ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 13 (2023) No. 4, pp. 624-639
DOI:10.33168/JSMS.2023.0438

An Exploratory Study on Ethics on the Internet

Anastasia Metsiou, Georgia Broni, Eleni Papachristou, Stavros Migkos, and Magdalini Kiki*

University of Western Macedonia, IEES, Koila Kozanis, Greece

dieees00004@uowm.gr

Abstract. Undoubtedly, the internet has become a part of people's daily life, since it supports activities that are related to communication, work, retrieving information, entertainment, and studies, Also the internet is increasingly used in the field of entrepreneurship, as it is widely used in the marketing. Nowadays, it has become a great part of people's socialization and moreover a necessary means of mediation in exchanging personal and governmental correspondence, as a standard and valid means of communication. Unfortunately, there appear to be not only positive but negative aftermaths to its use as well, for example, dark web, cyberbullying and problems concerning the private information online. The extent of the negative effects' appearance has aroused the importance of research to these fields and the necessity to take severe actions in order to abridge the negative effects. Thus, although the internet has been a great means in transforming the way that people interact with each other and the world around them, meanwhile, it has introduced new risks and challenges. In particular, the anonymity offered by the internet has made it easier for criminals to participate in illegal actions and bullies to engage in harmful behaviors, causing great harm. Therefore, further research is crucial to raise awareness about the dangers of the dark web, GDPR issues and cyberbullying, and to provide education and resources to help people protect themselves and others. As the interest of the investigation refers to quantitative parameters, we used a questionnaire to collect data from which we could derive conclusions regarding the present knowledge and perception of cyber security issues such as GDPR, internet safety, cyberbullying, and the dark web in Greece. Descriptive statistics and frequencies were applied to answer the research questions. The results have shown that, although people seem to understand the risks involved in the use of the internet, many of them don't fully seem to comprehend the extend of the risks that the internet can have to people's lives, and it is crucial for actions to be taken as to fully comprehend the depth of the problem. Therefore, theory and research should collaborate to raise awareness.

Keywords: Internet, ethics, dark web, cyberbullying, effects, actions.

1. Introduction

Without any doubt, the internet has "spread like fire" the last decades and has been a breakthrough in everyday life, but the risks involving its use have arisen a major challenge for society, enterprises and governments. The effects of its use concern the easiness for anyone to communicate and interact but also the easiness in the spreading of false or misleading information to a large audience. Misleading or criminal information and propaganda can lead to public confusion, distrust amongst people, and may even harm them. In addition, the rise of social media has amplified the problem, as it has become easier for the misinformation to be spread quickly through these platforms. Moreover, the internet has had a profound impact on privacy, as personal information can be easily collected, shared, and used without peoples' consent. There also appears to be a potential misuse of the people's personal information, as well as the rise of ethical and legal implications of data collection and usage. Overall, while the internet has brought many benefits to everyday life, it has also introduced new challenges that must be addressed, therefore further research in this field is always beneficial, as it is important for people to be aware of the dangers and to take steps to protect themselves and the information they share online. Therefore, governments, organizations, and individuals must work together to promote responsible and ethical use of the internet, to reduce the negative effects and to create a safer and more trustworthy online environment for everyone.

This paper aims in to investigate people's comprehension of the risks involved in the use of the internet nowadays that most of the population uses the internet. Additionally, it aims to raise awareness of the "new" dangers involved in the use of the internet.

2. Literature Review

2.1. Ethics in the Internet

There seems to be a relationship between technology and society that may appear complex in most cases. In fact, every technological exploit, and the internet in particular, can stimulate a variety of social reactions that depend on unpredictable variables. Moreover, the means of communication have altered in the past decades as to enhance the communication process (Postmes & Brunsting, 2002; Yus, 2011; Kalogiannidis, Chatzitheodoridis, Savvidou, & Macedonia, 2022). Nowadays, communication with the use of the internet has not only risen new ethical concerns but the existing ones are redefined as well. First of all, in relation to a central source of information, the main reference to the redefinition of private and public must be comprehended as the internet must comply with ethical values. In particular, there must be certain ethical limits complied to the use of the Internet (Kalogiannidis et al., 2022), and the users of the Internet must take into consideration whether the digital communities, that they participate in, follow certain, ethical rules regarding their creation and action and take into consideration the vulnerability of the privacy issues regarding these personal data (Broni et al., 2017). Many ethical dilemmas seem to arise from the use of the Internet, regarding the appearance of hackers, the dark web, and the distortion of reality, propaganda, and fake news as well as the preservation of the freedom of speech on the internet, the enhancement of cyberbullying and other illegal activities. The Internet seems to be ruled by complex means and consists of the interaction of people, consumers, businesses, researchers, and governments globally. And it is its rapid spread and the involvement of such diverse groups of people that incommode the ethical values to become worldwide through this global "ecosystem", which creates other ecosystems in it (Nie, & Hillygus, 2002).

The Internet is a powerful means of communication, inspiration, education, and entertainment that aims to bring its users "closer" by offering them an opportunity to create virtual communities and adapt to the world of technology. Problems arise when people's creativity is not always used for good but for illegal and harmful practices. Some examples of these practices are the presence of abusive content for people on the Internet and especially social media, most known as "Cyberbullying", the use of the dark and the darkest web for illegal actions such as the promotion of child pornography, drugs and weapons and terrorist communication. Moreover, many illegal online transactions and financial fraud take place

almost every day, by "stealing" GDPR context with the use of computer viruses and "fishing" or through chatrooms and social media, by people with technological skills who extract personal data (Juneja, 2013; Franks, 2020; Zhang, & Kim, 2020;).

2.2. Privacy on line

On the Internet, users choose the information they seek and approach it with specific procedures, by following their individual needs, seeking communication, or consuming through virtual shopping environments, such as "virtual malls". Communication however is the most important aspect of the Internet, and every user is exchanging personal messages via e-mail or other social applications and networks, through which users not only communicate with one another but also seek information, buy things and make their everyday life easier. In this "virtual" world however, there can be things that may jeopardize the users' privacy, meaning that all their actions are recorded, and every piece of information is stored and spread easily, while, nowadays the available software and applications are not as limited as they used to be. Through the Internet people tend to stream texts, images, videos, and audio in real-time, easily and anonymously (Isaivani, & Sivasankari, 2014).

As far as the applications that make one's life easier, most of them may be offered for free, as long as the user provides certain demographic and/or personal information and although users provide some information, they are usually asked if they want their information to be given to companies for purposes of exploitation advertising, known as "cookies", ensuring the privacy of their data (Kumar Bhoi, 2022). People tend to easily provide such information but the ease with which a model of complete monitoring of communications on the Internet can operate has made national and worldwide secret services proceed with the implementation of several forms of monitoring. But it's not just government agencies that are interested in the user's personal information, opinions, and needs but also the advertising and product promotion companies. Due to the fact that it is very difficult to accomplish a framework in order to "surf" the Internet without deviating in order to reach the bigger possible economic profit, the laws of the free market will prove to be the strongest opponent of privacy issues. For the first time in history, Internet ethics is such an important aspect due to the aspect of creation of a worldwide, electronic, cyber surveillance model (Koshti et al., 2016). But as Ahmed et al., (2012), have stated Internet is a means that gathers so many uses and so much information, offering to people the ability to interact with one another but all in all offers a common ground of contact for all kinds of information, users' age, personal data, professional history, medical history, purchases they have made, credit card information, banking transactions and people's everyday digital registries (Song, 2019).

Nowadays, the most important threat to privacy may come from the laws that apply to the free market, as the rapid development of information technology brings back imperatively the need for the development of mechanisms to protect its privacy (Broni & Velentzas, 2010). Technology, undoubtedly, offers many opportunities but it has serious side effects that lead to the need for new strategies and measures to solve privacy issues. The most important strategies-approaches suggest providing Internet users with the means to protect their private information. Also, quite important for preventing the "abuse" of private data is to apply holistic techniques of safeguarding the information, which will not allow the data to be recognizable. Last but not least, with the use of Privacy Enhancement Technologies, which are data encryption methods, users are offered multiple means to protect their personal data (Broni et al, 2013; Zahran et al., 2022).

2.3. Dark web

According to Parkar et al., (2017), the part of the internet that is inaccessible to conventional search engines is known as the "Deep" or "Dark" Web and it refers to messages, chat messages, private social media content, electronic banking messages, electronic health records and other deep web content, which, although accessible via the Internet, are not crawled and indexed by common search engines such as Google, Yahoo, Bing, etc. There are a variety of reasons why such information cannot be searched through conventional pages, as the primary priority is the protection of personal data and

private content, which only authorized visitors, can access through a virtual private network. Therefore, the access is protected through a portal site and is only available to people who have been granted access privileges and are protected by compliance regulations. It has not been ascertained how wide the “Deep” web is, but it is estimated by many experts that search engines reveal less than 1% of all deep web content. The “Deep” web is the fourth layer of the dark internet, with the layers starting from the first layer the “common web”, which people use almost every day, as it is open to the public. The second level is the “Surface” Web, which provides information and social content, with services such as Reddit, Digg, e-mail, and other communication platforms, and is also easily accessible. The third layer is called the “Bergie” Web and consists of Internet newsgroups, Google lock results, FTP sites, honeypots, and other sites such as 4Chan. Its use requires some knowledge of pathfinding. The fourth layer, as has been said, is the “Deep” Web, which is not managed by the broad "mass" of users but only by groups of hackers and other experts in the hidden layers of online society. The standard Web search engines are unable to find sites at this level, but an invitation from an existing member is required (Finklea, 2015; Zahran, Elkadi, & Helmy, 2022).

And finally, there is the fifth and “shadiest” part of the internet, the darkest web or “TOR Hidden Services”, with access being almost impossible, except for a certain group of users with the entry being almost forbidden. TOR network is a “paradise” of nefarious and criminal activities such as drugs, human and organ trafficking, pedophilia, sale of state secrets and arms trade, black market and other illegal activities (Chen, 2011; Biukšāne, 2015). The Dark web sites appear to be like almost any other site, but there are significant differences, primarily the name structure, since they do not end in “.com” or “.co”. The special ending “. onion”, features an anonymous hidden service accessible via the “Tor network” and can only be accessed with the appropriate proxy. The illegal activities that are possible within the “Dark web” are endless; a heaven of illegal activities, as it is possible to buy credit card numbers, drugs, weapons, counterfeit money, stolen credentials, and even software that allows access to other people's computers. In many cases, it is even possible to hire professional killers. There is of course the even darker side of the dark web, that it is the hub for activities, such as child pornography and the so-called “red rooms”, rooms where real human beings and animals are tortured, raped, and even murdered “live streaming”. Of course, the “Dark web” was not originally created as a “den” of illegal activities, but as a peaceful tool by the US government, in order to allow spies to exchange information completely anonymously. US military researchers developed the technology known as “Tor” and released it into the public domain for everyone to use. The reason for the seemingly non-existent decision was to keep them anonymous, since it would be harder to access the government's coded messages if thousands of others were using the same system for many different things, none related to government secrets (Weimann, 2016).

What is most important is the fact that although terrorists have been active on various online platforms in the past, nowadays they have found that the surface web is too dangerous for their illegal activities, since they were easy to track down, as many of the websites and social media are monitored by anti-terrorism agencies. The “Dark” web offered terrorists the anonymity that was a prerequisite for planning their illegal actions. Notably, extremist manifestoes are now being disseminated via the “Dark web”, as the terrorist action that has taken place after the November 2015 attacks in Paris, when ISIS used the “Dark” web to spread propaganda, in order to protect the identity of its supporters. Terrorists use the “Dark” Web as it provides them anonymity, ease in approaching and recruiting new terrorists, spreading radical ideas, raising funds, and coordinating their actions and attacks. Recently, it was discovered that ISIS and other jihadist groups have used new electronic applications that allow users to broadcast their messages to an unlimited number of members through encrypted mobile phone applications, using the Telegram software (encrypted instant messaging software) from the Islamic State and al-Qaeda. The communication channel was named Nashir, which translates to "Distributor" in English. The use of such channels has increased rapidly in recent years since in March 2016, 700 new channels were being used by the Islamic nation (Chen et al., 2008).

The payment method for illegal activities through the “Dark” web is cryptocurrencies, the well-known “bitcoins” and although the Bitcoin app has a tracker, it cannot be traced back to an individual, since there are various methods that hide the bearer's identity in a multitude of illegal transactions (Kim, 2020). When a payment with Bitcoin is entered into the system, it is transferred to the recipient's Bitcoin wallet in smaller denominations and then becomes almost untraceable and completely anonymous. This has serious consequences, as it drastically reduces the deterrence of malicious criminals, since the probability of their arrest is significantly reduced (Piazza, 2016; Kim, 2020). The use of Bitcoin in illegal online markets appear in every field of illegal action, from drugs to child pornography and weapons’ purchase, to human trafficking and is a lucrative business with profits exceeding $1 billion USD. While the percentage of Bitcoin transactions spent on illicit markets is declining, around $515 million of the digital coin has already been spent on the so-called “Dark web” in 2016, with dark-net spending on Bitcoin reaching its zenith in 2017, at $872 million (Kim et al., 2022).

2.4. Cyberbullying

Cyberbullying, as Li (2007), has characteristically said, is a “modern form” of bullying, meaning that although the traditional form of bullying was done face-to-face, cyberbullying manifests itself and is characterized as “an old wine in a new bottle” with its main characteristic being the use of technology that differentiates cyberbullying to traditional bullying. The main characteristics of this form of bullying are the use of information technology and communications, but also the fact that the hostile behavior is repeated and aims in causing harm to another person, who cannot easily defend himself and this leads to the repetition of the attack (Patchin, & Hinduja, 2015).

Cyberbullying is presented in several forms, depending on the way it is carried out and it targets specific persons seeking to intimidate them. Therefore, cyberbullying is an unpleasant situation that can be manifested by sending abusive messages, characterized as "flaming" (Moor et al., 2010). Moreover, harassment through the internet is also very common, and includes messages with abusive and offensive content that is characterized by repeated forms of harassment and attempts to defame and tarnish a person's reputation (Bayzick et al., 2011). Cyberbullying also appears in the form of an attempt to impersonate someone else's identity and make their personal information public. Yet, another form of cyberbullying is the so-called “happy slapping” and in that case the victim is physically attacked and being filmed by another person's mobile phone and the content is shared on the internet or on other mobile phones (Chan et al., 2012).

In fact, in several of these cases, despite the fact that cyberbullying has been characterized as “non-dangerous”, with only a small percentage of children to be victimized, however, it is impressive that the consequences of cyberbullying are very important, since it leads to children’s low self-esteem, drop in school performance, sleep disturbances, episodes of depression, desire to drop out of school or avoid contact with peers, as well as problems related to eating disorders, such as anorexia and bulimia. Most importantly, cyberbullying greatly affects children's desire to socialize and form healthy interpersonal relationships, which can be extremely traumatic for young and adolescent children (Patchin, & Hinduja, 2015). Studying the effects of cyberbullying, Baroncelli, & Ciucci (2014), concluded that children in their school environment are plagued by a sense of suspicion of their classmates, which leads to an inability to form interpersonal relationships as well as a lack of desire to open up and create friendly associations and hang out with their classmates, a feeling that opposes the innate human desire to create interpersonal relationships (Vazsonyi et al., 2012).

3. Research Methodology

3.1. Aim and research questions

The study aims to investigate the Greek people’s knowledge and perception of the terms in question, i.e., GDPR and Internet Safety, Cyberbullying, and the Dark Web. The secondary purpose is to investigate whether and to what degree the country’s citizens have encountered a leakage of personal

data or have been approached, harassed, or victimized by any action via the internet or have approached, harassed, or victimized others in any digital-based way.

The population under study, includes people above fifteen years of age, residing in Greece, with access to the internet for job or leisure purposes. The studied determinant is the degree of knowledge of the terms "GDPR" and "Internet Safety", "Cyberbullying", and the "Dark Web". A secondary determinant studied is the perception of the terms as Greeks declare to understand them. The outcome under study is the number of cases that have encountered one or more actions of personal data leakage, approach, harassment, or victimization of any kind caused by a third party via the internet or been caused by themselves to a third party.

Based on the stated purpose of the research and the individual objectives, the research questions were formulated as follows:

"In what degree the Greeks are aware of the concept of GDPR?"

"In what way do the Greeks perceive the concept of GDPR?"

"In what degree have the Greeks encountered a leakage of personal data?"

"In what degree the Greeks are aware of the concept of Cyberbullying?"

"In what way do the Greeks perceive the concept of Cyberbullying?"

"In what degree have the Greeks been victimized in an act of Cyberbullying of any kind?"

"In what degree have the Greeks done any actions of victimization using Cyberbullying?"

"In what degree the Greeks are aware of the concept of the Dark Web?"

"In what way do the Greeks perceive the concept of the Dark Web?"

"In what degree have the Greeks been approached, harassed, or victimized by someone via the Dark Web?"

"In what degree have the Greeks approached, harassed, or victimized someone via the Dark Web?"

3.2. Type of research

To answer the research questions posed and, given that the interest of the investigation refers to quantitative parameters, we used a questionnaire to collect data from which we could derive conclusions regarding the present knowledge and perception of cyber security issues such as GDPR, internet safety, cyberbullying, and the dark web in Greece. The questionnaire used was developed based on questionnaires previously used in related studies and/or governmental or official surveys. The collected data were then examined and analyzed in a descriptive approach, as, according to Finlay et al. (2013), descriptive research represents a fundamental methodology for examining a situation in its present form.

3.3. Data Collection – Measurement tool

To collect primary data for the purpose of conducting the quantitative survey, a structured closed-ended questionnaire was used, with questions adopted by the Adolescent Computer Use and Academic Achievement (Hunley, Krise, Rich, & Schell, 2005), and questions regarding the possible misunderstanding and abusive use of the internet. The later questions' answers were formed in case - statements, equivalent to possible issues or in simple "Yes/No" form. The questionnaire consisted of a total of 25 questions separated into five distinct parts. Seven questions concerned the demographic characteristics of the sample (first part) and four questions about computer and internet usage (second part). The following three parts consisted of questions concerning the knowledge and issues encountered and/or caused regarding the terms under investigation: four questions addressed GDPR and internet safety terms and issues (third part), five questions about cyberbullying (fourth part), and seven questions about the dark web (fifth part). Thus, three different research factors (dimensions) were defined.

The questionnaire was built in Google forms and distributed via e-mail and social media with extended information regarding the purpose of the survey, the preservation of anonymity, and the optionality of participating. The online questionnaire was active for a three-month period (1st of September to 31st of November 2022). The sample consisted of people of age greater than fifteen years,

living in Greece. 83 questionnaires were fully answered and submitted. Statistical analysis was contacted using the statistical program IBM SPSS Statistics 20.0. Descriptive statistics and frequencies were applied to answer the research questions.

4. Results and Discussion

4.1. Sample Description

Of the 83 participants of the study, 50 (60.2%) were females and 33 (39.8%) were males, while none of the respondents reported other gender or preference for non-disclosure (see Table 1). Concerning their location of residence, 40 participants (48.2%) resided at the time of the survey in Western Macedonia (see Table 2). Furthermore, the majority of the participants (32.5%) had a master's degree (see Table 3).

Table 1. Participants' distribution based on "gender"

Gender	Frequency (n)	Percentage (%)
Male	33	39.8
Female	50	60.2
Other	0	0.0
Prefer not to say	0	0.0
Total	**83**	**100.0**

Table 2. Participants' distribution based on "Location of residence"

Location	Frequency (n)	Percentage (%)
Attica	9	10.8
Central Greece	3	3.6
Central Macedonia	14	16.9
Crete	1	1.2
East Macedonia & Thrace	1	1.2
Epirus	7	8.4
Ionian Islands	1	1.2
North Aegean	2	2.4
Peloponessos	0	0.0
South Aegean	0	0.0
Thessaly	5	6.0
Western Macedonia	40	48.2
I don't reside in Greece	0	0.0
Prefer not to say	0	0.0
Total	**130**	**100.0**

Table 3. Participants' distribution based on "Educational Level"

Education	Frequency (n)	Percentage (%)
Primary Education	2	2.4
Secondary Education	11	13.3
Post-secondary Education	21	25.3
Bachelor's Degree	21	25.3
Master's Degree	27	32.5
Ph.D. or higher	0	0.0
Prefer not to say	1	1.2
Total	**83**	**100.0**

As far as concerns the marital status of the participants, statistical analysis showed that most of the sample (56.6%) were married or had a civil partnership agreement, while 50.6% hadn't got any children

(see Fig. 1). Furthermore, 51.8% of the participants were full-time employed (see Table 4).

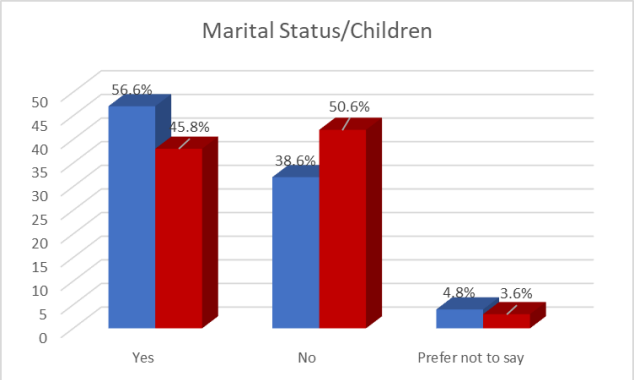

Fig. 1: Participants' distribution based on "Marital status" and "Children"

Table 4. Participants' distribution based on "Employment status"

Employment	Frequency (n)	Percentage (%)
Employed Full-Time	43	51.8
Employed Part-Time	6	7.2
Seeking opportunities	14	16.9
Student	19	22.9
Retired	1	1.2
Prefer not to say	0	0.0
Total	**83**	**100.0**

The age of the respondents was of a minimum value of 16 years of age and a maximum of 64, with a mean age of 32.41 years of age (±10.759) (see Table 5).

Table 5. Descriptive Statistics (Age)

	n	min	max	Mean	Std. Deviation	Variance	Skewness	Std. Error
Age (Numerical Value)	83	16	64	32.41	10.759	115.757	0.537	0.264
Valid N (listwise)	**83**							

4.2. Computer and Internet Use

Statistical analysis of the responses given showed that 98.8% of the sample (82 persons) stated that they owned or had access to a Personal Computer, laptop, tablet, smartphone, or another similar device at the time of the survey, while 73.5% (51 persons) reported that their work status required using a Personal Computer, Laptop, etc., 94.0% (78 persons) replied that they use a Personal Computer, Laptop, etc. for purposes other than working or studying and 98.8% (82 persons) that they had access to the Internet (see Table **6**, Fig. 2).

Table 6. Computer and Internet Use Frequencies Table

	Yes		No		Prefer not to say	
	n	%	n	%	n	%
Do you currently own or have access to a Personal Computer, laptop, tablet, smartphone, or another similar device?	82	98.8	1	1.2	0	0.0
Does your current work status require using a Personal Computer, Laptop, etc.?	61	73.5	21	25.3	1	1.2
Do you use a Personal Computer, Laptop, etc., for purposes other than working or studying?	78	94.0	5	6.0	0	0.0
Do you have access to the Internet?	82	98.8	1	1.2	0	0.0

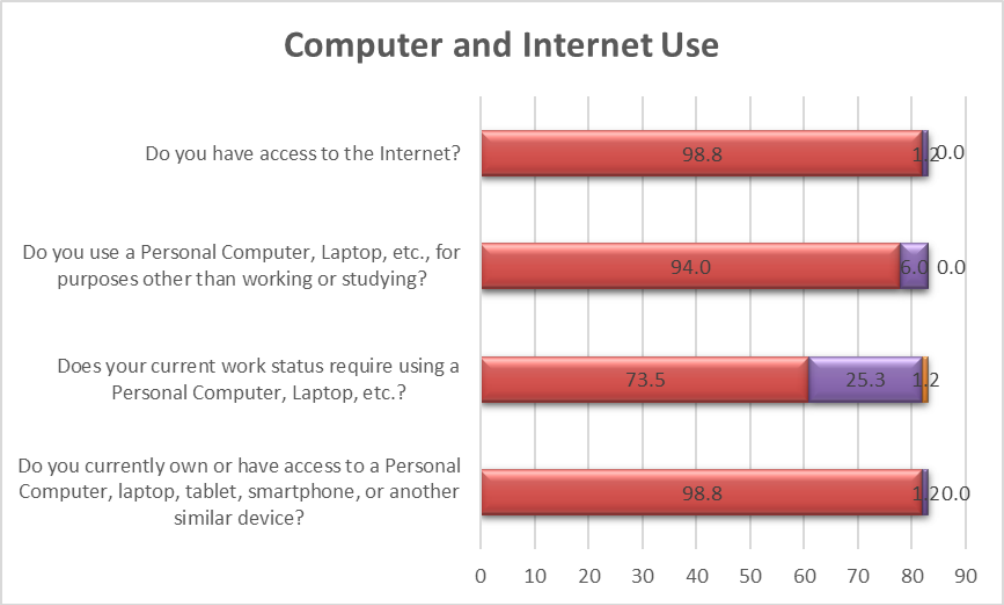

Fig. 2: Computer and Internet Use responses' frequencies

4.3. GDPR and Internet Safety

According to the responses given by the sample to the questions regarding the knowledge of the purpose of the General Data Protection Regulation (GDPR), the majority of the survey's sample (42.2% i.e., 35 responders) had only a general idea, while a significant portion of the respondents was not sure about the GDPR purpose although had seen statements on several websites or had never seen the term before (13.3% and 18.1% respectively, summing up to 26 persons in total not knowing the exact purpose of GDPR). Nevertheless, 22 persons (26.5%) replied that they fully understood the meaning and purpose of GDPR. As for the consent to Privacy Policy and Cookies terms, most of the participants (38.6%) stated that they usually choose the "Accept All" statement, although the "Necessary Only" statement was the answer of choice of the 36.1% of the sample. However, 14 respondents (16.9% of the sample) replied that they usually choose the "Reject All" statement and 7 (8.4%) that prefer to always read thoroughly all the options and choose respectively. The vast majority of the participants (78.3%) had never encountered a personal data leakage, though the 18.1% of the sample replied that they had encountered a leakage once and the 3.6% that they had a problem with personal data leakage many times. Similar responses were given concerning the knowledge of any case of personal data leakage in their social circle, with the 45.8% of the sample replying that no one of their close acquaintances have ever encountered a leakage problem, 38.6% that they knew someone who encountered such a problem

and 13.3% knew some people that have faced such a problem (see Table 7, Fig. 3).

Table 7. GDPR and Internet Safety Frequencies Table

	Yes	almost yes	kind of	no	prefer not to say
Do you know the purpose of GDPR (General Data Protection Regulation)?	22	35	11	15	0
Do you usually consent to the Privacy Policy and Cookies terms as written on a website?	32	7	30	14	0
Have you ever encountered a problem with the management or safeguarding of your personal data on a website?	3	15		65	0
Has anyone from your close acquaintances encountered a problem with the management or safeguarding of their personal data on a website (that you know of)?	11	32		38	2

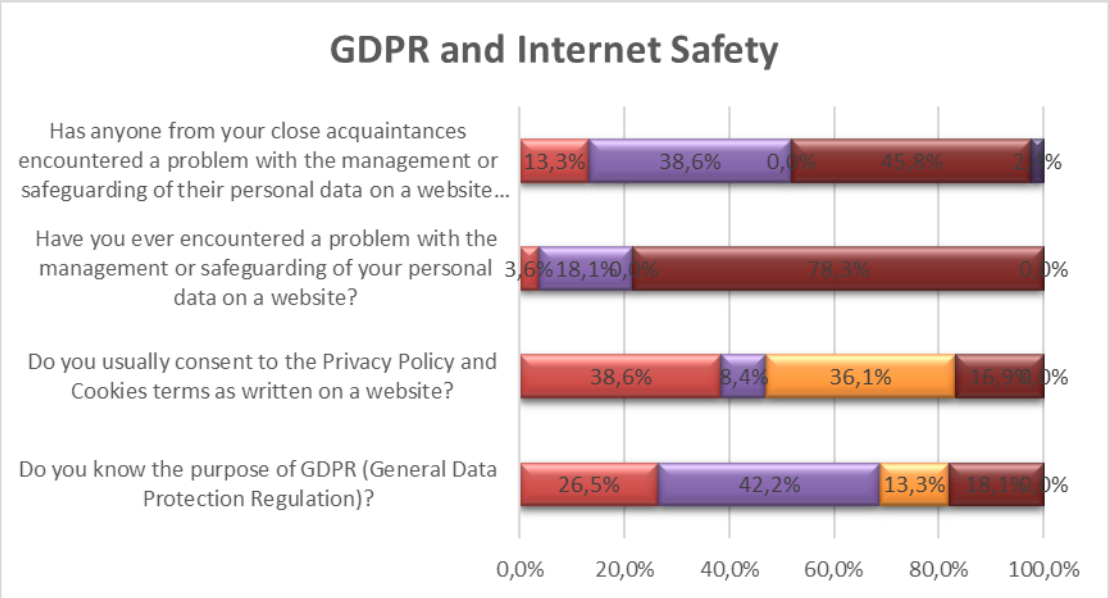

Fig. 3: GDPR and Internet Safety responses' frequencies

4.4. Cyberbullying

The responses collected regarding the knowledge of Cyberbullying meaning as well as the possibility of having been a victim or even having victimized others showed that 96.4% of the sample was familiar with the term. Most of the respondents (74.7%) replied that have never been victimized in an act of Cyberbullying of any kind, though the percentage of people who replied positively to the respective question is high enough to evoke concerns (21.7%). Also of concern is the fact that although most of the answers (56.6%) that were given as a response to the question of whether the responder has ever done any actions that could be characterized as "acts of Cyberbullying" were negative, a very considerable percentage (41.0%) has answered positively. Finally, the answers given to the fourth question, show that most of the respondents (80.7%) do not seem to know other people who have ever done any actions that could be characterized as "acts of Cyberbullying". Nevertheless, and in this case, as in the previously mentioned ones, the percentage of positive responses (14.5%) may be considered to be high enough to raise concerns (see Table 8, Fig. 4).

Table 8. Cyberbullying Frequencies Table

	yes		no		prefer not to say	
	n	%	n	%	n	%
Do you know what the term "Cyberbullying" means?	80	96,4	3	3,6	0	0
Have you ever been victimized in an act of Cyberbullying of any kind?	18	21,7	62	74,7	3	3,6
Have you ever done any actions that could be characterized as "acts of Cyberbullying" of any kind?	34	41	47	56,6	2	2,4
Has anyone from your close acquaintances ever done any actions that could be characterized as "acts of Cyberbullying" of any kind (that you know of)?	12	14,5	67	80,7	4	4,8

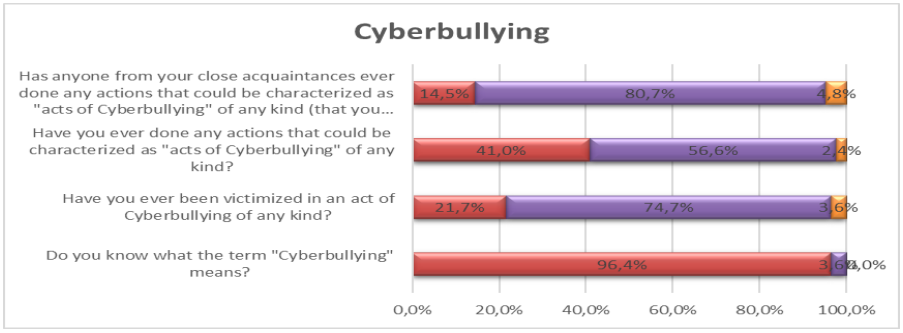

Fig. 4: Cyberbullying responses' frequencies

4.5. Dark Web

The last set of questions aimed at the measurement of the respondent's knowledge of the term "Dark Web", as well as the possibility of having engaged in an attempt of connecting to the Dark Web, and the possibility of having been approached by or have approached anyone via the Dark Web in a non-appropriate way or purpose. The results showed that most of the respondents (74.7%) were aware of the term's meaning. On the contrary, the majority of the responses regarding a previously made attempt of connecting to the Dark Web was negative (77.1%) as well as the responses regarding such an attempt made by a close acquaintance of each respondent (73.5%). According to the sample's replies actions like an approach, harassment, or victimization via the Dark Web were not experienced by the responders or their close acquaintances (94.0% and 84.3% negative responses respectively). Similar percentages were counted through the answers to the two last questions regarding the possibility of the sample or their close acquaintances having been responsible for an approach, harassment, or victimization of somebody via the Dark Web (92.8% and 89.2% respectively) (see Table 9, Fig. 5).

Table 9. Dark Web Frequencies Table

	yes		no		prefer not to say	
	n	%	n	%	n	%
Do you know what the term "Dark Web" means?	62	74,7	21	25,3	0	0
Have you ever managed or tried to connect to the Dark Web?	16	19,3	64	77,1	3	3,6
Has anyone from your close acquaintances ever managed or tried to connect to the Dark Web (that you know of)?	19	22,9	61	73,5	3	3,6
Have you ever been approached, harassed, or victimized by someone via the dark web?	1	1,2	78	94	4	4,8
Has anyone from your close acquaintances ever been approached, harassed, or victimized by someone via the dark web (that you know of)?	6	7,2	70	84,3	7	8,4
Have you ever approached, harassed, or victimized anyone via the dark web?	1	1,2	77	92,8	6	6
Has anyone from your close acquaintances ever approached, harassed, or victimized anyone via the dark web (that you know of)?	1	1,2	74	89,2	8	9,6

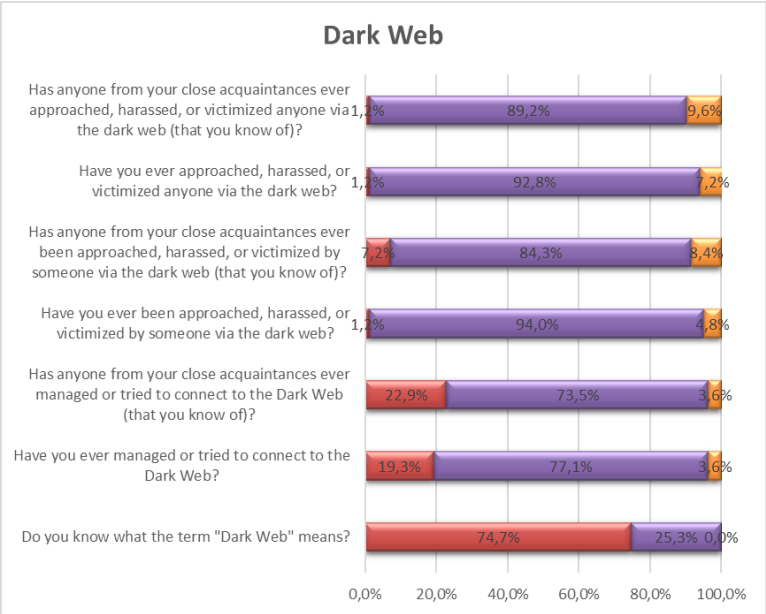

Fig. 5: Dark Web responses' frequencies

4.6. Discussion

The statistical analysis of the responses revealed that almost all (98.8%) of the 82 individuals surveyed owned or had access to a personal computing device such as a PC, laptop, tablet, or smartphone, and had access to the internet. Additionally, most (73.5%) of them reported that their work required the use of a personal computing device, while a large majority (94.0%) used these devices for non-work or study purposes. Based on the statistical analysis of the responses, personal computing devices and access to the internet are widely prevalent among the surveyed individuals. The high percentage of individuals who reported having access to these devices suggests that technology has become an integral part of their daily lives. Furthermore, the fact that most of the respondents reported that their work requires the use of these devices highlights the importance of technology in the modern workplace. Moreover, the number of individuals who reported using these devices for purposes other than work or study suggests that technology is not just a tool for productivity but also a source of entertainment and leisure. The widespread availability of the internet has made it possible for individuals to access information, connect with others, and engage in various online activities.

The survey results regarding the knowledge of the General Data Protection Regulation (GDPR) show that the majority of respondents had a general idea of its purpose (42.2%), while a considerable number were unsure or had never heard of it before (26 persons in total). A minority of participants (26.5%) fully understood the GDPR. When it comes to the privacy policy and cookie terms, most people usually accepted all (38.6%), while a smaller number rejected all (16.9%). A large majority of the sample (78.3%) had not experienced a personal data leakage, but a minority reported having experienced it once or multiple times. In regard to personal data leakage among close acquaintances, the majority (45.8%) of participants did not know anyone who had experienced it, while a significant minority (38.6%) reported knowing someone who had. The results of the survey on the knowledge of the General Data Protection Regulation (GDPR) raise some important questions about the awareness and understanding of privacy and data protection regulations. One of the key conclusions is that a large portion of the respondents had only a general idea of the GDPR and its purpose. This highlights the importance of increasing public awareness and education on these types of regulations, which are crucial for protecting personal data and privacy. Another interesting finding is the range of approaches to the privacy policy and cookie terms. While some individuals choose to accept all, others reject all, and a smaller group carefully reviews each option. This suggests that there is a need for more clarity and transparency in the presentation of these terms to enable individuals to make informed decisions

about their privacy. The fact that a significant minority of respondents reported having experienced a personal data leakage, either among themselves or among their close acquaintances, highlights the importance of ensuring that personal data is properly protected and secure. It also raises questions about the effectiveness of existing data protection regulations and the need for continuous improvement and enforcement.

The results of the Cyberbullying related questions showed that a large majority of the sample (96.4%) was aware of the term. However, while 74.7% of respondents reported that they have never been a victim of Cyberbullying, the 21.7% who have experienced it is a cause for concern. Additionally, while the majority (56.6%) reported that they have never engaged in acts of Cyberbullying themselves, the 41.0% who have is another concerning issue. Furthermore, 80.7% of respondents claimed that they do not know anyone who has engaged in acts of Cyberbullying, however, the 14.5% who have is again high enough to raise concerns. Thus, it is revealed that the vast majority of the respondents are familiar with the term. However, a significant number of respondents reported either being victims or having engaged in acts of Cyberbullying themselves. This highlights the need for greater awareness and education on the dangers and consequences of Cyberbullying. Of particular concern is the high percentage of respondents who reported having been victims of Cyberbullying and the even higher percentage of respondents who admitted to engaging in acts of Cyberbullying. This suggests that Cyberbullying is a widespread issue that needs to be addressed through education, prevention programs, and enforcement. Despite the high numbers of respondents who have either been victims or engaged in Cyberbullying, most respondents claimed not to know others who have done so. This may indicate a general lack of awareness and a reluctance to report incidents of Cyberbullying. The results indicate that while the general knowledge of Cyberbullying is high, there is still a significant portion of the population who have either been victims or perpetrators of Cyberbullying. It highlights the importance of education and prevention efforts to reduce the occurrence of Cyberbullying and create a safer online environment for all. Therefore, these results underline the need for greater public awareness and education on the issue of Cyberbullying, as well as the importance of providing support and resources to those affected by it.

The results of the survey on knowledge and experience with the Dark Web showed that most of the respondents (74.7%) were aware of the term's meaning. However, the majority of the respondents (77.1%) had not attempted to connect to the Dark Web and a similar percentage (73.5%) reported that a close acquaintance had not attempted to connect as well. The respondents and their close acquaintances reported no experiences of being approached, harassed, or victimized through the Dark Web (94.0% and 84.3% negative responses respectively). Similarly, the respondents and their close acquaintances reported no involvement in approaching, harassing, or victimizing someone through the Dark Web (92.8% and 89.2% negative responses respectively). These results suggest that while most of the sample is aware of the term "Dark Web," they have not been directly involved in any activities related to it. However, it's worth noting that the percentage of negative responses may not accurately reflect reality and it's possible that some incidents may have gone unreported. It's important for individuals to be cautious and aware of the potential dangers of the Dark Web, and for society to continue educating and raising awareness about the potential negative impacts of this part of the internet.

5. Conclusions

According to the results of this survey, the Greeks are not fully aware of the concept of GDPR, as only a minority of the sample (26.5%) stated that fully understood the term. Nevertheless, most respondents (78.3%) declared that had never encountered a leakage of personal data. The results of the Cyberbullying related questions showed that a large majority of the sample (96.4%) was aware of the term. The percentage of positive answers regarding the case of having been victimized via Cyberbullying acts though less than the negative ones (21.7% versus 74.7%) is concerning as it shows a significant number of cases. At the same time concerning is the fact that while the majority (56.6%)

reported that they have never engaged in acts of Cyberbullying themselves, 41.0% have. Consequently, these results indicate that while the general knowledge of Cyberbullying is high, there is still a significant portion of the population who have either been victims or perpetrators of Cyberbullying. The answers regarding knowledge and engagement with the Dark Web showed that although the majority of the respondents (74.7%) were aware of the term, most of them or their close acquaintances had never attempted to connect (77.1% and 73.5% respectively). Similar are the results concerning the experiences of being approached, harassed, or victimized through the Dark Web (94.0% and 84.3% negative responses for the answerers and their acquaintances respectively) as well as the results concerning the respondents and their close acquaintances as they reported no involvement in approaching, harassing, or victimizing someone through the Dark Web (92.8% and 89.2% negative responses respectively), showing a minimum involvement with this aspect of the internet in Greece.

Nevertheless, as the survey sample was limited, it is suggested that the subject should be further investigated, with an extended survey with a larger sample size. Furthermore, future research on cyberbullying could focus on exploring the psychological and emotional effects of cyberbullying on its victims, as well as on the individuals who engage in cyberbullying behaviours. Other possible areas of research could include examining the ways in which technology and social media platforms contribute to the prevalence of cyberbullying, as well as the development and implementation of effective prevention and intervention strategies for addressing cyberbullying. With regards to the Dark Web, future research could focus on the motivations and actions of individuals who engage in illegal or unethical activities on the Dark Web, as well as the measures that can be taken to monitor and regulate these activities. Additionally, further research could explore the potential positive uses of the Dark Web, such as for secure communication or protecting the privacy of sensitive information, and the steps that can be taken to ensure the safe and ethical use of the Dark Web.

Consequently, some future research topics related to these subjects could include:

- The impact of cyberbullying on mental health and well-being of individuals and the efficacy of interventions aimed at reducing its effects.
- The role of social media in cyberbullying and its influence on the prevalence of cyberbullying among adolescents and young adults.
- The relationship between cyberbullying and traditional bullying and the effectiveness of bullying prevention programs in reducing both forms of bullying.
- The examination of demographic and situational factors that contribute to cyberbullying, such as gender, age, socio-economic status, and location.
- An exploration of the motivations and psychological profiles of individuals who engage in cyberbullying.
- The development and evaluation of educational and awareness-raising programs aimed at preventing cyberbullying.
- A study of the legal and ethical implications of cyberbullying and the effectiveness of current laws in addressing cyberbullying.
- An investigation of the accessibility and use of the Dark Web and its relationship to cybercrime and illegal activities.
- A study of the ways in which individuals can protect themselves from the dangers of the Dark Web and the efficacy of current security measures.
- An examination of the impact of the Dark Web on society and the role of governments and law enforcement in regulating and controlling its use.

References

Ahmed, M., Sanjabi, B., Aldiaz, D., Rezaei, A., & Omotunde, H. (2012). Diffie-Hellman and its application in security protocols. *International Journal of Engineering Science and Innovative Technology (IJESIT)*, Vol. 1, No. 2, 69-73.

Baroncelli, A., & Ciucci, E. (2014). Unique effects of different components of trait emotional intelligence in traditional bullying and cyberbullying. *Journal of adolescence*, Vol. 37, No. 6, 807-815.

Bayzick, J., Kontostathis, A., & Edwards, L. (2011). Detecting the presence of cyberbullying using computer software.

Biukšāne, I. (2015). Index of the Fisheries Sector Cluster Competitiveness. *Journal of System and Management Sciences*, *5*(4), 63-83.

Broni, J. Velentzas. G. "Ethical dimensions in the conduct of business: business ethics, corporate social responsibility and the law. The "ethics in business" as a sense of business ethics," *International Conference On Applied Economics (ICOAE),* 2010, August, (p. 795).

Broni, G., Velentzas, J., & Kartalis, N. (2013). Hobbes's Meaning of Hostility & Politics of an Apology: the Double-edge of Organizational Legitimation. Strategic and Institutional Approaches in Crisis Communication. *Procedia Economics and Finance*, Vol. 5, 113-119.

Broni, G., Velentzas, J., & Papapanagos, H. "Marketing Ethics and Communication Strategy in the Case of Enron Fraud", *Advances in Applied Economic Research: Proceeding of the 2016 International Conference on Applied Economics (ICOAE), Springer International Publishing*, 2017, (pp. 269-278).

Chan, S., Khader, M., Ang, J., Tan, E., Khoo, K., & Chin, J. (2012). Understanding 'happy slapping'. *International Journal of Police Science & Management*, Vol. 14, No. 1, 42-57.

Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008). Uncovering the dark Web: A case study of Jihad on the Web. *Journal of the American society for information science and technology*, Vol. 59, No.8, 1347-1359.

Chen, H. (2011). *Dark web: Exploring and data mining the dark side of the web. Springer Science & Business Media*, Vol. 30.

Finklea, K. M. (2015). Dark web.

Finlay, I., Sheridan, M., Coburn, A., & Soltysek, R. (2013). Rapid response research: using creative arts methods to research the lives of disengaged young people. *Research in Post-Compulsory Education*, Vol. 18, No. 1-2, 127-142.

Franks, M. A. (2020). How the Internet Unmakes Law. *Ohio St. Tech. LJ*, Vol. 16, 10.

Hunley, S. A., Krise, J., Rich, T., & Schell, C. (2005). Adolescent computer use. *Adolescence*, Vol. 40, No. 158.

Isaivani, M., & Sivasankari, T. (2014). An Enhancement of Security Standards based on Pseudonyms in Near Field Communication. *International Journal of Innovative Research in Science, Engineering and Technology*, Vol. 3, No. 3.

Juneja, G. K. (2013). Ethical hacking: a technique to enhance information security. *International Journal of Innovative Research in Science, Engineering and Technology*, Vol. 2, No. 12, 7575-7580.

Kalogiannidis, S., Chatzitheodoridis, F., Savvidou, S., Kagioglou, F., & Macedonia, W. (2022). The Impact of Online Communications on Different Users' Social, Emotional, and Moral Competence as a Potential Business Communication Tool. *Journal of System and Management Sciences*, Vol. 12, No. 5, 359-373.

Kim, J. W. (2020). Blockchain technology and its applications: case studies. *Journal of System and Management Sciences*, Vol. 10, No. 1, 83-93.

Kim, M., Lee, J., Kwon, H., & Hur, J. (2022). Get off of Chain: Unveiling Dark Web Using Multilayer Bitcoin Address Clustering. *IEEE Access*, Vol. 10, 70078-70091.

Koshti, M., Ganorkar, S., & Chiari, L. (2016). IoT based health monitoring system by using Raspberry Pi and ECG signal. *International Journal of Innovative Research in Science, Engineering and Technology*, Vol. 5, No. 5, 8977-85.

Kumar Bhoi, S. (2022). A Cloud Based Machine Intelligent Human Activity Recognition System Using Internet of Things to Support Elderly Healthcare. *Bhoi, SK, & Krishna Prasad, K.,(2022). A Cloud Based Machine Intelligent Human Activity Recognition System Using Internet of Things to Support Elderly Healthcare. International Journal of Management, Technology, and Social Sciences (IJMTS)*, Vol. 7, No. 2, 386-400.

Li, Q. (2007). New bottle but old wine: A research of cyberbullying in schools. *Computers in human behavior*, Vol. 23, No. 4, 1777-1791.

Moor, P. J., Heuvelman, A., & Verleur, R. (2010). Flaming on youtube. *Computers in human behavior*, Vol. 26, No. 6, 1536-1546.

Nie, N. H., & Hillygus, D. S. (2002). The impact of Internet use on sociability: Time-diary findings. *It & Society*, Vol. 1, No. 1, 1-20.

Parkar, A., Sharma, S., Yadav, S. (2017). Introduction to deep web. *International research journal of engineering and technology (irjet*), pp 5650-5652

Patchin, J. W., & Hinduja, S. (2015). Measuring cyberbullying: Implications for research. *Aggression and Violent Behavior*, Vol. 23, 69-74.

Piazza, F. (2016). Bitcoin in the dark web: a shadow over banking secrecy and a call for global response. *S. Cal. Interdisc. LJ*, Vol. 26, 521.

Postmes, T., & Brunsting, S. (2002). Collective action in the age of the Internet: Mass communication and online mobilization. *Social science computer review*, Vol. 20(3), 290-301.

Song, Y. J. (2019). Blockchain-based power trading process. *Journal of System and Management Sciences*, Vol. 9, No. 3, 78-91.

The nature and management of ethical corporate identity: A commentary on corporate identity, corporate social responsibility and ethics. *Journal of business ethics*, Vol. 76, No. 1, 7-15.

Vazsonyi, A. T., Machackova, H., Sevcikova, A., Smahel, D., & Cerna, A. (2012). Cyberbullying in context: Direct and indirect effects by low self-control across 25 European countries. *European Journal of Developmental Psychology*, Vol. 9, No. 2, 210-227.

Weimann, G. (2016). Going dark: Terrorism on the dark web. *Studies in Conflict & Terrorism*, Vol. 39, No. 3, 195-206.

Yus, F. (2011). *Cyberpragmatics: Internet-mediated communication in context*. John Benjamins Publishing Company.

Zahran, S., Elkadi, H., & Helmy, W. (2022). Fog Computing Platform to Handle Internet of Things Data Heterogeneity. *Journal of System and Management Sciences*, Vol. 12, No. 1, 521-544.

Zhang, L., & Kim, H. (2020). The influence of financial service characteristics on use intention through customer satisfaction with mobile fintech. *Journal of System and Management Sciences, 10*(2), 82-94.