Authors: Adriana Iordache, Ioana Cărtărescu-Petrică

# Youth online behavior, risks and avenues for mitigating them

**National report: Romania**

Authors: Adriana Iordache, Ioana Cărtărescu-Petrică

# Youth online behavior, risks and avenues for mitigating them

## National report: Romania

Bucharest
2023

# RISE

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

# Table of contents

# I.    Introduction

This report will examine socio-demographic factors, social media use, risk perception, preventive behaviors, attitudes and other relevant factors in the context of the post-COVID-19 pandemic. The end-purpose of this report is to evaluate the current state of affairs and the learning needs of young people, in order to provide relevant information for the development of an online game aimed as equipping young people with the necessary tools for avoiding the risks identified.

This report will provide an overview of youth online behavior, the main online risks associated with youth, patterns of manifestation of these risks and their regulation in the Romanian law. This report will examine the socio-demographic characteristics of Romanian youth aged 16-30 (age, gender, socio-economic status, rural/ urban residence, level of education, ethnicity), the main characteristics of their social media use and online behavior, their risk perception, existing preventive behaviors and attitudes, as well as the manifestation of the risks, in the post COVID-19 pandemic. The study also explores the attitudes and behaviors of youth towards global threats, such as pandemics, international politics, armed conflicts and refugee and to identify the risk factors in youth regarding to fake news and disinformation, as well as other relevant risks.

The analysis of the collected data will establish a set of risk factors in young people, as well as specific and general recommendations and strategies for preventing and combating the identified risks. This research is based on both quantitative data, collected through an online survey addressed to young people, and on qualitative data, obtained through a series of ten interviews conducted with youth trainers, young workers and other professionals working with young people.

This report has been elaborated with the scope of 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 quantitative data for this study was collected through on online survey addressed to young people (16-30) conducted by the Center for Not-for-Profit law in Romania in the period of October-November 2022. The survey was based on a questionnaire including 29 multiple-choice questions designed to assess demographic characteristics of the sample, media use and online habits, risky behavior and manifestation of associated risks, feelings and attitudes towards current events as well as critical reading skills. The questionnaire was circulated through google forms and was filled in by 83 participants, on a volunteer basis.

The quantitative data analysis for this research focused on two main aspects: 1. a general, descriptive overview of the participants' socio-demographic profile (age, gender, area of residence, level of household income, etc.), as well as their habits and experiences in relation to internet use and to the gathering of information regarding current socio-political events. This was achieved through the generation of simple contingency tables; 2. determining whether there are any relationships between variables such as the respondents' socio-demographic characteristics, internet use habits, favored sources of online information and patterns of news consumption and their susceptibility to believing with fake news.

Since most of the variables were nominal in nature, simple frequencies were used in order to determine the participants' level of agreement with 5 widespread fake news statements. Then, these frequencies were displayed as percentages of the total number of respondents for each variable category (e.g. we counted how many respondents in each age group agreed with the fake news statements, how many disagreed and how many remained neutral and then converted the absolute numbers into the percentage they represented from the total number of participants in each age bracket). To simplify the analysis and obtain more clear and compelling visual representation of the findings, an average score was calculated for each answer option of all 5 fake news statements, for each variable category (e.g. an average was calculated between the frequencies of the 5 "somewhat/highly agree", "neutral" and "somewhat/highly disagree" responses to the 5 fake news statements for each of the age categories; this allowed us to analyze a single set of values for participants' responses instead of 5 different ones).

The small size of the sample, as well as its homogeneity, are likely to influence the quality of the results and to make it impossible to extract relevant data for some of the items which were tested in the survey. Since the study was conducted online and could be answered by any young person willing to do so, a self-selection effect occurred and respondents were mainly the kind of people who are inclined to respond to online survey, which means they share a significant number of characteristics and do not accurately reflect the structure and diversity of the wider population. Given the fact that certain socio-demographic categories are disproportionately represented among the respondents, it was decided in most situations to present percentages instead of absolute numbers when it came to frequencies. However, all percentages presented should be considered in relation to the absolute numbers they represent, given the small number of respondents. It should be kept in mind that all the findings in the present report are only applicable to the present sample and cannot be extrapolated to the general population, for methodological reasons.

The qualitative data was obtained through ten semi-structured interviews conducted with youth workers and youth trainers in Romania, conducted in November - December 2022. The professionals consulted for this research had between 2- and 18 years of working experience with young people (most of them working with youth for more than five years). Three of them were also specialized in research and/or advocacy on specific online risks affecting young people: image-based sexual abuses, online gambling and gaming and fake news. The age of young people within whom the interviewed professionals work ranged from 8-30 years old. The experience of the professionals interviewed includes: formal education (one high school teacher and one university professor), non-formal education (two youth workers), two youth counselors, one person providing extracurricular training for young people, one coordinator of a child safety center ran by a non-profit organization (who is also a researcher), one psychotherapist working with young people suffering from gambling addiction and one representative of a students' organization who is also working with youth. In the selection of respondents, we aimed for a balanced distribution in terms of territorial distribution and the socio-economic status of the youth that they worked with (two of the professionals worked with honors high school students and one teaches at the university and three professionals worked with youth from underprivileged backgrounds and/ or separated from their family, while the rest worked with youth from all social categories).

The interviews were conducted on-line, via Zoom and recorded, with the prior consent of the interviewees. The interview notes were then transcribed and coded using MAXQDA, using the following cores: Experience of the interviewee, On-line behavior of youth, Impact of the Pandemic, Cyberbullying and harassment, Fake news, Gambling/ gaming addition, Identity theft, Revenge porn, Training recommendations and other projects. The relevant information was then grouped according to these codes and analyzed.

## III.   Literature review

### 1.  Fake news and misinformation

A conspiracy theory can be defined as "the conviction that a group of actors meets in secret agreement with the purpose of attaining some malevolent goal" (e.g., Bale 2007).
Therefore, a conspiracy theory includes the following elements:
1. an assumption or pattern of how people, objects, or events are causally interconnected.
2. the intentionality of the alleged conspirators, or otherwise said, that their plans are deliberate.
3. the collaborative nature of the action, which is never carried out by just one individual;
4. a threat or harm or dishonesty
5. secrecy or uncertainty, which makes conspiracy theories difficult to invalidate.

Conspiracy theories also represent "alternative explanations of historical or ongoing events claiming that people or groups with sinister intentions are engaged in conspiratorial plotting." (Uscinski 2018)

Conspiracy theories are a widespread social phenomenon in both traditional and conservative societies (West and Sanders 2003). While such beliefs have circulated for a long time, they were traditionally perceived as "harmless" and "silly and without merit" (Keeley, 1999: 109). However, the rise of social media and the democratization of the knowledge production has changed this, by facilitating their viral spread and rapid evolution.
The literature on the factors that determine belief and willingness to share disinformation, conspiracy theories and fake news has established several hypotheses for the reasons which cause people to spread misinformation. These hypotheses can be defined as: 1. the political hypothesis - people tend to believe and share news that confirms 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 as opposed 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.

Researchers have focused on several possible types of variables which might support or disconfirm one of these hypotheses. Psychological variables refer to characteristics of personality that might make a particular person more liable to spread misinformation, such as low trust in others, narcissism, machiavellism. Social variables include aspects that relate to a person's social position and, especially, distance from decision-making. Political variables look to a person's political views as well as to the intensity with which these views are held. Cognitive variables look to the extent a person is willing to use heuristics in order to decide which pieces of news to share or whether they are willing to take time to evaluate the credibility of a piece of information. Thus, researchers have found evidence of a "conspiracy mentality", as the best predictor of belief in a conspiracy theory is a belief in other conspiracy theories.

Strategies to combat disinformation can generally be divided in two groups: the retroactive approach, or debunking, which aims to correct factually wrong information that has been widely shared already by disseminating the relevant corrections and the pro-active strategy, called prebunking (or preemptive debunking), which works by "innoculating" people from fake news through a set of tools, such as online games, so that they become aware of the techniques used by those who spread disinformation and are able to recognize them.

This section presents the literature on the factors supporting or stopping the spread of fake news and summarizes the main hypotheses and variables identified in the literature as relevant. The works in this section have been selected through a search carried out in Google scholar, looking for articles that focus on 1. factors favoring or mitigating the belief in and the sharing of disinformation and 2. strategies aimed at combating the belief and the sharing of disinformation. By undertaking a meta-analysis of the academic work in the area of fake news, Mahl, Scheffer and Zeng (2022) identify the following relevant topics. Studies might focus on the way that fake news is being produced, while most focus on the willingness to believe conspiratorial content. A distinct, sub-field of the studies investigated looks at why people are willing to share disinformation, while the vast majority look at the way conspiracy theories and those sharing disinformation represent reality. Finally, a small number of studies analyze strategies to combat fake news, such as debuking and pre-bunking.

Pennycook and Rand (2021) discuss several hypotheses for which people might fall for disinformation and support the heuristics view over political motivations view. They first present the two hypotheses circulated in the literature on fake news. They show that the political motivation conception predicts that people will more likely believe news with low credibility but which conforms to their political views and are more likely to reject news which they find credible but which contradicts their views. The alternative hypothesis, the reasoning/heuristics conception refers to the idea that people use intuition over deliberative reasoning when making decisions. By conducting a meta-analysis of 14 other studies in the literature and secondary analysis of the data they collected, the authors find clear support for the reasoning/heuristics hypothesis, as the effect of cognitive laziness was much more prominent that that of political partisanship.

The authors conclude that, given the fact that attention and deliberation weigh more in one's decision to believe disinformation, Pennycook and Rand (2021) recommend preemptive strategies such as pre-bunking through 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.

Mancosu and Vegetti (2020, 2021) take a new angle at the factors which influence belief in fake news and conspiracy theories, and argue that conspiracy mentality is crucial. However, even among those with high conspiracy mentality, most are willing to lend greater credence to conspiracy-endorsing news if it comes from an alternative-style outlet over a mainstream-type outlet. This leads the authors to conclude that measures taken against social media platforms might be useless, given that independent outlets have this strong effect on people with a high conspiracy mentality and that, the latter congregate around outlets they trust.

Ackland and Gwynn (2021) evaluate previous research on the spread of fake news and also mention two hypotheses, which are similar to those previously analyzed: on the one hand, the reasoning/heuristics hypothesis which relates to whether people are willing to stop and evaluate the veracity of a news item and the social identity theory, which concerns people being willing to be associated with a group and to be seen as sharing its values, despite the low credibility of some sources. In their study of the spread of news among Australian twitter users, they found that most people rank the credibility of news correctly and fake news are less spread than real ones.

Prooijen and van Vugt (2018) argue that the predisposition to believe conspiracy theories could be grounded in evolutionary psychology, as it might involve 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. The researchers evaluate two competing hypotheses. First, that belief in conspiracy theories is a by-product of evolution, in the sense that they do not solve any adaptive problems but are carried along with properly adaptive

mechanisms. Alternatively, they investigate the hypothesis that belief in conspiracy theories is an actually adaptive mechanism, developed in order to identify intentions of out-group aggression. Thus, correctly identifying hostile intentions avoids significant losses, while incorrectly doing so only involves minor reputational losses. By examining evidence from anthropology, especially of contemporary societies, the authors find evidence to support the second hypothesis.

Umbres and Stoica (2022) conducted a study in Romania to investigate factors that support or reduce the belief in COVID-19 related conspiracy theories. While some of their results converged with previous studies, such as that older people are more prone to believe in conspiracy theories, others diverged considerably. In the Romanian sample, education was inversely correlated with the belief in conspiracy theories, as more educated people were more eager believers. Furthermore, people who identified themselves as to the extreme right of the political spectrum were less willing to support conspiracy thinking. Researchers hypothesized that this might relate to the way in which left and right are defined in Romania, which differs significantly from the Western understanding. Finally, people with a high degree of collective narcissism were more likely to support conspiracy theories.

Buturoiu et al (2021) ran a similar study for Romania and found some opposing results. Their study did not identify any effect of either age or of a self-reported measure of critical thinking on the propensity to believe disinformation in Romania. However, they identified a positive effect of religiosity and a negative effect of education (more educated people are less willing to believe fake news). Further, in this study, those who believed that social networks were more useful as a source of information and those who believed in the omnipresence of disinformation were more willing to accept conspiracy theories related to COVID-19 as true.

The main narratives of COVID-19 conspiracy theories observed in Romania do not differ considerably from those found in other countries. The ideas that the pandemic has been planned for a reason, either by Bill Gates or by the pharmaceutical industry, was identified in a study by the Eurocomunicare (2020) organization. The same study showed how miracle cures such as Ivermectin were proposed and how masks were blamed for starving the brain of oxygen. Finally, the prospective introduction of 5G infrastructure was associated with the spread of the virus while vaccines were described as a way to control the population (Eurocomunicare 2020). In a non-COVID-19 context, disinformation in Romania focuses on the supposed „colonization" of Romania by the West, as evidenced by the presence of US military bases, and on the supposed superiority of the communist regime over the current political regime (Olaru 2022).

Halpern el al. (2019) ran a complex study testing the susceptibility of believing and sharing fake news on a Chilean sample. Their results are similar to those obtained by Mancosu and Vegetti (2020), in the sense that social media use, does not, per se, affect the propensity to believe in fake news. However, when people already tend to believe fake news, there is a strong effect of social media use, conspiracy mentality and confidence in what contacts share on the willingness to further distribute fake news. According to the authors, there is also a strong effect of political identification, as more people on the right of the political spectrum are more willing to believe and share disinformation, however, there is no identified effect of the extremity of political views.

Petrovic and Zezelj (2021) ran two studies on the factors that predict belief in mutually contradictory conspiracy theories in Serbia, which replicate a study conducted by Pennycook and Rand (2020). As several other authors, they found considerable support for the claim that a certain type of mentality is that which favor belief in conspiracy theories, even when these seem to contradict each other. Thus, the most important predictors identified by the two studies were a general tendency to accept conspiracy-like content, the predisposition to believe mutually contradictory statements. One of the study's most interesting findings was that people

who are willing to accept contradictory claims still rate themselves high on a scale of a preference for consistency. The authors' second study found that those who prefer experiential rather than rational thinking and are prone to rate pseudo-profound statements as profound are more willing to believe disinformation, but that digital literacy does not have significant effects.

Studies specifically carried out on young people and their relationship with disinformation have been relatively scant in the literature. While most studies focus on the sources of information that young people use and on the way they use the internet, little attention is paid in these studies at their susceptibility to disinformation. Farfan and Mazo (2021) look at the way young Spaniards accept information on the COVID-19 pandemic from different sources. They argue that official information from the government is relatively little believed, while those featuring scientists and medical profession has more credence. The authors also show that young people who are more exposed to disinformation are less willing to follow the rules for COVD-19 prevention. A study on Romanian young people showed that they tend to be generally aware that not all information on the internet is equally accurate. About 51% percent of young people are willing to believe online sources, while about 25% to believe magazine and newspapers. The percentage of those believing online information decreases with age and is lower in urban areas, while the converse relationship holds for those believing information from magazine and newspapers. Romanian youth are ready to accept their confirmation bias and state that they believe readily and information that confirms what they already know (CJI 2020) . Basch et al (2021) analyzed the content of TikTok videos discussing COVD-19 vaccination. The choice of analyzing Tiktok content was made given the fact that it is mostly used by young people. The authors of the study concluded that the videos that discouraged a vaccine received more likes and comments from the users, but that the difference was not strong.

Concluding, the most relevant factor which aggravated belief in conspiracy theory was a propensity for not thinking critically and for not verifying information that one interacts with. This was seen as significant across most of the studies identified. Alternatively, a rational style of thinking, taking time to verify information were more likely to decrease susceptibility to fake news. Personality traits such as narcissism and marginal socio-economic status were also sometimes relevant, as well as religiosity and political views. Proactive pre-bunking was seen as a considerably more effective way of combating disinformation as opposed to retroactive debunking.

**Fake news Manifestations and Patterns**

*The Barometer of informational social resilience,* published in 2022 by the Euro-Atlantic Center for Resilience, reveals that over half of all Romanians have been exposed to disinformation of the Fake News kind, particularly from a Russian origin. The result of concerted fake news campaigns was that over 60% of the population believes that the Covid 19 pandemic was purposefully provoked by occult international forces (Munteanu, 2022)

As revealed by a [Press One investigation](), The Romanian fake news phenomenon usually takes the form of mass mediatic intoxication for propagandistic purposes, most frequently spread through websites and social media accounts claiming orthodox religious affinities or affiliation (Simina, 2020; Despa, 2021). During the past years, the most intensely circulated fake news targeted the Covid 19 pandemic and vaccination campaign (fake information claiming the virus is not real and is only a means of controlling population and the vaccine has harmful effects and/or represents a means of gaining physical control of the people injected with it). In 2022, however, the focus of disinformation efforts shifted towards the war in Ukraine, as the Russian propaganda apparatus made considerable efforts to obscure the true causes and outcomes of the hostilities and to paint Russia as a victim rather than an aggressor.

**Examples of Fake news Manifestations and Patterns**

The most classic fake news pattern circulating in Romania is that of the social media account which spreads a variety of disinformation on health and political topics, while pretending to be an Orthodox religious page. There is little to no religious content on the respective page, instead adamant opinions on controversial socio-political topics are expressed and articles containing falsehoods or twisting actual events to fit the page owner's agenda. Such is the case of Ortodoxinfo, a Facebook page and Telegram channel claiming to be an "Orthodox news portal". However, its feed is overwhelmingly comprised of fake news on a multitude of health, economics and political subjects (Fig 1 and 2)

**Fig. 1. Example of fake news regarding Covid-19 vaccines posted on the "Religious News Portal" Ortodoxinfo Facebook page**
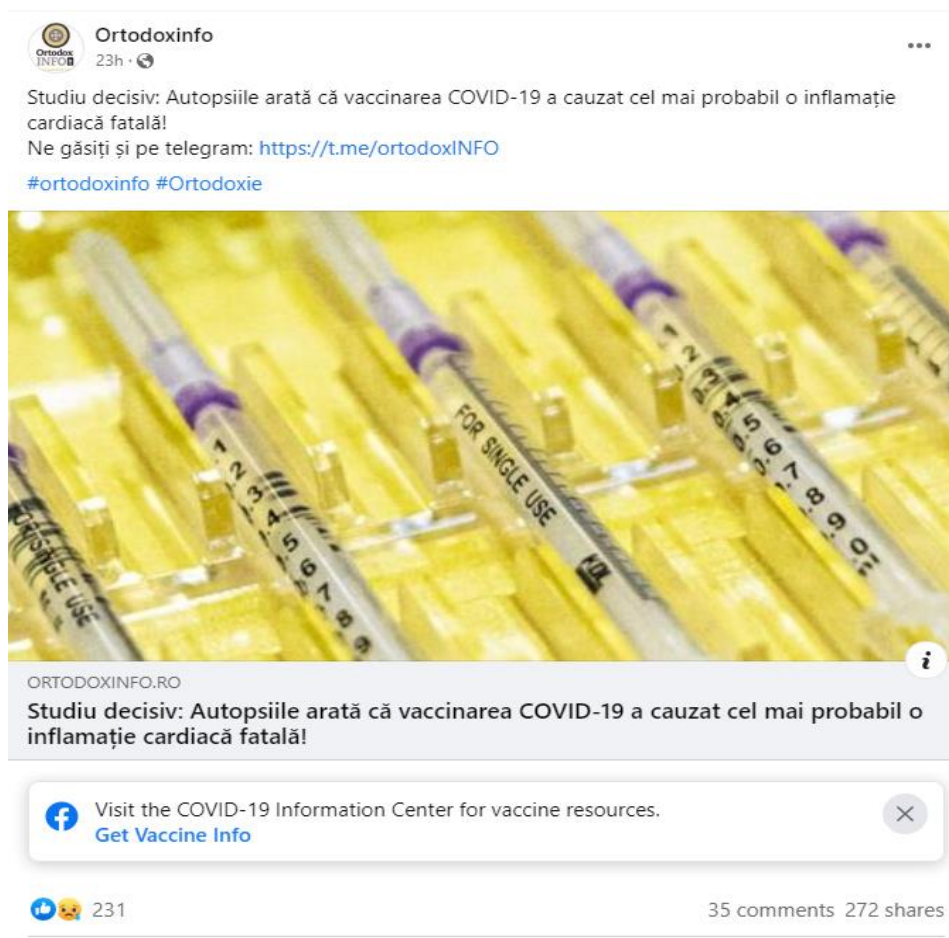


**Fig.2. Example of political fake news posted on the "Religious News Portal" Ortodoxinfo Facebook page**

Ortodoxinfo
2d · 🌐

Mecanismul prin care Guvernul de la București finanțează separatiștii pro-ruși din Transnistria
Ne găsiți și pe telegram: https://t.me/ortodoxINFO
#ortodoxinfo #Ortodoxie

ORTODOXINFO.RO
Mecanismul prin care Guvernul de la București finanțează separatiștii pro-ruși din Transnistria

The content posted by this kind of page is created specifically to be easy to read and persuasive even for people with a lower level of education, which is why it garners numerous believers and has good chances of becoming viral, as it is widely shared by users who believe the information in it.

As the fake news phenomenon has been gaining significant traction in Romania, efforts have emerged to counter it. Such is the case of website Veridica.ro, as well as the Facebook page Stop Fake News in Romania which is dedicated to systematically exposing and deconstructing disinformation with facts and arguments.

## 2. Cyberbullying

There is no universal definition of bullying, but most social scientists agree upon a set of characteristics behavior should possess in order to be classified as such. Thus, in relevant literature, when speaking of this phenomenon, authors refer to a type of *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* (Younan, 2018). While this kind of behavior has been around forever, it has started to be formally studied in the 1970s. Alongside the emergence and widespread adoption of the internet though, bullying has quickly made its way into the online environment, a medium which makes it much easier to harass others with impunity. The term "cyberbullying" was first introduced by Canadian educator, politician and activist Bill Belsey, the founder of the website bullying.org and it refers to acts of bullying performed through the use of online technology, such as social media, messaging apps, websites, etc.

While in the beginning, some experts treated cyberbullying as the same phenomenon as regular bullying, simply perpetrated through modern technological means, nowadays social scientists generally agree that there are significant elements which make this form of harassment unique (Slonje et al, 2013, Vaillancourt et al., 2017). One of these is the protection of anonymity which the internet offers, allowing cyberbullies to obscure their true identity and interact online through aliases, avatars and online personas. This process of deindividuation does not only make it easier for the victimization of others to go unpunished, it also enhances

malice and aggression on the part of the perpetrator. Furthermore, while traditional bullying involved in-person interaction which could be avoided, cyberbullying does not require this and its digital nature makes it very easy to replicate and difficult to escape, allowing others to easily participate in the harassment of the victim by distributing and commenting on the humiliating or harmful information shared by the bully. This places a significantly larger amount of power in the hands of the aggressor, deepening the imbalance between them and the victim and often causing more harm than traditional bullying, even where there is no threat to physical safety (Ansary, 2019; Bartlett et al, 2020; Vaillancourt et al., 2017 apud Ansary, 2019).

There are many types of cyberbullying which have been researched and described in relevant literature. The most common of these are online harassment (trolling, threats, mobbing), cyberstalking, doxxing, impersonation and exclusion (Scheitauer et al, 2021; Runcan, 2020)

## 2.1. Online Harassment

Online harassment is a consistent effort to cause someone negative emotions and psychological/material harm through digital means. It can take many forms, some of the most notable being (Runcan, 2020):

- trolling (purposefully contradicting or insulting someone online in order to cause them anger or distress),
- denigration (posting hurtful or offensive things 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).
- mobbing (encouraging others to join up in harassing someone, either in person or online, through digital means)

## 2.2. Cyberstalking

The phenomenon of 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). In order for a behaviour to be considered cyberstalking, rather than simple harassment, a series of criteria must be met, such as the fact they need to occur frequently, to incite fear in the victim (a sense of looming threat), to be intrusive and unsolicited in nature, to infringe on the victim's personal boundaries or privacy, etc.(Kaur et al, 2021, Wilson et al, 2021; Ahlgrim & Terrance, 2018)

## 2.3. Doxxing

Doxxing is defined as "the practice of publishing private, proprietary, or personally identifying information on the internet, usually with malicious intent" (Andersen & Wood, 2021). When speaking of doxxing, relevant literature refers to a serious breach of the victim's privacy, by making their personal information publicly available online, in hopes that anonymous users will use this data to harass or frighten the victim. This information could be anything from their real identity, their home address, phone number, place of employment, sensitive identification information (e.g. their personal numeric code), user credentials from various websites, etc. This form of cyberbullying is usually retributive in nature, meant to punish the victim for a real or imaginary fault and it can also be used as a technique of intimidation, to make other users

afraid of expressing certain views about society, certain people or organizations. Doxxing is most frequently aimed at women and it can have severe real-world consequences for its victims, who have, in many cases, received threats from anonymous online harasses after being doxxed, sometimes to such an extent that they needed to move to a different home or leave their job as a result (Eckert & Riftkin, 2020).

**Manifestation of the different types of cyberbullying**

A study performed by Save the Children in 2018, on a sample of over 1000 Romanian teenagers revealed that 70% of them had received "offensive or distressing messages" online and 54% declared that they had been upset by others while using the internet. 15% of them reported having had offensive or distressing content about them posted online, while 30% had faced online exclusion. Most of these incidents had taken place on social media platforms.

When it comes to the patterns of cyberbullying, international research (Festl et al, 2017; Iorga et al, 2022) has found that girls in particular and young people of mid-teenage are more likely to become victims. Another gender difference in cyberbullying patterns is that while girls seem to prefer forms which attack the victim's social relationships (rumor spreading, gossiping), boys are less inclined to do so, opting for directly insulting their target. While perpetrators are of both genders, girls who engage in cyberbullying are more likely to have been victims of this phenomenon at some point than boys (it is rather common for those who have been victims to become perpetrators). Moreover, cyberbullying is frequently associated with traditional bullying, and students who report higher levels of loneliness and lower satisfaction levels with their relationship to their classmates are more likely to become victims (Festl et al, 2017, Runcan, 2020; Iorga, 2022).

Cyberbullying is sanctioned both by a dedicated provision included in 2020 in the Law against domestic violence (Law no. 217/2003 - Republished), as well as by making use of the legal provision from the Criminal Code of 2009 (art. 208) which sanctions harassment as a criminal offense.

According to Art 4 para. 1), h) of Law 217/2003, cyber violence is defined as:

> *online harassment, online messages inciting gender-based hatred, online stalking, online threats, non-consensual publication of intimate information and graphic content, illegal access to intercept private communications and data and any other form of misuse of information and communication technology through the use of computers, smartphones or other similar devices that use telecommunications or can connect to the internet, disseminate information and use social or email platforms, with the purpose of shaming, humiliating, frightening, threatening, or silencing the victim"*

Meanwhile, the Criminal Code also defines a type of harassment as "telephone calls or technology-based long-distance communication which, through their frequency or content, cause a person to fear". (Art. 208 para. 2) Such acts are punishable by imprisonment from one to three months or by a fine, "unless the act constitutes a more serious offence". In order to this criminal offense to be investigated, the victim must file a complaint.

In Romania, some of the most common forms of cyberbullying come under the shape of online harassment, through offensive comments, insults or threats. Though both genders are susceptible to this, young women are more likely to receive them, especially through private messages.

For example, a young woman can be repeatedly insulted and threatened via Facebook messenger by a man who took offence with her having publicly criticized his work in a comment on the same platform. Despite being ignored, the perpetrator continues to harass the victim. Another example, is that of young women being the victims of cyberstalking and online harassment by people whom they may know in real life. In one case, the perpetrators posts offensive messages to the victim's social media profiles or to the profiles of her friends, using fake social media accounts to avoid being reported or blocked. In another case, the victim is being stalked both online and in real life and is receiving insults and even death threats. Of course, not only young women fall victim to cyberbullying. The press has also reported that a young student who has fallen into depression after having been bullied both online (through humiliating private messages) and in person by his schoolmates.

While Romanian legislation on the matter of cyberbullying is rather new and rarely enforced by authorities, some perpetrators have already begun to fear the legal ramifications of online harassment. In one case, a woman tried to downplay her actions as she turned to a legal advice website to ask whether they can be held liable for posting photos (some taken surreptitiously) of others, alongside insulting comments, on specially created fake Instagram profiles. The perpetrator only became concerned with the consequences of her actions after the victims threatened to involve the police, accusing them of online harassment.

Unfortunately, however, many victims of cyberbullying are blamed or doubted when they try to seek help or advice from others. Such is the case of a Romanian internet user who posts to a forum dedicated to the Romanian police officer community, seeking advice for having been doxxed - an unknown individual had posted photographs of them, alongside personal information, on a popular entertainment website. The response of the moderator of the police officer forum is to assume that the victim has done something to provoke the perpetrator, who must be exacting potentially justified revenge and to gratuitously accuse her of not telling the whole story.

## 2.4. Impersonation

Also known as "masquerading", impersonation involves the cyberbully posting online content while pretending to be the victim. This can be done by creating websites/fake accounts with the victim's information (name, photos, etc.) and using them to share humiliating or denigrating content about them in their name. Another way to achieve this is to hack (or otherwise illicitly access) the user's existing websites/accounts and posting content meant to damage their reputation (Runcan, 2020). While false information posted to someone's actual accounts has a greater potential to be taken at face value by their social network, it is also easier to remove by the owner, by simply deleting the offending content. However, if the perpetrator has created fake websites or accounts, it could be more difficult for the victim to get them shut down.

Impersonation happens frequently in Romania, as a form of harassment or revenge. This is the case of a local singer who discovered that an individual had created a fake Facebook account in his name, using his photographs and was using it to stalk and harass young women (Rosu, 2019). Upon further research, it became clear that the perpetrator was trying to exact revenge on the victim for having rejected his application to a music school he was teaching in.

## 2.5. Exclusion

Sometimes, young people can be caused distress in the online environment simply by barring their access to it (Runcan, 2020). That is, one way of cyberbullying someone is arbitrarily withdrawing or denying their access to internet places which they want or need to visit, such as chat groups, online gaming servers, mass blocking them on social media, etc. This can have a similar psychological effect as shunning and isolating someone in the offline world. It sends a clear message that they are not wanted and accepted among their peers and at the same time may block their access to resources they need, such as information about homework assignments on a school chat group, invitations to events posted on social media, etc.

## 3. Online Identity theft

While this phenomenon seems similar at a glance to the cyberbullying type known as impersonation/masquerading, there are significant differences between the two. While impersonation is performed mainly as a way to cause embarrassment or distress to someone in the online environment, identity theft does not primarily have a retributive purpose, but is performed in order to obtain material profit either by defrauding the victim or by defrauding others in the name of the victim. Defined as "the illegal or unauthorized use of personal information belonging to someone else for one's own benefit." (Soomro, 2018), identity theft manifests itself online in the following common forms (Ibidem):

- 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.). If they enter this data, the identity thief gains access to them and proceeds to access the victim's bank account to withdraw money, to make online purchases, etc. They can access other type of accounts as well, in order to obtain goods or services in the name of the rightful owner.
- Hacking - This method is very similar to phishing, except it uses force instead of deception. The hacker uses malware to launch a cybernetic attack on the victim until they gain access to their private information, which they use to impersonate them for fraudulent purposes.
- 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 ask for money, under false pretence (e.g. they may say that they were in an accident, are hospitalised and need money urgently for an intervention or that they are stranded in a different country and need a quick financial transfer to buy a plane ticket). Once they are discovered, they abandon the account and move on to the next victim.
- Identity spoofing - Similarly to social media cons, 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 request information, donations for fake causes or sell products in their name.

Regardless of the form it takes, identity theft is a crime everywhere in the civilized world. However, given the fact that the perpetrator is often not even in the same country as the victim

and is likely to use specific software to protect themselves from being traced, it can be difficult to find and prosecute online identity thieves.

**Online Identity theft - patterns and manifestations**

There is little data publicly available regarding the number of online identity theft cases in Romania, but a Recorder (Udișteanu, 2022) article reveals that internet fraud, which involves identity theft in a significant proportion of cases, has soared in the past few years. Basically, in 2019-2020, the number of reported incidents has doubled, resulting in 7862 criminal records, while unresolved cases soared to over 21.000. The police report being overwhelmed by citizens who seek their assistance, having fallen victim to online phishing schemes or other similar cybercrimes. Unfortunately, there is no specialized department within the Romanian police force to tackle internet crimes and the personnel who is assigned to resolve this type of cases is few and spread thin.

If serious criminal offences, such as identity theft resulting in financial fraud with significant damages to the victim, barely get solved on account of dwindling police resources, other, "milder" forms of identity theft go largely underreported. Such is the case of stealing someone's social media account or creating an account using someone else's photographs and personal information, in order to gain access to their friend network for material gain. While this phenomenon is rather widespread, there is no data as to its frequency, as users generally report it to social media platforms rather than local authorities.

Identity theft falls under the criminal offence of forged identity, which is define as:

> *Presenting oneself under a false identity or attributing such identity to another person, before a public servant or before an institution where he/she carries out his/her activity, by fraudulent use of a an identification document or proof of a certain status or the use of a forged such document, in order to mislead a public official or to reinforce his/ her error, in such a wat as to producing legal consequences, for oneself or for another person", shall be punished by imprisonment from 6 months to 3 years. (art. 327 para. (1) of the Romanian Criminal Code of 2009.*

When the perpetrator is using the real identity of another person, the punishment is imprisonment from 1 to 5 years.

When identity theft is connected to a financial fraud, the action also falls under the provisions of art. 250 of the Criminal Code of 2009, regarding fraudulent financial transactions, which are defined as:

> *Carrying out a cash withdrawal, placing, withdrawal or transferring of funds on an electronic financial instrument, monetary value or virtual currency by using, a non-cash payment instrument or the identification data enabling its use, without the holder's consent or by using fictitious identification data.*

This offense is punishable by imprisonment from 2 to 7 years.

**Examples of Online Identity Theft - patterns and manifestations**

Some phishing schemes have become so aggressive in Romania that the National Cybersecurity Directorate has to issue regular warnings on their Facebook page, making citizens aware of the most common ones.

When it comes to social media scams, many Romanians have found that their social media accounts had been hacked into and hijacked by strangers who wanted to profit from the social network the victims had built. The person whose account is hacked is usually locked out of it and has little means to warn their online friends that their identity has been stolen. The perpetrators then proceed to try to defraud the victim's social circle, using their authority and good name or simply change the account information and use it to spread disinformation and malware. In most of the cases, one of the targeted person's online friends becomes aware of the situation (or is informed by the victim) and they post a status to warn common connections about the identity theft. In other cases, the victim themselves use a different social media account to warn their friends about what has happened to their original one.

Alternatively, the identity thief does not hack into the victim's account at all, but impersonates them, creating a fake account with their photographs and personal information and interacting with others under their identity. This is what happened to a man who received a friend request from a suspicious Facebook profile, only to notice that the profile image had his own photograph, one which he had taken specifically to send to one acquaintance. That acquaintance was likely the target of a malware attack which stole her photos and friend list and used them to steal the identity of her online connections.

## 4. Image-based sexual abuse

While cyberbullying includes a wide range of hostile online behaviour, there is a specific kind of risk young people - especially young women - are exposed to while on the internet: image-based sexual abuse. The most serious of type, which has also been legally incriminated in many Western countries, is revenge pornography. However, other such risks include being unwillingly exposed to pornography or unsolicited sexual content, being pressured into sexting or sending nude photographs of themselves, having strangers misrepresenting their age and/or gender in order to obtain sexual content, etc.

### 4.1. Revenge pornography

Revenge pornography represents a specific form of nonconsensual media distribution, 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). This type of behaviour 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, media such as nude photographs or recordings of sexual encounters are posted on social media, shared on pornography websites or distributed directly to the victim's peers (and sometimes family, employers, etc.), in order to cause them humiliation.

Literature shows that revenge pornography victims are overwhelmingly female and that sometimes, this form of aggression is preceded by blackmail, in order to obtain material or sexual favours from them.

Research has revealed that having sexual imagery of them unconsensually distributed can have a devastating impact on the victim's psyche, similar to that of a physical sexual assault (O'Conner et al, 2018; Lageson et al, 2018). As a result, they can develop a number of mental health conditions, such as anxiety, depression, panic disorders, low self-esteem, and even PTSD. They are also prone to developing unhealthy coping mechanisms which can lead to addictions, self-harm, etc. (O'Conner et al, 2018; Lageson et al, 2018).

## 4.2. Exposure to pornography/unsolicited sexual content

Another highly gendered form of online sexual risk is that of being unconsensually exposed to sexual images, videos or text and/or to the solicitation of sexual favours by either strangers or people in one's social circle. This is especially serious when minors are involved, as sending explicit sexual content to minors, as well as possessing sexual media depicting minors is illegal in most countries. Research shows that people who send unsolicited sexual content to others are mostly male, while the recipients are overwhelmingly female. One of the most frequently encountered form of this phenomenon, which has greatly increased in prevalence over the past decade, as telephone cameras have become more and more performant and messaging app encryption has improved, is the sending of unsolicited pictures of one's penis in private messages on social media apps. Colloquially known as "dick pics", these unwanted images that female internet users are sometimes exposed to when they least expect it have been called in literature "the online equivalent of catcalling" (Paasonen et al, 2019). This means that even though the men who engage in this practice try to frame it as a "compliment" or an intimate invitation towards the (mostly) female recipients, the gesture is viewed by the women on the receiving end as a form of misogyny, sexual abuse and harassment. They 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). While most social media networks are rather strict when it comes to enforcing bans on posting graphic sexual images, private messages are not moderated unless they are directly reported by the recipient after viewing them, so there are effectively few mechanisms in place to prevent young people from having to see the sexually explicit images sent to them via this route.

**Image Based Sexual Abuse Manifestations and Patterns**

Research performed on Romanian teenagers who use the internet shows that 43% of them have received online messages with sexual content and almost half of this group (22%) report having received such messages daily or at least weekly. 20% of these teenagers state that they have been asked for nude videos or photographs of themselves in return, but only 5% admit to having accepted such a request. Boys were found more inclined to respond that they have sent messages with sexual media content than girls.

There is little data collected regarding the prevalence or patterns of revenge porn, partly because it is a sensitive topic, which very few victims are inclined to report or discuss. However, increasing media coverage of the phenomenon has provided in-depth insight into some particular cases, which are likely to paint a good picture of the phenomenon's local characteristics.

The Romania Government has acknowledged the widespread character of sexual violence and adopted the National Strategy for Preventing and Combating Sexual Violence "SYNERGY" (2021-2030) together with the Action Plan for Implementing this strategy, through Government Decision no. 592/2021.

The strategy includes actions for reducing sexual violence, through general prevention measures, counselling for women and girls and by improving the capacity of professionals, central and local public authorities, families, communities and civil society to prevent and react to such incidents.

The key objectives of the strategy are the following:

- Continuous training on preventing and combating all forms of sexual violence, including cyber violence, for all relevant professionals (teachers, medical doctors, psychologists, police officers, judges, prosecutors, social workers, etc.), and NGOs;
- Developing educational materials for preventing and combating sexual abuse of any type and in any environment, including online, to be used in compulsory educational programs at all levels;
- Conducting annual awareness-raising campaigns on preventing and combating sexual violence for journalists, bloggers and vloggers whose activity has an impact on children and teenagers;
- Examining the current legislative framework in view of ensuring a safe online environment, combating pornography, revenge pornography, harassment and blackmail regarding the dissemination of sexual material;
- Informing children, youth parents about the risks associated to accessing online social networking platforms and strategies for addressing those risks.

The Romanian legislation sanctions certain types of image-based sexual abuse manifestations, while others are only partially covered. If the sexual images depict a minor or a person pretending to be a minor, it is specifically covered by the legislation as a criminal offense. However, if the images depict a person over the age of 18, the victim must invoke other related provisions from the legislation, as there is no specific law against revenge porn.

Art. 374 of the Criminal Code of 2009 on Child pornography, which states that "the production, possession, procurement, storage, display, promotion, distribution and making available in any way of pornographic material involving minors" is a crime, which is punishable by imprisonment for one to five years. If this crime is committed with the use of a computer system or a data storing mechanism, the penalty is imprisonment for 2 to 7 years.

Child pornography is defined as "any material which depicts a minor or a person over the age of 18 depicted as a minor explicitly engaging in sexual conduct or which credibly simulates a minor engaging in such conduct, as well as any depiction of a child's genitals for sexual purposes." (Art. 374, para. (1).

The law also sanctions "the unlawful accessing of pornographic material with minors through computer systems or other means of electronic communication" by imprisonment from 3 months to 3 years or a fine.

Victims who are over the age of 18 can invoke a violation of their privacy or online harassment (defined above), depending on the actual conduct of the perpetrator.

Violation of privacy is defined by Art. 226 para. (1) of the Criminal Code of 2009 as "the unlawful invasion of privacy by photographing or recording images, listening in, by technical means or audio recording of a person inside a dwelling or in a space related to it, or of a private conversation", which is punishable by imprisonment from one month to 6 months or a fine. A more severe from of the same criminal offense is "the unlawful disclosure, dissemination, presentation or transmission of the sounds, conversations or images referred to [above], to

another person or to the general public", which is punishable by imprisonment for a term of 3 months to 2 years or a fine.

**Examples of Image Based Sexual Abuse Manifestations**

The classic form of revenge porn is usually perpetrated by a young woman's former sexual partner, who either posts nude photographs of her on the internet or sends them directly to her friends, colleagues and/or family. The victim is almost always blamed by peers and authorities alike for having taken the pictures in the first place. This is what happened in many cases documented in the local media.

Independent journalism website Casa Jurnalistului documented the case of Mara, a 19 year old Romanian girl who had been in a brief relationship with a 20 year old colleague (Dimulescu, 2020). While they were a couple, the girl sent her boyfriend some nude photographs of her, for his eyes only. But after they broke up, he created numerous fake accounts pretending to be a female friend of Mara's and used them to distribute the photographs on social media. He privately messaged people who knew her to get them to view the non-consensually shared images, claiming Mara would like them to do so. He then proceeded to cyberstalk and harass the girl, leaving her threatening messages and claiming nobody would punish him for his actions, because his family had connections in the police force. Eventually, he started posting Mara's nudes and personal information on prostitution websites. In spite of the fact that there are telephone recordings of Vlad's threats and evidence of him having engaged in several illegal actions against Mara, according to the journalists, the police was dismissive and unhelpful in instrumenting her case and actively blamed her for being victimized. One reason for this is the lack of a specific law against revenge pornography in Romania.

Similarly, according to Student Stories (Belu, 2021), Olivia shared intimate photographs of her with her then boyfriend of two years. He shared those photographs with other people, who did the same in turn. Soon, her family, friends, teachers and even strangers were in their possession. She then began to be harassed by strangers who, having also received the images, were propositioning her for sex through social media or private messages.

However, it is not only men who engage in the non-consensual sharing of female nude photographs. Sometimes, it is the female friends or rivals of young girls who come in possession of these pictures and share them in order to cause them humiliation and distress.

Casa Jurnalistului (Dimulescu, 2018) also reported the case of Alina, an honor student, as well as an honor citizen of her home town who had the misfortune of having her personal e-mail address illicitly accessed and her nude photographs stolen and shared with her schoolmates. As the compromising material had already circulated throughout her high school, Alina's teachers came in possession of them and proceeded to blame, shame and even punish her for having taken them. The teachers' council even decided to formally sanction her by lowering her behavior marks for having possessed sexual photographs (of herself) and she was threatened with being expelled. However, none of the other students who possessed and distributed her photographs suffered any kind of consequences. She quickly became ostracized, bullied and harassed even by colleagues she had formerly considered her friends and this brought her significant mental anguish.

An article published by Scena 9 (Dimulescu, 2020) speaks of an Instagram account named Fete Cuminti, created by a young girl of only 14, where she would post revenge pornography

sent in by anyone who wanted to participate, complete with the victim's names and private information. It appears that she did so after having herself been a victim of the same phenomenon. Her identity was discovered by one of the young girls whose intimate photos she had published, who was only 13 years old. While this particular Instagram account was shut down, others like it still exist on Instagram, Telegram and likely on other social networks teenagers use.

Finally, regardless of the type and pattern, revenge pornography is deeply devastating to its victims, leading to mental health issues such as anxiety, depression, PTSD, social isolation, and in tragic cases, even suicide. That was the case of an 18 year old girl from Cluj Napoca, who took her own life this year as a consequence of having had her nude photographs posted on the internet (Diac, 2022).

## 5. Online Gambling

Gambling is a powerful psychological addiction, which can draw young people in a spiral of self-destruction. However, while traditional gambling requires going to a specific place with the intent to partake in such activities, in the online environment, this habit can be much more subtle and insidious.

There are three major kinds of online gambling. The first two are merely the online equivalent of the traditional form: games of chance and sports betting. The final one is more recent and much more difficult to become aware of: loot box mechanics in video games.

When it comes to playing games such as online poker, virtual slot machines or placing sport bets on an app rather than in a physical store, it is more than just the added convenience which draws users in. Targeted advertising 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. Some websites offer newcomers a number of perks (such as free initial credit or the chance to win additional prizes) in order to entice them. It is, however, still clear for the player that they are gambling and risk losing the amount of money they bet.

However, more and more young people are playing online video games every year and their starting age becomes ever lower. It is quite easy for a teenager to fail to understand the fact that gambling is present in the video game they are enjoying and that they are unwittingly taking part in it. It has become an increasingly frequent practice of video game companies to add a loot box mechanic to their online titles. That means that players are allowed to use real money to buy a package which provides them with a mere chance to get very good items, which they need or desire in order to progress or to complete an objective in the game. While some of the items in these packages are rather common, there are also a few coveted very rare ones, which have extremely slim chances of being encountered (sometimes, these chances are not even revealed or are misrepresented by the companies, giving gamers the impression that they are more attainable than they really are). However, this mechanic is addictive and players keep investing money in these purchases, in hopes that they will eventually get the very special items. Research suggests that in the case of these loot boxes, "the thrill from gambling comes from associated increases in physiological arousal not possible monetary gains." (Brady & Prentice, 2019; Spicer et al, 2021), meaning that predisposed young people are more likely to become problematic gamblers after purchasing and opening loot boxes in video games (Kristiansen & Severin, 2020). Furthermore, studies have also

discovered that in time, problematic gamblers become hyposensitive to the arousal from opening loot boxes and feel the need to increase the amount they spend in order to re-experience the initial thrill (Ibidem). Finally, it has been found that problematic gambling and long hours spent in online games create a vicious circle, catalyzing each other and leading to mental distress for gamers who engage in them (Li et al, 2019).

**Online Gambling patterns and manifestations**

While data is scarce regarding how many Romanian people engage in online gambling, a Press One article (Olaru, 2021) provides an estimate that there are around 1 million user accounts on sport bets and casino platforms. According to studies performed by the gambling industry (Bogdan Cazino, 2022), 94-96% of Romanian gamblers engage in this activity from their own home, using online apps, especially on their mobile devices. The number of users on these platforms is constantly increasing, as massive amounts of money are invested in their online marketing budget. That is because while television and written press have strict rules regarding the conditions under which gambling advertisements may be broadcast, these regulations do not apply to the online environment. As such, internet users are aggressively targeted with such ads. However, in cyberspace there are also digital means of identifying and curbing problematic gambling, such as software designed to analyze user behavior and signal if they are at risk.

In Romania, gambling is regulated by Government Emergency Ordinance no. 77/2009, which defines the different types of traditional and internet fortune games that can be organized and regules their functioning and organization, and the Regulations approved by Governement Decision no. 111/2016.

According to Art. 7 para. (3) of the Ordinance, "The access of minors to venues dedicated to gambling and their participation in any type of gambling is prohibited" and art. 6 para (1) of the Regulations state that "promotional actions for gambling activities […] shall be carried out in compliance with the principles regarding the protection of minors and responsible gambling." Also, advertisements cannot pe placed in the campuses of educational institutions and must explicitly mention the prohibition of the participation of minors in gambling.

According to a 2020 marketing study (RGDA, 2020), approximately 1.200.000 Romanians play online video games, but there is no data regarding how many of them spend money on loot boxes.

**Examples of online gambling patterns and manifestations**

While online gambling is easier and more comfortable than its traditional counterpart, it is just as addictive and it has just as severe consequences. That is why many Romanian medical advice websites, such as sfatulmedicului.ro or sfaturimedicale.ro address online gambling alongside traditional gambling and include it when discussing symptoms of gambling addiction and ways to overcome it. The website of a private medical clinic Regina Maria goes even further and dedicates a special section to this digital form, raising awareness that it can lead to severe damage to one's finances, relationships and professional activity.

When it comes to online gaming, occasional reports in the media of children or teenagers having spent significant amounts of their parents' money on in-game items, such as a 6 year old boy from Timisoara who spent 6000 RON on virtual weapons and perks (stiri.tvr.ro, 2019). However, children are not the only ones who can find themselves unable to resist this

temptation. PressOne (Olaru, 2021) presents the case of Lucian, a husband and father who became addicted to popular soccer game, FIFA. And his addiction was not limited to investing all free time in it, it also entailed investing significant amounts of the family money. In order to be able to perform well in FIFA, one must have very good players on their virtual team. However, the only way to get the best ones is to buy packs with random players, where there are very slim chances of getting the big soccer stars. This makes gamers keep buying more and more packs, as Lucian explains: "At first, I spent money, about 150 euros. I didn't get any good player. I had thought that if you pay money, the good players are guaranteed, you know? But they weren't. I opened 10-15 packs and I only got poor players". When he finally managed to get a good player, his addiction was only reinforced, as he struggled to stop spending family money on gambling for virtual goods. And if for an adult, overcoming loot box addiction is very difficult, addiction expert Eugen Hriscu declared within the same article that using this mechanic in games played by kids and teenagers *"It's like giving heroin to children, in a way. It's introducing the concept of gambling, of games of chance, at an extraordinarily early age"*.

## IV.   Quantitative analysis

An online survey regarding online habits and risks for young people was filled in by 83 participants, on a volunteer basis. The socio-demographic structure of the sample is as follows:

### 1.  Socio-demographic structure of the sample

**Age, gender and ethnicity**

The survey was responded by 48 women and 35 men, between the ages of 16 and 30. Most of the respondents were in the 23-26 category (34), while the fewest were aged between 16 and 18 (12).
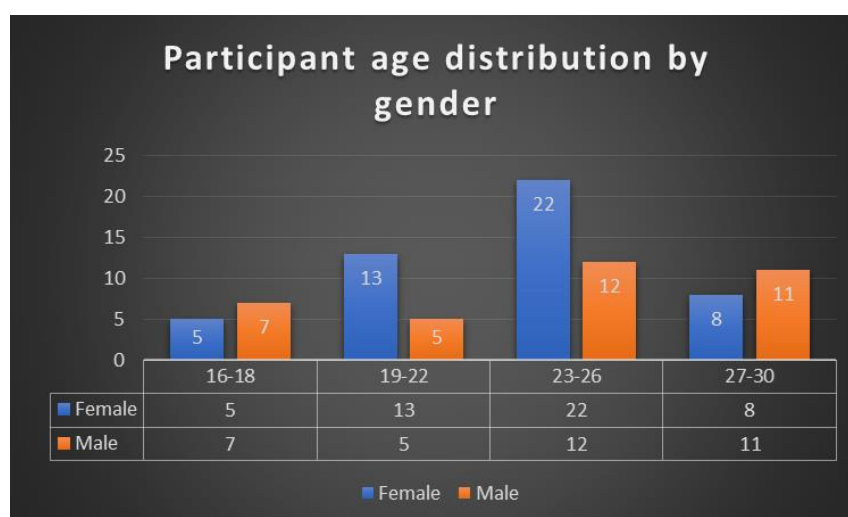


**Fig 3. Participant age distribution by gender**

Where ethnicity is concerned, with the exception of only a single Roma participant, all of the respondents were Romanian ethnics, which means that this category will be disregarded in analysis, due to complete homogeneity.

**Level of education**

The sample seems to be skewed significantly in favor of the highly educated, as over half of the respondents (48) have completed either University or postgraduate education. Only 7/83 participants have graduated elementary education or less and 28 of them have completed high school.
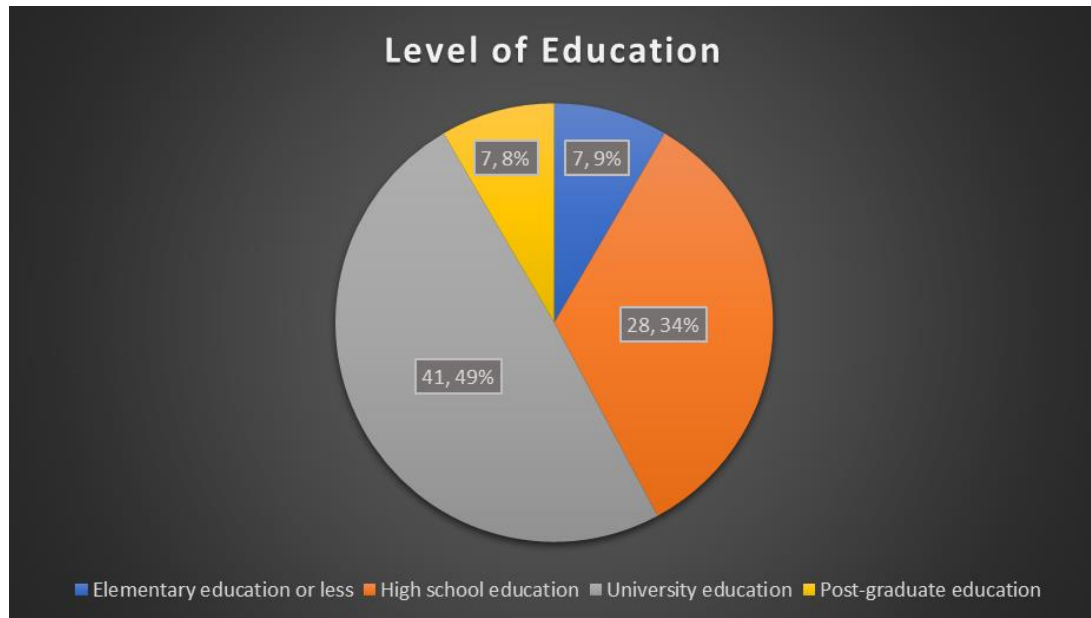


**Fig 4. Participant level of education**

**Occupational status and Levels of Income**

The overwhelming majority (88%) of respondents are either students (31/83) or employees (41/83). The remaining 11 participants are self-employed (2/83), stay-at-home parents (SAHP) (5/83) or unemployed (6/83). Due to this, in analysis, the self-employed were grouped with the employees under "employed" and the SAHP were grouped with the unemployed, under "not employed".
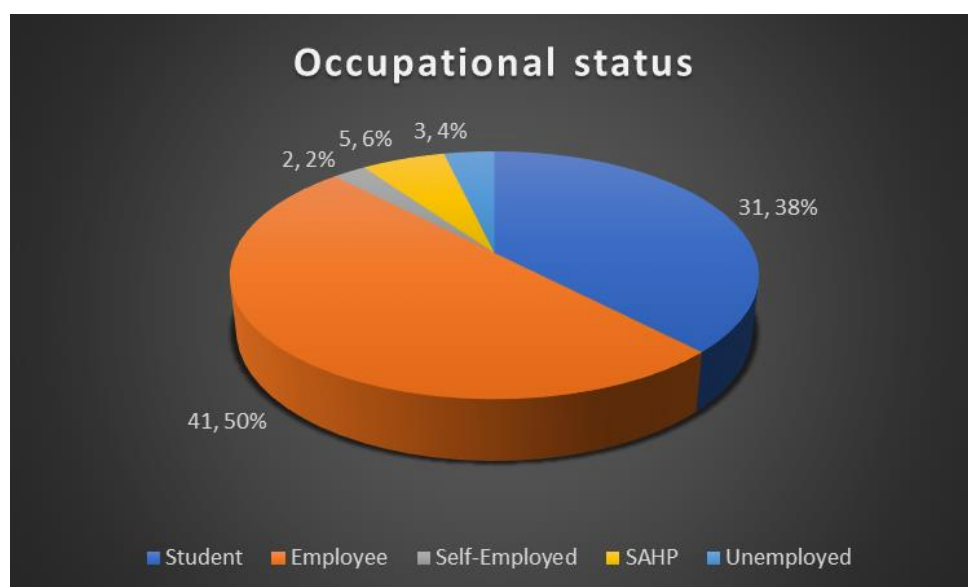


**Fig 5. Participant occupational status**

When it comes to household income for the first trimester of 2022, over half of the respondents (49/83) reported being slightly or significantly below the national average, almost one third of them (24/83) placed their income above the national average, while 12% (10/83) earned the national average. In order to simplify analysis and have sufficient units in each category, the "slightly" and "significantly" above, respectively below national average were grouped together in "above national average" and "below national average".
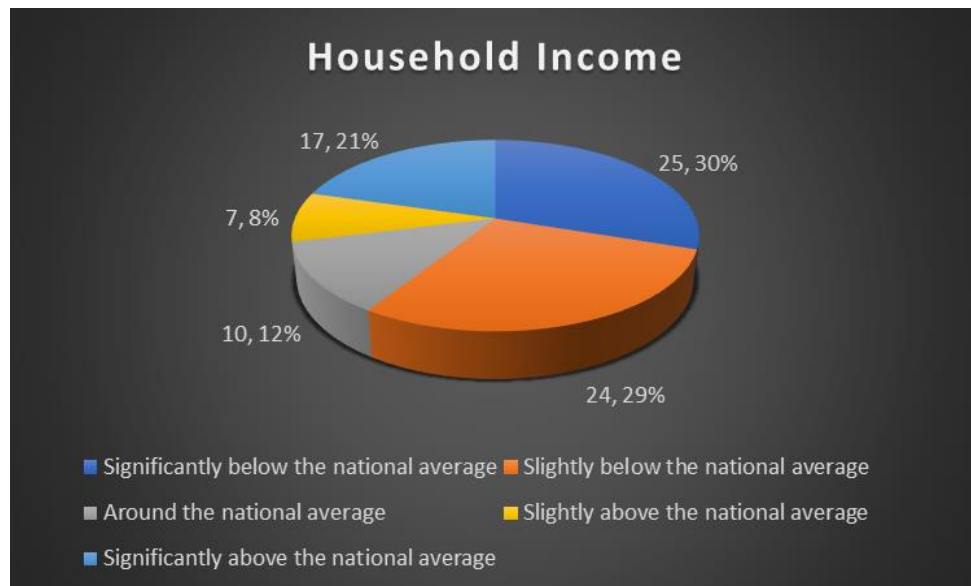


**Fig 6. Participant household income**

**Area of residence**

Most of the respondents (55%) live in an urban area, while the remaining 45% reside in a village. A quarter of all participants (21/83) live in a big city, while only 10 (12%) live in a small and medium city and 15 live in a town. In order to achieve more consistent categories, for the purpose of analysis, the area of residence was grouped in 3 major categories: rural area, small urban area and large urban area.
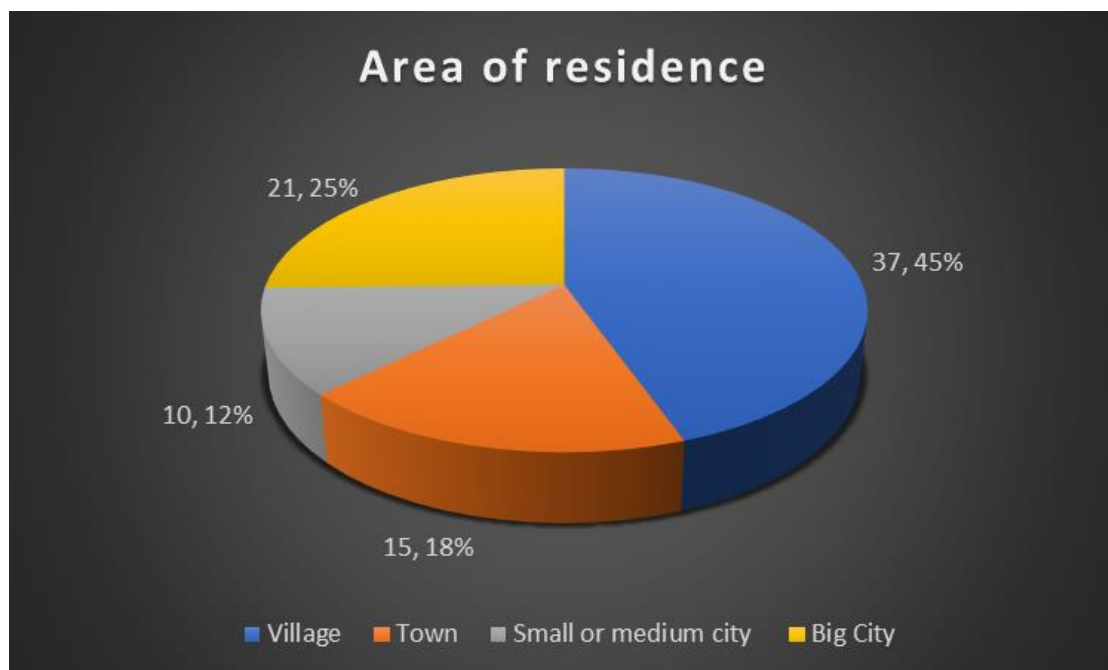
**Fig 7. Participant area of residence**

## 2. Internet use habits

With the exception of only 2 participants, who access the internet several times a week, all other 81 respondents access it daily, which means our entire sample is comprised of very frequent internet users. This means this variable will not be taken into consideration for establishing correlations, as it is shared by the entire sample. While online, the activities performed by the most respondents include watching movies or listening to music (73/83), looking up information and chatting with friends (72/83). The fewest participants use the internet to find friends or partners (6/83), to blog/vlog (4/83) or to gamble (1/83). None of the respondents reported engaging in online discussions in groups, forums, etc., which shows a lack of interest in debating and exchanging information with strangers.

When it comes to social media, all our respondents use it, but they access different platforms. Thus, the vast majority have Instagram accounts (74/83), almost 70% use Facebook, while only 27/83 use Tik Tok and under 10% (7/83) use Twitter. Given the fact that Twitter and Instagram are used by too few, and respectively, almost all respondents, they will be discounted from analysis as variables which might impact online risk.

## Fig 8. Participant internet use habits

**Online activities performed by responents**

- Gambling, 1
- Playing, 28
- Participating in educational programmes or working online, 32
- looking for friends/partners, 6
- Blogging/Vlogging, 4
- Shopping, 57
- Looking up information, 72
- Participating in online conversations in groups, forums, blogs,etc., 0
- Chatting with friends and family, 71
- Watching movies/listening to music, 73
- Reading news about politics/current events, 30
- Others, 11

Legend:
- ■ Gambling
- ■ Playing
- ■ Participating in educational programmes or working online
- ■ looking for friends/partners
- ■ Blogging/Vlogging
- ■ Shopping
- ■ Looking up information
- ■ Participating in online conversations in groups, forums, blogs,etc.
- ■ Chatting with friends and family
- ■ Watching movies/listening to music
- ■ Reading news about politics/current events
- ■ Others

**Social Media Platforms Use**

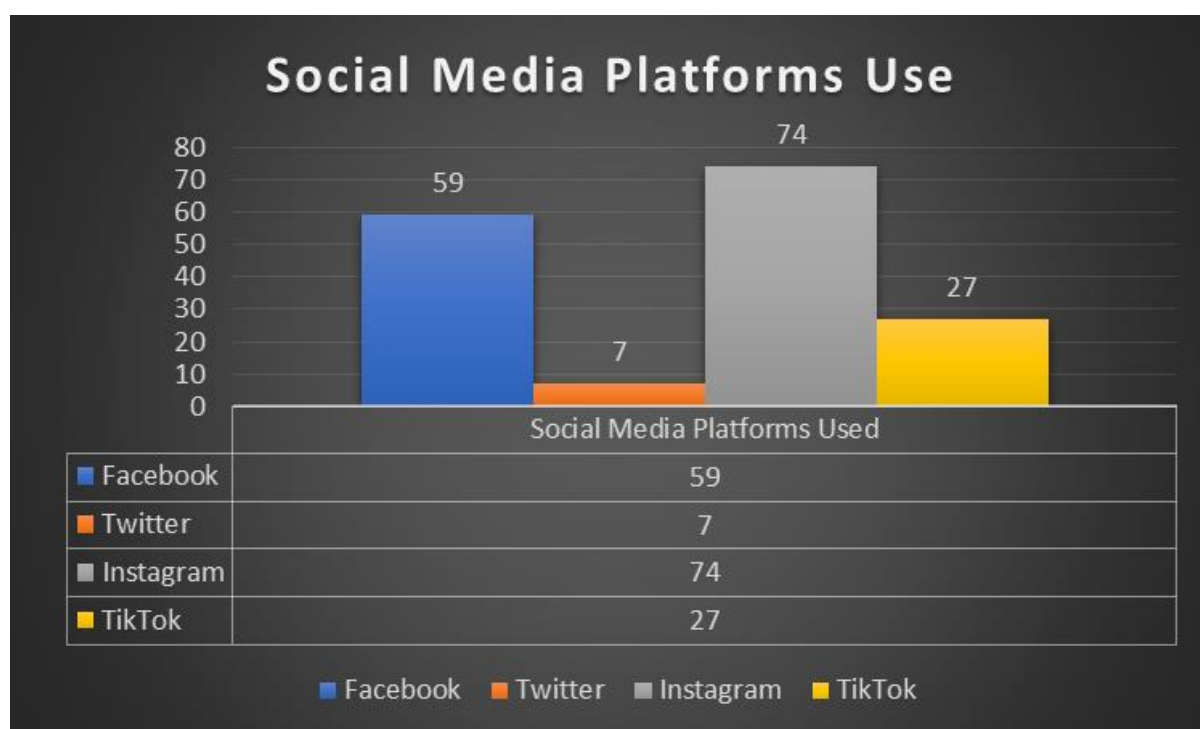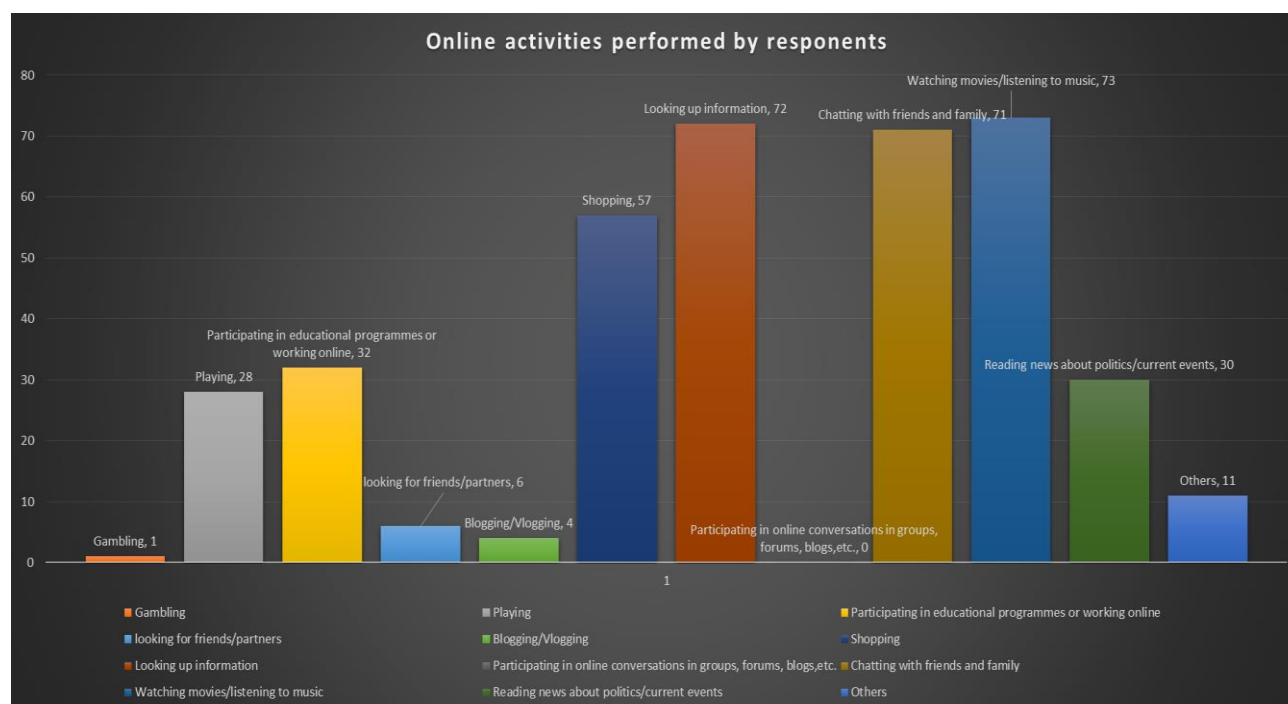| Social Media Platforms Used | |
|---|---|
| ■ Facebook | 59 |
| ■ Twitter | 7 |
| ■ Instagram | 74 |
| ■ TikTok | 27 |

■ Facebook ■ Twitter ■ Instagram ■ TikTok

Fig 9. Participant social media platforms use

Most respondents use social media and private messaging apps every day for interacting with others, both via public and private messaging. Private messaging is used more frequently than public conversation, being performed daily by 77% of respondents. Since there were quite few participants who reported interacting with others online less than once a week and less than

once a month, in order to achieve more consistent categories, they were merged for analysis into the category "occasionally".
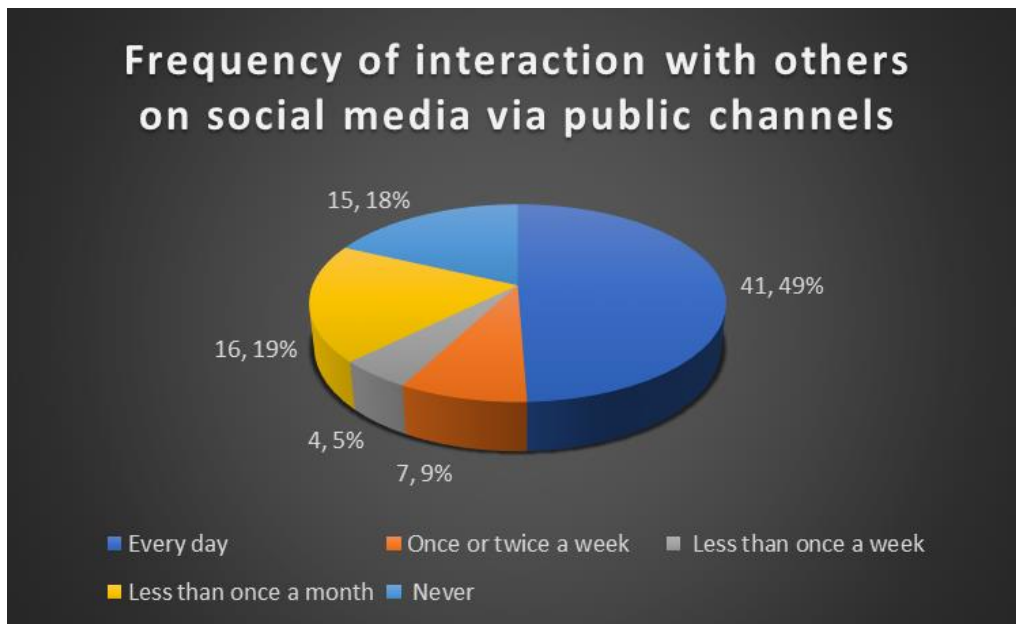


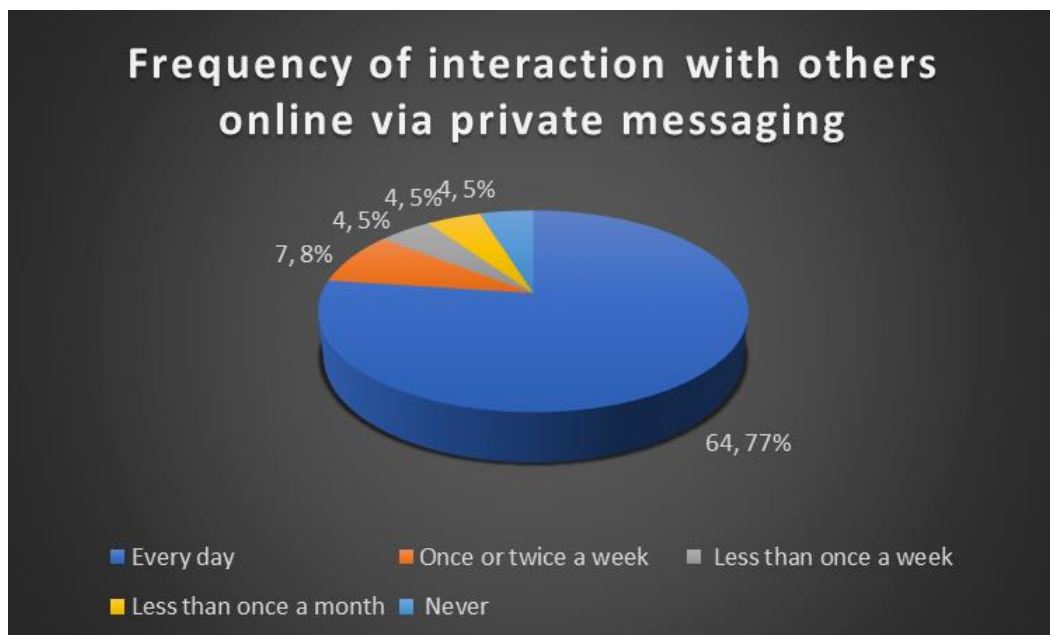**Fig 10. Participant frequency of interacting with others on social media via public channels**



**Fig 11. Participant frequency of interacting with others on social media via private messaging**

### 3. Information sources and practices

When asked to choose their top sources of information, most respondents selected social media networks, international and national news platforms, in almost equal proportion. The information sources used by the fewest respondents were friends, family or coworkers, local/regional news platforms and online chat groups or forums. This data shows that most

respondents are likely to be more susceptible to fake news distributed over social media than propagated by friends or family via messaging apps or by obscure local news sites.

Participants did not show great interest in keeping up with politics and local events, as less than 20% of them read news on these topics daily (16/83). The majority of the respondents only read the news occasionally (from once or twice a week to less than once a month) and 16% don't follow the news at all.
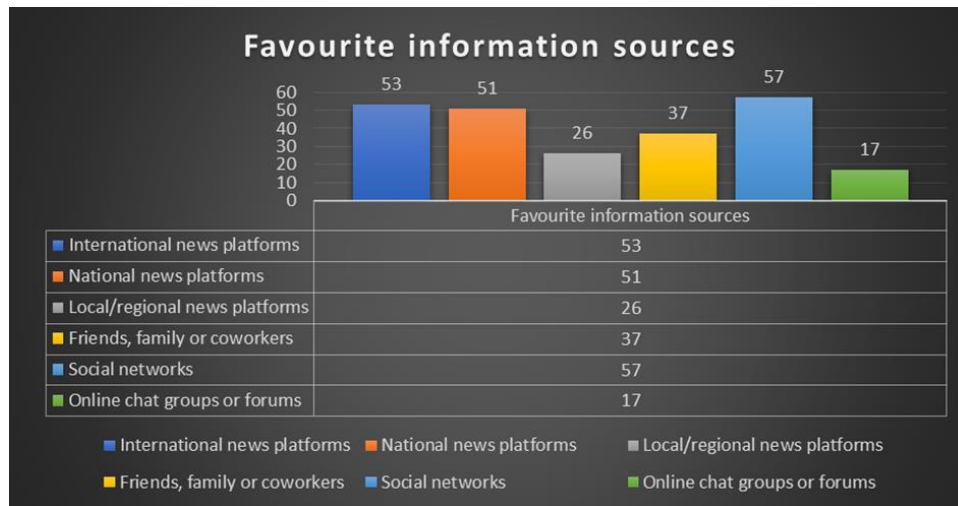


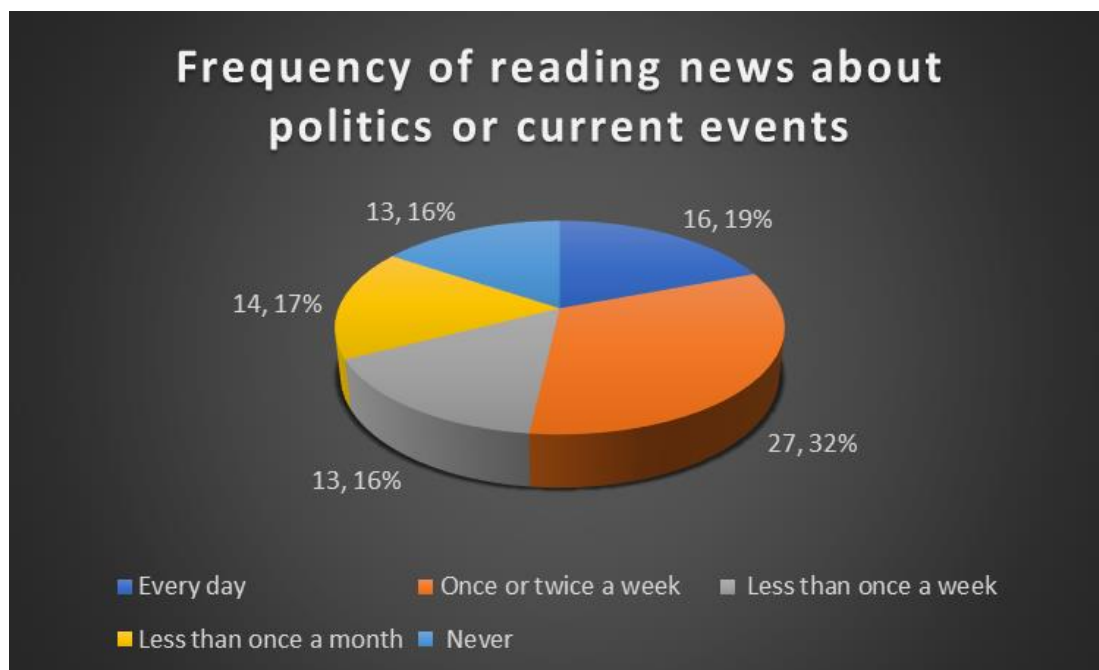**Fig 12. Participant favorite information sources**



**Fig 13. Participant frequency of reading news about politics or current events**

When reading the news, almost 60% (49/83) of respondents report reading the articles thoroughly, in their entirety. 34% of participants only read the title and the first paragraph of the text, while just 6 of them (7%) limit themselves to reading the title and looking at the main photograph. Since this last category included so few respondents, it was grouped for analysis with the second one, creating two main news reading thoroughness variables: Fully reading the article and Partially reading the article.
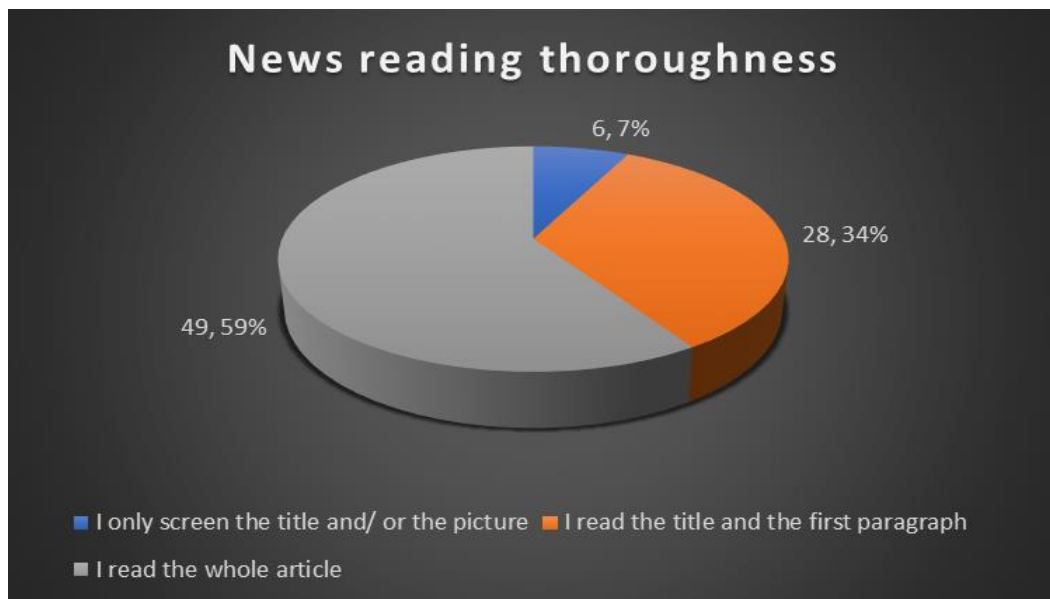
**Fig 14. Participant news reading thoroughness**

We tested the respondents for reading comprehension by asking them to read a short news fragment and then answer a few questions about it. In accordance with their scores, participants were grouped into 3 categories: high critical reading ability, medium critical reading ability and low critical reading ability. The majority of our respondents (48/83) exhibited medium critical reading ability, while a quarter (21/83) exhibited high critical reading ability and only 17% (14/83) exhibited low critical reading ability. This implies that most participants should be adequately equipped to be able to read and understand a piece of news and perform a basic critical assessment of its content.
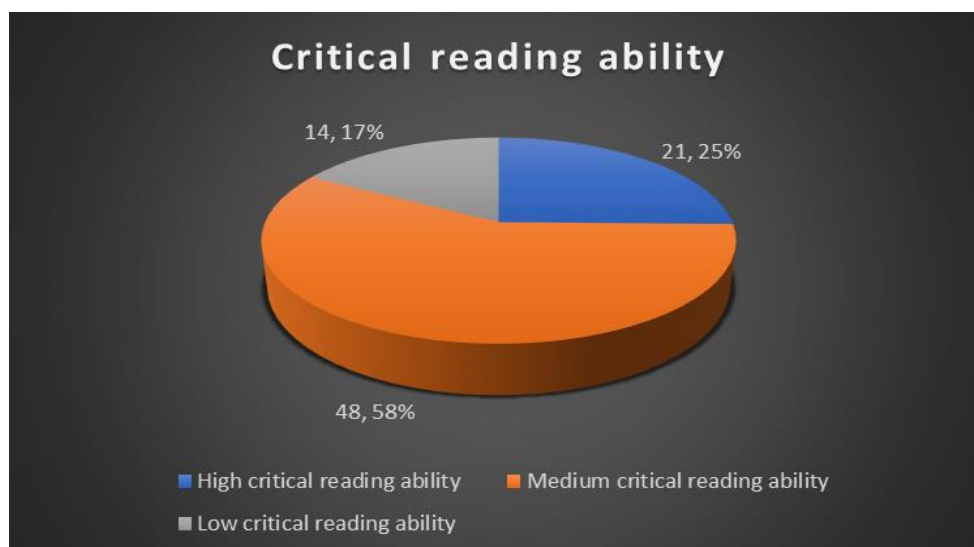


**Fig 15. Participant critical reading ability**

## 4. Cyberbullying, harassment and other adverse experiences

The majority of respondents (54/83) have never shared any kind of personal or intimate information online with people they had never met in real life. Out of the remaining 29 who

have, most have shared their identification data (14/83) and/or information about their location (18/83). Only 5/83 participants have shared information about their intimate or private life with strangers on the internet, while a mere 2 of them have shared intimate photographs or videos with people they had not met in person. While a greater proportion of participants (20/83) have indeed shared such photographs or videos with someone online, it was with people they knew in person and trusted.
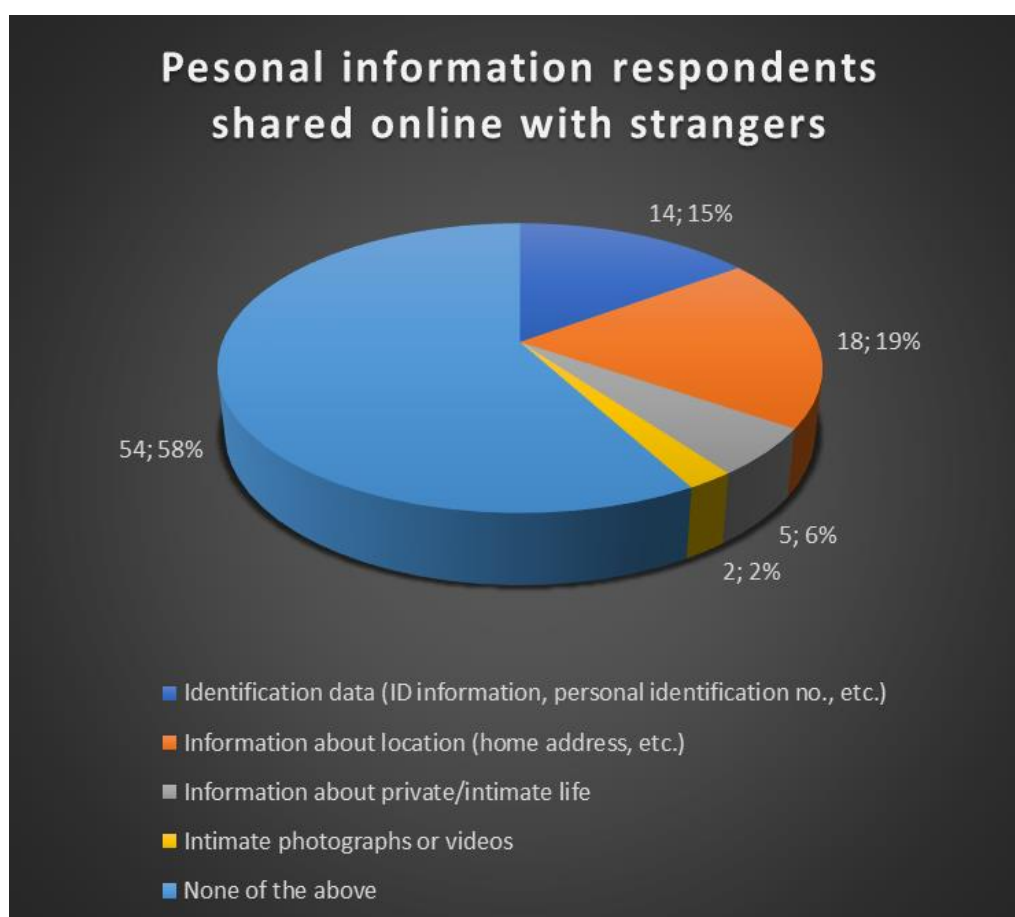


**Fig 16. Participant personal information shared online with strangers**

Given the fact that most respondents were very careful about sharing information online and rarely engaged in risky behavior from this point of view, it is not surprising that very few members of the research sampled have experience adverse events connected to online risks faced by young people online. The form of adverse experience most frequently encountered was online harassment or trolling, experienced by 9/83 participants. 6/83 participants received online threats and the same number were victims of identity theft. Cyberstalking was experienced by 4/83 respondents, while 1/83 was impersonated by another user. None of the young people in the research sample have experienced outing/doxxing or revenge pornography.

The very low incidence of adverse events associated with online risks facing young people experienced by respondents makes it impossible to make any relevant or meaningful correlations with participant characteristics, beliefs or behavior. Further research, on a larger sample of this population or specifically on population who has experienced such adverse

online events, is required in order to make such determinations. The only aspect which is relatively salient from this data is that participants who have shared at least one type of personal information online with people they have not met in person seem to be more susceptible to experiencing online harassment/trolling (6/9 cases) and cyberstalking (3/4 cases). However, since the number of total incidents is very low and the same does not apply for online threats or impersonation, it is difficult to say with any certainty that there is a causal relationship between online information sharing and experiencing cyberbullying.
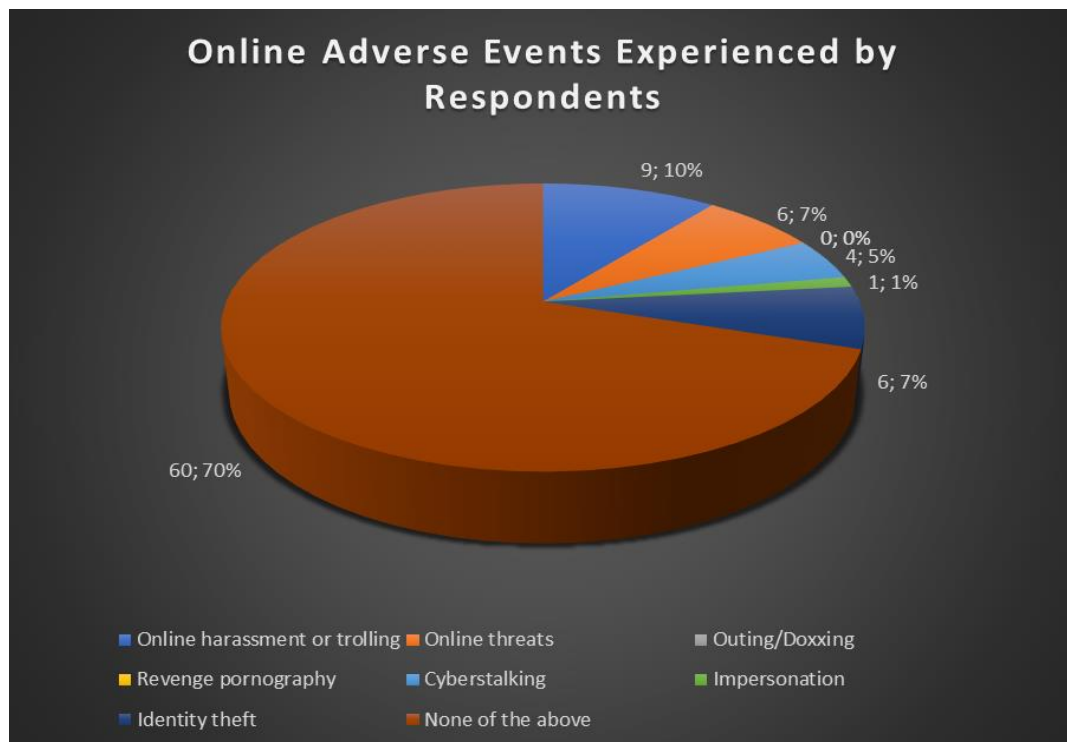


**Fig 17. Online adverse events experienced by participants**

There are two other major risks facing young people online, the risk of getting addicted to online gambling and the risk of being exposed to fake news. However, since almost none of the respondents in our sample engaged in online gambling (3/83 did so in the past 2 years, but only 1 still performs this activity online in the present), the risk which will be explored most in-depth in this analysis is that of being exposed to and believing fake news.

## 5. The Influence of Socio-demographic Factors on Agreement with Fake News

Since Fake News is a wide-spread phenomenon, with very serious consequences on public health, education, economy and politics, the present analysis will place specific focus on this particular risk which every young person going online is - to a smaller or greater extent - exposed to.

In order to determine which factors place a young person at a greater risk of fake news, we asked them to rate their agreement with a series of four statements, all representing misinformation frequently circulated in Romania. We selected statements related to the Covid

19 pandemic and vaccination, to the war in Ukraine, to Muslim immigrants and to global warming, in order to cover some of the most frequent subjects targeted by fake news.

While participant responses have varied significantly from one fake news example to another, showing differences in exposure and/or likelihood to believe misinformation on each topic, most respondents have not been susceptible to believing fake news and found them somewhat or highly inaccurate for each statement except the last one. The fake news regarding the crimes Ukraine was found the most inaccurate, probably due to the substantial media coverage of the war, the ongoing Ukrainian refugee migration to Romania and the emotionally charged nature of the issue. The fake news statement which obtained the greatest amount of approval was the one regarding global warming, which is an issue generally perceived as much more distant and theoretical. While in the survey, participants were presented with 5 rating options - highly accurate, somewhat accurate, neutral, somewhat inaccurate and highly inaccurate, they were grouped for analysis in 3 major categories - highly/somewhat accurate, neutral, highly/somewhat inaccurate - in order to give each category sufficient consistency, since there were too few responses for many of them, especially in the when it came to the highly accurate and somewhat accurate options, since the respondents were, overall, rather skeptical of the fake news.
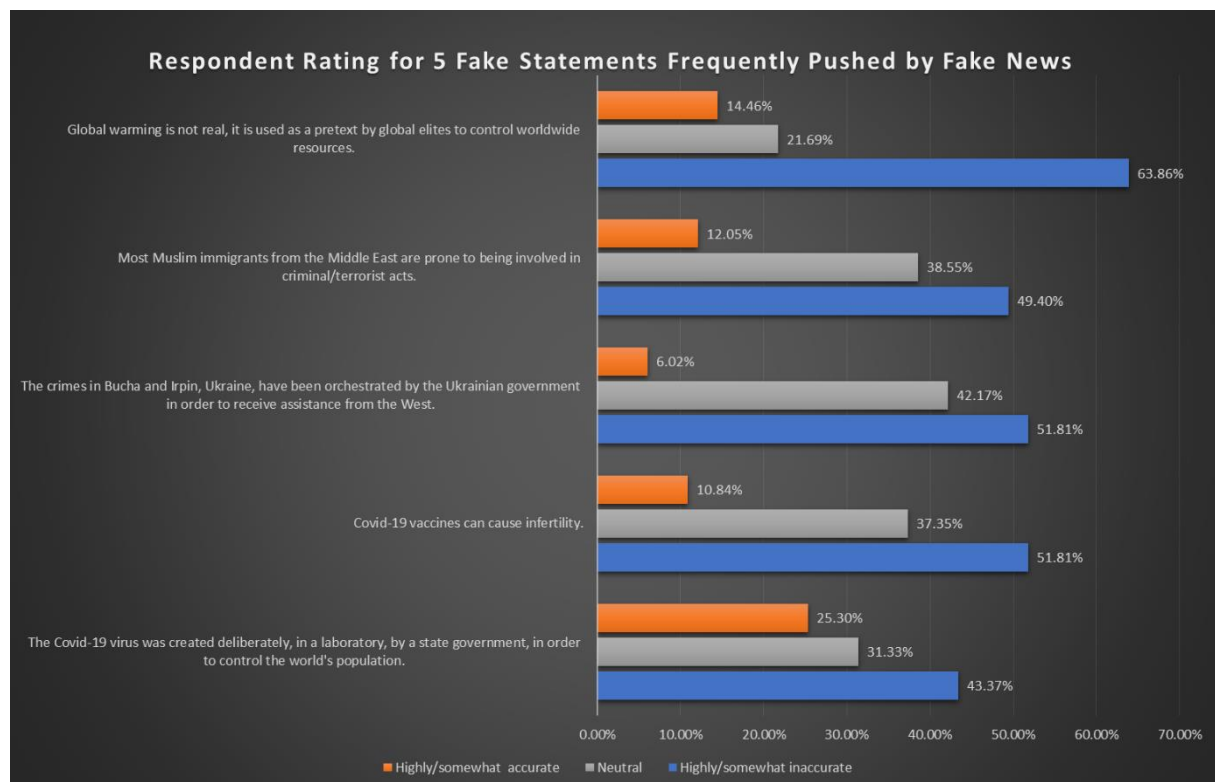


**Fig 18. Participant rating for 5 Fake Statements Frequently Pushed by Fake News**

Variations in the agreement ratings among statements, as well as the very low number of responses for some categories make it difficult to confidently pinpoint factors which influence susceptibility to believe fake news. In order to simplify analysis and to be able to identify such potential influences, an average has been made between the ratings provided for each statement, under each category. Thus, the overall Highly/Somewhat accurate category will be obtained by averaging the Highly/Somewhat accurate ratings for each of the 5 statements, etc. Then, the overall rating for each category will be converted to a percentage of the total ratings, making them easily comparable in spite of the fact that the number of respondents who have

selected each category varied greatly (so the absolute numbers did not provide significant information).

**Agreement with fake news by Age Group**

Given the fact that the respondents were all young, their assessment of the fake news statements did not vary greatly between the selected age groups. However, there was one notable difference between the 23-26 bracket and the others: respondents aged within this range were significantly more likely to consider the statements inaccurate, as their overall highly/somewhat inaccurate rating was 19 percentage points, respectively 16 percentage points higher than the other categories, while at the same time, their overall neutral rating was significantly lower (by 16 percentage points). This suggests that this particular age group might be more decisive when it comes to expressing their opinion or simply less susceptible to fake news.



| | Highly/Somewhat accurate | Neutral | Highly/Somewhat inaccurate |
|---|---|---|---|
| 16-22 | 15% | 41% | 44% |
| 23-26 | 12% | 25% | 63% |
| 27-30 | 12% | 41% | 47% |

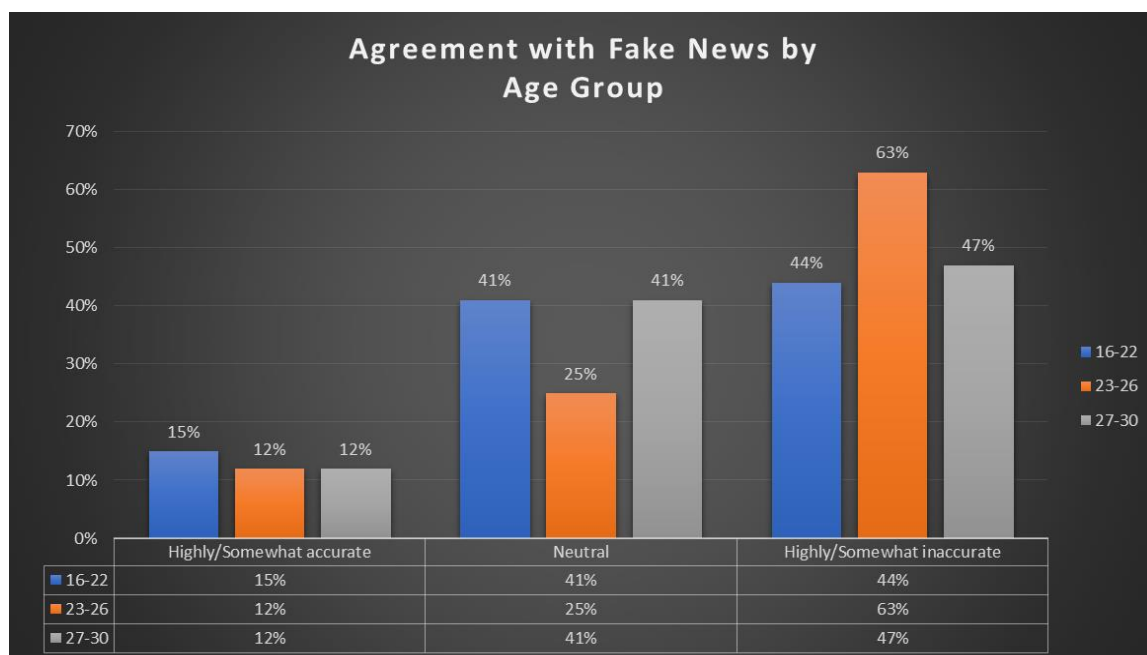**Fig 19. Participant agreement with fake news by age group**

**Agreement with fake news by gender**

No major differences have been identified between the agreement ratings of men and women within our sample. Only a small inclination for women to be more skeptical of fake news can be observed and that can be placed within the margin of error, as the difference is of only 3-4 percentage points.
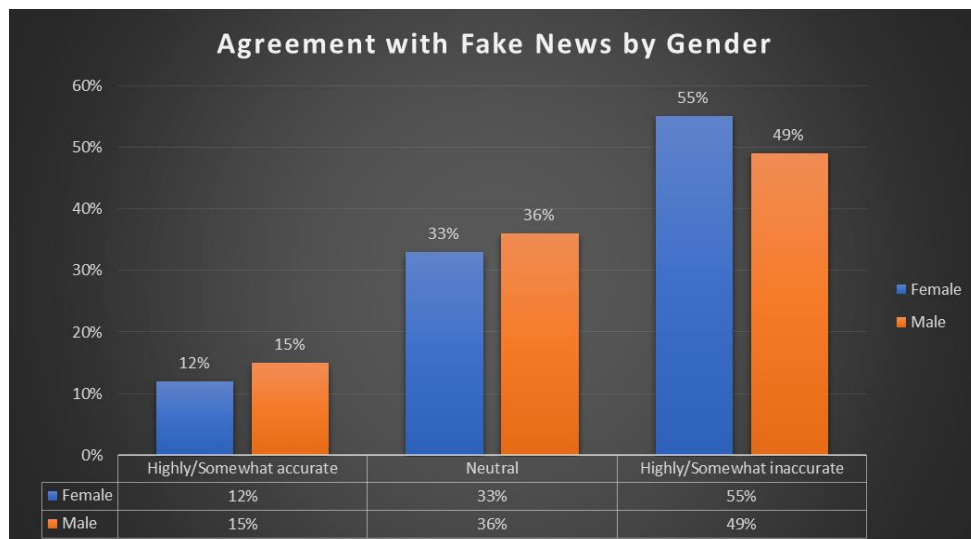
**Fig 20. Participant agreement with fake news by gender**

**Agreement with fake news by Area of Residence**

The respondents' area of residence seems to have a considerable impact on their rating of fake news statements. It appears that the larger the size of the settlement the participants dwell in, the more likely they are to find the false statements inaccurate. Thus, only 6% of residents from villages find them inaccurate, but 17% of those in small urban areas and 77% of those in large urban areas recognize them as such. In turn, respondents from rural areas are more likely to be neutral regarding the statements, with 15 percentage points above those in small urban areas and 29 percentage points below those living in big cities. However, it is not the people living in villages who most frequently rate the statements as highly/somewhat accurate, but those living in small urban areas. A hypothesis to explain these findings would be that people living in large urban areas have better access to high quality information, which makes them less susceptible to believing fake news.
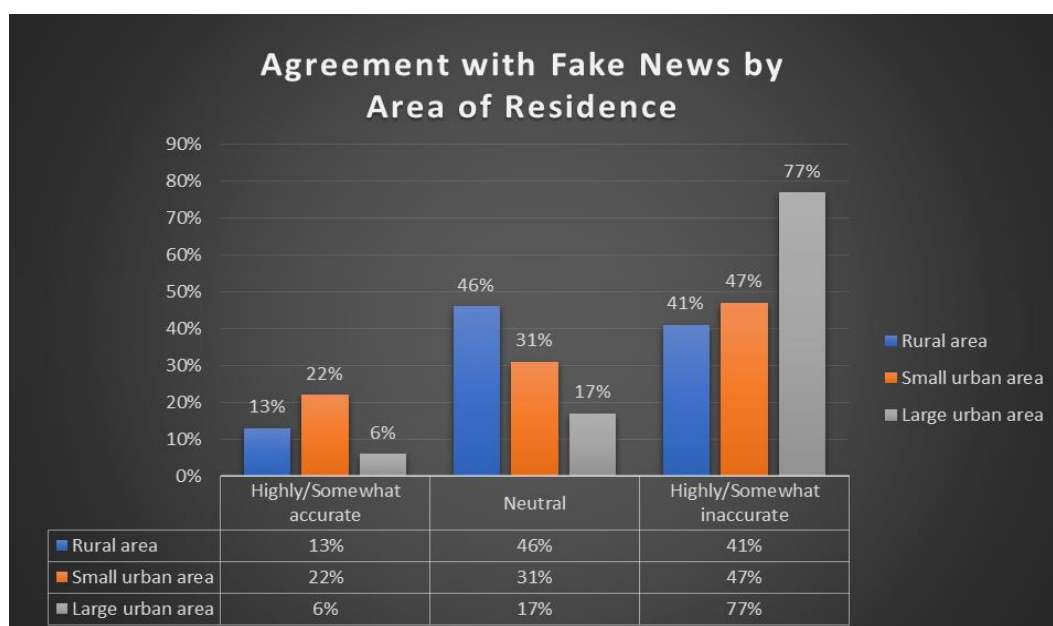


**Fig 21. Participant agreement with fake news by area of residence**

**Agreement with fake news by Level of Education**

As suspected, the participants' level of education seems to be a predictor of their likelihood to agree with the fake news statements. Thus, respondents who have attended university or postgraduate studies are 9 percentage points less likely to agree with the presented disinformation than those who have only graduated from elementary school or high school. At the same time, they are 12 percentage points more likely to consider the statements inaccurate. While the difference is undeniable, it is somewhat surprising that the gap in susceptibility to fake news is not higher, given that higher education is supposed to be a cornerstone of critical thinking development.



**Agreement with Fake News by Level of Education**

| | Highly/Somewhat accurate | Neutral | Highly/Somewhat inaccurate |
|---|---|---|---|
| High School or Lower | 19% | 36% | 45% |
| University or Higher | 10% | 33% | 57% |
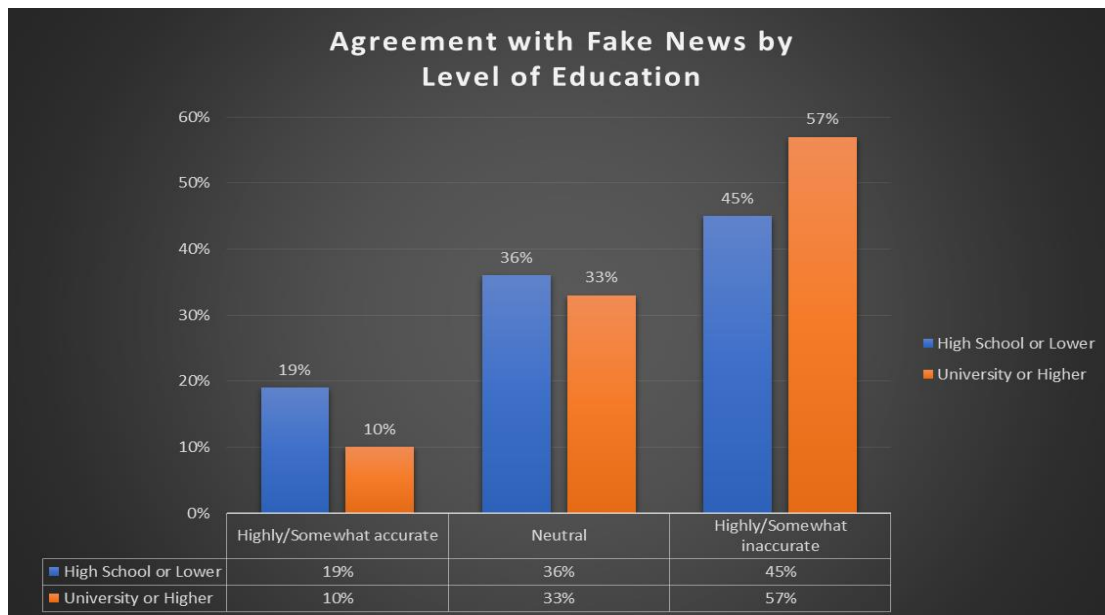
**Fig 22. Participant agreement with fake news by level of education**

**Agreement with fake news by Occupation**



**Agreement with Fake News by Occupation**

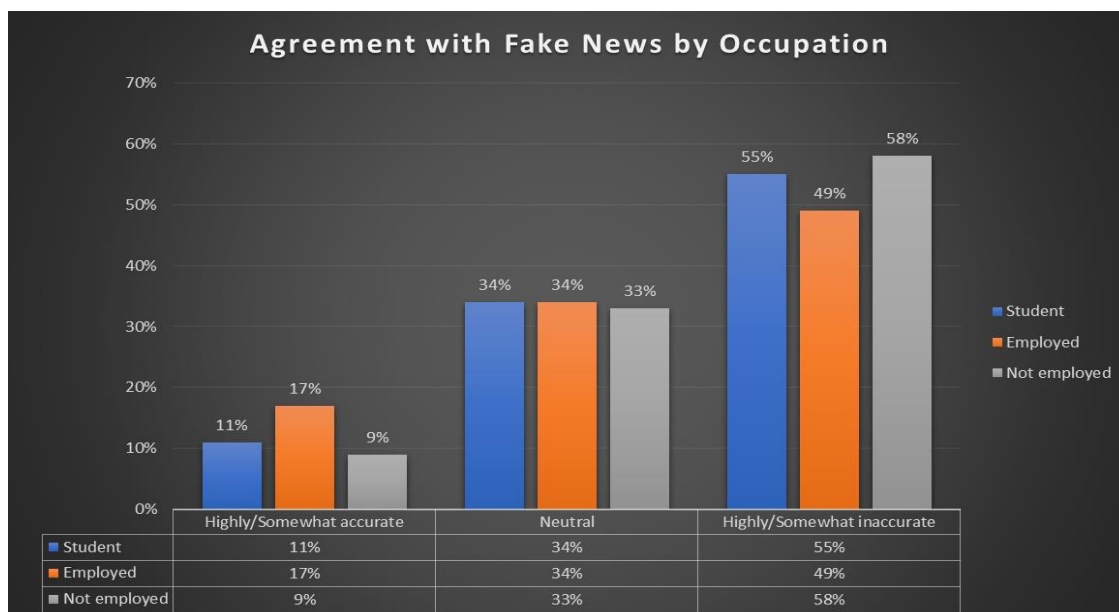| | Highly/Somewhat accurate | Neutral | Highly/Somewhat inaccurate |
|---|---|---|---|
| Student | 11% | 34% | 55% |
| Employed | 17% | 34% | 49% |
| Not employed | 9% | 33% | 58% |

**Fig 23. Participant agreement with fake news by occupation category**

Differences between students, the employed and the unemployed are rather small when it comes to agreement with fake news. While students and the unemployed have very close overall ratings (1-3 percentage points of difference), the employed stand out as slightly more likely to find the false statements accurate (by 6, respectively 8 percentage points) and slightly less likely to find them inaccurate (by 6, respectively 9 percentage points). However, all 3 occupational categories are almost identical when it comes to neutral responses.

**Agreement with fake news by Household Level of Income**

Differences between the likelihood to agree with the fake news statements are small between the respondents whose household income for the first trimester of 2022 was below the national average and those whose is around that amount. However, there are notable discrepancies between them and participants whose household income was above the national average during the same period. Namely, while the previous two income categories agree with the false statements in a proportion of 17%, respectively 22%, only 4% of the latter category do the same. At the same time, those having a household income above the national average are significantly more likely to consider fake news inaccurate, than their poorer counterparts.

The main hypothesis generated by these findings is that people with a higher level of household income are also likely to have higher levels of education and to afford better access to high quality sources of information. That is why respondents who have a household level of income above national average are better at identifying fake news as such.



**Agreement with Fake News by Household Level of Income**

| | Highly/Somewhat accurate | Neutral | Highly/Somewhat inaccurate |
|---|---|---|---|
| Below national average | 17% | 37% | 46% |
| Around national average | 22% | 32% | 46% |
| Above national average | 4% | 29% | 67% |
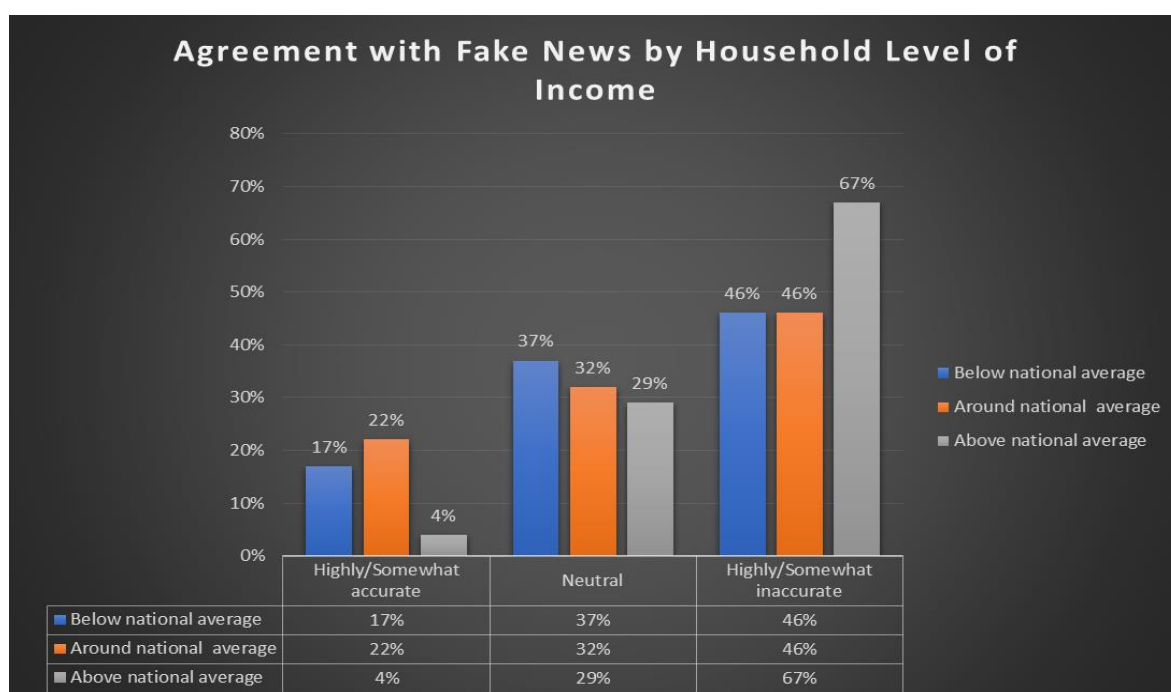
**Fig 24. Participant agreement with fake news by household level of income**

**Agreement with fake news by Frequency of Reading News About Politics/Current Events**

Differences between respondents who read news about politics/current events daily or every few days and those who do so weekly are rather small and they are identical when it comes to the proportion who find the fake news statements inaccurate (58%). However, those who are not in the habit of staying up to date with events, such as participants who only read the news once a month or less, are far less likely to find the false statements inaccurate than the rest

(by 19 percentage points) and also far more likely to be neutral about these issues (by 13, respectively 19 percentage points). Respondents who read the news daily or every few days are the least likely to find the fake news accurate, so it appears that being up to date with the news about politics and current events can function as a protective factor against misinformation.
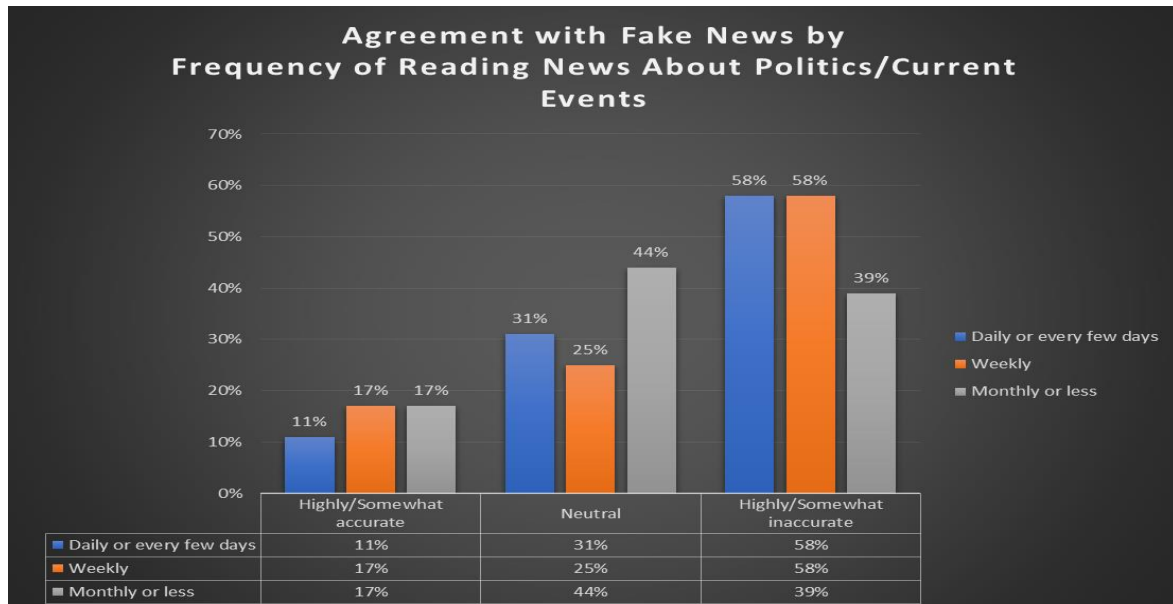


**Fig 25. Participant agreement with fake news by frequency of reading news about political/current events**
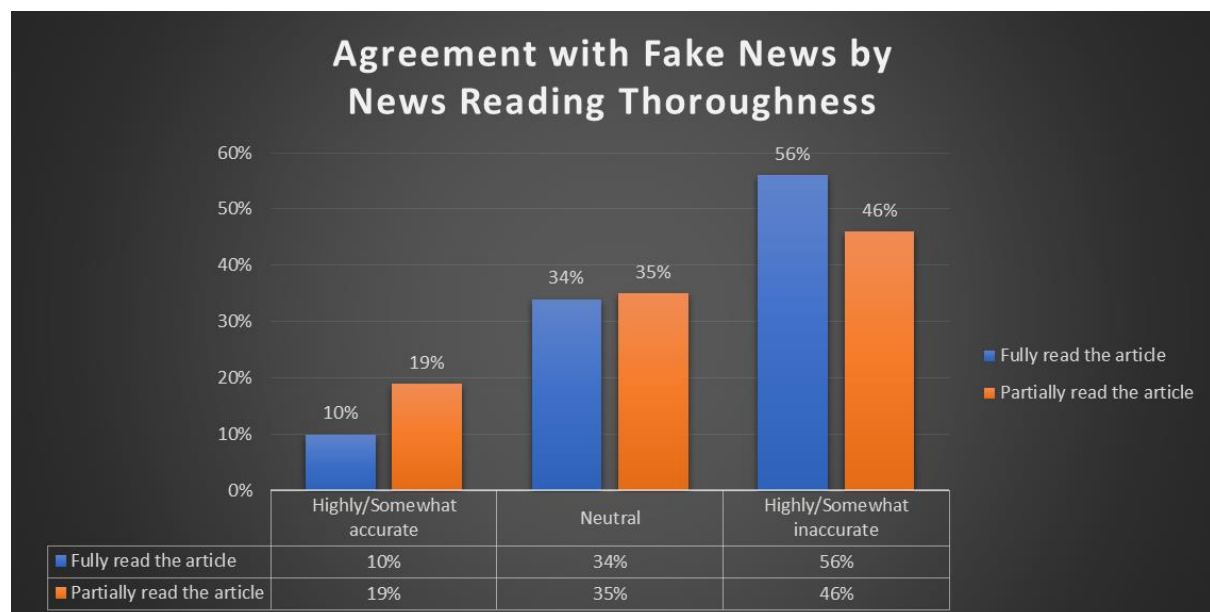


**Fig 26. Participant agreement with fake news by news reading thoroughness**

**Agreement with Fake News by Thoroughness in Reading the News**

While it would be expected to find considerable differences in agreement with fake news between respondents who are accustomed to reading the entirety of a news article and those who only skim through it or limit themselves to reading the title, the variance is rather small. Those who read the entire articles are indeed less likely to find the fake news accurate and more likely to find them inaccurate, but only by 9, respectively 10 percentage points, while they

are almost identical (1 percentage point difference) when it comes to declaring themselves neutral regarding the false information presented.

**Agreement with Fake News by Critical Reading Ability**

As it is probably to be expected, respondents with a high critical reading ability are more likely to find the fake news statements inaccurate than those with medium such ability and far more likely to do so than those with low critical reading ability. They are also less likely to remain neutral when faced with misinformation than the other two categories. At the same time, respondents with a low critical reading ability are 7 and respectively 8 percentage points more likely than the other two categories to agree with the false statements. Thus, reading comprehension and critical thinking seems to be a factor in protecting young people from fake news, but to a more limited extent than anticipated, given the findings in literature, which can be a result of the sample effect.

**Agreement with Fake News by Online Information Sources**



| | Highly/Somewhat accurate | Neutral | Highly/Somewhat inaccurate |
|---|---|---|---|
| High critical reading ability | 13% | 27% | 60% |
| Medium critical reading ability | 12% | 37% | 51% |
| Low critical reading ability | 20% | 36% | 44% |
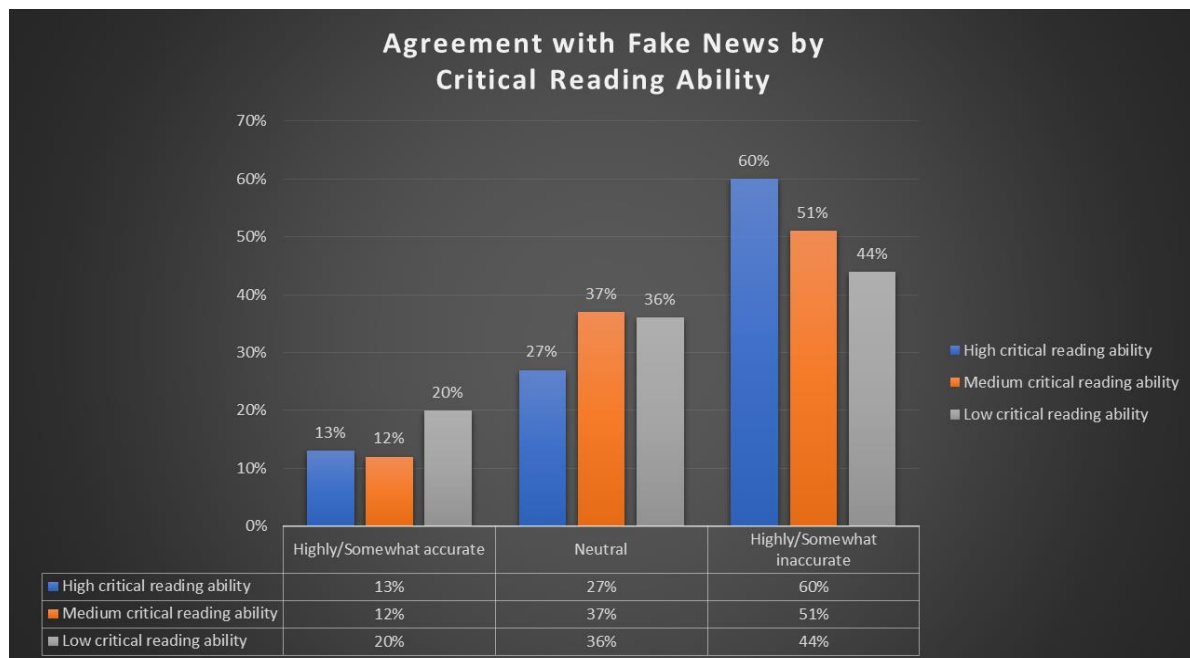
**Fig 27. Participant agreement with fake news by critical reading ability**

The top picked source of information about politics and current events (by 57/83 respondents) was social media. However, when it comes to rating the fake news statements, there were no notable differences between participants who selected this as part of their top sources of information and those who did not, which means it is likely that social media, as a whole, is similarly informative (or misinformative) as other sources, such as online news platforms. Another possible explanation is that social media platforms are simply a reflection of the news shared on them from other sources, such as media platforms.
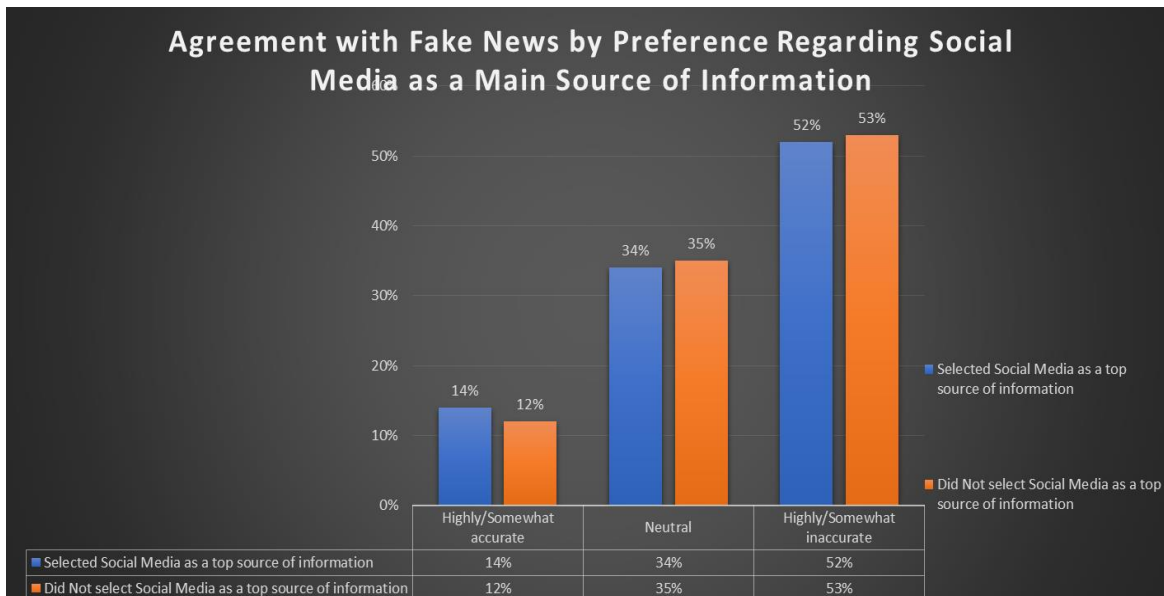
**Fig 28. Participants' agreement with fake news by main source of information (online chat groups)**
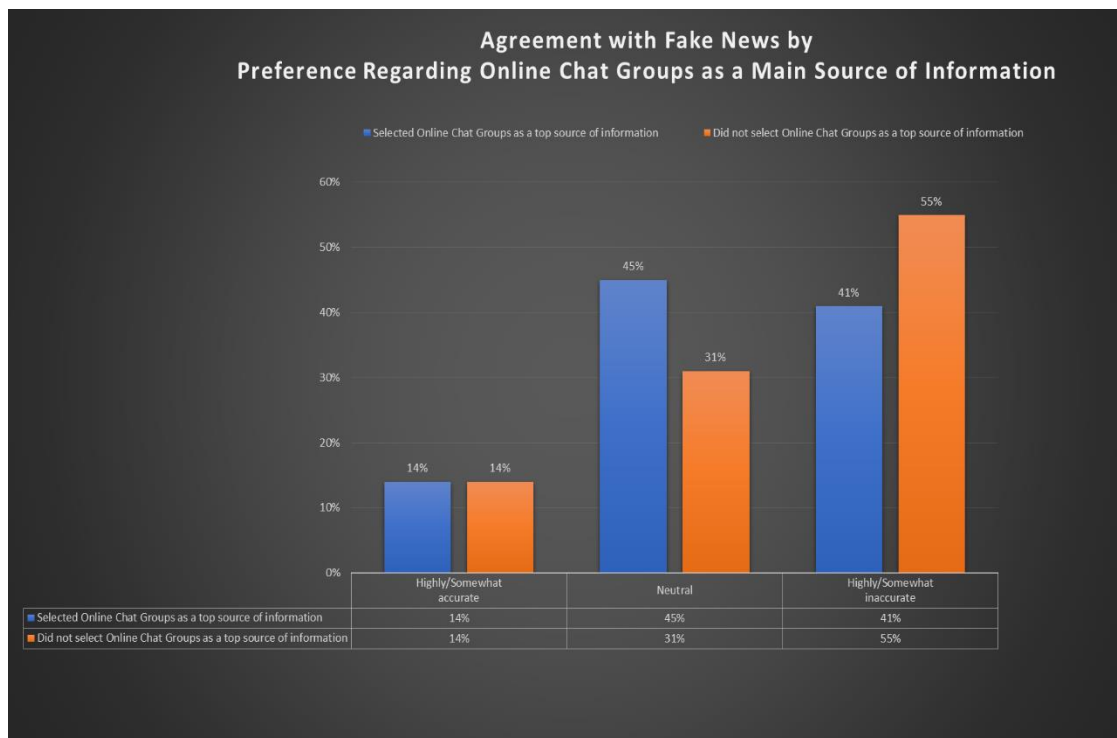


**Fig 29. Participant agreement with fake news by main source of information (social media)**

The least chosen source of information, selected by only 17 respondents was online chat groups. Here, using this source seems to be rather detrimental to its users, as many of them are significantly less likely to find the fake news statements inaccurate than those who do not use this source (by 14 percentage points). One potential interpretation for this finding is that online chat groups are not moderated by an administrator and they are likely to become echo chambers of fake news.

When it comes to specific social media platform use, the responses are somewhat paradoxical. While more of those who use Facebook and TikTok are inclined to deem the fake news statements inaccurate (by 16 percentage points in both cases) than those who do not, slightly more of these respondents are also inclined to find the false statements accurate (by 2, respectively 7 percentage points). In both cases, significantly fewer Facebook and TikTok users are neutral regarding the fake news statements (by 14, respectively 9 points), which indicates that social media participation might increase active engagement with current issues. An explanation for the ambivalence of these results could be that the quality of information found on social media varies greatly with the type of bubble the user is in, which has a decisive impact upon the type of contact that the user is viewing. Also, the use of online social networks in themselves does not seem to be a relevant factor in regard to the likelihood to believe in fake news.



**Agreement with Fake News by Facebook Use**
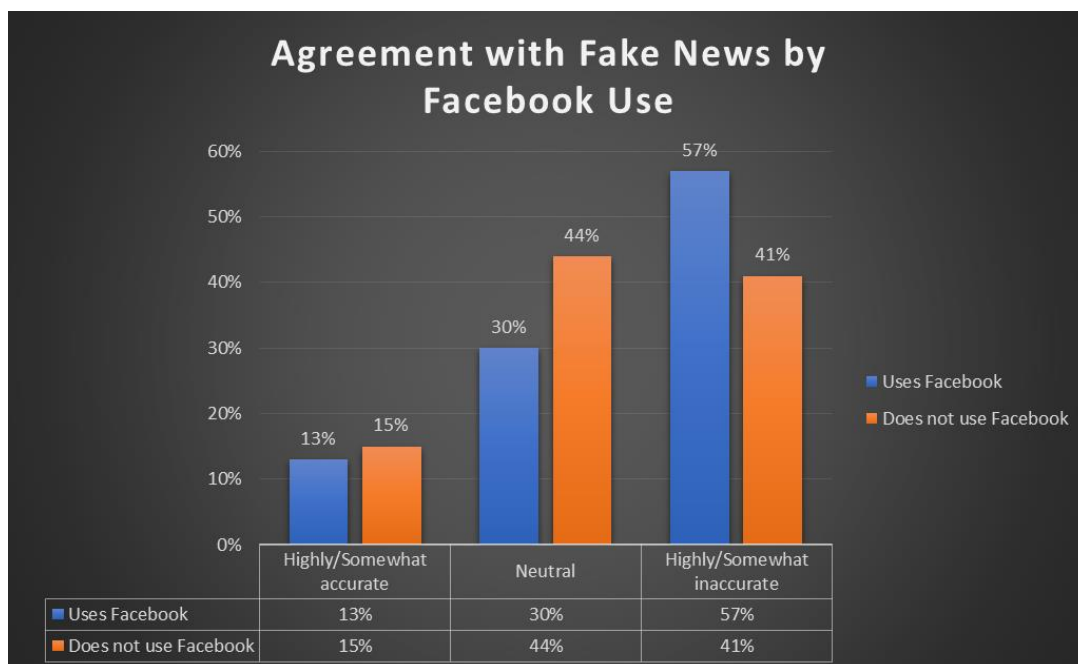
|  | Highly/Somewhat accurate | Neutral | Highly/Somewhat inaccurate |
|---|---|---|---|
| Uses Facebook | 13% | 30% | 57% |
| Does not use Facebook | 15% | 44% | 41% |

**Fig 30. Participant agreement with fake news by Facebook use**

**Agreement with Fake News by TikTok Use**

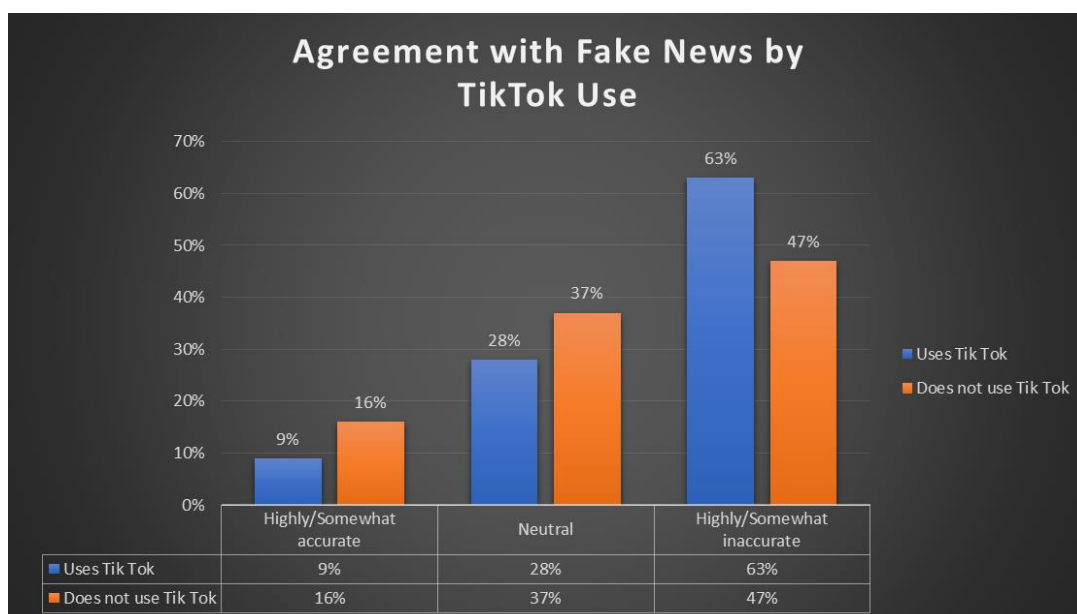| | Highly/Somewhat accurate | Neutral | Highly/Somewhat inaccurate |
|---|---|---|---|
| Uses Tik Tok | 9% | 28% | 63% |
| Does not use Tik Tok | 16% | 37% | 47% |

**Fig 31. Participant agreement with fake news by Tik Tok use**

**The Influence of Psychological Factors on Agreement with Fake News**

The only psychological factor tested for in this survey was the level of anxiety caused by the Covid 19 pandemic, respectively by the War in Ukraine. According to relevant literature, a higher level of anxiety should lead to higher levels of agreement with fake news. However, our sample contained very few participants who reported high levels of anxiety (only 3/83 for Covid-19 and 12/83 for the War in Ukraine). Thus, they were merged, for consistency, into the "somewhat anxious" category. Paradoxically, those who reported no anxiety over the events were more likely to find the fake news statements inaccurate and a smaller proportion of them were inclined to find the misinformation accurate. This difference is greater in the case of Covid 19 anxiety, which could be attributed to the fact that the pandemic had already ended in Romania and the memory of its anxiety could have faded away from people's minds, while the War in Ukraine is ongoing and pressing to the population. Thus, there are insufficient highly anxious respondents to influence the proportions, but as the number of such respondents grows within the sample, the proportions could become reversed. Further research is needed in this matter.

All things considered, this mostly exploratory analysis helped create a tentative profile of the young persons who are the most exposed to the risk of fake news on the internet. They are 16-22 years old, they live in small urban areas. They have graduated from elementary school or at most from high school, they are employed and their household income level is around the national average. They are uninterested in reading news about politics or current events and only do so monthly or less. When they do, they skim through the article rather than reading it in its entirety and have low critical reading skills which prevents them from understanding it properly. When it comes to sources of information, they tend to turn to online chat groups instead of reading articles on social networks, such as Facebook or TikTok, which they likely use primarily for other purposes (e.g. entertainment). Further research is needed into

establishing their psychological characteristics and whether their anxiety influences their susceptibility towards misinformation and to what extent.

# V.  Analysis of the qualitative data

Ten interviews were conducted with youth workers and trainers with vast and diverse experience in working with young people of different ages, locations and socio-economic backgrounds, in order to gain a better understanding of the online behavior of youth in Romania. The professionals interviewed were also consulted on the manifestation of the risks associated with use of internet by young people and potential measures for preventing and mitigating these risks and the educational needs of young people in this area.

## 1.  Online behavior of young people

Most interviewees consider that, when going online, teenagers are primarily interested in social media and playing online games. They generally spend their time on social media, talking to their peers and sending messages, as well as watching videos, YouTube and TikTok. They also access Instagram, Snapchat, to a lesser extent, Reddit and Facebook, the last being seen as more of a platform for older users. They also play online games in a network and watch others playing games or for finding new friends. Young people also use social networks to follow vloggers/ bloggers and influencers. The use of internet as a tool for searching information or following the news on current events and politics is significantly less common and often done by those over the age of 24-25.

Picture and video content is most likely to be accessed by young people, while written content is "out of fashion." (Claudia, university professor).

Overall, the professionals interviewed think that the young people nowadays spend too much time online, from an early age and without any boundaries or education:

*From the age of 13-14 young people start having smartphones. There are few boundaries or education on how to behave while using the phone to go online. (Claudiu, youth trainer)*

*They post on Facebook from morning until the night. They post everything they do there. (Gabriela, vocational trainer)*

Overall, the main drivers of youth activity online seem to be related to the need of young people to socialize with other young people, become famous and meet the social norms promoted by the online influencers.

*The vast majority of young people would like to become influencers and make money from this. (Claudia, University Professor).*

*We also have a young man who has become famous, he's a youtuber. The most dangerous thing, I think, is the time spent on the internet and the illusion that the people you talk to on the internet are your friends. (Mila, Youth counselor)*

## 2.  Impact of the Covid-19 Pandemic

As expected, the vast majority of the professionals interviewed think that young people spent more time online during the Pandemic, as virtually all social activities became virtual during

that time[1]. Teenagers and young adults started to spend around 7-8 hours in front of the screen each day, while attending classes, doing homework and socializing with their peers. Some mentioned that during the pandemic, young people often spent time online unsupervised by their parents. For young people living in child protection centers, internet became their only contact with the outside world, during that period, as their campus was quarantined. This increased internet and especially social media use has left young people even more vulnerable to online threat.

*During pandemic they used social networks much more than before. Thus, children have become even more vulnerable in the absence of the necessary resources that they should receive from school in order to defend themselves. (Andrada, activist)*

Increased screen time was not the only relevant change upon youth online behavior, in addition to being permanent since young people continue to be present online all the time. Some of the professionals interviewed consider than this has also determined other changes, such as the lowering of the age at which children start going online and the decrease in the ability of young people to focus for longer time.

*The average age at which children start using the internet has dropped significantly. There are children who have social media accounts by the age of 8. (Claudia, Children's safety center coordinator)*

*Young people are much more present online than before the pandemic. It seems to me that their mental health was affected also. The fact that they spend a lot of time on TikTok limits their ability to focus on something for more than a few minutes. We see this in trainings all the time, we have to make things much shorter and diversified. (Diana, youth trainer)*

*Some studies show that show that even tik tok clips are not fully watched. They are approx. 15 seconds long, but they [young people] only watch 3 seconds. (Claudia, Children's safety center coordinator)*

Some argue that the level of education which students receive from school has also decreased during the pandemic, in addition to lacking information about safe internet use. This has been aided by the increased physical distance between teacher/ professor and student during the educational process.

*At first, all students had their cameras on, they were excited and participated in the lesson, as if they were in class, but after several weeks they had a screen full of letters and there was no way to force them to open their cameras. (Andreea, Hight school teacher)*

*I think the collapse of the quality of education offered by the education system has accelerated [during the pandemic]. Many have complained that teachers gave up on their responsibility regarding the lessons that they teach and the bond they must foster with the student. Previously, there used to be some discipline in the learning process, but when the lessons moved online, there was a wave of complete disinterest […] An online course needs to be adapted, in order to be much more interactive. (Eugen, psychiatrist)*

Another change in the online behavior of youth, pointed out by some of the professionals working with them refers to the emergence of online communities hidden from the eyes of the parents and educators. These communities are often the space for the manifestation of the risks associated to youth internet use, such as cyberbullying, online gaming/ gambling and revenge porn.

---

[1] One person argued that the time spent online during the pandemic has not increased as young people were always going online from their phones also before the pandemic.

*It seems to me that, especially during the pandemic, there has been a lot of socializing online and that young people tend to access more [online] spaces that are inaccessible to parents. They don't use Facebook or whatsapp so much anymore. Meanwhile, online gaming communities have become extremely popular. And things can get extremely problematic there, as they may allow bullying, trolling etc. (Eugen, psychiatrist)*

*During the pandemic […] was when we started hearing about Instagram accounts such as "fete cuminți" ("good girls") where images of revenge porn and child pornography were being posted. (Andrada, activist)*

Last, but not least, the pandemic has also played a role in lowering the level of wellbeing in youth, most likely making young people even more prone of seeking opportunities to socialize and gain acceptance from their peers.

*Depressive symptoms have increased greatly. The stimulation given by the online environment is empty stimulation. It's a mental stimulation, but the body is not stimulated. (Eugen, psychiatrist).*

## 3. Cyberbullying

According to respondents, cyberbullying and harassment is one of the most online risks that manifests most often for young people. Some say that such incidents happen every day, based on the social media profiles of the young people that they are in contact with, while others estimate that approx. 60% of young people have had this experience at least once.

When it comes to the reasons for cyberbullying, experts argue it has to do with young people's need for social competition and acceptance, as well as emotional validation, in a time when artificial standards of perfection and happiness are being promoted by social media:

*Low self-esteem, dependence on the opinion of others - often other young people. It's about personal validation, acceptance. They don't necessarily think about the consequences, even if they have the ability [to envision the consequences], they don't necessarily choose to do good (Andreea, High school teacher)*

*There is also a lot of pressure online to live an ideal life and that puts a lot of pressure on their mental and emotional health to meet that standard. What they post online is often not who they really are offline. (Diana, Youth trainer)*

The lack of education regarding the risks associated with the use of internet and the potential legal consequences, is also cited as a factor leading to the proliferation of cyberbullying.

Youth workers point out that there can be two categories of perpetrators of cyberbullying and we should be aware of them. One is that of trolls, which are fake accounts that spread online information, spam and harassment, while another is that of real people who attack and harass others, just like in the classical form of bullying, but it happens online. In the online, "the circle of bullying may become a little wider than in a regular classroom" (Ariana, Representative of Student Association).

Last but not least, individual factors, such as the need for attention and reluctance to new things can also come into play.

*It is important to understand the profile of people who do this, people who are not tolerant of the new, they need attention and is not being offered to them, they do not see the effects of*

*their actions. They find someone different and harass him/ her. (Claudia, Coordinator of children's safety center).*

## 4. Fake news

When asked about news reading, most professionals working with youth argue that young people – especially those until the age of 21 are generally not following the news on current and political events closely. They are most likely to read news about sports (especially boys), about lifestyle and pop stars or about events that affect them directly.

Alternatively, they may read news that are shared online by their contacts. The problem is that sometimes they also take up the opinion of the person who shared that news on that topic.

Respondents also believe that even when they do read the news, young people are generally not likely to read it thoroughly.

*I think most of them read the news between the lines, they look at what stands out, what seems most important to them. If it's a long article, they certainly don't read the whole thing. (Gabriela, vocational trainer)*

The question of whether or not young people have the necessary critical reading skills and the ability to discern true from false information has been disputed: while some of the professions argue that the young people they work with have this ability, others say the contrary. Consistent with the results of the survey, it appears that a relatively small portion of young people have high critical reading ability, a significant portion of them have medium critical reading ability and the remaining had low critical reading ability. This means that most young people can understand the majority, but not all the information presented to them.

*Young people understand about 70% of information, in the sense of discerning whether information is true or false. (Ariana, Representative of Student Association).*

Respondents consider that the lack of critical thinking is widespread in Romania and is caused by the educational system which does not encourage this ability. From an early age, students are taught how to memorize information and not to question. This trend is often perpetuated up to college. In some cases, university professors try to encourage students to improve their critical reading skills, but it is a difficult process.

There are exceptions to this trend however, some respondents arguing that they successfully promoted critical reading in youth:

*The young people that we work with have good critical thinking skills. In my view, there is a significant difference between those who participate in voluntary activities and non-formal education and those who did not. Those who did engage in such activities tend to develop their critical thinking skills much more. Critical thinking is not taught as such but we have activities where we facilitate the exchange of ideas and expose them to more perspectives. (Diana, youth trainer)*

While some respondents consider that young people – especially those from urban areas – have the necessary tools to identify fake news, the majority of those interviewed think otherwise. According to them, young people are likely to become victims of fake news and misinformation due to their low level of knowledge and limited critical thinking skills. Two of the professionals interviewed even encountered such misinformation among the youth that they work with.

*They are most likely to be victims because their general level of knowledge is very limited. For example, they thought that they get the [Covid-19] virus if they catch a cold, not if they sit next to someone who is sick. The same with the war, they thought that we would go to war too, that Russia was coming to occupy us (Claudiu, youth trainer)*

Moreover, young people sometimes share information even though they know it is fake, because they want to be the first informing their peers about it.

*There is also the fear of missing out. They want to be the first to distribute whatever information is new, to be trendsetters. (Claudia, Children's safety center coordinator)*

The lack of regulation of speech in the online setting has also been mentioned as a cause of the proliferation of fake news and misinformation.

*Beyond critical thinking skills, there is no control over what's on social media, no one checks. Many people call themselves online experts. The flow of information is very high and we don't have the tools to stop [misinformation] in [due] time. (Diana, youth trainer)*

Finally, according to the professionals interviewed, an important source of fake news and misinformation online is likely to be influencers who initially attract their followers by providing a content that is relevant to young people, such as lifestyle advice or online games.

*Generally speaking, those who spread misinformation are people who offer lifestyle advice online (for example on going to the gym). They create a base of followers, and then they start spreading propaganda, including misogyny. These are real people. [….] Another example, gaming channels, where the videos were getting more and more extremist. They're not extremist from the beginning, it's a gradual process. (Ariana, representative of a students association).*

## 5. Online gambling/ gaming

Most of the professionals consulted think that online gambling addition is not a very widespread phenomenon among the young people that they work with. Nevertheless, they think such fortune games pose a significant risk to youth, especially boys, who are often subject to social pressure to make money fast and follow their role models and influencers. Moreover, boys are more likely to be interested in sports and in sports betting. Based on his long-term experience as a psychiatrist working with youth addicted to gambling, one of our respondents explains that:

*Everyone I work with started gambling when they were 13-15 years old, either sports betting, slot machines, sometimes even the lottery. Sports betting is extremely popular with young people. It is a discussion topic in their social circle. (Eugen, psychiatrist)*

Another important factor is the unrestricted access of youth (over 18 years old) to online gambling and high exposure to it, through extensive online advertising. While the gambling activity is regulated in Romania, there are very few limitations in terms of advertising and there are no mechanisms in place for safeguarding against gambling addiction.

*For example, it should be mandatory [for gambling providers] to inform the player about the winning rate. In some of these games the winning rate is about 5% - 10%, at most. Also, in some countries, players are obliged to take a 15 minutes break after an hour of continuous play, online and in casinos. [….] There are also countries where (online) online gambling*

*requires the registration of the identification number of or individual account of the player and there is a loss limit. (Eugen, psychiatrist)*

The access of young people (over 18 years) to gambling is also facilitated by the expansion of Non-banking Financial Institutions in Romania, which grant loans easily, but at a very high interest.

Finally, another important risk for young people associated with online gambling is of online gaming addicting, especially when associated with loot boxes. According to the professionals interviewed, online gaming addition seems to be more prevalent than gambling addiction and cam pose serious problems for the wellbeing of young people.

*Online games are also a risk, because they attract them. We have a young man, who should get a job, but he spends all his time in an internet room, playing online games. I don't know what game he is playing. We went to visit him and he had been in the internet room for two days, he had been in the room since the day before. He didn't want to talk to us. He continues to play and refused to get a job. (Mila, Youth counselor)*

*In recent times, video-game producers introduced a gambling element to gaming, namely the loot boxes, which require players to pay money in real life in order to be able to unlock unknown treasures in the game. Unlike other type of fortune games which are covered by the specific legislation on gambling and are prohibited for minors, loot boxes are not regulated. (Eugen, psychiatrist)*

*There is a phenomenon called the gamification of gambling. There is this conflation between gambling and video games. The famous loot boxes have emerged - users pay to open a box in the virtual realm that can bring help them win. Gambling is thus made accessible for youth under the age of 18.*

### 6. Revenge porn other forms of image-based sexual abuse

There is no comprehensive public data regarding the scale of sexting among young people or the revenge porn phenomenon in Romania, but all the professionals who participated in this study agree that this practice and the risks associated with it are very widespread. In the vast majority of cases, girls are the ones sending the intimate pictures/ videos - whether at their own initiative or in response to a request - and boys are on the receiving side. Sexting typically happens between people who are engage in an intimate relationship or who have such interest in each other. It is rarer for men to send (solicited) intimate content and most respondents argue that it is significantly less compromising for them, as compared to girls.

The reasons for this situation and many and complex. The first of them is the fact that such behavior has become the norm among teenagers and it is very easy to do so with a smartphone: "They do a lot of photo and video sharing with them or others, including intimate photos and videos. They do it because others do it. I feel like it's been normalized" (Diana, youth trainer)

But this is explanation is only skimming the surface of the problem. The main underlying factors leading to this situation are the oversexualization of women and girls by the media and society as a whole, coupled with the lack of information and sex education among young people, which would enable them to foresee the potential consequences of their actions.

*For girls it's related to the role models promoted by the media, this aspect of explicit sexuality seems normal to them, because those promoted by the media as successful women are exactly like that. (Claudia, University professor)*

*It's social pressure, I have heard of cases where boys were very persistent. They said they had certain needs too. If the guy doesn't insist, it's a matter of pleasing him.(Ariana, representative of a students association)*

*[Those sending intimate content] do not receive information before doing so, and do not know how they could prevent an incident such as revenge porn. […] Often young people who engage in revenge porn don't realize they are responsible of a criminal offence (Andra, activist)*

Another important aspect which determines young people to engage in send intimate pictures is the discovery of sexuality, desire for intimacy and lack of experience. The desire to have intimate interaction mediated by the internet is particularly relevant when young people cannot have this in real life.

*If parents don't allow young people to meet, it's a way to have some privacy online, hidden from parents. (Ariana, representative of a students association)*

When the victim of revenge porn in an underage, this conduct also qualifies as child pornography, which is specifically regulated in Romania.

Once published on the internet, the content used for revenge porn spreads out like a snowball and ends up on online groups that specialize in publishing such content. It is generally very difficult, if not impossible, for victims or persons supporting them to convince the administrators of these groups to take down this content, primarily because the real identity people behind these accounts is unknown.

As child pornography is specifically covered by the Romanian law and it can be investigated without the victim's prior complaint (unlike in the case when the victim is over the age of 18), it benefits from more robust prevention. Therefore, content of child pornography is often published on different online groups, where the membership is smaller and more carefully vetted.

**Other forms of image-based sexual abuse**

Firstly, when it comes to the sharing of intimate pictures or videos are shared without the consent of the persons depicted in them, it is important to note that it not always a case of revenge porn, but rather a different type of abuse. Sometimes, the reasons for committing this act are diverse, including boys wanting to show-off in front of their peers. "It's not necessarily always out of revenge. Sometimes guys show off their girlfriends' pictures. I think 40% of guys who get them pass them on. (Ariana, representative of a students' association)

Young women are also often faced with unsolicited sexual content, either from men or from unknown persons hiding behind false online accounts.

*I don't know any girl my age who has never received an unsolicited picture of a male organ from strangers on Instagram or Facebook. There are also certain viruses […] who send. There are cases when even men whom they know send unsolicited pictures, but not so often. […] In the case of fake accounts, the aim is generally to deceive. In the case of real accounts, it's basically a way for men to pick up girls. (Ariana, representative of a students' association).*

## 7. Identity theft

The experience of the professionals in consulted in this area differ significantly, some arguing that young people are generally aware of the risks associate with providing personal

identification information or passwords to strangers, while others thinking the contrary. Nevertheless, when such incidents do happen, the main factors leading to them are the lack of awareness and information or low self-esteem and the desire to please others (especially for girls).

*One factor is the lack of systematic risk awareness exercises: with concrete scenarios. (Claudiu, youth trainer).*

*I've heard this a lot more often from girls, for example they were asked to give the CVV of the card, are were told that they have to share such information [with their partner] if they love [them] (Gabriela, vocational trainer)*

## 8. Training methods for preventing and combating online risks

The professionals consulted in this study provided a series of recommendations regarding the design and content of training programs aimed at preventing and combating online risks among young people in Romania.

In terms of content, the trainings should provide information about the main risks identified, especially cyberbullying, image-base sexual abuse, online gaming/ gambling and fake news and the actions to be taken in order to avoid them. Meanwhile, such trainings should also encourage young people's critical reading abilities and develop their information-checking skills. These abilities should be mainstreamed within education.

For example, in the case of online gaming/ gambling, some professionals consider that:

*There is a need for classes, held either by professionals specifically trained for this or by the school counsellors, to provide a kind of psychological training. [Young people must] be warned of the mechanisms that these games trigger in their minds. (Eugen, psychiatrist)*

Another area in which there is a training need is related to building self-esteem in order to prevent risks and resist peer pressure. This was mentioned in relation to gambling but it is equally relevant for preventing other risky behavior, such as sending intimate pictures or personal data online.

*There should also be some programmes that develop young people's self-esteem so that they are not so dependent on winning for validation, learn how to resist peer pressure, about expressing emotions and problem solving etc. (Eugen, psychiatrist)*

The training programs and online resources (i.e. games, e-learning platforms) should employ a participatory method, in which young people have a say and feel involved. Also, the framing of the subjects discussed should be in such a way as to make the audience feel connected and directly concerned by the subjects discussed.

*The style of teaching should be appropriate to them: they need to feel that it affects them, that it is a subject present in their lives, in order to be motivated. For example, the trainer should use scenarios, role play games, learning by doing. They are not mere recipients, they can be valuable resources in understanding these phenomena, because they have more experience with them than adults. (Andreea, High school teacher)*

*The game could be like a social experiment. For example, they create a fake news and analyze its impact on other people in their group […] or like Monopoly or casino, where you can win money and then lose it. (Mila, youth counselor)*

Another key element brought forward by the professionals consulted is that of involving people with whom the audience can relate, be it other young people, influencers or persons who experienced the risk that it being discussed.

*As a teaching technique, I bring in people who have used drugs and let them talk about their experience. It's not necessarily that the presenter has to be young. It's one thing when I say it's wrong [to do something] and another when a person who has been a victim comes in. (Gabriela, vocational trainer)*

Last, but not least, online learning resources (games) dedicated to addressing online risks for young people should be optimized for smartphones, as this is the preferred device by young people, for accessing the internet, unless it they are also addressed to other stakeholders (such as teachers), in which case it should be played on the computer. Also, they should include avatars and social rewards, such as the option to share online, unless they are marketed as "educational games", which are not perceived as cool among young people.

*In order for a mobile app or computer game to be a successful, it needs to include rewards (level advancement) and/or social media sharing. It must have a character/ avatar and the design of the game should be done in collaboration with experts and with feedback from young people. (Claudia, Coordinator of children's safety center).*

## VI.    Conclusions and recommendations

Young people in Romania have increased their online presence during the Covid-19 pandemic and are spending more and more time on social networks, such as Instagram, Tik tok. Communicating with their friends and family are among the key activities performed online, but young people are also using the internet for watching movies, playing games (often in a network with other users) and shopping.

The key risks associated with youth online activity are cyberbullying, revenge porn and other image-based sexual abuse, the spread of fake-news and misinformation, online gaming/ gambling addiction and identity theft. One of the key factors behind all these risks is the lack of preventive campaigns and education (e.g. sexual education, internet use education, training on how to search and check information etc.) as well as training aimed at improving their critical reading skills.

Other factors facilitating the manifestation of such risks include: the hyper-sexualization and role-models promoted by mass-media, the under-regulation of certain industries targeting young people, such as online gambling/ gaming, the under-regulation of revenge porn and of the obligations of social networks on preventing image-based sexual abuse, the low self-confidence of young people and the limited information among parents regarding online risks.

In order to prevent and combat these risks, we have the following:

**Recommendations for the training of young people**

In order to combat the identified risks, young people should be provided training and other online resources (games, e-learning platforms etc.) which provide clear and easy-to-follow information about these risks, preventive behavior, main patterns of manifestation as well as social and legal consequences. They should also contribute to building young people's self -

esteem and their ability to understand and address their emotional needs, in order to resist social and peer pressure of pursuing certain risky behaviors.

Future trainings in this area should involve trained professionals (such as psychologists) as well as influencers and persons who can speak about their experience or other people whom the audience can relate to. They should include participatory methods of teaching and non-formal education techniques and the information should framed in such a way as to make young people feel directly concerned and included.

Online learning tools, such as games and e-learning platforms should also provide young people with practical examples, real-life scenarios showing the manifestation of these risks. In terms of technical set-up, they should be optimized for smartphones, unless they are also addressed to other stakeholders who use primarily other decides for accessing the internet. Games should include avatars and social rewards, such as the option to share online, which is perceived as cool among young people. Educational games are more likely to be successful if there are played individually.

**General policy recommendations**

**<u>Cyberbullying</u>**

According to relevant research (Cheianu-Andrei, 2017; Allison, 2018; Gaffney et al, 2019; Ansary, 2019), there are several pillars which need to be involved and take responsibility for curbing cyberbullying, in all its forms:

**State authorities:**

- Creating a coherent and applicable legislative framework to explicitly address severe forms of online harassment;
- Investing in nation-wide awareness campaigns and programmes regarding the harms of cyberbullying and how to curb this phenomenon (Ministry of Education, Ministry of Internal Affairs, Ministry of Health, Ministry for Young People and Sports, Ministry for Digitalization);
- Ensuring that law enforcement agencies are educated regarding the different forms and implications of cyberbullying, that they take this phenomenon seriously and that they have all necessary resources to respond to complaints of online harassment;
- Including cyberbullying prevention in strategic documents regarding the wellbeing of children and young people.

**Online Media Industry:**

- Offering efficient mechanisms to identify, report and resolve cyberbullying;
- Using human rather than automated moderation systems when users report online harassment;
- Offering sufficient privacy features in order to shield users from being harassed, stalked or doxxed online;
- Implementing fast and efficient methods to verify user identity and resolve reports of online impersonation;
- Taking proactive steps to offer increased protection to children and teenagers from online harassment.

**Educational institutions:**

- Creating a safe online environment for their students;
- Implementing anti-cyberbullying programmes and campaigns among their staff and students

- Implementing efficient policies and confidential procedures for reporting and resolving cyberbullying incidents among students or staff;
- Implementing a zero-tolerance policy for cyberbullying;
- Working together with parents and state authorities to curb the cyberbullying phenomenon.

**Educators:**

- Educating themselves on the forms and nature of cyberbullying and identifying it when it occurs;
- Intervening promptly if they learn one of their students is the victim of cyberbullying;
- Raising awareness of the harms of cyberbullying and how to prevent it among their students.

**Parents:**

- Staying up to date with technology and educating themselves regarding the online risks that their children are facing and how to curb them;
- Attending courses or seminars regarding bullying in general and cyberbullying in particular whenever offered the chance;
- Monitoring their teenagers' social media use closely and limiting their access to sites which may contain harmful content;
- Taking prompt action as needed whenever there is suspicion that their child is involved in cyberbullying, either as a victim or a perpetrator;
- Working together with educators and authorities to create a safe online environment for their children;

**Young people who use the internet:**

- Educating themselves regarding online risks;
- Limiting the time they spend online, especially their exposure to social media;
- Taking action when they see that one of their peers is the victim of cyberbullying;
- Reporting cyberbullying immediately to a relevant authority figure (teacher, employer, etc.) or, if severe, to the police.

## Image Based Sexual Abuse

According to the literature (Said & McNealy, 2022; Sullaway, 2022; Lageson et al, 2018; O'Conner et al, 2018; Gradinaru & Stoica, 2018; Livingstone Obe & Mason, 2015; Rodideal, 2021) as well as the experts interviewed for this research, the main recommendation for combating revenge porn and other forms of image-based sexual abuse are the following:

**Public authorities**

- Adopting a specific law which sanctions revenge porn (also when the victim is over 18 years old), punishable with prison time. The law should not condition the crime upon the intent of the perpetrator, as this is irrelevant and is also very difficult if not impossible to prove. The victim should not have to prove that the perpetrator aimed to humiliate or to take revenge on her/ him;
- Educating legislators, lawyers, magistrates and law enforcement personnel about the nature and consequences of revenge pornography;
- Allocating sufficient resources, such as adequately trained officers, to investigate reports of revenge pornography or other forms of online image-based sexual abuse.

**Educational institutions**:

- Introducing sexual education classes which include discussions about online sexual conduct and sexual abuse and ways to prevent it. This should equip young people with the tools to envision the potential consequences of their actions;
- Ensuring that management and teaching staff are aware about the nature and implications of revenge pornography and other forms of online sexual abuse (such as unwanted sexual images and content), that they take immediate action to resolve reports of such incidents and that they never blame the victim for it;
- Implementing a zero-tolerance policy regarding online sexual abuse of any kind among students;
- Putting in place a system for victims to safely report online image-based sexual abuse.

## Fake News

In order to curb the phenomenon of fake news from spreading, the literature recommends a combination of specific education and public awareness, but also greater responsibility on the part of the IT industry (Munteanu, 2022). For Romania, this would entail:

**Public authorities:**

- Reacting promptly to fake news which can be damaging to public health/safety or cause civil unrest, by having the appropriate institutions communicate clearly all the correct facts;
- Communicating regularly and transparently with the public, on all available channels, in order to foster trust in authorities;
- Implementing strategies and policies on an institutional level in order to address and prevent the spread of fake news.

**Health system:**

- Communicating clearly and transparently facts and information about any emerging public health crisis. The information campaigns should feature medical professionals and not politicians;
- Creating public education campaigns regarding health subjects most frequently targeted by fake news (e.g. vaccination, medication approval process, airborne disease spread and prevention during pandemics, etc.);
- Implementing severe sanctions, up to removing the right of practice, for physicians who spread medical fake news to their patients or to the general public;
- Investing in keeping doctors and medical staff educated and up to date with the latest advances in medicine relevant to their field of practice, in order to prevent fear of the unknown.

**Online Media Industry:**

- Increasing moderation efforts in order to promptly remove, signal or debunk fake news;
- Increasing efforts in identifying and removing fake accounts created to spread disinformation;
- Implementing user behavior monitoring software to prevent the functioning of troll farms and other similar hubs of users who mass-spam the online environment with fake news and informational intoxication;
- Limiting the capacity of individual users to mass circulate information via private messaging without going through a fake news filter.

**Education system:**

- Shifting away from the traditional form of teaching based on lectures ("magister dixit") and putting greater emphasis on inquisitiveness and critical thinking during existing classes;
- Implementing specific courses in the curriculum meant to develop students' skills in identifying online scams and fake news and in finding trustworthy information sources;
- Creating awareness campaigns for the wider public to support them in identifying and debunking fake news;
- Implementing more severe sanctions for teachers who spread fake news and other forms of misinformation among their students.

### Identity theft

According to the 2019-2020 ENSIA Report on identity theft, there are several measures which could be taken to help curb online identity theft are the following:

**Law enforcement authorities:**

- Ensuring that relevant law enforcement agencies have sufficient trained and experienced personnel allocated to identifying and addressing online identity theft. This may imply establishing a specialized department within existing law enforcement structures, specifically tasked with resolving identity theft cases.
- Ensuring that there are sufficient resources allocated for the investigation of online identity theft reports (sufficient specifically trained officers, all necessary technology, etc.);
- Training police officers to recognize the signs of online identity theft when victims report suspicious activity with their online accounts or their bank accounts.

**Educational institutions:**

- Providing training for students and staff regarding online safety, privacy and security;
- Installing all necessary software on shared computers to prevent the installation of malware that could be used to steal the identity of students or staff;
- Setting in place policies to respond to incidents of student or staff identity theft.

**Online media industry and financial institutions who offer online services**

- Setting in place solid identification measures to protect their clients from identity theft (e.g. video identification);
- Implementing state of the art security systems such as two-factor authentication and end-to-end encryption in order to prevent identity theft;
- Creating awareness campaigns to teach their clients how to avoid identity theft while using their specific platform;
- Making their clients aware of any major phishing schemes circulating on the internet.

**Young people who use the internet:**

- Never revealing their confidential information to strangers online;
- Making sure that the websites which require their personal information are legitimate and trustworthy by carefully looking at the aspect and address of websites before providing any of their information;
- Always remembering to log out of their accounts when using a shared computer;
- Using strong passwords for their accounts and locking their devices when not in use;
- Using updated anti-virus and anti-malware software on their devices;
- Reporting any suspicious activity in their online or bank accounts to the appropriate authorities immediately.

## Online gambling

According to international research (Lozano et al, 2022; Shi et al, 2021; Kristiansen & Severin, 2020, Li et al, 2019), the findings of local journalistic investigations and of this research (Olaru, 2021), the following measures should be implemented to combat online gambling addiction:

**Public authorities:**

- Regulating advertisements for online gambling to the same standards as for offline gambling;
- Restricting advertising for online gambling in public spaces visited by children and young people;
- Strengthening the control on the implementation of the legislation banning the access of minors to online gambling and implementing measures to limit the possibility of adults assisting minors in accessing online gambling;
- Putting in place legal provisions requesting online casinos to limit the time at that players can spend at a certain time as well as the amount of money they can invest in online gambling each month;
- Recognizing loot box mechanics in video games as a form of online gambling, with all the legal consequences that entails.

**Health system:**

- Providing free mental health support for children and young people addicted to online gambling;
- Creating awareness campaigns regarding the mental health risks of online gambling.

**Parents:**

- Monitoring their children's online activity and preventing them from engaging in any form of online gambling;
- Ensuring that the online games their children play do not contain loot box mechanics.
- Ensuring that their children do not have access to their credit card information or that there are safeguards in place to let the parent know when an online purchase has been made.

## References

Ackland, Robert, and Karl Gwynn. "Truth and the dynamics of news diffusion on twitter." in Greifeneder, R., Jaffe, M., Newman, E., & Schwarz, N. *The psychology of fake news: Accepting, sharing, and correcting misinformation* Routledge, 2020. 27-46.

Ahlgrim, B. and Terrance, C. (2018) "Perceptions of cyberstalking: Impact of perpetrator gender and cyberstalker/victim relationship," *Journal of Interpersonal Violence*, 36(7-8). Available at: https://doi.org/10.1177/0886260518784590.

Alexandru, P. (2019) *Elev La școală privată Din București, Victimă de Hărțuire: Cum a ajuns victimă de bullying LA 12 ani*, *Playtech Știri*. Available at: https://playtech.ro/stiri/elev-la-scoala-privata-din-bucuresti-victima-de-hartuire-bullying-52245 (Accessed: December 9, 2022).

Amundsen, R. (2020) "'a male dominance kind of vibe': Approaching unsolicited Dick Pics as sexism," *New Media & Society*, 23(6), pp. 1465–1480. Available at: https://doi.org/10.1177/1461444820907025.

Anderson, B. and Wood, M.A. (2021) "Doxxing: A scoping review and typology," *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, pp. 205–226. Available at: https://doi.org/10.1108/978-1-83982-848-520211015.

Anderson, B. and Wood, M.A. (2022) "Harm imbrication and virtualised violence: Reconceptualising the harms of Doxxing," *International Journal for Crime, Justice and Social Democracy*, 10(4). Available at: https://doi.org/10.5204/ijcjsd.2140.

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.

*Aproape 8 Milioane de Români Joacă jocuri video, relevă cel mai cuprinzător studiu despre gaming-ul local* (2021) *Romanian Game Developers Association*. Available at: https://rgda.ro/aproape-8-milioane-de-romani-joaca-jocuri-video-releva-cel-mai-cuprinzator-studiu-despre-gaming-ul-local/#:~:text=Hyper.Play%202021-,Aproape%208%20milioane%20de%20rom%C3%A2ni%20joac%C4%83%20jocuri%20video%2C%20relev%C4%83%20cel,studiu%20despre%20gaming%2Dul%20local&text=7.9%20milioane%20de%20rom%C3%A2ni%20joac%C4%83,%2Duri%2C%20console%20sau%20tablete. (Accessed: December 9, 2022).

Balaban-Popa, O. (2022) *Dependenta de Jocuri de Noroc: Semne, Modalitati de tratament Si Gestionare*. Available at: https://www.sfatulmedicului.ro/Psihologie-si-psihoterapie/dependenta-de-jocuri-de-noroc-semne-modalitati-de-tratament-si-gestionar_19236 (Accessed: December 9, 2022).

Bale, Jeffrey M. "Political paranoia v. political realism: On distinguishing between bogus conspiracy theories and genuine conspiratorial politics." *Patterns of prejudice* 41.1 (2007): 45-60.

Basch, Corey H., Grace C. Hillyer, and Christie Jaime. "COVID-19 on TikTok: harnessing an emerging social media platform to convey important public health messages." *International journal of adolescent medicine and health* (2020).

Belu, G. (2021) *Revenge porn sau „Vezi că au fost publicate Niște Poze cu tine"*, *StudentStories*. Available at: http://stories.studentpress.ro/2021/01/07/16584/ (Accessed: December 9, 2022).

Benea, I. (2021) *Cum îi pedepsește România PE Hoții de identitate de pe net. senator „clonat" Pe facebook: Te simți strivit*, *Europa Liberă România*. Radio Europa Liberă România (RFE/RL). Available at: https://romania.europalibera.org/a/cum-%C3%AEi-pedepse%C8%99te-rom%C3%A2nia-pe-ho%C8%9Bii-de-identitate-de-pe-net-senator-clonat-pe-facebook-te-sim%C8%9Bi-strivit/31070050.html (Accessed: December 12, 2022).

Brady, A. and Prentice, G. (2019) "Are loot boxes addictive? analyzing participant's physiological arousal while opening a loot box," *Games and Culture*, 16(4), pp. 419–433. Available at: https://doi.org/10.1177/1555412019895359.

Buda, A. (2022) *Dependența de internet*, *Acasa*. Available at: https://www.reginamaria.ro/utile/dictionar-de-afectiuni/dependenta-de-internet (Accessed: December 9, 2022).

Burnes, D., DeLiema, M. and Langton, L. (2020) "Risk and protective factors of identity theft victimization in the United States," *Preventive Medicine Reports*, 17, p. 101058. Available at: https://doi.org/10.1016/j.pmedr.2020.101058.

Buturoiu, Raluca, et al. "Who Believes in Conspiracy Theories about the COVID-19 Pandemic in Romania? An Analysis of Conspiracy Theories Believers' Profiles." *Societies* 11.4 (2021): 138.

Campbell, M. and Bauman, S. (2018) "Cyberbullying: Definition, consequences, prevalence," *Reducing Cyberbullying in Schools*, pp. 3–16. Available at: https://doi.org/10.1016/b978-0-12-811423-0.00001-8.

*Ce tipuri de jocuri de casino online sunt populare în românia?* (2022) *Bogdan Cazino*. Bogdan Cazino. Available at: https://www.bogdancazino.ro/stiri/ce-fel-de-jocuri-prefera-jucatorii-de-cazino-din-romania/ (Accessed: December 9, 2022).

Centrul pentru Jurnalism Independent, *Conectat la media! Interacțiunea tinerilor din România cu media, 2020, https://cji.ro/studiu-conectat-la-media-interactiunea-tinerilor-din-romania-cu-media-2/* Accessed 26.08.2022

Chirita, L. (2022) *Furtul de indentitate – adevar sau provocare?*, *Furtul de indentitate – Adevar Sau provocare?* Available at: https://www.apcf.ro/ro/articole/furtul-de-indentitate-adevar-sau-provocare (Accessed: December 12, 2022).

Chun, J.S. *et al.* (2020) "An international systematic review of cyberbullying measurements," *Computers in Human Behavior*, 113, p. 106485. Available at: https://doi.org/10.1016/j.chb.2020.106485.

Costin, O.C. (2019) *Dependenta de Jocuri de Noroc – cum scapi de ea*, *Sfaturimedicale.ro*. Available at: https://sfaturimedicale.ro/dependenta-de-jocuri-de-noroc/ (Accessed: December 9, 2022).

*Datele personale Si Pozele Imi Sunt postate pe internet* (2020) *POLITISTI.ro*. Available at: https://www.politisti.ro/forums/topic/7327-datele-personale-si-pozele-imi-sunt-postate-pe-internet/ (Accessed: December 9, 2022).

Davis Kempton, S. (2020) "Erotic extortion: Understanding the cultural propagation of revenge porn," *SAGE Open*, 10(2), p. 215824402093185. Available at: https://doi.org/10.1177/2158244020931850.

Despa, O. (2021) *Top Cinci Dezinformări virale în 2021*, *Europa Liberă România*. Radio Europa Liberă România (RFE/RL). Available at: https://romania.europalibera.org/a/dezinformari-2021/31626510.html (Accessed: December 9, 2022).

Diac, M. *(2022) Umilită pe internet, o fiică de preot S-A Sinucis și este înmormântată ...* (no date) *Romania Libera*. Available at: https://romanialibera.ro/social/eveniment/umilita-pe-internet-o-fiica-de-preot-s-a-sinucis-si-este-inmormantata-fara-slujba/ (Accessed: December 9, 2022).

Dimulescu, V. (2018) „*Vezi că Umblă Niște Poze cu tine Goală Prin Liceu"*, *Casa Jurnalistului*. Available at: https://casajurnalistului.ro/poze-goala-liceu/ (Accessed: December 9, 2022).

Dimulescu, V. (2020) „*Umilința Supremă"*, *Casa Jurnalistului*. Available at: https://casajurnalistului.ro/umilinta-suprema/?fbclid=IwAR1xdgb9wtCjvSUDUPqb_C_U8f8z-2S09OWaupUHbxUZsmUTrmd2G8haVSU (Accessed: December 9, 2022).

Dimulescu, V. (2020) *Te-am Văzut Goală Pe Pagina „fete cuminți"*, *Scena 9*. Available at: https://www.scena9.ro/article/revenge-porn-adolescenti-pandemie (Accessed: December 9, 2022).

Eckert, S. and Metzger-Riftkin, J. (2020) "Doxxing," *The International Encyclopedia of Gender, Media, and Communication*, pp. 1–5. Available at: https://doi.org/10.1002/9781119429128.iegmc009.

Eurocomunicare, *Infodemia COVID-19 în România. O analiză a dezinformării în spațiul digital,* 2020 https://www.antifake.ro/infodemia-covid-19-in-romania/, Accessed 26.08.2022

Farfán, Juana, and María Elena Mazo. "Disinformation and Responsibility in Young People in Spain during the COVID-19 Era." *Publications* 9.3 (2021): 40.

Festl, R. *et al.* (2017) "Longitudinal patterns of involvement in cyberbullying: Results from a latent transition analysis," *Computers in Human Behavior*, 66, pp. 7–15. Available at: https://doi.org/10.1016/j.chb.2016.09.027.

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.

Giménez Lozano, J.M. and Morales Rodríguez, F.M. (2022) "Systematic review: Preventive intervention to curb the youth online gambling problem," *Sustainability*, 14(11), p. 6402. Available at: https://doi.org/10.3390/su14116402.

Government Decision no 111/2016 for the approval of the Regulations for the implementation of Government Emergency Ordinance No 77/2009 on the organization and operation of gambling

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,

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

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

Hayes, R.M. and Dragiewicz, M. (2018) "Unsolicited dick pics: Erotica, exhibitionism or entitlement?," *Women's Studies International Forum*, 71, pp. 114–120. Available at: https://doi.org/10.1016/j.wsif.2018.07.001.

Holloway, I.W. *et al.* (2014) "Online social networking, sexual risk and protective behaviors: Considerations for clinicians and researchers," *Current Addiction Reports*, 1(3), pp. 220–228. Available at: https://doi.org/10.1007/s40429-014-0029-4.

Iorga, M. *et al.* (2022) "Exploring the importance of gender, family affluence, parenting style and loneliness in cyberbullying victimization and aggression among Romanian adolescents," *Behavioral Sciences*, 12(11), p. 457. Available at: https://doi.org/10.3390/bs12110457.

Jibril, A.B. *et al.* (2020) "Online identity theft on Consumer Purchase Intention: A mediating role of online security and privacy concern," *Lecture Notes in Computer Science*, pp. 147–158. Available at: https://doi.org/10.1007/978-3-030-45002-1_13.

Kaur, P. *et al.* (2021) "A systematic literature review on cyberstalking. an analysis of past achievements and future promises," *Technological Forecasting and Social Change*, 163, p. 120426. Available at: https://doi.org/10.1016/j.techfore.2020.120426.

Keeley, Brian. "Of conspiracy theories." *Journal of Philosophy* 96.1 (1999).

Kristiansen, S. and Severin, M.C. (2020) "Loot box engagement and problem gambling among adolescent gamers: Findings from a national survey," *Addictive Behaviors*, 103, p. 106254. Available at: https://doi.org/10.1016/j.addbeh.2019.106254.

Lageson, S.E., McElrath, S. and Palmer, K.E. (2018) "Gendered public support for criminalizing 'Revenge porn,'" *Feminist Criminology*, 14(5), pp. 560–583. Available at: https://doi.org/10.1177/1557085118773398.

Law no. 217/2003 for preventing and combating domestic violence - republished

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.

Lozano-Blasco, R., Cortés-Pascual, A. and Latorre-Martínez, M.P. (2020) "Being a cybervictim and a cyberbully – the duality of cyberbullying: A meta-analysis," *Computers in Human Behavior*, 111, p. 106444. Available at: https://doi.org/10.1016/j.chb.2020.106444.

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.

Mancosu, Moreno, and Federico Vegetti. ""Is it the message or the messenger?": Conspiracy endorsement and media sources." *Social Science Computer Review* 39.6 (2021): 1203-1217.

Munteanu, D. (2022) *Barometrul rezilienței societale în domeniul informațional 18/04/2022*. Available at: https://e-arc.ro/ (Accessed: December 9, 2022).

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*, 72(4), pp. 344–359. Available at: https://doi.org/10.1111/hequ.12171.

Olaru, A. (2021) *Drogurile virtuale: FIFA și jocurile video care Creează dependență. „simțeam că Devin Agresiv. Că Familia e UN Ceva Care Nu mă lasă să joc"*, *PressOne*. Available at: https://pressone.ro/drogurile-virtuale-fifa-si-jocurile-video-care-creeaza-dependenta-simteam-ca-devin-agresiv-ca-familia-e-un-ceva-care-nu-ma-lasa-sa-joc (Accessed: December 9, 2022).

Olaru, A. (2021) *Frăția Păcănelelor. „joacă, joacă, Joacă!" ce face Statul Român când jocurile de noroc Devin O Problemă Socială*, *PressOne*. Available at: https://pressone.ro/de-ce-vezi-mai-multe-reclame-la-pariuri (Accessed: December 9, 2022).

Olaru, Alexandru *„Suntem o colonie a Occidentului. Putin ne salvează de globalism". Cum se infiltrează propaganda rusă în România și ce face statul să o prevină, 14.04.2022 https://pressone.ro/suntem-o-colonie-a-occidentului-putin-ne-salveaza-de-globalism-cum-se-infiltreaza-propaganda-rusa-in-romania-si-ce-face-statul-sa-o-previna,* Accessed 26.08.2022

Paasonen, S., Light, B. and Jarrett, K. (2019) "The dick pic: Harassment, curation, and desire," *Social Media + Society*, 5(2), p. 205630511982612. Available at: https://doi.org/10.1177/2056305119826126.

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

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.

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.

Romanian Criminal Code of 17 July 2009 (Law no 286/2009)

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

Said, I. and McNealey, R.L. (2022) "Nonconsensual distribution of intimate images: Exploring the role of legal attitudes in victimization and perpetration," *Journal of Interpersonal Violence*, p. 088626052211228. Available at: https://doi.org/10.1177/08862605221122834.

Scheithauer, H. *et al.* (2021) "Types of Cyberbullying," in P.K. Smith and J. O'Higgins Norman (eds) *The Wiley Blackwell Handbook of Bullying*. 1st edn. Wiley Blackwell.

Shi, J. *et al.* (2021) "A perspective on age restrictions and other harm reduction approaches targeting youth online gambling, considering convergences of gambling and videogaming," *Frontiers in Psychiatry*, 11. Available at: https://doi.org/10.3389/fpsyt.2020.601712.

Simina, C. (2020) *Propaganda rusiei în România şi Moldova (i): „România N-A Reuşit să-şi creeze instrumente proprii de soft power în Moldova"*, *PressOne*. Available at: https://pressone.ro/propaganda-rusiei-in-romania-si-moldova-i-romania-n-a-reusit-sa-si-creeze-instrumente-proprii-de-soft-power-in-moldova (Accessed: December 9, 2022).

Stoica, Cătălin Augustin, and Radu Umbreș. "Suspicious minds in times of crisis: determinants of Romanians' beliefs in COVID-19 conspiracy theories." *European Societies* 23.sup1 (2021): S246-S261.

Sullaway, M. (2022) "Lone Wolves and Wolf Packs: Revenge Porn, Cybermobs and Creepshots," in E.W. Dunbar (ed.) *Indoctrination to Hate: Recruitment Techniques of Hate Groups and How to Stop Them*. Library of Congress.

Toma, A. (2022) *„ferma de troli" ai lui putin umple internetul CU Dezinformări Dintr-O Fostă Fabrică din Sankt Petersburg*, *Ziare.com*. Available at: https://ziare.com/razboi-ucraina/razboi-ucraina-ferma-troli-vladimir-putin-sankt-petersburg-1738590 (Accessed: December 9, 2022).

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).

Uscinski, Joseph E. *Conspiracy theories and the people who believe them*. Oxford University Press, USA, 2018.
van Prooijen, Jan-Willem, and Mark Van Vugt. "Conspiracy theories: Evolved functions and psychological mechanisms." *Perspectives on psychological science* 13.6 (2018): 770-788.
Vegetti, Federico, and Moreno Mancosu. "The impact of political sophistication and motivated reasoning on misinformation." *Political Communication* 37.5 (2020): 678-695.

*Video Jocuri pentru Copii, coşmar Pentru Părinți* (2019) *Stiri.tvr.ro*. Available at: http://stiri.tvr.ro/jocurile-pentru-copii--co--mar-pentru-parin--i--un-copil-din-timi--oara-a-cheltuit-6-mii-de-lei-pe-jocuri-online_840711.html#view (Accessed: December 9, 2022).

West, Harry G., and Todd Sanders, eds. *Transparency and conspiracy: Ethnographies of suspicion in the new world order*. Duke University Press, 2003.

Wilson, C., Sheridan, L. and Garratt-Reed, D. (2021) "What is cyberstalking? A review of measurements," *Journal of Interpersonal Violence*, 37(11-12). Available at: https://doi.org/10.1177/0886260520985489.

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.

Zhu, C. *et al.* (2021) "Cyberbullying among adolescents and children: A comprehensive review of the global situation, risk factors, and preventive measures," *Frontiers in Public Health*, 9. Available at: https://doi.org/10.3389/fpubh.2021.634909.

Zych, I., Farrington, D.P. and Ttofi, M.M. (2019) "Protective factors against bullying and cyberbullying: A systematic review of Meta-analyses," *Aggression and Violent Behavior*, 45, pp. 4–19. Available at: https://doi.org/10.1016/j.avb.2018.06.008.