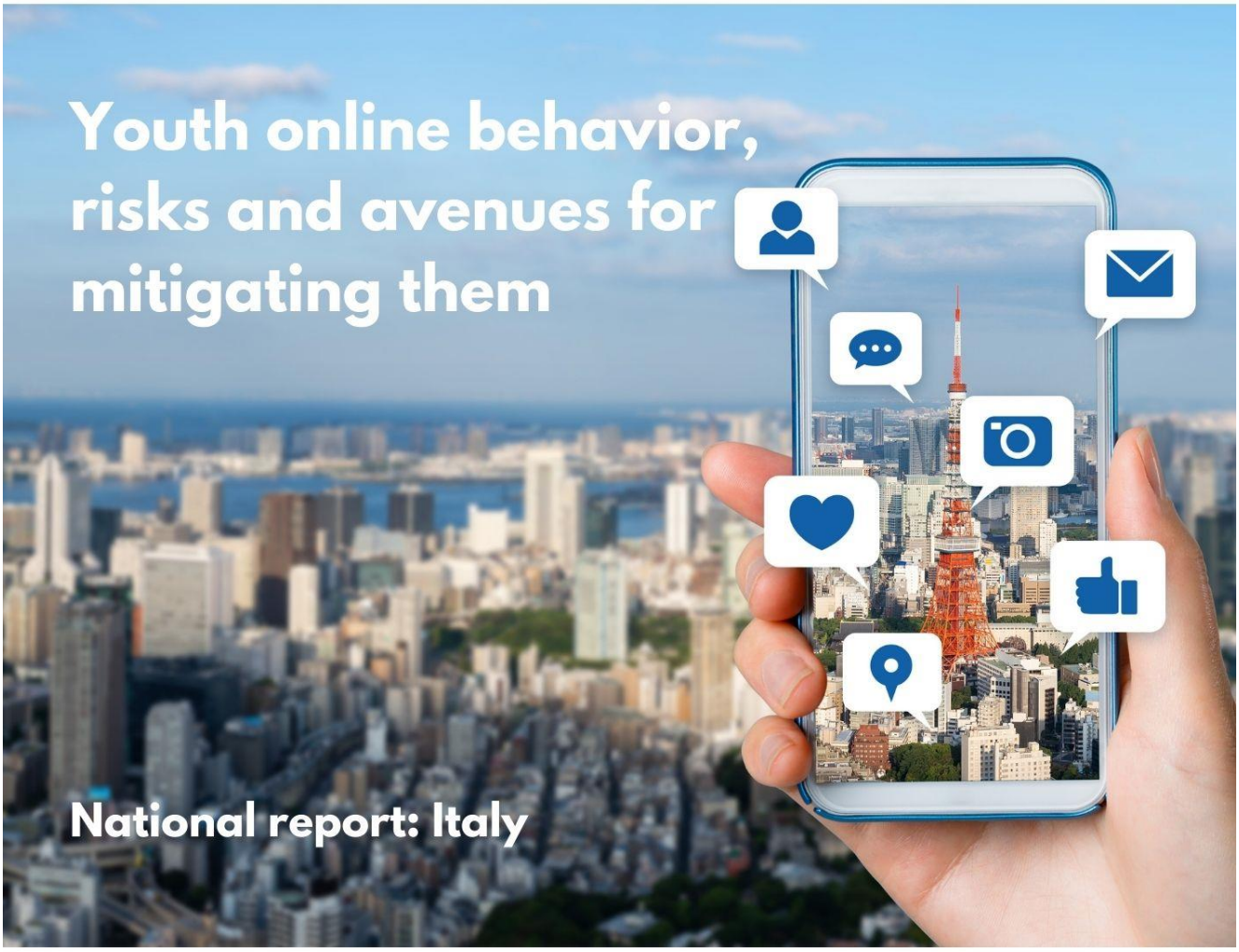
Authors: Corso Giulia, Ursino Giuseppe Fabio



Co-funded by the European Union

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**

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

1. Introduction

The **Internet** and **social media** are not new to society, they have increasingly permeated people's everyday life, revolutionised - reshaped and redefined - people's approach with others, news, shopping, their job, etc. Along with the infinite perks related to the internet and social networks, the latter also brought brand new **risks**, making the users more vulnerable.

Whilst the Internet and, later, social media platforms were originally created to enable connections among people, these channels have become important routes for **reaching services** and for the **production and exchange of information and news**. Particularly, the pandemic of **Covid-19** highlighted how digitization, the Internet and social networks have progressively **broken down the barriers between the "offline"** physical world **and "online"** virtuality and can represent a tool, a vehicle of amplification of benefits but also of insidious dangers and risks for those like **young people** who inhabit them, with a totalizing experiential approach, connected to a continuous and assiduous exposure and interaction that should not be underestimated.

Unfortunately, today's social media is a fertile ground for the spread of several risks generated online, such as **fake news**, **identity theft** on social medias, **revenge porn**, **image-based sexual abuses**, **cyberbullying** and **online gambling**. **This kind of risks and contents** can travel very quickly and reach widely among users without any third-party fact-checking or editorial judgement. The reasons of this kind of risks are very diversified. Populism or manipulation can be one of the main reasons of the spread of fake news, while cyberbullying may happen when a school climate foster aggressive behaviour among young people.

Given the risks and complexity of the phenomenon so far, this research report, after illustrating the **methodology** used, focuses firstly on identifying and understanding the **risks young people may encounter** online, taking into account the current stare of the literature, and secondly specific risks we mentioned before, what factors and conditions may favour or have contributed to the exposure of digital platform users to certain misleading, manipulative situations. Therefore, the report moved its efforts by attempting to investigate, test and analyse, based on **desk research** and **field research** on the actual risks, especially the propagation of misinformation phenomena, cyberbullying, online gambling and revenge porn.

The **research question** is: which are the main factors making young people (aged 16-30) vulnerable to several online risks? What are the main factors affecting the spread of these behaviors and which events have fortified these risks?

The research and report are carried out within an Erasmus Plus Project, entitled **RISE - Action-based approach in addressing and mitigation risks of young people in online social networks**, project number 2021-1-RO01-KA220-YOU-000028688, **co-funded by the European Union**. RISE explores the dimension of online risks young people encounter, among which disinformation, fake news, cyber propaganda and the digital spaces, where such risks can multiply and spread undisturbed among the endless avenues of the web. The project focuses on four elements: **prevention**, **identification**, **mitigation**, and **tools** to mitigate such risks.

Specifically, RISE aims at developing:

1. A **methodology** designed to address the needs of young people in the framework of digitalisation and especially of social media in the age post-COVID-19 pandemic;
2. An **educational game** for young people and prevent and mitigate risks of social networks;
3. A **Capacity Building Programme** for youth trainers aiming to help them to build capacity when dealing with risks of young people in social networks.

C verification strategies, such as checking the author or the source of the news[1]. Despite that, when asked about the characteristics of fake news, Italian youngsters mentioned: the **linguistic aspect**, as the '**sensationalistic' feature of the title** and the **high presence or total absence of details**, along with the **technical aspect**, as a photoshopped image[2]. In addition, it would appear that the **easier topic to fall for fake news is gossip**, including actors of the cinema or TV series, football news and sport in general; even though they recognise the click-bait function, youngsters are likely to fall for fake news when a strong emotionality - as the love for an idol - occurs.

Whereas in echo chambers people **reinforce their attitudes and orientation**, as on the Internet it is always easy to find more extreme versions of one's opinions, at the same way **people tend to resist** and neglect **factual evidence** in contrast with their own beliefs, and corrections frequently fail to reduce misperceptions and often act as a backfire effect.

As a matter of fact, despite the introduction of a **section dedicated to Covid-19** on the Italian Ministerial website and **to related debunked fake news**, specific **communication campaigns**, as well as the **Ministry of Health's Facebook page** which - among the others - strived to counter false information by providing fact-checked information[3], these tools are **supported mainly by scientific echo chambers**. Indeed, only few conspiracy users usually interact with debunking information - and in any case, it generates an increase of conspiracy-related activity, hence a backfire effect[4]. Those who seem to be impactful in **debunking fake news for young people are closer figures** as parents, older cousins and educators; however, a recurrent strategy when dealing with specific person-related news is to check their official accounts. Some experiences have already shown that **comprehensive training**, **awareness raising** and **literacy campaigns** against misinformation have positive effects.

Fake news is likely to provoke **risky social and health behaviour**, for example COVID19-related pseudoscientific theories about **the role of 5G networks in the spread of the virus**, and about **'alternative cures'** based on garlic, vitamin C and D[5] would have led to **lower**

1 Papapicco, C., Lamanna, I. and D'Errico F. 2022. Adolescents' Vulnerability to Fake News and to Racial Hoaxes: A Qualitative Analysis on Italian Sample. Multimodal Technologies and Interactions. hptts://doi.org/10.3390/mti6030020

2 Papapicco, C., Lamanna, I. and D'Errico F. 2022. Adolescents' Vulnerability to Fake News and to Racial Hoaxes: A Qualitative Analysis on Italian Sample. Multimodal Technologies and Interactions. hptts://doi.org/10.3390/mti6030020

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

4 Zollo, F. and Quattrocchi W. 2017. Misinformation spreading on Facebook. Available online (web pdf): https://arxiv.org/pdf/1706.09494.pdf

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

compliance with protective measures of social distancing, hindering them, and **low rates of trust in scientists and authorities** as well as **of vaccinated people**. **False information about migrants or other ethnicities** (e.g., the idea that immigrants are criminals and that COVID19 was created in a laboratory in Wuhan) - carried out unfortunately also by political figures such as former Minister of the Interior Matteo Salvini - lead to **forms of racism**, which will influence young people's adulthood.

Cyberbullying

Some other risks may involve fake profiles mainly on Instagram and Facebook, willing to **cyberbully or lure youngsters**, or deceive them to **get confidential data**, **intimate pictures**, or **money**.

Cyberbullying is an inappropriate use of the Internet, whereby **young people exchange violent, denigrating, discriminatory content**, aimed at peers considered different in terms of physical appearance, clothing, sexual orientation, social class or because they are foreigners. This is a broad definition that includes but is not limited to **harassment**, **denigration** and **impersonation**. According to a survey conducted in 2019 by ISTAT – the Italian National Statistics Institute – around 7.1% girls and 4.6% of boys who own a smartphone or can access an Internet connection have been subjected to continuous harassment via the Internet or cell phone[6].

The pandemic period and the various lockdowns have brought about a fundamental change in the lives of citizens, including children and adolescents. The overall effects have also hit the world of online deviance, **increasing the presence of paedophiles, child pornographers and groomers**, and leading to a significant increase in online crimes against youngsters (+47% in 2021 compared to 2020). During 2021, hundreds of girls, boys and teenagers (531 minors in total) were approached on the web by groomers, the vast majority of them under 13 years of age (338 minors). The most common grooming spaces are **social networks**, followed by **messaging apps** and **online games**[7].

Revenge Porn and Image-based sexual abuses

Image-based sexual abuse, commonly known as **'revenge porn'**, describes the act of sharing images or videos of an individual, the **victim**, that are sexually explicit (displaying nudity or showing the person engaged in a sexual act) without that **person's consent**. The images or videos may be shared on specialized revenge porn websites, on social media, via email, text, or messaging services, or shared with specific individuals, such as the victim's family or employers.

6 Commissione parlamentare per l'infanzia e l'adolescenza (2019) "Indagine conoscitiva su bullismo e cyberbullismo", Roma.

7 Servizio Polizia Postale e delle Comunicazioni - Polizia di Stato e Save the Children Italia Onlus (2021) L'abuso Sessuale Online In Danno Di Minori. Available at: https://www.commissariatodips.it/dossier-dati_def.pdf

Consent is required at **two stages**: when the image or video is taken and again when it is shared with any third party.

According to a survey conducted from **2019** to **2020**, nearly **13%** of **Italians** respondents know a victim of revenge porn. The **psychological harm** of such a violation can be devastating for the victim and even push the person to commit **suicide**. Facing the frequency of such acts and the media coverage that some cases receive, the Italian government acted. From 2018 to 2019, four draft laws on **criminalizing revenge porn** were presented by different Italian politicians.

According to a survey conducted in **2018**, roughly **78%** of Italian **women** and **65,5%** of Italian **men** perceived such laws as a social achievement. In July **2019**, a law on revenge porn was passed by the **Italian parliament.**

Being recognized as a crime, revenge porn became a particular instance of sexual violence. Although the violence is psychological rather than physical, the potential harms are equal.

In **2018**, almost five thousand sexual violence cases were reported to the authorities in Italy. This figure was likely to be an underestimation as many victims of abuse do not report themselves. In the same year, a survey revealed that **77%** of respondents in Italy believed that a **zero-tolerance policy** for sexual harassment was essential to change society.

Identity theft

Identity theft is a devious crime, because it is difficult to combat, in some forms, also particularly difficult to prevent, and because there is still too little information about it, often limited to **phishing**. Italy is a very exposed country; according to the latest available data (CRIF), over 25.000 cases of identity theft have occurred in our country, with a total value of over EUR 200 million.

Identity theft may cause the victim both economic/financial damage and moral/psychological moral/psychological damage, related to the emotional stress caused by the feeling of powerlessness which in turn generates anger and fear as well as the feeling of being violated.

Whereas until a few years ago it was mainly adults between 40 and 50 years old who were affected, now, after the pandemic, it is **mainly young and very young people** between the ages of 18 and 30 who end up in the crosshairs of online fraudsters. These in fact account for 24.2% of the total. However, their gender does not change: as in the past, there is a clear predominance of males, 64.1% in the first 6 months of 2021.

Internet addition

Internet addiction in adolescence can be a real syndrome: it affects boys and girls who cannot stay without the internet and, deprived of the Net, experience a strong discomfort that they cannot alleviate in any other way. The addiction points out that the phenomenon can include **addiction to social networks, online gaming, shopping or pornographic sites**.

The numbers of internet use and addiction tell us that internet addicts in Italy are almost all youngsters and young adults and, considering the severe and moderate levels of severity, they constitute about 6%.

In Italy, there are an estimated 300.000 people between the ages of 12 and 25 who are addicted to the Internet. Young people who develop a real addiction to the Internet or gaming or social networks, may do so to the **detriment of their real life, school and relationships,** risking **to isolate themselves** by not fully experiencing adolescence, a fundamental period in the creation of emotional, affective and relational competences.

Technology brings about a change in the concepts of time and space, allowing us to observe a profound **acceleration in the pace of life** while at the same time reducing distances. All this leads to sensory **overstimulation**, which can have important **consequences on attention, memory and sleep patterns - having repercussions on individual psychic well-being**.

Almost 90% of youngsters report having experienced the phenomenon of the 'phantom vibration' that is the false alarm of receiving a message on their mobile phone. Of course, even the mere presence of a potentially active device is linked to a **lengthening** of the **time it takes to complete a task**, as a state of alertness occurs leading us to check the phone several times even in the absence of real signals.

Memory is externalised: we outsource the storage of more and more information to the mobile phone or the internet, creating different mental maps that we need to retrieve it.

As regards **sleeping patterns**, the abuse of new technologies and its overstimulation before sleep negatively impacts brain circuits by altering the sleep-wake rhythm. Light from smartphone and tablet screens stimulates the retina, as a result of which the secretion of melatonin (sleep hormone) is reduced.

Subjects with **Internet addiction** - including **Internet Gaming Disorder** - complain of **carpal tunnel syndrome** and head-neck syndrome[8]. The former is the result of a muscular imbalance caused by excessive use of a smartphone or tablet and is characterised by pain in the wrist, hand and fingers, while the latter is caused by prolonged forward bending and alteration of the natural cervical lordosis. Among the **musculoskeletal disorders** resulting from the excessive use of video games is also radial

8 Adamczyk R., (2019), Non-substance addictions in the context of individual and social health, Social Pathology & Prevention, vol.5, pp.23-28

To learn more: https://www.stateofmind.it/2021/03/internet-gaming-disorder-conseguenze/

stenosing tendonitis, characterised by the inflammation of the tendons of the hand due to the continuous repetition of a gesture (as the continuous movement of the buttons on a play-station joystick). In addition, several studies have analysed the cognitive effects of gaming exposure with preliminary but extremely interesting results. Video games improve visual attention and coordination, but some data suggest **an increase in impulsive and aggressive behaviour**. Specifically, one study of 221 Italian university students found a prevalence rate as high as 14.9% of IGD.

Online Gambling

Online gambling possesses a unique set of risks. Combined with the challenges of the COVID-19 crisis, online gambling can be especially tempting and destructive for youngers and for those with gambling problems. There are several risk factors concerning the online gambling; the first one, is the easy access, in just a few clicks or taps, gamblers can access games and betting opportunities right from their devices. Also, while gambling in casinos allows people to socialize, online gambling is often done alone. And for those with a gambling problem, it may be easy to conceal how often and where they're playing.

In terms of time, online gambling allows unlimited play time to gamblers: gambling sites are open 24/7, giving people the chance to play night and day.

Economically speaking, online gambling gives the impression of holding unlimited money to bet. Using a credit card enables fast bets and losses. In casinos, money is exchanged or loaded onto registered loyalty cards. But credit cards require no loading or reloading, making it easier to lose track of the money spent.

Another relevant matter in the digital world is the constant increase of unregulated websites that may take advantage of players and can be hard to track down and take action against if problems occur.

To conclude, cybersecurity issues may occur as well. Because sites can be unregulated, personal data, including credit card and banking account numbers, may be vulnerable and accessible to hackers or scammers. Additionally, contact information may be shared with third-party partners to promote gambling sites and offers.

4. Main findings of the research

Beside a detailed desk research, the study consists also of field research. Specifically, the field research was two-fold: on one hand, a survey was conducted online on 70 people aged 16-30, on the other hand interviews were conducted on 4 people working with the group of interest.

In the following paragraphs the main findings of the field research will be explored.

4.1 Survey report

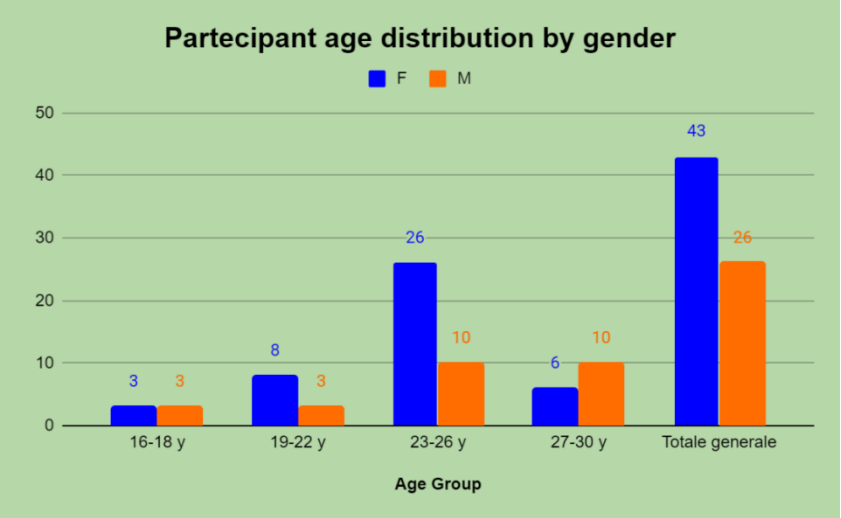
This quantitative survey conducted on 70 young people aged 16-30 years old allowed to identify specific patterns and correlations between particular socio-economic characteristics, and the possibility of falling into online traps.

This section shows all the data collected and their interpretation. Specifically, the tables contain the correlation made between a cluster and the agreement or disagreement with the different statements asked to the participants. What was obtained is as follows:

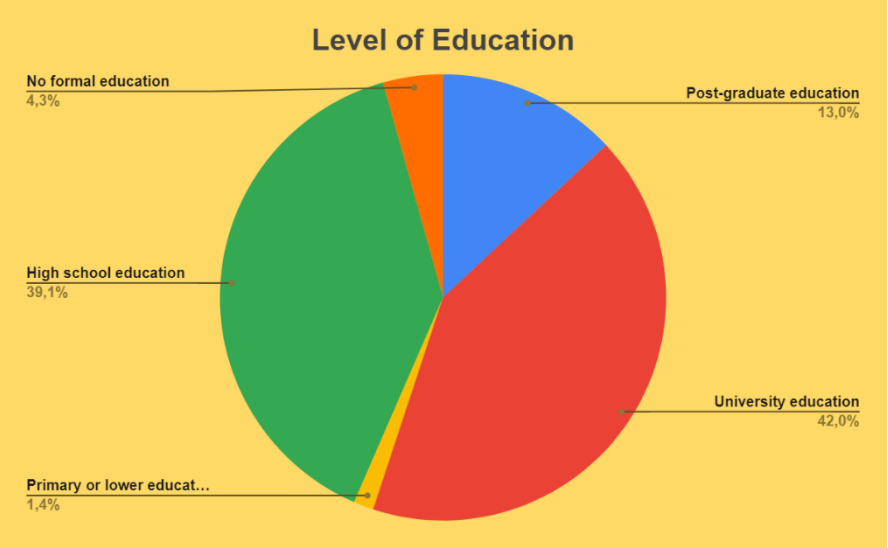
1. **Socio-demographic structure of the sample**

Age, gender

The survey involved 43 women and 26 men, aged between 16 and 30 years. The majority of the respondents belonged to the 23-26 age category (36), while the group with the lowest number of respondents belonged to the 16-18 age group (6).



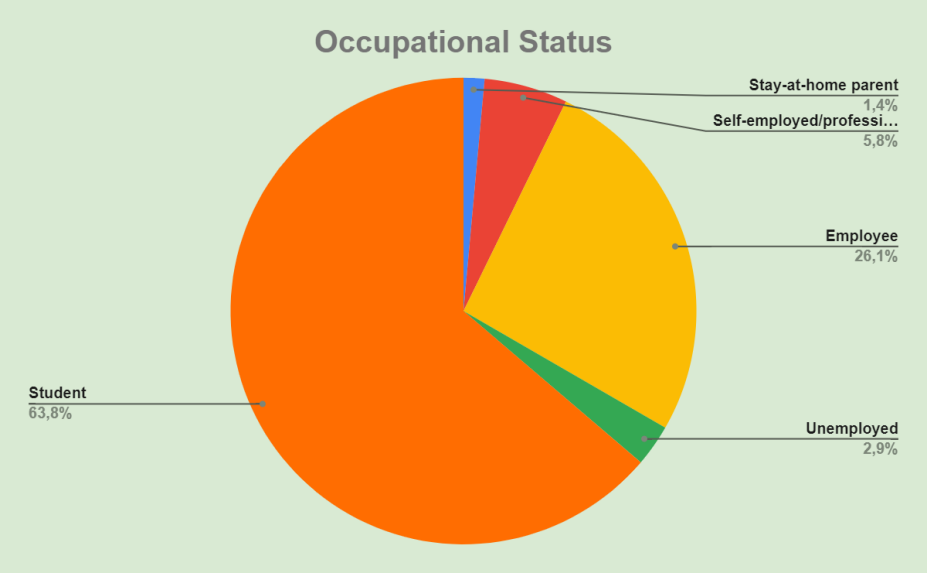
Level of education



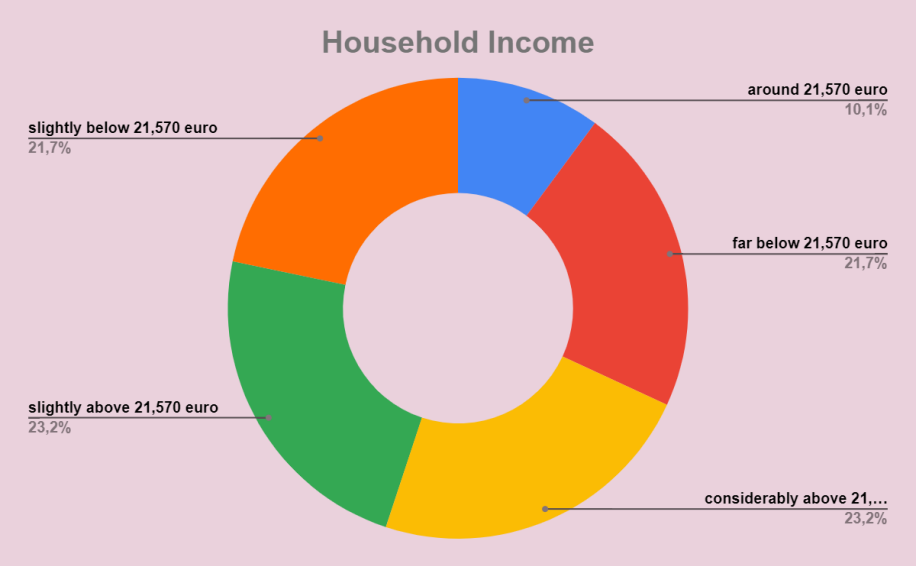
From the analyses carried out on our sample of participants, it is clear that there is a significant and almost equal number of people who have completed university education (29), and those who have obtained a high school education (27), followed by the cluster of participants who have attained a postgraduate level of education, which represents the third largest cluster (9). Only 3/69 participants had no formal education at all and only one participant had completed primary school or less.

Occupational status and Levels of Income

From the analyses conducted through the survey, it is evident that the majority of participants are students (63.8%). The second largest participation group is employees (26.1 %). The remaining participants are self-employed (5.8%), unemployed (2.9%) or stay-at-home parents (1.4%).

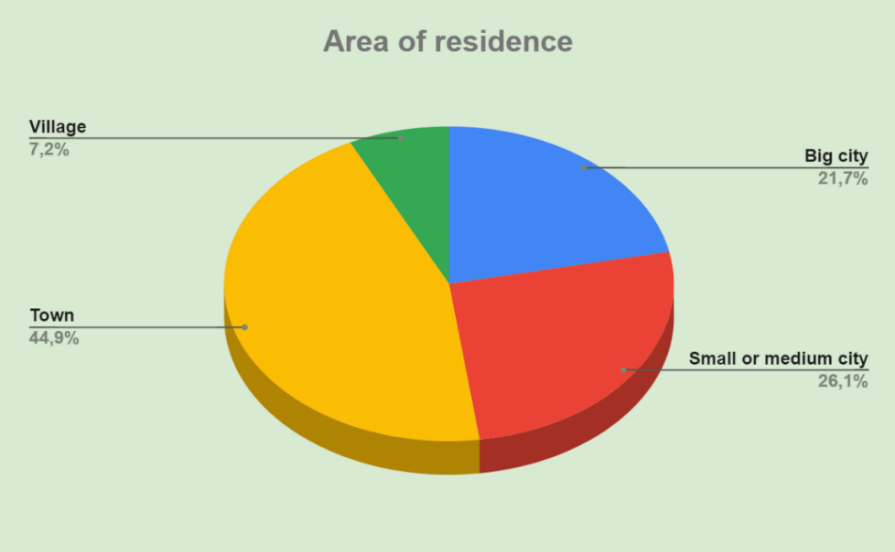


Regarding household income in the third quarter of 2022, as you can see in the chart below, our participants are mostly distributed in different income brackets with the average percentage being around 20 percent. Exception made for those who receive an income around 21,570 euros who got an attendance of 10.1%.

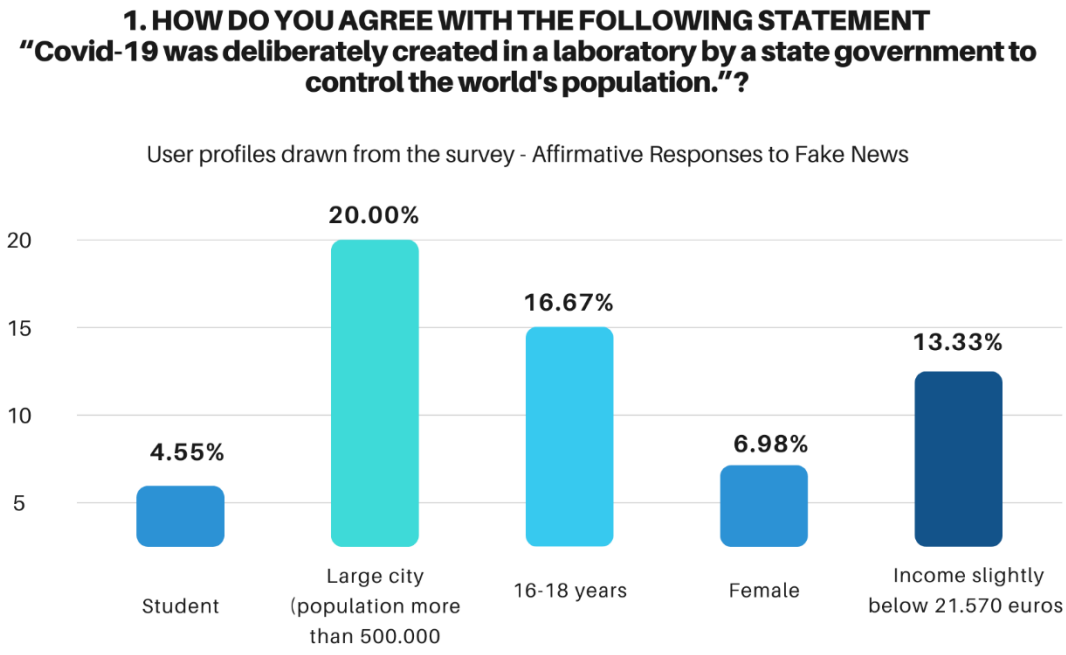


Area of residence

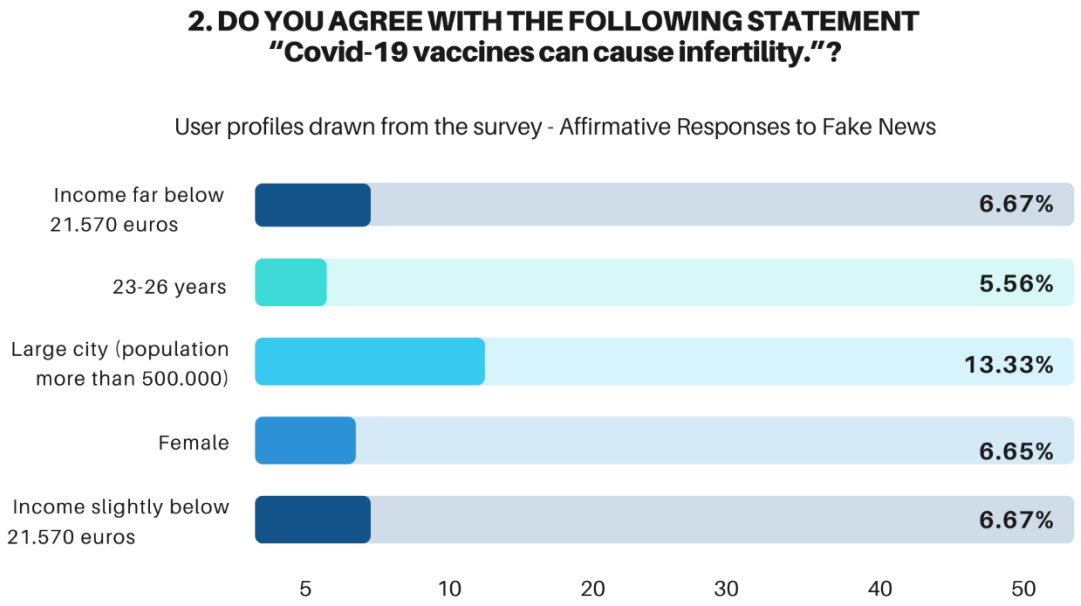
Most respondents (44.9%) live in a Town, while the remaining 26.1% reside in a Small or medium city. Another 21.7% of the participants live in a large city, while only 7.2% of the respondents live in a village. Obtaining the geographic location of the participants allow us to understand the origin of the survey participants, a fact that allowed us later further analysis.



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



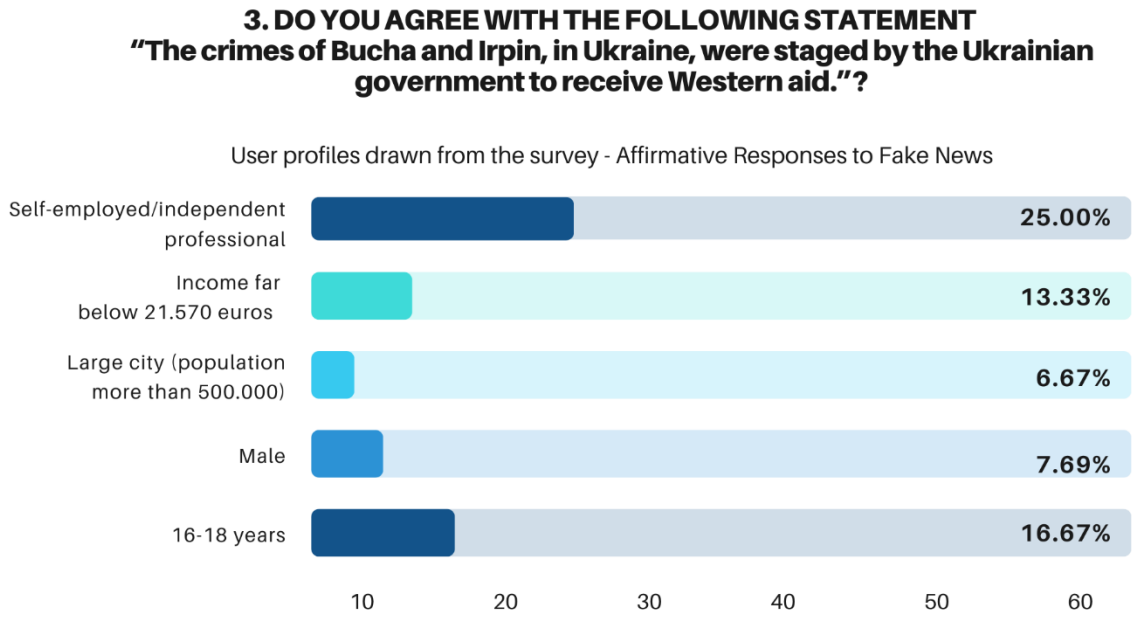
Taking into consideration the percentages resulting from the correlation between the above statement and the different clusters considered, we can observe that the group of respondents belonging to: the 16-18 age group (16.67 %), among those living in a large city (20 %), among those with an income slightly below 21,570 euros (13.33 %) female (6.98 %) and student (4.55%) account for the highest percentage among those who consider the false statement "accurate."



To the question "Can the Covid-19 vaccine cause infertility?" several conflicting positions emerged, for understandable reasons.

Taking into consideration the most relevant and impactful correlations in terms of research, the clusters that most supported the false statement were: the age group "23-26 years old" with 5.56 %, those with "income far below 21,570 euros" and "income slightly below 21,570 euros" both at 6.67 %. Then the "Female" cluster with 6.65%.

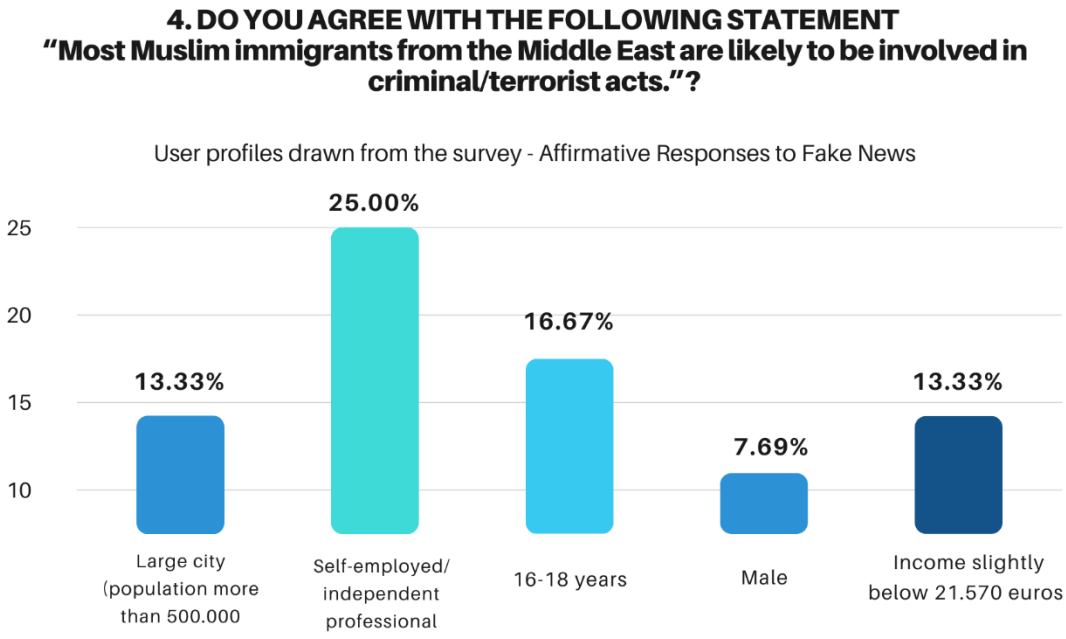
Finally, the analyses conducted show that those who most supported the false statement was among those living in "large cities" with 13.33%.



The correlations carried out between the different clusters considered and the mendacious statement posed to the participants, reflects their different level of acceptance to the question.

Among the clusters that answered affirmatively "accurate" we find the "Age 16-18 years" group with 16.67%, "Income far below 21,570 euros" with 13.33%, the "Male" group answered in the affirmative with 7.69%, followed by those living in a "Large city" reaching 6.67%.

Finally, the highest percentage of adherence to the statement was found in the "Self-employed/independent professional" group with (25%).



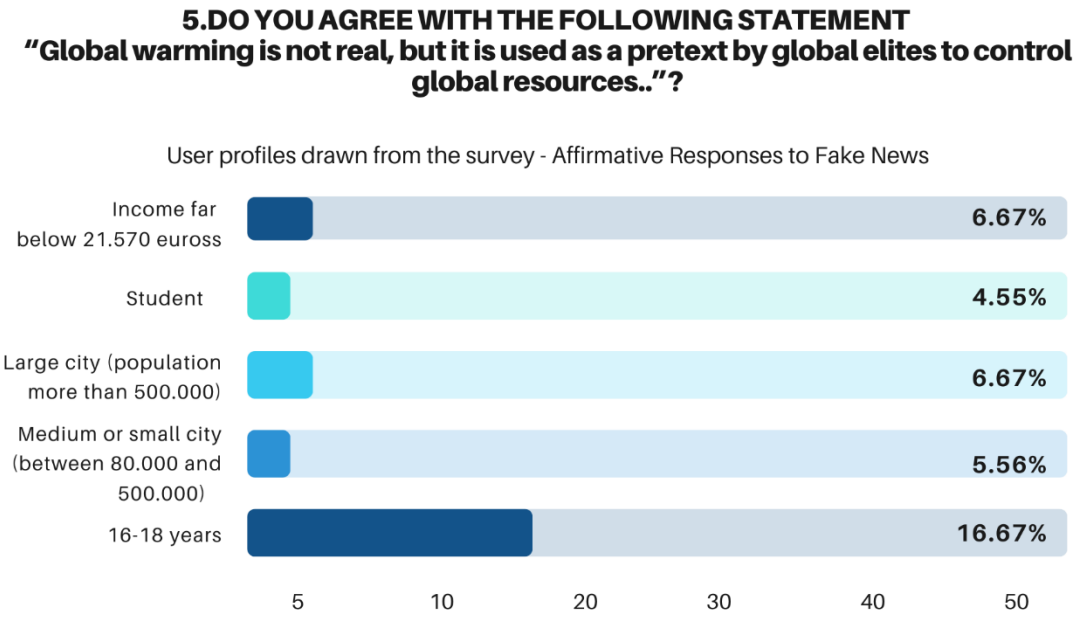
The correlations carried out between the different clusters considered and the mendacious statement posed to the participants, reflects their different level of acceptance to the question.

The graph highlights how the different clusters interfaced with ethnic and racist prejudice by answering the question, "ARE MOST MUSULMAN IMMIGRANTS FROM THE MIDDLE EAST MOST LIKELY TO BE INVOLVED IN CRIMINAL/TERRORIST ACTS?"

Our analysis shows that the groups most likely to consider the statement "Accurate" were:

the "16-18 age" group with 16.67%, "Income slightly below 21.570 euros" and "Large city" both at 13.33%, and the "male" cluster 7.69%.

The highest percentage of those who adhered to the false declaration was found in the "Self-employed/independent professional" cluster with 25 %.



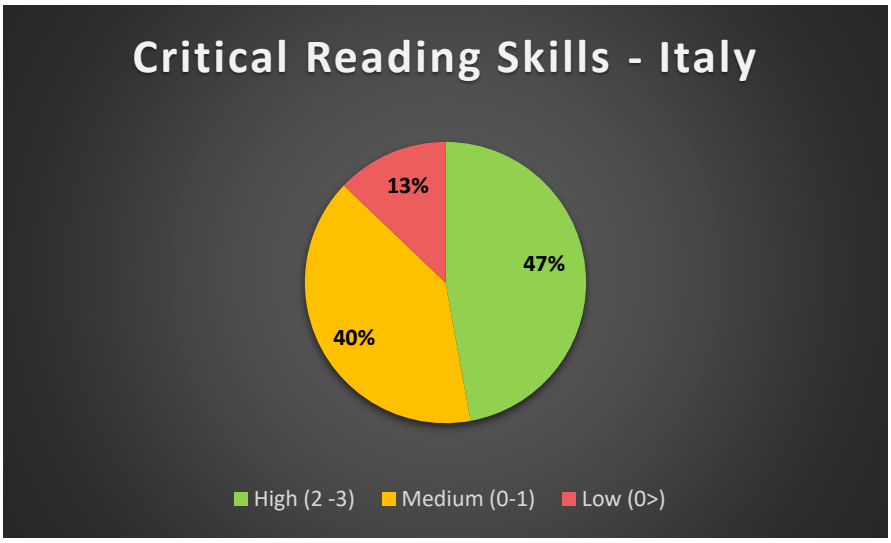
Concluding this part of quantitative and interpretive analysis of the collected data, a careful correlation clarifies the relationship between misrepresentation and the different clusters considered.

It is in fact asked "**GLOBAL WARMING IS NOT REAL, BUT IT IS USED AS A PRETEXT BY GLOBAL ELITES TO CONTROL GLOBAL RESOURCES.."?"**.

From the analysis of the related data, we were able to extrapolate profiles where they reject the climate crisis as most truthful, considering the statement shown above accurate.

Among those who answered in the affirmative we have the "**16-18 years old**" cluster with 16.67% agreement. Those who live in "Medium or Small Cities" (5.56%) and those who live in "Large City," seem most exposed. An agreement rate of 6.67% was found in those who receive an "**Income far below 21.570**" during the last year.

Finally, with a slightly lower intensity, but emerging among the many clusters analysed is a conspicuous presence of students (4.55%) who have considered the fake news to be true.

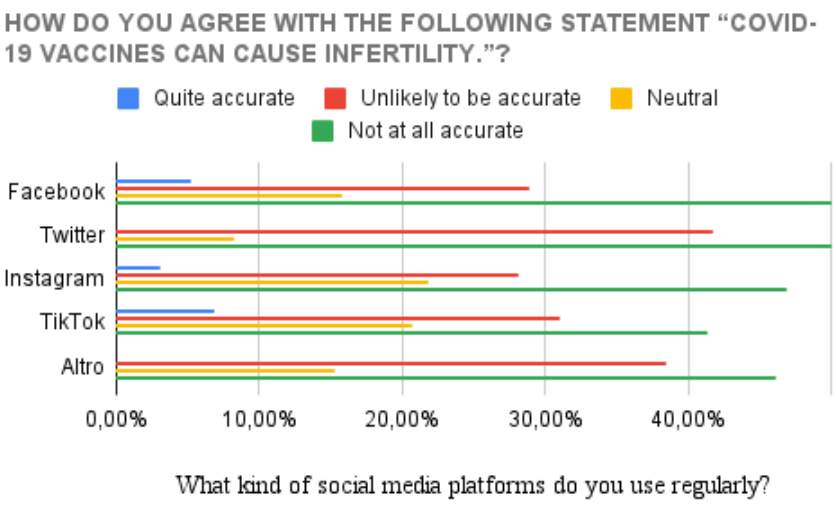


Thanks to this questionnaire, it has been possible to analyse the critical reading skills of youth. As it is easy to understand from the graphic above, almost half of the participants present high level of critical reading skills, allowing them to recognise more easily fake news from real ones. On the other hand, 13% of the participants to the questionnaire resulted to have low critical reading skills, which will make them more vulnerable to the risks they may encounter online.

3. Social media use and General Risk exposure

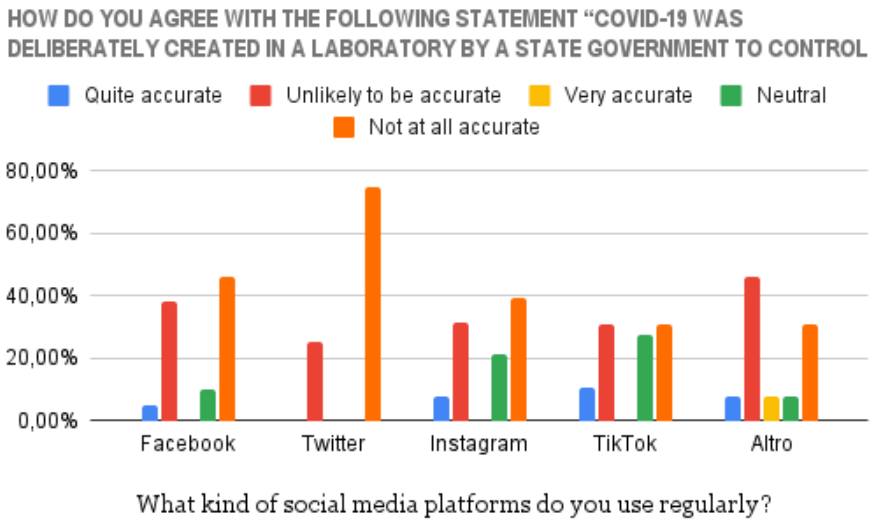
Social media are an almost totalizing dimension of interaction, communication, and contribute to new realities and dynamics. Not only that, social networks are increasingly an important tool fortransmission and collaboration among networks of people, communities and organisations empowered by technological capabilities and mobility.

For this reason, one part of the investigation focused on understanding how the use of social media can influence opinions and expose one to the risks of spreading fake news and misinformation. Correlation of data, development of appropriate graphs was carried out in order to have a clear visual representation of the impact of different channels:



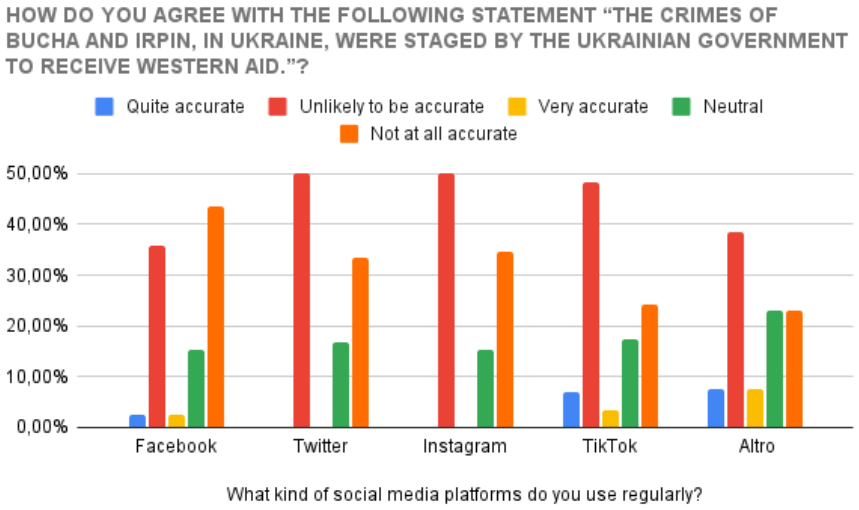
Correlating the users of social platforms and the degree of agreement to the following false statement.

An interesting fact that emerges from the graph is the absence of endorsements for those who use **Twitter** or other platforms, while we find **Tik Tok** followers in first place with 6.90%, followed by **Facebook followers** 5.26% and Instagram followers 5.26%, among those who consider the statement accurate enough.



Correlating the users of social platforms and the degree of agreement to the following false statement.

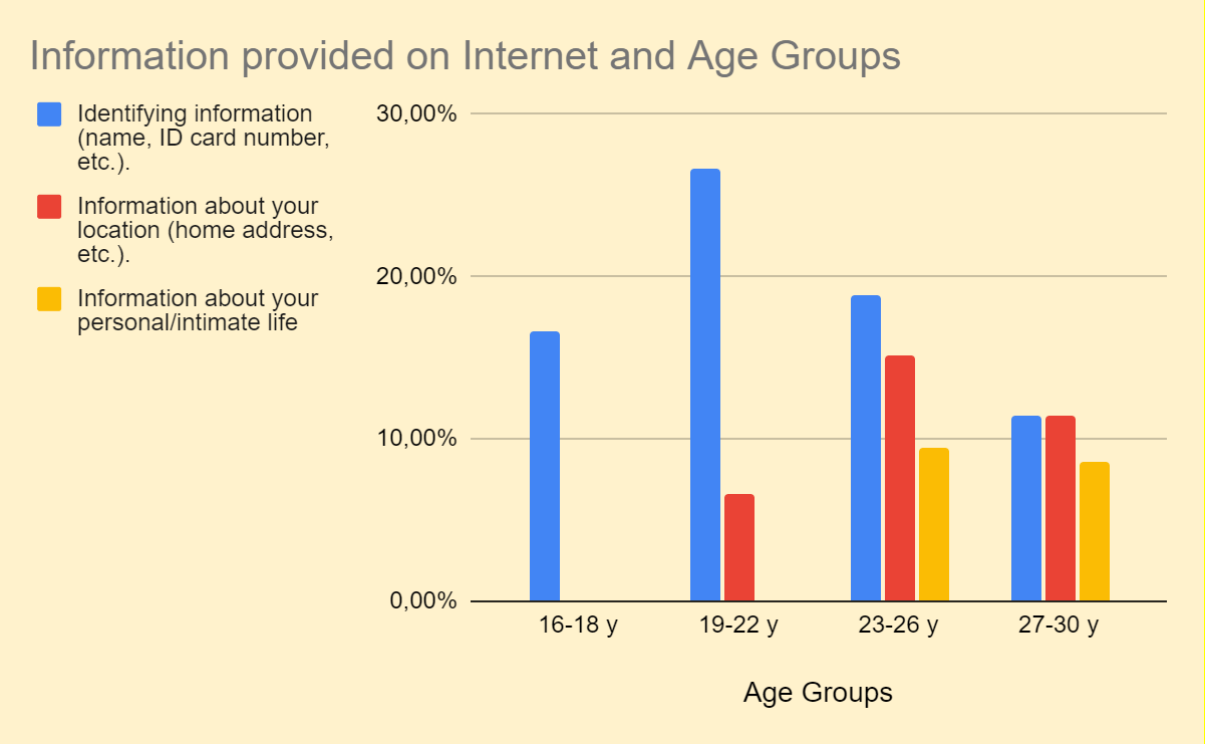
Continuing to emerge is the absence of affirmative statements for those using **Twitter**, while **Tik Tok** comes out as the platform with the highest percentage where users consider the statement "**Quite accurate**" with 10.34%, followed by **Instagram** 7.89%, other platforms 7.69% and **Facebook** 5.13%.



Correlating the users of social platforms and the degree of agreement to the following false statement.

The highest percentages of non-adherence to the statement were found among those who use **Twitter** and **Instagram**, in contrast the highest percentages among those who think it is accurate enough, we find other platforms with 7.69% and **Tik Tok** with 6.90%, and finally **Facebook** with 2.56%.

4. The Online risks exposure and socio-demographic factors

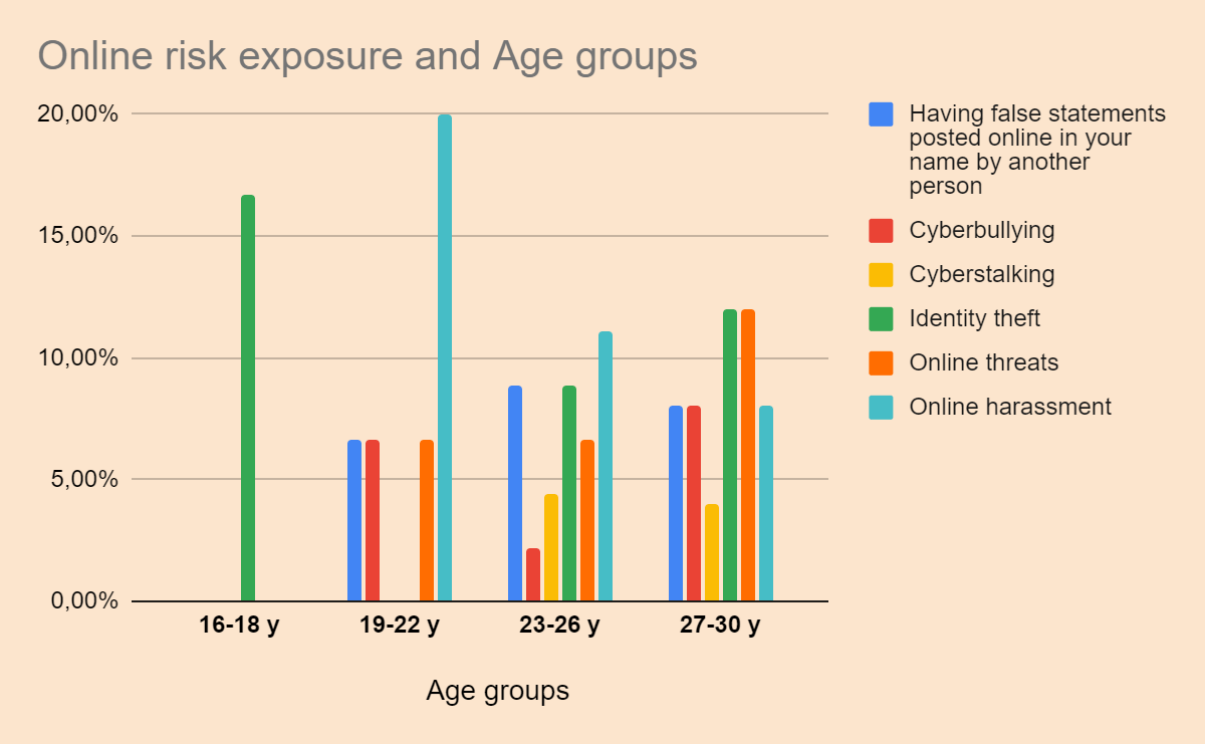


This chart shows the correlation between the different age clusters and the type of information they tend to share.

It appears evident that all four age clusters tend to share information regarding their identity (such as name, ID Card Number etc.). Among them the 19-22 y group, reached a 26.67% (4/15), followed by the 23-26 y with 18.87% (10/53), and finally 16-18y with 16.67% and the lowest percentage of 11.43% for the 27-30 y cluster.

Different is the case with the type of information pertaining to location (such as address etc.), the 23-26 y cluster seems to be more to share such types of information with 15.09%, followed by 27-30 y with 11.43%, and 19-22 with 6.67%.

A final type of information provided by survey participants, and one that is relevant, is personal/intimate information. Only the 23-26 year old group with 9.43% and the 27-30 year old group with 8.57% conveyed more of this type of information.



In this section, we tried to extrapolate which age groups had more exposures of incurring online risks.

We found relevant correlation with age groups and the following categories of violence: Identity Theft, Online harassment, Cyberstalking, Online threats and Having false statement posted online.

Identity theft occurred most in the 16-18 y age group with 16.67%, followed by the 27-30 y group with 12% and finally 23-26 y with 8.89%.

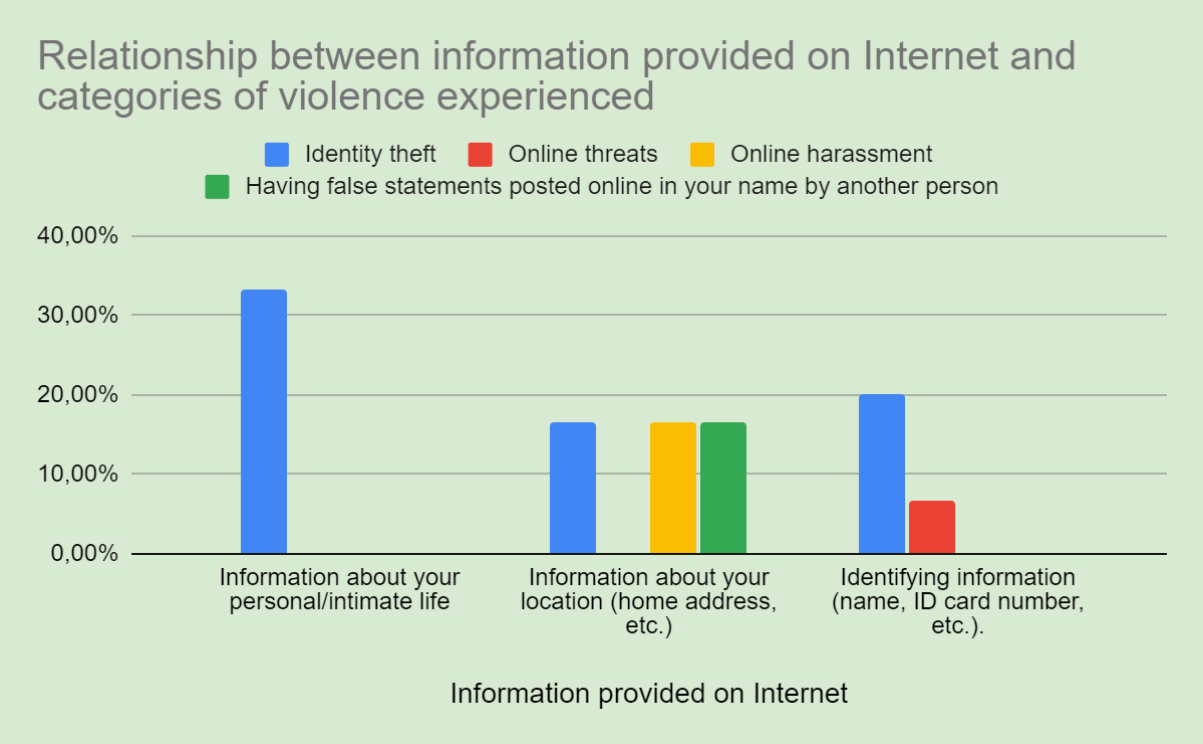
Another risk found is that of Online harassment. Specifically, the age group with the highest exposure to this risk is the 19-22 y group with 20%, followed by the 23-26 y group with 11.11% and finally the 27-30 y group with only the 8%.

As for the presence of cases of online threats received by our survey participants. The 27-30 y group had the most relevant percentage with 12%, followed by the 19-22 year old and 23-26 year old clusters with both 6.67%.

The age groups that had more exposure to cyberstalking, are 23-26 y with 4.44%, and the cluster 27-30 y with only 4%.

Cyberbullying was instead reported by 8.89% of participants belonging to the 23-26 y group, a similar result with the 27-30 y group with 8%. The lowest percentage was shown in the 19-22 y group with 6.67%.

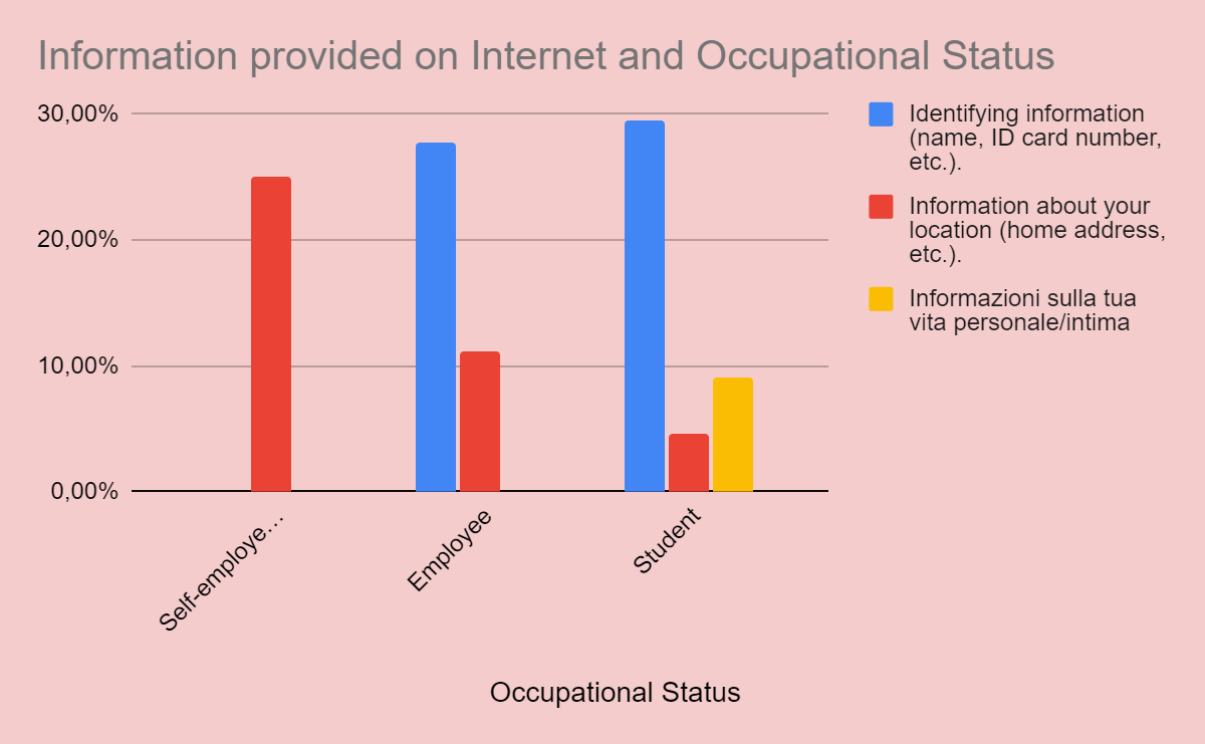
Finally, the groups that showed particular exposure to the risk of "Having false statement posted online " are the 23-26 y cluster at 8.89%, then the groups 27-30 y with 8% and finally those who belong to the 18-3 group with 6.67%.



From the data collected and processed in the following section, there is a correlation between the information provided on the Internet by participants and their exposure to the risks of Identity Theft, Online Threats, Online harassment, and “Having false statement posted online"

For those who provided Personal/Intimate Information 33.33% experienced incidents of Identity Theft. In contrast, in the category of respondents who provided information about their location, there were incidents of identity theft, cases of online harassment, and online threats all with 16.67%.

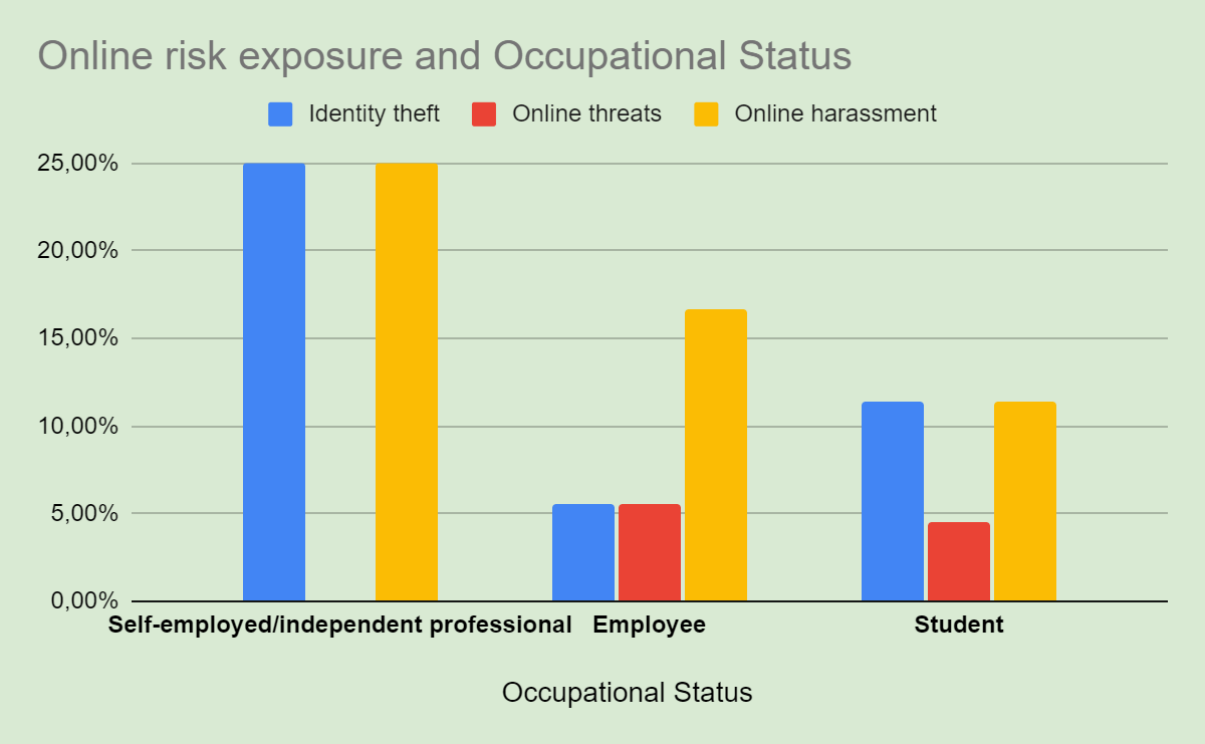
Finally, we found among those who provided Identifying information (name, ID card number, etc.) a 20% of Identity theft and a lower percentage of Online threats with 6.67%.



This part analysed the relationship between occupational status and the types of information released on the web.

This allowed the analysis of the different groups involved, among them we have the 25 % of Self-employees who provided information regarding their location. As for the Employee, the release of identifying information was prevalent with 27.78% followed by information regarding their location by 11.11%.

Finally, the largest category, that is, students, who showed a high percentage, 29.55% in providing Identifying information. Part of them, 9.09%, provided personal/intimate information, and finally a small percentage 4.55% provided information regarding their location.



In this section we move attention toward the correlation between different clusters by occupational status and their exposure to the risks of Identity Theft, Online threats, Online harassment.

In particular, the Self-employed cluster reached percentages of 25% in exposure to Identity theft and online harassment with 25%. On the other hand, if we analyze the Employee category, it shows the highest percentage of Online harassment with 16.67%, followed by exposure to Identity Theft with 5.56% and finally 5.56% in Online Threats.

Among those belonging to the student cluster, we show the following percentages: 11.36% exposure to Online harassment, 11.36% reported receiving Identity Theft, and finally 4.55% of the following cluster reported experiencing Online Threats.

4.2 Interviews

Interviews were conducted with 4 professionals: two teaching professionals - a high school and a conservatory professor - and two psychologists. They all work with the target group, even though the high school teachers cover the youngest range of the target group.
The interviewees agreed on the fact that the youngsters embed social media into their daily life and consider them as a relevant component of their identity. Once they become young adults, as they mature, their approach towards social media changes gradually and it becomes less engaged: they continue to enjoy social media but their identity and personal life is less integrated. Moreover, professors and psychologists agreed on the fact that Covid-19 has enhanced the time spent online, and social media became the main channel of communication.
According to their experience, young people share **personal information** online because it is a way to know each other, to establish new social relationships - which is even more common when they feel lonely. They also share **intimate media content** because they trust the recipient, in order to be appreciated sexually or to give value to that moment, rather than have just a memory. The interviewees have had little experience with **gambling addiction** so they just suggested possible reasons for it, such as the willingness to easily gain money by little effort, or boredom, willingness to try something new and the thrill of betting.

As regards to the level of media use, they all agreed that young people use social media on a daily basis, resulting in an everlasting connection, but the majority of them use social networks only to stay in contact with their own friends, not to **inform themselves** and read the news. When interested in the news, young people seek for what they are already interested in. As a matter of fact, the interviewees agreed that young people fall for **fake news** and disinformation because, on one hand, they do not possess the adequate tools to recognise the truth from the false, especially during an infodemic, and on the other hand they are not interested enough to check and double check the source of information and to carefully read the articles.

It was also agreed that **education and preventive information** - how to recognise the risks, how to avoid or mitigate them - are the best way to protect the youngest. All the interviewees were not aware of any past or ongoing project or initiative, apart from the ones launched internally by the school of affiliation for their own students.

The interviewees agreed in almost every point, the only aspect which was more diverse is about young people's **critical thinking**: the psychologists stated that youngsters have a high level of critical thinking, while the teaching professionals affirm that, given their age, they do not have a mature critical thinking, which still needs to be trained.

4.3 National laws and recommendations

National laws are relevant to make the victims feel protected, encouraging them to report such despicable crimes. In Italy, steps forward from a cultural standpoint have been made: violations have been clearly identified and an effort in terms of jurisdiction is underway. New laws and regulations have been passed with great consensus to regulate the virtual space that is increasingly becoming part of young people's leisure time. Preventing the abuses and mitigating the negative implications of the online world is the main objective of the regulatory national system in the last 10 years, which is proceeding also through the supervision of the European Union, as it is constantly evolving and difficult to monitor.

Cyber bullying

Law: A new law dealing with the phenomenon of cyberbullying came into force on 18 June 2017. That is **Law No. 71 of 29 May 2017**, Provisions for the protection of minors for the prevention and fight against the phenomenon of cyberbullying, published in the Italian Gazzetta Ufficiale on 3rd June 2017.

What to do: A victim of cyberbullying who is 14 years old or older may submit a request to the operator of the website or social media on which he or she has received insults and threats, for the obscuring, removal or blocking of the content disseminated on the network.

If the responsible person has not done so within 24 hours, the person concerned may address a similar request to the Data Protection Authority, which will remove the content within 48 hours.

If the victim is under 14 years of age, the request must be submitted by the parents or guardian.

Preventing cyberbullying: The victim of cyberbullying should promptly inform a trusted adult (e.g., teachers or parents). It is important for the latter to be aware of the amount of time their child (especially a minor) spends on the Internet and to monitor its activity. It is also essential that special training courses are organised in schools for teachers and students to help them prevent cyberbullying.

Revenge Porn

Law: **Law No. 69 of 19 July 2019**, introducing other provisions to protect against domestic and gender-based violence, provides penalties for the phenomenon, stating in Article 10 that:

'Whoever, after having made or taken them, sends, delivers, assigns, publishes or disseminates images or videos with sexually explicit content, intended to remain private, without the consent of the persons depicted, shall be punished by imprisonment from one to six years and a fine ranging from EUR 5.000 to EUR 15.000.

The same punishment shall apply to any person who, having received or acquired the images or videos referred to the above-reported paragraph, sends, delivers, assigns, publishes or disseminates them without the consent of the persons represented for the purpose of causing them damage.

The penalty shall be increased if the acts are committed by the spouse, including a separated or divorced spouse, or by a person who is or has been linked by emotional relationship to the offended person, or if the acts are committed by means of computer or telematic tools.

The penalty is increased by between a third and a half if the acts are committed to the detriment of a person in a condition of physical or mental inferiority or to the detriment of a pregnant woman.

The offence is punishable on complaint by the victim.

The time limit for filing a complaint is six months.

The dismissal of the complaint may only be procedural.

The law entered into force on 9 August 2019.

What to do: Against revenge porn, there is an emergency channel for potential victims that was set up in cooperation between the Italian Data Protection Authority and Facebook.

The channel was created to help people who are afraid of their intimate photos or videos being spread without their consent.

The current measure is one of the tasks assigned to the Authority by the regulatory changes introduced to the Privacy Code in December 2021.

It is now the Italian Data Protection Authority's task to receive reports from anyone, including minors over the age of fourteen, who have a well-founded reason to believe that audio recordings, videos, or photos with sexually explicit content that interest them may be published on digital platforms without their consent.

Once the report is received, the Italian Data Protection Authority acts promptly to order a preventive block against the platforms indicated by the reporter, usually through the implementation of specific technologies, such as hash codes.

Preventing revenge porn: In order to avoid becoming a victim of revenge porn, it is essential not to send sexually explicit photos or videos, not even to intimate partners. It is often the latter who, at the end of the relationship, send the pictures to friends or forward them to revenge porn chats. Likewise, it is important not to keep such images on one's own devices or in the cloud, as they could be hacked.

If one decides not to follow this advice, it is still good practice to only take pictures that do not allow the protagonist to be recognisable, thus avoiding framing the face and other physical features, such as tattoos or distinguishing marks, that could easily be traced back to a person.

Cyberstalking

Law: In 2017, The Supreme Court ruled on the issue of the configurability of the crime of stalking, pursuant to **Article 612 bis** of the Criminal Code, when the harassing or persecutory behaviour typical of the criminal offence is perpetrated through the use of new technologies or tools related to them.

The judgement has helped to establish an incisive form of protection, both preventive and repressive - the sentence ordinarily imposed for the crime of persecutory acts ranges from a minimum of six months to a maximum of five years - against those who, given the particular pervasiveness of the media showcase of Facebook message boards, are exposed to public ridicule on a daily basis.

What to do: If one is the object of threats, insults and harassment in the web space, they are the victim of a crime that can be reported to any office of the Communications Police. See addresses and phone numbers at www.commissariatodips.it.

Digital Identity Theft

Law: The conduct of one who commits digital (or computer) identity theft can fall under two criminal categories:

- The crime of substitution of person (**Article 494** of the Criminal Code)
- The offence of computer fraud (**Article 640ter(3)** of the Criminal Code).

Article 9 of Law Decree No. 93/2013 introduced in the third paragraph of Article 640-ter of the Criminal Code, a new aggravating circumstance with special effect of the crime of computer fraud: the theft of the user's identity with the declared intention of providing greater criminal protection.

In the offence of computer fraud (Article 640ter(3) of the Criminal Code), a user's identity theft is therefore an aggravating circumstance of the crime of computer fraud.

Computer fraud aggravated by digital identity theft occurs when a person, by altering a computer system in any way, succeeds in obtaining an unfair profit with consequent damage to the victim.

The penalty is imprisonment of two to six years and a fine of between €600.00 and €3000.00 (Article 640ter(3) of the Criminal Code).

How to prevent it: While this is not an exhaustive list, here are some useful tips for protecting personal data and preventing anyone from getting hold of them:

- choose non-trivial passwords with lower case letters, upper case letters, numbers and symbols and update them periodically;
- be careful about opening suspicious emails and in any case do not communicate your personal data, email account credentials, passwords and pins;
- access social networks from personal internet, and avoid the public open one.

5. Conclusions and recommendations

The research resulting in the current country report is embedded within the Erasmus Plus project **RISE - Action-based approach in addressing and mitigation risks of young people in online social networks**. The general goal of the above-mentioned project, and thus of the country report, must be identified in its persistent aim to broadly draw a clear picture of the online scenario and its implications in the personal and social context. The project aims at investigating, understanding online risks youngsters may face online, and providing them with tools to prevent and mitigate such dangers. As a matter of fact, the Erasmus+ Rise aims at developing:

- A **methodology** structured with the purpose of tackle the needs of young people in the framework of digitalisation, especially of social media in the age of the COVID-19 pandemic;
- A **game** for young people to educate them on online risks, in order to make them able to identify, prevent and mitigate online risks, particularly on social networks; and
- A **Capacity Building Programme** for youth trainers designed with the aim of helping them to build capacity when dealing with risks of young people in social media.

The report is based on a two-fold methodology consisting of **desk research** and **field research**, conducted in a complementary way. Desk research has been carried out via a literature review and field research has been conducted via a quantitative survey and interviews, with the purpose of understanding and assessing the actual weight of the risks of digitalization.

The literature review showed that Gen-Z consisting of "digital natives" - due to their ease with technology and the increasing time spent online - are likely to face a wide range of risks online. It includes **fake news**, with youngsters being characterised as "new avoiders", **cyberbullying** especially involving minors, **identity theft** causing financial and emotional damage, **grooming** which is an increasing phenomenon, and **internet addictions**, including **internet gaming disorder**, which negatively impact attention, memory, sleeping patterns and physical well-being.

As regards the field research, both the survey and the interviews revealed interesting data and information.

Starting with the survey, the empirical research and analysis carried out on an Italian sample of participants of different professional status, age, etc. showed how exposure to manipulative, deceptive, harassing and misinformative risks can have different outcomes based on the different social platforms used, on the level of education, income and accessibility to different sources of knowledge, age group, occupation and countless other factors. Specifically, the **group aged 16-18**, those who live in **large cities** and the ones having an i**ncome below the Italian average** are more likely to fall for fake news. Another relevant data emerged is about the platforms used: those using **Twitter** are far less likely to believe in fake news, vice versa **Tik Tok** users demonstrated a tendency towards disinformation.

The interviewees agreed on almost all the main points, among which that young people share **personal information** and **intimate content** because they trust the recipient and treat social media as another way to communicate, juxtaposing online and in-person relationships. It was added also that the target group is not likely to search for information, it is likely to fall for **fake news** mainly because young people do not possess the appropriate tools to filter information or because they are not willing to check and double check the source of information and to carefully read the articles. Typologies of risks include four broad categories: content, conduct, contract and contact.

Just as in everyday life, a zero-risk digital environment is unattainable. However, setting the conditions for a safer one is feasible. Professors and psychologists agreed that **appropriate education and preventive information** - how to recognise the risks, how to avoid or mitigate them - are the best way to protect the youngest, especially when digital education is tailored on the different ages of users.

Few key points have been identified to face the digital space risks:

- **Information campaigns and resources**: Youth-centred support outside of the school and reporting mechanisms; information and guidelines for parents, youngers and teachers; awareness-raising activities; campaigns in partnerships with other community actors.
- **Teacher support:** Coordinated policy and frameworks; Information campaigns and reporting mechanism; information and guidelines for parents, teachers and youngers; resources and pedagogical tools, examples of good practice; teacher education on identifying and reacting to digital risks; creation of information materials and training tools.
- **Teenager-centred support outside of the school** and reporting mechanisms for illegal digital activity: helplines for victims, parents and teachers to receive support on psychological, social, legal or administrative processes.
- **Coordinated policy and frameworks elaboration of legal frameworks** and/or action plans; laws, measures and enforcement; coordination across jurisdictions: the digital world does not respect national boundaries.

In order to develop a tool able to educate youth on how to prevent, identify, mitigate and fight online risk, the project will develop a game taking into consideration what learnt through the current national report.

With the aim of being attractive, the game has to be user-friendly and visual oriented. It has to replicate possible daily life situations, to facilitate the replicability and adaptability of what the used has learnt and lived online through the game to his/ her real life. The scenarios have to be designed with the purpose of stimulating the critical thinking of the gamers, therefore multiple choices which are really easy to take into consideration are necessary, providing the user with the chance to think and select their preferences. The game will have to account for the consequences of each action and each scenario will include possible consequences based on the choices made by the user.

In conclusion, despite the innumerable benefits that today's societies enjoy in terms of commercial and informational exchanges, the complexity of the social media phenomenon and the digital world should not be underestimated, especially in terms of the possible dangers one may face.

References

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

Papapicco, C., Lamanna, I. and D'Errico F. 2022. Adolescents' Vulnerability to Fake News and to Racial Hoaxes: A Qualitative Analysis on Italian Sample. *Multimodal Technologies and Interactions.* hptts://doi.org/10.3390/mti6030020

UNESCO. Journalism, 'Fake News' and Disinformation: A Handbook for Journalism Education and Training. Available online: https://en.unesco.org/fightfakenews (accessed on 22 August 2022)

Herrero-Diz P, Conde-Jiménez J, Reyes de Cózar S. 2020. Teens' Motivations to Spread Fake News on WhatsApp. Social Media + Society. July 2020. doi:10.1177/2056305120942879

Sørensen, K., Pelikan, J. M., Röthlin F., Ganahl K., Slonska Z., Doyle G., Fullam J., Kondilis B., Agrafiotis D., Uiters E., Falcon M., Mensing M., Tchamov K., van den Broucke S., Brand H. 2015.

Health literacy in Europe: comparative results of the European health literacy survey (HLS-EU), European Journal of Public Health, Volume 25, Issue 6, December 2015, Pages 1053–1058, https://doi.org/10.1093/eurpub/ckv043

Midoro V. 2018. Digital literacy e nuovi analfabeti, perché bisogna ripensare il sistema educativo. Agenda digitale. Available online at (last access on August 23rd 2022): https://www.agendadigitale.eu/scuola-digitale/digital-literacy-e-nuovi-analfabeti-perche-bisogna-ripensare-il-sistema-educativo/

Brando, M. 2022. Il rapporto degli italiani con media e fake news. Magazini Treccani. Available online at (last access on 30 August 2022): https://www.treccani.it/magazine/atlante/societa/Il_rapporto_italiani_media_fake_news.html

Zollo, F. and Quattrocchi W. 2017. Misinformation spreading on Facebook. Available online (web pdf): https://arxiv.org/pdf/1706.09494.pdf

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

Commissione parlamentare per l'infanzia e l'adolescenza (2019) "Indagine conoscitiva su bullismo e cyberbullismo", Roma.

Servizio Polizia Postale e delle Comunicazioni - Polizia di Stato e Save the Children Italia Onlus (2021) L'abuso Sessuale Online In Danno Di Minori. Available at: https://www.commissariatodips.it/dossier-dati_def.pdf

Adamczyk R., (2019), Non-substance addictions in the context of individual and social health, Social Pathology & Prevention, vol.5, pp.23-28

To learn more: https://www.stateofmind.it/2021/03/internet-gaming-disorder-conseguenze/

Burns, T. & Gottschalk, F. eds. (2019). Educating 21st Century Children: Emotional Well-Being in the Digital Age. Educational Research and Innovation, OECD Publishing, Paris, https://doi.org/10.1787/b7f33425-en.

Statista, 2023. Do you know anyone who has been victim of revenge porn? Available at: https://www.statista.com/statistics/1092744/spread-of-revenge-porn-in-italy/

Project's Partners

Institute Of Entrepreneurship Development
https://ied.eu/
info@ied.eu
https://www.facebook.com/ied.europe/

VITALE TECNOLOGIE COMUNICAZIONE - VITECO S.r.l
https://www.vitecoelearning.eu/en/
projects@jogroup.eu
https://www.facebook.com/VITECO.eLearning.LMS.SeriousGames.SCORMConversion

BK Consult GbR
https://bk-con.eu/
info@bk-con.eu
https://www.facebook.com/bkcon.eu

Learning For Integration Ry
https://www.lfi.fi/
marjaliisa@lfi.fi
https://www.facebook.com/LearningForIntegration

Asociatia Centrul Pentru Legislatie Nonprofit
https://clnr.ro/
office@clnr.ro
https://www.facebook.com/clnr.ro

Synthesis Center For Research And Education Ltd
https://www.synthesis-center.org/
info@synthesis-center.com
https://www.facebook.com/synthesis.cyprus

Action-based approach in addressing and mitigating risks of young people in online social networks

Co-funded by
the European Union

This project has been funded with support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.