CRPM Center for Research and Policy Making
... policy impact since 2004

CYBER SECURITY, CORPORATE SECURITY AND CRISIS MANAGEMENT INITIATIVE

Passage4Prevent: use of education to prevent youth online radicalization

# RESEARCH REPORT

## Baseline assessment for awareness raising and capacity building

Hedayah
countering violent extremism

Project funded by the EUROPEAN UNION

*This publication was produced with the financial support of the European Union. Its contents are the sole responsibility of Center for Research and Policy Making and does not necessarily reflect the views of the European Union nor of Hedayah"*


# TABLE OF CONTENTS

# 1 INTRODUCTION

With the development of modern technologies, especially the internet and its availability for the people around the globe, many social threats such as radicalization and violent extremism have also gained both global and cyber dimension. Thus, the opportunity the internet creates to communicate without having to travel and without being who you really are, has also become an opportunity for those who want to share content related to radicalization that leads to violence and incite violence. Hence, the radicalization, especially radicalization that leads to violent extremism is no longer associated with specific region, territory or even group of people. Moreover, by using the internet and social networks, the process of radicalization could be initiated from anywhere in the world, by anyone and could target individuals from all over the world including children. The latter, having in mind that are the keenest users of the internet and the social networks, are even more vulnerable to the cyber risks and threats.

It is therefore of utmost importance to understand the online radicalization as a complex phenomenon and that, one should examine it from different perspectives: content, process, methods and instruments used in the process, as well as the target groups it affects.

Within this study, we seek to contribute to the growing research on online radicalization of youth by assessing the perceptions of the high school students regarding the cyber security threats and radicalization, especially radicalization that can lead to violent extremism. We do this through examining how and how much they use the internet, what content they access, what challenges and threats they face while online and what do they do when faced with such challenges. Furthermore, the task of the study is to provide data driven evidence-based recommendations and programs aiming at reducing and preventing online radicalization and cyber threats in general.

The study is conducted within the project “Passage4Prevent: use of education to prevent youth online radicalization” supported by the European Union through Hedayah – Center of Excellence in countering violent extremism.

# 2 RESEARCH METHODOLOGY

The Project Management Team (PMT)[1], in cooperation with experts in cyber security and on-line radicalization developed a questionnaire for the purpose of the research. The questionnaire was designed as a tool for analysis of training needs of both high-school students and the front-line school workers through assessment of their pre-existing perceptions and attitudes towards on-line radicalization. Regarding its structure, the questionnaire covers the following three aspects (1) knowledge and skills needed by students and frontline school workers for recognizing and blocking radicalization content on internet (2) knowledge and tools required for reporting potential violent extremist behavior within the school, the community, and radical content on internet; (3) preferable methods for acquiring such skills.

In order to improve the data collection process in terms of efficiency and effectiveness, the PMT, in coordination with the experts, has also developed electronic version of the questionnaire using google forms application[2].

The CRPM Project Management Team collected the data from high schools in five municipality (Kumanovo, Shtip, Tetovo, Gostivar and Veles) and the City of Skopje in February and March 2020. The selection of the municipalities was done in two phases. In the first phase, as part of the previous project[3] implemented by the CRPM and its partners, were selected City of Skopje, Kumanovo, Tetovo and Gostivar based on the data about the number of foreign fighters from these municipalities that went to fight for causes related to Islamic radicalism. In the second phase, within the project Passage4Prevent – use of education to prevent youth online radicalization", to this municipalities were added two new municipalities from the Vardar and East Region (Veles and Shtip, respectively) to account for the rise of the far right extremism during the recent years in North Macedonia. Thus, the selection of municipalities covers both Islamic and religious radicalism and far right (nationalistic) extremism.

[1] Consisting of project implementing partners, the Center for Research and Policy Making (CRPM) and the Cyber Security, Corporate Security and Crisis Management Initiative (C3I

[2] Available at the following link:
https://l.facebook.com/l.php?u=https%3A%2F%2Fforms.gle%2FKmHcywYRYTSsTjwV9%3Ffbclid%3DIwAuR3tTa70mzqbP2FjOkTP0JmR4fX_Sa_NBdOSCyKwYj83JTizkt2Ez_VeZO4&h=AT1Y8x7r86jvQesneZhijLYCEldTE-ggJJRG2gsfGJiSJ4twTF7NyRByhasBn29oeUtEGHMYM1yLQngINNv-3fEkP7qej6k7-QInw3eOeyki9w3T-e6v5YayAK0OeIpPp-Y

[3] "Educate2Prevent - Strengthening Front-line School Workers and Parents to Build Youth Resilience to Violent Extremism", funded by the EU and Hedayah – Center of Excellence in CVE

Before the data collection process began, the PMT signed Memorandum of Cooperation[4] with the municipalities under whose competence high schools fall in. Data collection process consisted of presenting the objective of the research by the local researcher and the assigned school worker (teacher, psychologists, pedagogics, etc.), followed by filling in the e-questionnaire by the students using their mobile phones or school computers.

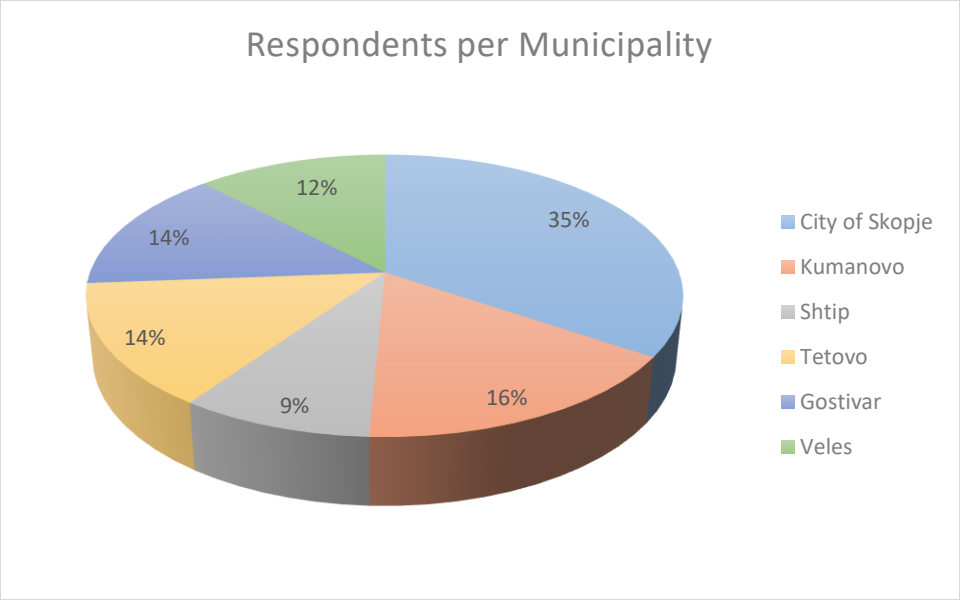
The collected data in google forms was first exported in excel files, and then it was recoded and imported into SPSS for further analysis, since this software allows for more complex statistical operations. Data analysis strategy included descriptive reports (frequencies and averages) and cross-tabulation of different variables as to be examined their relationship. Data was analyzed both generally for all targeted municipalities and for each municipality individually, comparing the findings between municipalities as well as between individual municipality and the general findings as to examine the differences between the subsamples.

## 2.1 SOCIO-DEMOGRAPHIC CHARACTERISTICS OF THE SAMPLE

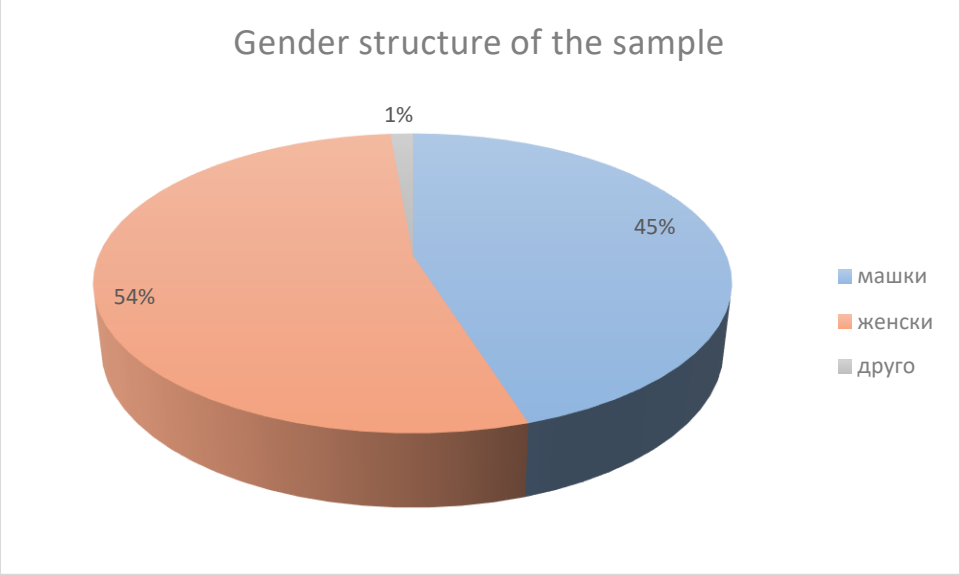
The sample consisted of 737 high school students from five municipalities and City of Skopje (City of Skopje 242, Kumanovo 114, Shtip 63, Tetovo 99, Gostivar 99 and Veles 85[5]), from all four years of study, at the age between 15 -19. Most of the respondents were in the second year of studying (44.5%), followed by students in the first year (20.9%), in third year (18%) and in the fourth year of studying (16.6%).

[4] Depending on the preferences of a municipality, the form was either Memorandum of Understanding or Memorandum of Cooperation

[5] Total answer for this question: 702. There are 54 missing values within the question.



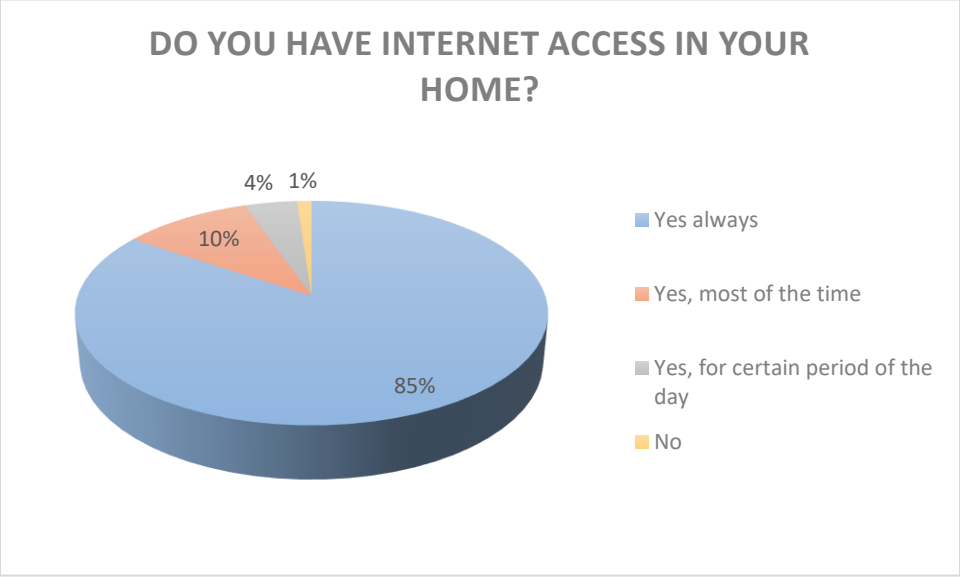

Regarding the gender structure of the sample, 53.5% were female, 45.1% were male and 1.4% declared as “other”. Furthermore, we took into account the place of living of the students, i.e. whether they live in an urban or rural area. Thus, 66.9% of the students included in the research said that they live in an urban area (city), while 33.1% of the students live in the rural area (village).



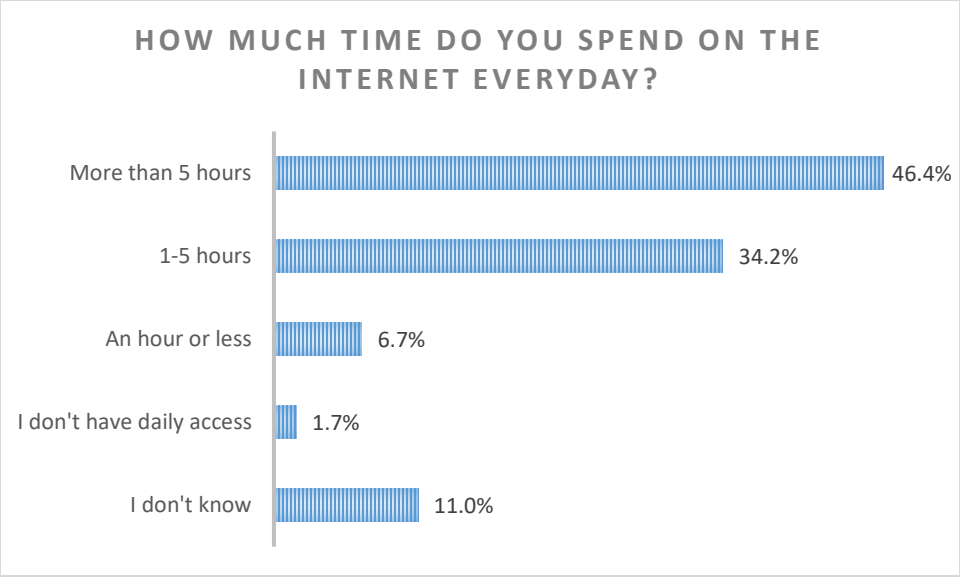
# 3 ACCESS AND USE OF INTERNET

The first set of questions was designed to collect information about the accessibility and the use of internet by the youth in the targeted municipalities (Kumanovo, Shtip, Tetovo, Gostivar, Veles and the City of Skopje).

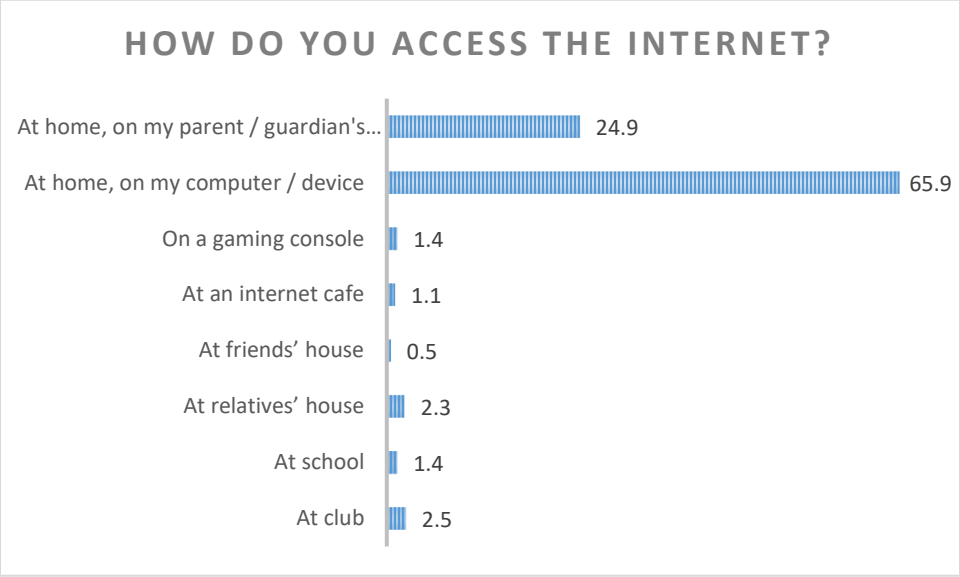
According to the findings, 99% of the students have internet access in their home, out of which, 85% said that they have access always, 10% most of the time and 4% have access to the internet but only for certain period of time. Only 1% of the students do not have access to the internet in their homes.




The next question asked the students how much time they spent on the internet. According to the findings, 46.4% of the high school students in the targeted municipalities spend more than 5 hours every day on the internet, and 34.2% spend from one to five hours. 6.7% spend 1 hour or less while 1.7 % said that they do not have access every day. Of these, 11% said that they do not know how much time spend on the internet. From a gender perspective, far more female students spend 5 hours or more on the internet every day (42.3%) compared to the male students (28.3%).




The figure bellow shows that more than 90% of the students access the internet from their homes, of which 65.9% on personal devices while 24.9% on their parents' devices. Only 1.4% said that they access the internet at school, while 2.5% go to internet clubs or another public network to access the internet.

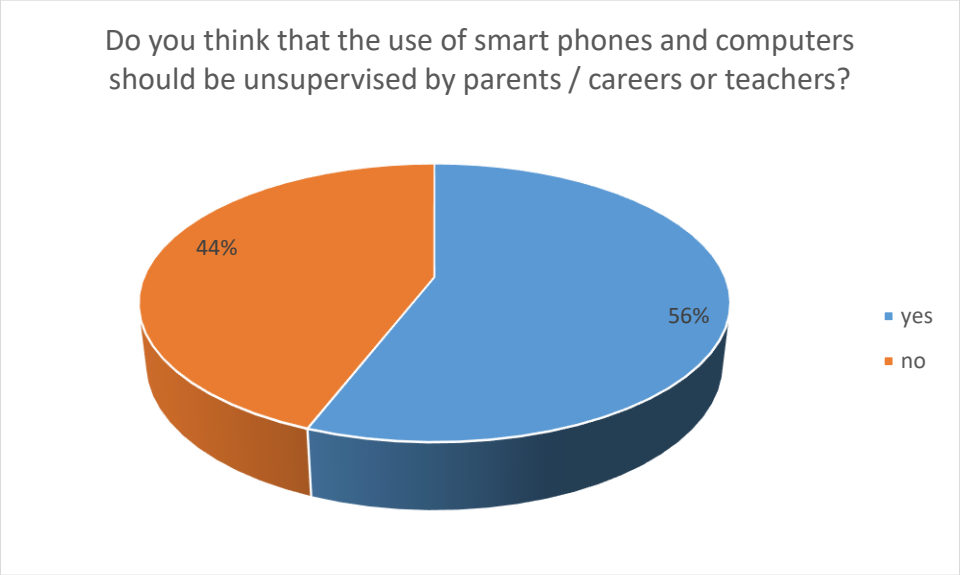



## 3.1 RULES FOR USING THE INTERNET AND SMART DEVICES BY STUDENTS

Furthermore, high school students from targeted municipalities were asked about their opinion on whether they should be able to use smart phones and computers without any parental supervision or

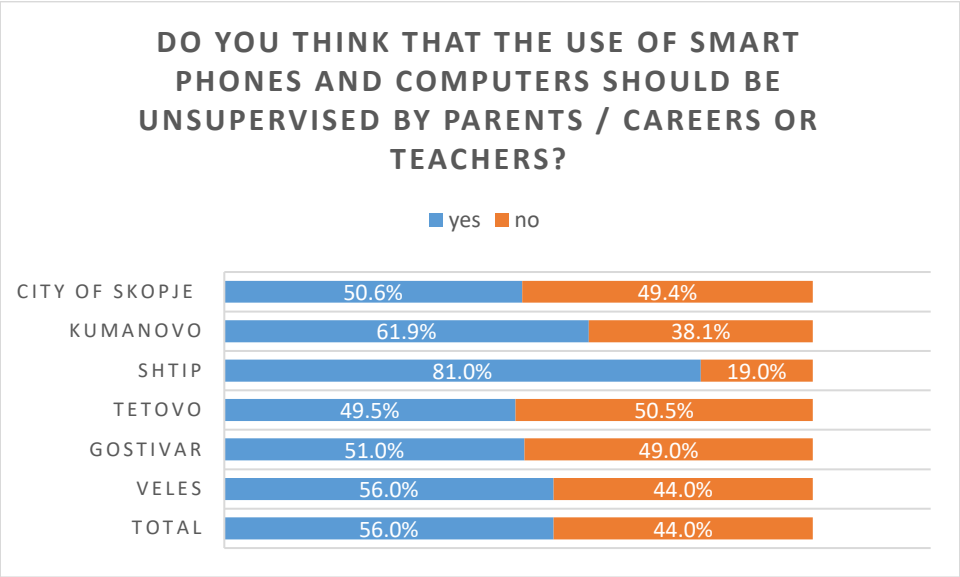
control. On this question, the opinions are divided. In average, 55, 9% of the students think that parental supervision or control is not necessary, while the other half (44,1%) think that parental supervision or control on their use of smart devises is acceptable to a certain extent. There are no significant differences or discrepancies across gender variable. When asked to elaborate their answers in more detail, those who think that no supervision or control by the parents should be imposed, say for example that "..[supervision/control] could often be misused by anyone.." , "[youth] are entitled with some privacy rights and this could breach these rights", "parents should trust their children more", "…as long as children respect the rules for using the internet, there is no need for such think" or that "as soon as child turns 12 years, should be able to use smart devices without supervision". On the other hand side, students that support parental supervision and/or control on using smart devices at home, say that "it is better for the children and youth because parents could protect them for the internet risks", or that "parents should be acquainted with how their children use the internet or their smart devices".

In general, many of the students agree that the internet could be potentially dangerous place that hides some risks and menaces, so they would have accepted some degree of supervision or control by their parents as long as they feel this is in direction of their protection rather than limiting their freedom.

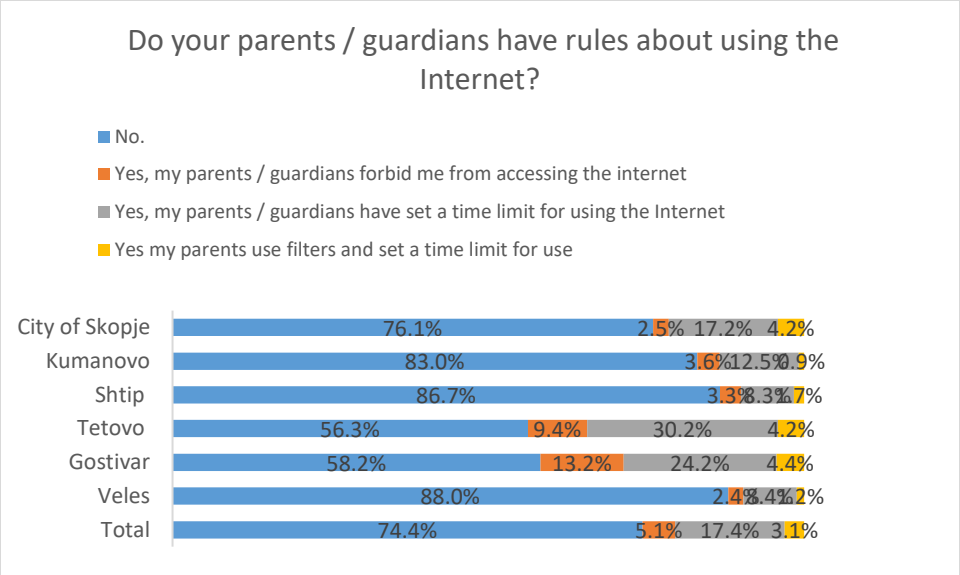



There are some differences across the municipalities regarding this question. For example, 81% of the high school students in Shtip think that use of smart phones and computers should be unsupervised by parents, as opposed to 49, 5% of high school students in Tetovo. In addition, supervision by parents or

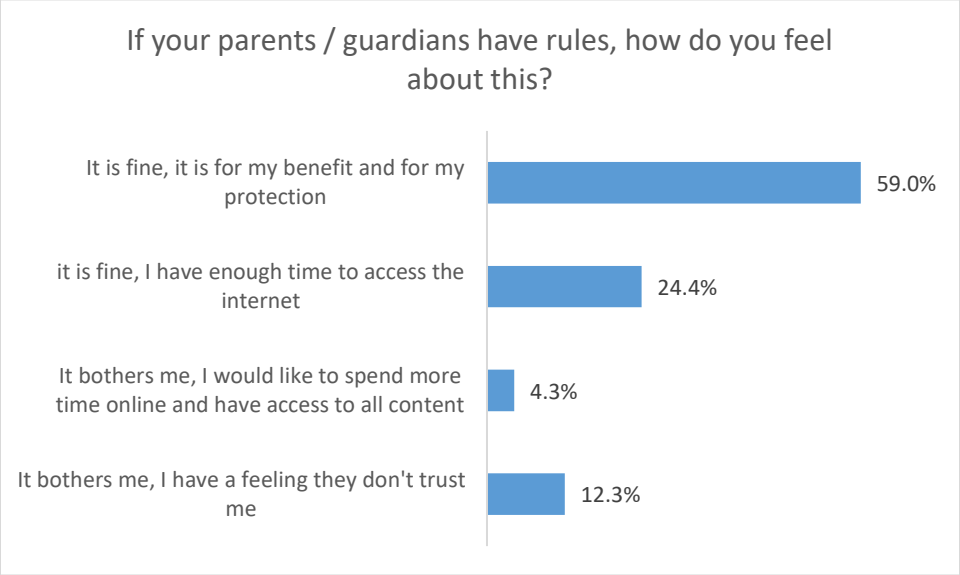
care givers is consider as obsolete by 61.9% of the high school students in Kumanovo, 50.6% in City of Skopje, 51%  and 56% in Veles.




Similar trend is followed when students from the targeted municipalities were asked whether their parents/guardians have set rules on the use of the internet. 74.4% said that in their home there are no rules on the use of the internet, while in 25.6% of the respondents' families there are time limits for using the internet. 5.1% of the parents/guardians do not allow their children to access the internet, while 17.4% of the students said that their parents have set time limits for the use of internet traffic in their homes. Analyzing the data for this question across municipalities the findings show that parents/guardians in Veles have least set up rules for using the internet for their children in their homes. In other words, 88% of the high schools students in Veles said that in their homes there are no any rules for using the internet, while in 4% of the families there are time limits on using the internet. This trend in the responses is following in Shtip, where 86.7% of the high school students said that there are not any rules in their homes on using the internet, Kumanovo (83%) and Skopje (76.1%). On the other hand, in Tetovo the percentage of respondents' homes without any rules is 56.3%, while in Gostivar is 57.2%. In addition, in Tetovo there are the most students who said that there are some kind of rules on using the internet. Thus, 30.2% of the students said that there are time limits on using the internet in their homes, while in 9.4% of the respondents' homes the internet access is forbidden under some circumstances.

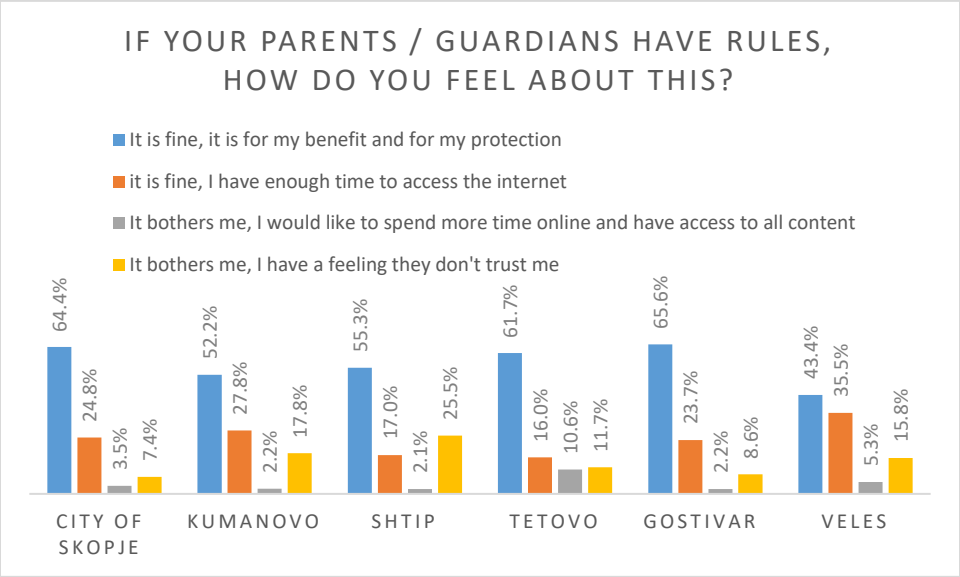



As many as 59.0% of the respondents whose parents have set rules on the use of the internet in their homes said that that is fine, because it is for their benefit and protection. 24.4% of the students think that besides the rules on the use of the internet, they still have enough time to use it. Cumulatively, however, around 16.6 % would feel upset by those rules because they would like to spend more time on the internet (4.3%) or they have feeling that parents/guardians do not trust them (12.3%).




Across the targeted municipalities, the biggest percent of high school students who think that it is fine if their parents/guardians have set rules, is in Gostivar (65.6%) followed by City of Skopje (64.4%), Tetovo (61.7%), Shtip (55.3%) and Kumanovo 52.2%. The lowest number of high school students who do not

support having internet rules is Veles with 43.4% of the respondents. In the same time, high school students in Veles think that even if their parents have rules for using the internet, they would still have enough time to access the internet (35.5%). No significant difference between the responses of male and female students is detected on this question.




According to the findings, half of the students that fulfilled the questionnaire would use certain limits on the use of the internet, while the other half said that they would not use any limits on the use of the internet. Across the targeted municipalities, most willing to use certain limits on the use of the internet are the high school students from Shtip and Gostivar, where 58.7% and 57.7% respectively said that they would use limits on the use of the internet.

Asked to name the limits/rules that they would use, students from the targeted municipalities enlisted the following:

- Time limit on the use of the internet
- Not using a hate speech on the internet
- Banning access on non-educational web sites
- More internet access on the weekends, and less on the weekdays.

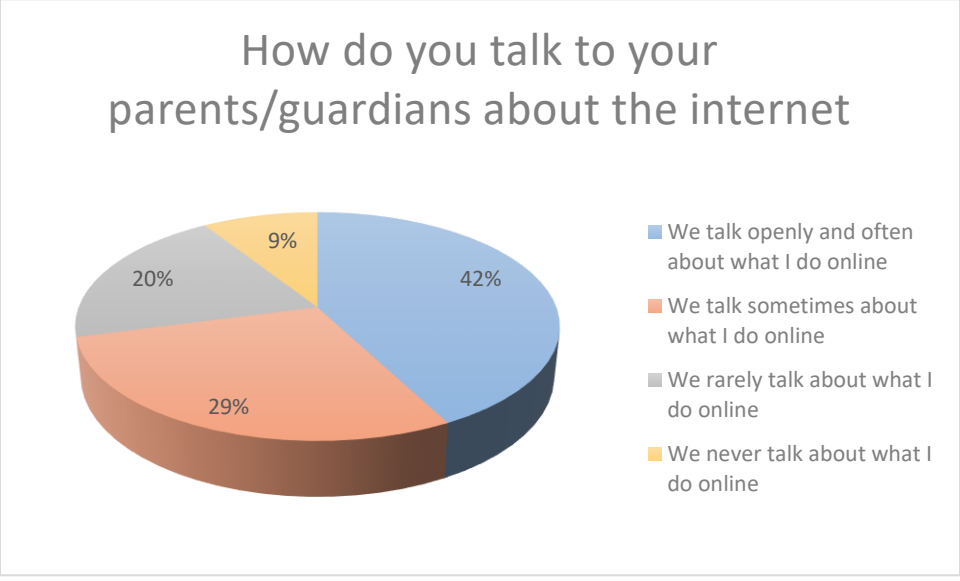
## 3.2 USE OF PRIVACY AND SECURITY SETTINGS

Cumulatively, 91,3% of the students think that privacy settings are useful when browsing the internet (54.4% consider it always useful, 36.8% as relatively useful). Only 8.6% do not think that these setting are useful at all.

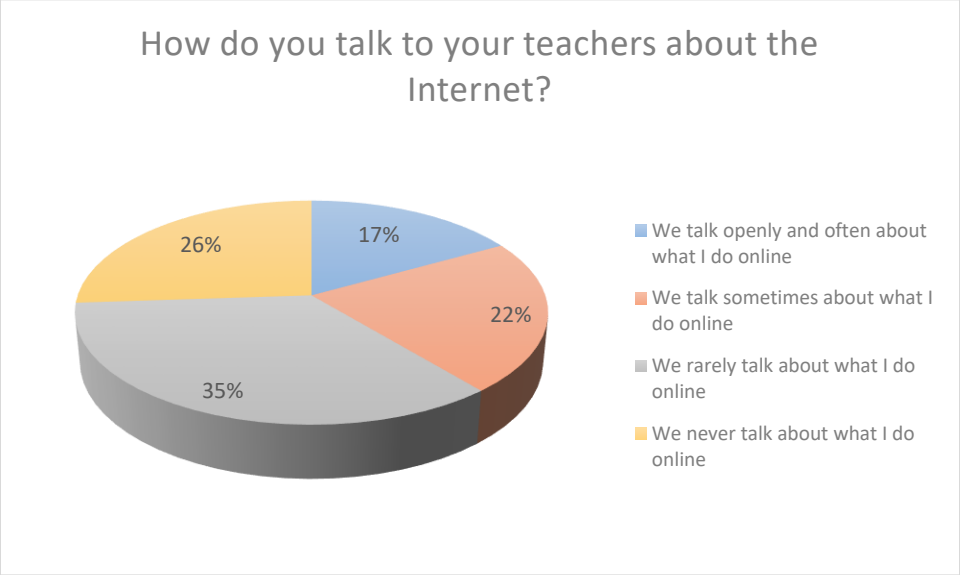
Sharing personal information on the internet is considered as one of the things that could compromise your online safety and security, which is why not recommended to do so. However, 26.4% of the high school students sometimes share their user name and password with their friends, while 2.9% regularly do so. 70.7% said that they have never share their account information with anyone.

Similar percentage of the high school students use automatic save option for their accounts on the internet browsers (33.8%) while 66.1% do not use this option. From a gender perspective, male students use this option more than their female counterparts do. Thus, among male students 42.1% use this option, while on the other hand only 27.1% of the female students use automatic safe option for their accounts on browsers or computers.

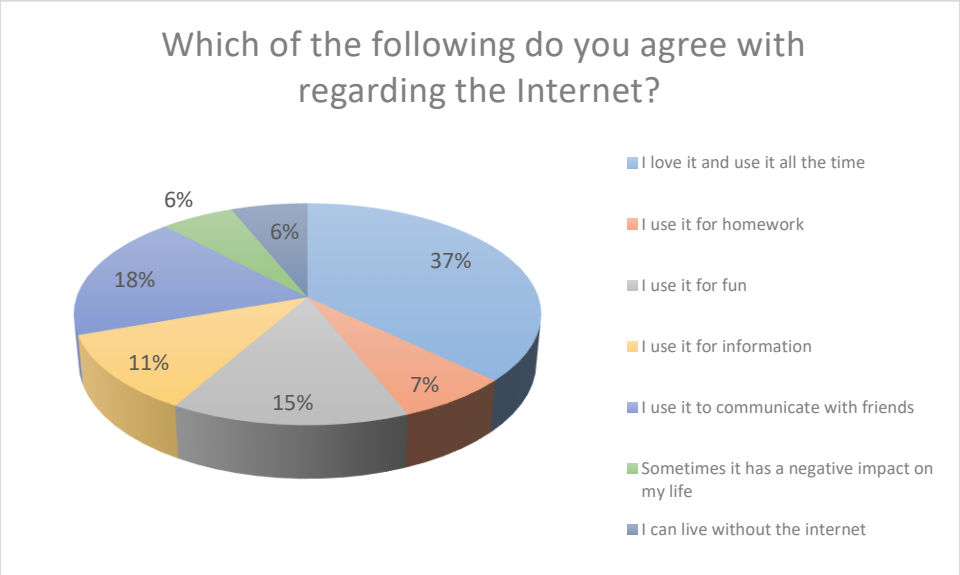
Most of the respondents in targeted municipalities, said that they talk with their parents about what they do on the internet. 42.3% talk with their parents often and openly about their online activity, while 28.6 % said that sometimes talk about it. From the graph below it seems that female students are slightly more open to talk about the online activity they have (45.8%) in comparison with their male counterparts (38.5%). As many as 20.1 % of the respondents rarely talk with their parents about their internet activity, while 9.1% never talk about what they do on the internet.



However, when asked how they talk with the teachers about their online activities, it seems students are more reserved towards them, or simply teachers do not bring up the topic in the schools as much as they should. Thus, the percentage of the respondents who said that openly and often talk with teachers on this topic is 16.9%. The percentage of respondents that said that sometimes they talk to the teachers is somewhat similar to that with the parents (22.1%) while most of the students reckon, they rarely talk to the teacher about what they do on the internet (35%). 26.1% said they never talk to the teachers about their online activity.




With the next questions, the respondents were asked to assess which of the statements presented would be true for them. Most of the students choose "I love the internet and I use it all the time" as to best suits their perception (37.1%), followed by the statement "I use [the internet] to communicate with friends" with 18.3%. 14.4% of the respondents said that they use the internet for fun, 11.4% to inform themselves and 6.8% use it for doing their homework. 5.9 % consider the internet has negative impact on their lives, while 6.2% think that the internet is not so indispensable thing in live, i.e. they can live without it. No significant deviations are detected when data is analyzed employing the gender perspective, except for the fact that female students use the internet more to inform themselves as compared to the male students, while the male students use the internet more for fun compared to the female students.



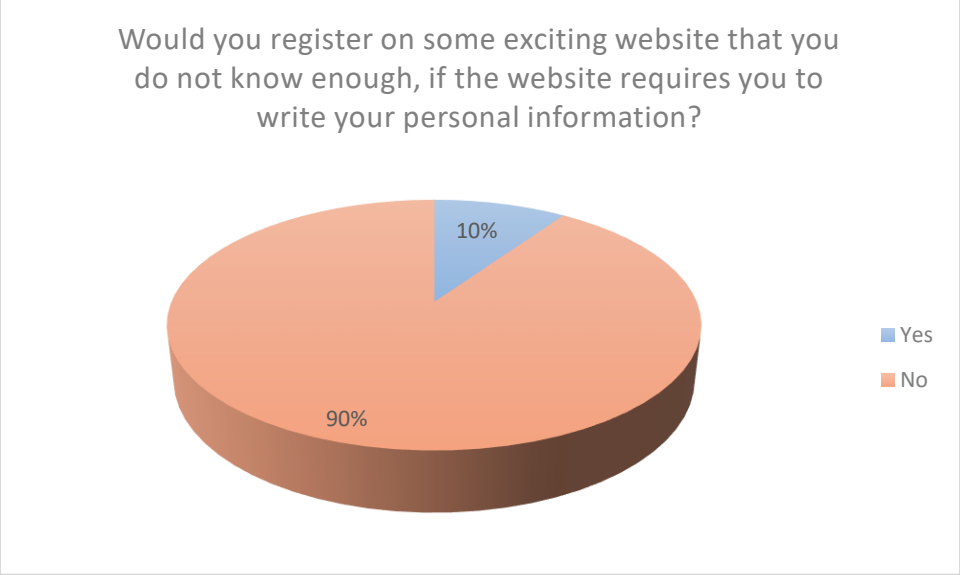

Furthermore, the students from targeted municipalities were asked to select the services or the applications they most use on the internet. According to them, most popular application or service they use is Instagram with 407 entries, followed by YouTube with 400 entries, snapchat (299), Facebook (281) and Viber (275).

## 3.3 PERCEPTIONS ON CYBER SECURITY

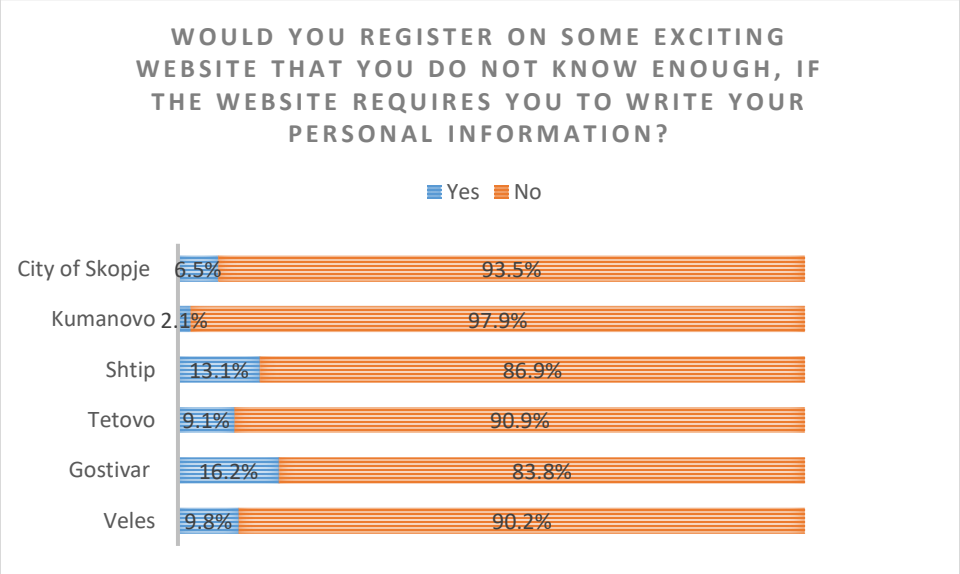
How safe do students feel while online, was the next question that was posed to the high school students. According to the findings, in general, students do feel safe to a certain extent, think that they are aware of the dangers and most of them have not had any bad experience neither personal discomfort. 34.4% said that they have never faced threat or discomfort on the internet, while 14.6% believe that even if they face some kind of threat or danger on the internet they are able to handle the situation by themselves. It should be noted however, that there are no significant differences between the answers of the male and female respondents. In general, 14.6% of the respondents believe that they can handle any threat or discomfort they might face. Slightly more female students believe in this statement (15.1%) than male students, whose percentage is 13.9%. Furthermore, 32.8% of the respondents are aware of the risks and dangers on the internet based on some else's bad experience they heard about and therefore feel safe only sometimes. Personal bad experience on the internet has been reported by 8.5% of the high school

students in targeted municipalities, slightly more by boys (9.3%) as compared to the girls (7.7%). 9.7% of the all respondents said that they never feel safe on the internet and always think about the dangers while online.


The next question asked the respondents if they would register on some exciting website that they do not know enough, if the website requires them to write their place of residence and address, their parent's names, their email address or their social media profile. To this question, 90,4% of the respondent said that they would not register on such web sites, while 9.6% would register and submit the required (personal) information.



Across the targeted municipalities, the highest percentage of youth that have registered on an exciting website asking for some personal information are from Gostivar 16.2%, followed by high school students in Shtip (13.1%) and Veles (9.8%). Municipality of Tetovo (9.1%), City of Skopje (6.5%) and Kumanovo (2.1%) are below the average of the targeted municipalities of 9.4% of students that would not register if a website requires submitting personal information.




### 3.3.1 Awareness about radicalization and violent extremism

In the next part, the questionnaire presented the following types of internet content that respondents may face on the internet:

- *Hate speech that directly encourages people to behave violently or commit an act of violence*
- *Content that shows cruel violence, rape, murder*
- *Hate speech that does not directly encourage people to behave violently or to commit violent acts*
- *Contents that shows beheading or torture*
- *Content showing physical assault, ignition and beating*
- *Hard porn*
- *Trolling, bullying and online insults*
- *Contents that show destruction of private property / property in the struggle for social justice*
- *Violent content that is humorously portrayed (using pictures, music, drawings, etc.)*
- *Contents showing how to make a bomb*
- *Fascist content showing supremacy of one group / nation and is identified with a swastika / hooked cross*

Subsequently, they were asked to describe them with the predefined qualifications, i.e. whether the content is: 1) violent extremism, 2) extremism 3) not related to extremism and 4. I do not know. Based on their responses we ranked top five types of content according to each of the predefined qualifications.

Hence, based on the responses of the high school students in targeted municipalities, the following types of internet content are considered as **violent extremism**:

*Content showing physical assault, ignition and beating*, by 61.1% of the respondents, *Hate speech that does not directly encourage people to behave violently or to commit violent acts* by 60.7% and *Hard porn* by 55.2% of the high school students, *Content that shows cruel violence, rape, murder* (52.6%) *Fascist content showing supremacy of one group / nation and is identified with a swastika / hooked cross* (42.6%).

It should be noted however that there are certain differences between the municipalities regarding which of the presented content is considered violent extremism. In the following table, we present the top five internet content that high school students consider violent extremism according to the municipality they live in. Thus for the high school students in the City of Skopje those are:

1. Content showing physical assault, ignition and beating
2. Hate speech that does not directly encourage people to behave violently or to commit violent acts
3. Hard porn
4. Content that shows cruel violence, rape, murder
5. Trolling, bullying and online insults

For the high school students in Kumanovo the five internet contents that are considered violent extremism are:

1. Content showing physical assault, ignition and beating
2. Hate speech that does not directly encourage people to behave violently or to commit violent acts
3. Hard porn
4. Content that shows cruel violence, rape, murder
5. Fascist content showing supremacy of one group / nation and is identified with a swastika / hooked cross

In Shtip, the respondents perceived the following top five internet content as violent extremism:

1. Hate speech that does not directly encourage people to behave violently or to commit violent acts
2. Content showing physical assault, ignition and beating
3. Hard porn
4. Content that shows cruel violence, rape, murder
5. Contents that shows beheading or torture

Students from Gostivar have chosen the following:

1. Content showing physical assault, ignition and beating
2. Content that shows cruel violence, rape, murder
3. Hate speech that does not directly encourage people to behave violently or to commit violent acts
4. Hard porn

5. Violent content that is humorously portrayed (using pictures, music, drawings, etc.)

The respondents in Veles perceive the following top internet content as violent extremism:

1. Hate speech that directly encourages people to behave violently or commit an act of violence
2. Content that shows cruel violence, rape, murder
3. Hate speech that does not directly encourage people to behave violently or to commit violent acts
4. Contents that shows beheading or torture
5. Content showing physical assault, ignition and beating

Finally, the high school students in Tetovo consider violent extremism the following internet content:

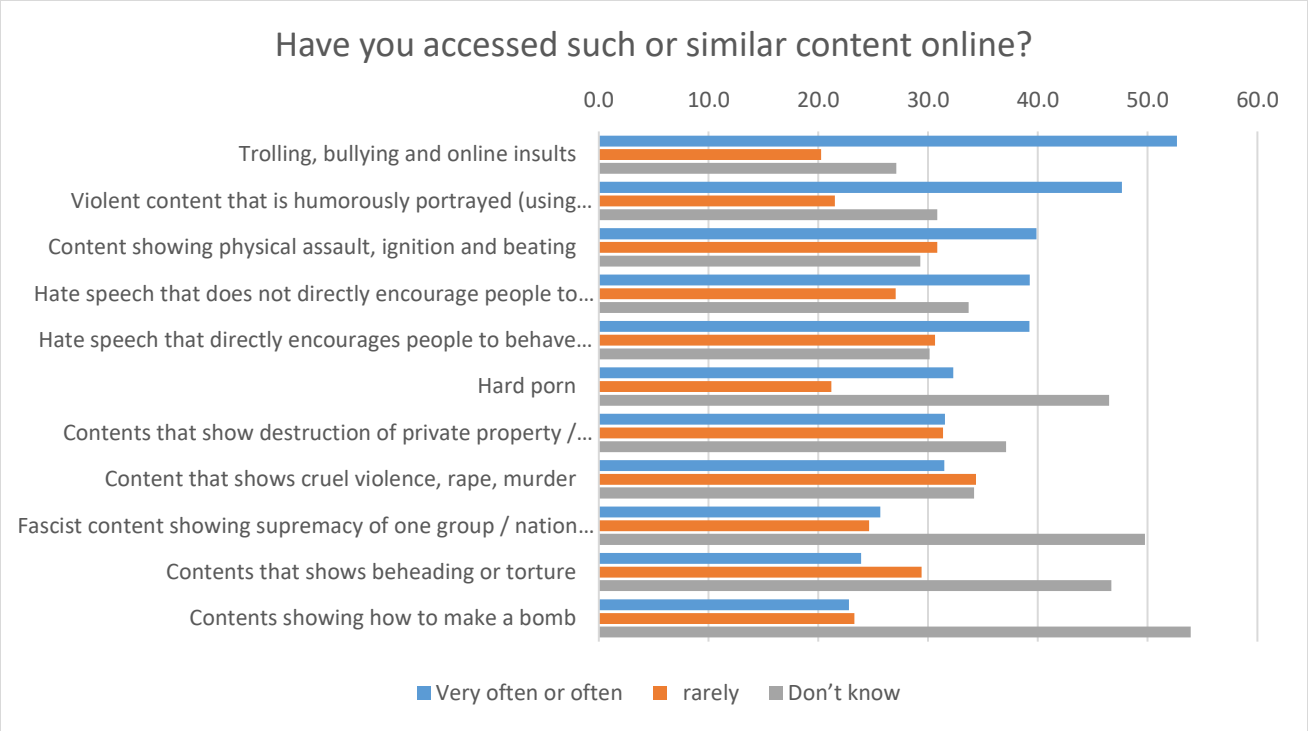
1. Hate speech that directly encourages people to behave violently or commit an act of violence
2. Content that shows cruel violence, rape, murder
3. Hate speech that does not directly encourage people to behave violently or to commit violent acts
4. Contents that shows beheading or torture
5. Content showing physical assault, ignition and beating

Furthermore, we ranked the top five types of content that according to the respondents are considered to induce **extremism,** and those are:

1. Contents that show destruction of private property / property in the struggle for social justice (31.8%)
2. Contents showing how to make a bomb (28.3%)
3. Violent content that is humorously portrayed (using pictures, music, drawings, etc.) (28.1%)
4. Contents that shows beheading or torture (26.7%)
5. Fascist content showing supremacy of one group / nation and is identified with a swastika / hooked cross (26.3%)

In the next part, the respondents were asked whether and how often[6] they access the same types of content as above while on the internet. According to the findings, the most accessed content by students from the targeted municipalities is trolling, bullying and online insults (52.7%). The next content which students said they access very often or often is violent content that is humorously portrayed (47.7%), followed by Content showing physical assault, ignition and beating (39.9%). Hate speech that does not directly encourage people to behave violently or to commit violent acts is fourth most frequent accessed content on the internet (39.3%) while Hate speech that directly encourages people to behave violently or commit an act of violence (39.2%) is on fifth place as most accessed content by youth from targeted municipalities.

[6] On a scale: “very often”, “often”, “rarely” and “I don’t know”



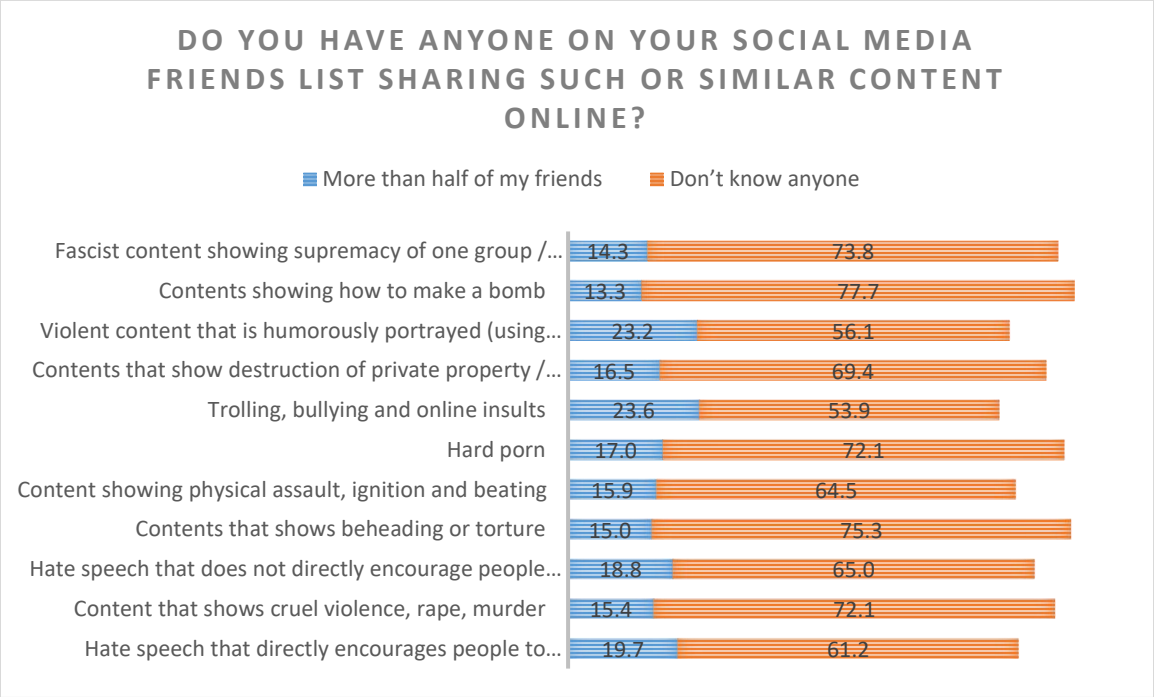

In the following part, the respondents were again presented with the same types of violent internet content[7], this time asked to indicate whether they have anyone on the social media friends list sharing such or similar content online. The predefined answers were: 1. Large number of my friends; 2. Around half of my friends; 3. Few of my friends, but rarely; 4. Don't know anyone.

From the findings presented in the table below, we can see that most shared violent content, shared by respondents' online friends is trolling, bullying and online insults. 23.6% of the respondents said that this type of violent internet content is shared by at least half of their friends. This is followed by violent content that is humorously portrayed (using pictures, music, drawings, etc.) for which 23.2% of the respondents said that more than half of their online friends share such or similar content on the internet. The third

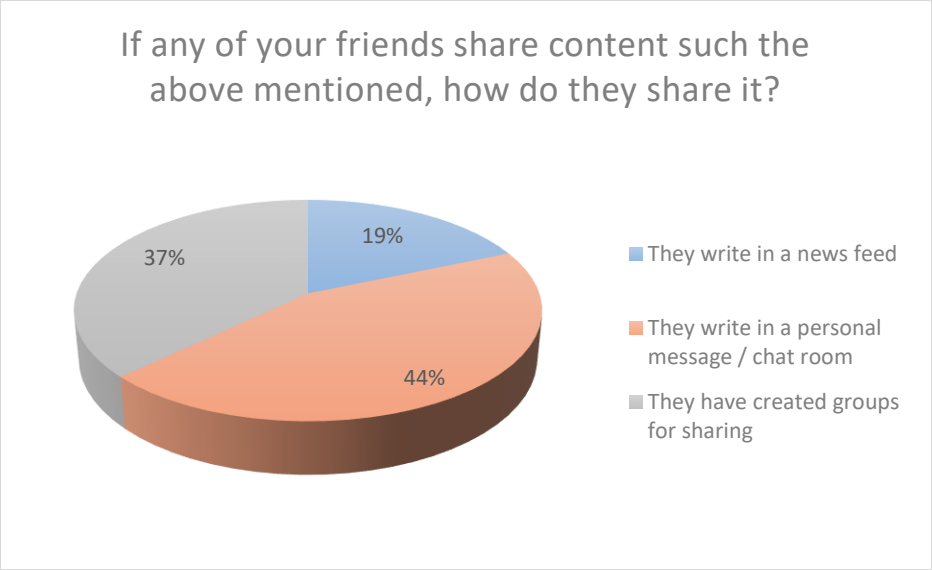
[7] Types of internet content:

- *Hate speech that directly encourages people to behave violently or commit an act of violence*
- *Content that shows cruel violence, rape, murder*
- *Hate speech that does not directly encourage people to behave violently or to commit violent acts*
- *Contents that shows beheading or torture*
- *Content showing physical assault, ignition and beating*
- *Hard porn*
- *Trolling, bullying and online insults*
- *Contents that show destruction of private property / property in the struggle for social justice*
- *Violent content that is humorously portrayed (using pictures, music, drawings, etc.)*
- *Contents showing how to make a bomb*
- *Fascist content showing supremacy of one group / nation and is identified with a swastika / hooked cross*

most shared violent content is Hate speech that directly encourages people to behave violently or commit an act of violence, pointed by 19.7% of the respondents.

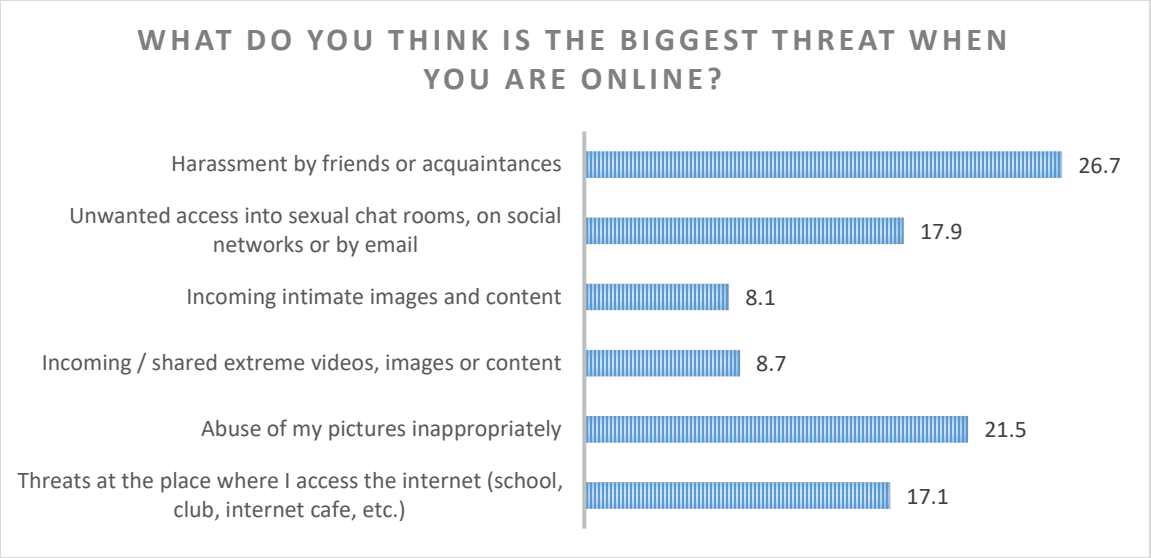



The above-mentioned types of violent internet content, as the graph below shows, is mostly shared, according to 44% of the respondents via personal messages (inbox). Furthermore, 37% of the respondents said that these types of violent content also shared via created groups for sharing. Only 19% of the respondents said that these type of violent content is shared in the news feed.




## 3.4 PERCEPTIONS ON CYBER THREATS, SHARING PERSONAL INFORMATION AND FAKE NEWS

When the respondents are online, the biggest threat for 26.7% of them is the harassment by friends or acquaintances, followed by unwanted access into sexual chat room, on social networks or by email (17.9%). Third biggest threat is the abuse of their pictures inappropriately (21.5%). Incoming/shared extreme videos, images or content is security threat for 8.7% of the respondents, while incoming intimate images and content is considered as an online security threat by 8.1%. Threats in the places of accessing the internet are taken into account by 17.1% of the respondents.




Across the targeted municipalities, for 25.2% the high school students in the City of Skopje, the biggest threat while online is the abuse of their pictures inappropriately, followed by online harassment by online friends or acquaintances (23.3%), threats at the place where I access the internet (school, club, internet cafe, etc.)(22.8%), unwanted access into sexual chat rooms, on social networks or by email (15.%) Incoming / shared extreme videos, images or content (7.8%) and incoming intimate images and content (5.8%).

In Kumanovo the respondents ranked the following internet threats: Abuse of my pictures inappropriately (26.4%); Unwanted access into sexual chat rooms, on social networks or by email (22.6%); Harassment by friends or acquaintances (19.8%); Threats at the place where I access the internet (school, club, internet cafe, etc.) (14.2); Incoming / shared extreme videos, images or content (10.4%); Incoming intimate images and content (6.6%).

For high school students from Shtip the biggest threats online are: Harassment by friends or acquaintances (22.0%); Incoming intimate images and content (18.6%); Unwanted access into sexual chat rooms, on social networks or by email (16.9%); Threats at the place where I access the internet (school, club, internet cafe, etc.) (16.9%); Abuse of my pictures inappropriately (15.3%); Incoming/shared extreme videos, images or content (10.2%).

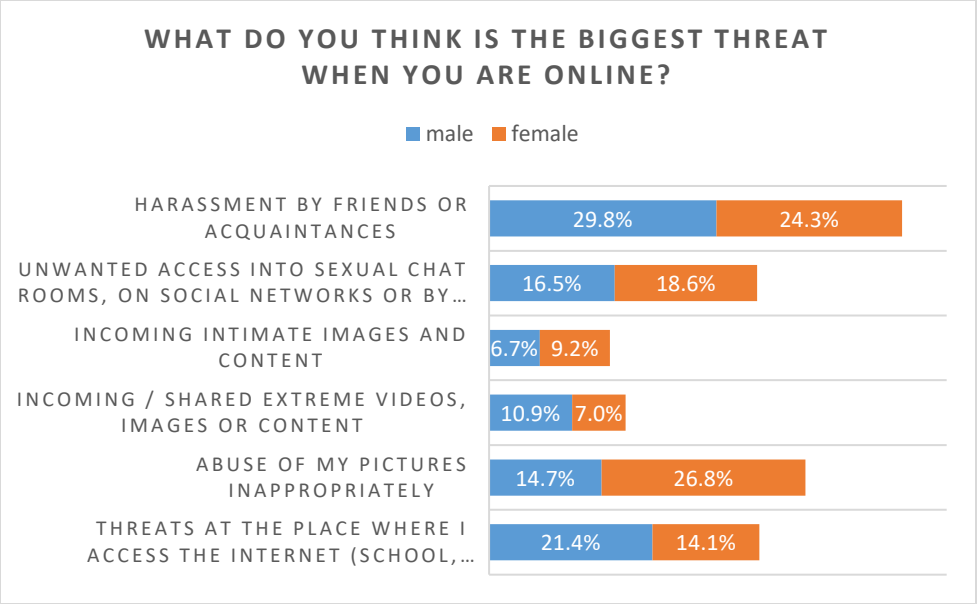
Harassment by friends or acquaintances is seen as the biggest threat for high school students in Tetovo (42.2%), followed by unwanted access into sexual chat room, on social networks or by email (16.7%). Third biggest threat is the abuse of their pictures inappropriately (14.4%). Incoming/shared extreme videos,

images or content is security threat for 10% of the respondents, while incoming intimate images and content is considered as an online security threat by 8.9%. Threats in the places of accessing the internet are taken into account by 7.8% of the respondents.

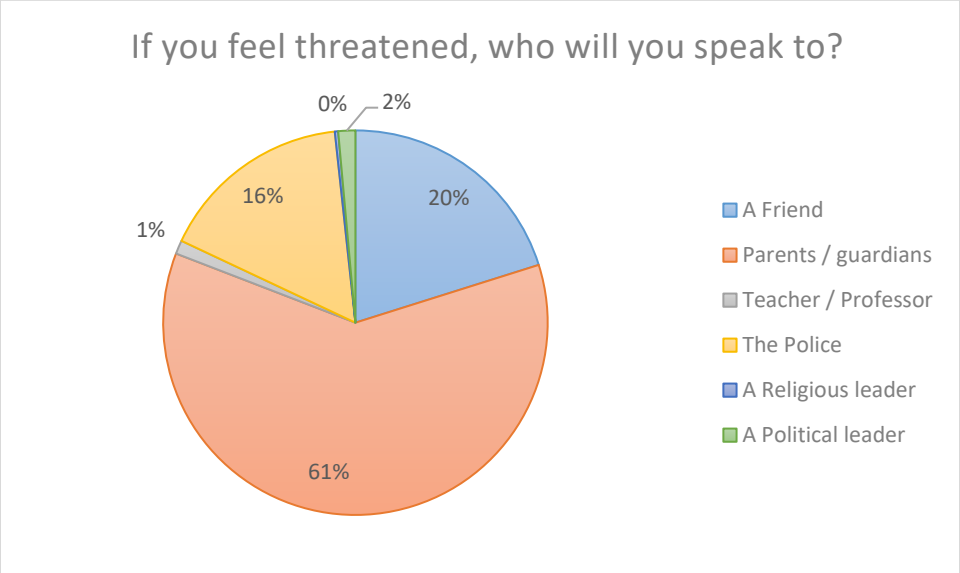
Harassment by friends or acquaintances is also seen as the biggest threat for high school students in Gostivar, with a slightly smaller percentage than Tetovo (25.8%). As next threat the respondents pointed the abuse of their pictures inappropriately (22.6%). Threats in the places of accessing the internet are perceived as a threat by 20.4% of the respondents, while unwanted access into sexual chat room, on social networks or by email by 12.9%. Incoming/shared extreme videos, images or content is security threat for 11.8% of the respondents, while incoming intimate images and content is considered as an online security threat by 6.5%.

In Veles, the respondents ranked the following internet threats: Harassment by friends or acquaintances (28.8%) Unwanted access into sexual chat rooms, on social networks or by email (23.8%); Abuse of my pictures inappropriately (18.8%); Threats at the place where I access the internet (school, club, internet cafe, etc.) (17.5%); Incoming intimate images and content (5.0%). Incoming / shared extreme videos, images or content (6.3%).

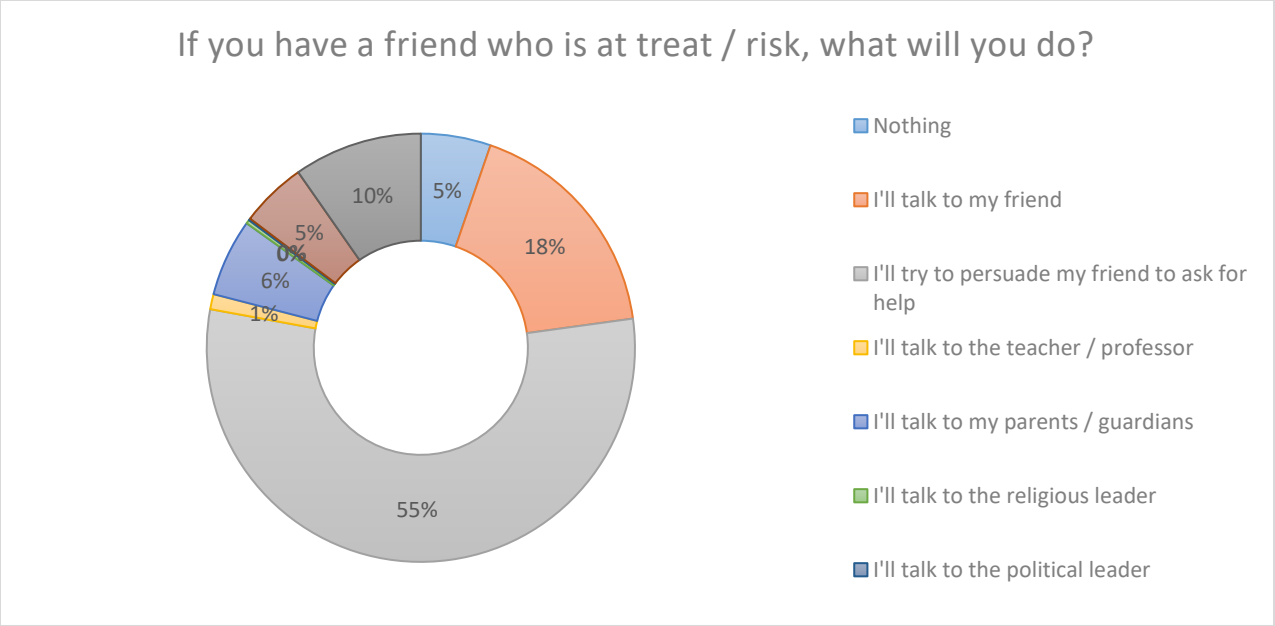
Analyzing the data from a gender perspective, we can see that harassment by friends or acquaintances is the biggest security threat online for both male and female respondents (29.8% and 24.3% respectively). The second biggest threat for the male respondents are the threats at the place where they access the internet (school, club, internet cafe, etc.) (21.4%) followed by unwanted access into sexual chat rooms on social networks or by email (16.5%). On the other hand, for the female respondents second biggest threat is abuse of personal pictures inappropriately (26.8%). The latter is perceived as a threat by 14.7% of the male respondents. The third biggest threat for male respondents is abuse of their pictures inappropriately (14.7%), while for the female respondents that is unwanted access into sexual chat rooms, on social networks or by email (14.9%).



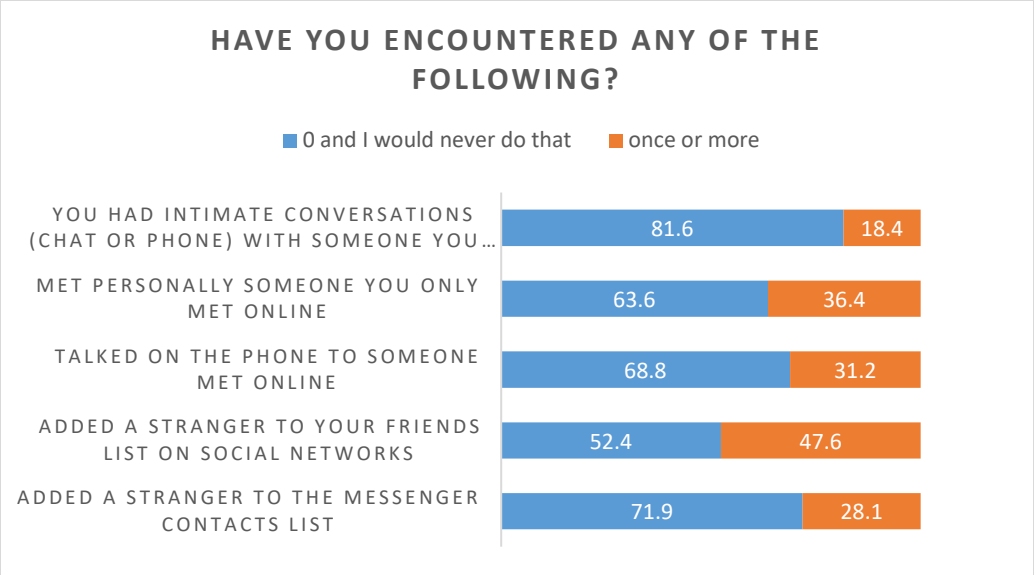

In case the respondents feel threatened while online, 61% of them will speak to their parents/guardians, 20% choose to speak with a friend, while 16% will report the threat to the policy. From the findings, it seems that teachers/professors are not seen as adequate for such conversation, since only 1% said that would speak with them if they feel threatened online. More adequate for such conversation compared to teachers, according to the findings are the political leaders, who are chosen by 2% of the respondents.



The next question asked the respondents what will they do in case a friend of them is at threat or risk while online? 55% of the respondents said that first, they will persuade their friend to ask for help, or they will try to talk to that friend themselves (18%). 10% of the respondents said that either they will do nothing, or will talk to a political leader, while 6% will tell about the problem to a political leader or will speak to their parents/guardians or the teachers.

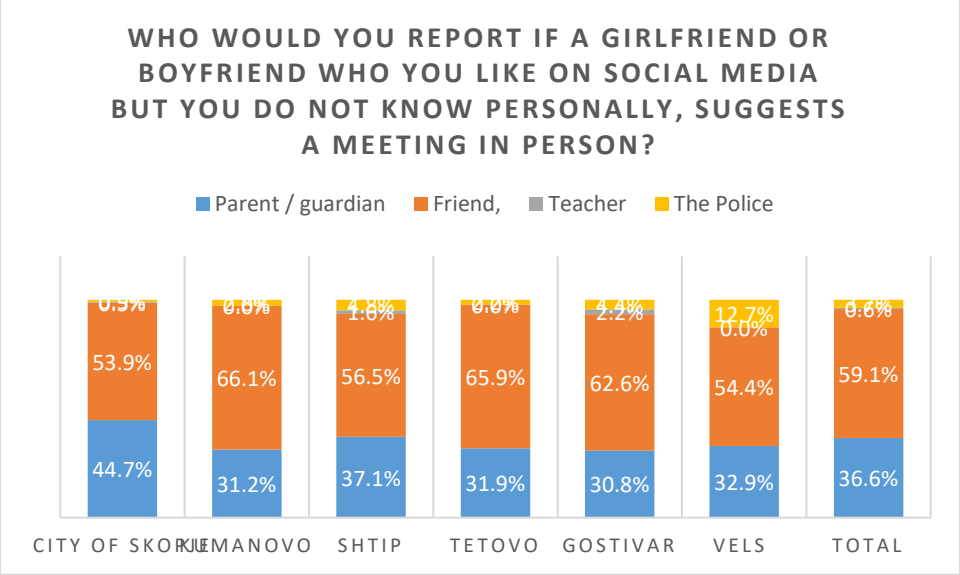



47.6% of the high school students from the targeted municipalities that filled in the questionnaire at least once have added stranger to the messenger contacts list, while 36.4% have met personally someone they have only met online. 31.2% of the respondents said that at least once they have talked on the phone to someone they only met online. 28.1% have at least once added a stranger on a social networks messenger's list. Furthermore, the analysis reveals that 18.4% of the high school students in the targeted municipalities at least once have had intimate conversation (chat or phone) with someone they have met only online. What is more, 5.5% have done it more than ten time while online.

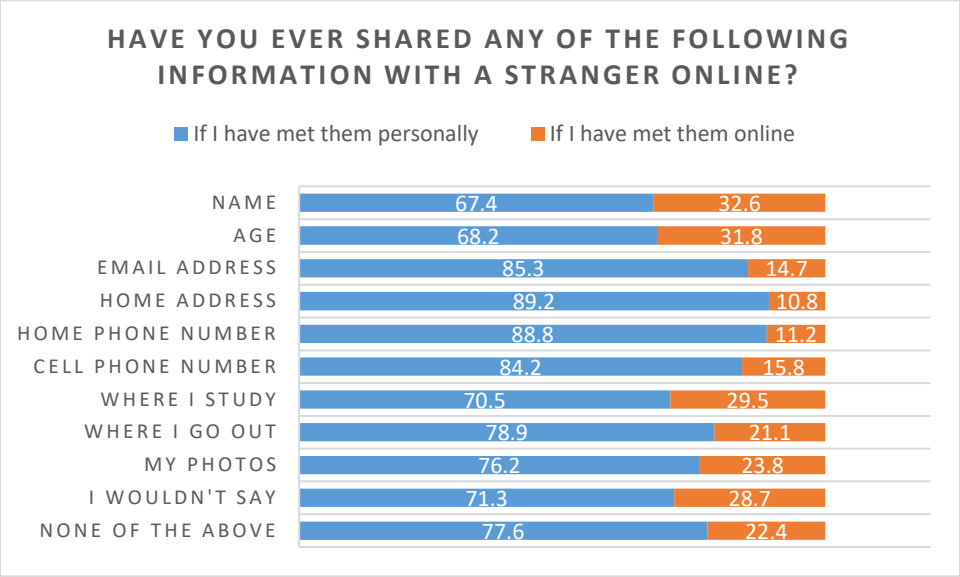



Based on the responses of the high school students in targeted municipality, the most frequent application/social network on which some of the above listed experiences have occurred is Instagram, followed by Facebook and Facebook messenger, snapchat etc.

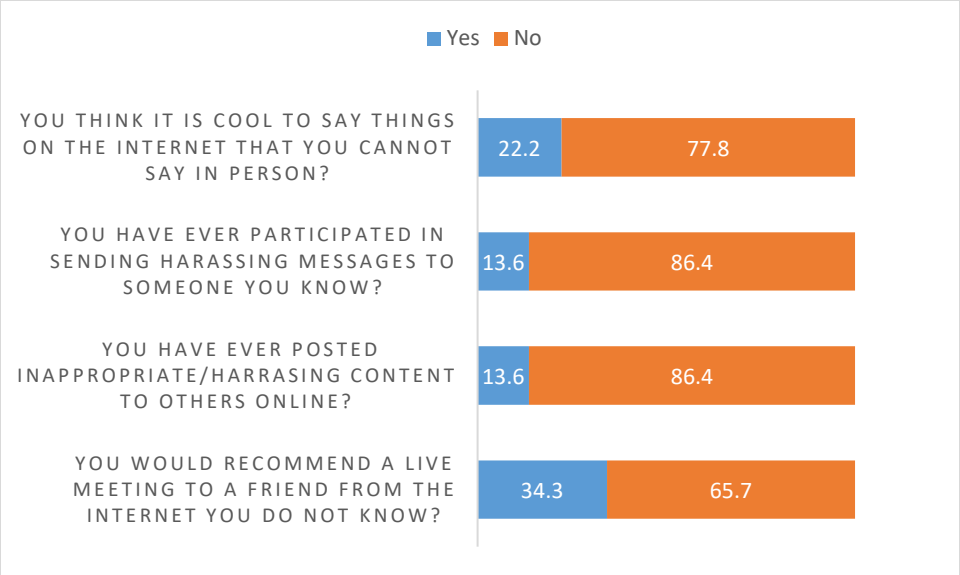
Answering the following question from the questionnaire, the respondents said that in case a girlfriend of boyfriend who they like on social media but they do not know personally suggests a meeting in person, they would first turn to a friend (59.1%), 36.6% of them would tell their parents/guardian, while 3.7% would report to the police. Only 0.6% said that they would report to a teacher. As it can be seen from the graph bellow, the same trend is followed across the targeted municipalities.



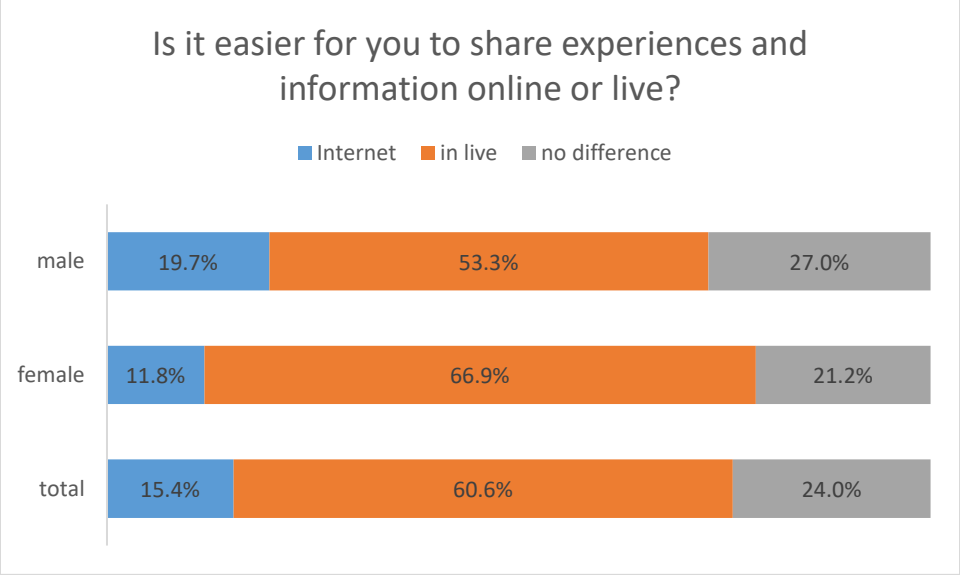
Many of the high school students share information online as it has been seen from the analysis of the previous questions. To certain extent, the same trend is followed when it comes to sharing personal information with strangers online, such as name, age, email addresses, school, personal photos etc. Thus, 32.6% of the respondents said that they have shared their name with someone they met only online, 31.8% shared their age, 29.5% shared information about the school they study in, while 23.8% have shared their photos. 21.1% of the high school students have shared information with someone they only met online about where they do out. However, 22.4% of the respondents said that they have never shared any of the enlisted personal information with someone they know only from the internet.



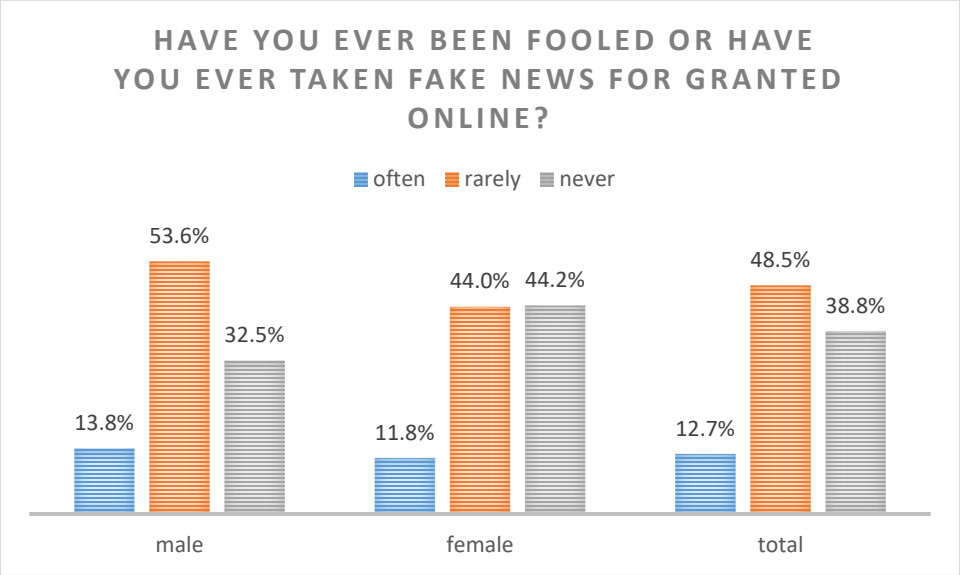

34.3% of the respondents do not have any problem to suggesting a live meeting to a friend they only met on the internet and they do not know in person. In addition to that, 22.2% said that they think it is cool to say things on the internet that cannot be said in person. 13.6% have both participated in sending harassing massages to someone they know and have posted inappropriate/harassing content to others online.




In general, for 60.6% of the high school students in the targeted municipalities it is easier to share experiences and information in live than online, which is easier for 15.4% of the respondents. Taken gender perspective into account, male students are slightly more confident to share things online (19.7%) than their female counterparts (11.8%). In total however, 24% said that there is no difference for them whether they share experiences and information online or in person.

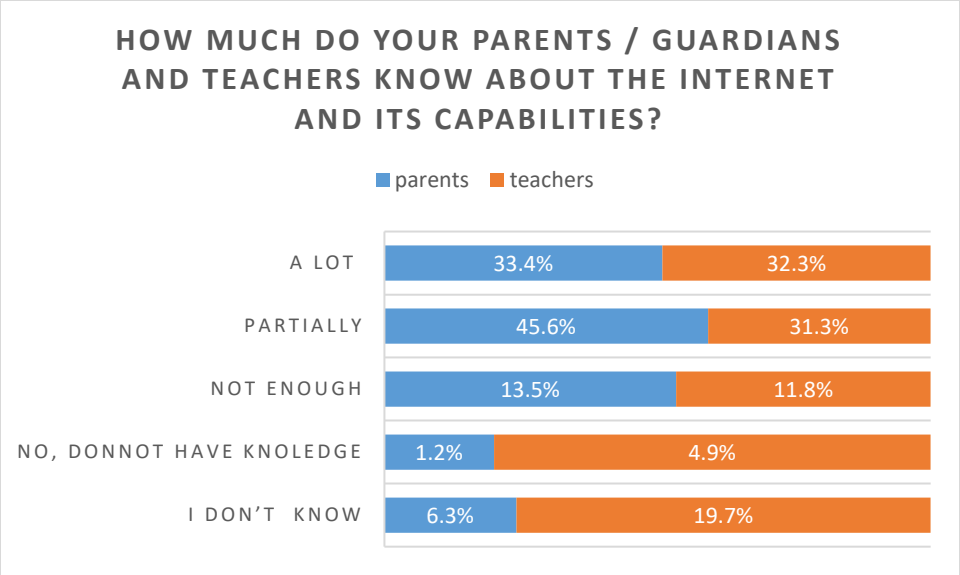


Sharing or creating fake news on the internet and social media is widespread phenomenon. The purpose of creating and/or sharing fake news varies, but it could range from fun and lucrative reasons, to more serious reasons, such as radicalization, radicalization that leads to violent extremism etc. In the targeted municipalities, 12.7% of the respondents said that have been often fooled or have taken for granted fake news shared online, while 48.5% said that that happen(ed)s but rarely. That means that almost 2 out of 3 respondents have at least once been victims (to some extent) of the fake news, even though at least 59.3% of them said that always or often check the reliability for the information shared on the internet. In addition to this, It should be noted that the female students are slightly more careful when fake news are in question than the male students. However, still large portion of them said that rarely or never check the reliability of the information on the internet (40.7%).



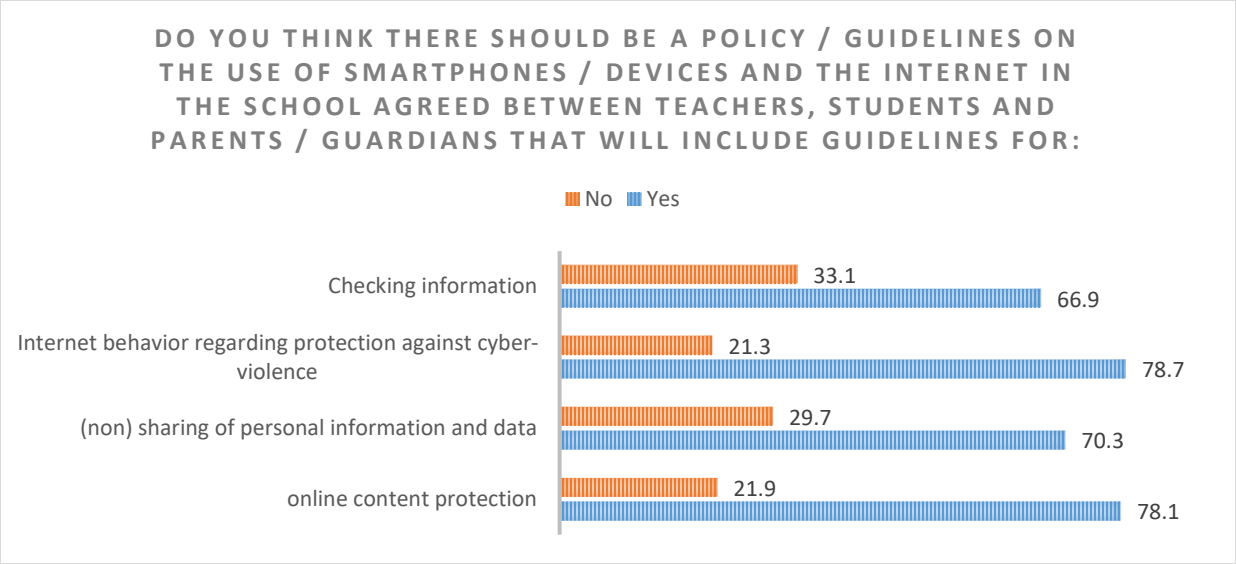

## 3.5 TRAINING NEEDS ASSESSMENT

In general, respondents in the survey think that their parents and teachers have basic knowledge of the internet and its capabilities. Cumulatively, high school students think that their parents have more knowledge (79% of the respondents), as compared to the teachers for whom 63.6% of the respondents said have somewhat knowledge about the internet and its capabilities. 16.7% of the students said that their teachers lack knowledge, while 14.7% said the same for their parents.




Having in mind that parents and teacher also use social networks, students often befriend teachers and parents. In general, 69.3% of the respondents said that they are friends with their teachers and 85.9% are friends with their parents on the social networks.

Regarding whether there should be a policy / guidelines on the use of smartphones / devices and the internet in the school agreed between teachers, students and parents / guardians that will include guidelines for certain aspects of the use, 73% of the respondents would approve such guideline in general. By specific aspects that should be covered by the guidelines the support is: a) online content protection (78.8%), b) not sharing personal information and data (70.3%) c) Internet behavior regarding protection against cyber-violence (78.8%) d) checking information (66.9%)




Next set of question examined whether the students have had any training on the safe use of internet and data protection and access. Around 63% of the respondents said that they have never had training on the topics.

Asked whom they would tell if they come across information on internet that they "…. feel is somewhat strange (e.g. communication about religion, cult, belief, etc. different from what they are taught at home or in the environment in which you live)", 52.4 of them choose to tell their parents, then friends (41.8%) and last are their teachers (5.8%).

On the question how often their teachers or parents have asked for help on how to use the internet, respondents said that the teacher more often seek their help (85.4%) in comparison to their parents that asked 67.4% of the respondents.

# 4 CONCLUSION

The main objective of the study was to assess the perceptions of the high school students regarding cyber security threats and radicalization, especially radicalization that can lead to violent extremism by examining how, and how much they use the internet; what content they access; what challenges and threats they face while online and what they do when faced with such challenges. Furthermore, the task of the study was to contribute towards better understanding of the online radicalization in North

Macedonia and especially in the targeted municipalities (Kumanovo, Shtip, Gostivar, Tetovo, Veles and City of Skopje), and to provide data driven evidence-based recommendations and programs aiming at reducing and preventing online radicalization and cyber threats in general.

The analysis of the data has shown that the internet now days is available to every student, with almost 95% of the students in the targeted municipalities having permanent access via smart phones or computers, mostly in their homes. This means that youth are constantly exposed to flux of information and communication with both friends and strangers, which significantly increases the vulnerability of young people to cyber threats, including radicalization and violent extremism. Therefore, there is a growing need for regulating the access to certain content and supervising the online activity of the youth. Nonetheless, students are divided when it comes to respecting rules set up by their parents or teachers. Many of them would prefer to deal with the cyber threats themselves rather than conceding part of their privacy to their parents. Thus, in more than have of the families there are no rules for accessing and using the internet at home. The lack of supervision and other more restrictive measures is somewhat complemented by open talks within the family about the use of the internet and internet activity which takes places in almost 90% of the respondents' families. The same practice of open talks about their internet activity is not developed as much in schools, with their teachers. In the same time though, around 60% of the students would be fine if rules for using the internet are being established by their parents.

The awareness of the students about the cyber security threats needs to be further strengthen, given that 40 % of the students feel that they are vulnerable while on the internet of which more than 13% have had some kind of bad personal experience themselves.

Most of the students are able to recognize radical content on the internet, as well as content that leads to violent extremism. Trolling, bullying and online insults are one of the most spread out content on the internet that high school students come across while on the internet, followed by content showing physical assault, ignition and beating. Large number of respondents' friends are sharing "Hate speech that directly encourages people to behave violently or commit an act of violence" and around half of their friends on the social media share content that involves trolling, bullying and online insults, as well as Violent content that is humorously portrayed. The content in most cases is shared through a personal message or in previously created groups for sharing of such content.

Analyzing the data from a gender perspective, we can see that harassment by friends or acquaintances is the biggest security threat online for both male and female respondents. Second biggest threat for the

male respondents is the unwanted access into sexual chat rooms on social networks or by email while for the female respondents that is abuse of personal pictures inappropriately.

If faced with internet threat the respondents would tell their parents and friends in most cases, while other local stakeholders are not in the picture, such as political, religious leaders or even teachers. One quarter of them said that they would report to the policy.

The research findings also show that youth from the targeted municipalities often practice to add strangers on their messenger or friends lists. But what is more worrying is that very often, they speak these people that only met on social media on the phone, they meet them in person or even have intimate conversations with them. Therefore, there is an urgent need to raise awareness for the possible risks these practice entails. As in the previous case, the invitations for in person meeting by an internet friend, respondents would report to the parents and friends in 98%.

Fake news could well be another factor that adds to the vulnerability of the youth to online radicalization and other forms of cyber threats. It is therefore essential to build youth's resilience to fake news through checking the reliability of the information on the internet as well as to build their capacities for critical thinking. This is more relevant if we know that almost half of the respondents in the survey said that rarely or never check the reliability of the information on the internet.

Regarding whether there should be a policy/guideline on the use of smartphones / devices and the internet in the school agreed between teachers, students and parents / guardians that will include guidelines for certain aspects of the use, the respondents would approve such guideline in average by close to 60%.

The development of training program for both teachers and students should be priority for policy creators at local and national level since there are many aspects that have not been addressed so far which are crucial in building resilience to online radicalization among youth and given that around 60% of the respondents said that they have never had training on the topics.

At the end, it must be noted that when analyzing the data across municipalities, in general, the same trend in most of the questions is followed in all municipalities, which suggests that youth in Macedonia perceive the threats related to the use of internet in more or less the similar manner. This is to great extent result of the fact that the youth from different municipalities, different socio-economic background and different ethnicity are part of the same educational system. Furthermore, the youth in North Macedonia

share the same socio-economic and political system, which adds up even more to shaping similar perception of the world in general and about specific phenomena such as cyber security and radicalization.

## 4.1 RECOMMENDATIONS

Based on the findings of the research, the project management team proposes the following recommendations for building youth resilience to online radicalization and cyber threats in the targeted municipalities:

1. The internet access of youth and their online activity should be regulated in their homes (by the parents/guardians) through:
    - Setting general rules for using the internet which should be in line with the good practices in this area[8]
    - Setting time limits for using the internet in the house as well as the time when the access is permitted in the house
    - Setting filters adequate for the age of the children
2. School workers should assume greater role in addressing cyber security and online radicalization through
    - Improving communication with students as to encourage them to talk to them more openly about their internet activity as they do with their parents at home;

School workers should improve their internet and computer skills to understand better students' needs and activity and to be able to help them in solving various issues in this field;

- Allocating more time during school classes and in extracurricular activities for covering the issues related to cyber security and radicalization

[8] For instance you can check CRPM's guidebook on cyber security http://www.crpm.org.mk/wp-content/uploads/2019/12/Vodich_za_sajber_bezbednost_PRINT.pdf

3. Development of awareness raising program to enable students and school worker to understand better, recognize and react to various cyber security threats and online radicalization at home and in schools.
4. Development of training program for students that will address the issues that according to the findings are most present on the internet and in the same time are perceived as biggest threats by the students, such as:
    - Trolling, bullying and online insults
    - Hate speech in all forms
    - Violent content in all forms
    - Harassment by friends and acquaintances online
    - Sharing information and privacy rules and settings
5. Development of protocols for early detection of victims of cyber threats and radicalization with adequate referral mechanism for the victims.
6. Establishing support groups for victims of cyber threats including radicalization which will include more stakeholders at both local and national level such as psychologists, pedagogists, social workers, civil society organization, policy etc.
7. Creating/development of reporting mechanisms that are effective, safe and fast such “red button” that will send notification to relevant institutions on radicalization and cyber threats.