarding the issue of regulation, most national legislations sanction cyberbullying. In Romania, the law on domestic violence has been updated in 2020, to include aggressive

online behavior, while the Criminal Code of 2009 punished both harassment and identity theft. In Germany, Section 1 of the Gewaltschutzgesetz—the civil law prevention of acts of violence and stalking—is employed to take the necessary measures to prevent such conduct. Cyprus uses several laws punishing cybercrime, including one which allows for the retention of telecommunications metadata and their release upon a court order.

3. Online identity theft

Unlike cyberbullying, even in the form of impersonation, online identity theft is much more dangerous, as it involves impersonating the victim in order to obtain material profit, either by defrauding the victim or by defrauding others in the name of the victim. Some of the forms under which online identity theft has been manifested include: phishing - the perpetrator sends the victim a link to a copy of a legitimate website, such as a bank website, where they are asked to enter their confidential information (personal information, credit card information, sensitive passwords, etc.), hacking - which uses force instead of deception, social media cons - online identity thieves sometimes steal a regular social media user's name and photographs and create a fake account, which they use to connect with their friends and family and to ask for money and identity spoofing - the identity thief creates a fake webpage or social media account in someone else's name, but it is usually a public person (a famous artist, politician, influencer, etc.) and requests information, donations for fake causes or sells products in their name (Soomro, 2018).

Depending on the goal of the perpetrator, identity theft has been classified as: financial identity theft – the perpetrator uses the victim's identity to obtain financial gain, criminal identity theft - the perpetrator uses the victim's identity when committing a crime, medical identity theft - where the perpetrator uses the victim's identity to receive medical treatment, prescription drugs or to file false insurance claims, synthetic identity theft: where the perpetrator creates a new identity by combining real and fake information to open new accounts, government identity theft - perpetrator uses the victim's identity to obtain government benefits or documents, such as passports or driver's licenses and child identity theft: where the perpetrator the perpetrator uses a child's identity to open credit accounts or apply for government benefits.

The national reports present the main patterns of manifestation of this risk and the national regulation of the topic. Regarding the first, in Romania, a Recorder investigation (Udișteanu, 2022) revealed that in 2019-2020, the number of reported incidents of internet fraud, including identity theft has doubled, resulting in 7862 criminal records, while unresolved cases soared

to over 21.000. Conversely, in Italy, over 25.000 cases of identity theft have occurred, with a total value of over EUR 200 million. According to the Hellenic Data Protection Authority (HDPA), there were a total of 2,828 data breaches reported in Greece between May 2018 and December 2019. Of these, 115 were related to identity theft.

Regulation of online identity theft is considerably better developed than other forms of online abuse, as it relies on the incrimination of classical forms of fraud. In Romania, this is regulated through the 2009 Criminal Code, as well as in Germany, which sanctions fraud through the criminal code (Niethammer, Rieks, Saerbeck, Norbu, 2022).

4. Image-based sexual abuse

The third risk addressed by this report is that of image-based sexual abuse. According to the literature, it can be encountered in two different forms, both of them with significant negative consequences for the victim. The first one is revenge pornography, which can be defined as "the posting of revealing of sexually explicit images or videos of a person, without the consent of the subject, in order to cause them distress or embarrassment" (O'Conner et al, 2018). Generally, the aim of such behavior is to hurt the person it targets, as the perpetrator believes he has a good reason for revenge. In certain cases, the photos shared have been given to the perpetrator willingly by the victim, generally as a memory of a sexual relationship, however, without the consent to share further. In other cases, these images are obtained fraudulently, without the victim's consent, for example by accessing the victim's e-mail, phone, computer or other storing devise.

This type of behavior is usually retributive in nature, meant to humiliate a former sexual partner (or a sexual/social rival) who the perpetrator feels has wronged them. However, at other times, there is no personal relationship between the victim and the perpetrator, but the latter has come in possession of the material and believes the person depicted in it deserves to be publicly exposed. Sometimes, the distributed media content has been shared consensually by the victim, for the recipient's eyes only, other times, the images were obtained illicitly, without the victim's knowledge or consent (Sullayway, 2022 in Dunbar, 2022). Regardless of how they are obtained, nude and/ or sexually explicit photographs or recordings are posted on social media, shared on pornography websites or distributed directly to the victim's peers, in order to cause them humiliation.

The second form of image-based sexual abuse encountered is the sharing of unsolicited sexual photographs of oneself. Given that most recipients are female and most perpetrators

are male, the sender generally frames the act of sending as a compliment. However, the gesture is viewed by the women on the receiving end as a form of misogyny, sexual abuse and harassment. The recipients of the pictures perceive an aggressive intent behind the explicit pictures, which they believe are meant to scare, disgust or humiliate them rather than stir their desire (Paasonen et al, 2019; Amundsen, 2020).

The main problem identified in the national reports regarding image-based sexual abuse is the incoherent regulation at national level aimed at combating the phenomenon. Also, there is a tendency of both peers and law enforcement authorities to blame the victim for taking and sharing explicit photographs of oneself and, thus, becoming exposed to revenge pornography.

Romania has only very recently incriminated revenge pornography, through a law which entered into force in June 2023. The national report refers to the 2021 National Strategy for Preventing and Combating Sexual Violence "SYNERGY" (2021-2030) and the Action Plan for Implementing this strategy. Further, the report presents other regulations which might have been used to combat revenge pornography before the adoption of the new law, as well as some cases in which the victims of revenge pornography were blamed for their own abuse. The German report briefly mentions the lack of any specific legislation to combat revenge pornography, while the Italian report argues that four different drafts of legislation have been presented by different politicians and that, according to a survey conducted from 2019 to 2020, nearly 13% of Italians respondents know a victim of revenge porn. Similarly, in Greece, 18.8% of respondents in a survey reported that they knew someone who had been a victim of revenge porn. Greece criminalized revenge porn in 2019, through a new law, that makes it a criminal offense to share sexually explicit images or videos without the consent of the person depicted. The law provides for fines and imprisonment for those found guilty of this offense, and it also includes provisions for the removal of such content from online platforms.

5. Online gambling

While the addictive effects of traditional gambling have been well documented, the move of gambling activity online is a relatively new phenomenon, which has shown the same effects on people. People addicted to gambling tend to spend more and more money online, which is facilitated by the simple system of having a credit card attached to the game. Moreover, in addition to the classical forms of online gambling, such as sports betting and games of chance, a new phenomenon has emerged: loot boxes in online games. These presuppose that a player, engaged in a virtual game, pays real money, either to acquire an object that helps him or her complete a quest, or the chance to win such an object. Young people’s vulnerability to

online gambling is enhanced through the use of targeted advertising, which recognizes user profiles which are most likely to be persuaded to gamble by the data they have shared on social media and exposes them relentlessly to pop-ups and sponsored advertisements for such activities. Further, loot boxes in online games generally target young people, who are more vulnerable to these.

The comparative reports documented the extent and patterns of manifestation of the risk of online gambling and gaming addiction. In the Romanian report, the case of a 6-year-old boy was documented who spent 6000 RON on virtual weapons and perks (stiri.tvr.ro, 2019). In Greece, several studies were conducted on the adult population: in 2016, the prevalence of the gambling problem in Greece was estimated to be affecting around 3.5% of the adult population, while another study published in 2018 by the Hellenic Gaming Commission found that the percentage of Greeks with gambling problems had risen from 0.6% in 2011 to 1.5% in 2017.

In terms of the regulation of online gambling, in Germany a new treaty was adopted regulating the practice in July 2021. The new German Interstate Treaty on Gambling (ISTG) or Glücksspielstaatsvertrag (GlüStV 2021) legalizes and regulates online gambling in Germany across all 16 states. Its main purpose is to regulate the opaque online market for gambling in a uniform manner and to curb illegal offerings. Alternatively, in Romania, gambling is somewhat covered by Government Emergency Ordinance no. 77/2009, banning advertisements in the campuses of educational institutions explicitly requiring the mentioning of the prohibition of the participation of minors in gambling.

IV. Analysis of the data

1. Socio-demographic characteristics of the study participants

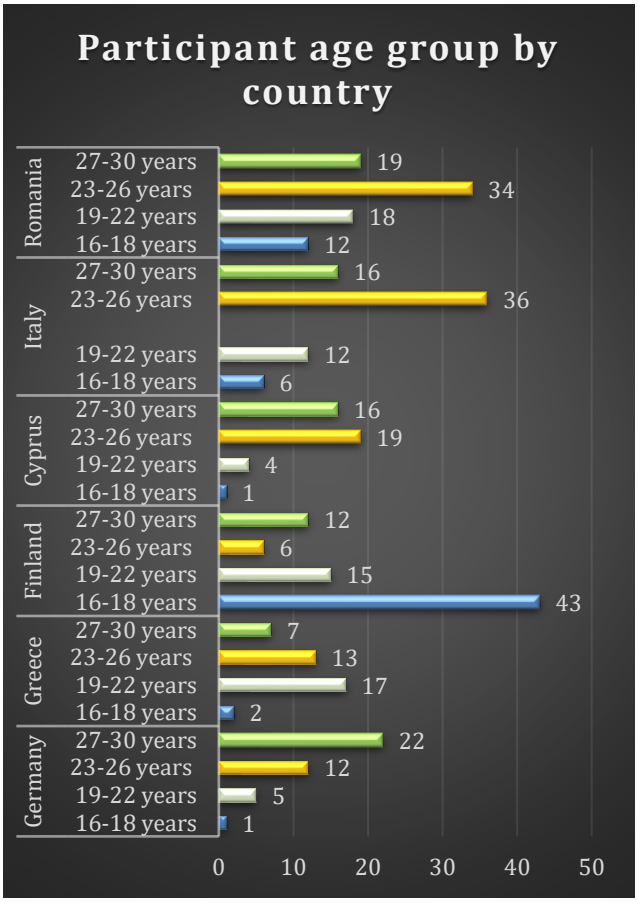
When conducting an international study which spans across six European countries, it is important to be aware not only of the overall characteristics of the respondents, but also of the differences in socio-demographic configuration between research samples in each state. Since the present study was conducted online, using non-probabilistic, voluntary response-based sampling, it was not possible to control the characteristics of respondents in such a manner that they would be similar and comparable across all states. This is amplified by the rather small number of participants per country (under 100) and by cultural differences which influence the response likelihood of people from certain socio-demographic backgrounds.

Since aspects such as respondent age group, gender, level of education and income or occupational status can significantly influence their attitudes, practices and experiences, discrepancies among research samples from different states can lead to misleading overall results if left unaddressed.

That is why this section provides an overview of both the overall characteristics of the participants to our research and their breakdown by country, showcasing any outliers or discrepancies which need to be taken into consideration when analyzing the quantitative data.

Number of participants

A total number of 348 young people responded positively to our invitation to take part in the present study, by answering an online survey. Given the voluntary nature of participation, the number of answers received in each of the six states differed, ranging between 39 and 83. While it is true that smaller sample sizes make a sample size effect more likely to occur, due to the increased likelihood of distribution which does not reflect that of the general population, it must be kept in mind that the findings of the quantitative research will be corroborated with those obtained through qualitative methods (interviews with youth workers carried out in each state), as well as with the insights from each country's literature review and legislative analysis.

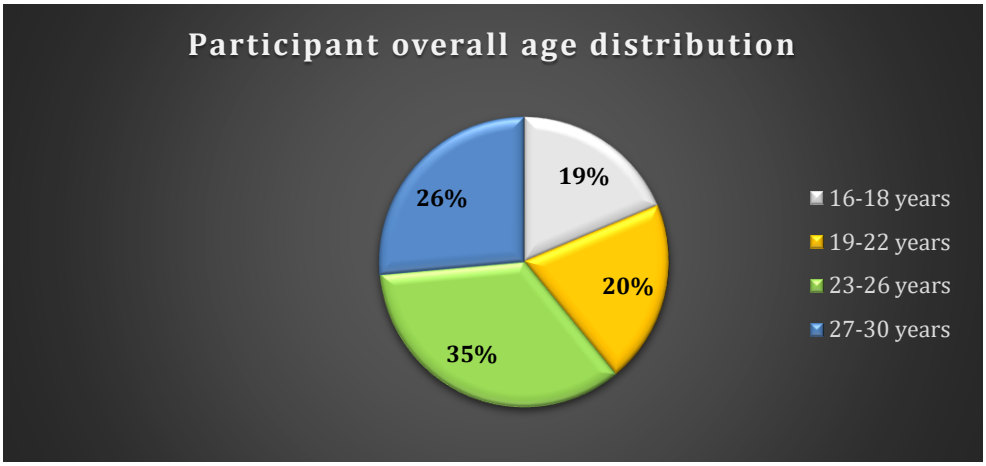


Participant age group

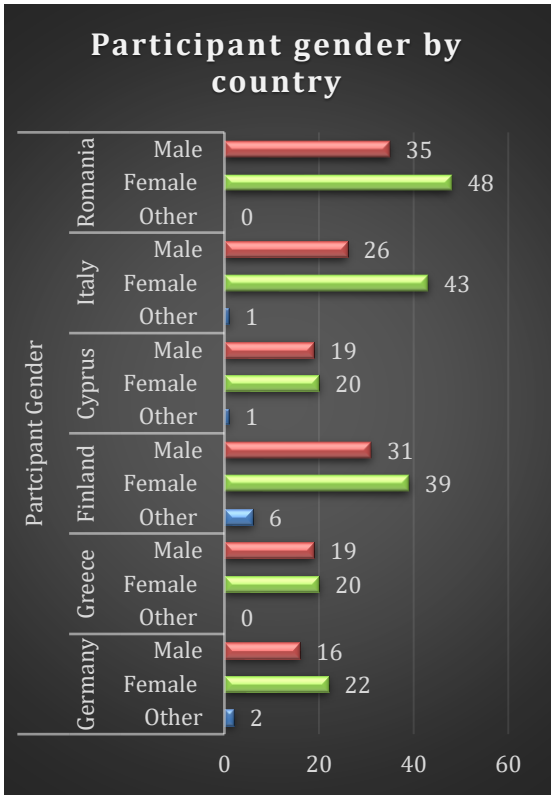
The age of participants ranged from 16 to 30 years. Overall, the majority (61%) of participants fall into the 23-30 age group, with the 23-26 category being the most represented (35%). The fewest participants are, almost equally, in the 16-18 and 19-22 age group (19%, respectively 20%). However, distributions of age groups per country show significant differences. For example, the bulk of the already under-represented 16-18 age group stems from Finland (66% of the total respondents in this age group and the most numerous category for this country), while Germany, Greece and Cyprus combined only add up to 4 respondents

from the 16-18 year old group in total. Similarly, while in Italy and Romania, respondents in the 23-26 age group are significantly more numerous than the rest, in Germany, the 27-30 age group is by far the best represented.

The fact that the youngest age groups are the least represented in this study could represent a limitation, as they are frequently the most exposed to online risks, due to their intense use of social media, combined with less experience in identifying and warding off potential danger, specific to teenagers.



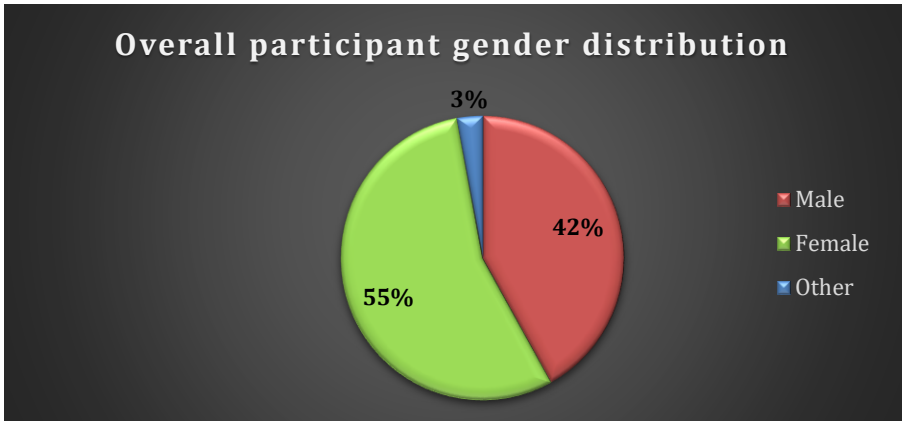
Participant gender



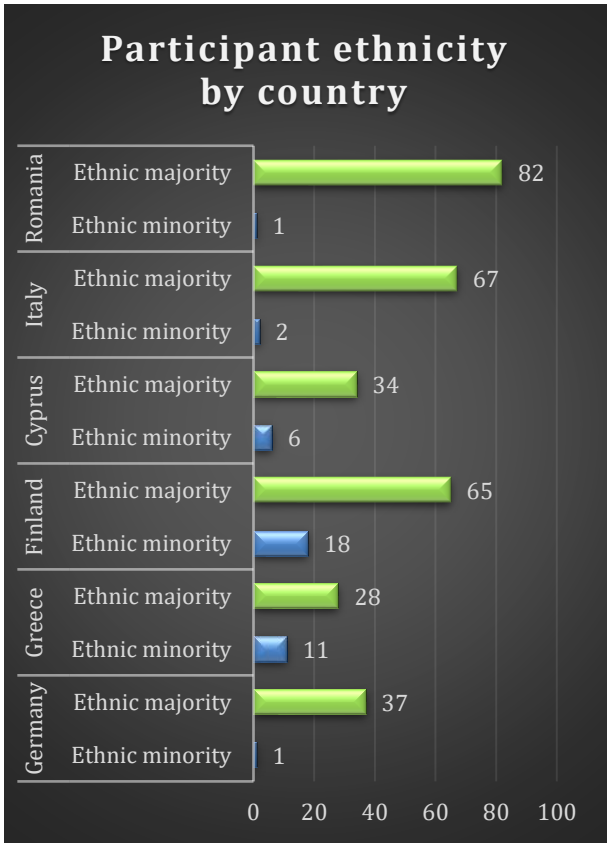
On an overall level, the gender ratio leans towards women, with 46 more female than male participants. This trend holds true for most of the individual countries as well, 5 of them revealing a female majority. Cyprus and Greece are the most balanced from this point of view, with 19 male to 20 female respondents, while Italy and Romania show significantly higher female participation.

When it comes to people of other genders, there are only very few participants in the entire research sample (10) who match this criterion, most of them from one country, which does not allow for significant correlations to be made. That is why, for the purpose of this analysis, when discussing participant gender, only “male” and “female” variables will be taken into account.

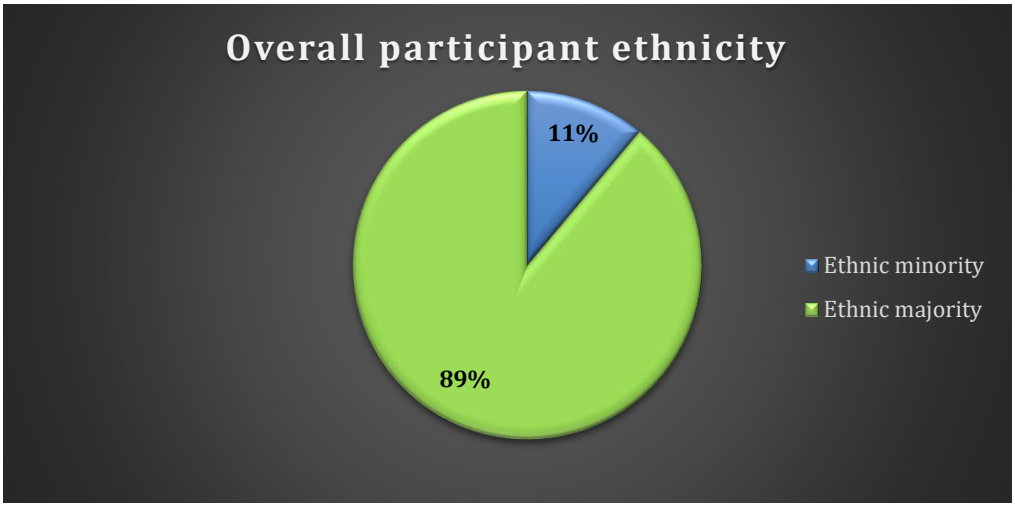
The gender distribution is important in the present analysis due to the fact that, as shown in the literature review, some online risks are gendered, such as women and girls being more frequently victims of revenge pornography, cyberstalking or cyberbullying.



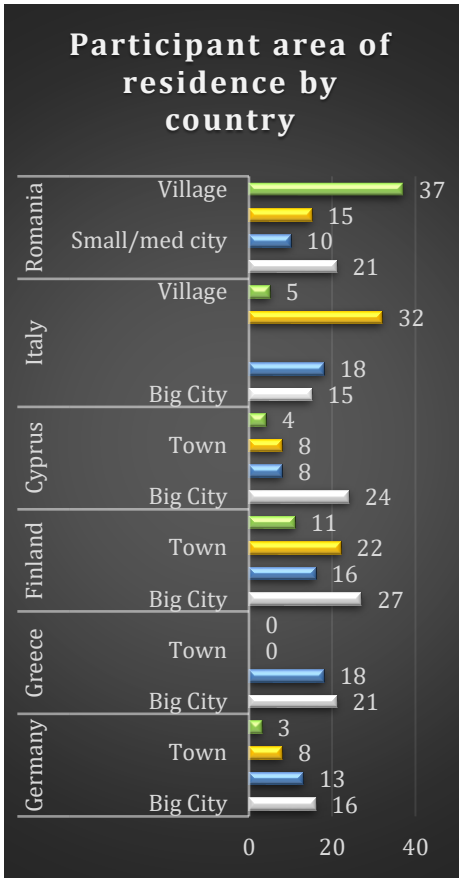
Participant ethnicity



Participants in this study belong to their respective national majority ethnic group in an overwhelming proportion (89%). Over 75% of ethnic minority respondents stem from Finland and Greece, while countries such as Romania, Italy and Germany each have only 1, respectively 2 minority participants in their samples. Taking into consideration the very small proportion of ethnic minorities in the research sample, as well as their diversity, which further fragments this number (each country has participants from different minority groups this variable will not be taken into account for the present study.

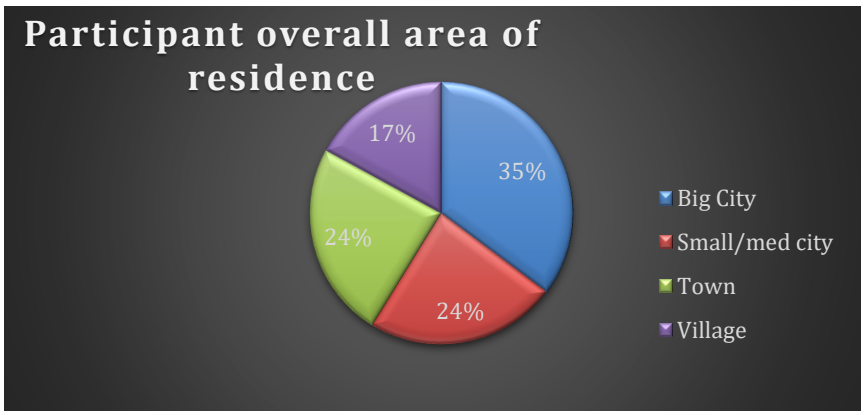


Participant area of residence

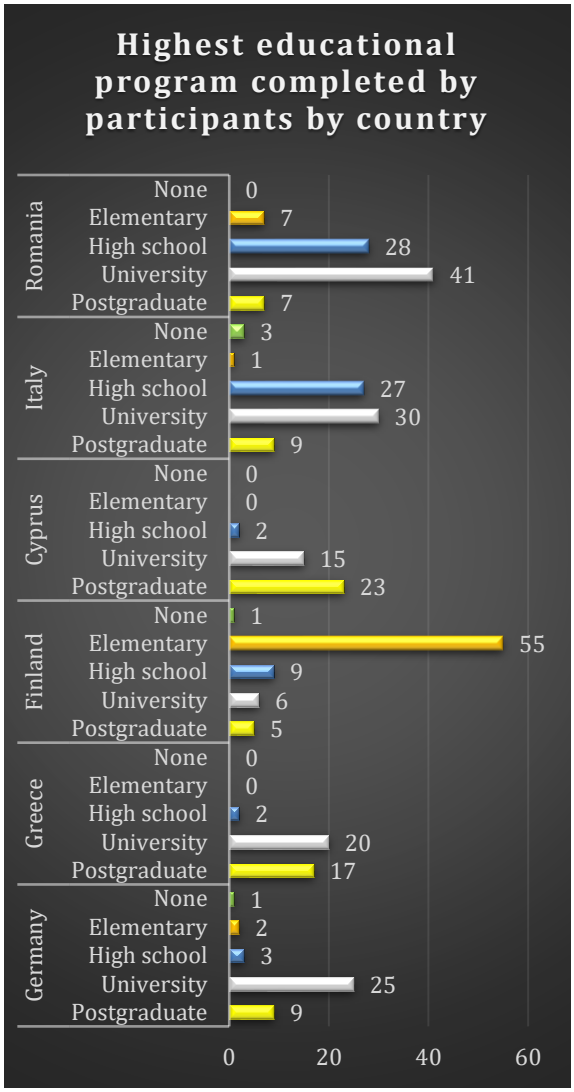


The overwhelming majority of participants live in an urban area (83%) and big cities are, overall, the most represented area of residence for respondents (35%). Respondents from big cities are the most numerous in Germany, Greece, Finland and Cyprus, while in Italy, town inhabitants hold first place. Only 17% of the people who filled in the survey live in a village, over half of them stemming from Romania (where they represent the most numerous category in the sample).

However, when correlating this information with respondents' online habits, there do not seem to be any major differences in the frequency of internet or social media use by area of residence.

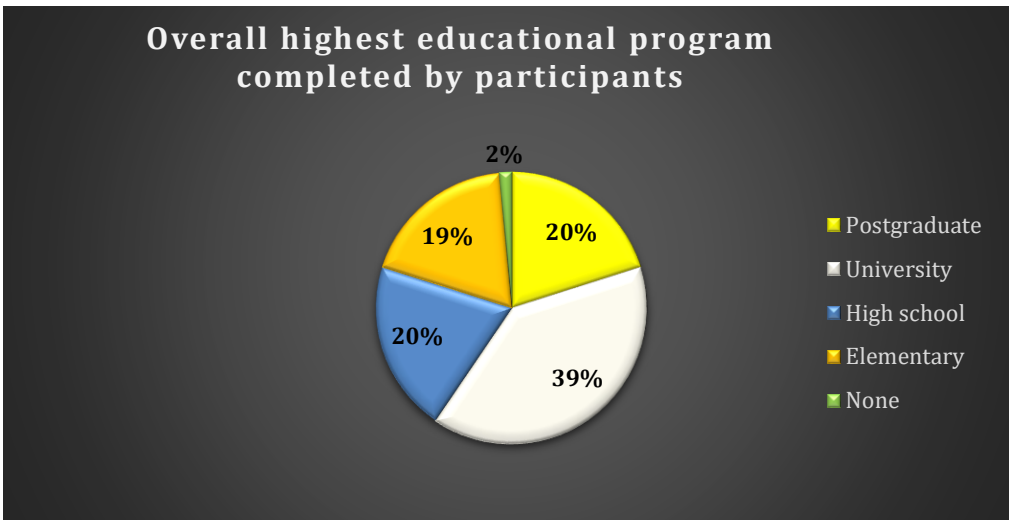


Participant level of education

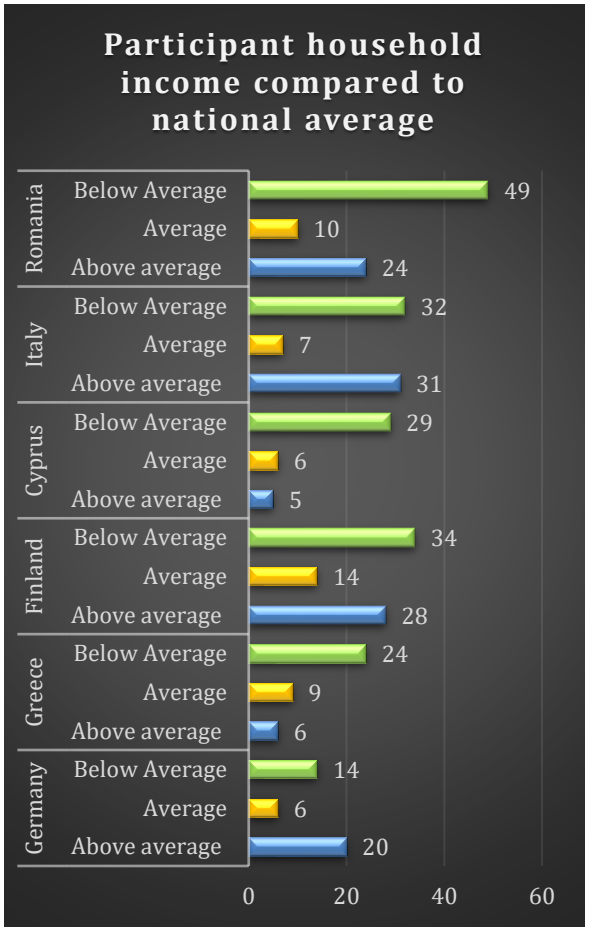


Almost 60% of respondents in the survey have completed higher education (39% of them are university graduates, while 20% are postgraduates). Only 19% of respondents have completed just elementary education or lower and another 20% have only graduated from high school. The great majority of elementary school graduates stem from Finland (84%), while Greece and Cyprus have none in this category (and Italy and Germany only have 1, respectively 2 each). This is likely due to the fact that Finland has a significantly higher number of young respondents (16-18 years old), who have not yet completed their education.

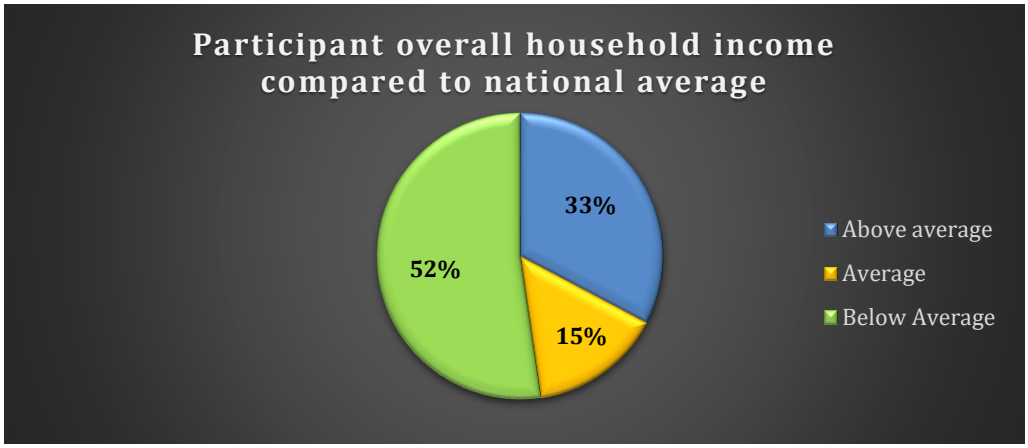
It must be kept in mind that having a mostly highly educated sample can lead to a lower rate of online incidents than the general population, as higher education is correlated to higher levels of critical thinking and cyber literacy, which can make it easier for them to avoid online risks and pitfalls.



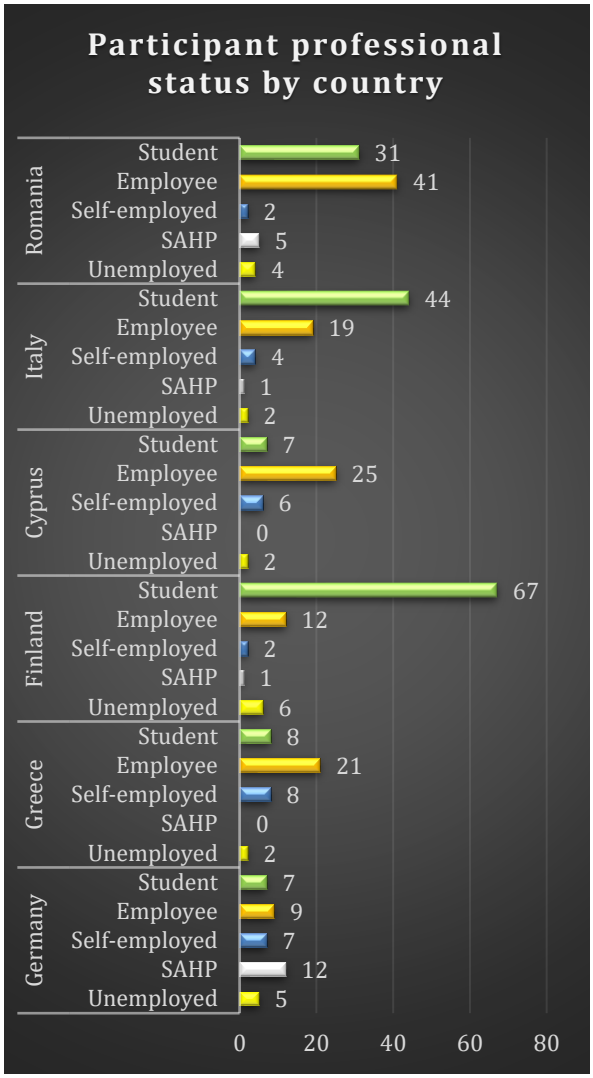
Participant level of household income, compared to the national average



Over half of the participants (52%) reported that during the first semester of the respective year, their household income was below the national average. Only 15% of respondents placed their income around the national average, while 33% answered that their household had accrued an above average income. This distribution is reflected, to various proportions, in 5 out of 6 countries, with the exception of Germany, where respondents with above average household income were slightly more numerous than those below the average. One potential explanation why, in spite of predominantly high levels of education and urban areas of residence, most of the participants' household income was lower than the national average is the large proportion of students in the sample, who are likely not to contribute to said income at this time.

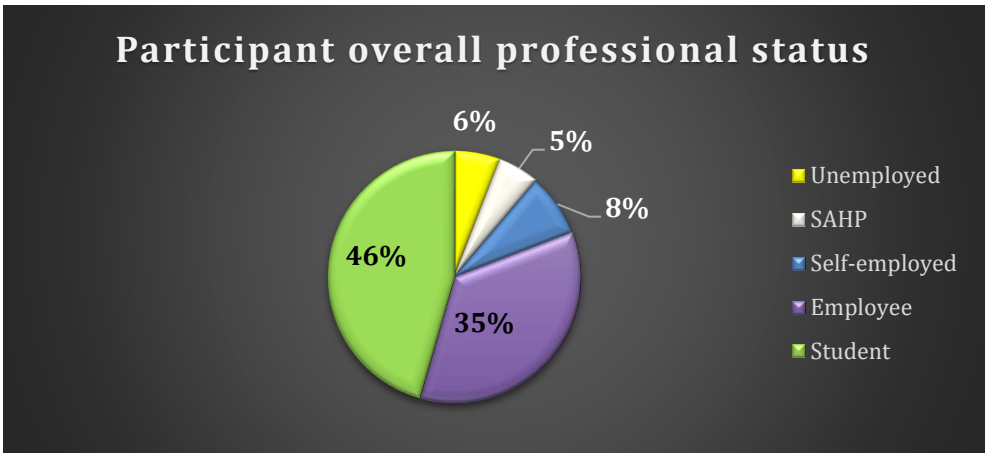


Participant professional status



The professional category with the overall highest number of respondents is students (46%), which is to be expected, given the fact that the present study targeted young people. Employees are a close second, with 35%, while the self-employed only make up 8% of the sample. Stay-at-home parents (SAHP) and unemployed participants are relatively few, making up 5%, respectively 6% of the total, not enough to influence research results in a considerable fashion.

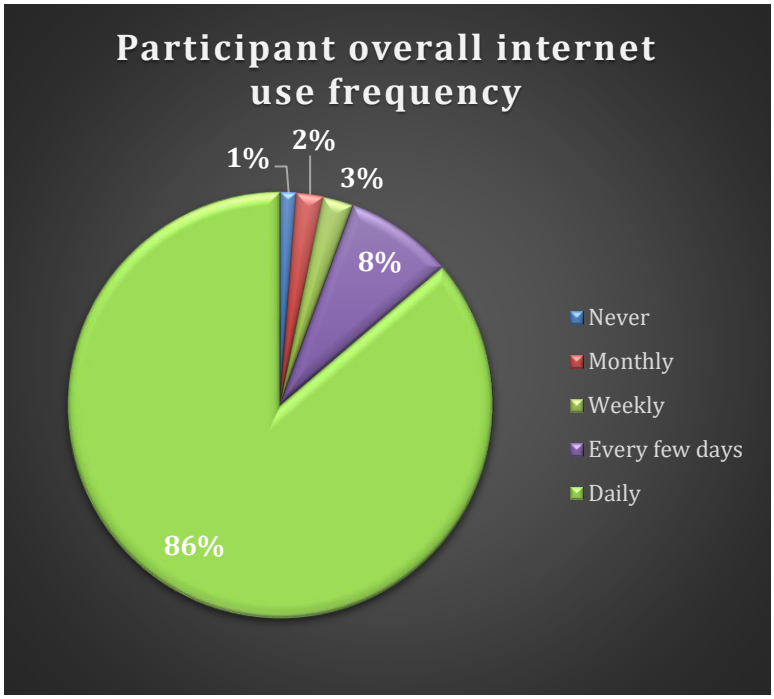
Finland registers the highest proportion of students, significantly more numerous than employees, likely due to the much younger age of their respondents, many of whom are likely still in high school. Students are also predominant in Italy, while employees are the most numerous in Romania, Cyprus and Greece. Stay-at-home parents are the largest professional category in Germany, which is likely to be due to the sample size effect.



2. Participants' online habits

In order to gain an understanding of the online risks that participants are exposed to, it is necessary to first understand their online behavior: how often and for how long they use the internet, what kind of platforms they access, how well they protect their personal information, etc.

Overall participant internet use frequency



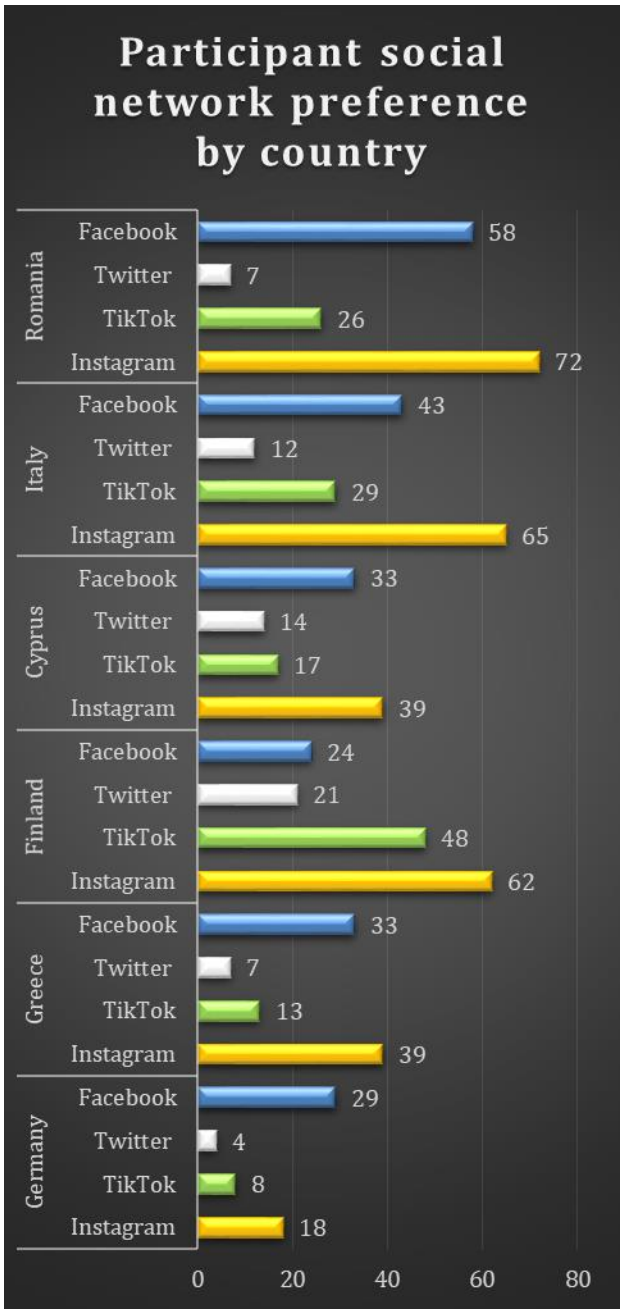
An overwhelming majority of participants (86%) access the internet daily. This category is the most numerous in 5/6 countries (Germany being the outlier, where only 4 respondents who access the internet daily, most going online every few days - likely also due to the sample size effect). All participants from Italy and almost all from Romania, Cyprus, Finland and Greece log in to the World Wide Web each day. Respondents who access the internet every few days make up 8% of the research sample, while those who do so less frequently only amount to 6%. Provided that this study was conducted online, on a voluntary basis, it must be kept in mind that there is also a self-selection effect, where people who spend more time online are more likely to come across on online survey and fill it in than those who do not access the internet frequently.

Since the amount of time spent online correlates with the chances of experiencing negative online events (e.g. cyberbullying, cyberstalking, etc.), a sample where the great majority of participants access the internet frequently increases the likelihood that they have been exposed to online risks, which can act as a mitigating factor for the small sample size.

Qualitative data obtained from interviews with youth workers confirms that young people spend an increasingly high amount of time on the internet, especially on their mobile devices. This was particularly true given the fact that the present data was collected in a pandemic context, where lockdowns and social distancing forced youths to have the bulk of their interactions and communication in the online environment rather than face to face. Key

informants tend to agree that young people's main online activity involves perusing social media: "*Young people use a lot of social media, less these days Facebook, TikTok and the like quite a lot, [taking] pictures from different places where they are and posting them on Facebook and Instagram. Probably a quarter of the youth's time. That's a lot of internet usage*" (Film and theater director, Finland).

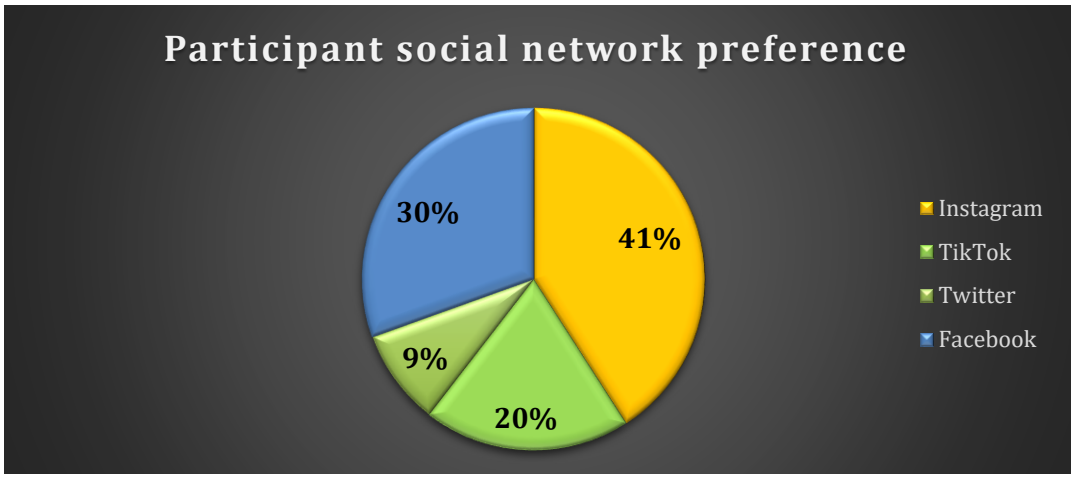
3. Participants' preferred social media platforms



Instagram (41%) and Facebook (30%) make up the majority of social media platforms favored by respondents, followed by TikTok (20%) and Twitter (9%). Participants from all countries except for Germany (who prefer Facebook) use Instagram the most. Facebook is the second choice for young people in most countries, with the exception of Finland, where TikTok comes second, likely due to the younger age of the respondents. Twitter is universally the least popular choice.

The type of social media platform participants use regularly can influence the types of online risk they are most exposed to. Instagram, for example, is mostly focused on photos and is popular with most young audiences, Facebook is focused on a combination of text, links and images, with less focus on video and caters more to older age groups. Tik Tok is short video-based and represents a staple for younger users, while Twitter is mostly text and link focused (though images and videos can be shared as well) and is more popular with an older, more news-focused public. Social media platforms based more heavily on users sharing photographs and videos can expose them to a higher risk of cyberbullying, cyberstalking,

impersonation, exposure to unwanted graphic or sexual imagery, as they allow users to expose more of themselves to public view.



Data from the interviews with youth workers and trainers in several countries shows that even though most young people use the same trendy social media sites listed above, there are also some age-related patterns in the way they use them. Thus, teenagers who are still in high school tend to use these platforms primarily for entertainment and for making new social connections. They are more eager to meet new people and more trusting in relation to them, which places them at higher risk for falling victim to online abuse. Young adults in older age groups - such as university students and employees - tend to use social media more for maintaining their existing connections with people they have met offline ("*I have observed differences, in adolescence online behavior also has a purpose of knowledge, of creating new contacts, new ways of getting to know people while for the older ones it has an entertainment function with people already known, less exploratory*" (psychologist, Italy)

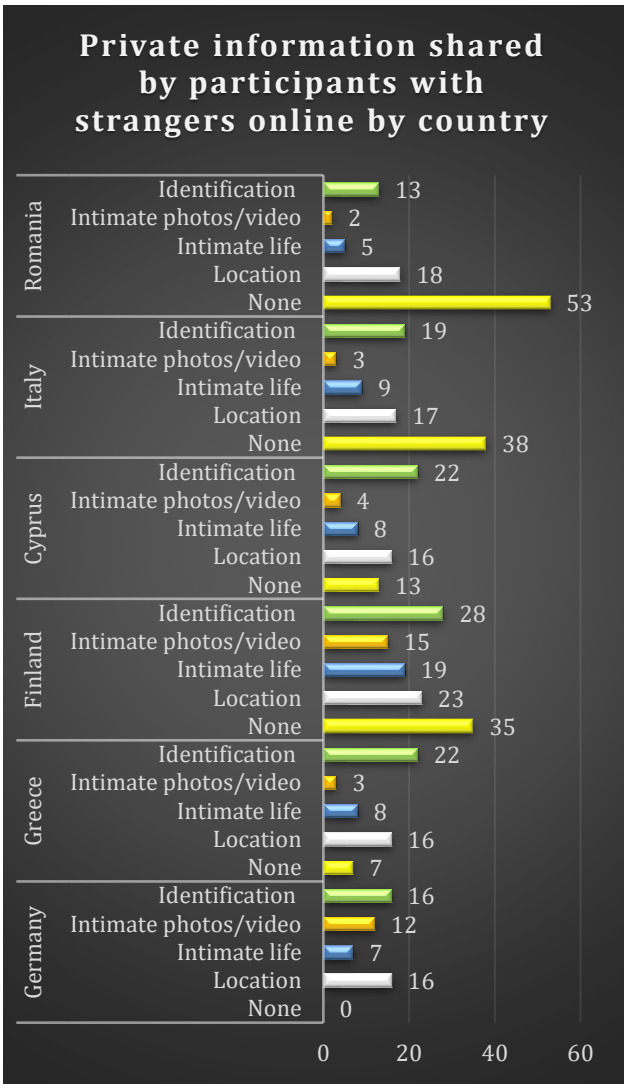
Older users also use online resources more to inform themselves regarding world events, to educate themselves or to develop their professional skills ("*In principle, teenagers are only interested in social media and online games. The older ones use the internet as a work instrument: for information, connection, e-mails, etc*. - youth worker, Romania).

Participants' engagement with other users on social media

The great majority of respondents in most countries communicate daily with other users on social media, both publicly, via comments and privately, using direct messaging. The only exception to this is Germany, where most participants only communicate with others via private chats less than monthly - this result can likely be attributed to the sampling effect. This level of engagement shows that the respondents are highly interconnected with other users,

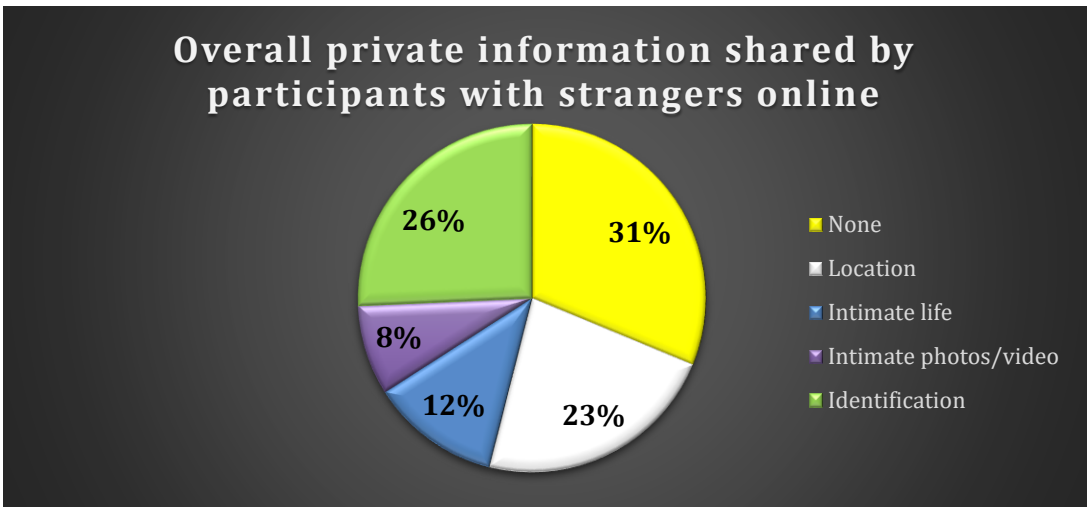
including strangers and that they share information and personal opinions both publicly and privately. This creates more opportunities for them to have adverse online experiences, such as being subjected to cyberbullying, cyberstalking or doxxing, but also increases the risk of being exposed to fake news shared by their online connections. While public conversations provide access to a higher number of users from the respondents' virtual space and the information they choose to reveal, private ones are unmoderated and offer an illusion of intimacy, making it easier to share personal/intimate content or to be targeted with cyber harassment or abuse.

4. Participants' risky online behavior



Of course, simply accessing social media does not automatically place one at risk of becoming a cyber victim. However, sharing private information with strangers online increases chances for adverse online experiences to happen. And most of the participants (69%) in our sample have shared at least one kind of private information with online-only friends/ acquaintances. The information most frequently shared pertains to identification (name, ID number, etc. - 26%), followed by location data (home address, etc.- 23%). While these may seem like the most innocuous details to be shared with strangers online, they can expose young people to cyberbullying, cyberstalking, online impersonation, outing/doxxing and even identity theft. 12% of respondents have shared personal or intimate details with strangers online, while 8% have shared intimate photos of videos.

Sharing personal information with people they have only met online

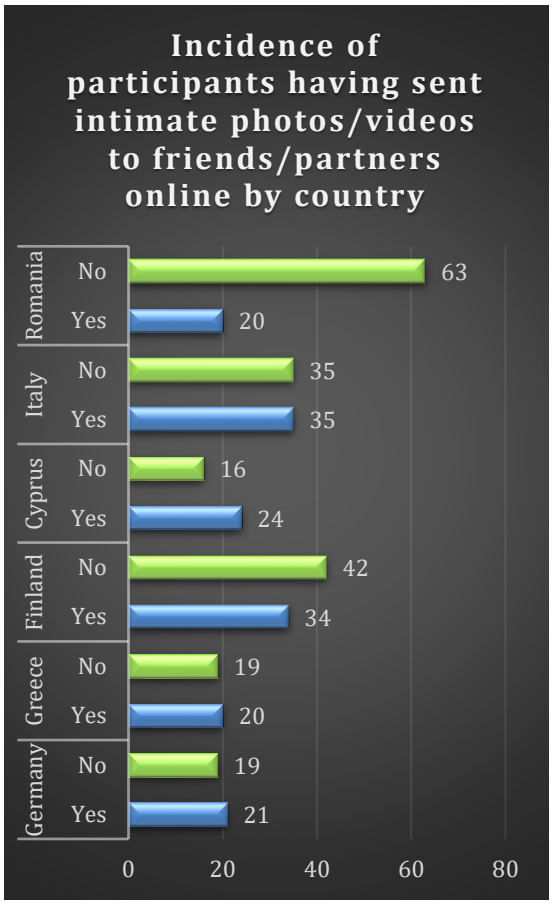


Interviewed youth workers agree that the main reason why young people engage in revealing personal information about themselves to strangers is that for them, online interaction can feel as real as face-to-face bonding. This makes them - especially the younger ones - very open and trusting towards online connections, whom they consider akin to offline friends ("*There is not a clear distinction between virtual and real world. It is an extension of reality, so you feel you are part of the community. They don't know that there is a risk of people using their personal data, or phishing, or stealing their personal data. Especially for teenagers, it is an extension of their reality, so if they have a community that they feel safe in, they share their data*." - teacher, Cyprus). In order to foster these connections, they reveal details about themselves as carelessly as they would to any friend. Most states covered in this study (except Germany and Finland) do not have significant educational programmes to teach young people about the danger of oversharing information with someone whom they have never met face to face and whose identity they cannot be certain of. This leads to many young people being unaware of the risks they are exposing themselves to. Moreover, being behind a screen makes them feel safer and more prone to revealing things about themselves that they normally might not. However, youth workers in Germany and Finland are hopeful as they found students are becoming increasingly risk - aware, possibly also due to the fact that these countries have added internet safety classes to their curriculums:

"*Though, I think they are eager to share information, such as their location, I believe that they are more careful in sharing data such as ID number or other, which can be used in scams. They are not a little bit technophobic, I just feel they are risk-conscious". (non-formal educator*, Germany)

"*I think that younger users share [such information], but older people have learned through their own experiences to beware of excessive openness and sharing of personal things. (social worker*, Finland)"

Sharing intimate photographs or videos online



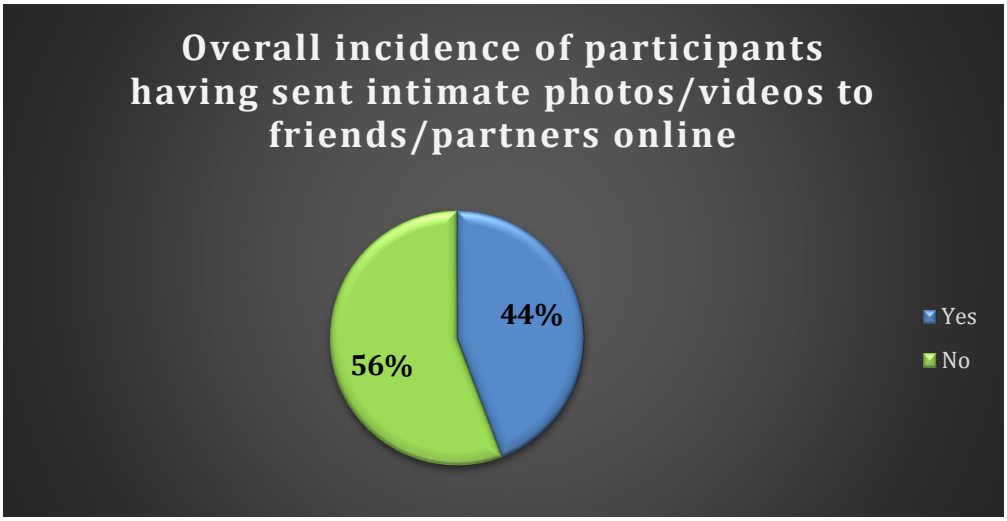
While only a few respondents (8%) shared intimate photos or videos with strangers online, considerably more (44%) have shared them online with real-life friends or partners. The sharing of intimate photos or videos can be especially perilous, as it exposes the sender to the risk of having their private media content distributed without permission and to revenge porn.

The experts interviewed raise an alarm signal that the sending of sexual multimedia content of oneself is an increasingly frequent, highly risky and gendered practice. They point out that there is a growing pressure on girls and young women to provide their male partners with photographs or videos of them in the nude, in sexual poses or engaging in sexual acts. Part of this pressure comes from their partners, who are looking for quick sexual gratification, as well as "proof" of their girlfriend's love and trust . Another part comes from the peer group, where this practice has become mainstream and socially acceptable (via influencers, pop culture, etc.) and girls who refuse to engage in it can be seen as challenging the morality of their female friends who do.

"*I think peer pressure is an issue to share for example nude pictures. In the romantic relationships especially girls feel obliged or experience a certain pressure to share more personal photos in order to be accepted or cool, usually by their boyfriends or by their male friends. It is a gender issue mostly.*" (non-formal educator, Cyprus)

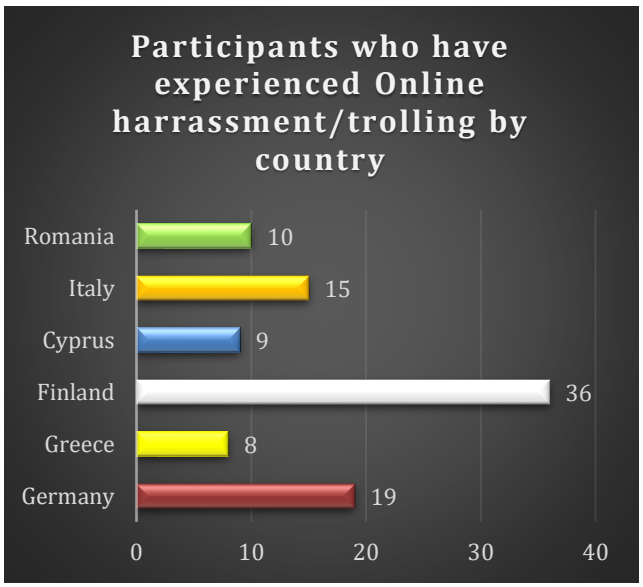
"*Solicited pictures are generally requested by boys and sent by girls. It is generally done among intimate partners or people who share a common interest. But there are also men who*

ask girls [for nudes] without there being any relationship between them. I think most girls (60%-70%) have sent such photos at least once: photos where the girl is naked or sexually explicit images" (student rights activist, Romania)



5. Online adverse experiences encountered by participants

Online Harassment/trolling (Cyberbullying)



Out of the forms of online adverse events experienced by respondents, cyber harassment (in all its forms - trolling, cyberbullying, flaming, etc.) was by far the most prevalent in our sample. experiences by 97 of all respondents (28%). That is because it is also the easiest to perpetrate, especially under the cover of anonymity. All that is needed is a user account on social media and the desire to embarrass, trigger or hurt another person.

While, in absolute number of incidents, Finnish participants have been victims of online harassment the most, in terms of percentage, German respondents have equally experienced this kind of incidents (47.5%).

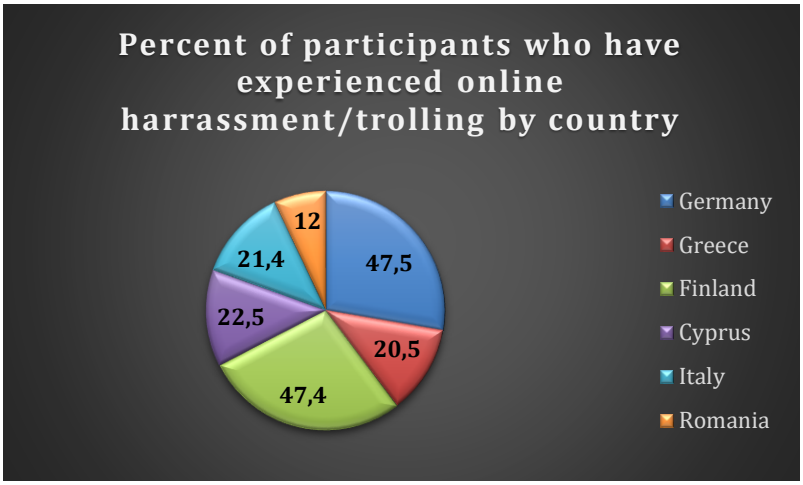
When it comes to the lowest incidence rate, Romanians were the least affected by online harassment out of all 6 studied countries, with only 10 incidents/83 participants (12%). One

possible explanation for this may be the fact that Romanian participants had the lowest rate of risky online behaviors (only 34% of the sample engaged in such behaviors).

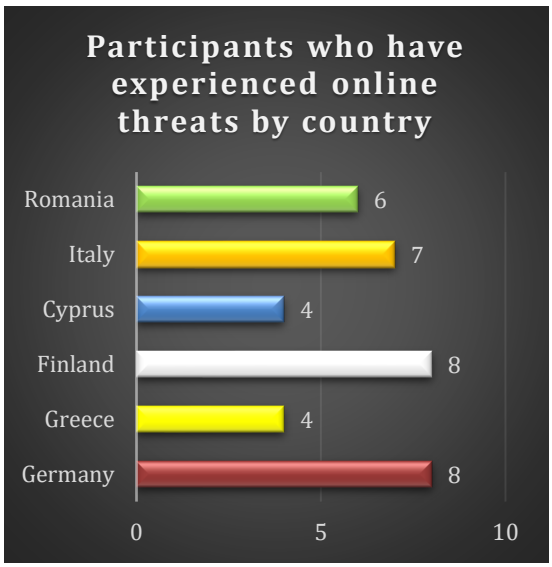
Qualitative data from interviews confirms that online harassment is widespread among young people, often underreported to f public authorities and accepted as part of online life.
"*I would say that incidents of bullying and online aggression happen daily. I look at their profiles and see the comments*." (Youth worker, Romania)

"*There is no exact data, but I would estimate that about 30 percent of young people fall into that group that has been bullied and harassed and so on*." (Social worker, Finland)

However, experts working with young people raise an alarm signal that cyberbullying, along with other online risks faced by the youth, can have severe consequences on their mental health.

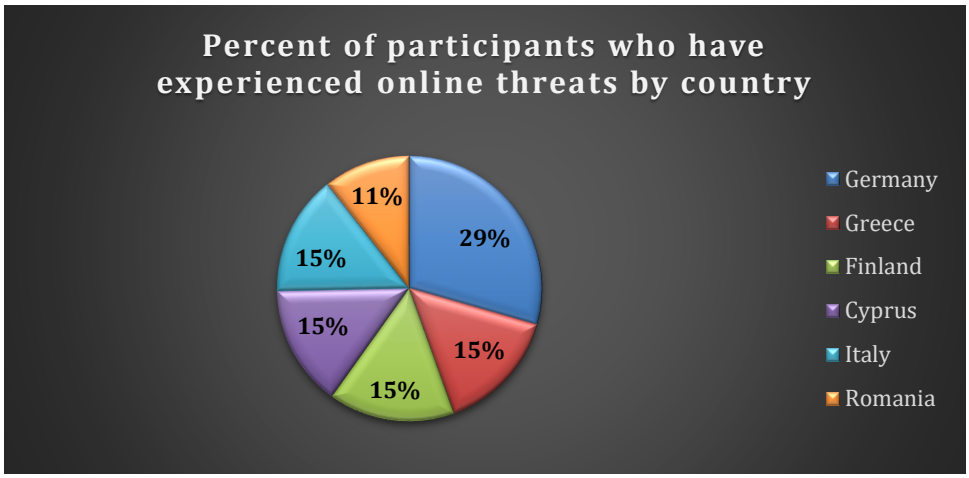


Online Threats

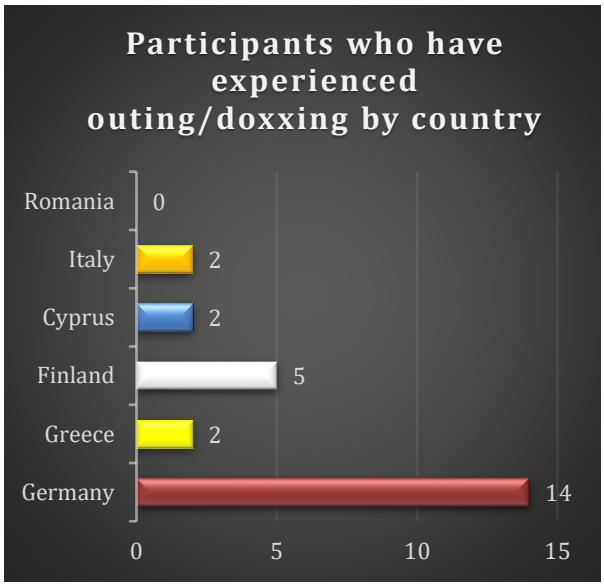


While receiving threats in an online environment may seem less frightening than face to face, that is not always the case. As many perpetrators hide behind usernames and avatars or fake social media profiles, it can be difficult to identify the author and to assess the credibility of the online threat, so fear of the unknown can compound with the victims' fear of the threat itself. While respondents from most participant countries have reported a similar number of online threat incidents (6-8), when looking at the data

percentually, in relation to sample size, German participants have the highest incidence rate - 20% - double or more than that of the other states. Cyprus, Finland and Italy have an approximately 10% rate of online harassment, while Romania's incidence remains the lowest, at 7%.



Outing/Doxxing

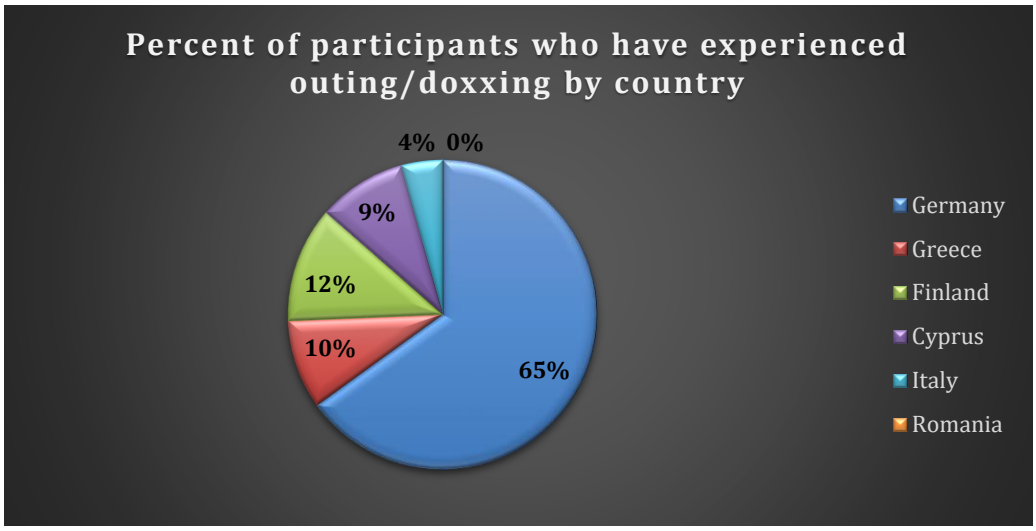


Outing or doxxing someone online can be not only embarrassing and isolating, it can be downright dangerous. That is because it frequently entails the revealing of private information, such as the victim's home address, telephone number or place of employment to the general public, often accompanied by instigations for others to harass them.

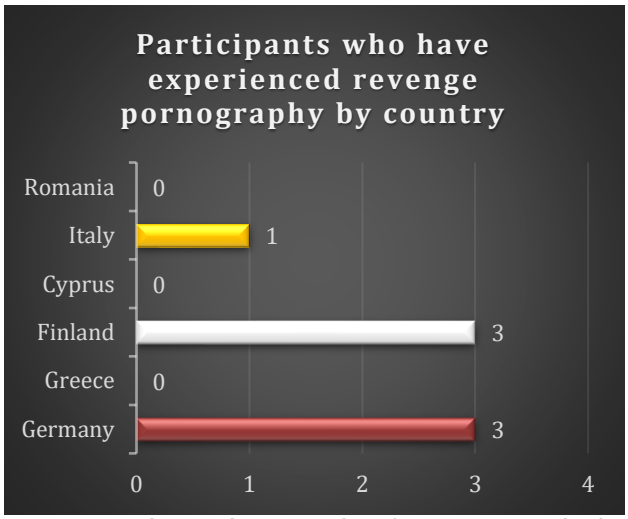
Fortunately, there were relatively few (25) incidents of outing/doxxing in the overall sample of this study, outing/doxxing being the online risk with the second-smallest frequency. Only 2 participants each from Italy, Greece, respectively Cyprus, 5 from Finland and none from Romania have been victims to this form of online abuse. However, Germany once more registers the highest incidence rate, with 14 cases (35% of the sample, 7 times more than the next country).

Just like online harassment and online threats, outing/doxxing has been recognized by interviewed youth workers as a major source of damage to young people's psychological well-being, generating feelings of anxiety, fear, poor self-image and more:

"*Trolling, online threats and doxing have essential effects on persons' psychological health. Low self-esteem, disturbed sleep, and high level of anxiety are some of the most common cases.*" (Teacher, Germany)



Revenge pornography and unwanted sexual content



Revenge pornography is one of the most devastating experiences that one could have online, as it involves the public sharing of their most intimate photos and videos, making it bone fide sexual victimization. This sort of experience has destroyed lives to the extent where it has been known to cause suicides among young victims. Fortunately, it has only happened to very few participants in our overall sample (2%, or 7 cases in total, stemming from 3 countries). Thus, 3 people in Germany, 3 in Finland and 1 in Italy have been targeted by revenge pornography.

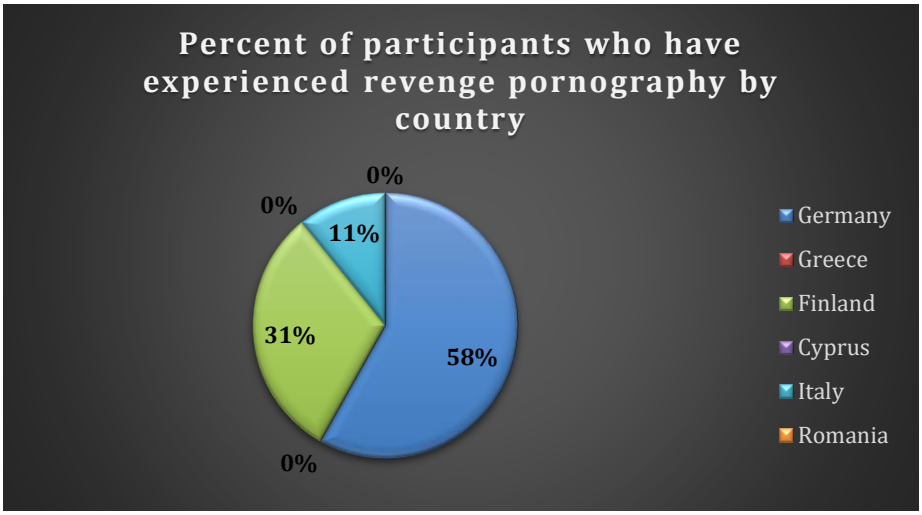
Since it is still a rare (but increasingly frequent) occurrence, most youth workers interviewed have not had personal experiences with cases of revenge pornography. However, they are aware of the existence and gravity of such cases and highlight the fact that young people have insufficient information regarding the appropriate handling of intimate content, its dangers and its legal implications. Additionally, shame and guilt often prevent victims from seeking help and justice:

"*Often times, young people who engage in revenge porn are not aware that they are committing a crime. Youth continue to message each other - sexting, photos and other erotic content. A significant part of this content has become revenge porn. Many girls have said that the source of this content is their former partners. […] often times, they do not discuss boundaries with their partners, but blindly trust them. [...] Most times, revenge porn starts from within an intimate relationship. Then it snowballs and gets on online groups which are specialized in this kind of content. These groups actively encourage users to send this type of content.*". (Student rights activist, Romania)

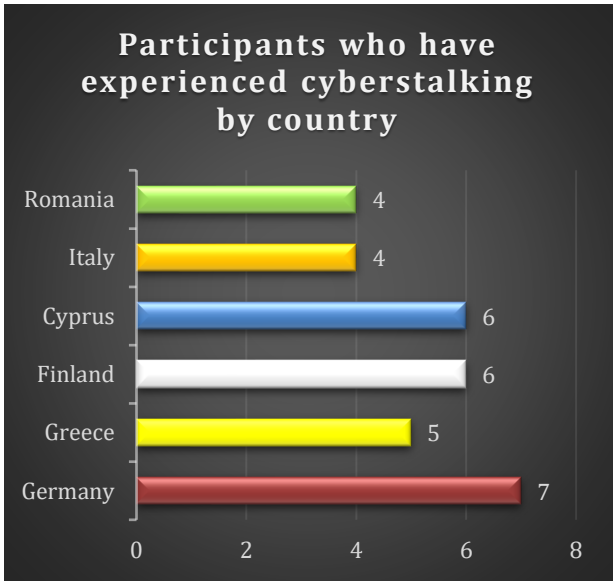
While young men are at far lower risk of having their intimate multimedia content shared for revenge porn (and would suffer less severe social consequences if that were to happen), according to the qualitative data, they are less inclined to send such content to their partners ("*Boys send intimate photos of themselves as well, but I don't think the risk is as high for them: For girls, it's more embarrassing.*" - vocational counsellor, Romania).

However, revenge pornography is not the only danger related to sexual imagery in the online environment. As young people become more and more interconnected and getting to know each other online, in a private, often unsupervised space is becoming the norm, receiving unwanted sexual content - from strangers or friends - has also become increasingly frequent. Young men are sending more and more unrequested photos of their sexual organs (dick pics) to their crushes, colleagues or random women they do not know, in hopes of eliciting a response. This is a form of online sexual harassment which is hard for young women to protect themselves from, as anyone who has access to their inbox, private messages or telephone number can send them such imagery and they would have to view it before being able to block the abuser, since social messaging apps do not censor contents of direct messages:

"*I think the receiving of unsolicited photos is important as well. I don't know any girl my age who has never received an unsolicited photo of a male genital organ from a stranger on Insta or Facebook. There are even some people who send viruses with that. There are also cases where people you know (men) send such unsolicited pictures, but not as often.*" (student rights activist, Romania)

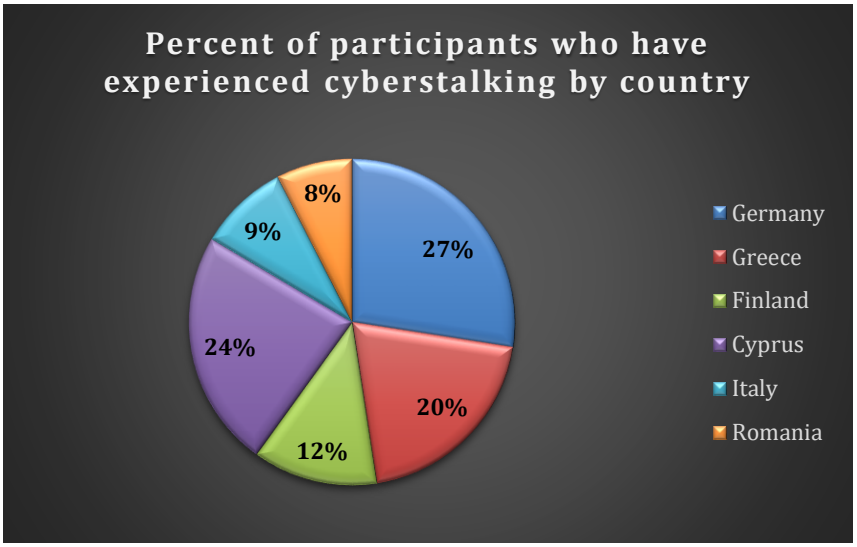


Cyberstalking

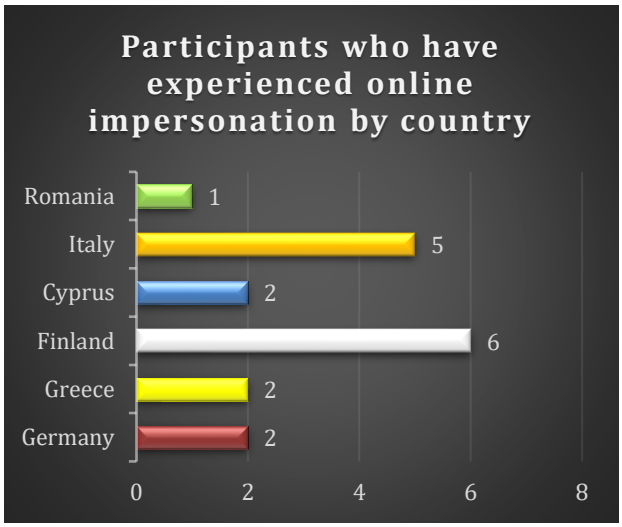


Usually accompanied by online threats or harassment, cyberstalking can be unnerving, as the victim can be stalked on a variety of social media by a perpetrator who hides behind a number of fake accounts. This can instill a sense of fear and ultimately force the victim to retire from online presence completely.

Cyberstalking is one of the more common incidents experienced by young people from our research sample. Cyprus and Finland each reported 6 cases among their respondents, Greece reported 5, Italy and Romania each reported 4, while Germany once more holds the lead with 7 incidents (18%, percentually close to Cyprus' 15% and more than triple Romania's 5%).

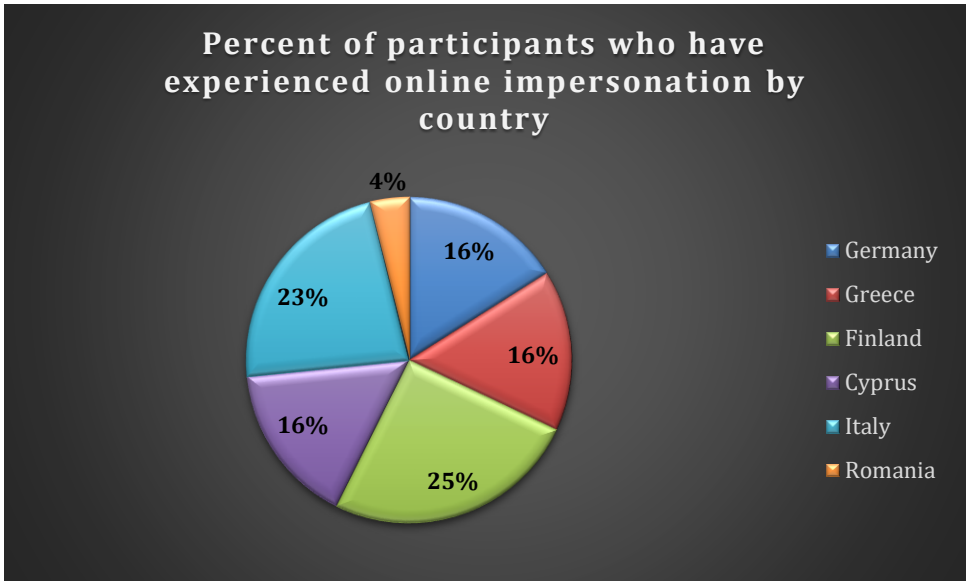


Online impersonation

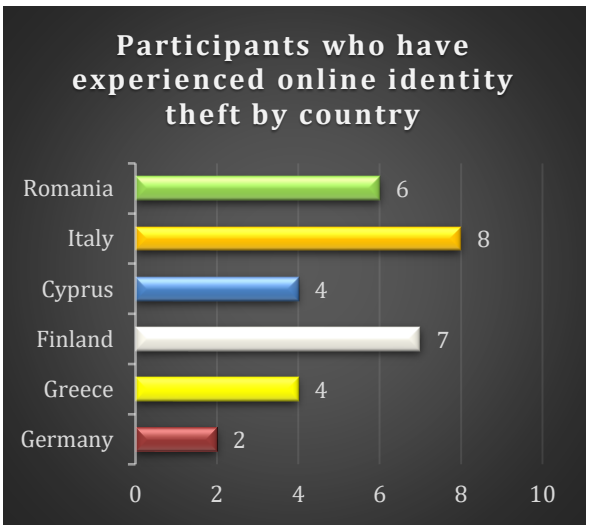


With the widespread use of social media and the abundance of information that young users are willing to share about themselves (photos, personal data, location, etc.), creating a fake profile and pretending to be someone else has become very easy. This does not only constitute an inconvenience for the victim, who can incur significant reputational and relationship damage if the perpetrator impersonates them to cause embarrassment or actual harm, but it is also dangerous for the victim's other online friends, who can be tricked into sharing private/compromising information with the impersonator.

Respondents from Finland and Italy seem to have been most frequently victims of online impersonation (6, respectively 7 cases, representing 7%, respectively 8% of the sample). Only 2 participants each from Germany, Greece and Cyprus and 1 Romanian have experienced such incidents.

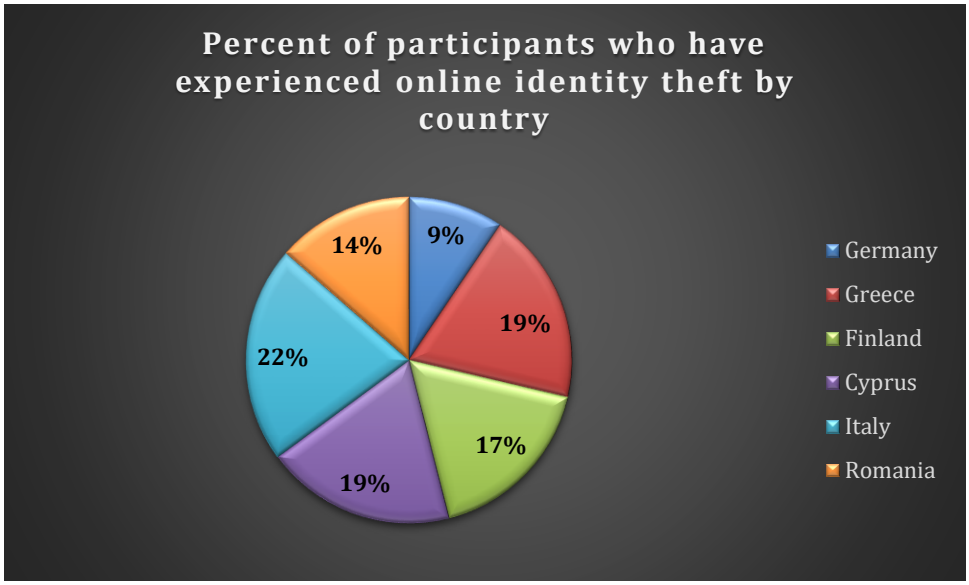


Online identity theft

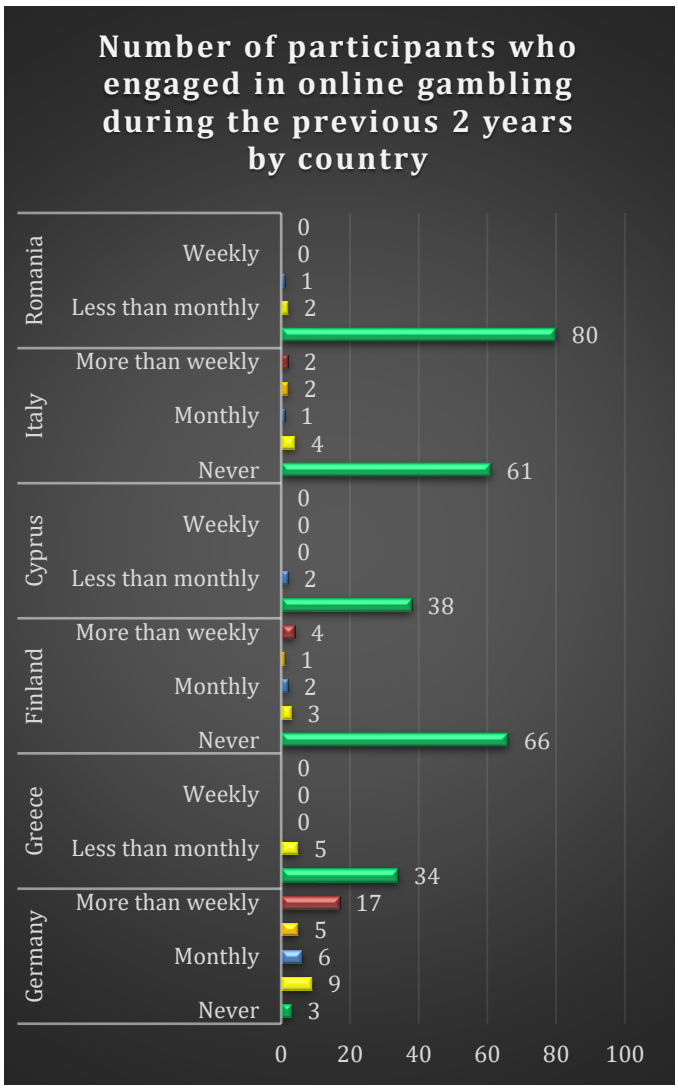


Since identity theft is recognized world-wide as a serious crime, one might expect its rates to be lower. However, the online environment makes it easy to trick young users out of their personal and particularly financial information. Phishing methods have perfected during the past years, as it is becoming increasingly difficult to tell apart a safe link or software from a malicious one.

Participants from Italy, Finland and Romania have reported similar frequencies in online identity theft (6-8 cases). However, percentually speaking, Italy and Cyprus register the highest rates, representing 11%, respectively 10% of their respective sample). Romania and Germany reveal the lowest incidence - 7%, respectively 5%.



Online gambling

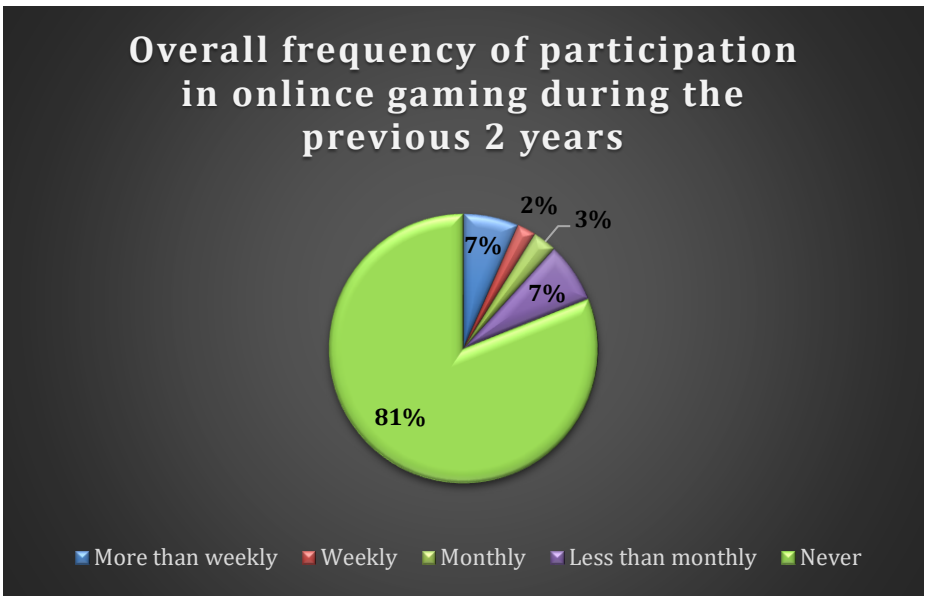


Just like any other form of gambling, the online variety is very dangerous for young people, as it can cause severe addiction. It can lead to important financial losses, which in turn can cause debt, place strain on family relationships and ultimately generate other associated mental health issues, such as anxiety, depression, low self-esteem, even suicidal ideation or attempts. Unlike the case of traditional gambling, however, in many of the studied countries, the legislation regarding advertising for online gambling is more relaxed, making it easier for young people to access this kind of games. Furthermore, new forms of online gambling, not yet universally recognized as such - like loot boxes which can be bought in certain video games - can act as a gateway to getting children and young adults addicted early on in life.

Fortunately, the great majority of overall participants (81%) have never engaged in online gambling. Out of those who have, 10% have only done so monthly (3%) or less than once a month (7%). This means that only 9% of respondents from all countries can be considered problematic gamblers, engaging in this behavior weekly (2%) or more than once a week (7%).

Out of all the studied countries, Germany seems to be the most affected by online gambling, as it has the only sample where most of the participants have been gambling online more than once a week (17 out of the overall 25 respondents who did so are German). This has been explained by the interviewed local youth workers by the fact that there is a strong gambling tradition in this state, rooted in sports betting:

"In my experience I think that the entry point to gambling in Germany is related to sports. Young people are enthusiastic with group sports, such as football and basketball. Gambling is a mean to prove their skills and knowledge to find out which team wins. Combined with easy profit, young people are easily engaged in gambling. Online gambling is not accessible to under-aged young people, who do not have a credit or debit card, but honestly, for many I do not think that this is a real obstacle. Many parents lend them with their cards, thinking that they will buy something online. Not many parents, I think, are in position to check and control their children. For young people over 18, I think it is much easier to get engaged, especially during their student years." (non-formal educator, Germany)



At the other side of the spectrum, only very few respondents from countries like Romania (3/83), Cyprus (2/40) and Greece (5/39) have engaged in this kind of activity and almost all of them only did so less than once a month. There are several potential explanations for this, ranging from cultural negative attitudes towards gambling to the lower percentage of teenagers who have access to credit cards and sufficient funds to gamble online. The wide availability of traditional gambling opportunities (e.g. sports betting centers, casinos, slot machine arcades, etc.) can also contribute to the smaller appeal of engaging in such activities online, as they provide an opportunity to practice them socially, with friends.

Youth workers who have encountered this phenomenon warn that even where there are still low percentages of online gambling, there is an ascending trend, enabled by the legislative void related to this kind of activities, compared to their traditional variety, as well as by their highly addictive character:

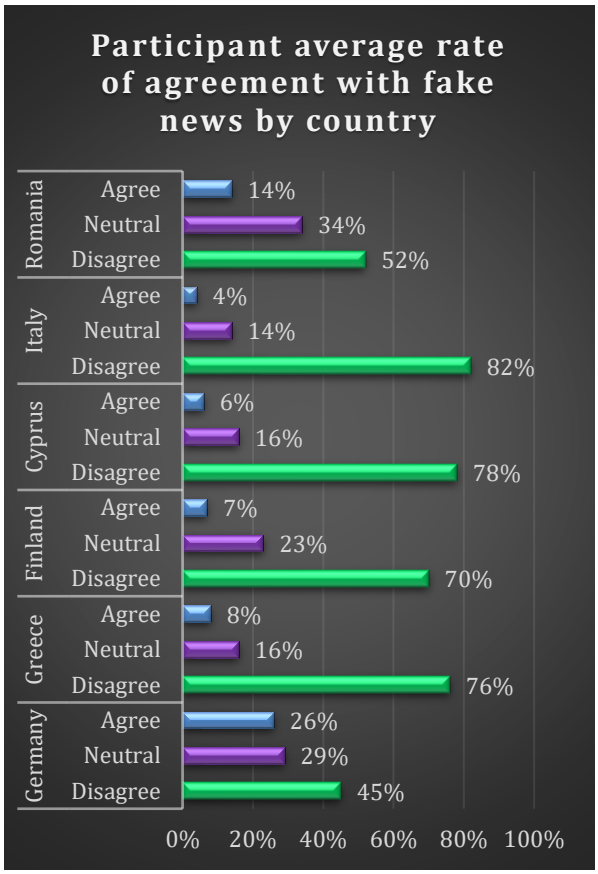
"*There is a phenomenon called the gamification of gambling. There is this juxtaposition of playing video games and gambling. The famous loot boxes have emerged - users pay to open a box in the virtual environment which can give them an advantage. This introduces betting to the under 18 category. Peer pressure emerges, because there are items in the game which can be obtained very easily with money or much harder by playing. This creates the social pressure of spending money in the virtual environment. Normally, gambling is not accessible to minors, but this kind is.*" (Psychologist specialized in online gambling, Romania)

Just like other online risks, this phenomenon is also heavily gendered, with young men being much more susceptible to it than young women. This often has to do with patriarchal values and beliefs, where men are expected to be providers, so they feel under added pressure to have financial possibilities, making them more susceptible to the prospect of easy gain. Also, men are much more likely to be interested in sports and thus in sports betting.

"I think this turns into addiction very quickly, especially in young people: they don't have steady and sufficient income, they often don't get enough money from their parents. Some may win in the beginning and be motivated by it. They also influence each other. I believe most of them are boys. Maybe also because they want to make money more, but also because they're passionate about different sports, they think much more pragmatically. I believe it's a real danger [...]. I believe young people are an important audience, targeted by the companies who make these apps." (Teacher, Romania)

Exposure to fake news

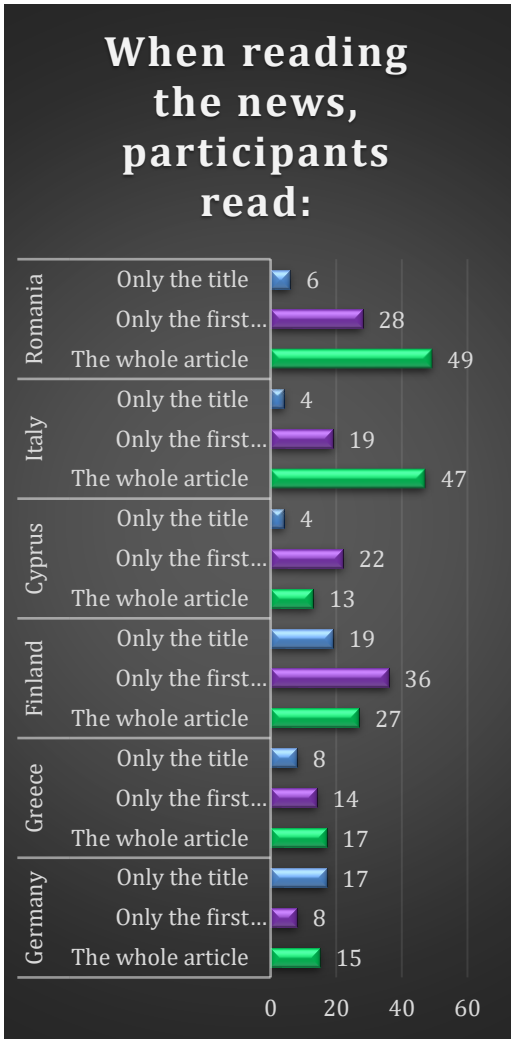
Fake news have been quite a buzzword in the past few years, especially in the context of the Covid-19 pandemic. While everyone knows they exist, determining what information is true and what is simply widely circulated fabrication has become one of the great challenges of the decade. Unlike the other online risks presented here, this phenomenon does not pose a direct threat in itself to young people. However, depending on the content of the misinformation, it can lead to both individual and social harm (e.g. by refusing hygienic practices such as mask wearing during a global pandemic).



In order to get some idea of how susceptible participants from the different countries included in this study are to believing fake news, they were asked to express their level of agreement with 5 false, but ideologically charged statements. Averages were then calculated, showing respondents' tendency to agree, disagree or remain neutral in relation to the misinformation.

Out of all countries, German participants were the most likely to believe fake news, as 26% of them agreed with the false statements, while only 45% disagreed with them. Romania came in second, with 14% agreement rate and 52% disagreement. Respondents from the other countries appeared to be the least susceptible to being misinformed online, as follows: Italy (4% agreement to 82% disagreement), Cyprus (6% agreement to 78% disagreement), Finland (7% agreement to 70% disagreement) and Greece (8% agreement to 76% disagreement).

Hypothetically speaking, these results should correlate with each country's critical reading score (calculated from the participants' ability to answer questions regarding a short text they were asked to read), as well as with their news reading thoroughness. In the case of the highest and lowest susceptibility to believing fake news, data shows this holds true. Thus, respondents from the German sample have the lowest critical reading score of all: -0.2 and most of them (62%) report only reading the title or the first paragraph of a news item. At the same time, Italian participants have the highest scores in critical reading (1.1) and they report reading news articles in their entirety in a higher percent than any of the other countries (67%). However, there are discrepancies between rates of agreement with fake news and the rest of the scorings in other countries, such as Romania. Although they are the second most likely to agree with fake news and least likely to disagree with it, they also have the second highest critical reading score (0.9) and also the second highest percentage of reading news articles in their entirety after Italy (almost 60%). An explanation for this may be that while they are equipped in reading and understanding news, respondents from some of the countries may be getting their news from sources they trust, but which propagate misinformation in accordance to their own agenda. For example, Romania is known for attacks on free press and for the political weaponization of the media, according to the Reporters Without Borders World Press Freedom Index (RSF, 2018). This means that young people might be equipped to read good quality news but their trust in media outlets which constantly publish fake narratives may prevent them from identifying misinformation, due to ideological motivations.



When it comes to youth workers' assessment of young people's media literacy and critical thinking, the factors which should dictate their ability to prevent being taken in by fake news, opinions greatly diverge even between experts from the same country. While some say young people are flooded with massive amounts of information and have no training or compass for discerning between what is true and what is false, others find youths significantly more online

media-savvy and more skeptical than adults and trust their abilities to prevent media manipulation:

This discrepancy is largely the result of the type of youth work our interviewed specialists did and what segment of young people they came in contact with: those who are constantly working with highly educated and motivated beneficiaries (e.g. music/art students, high achievers attending in self-improvement programmes, etc) are naturally more optimistic than those who are working with beneficiaries who have lower levels of education and belong to minority or underprivileged groups (e.g. social workers).

"*Given that the young people we work with have graduated 11 grades at most, we rarely have youths who have graduated 12 grades and have gotten their Baccalaureate, I don't believe they have a very profound critical thinking. And I blame this on them not having much education in this respect*" (vocational counsellor, Romania)

"My students have this capacity, even more so as they read original texts in English written by native speakers. But I don't know if this is true for all backgrounds." (teacher, Romania)

However, what most experts do agree upon is that fake news is a real threat, that people of all ages are bombarded with it on a daily basis and that young people, who are the most inexperienced and spend the most time online, are highly likely to be exposed to it.

"Young adults who are looking for their place in the world believe everything more easily - there is so much information on the internet and in the media that it is easy to grab such pleasant information for yourself. (child welfare worker, Finland)

"The main reason [for believing fake news] is that they use social media as the primary source of information. However, young people are usually not educated on how to deal with misinformation and how to identify the credibility of the authors, websites and social media accounts." (teacher, Germany)

V. Conclusions

The research has confirmed the fact that young people spend a significant amount of time surfing the internet and accessing online social networks. Youth online presence has increased during the Covid-19 pandemic and this trend has been maintained in its aftermath, as young people tend to be permanently connected to the internet on their phone. 86% of respondents reported accessing the internet daily, including all participants from four of the six countries surveyed (Romania, Cyprus, Finland and Greece). This significantly increases

the chances of young people becoming victims of online threats identified in the literature, namely fake news, cyberbullying, cyberstalking, online threats, identity thefts, image-based sexual abuse or online gambling.

Online social networks represent one of the main activities of young people on the internet. The most popular social platforms are Instagram (favored by 41% of respondents) and Facebook (favored by 30% of respondents), followed by TikTok and Twitter (9%). The type of social networks used by young people also influences the type of online risks that they are most likely to be exposed to, as some platforms focus more on images, other on texts and links or videos. Also, some platforms are most often used for sharing private information while others are more news-oriented.

In terms of internet behavior, teenagers who are still in high school primarily use social platforms for entertainment and for making new acquaintances, which makes them more likely to become victims of online abuse, while young adults are more likely to use social networks for keeping in contact with existing connections.

When it comes to online behavior, the majority of our sample (69%) has shared private information with online-only acquaintances at least once, most often identification information and location data, but also personal or intimate details or even intimate photos of videos. This opens the door for multiple online threats, such as cyberbullying, cyberstalking, online impersonation, outing/doxing, identity theft and revenge pornography. The main reasons for such risky behavior relate to young people's assimilation of online socializing to face-to-face bonging and their limited awareness about online risks, as well as the false sense of being protected by the screen.

While sharing intimate pictures with strangers is not very common, almost half of respondents (44%) have shared such content with real-life friends or partners. This practice is highly gendered, with women and girls experiencing a social pressure from their partners and peers to provide such content. Some youth workers estimate that as much as 60-70% of young women having sent such content at least once.

In terms of the manifestation of online risks, cyberbullying (in all different forms - trolling, cyberbullying, etc.) is the most commonly experienced type of incident, reported by 28% of young people. Online threats have also been reported by 20% of German respondents and 10% of participants from Cyprus, Finland and Italy. Such incidents can have severe consequences on youth mental health.

Incidents of identity theft ranged from 5% to 11% in the countries analyzed, cases of online impersonation were not very frequent in our research and most often reported by young people from Finland and Italy. Incidents of outing and doxxing as well as revenge pornography were also present but rarely reported.

Online gambling addiction is also not a widespread phenomenon as only 9% of young people from our research could be considered problematic gamblers (engaging in this activity at least once a week), with German participants being the most gambling-savy. This behavior is highly gendered, with young men being most at risk, due to their interest in sports and the social pressure to earn money.

According to the experts interviewed, despite the manifestation of some of these online risks being relatively limited, some risky behaviors – such as sending intimate pictures of online gambling – are on an ascending trend, enabled by legislative voids and young people's lack of awareness regarding the consequences. Potential consequences of such actions include significant psychological, social and/ or financial damage for the victim, as well as potential legal sanctions for the perpetrator.

Fake news and disinformation represent a real threat to young people, given that they spend a large amount of time online and that they lack experience. Not all variables that could affect young people's likelihood to believe in fake news could be tested in this research. However, critical reading abilities and the thoroughness in reading the news did play a significant role, as German respondents had the lowest critical reading score and they were also most likely to believe in fake news. However, this correlation did not necessarily hold true for the other countries, which clearly shows that there are also other factors which may influence the manifestation of this risk.

Also, it must be kept in mind that our research sample is not representative at the nation level and that some of the results presented above could be due the sampling effect.

VI. Recommendations:

Young people and young workers and trainers should be provided training and educational tools in order to avoid and mitigate the identified risks.

1. Capacity-building programs

Training sessions addressed to young people and youth workers and trainers should include thematic training sessions on sex education, gender equality, internet use, cybersecurity, soft skills and fact-checking.

The main topics to be addressed in training sessions addressed to youth trainers and workers are the following:

a) understanding social platforms and online risks for young people
b) identifying risky behavior online
c) creating a safe online environment/ network: tools and technical information about how to secure accounts
d) addressing youth vulnerability and disinformation: risk mitigation from a personal growth perspective
e) developing soft skills in youth
f) establishing the trainer-trainee relationship

Trainings targeting young people should address the following topics:

a) description and patterns of manifestation of the key risks identified;
b) how to build an online profile: the difference between online and real life
c) how to avoid becoming a victim of online harassment;
d) how to address hate speech online;
e) how to promote gender equality and prevent sexual harassment;
f) how to know whom they can trust online;
g) what information should and should not be sent or posted online;
h) how to address their own emotional needs in order to resist online risks (self-empowerment, self-esteem, self-awareness).

In terms of the methodology of these capacity-building programs, the following recommendations should be taken into account:

a) trainers/ facilitators should include participatory methods and non-formal education techniques (for example: simulations, role-play games, group work)
b) trainers/ facilitators should provide practical examples and real-life scenarios;
c) trainers/ facilitators should be empathic and encourage all participants to share their views and experiences, especially if they had any experience with online risks;

d) trainers/ facilitators should create a safe environment, in which all participants respect each other and are confident enough to speak their mind;

e) training sessions should address the potential victim and the aggressor differently;

f) when possible, such programs should include, as guest speakers, persons who experienced the manifestation of these risks or vloggers/ influencers whom young people look up to.

2. Online/ smartphone games

In order for an online/ smartphone game to be innovative, successful among young people as well as efficient in combating online risks, it should meet the following criteria:

a) address the identified risks individually, by using real-life scenarios that young people can relate to;

b) provide the players with the opportunity to make choices and present the outcome(s) of their choices, so that they can learn from their mistakes;

c) include a debriefing phase at the end of each scenario, in which the player finds out if he did the right thing or not and why, as well as how to do better next time;

d) include game levels and points in order to motivate players;

e) have an attractive graphic design;

f) be optimized for computers as well as for smartphones (the preferred devise for accessing the internet for young people);

g) include the possibility to share information about the game on social networks.

Also, the game should be tested by young people from different countries and different settings, and their feedback should be used for perfecting this online educational tool.

VII. Bibliography

1. Ansary, N.S. (2020) “Cyberbullying: Concepts, theories, and correlates informing evidence-based best practices for prevention,” Aggression and Violent Behavior, 50, p. 101343. Available at: https://doi.org/10.1016/j.avb.2019.101343.

2. Antoniadou, Nafsika, and Constantinos M. Kokkinos 2018. “Empathy in Traditional and Cyber Bullying/Victimization Involvement From Early to Middle Adolescence: A Cross Sectional Study.” Journal of Educational and Developmental Psychology 8 (1): 153. https://doi.org/10.5539/jedp.v8n1p153.

3. Antoniadou, Nafsika, and Constantinos M. Kokkinos. 2015. “A Review of Research on Cyber-Bullying in Greece.” International Journal of Adolescence and Youth 20 (2): 185–201. https://doi.org/10.1080/02673843.2013.778207.

4. Aslanidou, Sofia, and George Menexes. 2008. “Youth and the Internet: Uses and Practices in the Home.” Computers & Education 51 (3): 1375–91. https://doi.org/10.1016/j.compedu.2007.12.003.

5. Athanasiades, Christina, Anna Costanza Baldry, Theocharis Kamariotis, Marialena Kostouli, and Anastasia Psalti. 2016. “The ‘Net’ of the Internet: Risk Factors for Cyberbullying among Secondary-School Students in Greece.” *European Journal on Criminal Policy and Research* 22 (2): 301–17. https://doi.org/10.1007/s10610-016-9303-4.

6. Barkoukis, Vassilis, Lambros Lazuras, Despoina Ourda, and Haralambos Tsorbatzoudis. 2016. “Tackling Psychosocial Risk Factors for Adolescent Cyberbullying: Evidence from a School-Based Intervention: A School-Based Intervention Against Cyberbullying.” Aggressive Behavior 42 (2): 114–22. https://doi.org/10.1002/ab.21625.

7. Commissione parlamentare per l’infanzia e l’adolescenza (2019) “Indagine conoscitiva su bullismo e cyberbullismo”, Roma.

8. Donato, Vese "Governing fake news: the regulation of social media and the right to freedom of expression in the era of emergency." European Journal of Risk regulation 13.3 (2022): 477-513.

9. Ebrand. 2022. Some ja nuoret -katsaus. https://www.ebrand.fi/some-ja-nuoret/, [Accessed September 2022]

10. European Commission: Tackling online disinformation https://digital-strategy.ec.europa.eu/en/policies/online-disinformation [Accessed September 2022],

11. Gaffney, H. et al. (2019) “Are cyberbullying intervention and prevention programs effective? A systematic and meta-analytical review,” Aggression and Violent Behavior, 45, pp. 134–153. Available at: https://doi.org/10.1016/j.avb.2018.07.002.

12. Government Decision No 592/2021 approving the National Strategy for Preventing and Combating Sexual Violence "SYNERGY" 2021-2030 and the Action Plan for Implementing the National Strategy for Preventing and Combating Sexual Violence "SYNERGY" 2021-2030

13. Government Emergency Ordinance 77/2009 on the organization and operation of gambling

14. Halpern, D., Valenzuela, S., Katz, J., Miranda, J.P. (2019). "From Belief in Conspiracy Theories to Trust in Others: Which Factors Influence Exposure, Believing and Sharing Fake News". In: Meiselwitz, G. (eds) Social Computing and Social Media. Design, Human Behavior and Analytics. HCII 2019. Lecture Notes in Computer Science, vol 11578. Springer, Cham. https://doi.org/10.1007/978-3-030-21902-4_16

15. Hinduja, Sameer & Patchin, Justin. (2010). Bullying, Cyberbullying, and Suicide. Archives of suicide research : official journal of the International Academy for Suicide Research. 14. 206-21. 10.1080/13811118.2010.494133.

16. Li, W., Mills, D. and Nower, L. (2019) “The relationship of loot box purchases to problem video gaming and problem gambling,” Addictive Behaviors, 97, pp. 27–34. Available at: https://doi.org/10.1016/j.addbeh.2019.05.016.

17. Lovari, A., and Righetti, N. 2020. La comunicazione pubblica della salute tra infodemia e fake news: il ruolo della pagina Facebook del Ministero della Salute nella sfida social al Covid-19. Mediascapes journal 15/2020.

18. Magkos, Emmanouil, Eleni Kleisiari, Panagiotis Chanias, and Viktor Giannakouris-Salalidis. n.d. “Parental Control and Children’s Internet Safety: The Good, the Bad and the Ugly.

19. Mahl, Daniela, Mike S. Schäfer, and Jing Zeng. "Conspiracy theories in online environments: An interdisciplinary literature review and agenda for future research." *New media & society* (2022): 14614448221075759.

20. Moscadelli, A., Albora, G., Biamonte, M. A., Giorgetti, D., Innocenzio, M., Paoli, S., Lorini, C., Bonanni, P. and Bonaccorsi, G. 2020. Fake News and Covid-19 in Italy: Results of a Quantitative Observational Study*. International Journal of Environmental Research and Public* Health. 17. 5850. 10.3390/ijerph17165850.

21. Niethammer, A et al. Cybersecurity Laws and Regulations Germany 2023, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/germany, Accessed 28.02.2023

22. O'Connor, K. et al. (2018) “Cyberbullying, revenge porn and the mid-sized university: Victim characteristics, prevalence and students' knowledge of university policy and reporting procedures,” *Higher Education Quarterly*

23. Pennycook, Gordon, and David G. Rand. "The psychology of fake news." *Trends in cognitive sciences* 25.5 (2021): 388-402.

24. Pennycook, Gordon, and David G. Rand. "Who falls for fake news? The roles of bullshit receptivity, overclaiming, familiarity, and analytic thinking." Journal of personality 88.2 (2020): 185-200.

25. Petrović, Marija, and Iris Žeželj. "Both a bioweapon and a hoax: the curious case of contradictory conspiracy theories about COVID-19." Thinking & Reasoning (2022): 1-32.

26. Quicke, Audrey. 2020. Media literacy education in Finland. Nordic Policy Centre. https://www.nordicpolicycentre.org.au/media_literacy_education_in_finland
27. Romanian Criminal Code of 17 July 2009 (Law no 286/2009)

28. Runcan, R. (2020) “Conflict Solution in Cyberbullying,” Revista de Asistenta Sociala [Preprint], (2/2020).

29. Sammons, John, and Michael Cross. *The basics of cyber safety: Computer and mobile device safety made easy*. Elsevier, 2017.

30. Udișteanu, A. (2022) Analiză Recorder. Poliția Română E Copleșită de Criminalitatea Informatică: Peste 21.000 De Dosare Zac Nerezolvate, Recorder. Available at: https://recorder.ro/politia-romana-e-coplesita-de-criminalitatea-informatica-peste-21-000-de-dosare-zac-nerezolvate/ (Accessed: December 9, 2022).

31. Younan, B. (2019) “A systematic review of bullying definitions: How definition and format affect study outcome,” Journal of Aggression, Conflict and Peace Research, 11(2), pp. 109–115. Available at: https://doi.org/10.1108/jacpr-02-2018-0347.