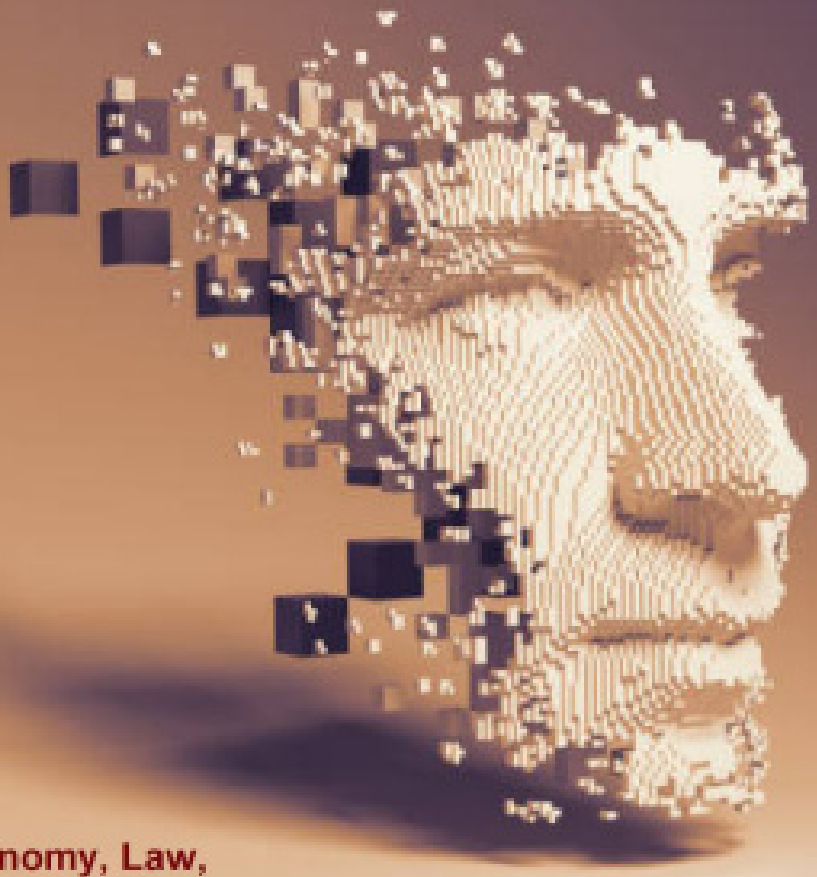
ISSN 2955-2036
ISSN 2955-2044

INTERNATIONAL JOURNAL OF SOCIAL SCIENCES

SCIENTIFIC INSTITUTE OF MANAGEMENT & KNOWLEDGE

Vol. 1 Issue 1

SCIENCE IJ



Sociology, Economy, Law,
Politics, Demography, Psychology
Security, Education, Humanities

IJSS Vol, 1 Issue 1 Skopje 2022

ISSN 2955-2044 (Online)

SCIENCE International journal

Volume 1, Issue 1, December 2022.

https://scienceij.com/

IMPRESSUM

SCIENCE International journal

(Volume 1, Issue 1, December 2022.)

Editor in chief:
Prof. d-r Robert Dimitrovski

Executive editor:
Prof. dr. Lazar Stošić

Publisher:
Institute of Management and Knowledge
Address: Gjuro Gjonovikj, 11/4 , Skopje 1000, Macedonia
Phone: +389 70 207 370, + 381 63 700 4281

https://scienceij.com/
E-mail: editor@scienceij.com

For publisher:
Prof. d-r Robert Dimitrovski

Print:
GRAFOPROM Bitola

Circulation:
50 copies

CONTENTS

Mujević, M. (2022). Synthesis of threats and risks of cyber security of Montenegro - the vulnerability aspect of information communication infrastructure, *SCIENCE International journal, 1*(1), 1-12. doi: 10.35120/sciencej010101m
UDK: sss

SYNTHESIS OF THREATS AND RISKS OF CYBER SECURITY OF MONTENEGRO - THE VULNERABILITY ASPECT OF INFORMATION COMMUNICATION INFRASTRUCTURE

Mersad Mujević[1*]

[1]International University in Novi Pazar, Republic of Serbia, e-mail: mersad.mujevic@uninp.edu.rs

Abstract: That there are no untouchables and that cyber threats are entering Montenegro through the big doors, is indicated by the hacker attack on the Government of Montenegro. Fortunately, the hackers did not get hold of confidential data, but their act itself caused a serious act of endangering state security, especially because they breached the system that is networked with all state bodies. It was not the first time in 2022 that hackers broke into Government IC systems and state and private companies and organizations. Experts from the IT sector have been warning about the vulnerability of the system for a long time, but not loudly enough to be taken seriously. Let's also mention the attack on Montenegro on the eve of joining NATO, where Montenegro was under increased cyber attacks, and the Ministry of Defense says that it is similar today.

Cyber is no longer the world of gamers and geeks, it is increasingly becoming a prefix for terrorism, crime, and other types of threats (Kazerić 2017). Internet trade and the use of electronic services such as e-government are also on the rise. To the global trend, almost everything that was only tangible and materialized in the real world is moving to the virtual community. This brings with it many advantages, but also disadvantages, and one of them is certainly the vulnerability of critical information and communication infrastructure and the danger of cyber attacks. In such circumstances, the issue of security partially shifts the focus to cyber, that is, cyber security. Precisely for this reason, it is necessary to take a critical look at the existing information and communication infrastructure and analyze the existing threats and risks brought by the modern, cybernetic age. The synthesis of threats and risks is necessary so that we can adequately face them and predict the difficulties that may come our way, which could have significant consequences for national security.

Keywords; cyber, critical infrastructure, hackers, cyber security.

1. INFORMATION SECURITY

When it comes to information security, there is no system, data, or completely secure. Experts like to joke that "the only information system that is truly secure is shut down, unplugged, locked in a titanium safe, buried in a concrete bunker, and surrounded by nerve gas and well-paid armed guards" (Spafford, according to Hadjina, 2009:7). There is a half-truth in every joke, and so it is with the mentioned quote about information security, which today, more than ever, is becoming a point of reference for every state, private, profit, and non-profit organization. Important information about company operations, state secrets, and confidential matters are no longer stored only in thick, old binders or safes. Today, they are located in the computer cloud, on the internal network of a particular company, on an employee's computer. The security of that data depends not only on hardware and software protection - but also largely on the security culture and the behavior of employees with that, often sensitive, data. Therefore, information security can be defined as the preservation of confidentiality, integrity – completeness, and availability - availability of data (Brnetić et al., 2013:6), which according to the Law on Information Security of Montenegro "is ensured by the application of information security measures and standards".

1.1. Information system

"All objects that contain all the company's information in some form are called an information system. An information system can be defined as the comprehensiveness of technological infrastructure, organization, people, and procedures for collecting, processing, generating, storing, transmitting, displaying, and distributing information as well as disposing of it" (Nađ and Adelberger, 2016:117).

The key element in that system is information that ceases to be data at the moment when it acquires meaning in a certain context. For example, data can be unrelated terms and numbers like 789, CIRT, and 2021, which are raw and have no meaning for the individual. When these data are interpreted, they acquire

*Corresponding author: mersad.mujevic@uninp.edu.rs

meaning for an individual, company, and/or institution. Thus, previously unrelated and insignificant data gain meaning when we say: According to CIRT data, 789 cyber attacks were recorded in Montenegro in 2021.

Support resources within an information system can be defined as resources within which information is located. These include hardware, software, networks, staff, locations, core services, and the organizational environment.

1.2. Aspects of information security

Aspects of information security are connected through the security triangle (CIA triad), which consists of confidentiality, integrity, and availability. In recent times, certain experts have added the aspects of provability, authenticity, and irrefutability to the mentioned categories (Kezerić 2017).

1.2.1. Confidentiality

When it comes to the first aspect of information security, confidentiality, refers to the preservation, that is, the protection of the secrecy of data and the impossibility of unauthorized persons accessing that data. Threats to the violation of data confidentiality are different, and the most common are hacking, masking, unauthorized user activity, unprotected file downloads, Trojan horses, and the like (Juran, 2012:18). “Trust attacks are attempts to break into a computer or network monitor activities or extract system information or user data. A criminal who steals a bank card or a spy who steals the design of an airplane commits an attack on trust, but the consequences of financial fraud or espionage are different” (Singer and Friedman, 2014:70). Methods of preserving data confidentiality are the use of access control and encryption methods. In the case of data access control, the point is to limit access to data marked as classified or secret through the principles of physical or logical security, and that only authorized persons can access them, while others, through physical or logical control, are denied access to that data (Kezerić 2017).

1.2.2 Integrity

Brnetić et al. (2013:6) define integrity as “protecting the existence, accuracy, and completeness of information as well as process methods”. Integrity or completeness as an aspect of the security triangle refers to the fact that data/information must remain unaltered, complete, and accurate. In other words, when processing data and information, they must not be modified or changed without authorization from authorized persons.

1.2.3. Availability

To fulfill the condition of availability, data and information must be timely available and accessible to authorized users whenever there is a need for it. “Availability attacks are those that defend access to a network, either by overwhelming it with traffic or denying access or even taking it off the network and even physically shutting down virtual processes that depend on it” (Singer and Friedman, 2014:70).

1.3. Informational vs. IT security

The areas of information security specified in the Law on Information Security of Montenegro are security checks, data security, physical security, information system security, and business cooperation security. As is evident from that division, information security covers a much wider area than IT/computer security, security which mainly covers only technical parts of security. As Vuković (2012:23) concludes, “information security is only one part of information security that deals with technological protection (eg antiviruses, encryption, etc.). However, IT security does not cover e.g. managing people who are often a very big source of risk”.

1.4. Information security vs. cyber security

I have already defined information security. But what does it have to do with the term cyber (cybernetic) security, which is so popular today? The point is very simple - since most information today is in digital form, information and cyber security can be considered almost synonymous. The definition of cyber security stated in the Dutch Cyber Security Strategy from 2011, and referred to by Košutić (2012:24), states that cyber security means being free from danger or damage caused by interruption, disruption, or failure of information and communication technologies or abuse of ICT a. As they further state, the damage caused by a cyber attack can consist of “limiting the availability and reliability of ICT, violating the confidentiality of the information stored in ICT or damaging the integrity of that information” (Dutch Ministry of Security and Justice, 2011, according to Košutić, 2012: 24). So, in the aforementioned

definition of cyber security, we can see all three aspects of information security, that is, the security triad. "Cyber security is 95% of information security" (Košutić, 2012:26). As the only difference between them, Košutić (2012:26) cites the fact that information security includes information security in the matter of non-digital media, that is, information security in its traditional form. On the other hand, cyber security focuses exclusively on the security of information in digital form.

1.5. "Myths" about cyber security

In today's world, cyber security is a large and indispensable part of information security and will be considered as such in the continuation of this work. However, cyber security does not "revolve" only around new technologies and is not a one-time process, which is the most common myth associated with it. Technology is only one element of a successful information security policy, but alongside it are people and processes, the importance of which should not be ignored (Klaić, 2010: 1). This is precisely why Košutić (2012) warns of six prevailing myths when it comes to cyber security, especially in modern companies.

These are the following myths:
1. Everything revolves around ICT,
2. Cyber security is not a problem of top management - they have nothing to do with it,
3. Most (future) investments in cyber security will be in technology,
4. There is no return on investment in security,
5. Cybersecurity is a one-time project,
6. The myth of documentation.

2. THREATS TO INFORMATION SECURITY

Different authors define threats to information and cyber security differently. For example, Košutić (2012:12) classifies threats as natural disasters, external malicious attacks, internal attacks, malfunctions, and unintentional human errors. They are classified by Hadjina (2009:11), who claims that there are four general types of threats in terms of computer/information systems:

- natural threats,
- unintentional threats (accidents),
- intentional active human attacks i
- deliberate passive human attacks.

2.1. Difference between risk, threat, and vulnerability

Before looking at the catalog of the tethe at it is necessary to specify the difference between risk, threat, and vulnerability. Those three terms are defined in the ISO/IEC 27001:2005 and ISO/IEC 17799:2005 standards, and they are cited by Klaić (2010:2): "Risk is a combination of the probability of an event and its consequences." A threat is a potential cause of an unwanted incident that can harm a system or organization, and a vulnerability is a weakness of a resource or group of resources that can be exploited by a threat". Therefore, the risk is always present, and the threat is realized if it takes advantage of the weakness, that is, the vulnerability of a system, and it can cause damage and cause disastrous effects to the system (Kezerić 2017).

2.2. Mapping cyber threats

The research team that sought to map EU cyber security threats in the study Cyber Security in the EU and Beyond: Exploring Threats and Policy Responses, commissioned by the European Parliament, states that there is no standard or universally accepted definition of cyber security, but that threats can be reflected actors, tools and types of threats and potential targets. Threat actors can be states, profit-motivated criminals, hacktivists, and extremists. As threat tools, they cite malware and its variants, such as banking (trojan), ransomware, point-of-sale malware, botnets, and exploits (Kezerić 2017).

2.3. Categories of malicious attacks

Vuković (2012:17) divides malicious cyber activities into:

- cybercrime,
- cyber espionage,
- cyber terrorism and
- cyber warfare.

This division can be added in recent times, especially in the widespread form of hybrid war. Considering the goal, attacks can be aimed at data or surveillance systems (Vuković, 2012:17). When an attack is aimed at data, its goal is to steal or destroy data using various tools (eg, DDoS attack) and thus sabotage an individual, company or institution, i.e. their information assets. Another type of attack is aimed at surveillance systems, whose goal is to penetrate facilities that are designated as critical infrastructure and that are necessary for the normal functioning of society and life. The boundaries between individual forms of malicious activity are sometimes very thin and intertwined. In his work, Vuković (2012:18) cites a good example of Lech J. Janczewski and Andrew M. Kolarik, who compare cyber attacks to breaking into a hospital database. According to them, if someone breaks into that database and prescribes medicine to a patient who is allergic to it, he will die. It is about cyber murder, that is, a criminal act committed using computer technology, which can be interpreted as a form of cybercrime. If, after such an act, the same attacker announces to the public that this is just the beginning and that in achieving his goals he is ready to commit more such and similar (mis)deeds, (Kezerić 2017) then it is cyber terrorism. At the same time, the cyber-terrorist will very likely try to blackmail e.g. the government of a country, stating the conditions under which they will stop their criminal activities. If the cybercriminal/terrorist is an agent of the opposing structures, then it is cyber warfare.

DDoS (distributed denial of service) is an attack that tries to overload a computer network so that thousands of computers try to connect to the same network at once, to make it difficult or impossible to access a certain computer network and/or page. Cybercrime, as I have already stated, is a type of crime carried out using computer technology. This type of crime "includes fraud in the field of Internet banking and Internet fraud with credit cards, and it is estimated that with an annual growth rate of about 40% and with current earnings of about 100 billion dollars, it is the fastest growing sector of global organized crime" (Vuković, 2012:20). In the future, cybercrime will grow even more, as well as other forms of cyber (mis)deeds due to their obvious advantages. Primarily, in carrying an attack, taking down the website of NATO or some media houses, or activating a bomb with one click, you can be in a completely different part of the world, thousands of kilometers away from your target. Also, it is very likely that an ignorant and computer illiterate individual will not do such a thing and that, of course, he will not carry out the attack from his IP address and risk having armed special forces break into his apartment, but will, thanks to his knowledge and skills, make sure that he doesn't get in the way. They probably won't learn those skills in college, but unfortunately or fortunately, Google knows everything these days. Thanks to the information that the Internet (especially the dark web) abounds in, it is more likely that they will acquire the necessary knowledge on various interactive forums and Internet guides, of which there is no shortage (Kezerić 2017). In addition to cybercrime, there are also cyberespionage, cyberterrorism, cyberwar, hybrid war, etc.

2.4. Review of some cyber incidents in Montenegro and the world

Cybercrime costs global companies around six trillion dollars a year. The largest part of the attacks refers to the world of industry, where about 21.5% of companies were affected (Passeri, 2017). In second place is the world of finance with around 15.10%. What IT experts warn about is that users of social networks are increasingly at risk. The galloping global digital transformation had strong repercussions on the proliferation of cybercrime on a planetary level, the article entitled "Cybercrime knows no borders" (see the site www.rtnk.me/me/dru% C5%A 1tvo/43846/cyber-security-ne-knocyberndaries). This is best illustrated by the assessment of leading economic experts that due to the expansion of information technology and the exponential growth of digital solutions, cyber-attacks have cyber-attacks the global economy of over six trillion dollars, which is twice as much as compared to 2015, with expectations that it will exceed the amount of 10.5 trillion US dollars by 2025. These were some of the data cited by the European Commission in the new Cybersecurity Strategy, which characterizes cybercrime as "the largest transfer of economic wealth in history that exceeds the scale of transnational drug trafficking."

In the last few years, Montenegro has faced an increase in cyber-attacks and crimes in the field of high-tech crime. Criminal offenses related to identity theft, computer fraud, account theft, ransomware, and violation of intellectual property rights are a threat, and criminal offenses of child pornography

are increasingly present, i.e. dissemination of content about sexual abuse of children. This is written in the Risk Assessment of Serious and Organized Crime (SOCTA 2022) - a document prepared by an interdepartmental team including representatives of the security sector and the prosecution, the Government of Montenegro - Bureau for Operational Coordination (2021), "Assessment of the Risk of Serious and Organized Crime in Montenegro", (see website www.gov.me).

The authorities conclude that there is a widespread use of online platforms, primarily social networks, to spread hate speech and threats, cause panic, and spread false news and misinformation: "Both individually or in smaller groups, as well as in a very organized manner." Last year, the Montenegrin police handled 672 cases in the field of high-tech crime.

Of that number, 21 attacks on websites, 75 frauds via the Internet, 86 misuse of profiles on social networks, nine inappropriate content, and 430 malware were reported to them. In the same period, 51 cases of harassment, blackmail, and identity theft were reported to them.

"The most common forms of crime are related to abuse of profiles on social networks in the form of threats, false identity, and the like, where the attacker takes control of the victim's user profiles on social networks and leaves inappropriate content in the name of the owner, all with the aim of compromise the owner of the profile," it says. document.

Officials add that among the most common forms of cybercrime are the publication of inappropriate content on the Internet, including material related to minors, and the spread of malware, including malicious blackmail programs, i.e. ransomware, the article "SOCTA 2022: Cybercrime is growing, the sharing of videos of sexual abuse of children is increasingly present (see the website www.vijesti.me/vijesti/crna-hronika/603933/socta-2022-is growing-cyber-security-all-more- sharing-videos-of-sexual-abuse-of-children). Cybercrime is growing and its presence is increasing. This means that viruses encrypt data on the infected computer and the attacker asks the victim to pay a certain amount of money to a certain account, to get the key for the encrypted data.

Among the most common attacks are DDoS attacks on the information systems of state bodies and legal entities, on the websites and portals of the Government, the websites of media companies and political parties, as well as fraudulent electronic mail and financial fraud.

2.4.1. Previous activities in the cyberspace of Montenegro

According to the data of the Digital Forensic Center (DFC) from Podgorica, the most common hacker attacks in Montenegro took place in 2017 at the time of Montenegro's accession to the NATO alliance and on the day of the parliamentary elections in 2016. During three months of 2017, government services were compromised and state institutions as well as some pro-government media. "At the time, the Montenegrin Ministry of Defense reported that it was the target of a "phishing attack", through emails that came from the EU and NATO with attachments, and which allowed hackers to install Gamefish malware on the computers of the Ministry of Defense," the DFC states. clarifying that these are methods used by the APT28 group (Advanced Persistent Threat 28, known as Fancy Bear). A gamefish is a trojan (virus) that offers a hacker broad access to a target computer, including data exfiltration, log access, and other surveillance capabilities. US intelligence has further indicated that the APT28 group is linked to the Russian military intelligence service GRU. On the day of the parliamentary elections on October 16, 2016, Montenegro faced frequent DDoS attacks, which targeted websites of state institutions, pro-NATO and pro-EU political parties, civil society websites, and election observers. Through these efforts, news websites and some political parties were taken down. After a series of attacks in early 2017, Montenegro sought the help of NATO and Great Britain, which helped to successfully repulse two attacks at the end of the same year. Due to these events, at the beginning of October 2019, members of the American Cyber Command arrived in Podgorica, of investigating signs of Russian penetration into the networks of the Montenegrin government, and also to create an insight into the opponent's cyber threats to meet the upcoming American and Montenegrin elections in 2020. year, the article entitled "FBI and ANSSI cyber experts completed the mission in Montenegro, forensic results are expected" see the website (https://dnevno.me/Dru%C5%A1tvo/-/fbi-i-anssi-sajber-strucnjaci- completed-mission-in-Montenegro-expected-forensics-results-22-09-2022-07-32-15). Based on the already mentioned data, we can conclude that the consequences of cybercrime, which does not bypass Montenegro, are severe and far-reaching, both in financial and political terms. It is official data that in the previous five-year period, more than 2,600 cyber attacks were recorded in Montenegro.

Table 1.
The number of different forms of cybercrime by year

Year	Attack on websites and IS	Internet scams	Abuse of profiles on social networks	Inappropriate content on the Internet	Malware	Others (harassment, blackmail, identity theft...)	In total
2011	1	-	-	-	-	-	1
2012	3	2	-	1		-	6
2013	5	3	10	-	1	3	22
2014	5	6	20	5		6	42
2015	6	17	37	19	17	36	132
2016	18	20	36	14	50	25	163
2017	91	18	34	9	368	12	532
2018	13	68	50	6	363	37	537
2019	19	70	79	11	387	38	604
2020	25	84	90	15	383	44	641
2021	21	75	86	9	430	51	672

3. CRITICAL INFRASTRUCTURE

Hacking websites, stealing data from bank cards, intrusions into computers and e-mails, viruses, worms... In the world we live in, these have all become common terms that people more or less encounter daily basis, but they are generally no longer surprised- because they are aware that sooner or later they can become a victim of such an attack. However, the thought of the possibility of the breakdown of the power system, the hacking of airplanes and pacemakers, or the complete interruption of communications, is not so present in the mainstream and public discourse. Such things still seem to most people to be reserved for movies or science fiction, while security experts and governments of most countries are seriously concerned about the real possibility of such scenarios. Blunden (2010:11, Kovačević, 2014:97) rightly describes the consequences of (cyber) attacks on critical infrastructure, that is, SCADA systems on which a large number of plants that are part of that infrastructure rest, as a cyber Katrina, stating that "a successful cyber - the attack on the networks that manage the vital infrastructure turned the whole of America into one big Saint Louis after Hurricane Katrina". Montenegro could feel only a small part of such a situation when in the middle of 2022, the Government's website crashed and e-mail communication was interrupted. "As a consequence of that event, there were significant negative effects such as the complete unavailability of all government services, the communication services of the PIO Fund, the Health Insurance Fund, the Employment Office, the Tax and Customs Administration, and most other services that rely on telecommunication connection". It was a case of classic system hacking, and this example pointed out the weaknesses of the critical (information) infrastructure and the need for better protection.

Montenegro adopted the Law on Designation and Protection of Critical Infrastructure in December 2019. As national critical infrastructure, the mentioned Law recognizes "systems, networks, facilities, i.e. their parts located on the territory of Montenegro, the interruption of their functioning, i.e. the interruption of the supply of goods or services via those systems, networks, facilities, i.e. their parts can have serious consequences for national security, health, and life of people, property, environment, citizens' safety, economic stability, i.e. performance of activities of public interest (Kezerić 2017). The regulation that should have been passed 12 months after the law came into force has still not been passed, it should prescribe sectoral criteria for determining critical infrastructure in the fields of energy, transport, water supply, health, finance, electronic communications, and information and communication technologies, protection environment and the functioning of state bodies and other binding norms of behavior in critical situations and the aspect of protection thereof.

3.1. Critical information infrastructure

Information infrastructure can be defined as "a combination of computer and communication systems that serve as the basic infrastructure of public bodies, industry, and economy. Critical infrastructures such as the transportation and distribution of electricity necessarily depend on telecommunications,

public telephone networks, the Internet, terrestrial and satellite wireless networks, and related computer resources for information management, communication, and control" (Brnetić et al., 2013:6). It is precisely this interdependence that makes systems, that is, infrastructure, the most critical and the most vulnerable. The two most connected systems in this sense are the electricity system, on which all other infrastructures depend, and yet it depends on the communication system and vice versa. Thus, "an outage of a hydropower plant or thermal power plant will not only hurt the energy sector, but also on the information, telecommunications, economic, financial and a whole range of service activities, but the reverse is also true" (Matika, 2009:51). Perhaps the biggest problem facing the critical infrastructure system today is asymmetric threats, which include cyber threats, and which, as stated by Klaić and Perešin (2012: 337), are very difficult to predict analytically and predict, which is why it is difficult to develop mechanisms their protection. In Montenegro, the sectoral criteria in the field of electronic communications and ICT are - infrastructure damage that causes the inability to function of the ICT system that supports key functions in Montenegro, and which relates to ensuring the operation of one of the key infrastructure sectors, the national security system, the energy system, health system and finances that lead to a drop in support lasting more than six hours. The infrastructure that can be determined as critical includes: infrastructure whose serious malfunction or interruption of operation can result in the inactivity of electronic communication networks and services for a duration of at least four hours, and which supports the work of at least one sector of critical infrastructure or national security system; infrastructure whose serious malfunction or interruption may result in non-functioning of public sector electronic services for at least six hours; infrastructure whose serious malfunction or interruption may result in non-functioning of electronic communication networks and services for at least 24 hours, in the territory where more than 15,000 inhabitants are inhabited.

3.1.1. Costs of attacks on critical information infrastructure

Cyber incidents affecting critical information infrastructure are now considered global risks that can have a significant negative impact on many cities and industries in the next 10 years" (Tofan et al., 2016:4). According to the report by Tofan et al (2016:4), attacks on critical information infrastructure mostly affect the financial, ICT and energy sectors. In the report on the costs of attacks on critical information infrastructure, the authors combined a total of 17 studies, six of which refer to the EU area, and 11 to the area outside the EU. The methods used by the authors of certain studies to extract data were surveyed/ questionnaires, analysis of logs related to cyber attacks investigated by specialized security companies, and publicly published data in the media and open sources. The most common types of attacks on critical sectors are DDoS attacks and malicious programs [Kezerić]. In terms of national loss due to attacks on information infrastructure, it reaches up to 1.6% of GDP in certain European countries. Other studies mention losses from 425 thousand to 20 million euros per company per year. One study estimates that the average cost of cyber losses per company varied between 2.3 and 15 million euros in 2015, while another study estimates the economic loss to the global economy to be between 330 and 506 billion euros. The countries whose economies suffer the greatest damage due to attacks on information systems are the USA, Germany, Japan, Great Britain, Australia, and Russia. Tofan et al. (2016:5) conclude that countries tolerate malicious activity as long as it remains at an acceptable level, less than 2% of national income, and the urgency to prepare and invest in responding to a security incident usually arises only after an event with a significant impact. Also, companies lack qualified employees, and the problem is that the vast majority of organizations still do not have basic security controls implemented. At the same time, attackers are adapting and upgrading their techniques, making them even more effective, while companies struggle with old tactics.

3.1.2. The issue of protection of information communication (critical) infrastructure in Montenegro

Very little has been written about the history of critical information infrastructure in Montenegro. However, we can say from certain sources that in Montenegro, the information infrastructure was divided into civil and military components. After the 90s, such a division was abandoned, the information infrastructure was unified, and the Ministry of Information Society and Telecommunications was responsible for the complete communication network. Since the communication of state administration bodies also went through the same communication network, when public communications were privatized, security was put on the back burner.

In this sense, unprotected critical infrastructure would have a strong impact on weakening state security, and thus the economic and social well-being of the nation. Critical information infrastructure is information infrastructure that initiates multiple elements of critical infrastructure. As information systems

are largely interconnected or connected to public systems, critical information infrastructure nowadays becomes increasingly exposed, not only to failures and breakdowns- but also to various types of deliberate attacks. The basic problem from which the necessity of recognizing critical infrastructure arises is the fact that an attack on a certain critical infrastructure in itself multiplies even greater damage because a relatively small attack on one infrastructure object can have a huge impact and cause damage to a whole series of interconnected infrastructure objects.

In the information of the Government of Montenegro, it was assessed that the operational part of cyber capacity in Montenegro is not sufficiently developed to be able to guarantee adequate protection of citizens, institutions, economic entities, and business activities of investors from cyber-attacks, fraud on the Internet, cybercrime and other threats that come from cyberspace. The National Center for the Response to Computer Security Incidents in the Cyberspace of Montenegro - CIRT, at the moment, cannot provide any response to cyber-attacks because hackers have blocked them. So much for defense against cyber attacks, and if we can't blame only CIRT for this state of affairs. In the Government announcements, which contain recommendations containing preventive measures, so that citizens do not become victims of fraud and cyber attacks, the phone number to which cyber attack -should be reported is highlighted because "the site for reporting incidents is currently unavailable (www.cirt.me)". And it is unavailable because it is under cyber attacks. And CIRT's FB profile was last updated in June 2021.

It is also a fact that we were aware of the situation and our strength in cyberspace and thus at the same time the protection of critical infrastructure in the field of ICT.

One year ago, on September 12, 2021, the Government of Montenegro determined that the strengthening of national capacities for cyber security was necessary, and the difficult conditions in which the National Computer and Computer Incident Response Team (CIRT) works were recognized as a major risk. CIRT moved from the Ministry of Public Administration, Digital Society, and Media to the Directorate for the Protection of Secret Data in November last year. In the information that was discussed at one of the Government sessions at the time, it is pointed out that the Administration for Cadastre and State Property temporarily provided premises that do not meet the requirements for the work of that body ... and especially not from the aspect of the security operations center, the processing of sensitive data, and data marked with a degree of secrecy that require the provision of a specialized room for forensics and analytics with access control and monitoring. Given that the premises in which the CIRT is located do not comply with the standards, it is not possible to use the infrastructure and systems that are under special supervision and control," the explanation states, adding that this led to a situation where the functioning of this body extremely difficult, which "represents a great risk, bearing in mind the increase in threats in cyberspace".

The document states that three types of challenges facing CIRT have been identified, and they concern not only spatial- but also technical and personnel capacities.

As for technical capacities, the document mentions that- bearing in mind budget constraints, talks with the British and American embassies have been renewed to provide technical support. Both embassies also offered help through professional training. In the information, it is added that at the operational level, access to the infrastructure of the Ministry of Internal Affairs is provided for the performance of regular activities.

It is also emphasized that, although in the age of digital expansion, information technologies are positioned as a driving force for economic development, the scope for misuse of technologies is also increasing, and cyber security is seen as an inseparable and important part of the security of any organization and state.

The draft Cyber Security Strategy of Montenegro from 2022 to 2026 envisages the establishment of a new administrative body - the Agency for Cyber Security. The plan is to establish a new and sustainable body for cyber security at the national level, within which a team for responding to computer security incidents in the cyberspace of Montenegro would function. But it was not specified what the Agency's competencies would be, whether CIRT would be transformed into an Agency, whether the Agency would be independent of CIRT, the way the Agency would be financed, etc.

Therefore, new challenges require the updating of existing cyber defense mechanisms, but also the implementation of innovative responses, especially in terms of crisis management, raising the level of digital literacy and education about the importance of cyber security issues, and the protection of privacy and personal data".

The project, launched by the Ministry of Foreign Affairs of France, through the French presidency of the European Council, in partnership with the Government of Slovenia, aims to be a center for the development of cyber security capacities in the Western Balkans region. "The Western Balkan Cyber Capacity Campus (WB3C) is designed to cover two domains - the fight against cybercrime with a focus

on educating members of the security sector and holders of judicial functions for conducting investigations and prosecuting cybercrime crimes and strengthening the regional cyber defense system, from cyber hygiene to prevention and risk management, the study entitled "eGA strengthens cyber resilience of the Western Balkans" see the website (https://ega.ee/news/ega-strengthens-cyber-resilience-western-balkans). The decision to make the Regional Science and Technology Park the location of WB3C represents an unequivocal recognition of Montenegro as a credible partner by European partners on the way to accomplishing this important task of essential importance for the region".

The educational programs of the Center are implemented in cooperation with European cyber security experts, with the support of the "Balkan institute of science and innovation of the Université Côte d'Azur" (BISI), with which Montenegro, i.e. The University of Montenegro has concluded a Memorandum of Cooperation.

There is no going back to addressing virtual security and it can no longer be treated in isolation from security in the real world. This was confirmed back in 2016- when at the Warsaw Summit, cyberspace was declared as the fourth operational domain, which created the conditions for the activation of Article 5 of the NATO Founding Treaty, which allows effective defense on an equal footing with air operations, when confronting 'aggressive behavior in cyberspace on land and sea. Therefore, it is evident that the time has passed when peace and war were two differentiated concepts- because on the cyber front we face hybrid threats of destabilization such as cyber warfare and disinformation that require a wide range of defensive means.

The tension of the drama is further fueled by the fact that cybercrime is becoming more and more intrusive and sophisticated throughout the world, which logically affects the countries with the highest degree of dependence on information technologies. This trend will continue to grow in the future because it is expected that by 2025 there will be 25 billion devices connected to the Internet on a global level, which already at this moment exceeds the total number of inhabitants on the planet.

3.1.3. Spending on the protection of critical infrastructure in the world

Critical infrastructure is undergoing an unprecedented radical transformation, initiated by the rapid adoption of smart operational technologies. Cybersecurity is a growing part of that evolution. ABI Research, a consulting company that provides strategic guidance on the most impactful transformative technologies, predicts that by 2023, $125 billion will be spent on critical infrastructure protection globally, A&S Adria, "Critical Infrastructure Protection Spending $125 Billion" by 2023, (see website www.asadria.com), 2018-;. Among the biggest investors in security are manufacturers of defense systems (Lockheed Martin, BAE Systems, Harris,), industrial OEMs (Honeywell, Siemens, Airbus, Rockwell,), technology giants (IBM, Amazon, Microsoft, Verizon), and energy companies (Shell, Total,).

Three main factors initiate better digital security;

1. in sectors such as communal services, transport, and health care,
2. digital transformation and increased connectivity of operational technologies, then
3. the democratization of cyber attacks on AI and the maturing of the market for industrial and IoT security.

Connected operational technologies have enabled the optimization and greater efficiency of decades-old systems- cost reduction and significant improvement of operator operations. But on the other hand, new vulnerabilities and threats have appeared to technologies that were previously physically separated from vulnerable networks. The first specialized attacks on industrial control systems occurred more than ten years ago, and today the tools and methods of attack are available to even the most common cybercriminals. Fortunately, the cybersecurity industry is working in tandem to bridge the gap between IT and OT. As a result, security solutions for industrial control systems and the Internet of Things are rapidly maturing and becoming more available and affordable. So, even if security personnel in critical infrastructures are faced with an increasing number of threats, they also have more choice and support in terms of digital protection of their operational and information systems. Budgets for security systems are significantly higher, which is encouraging news for those sectors that have long lagged in digital security.

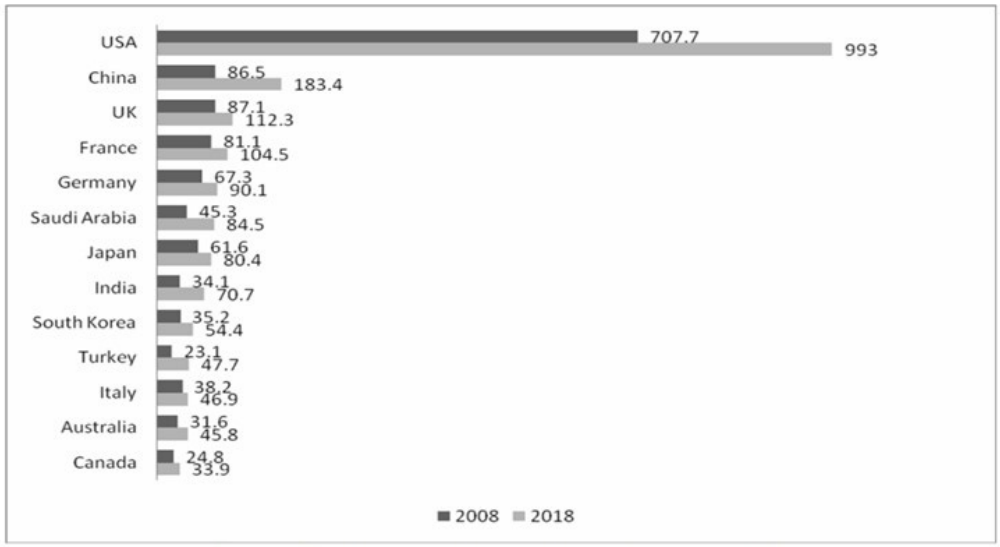
However, these positive developments face several obstacles affecting key infrastructures:

- the slowdown produced by governments about national cyber security strategies, especially in the US and the EU,
- by the continuation of resistance to the regulation of cyber security and information sharing within the sector, as well as

- by ignoring cyber security threats within the private sector, leading to his apathy towards the issue.

Many view cybersecurity as a one-time investment rather than an ongoing investment. So, even if current investments for protection are significantly higher than just a few years ago, there is still room for further investment.

Figure 1.



Slika 1 – *Potrošnja na zaštitu kritične infrastrukture ($Mr)*

As far as Montenegro is concerned, the investments are very modest, but what has been done so far inspires moderate optimism, especially if we consider the good institutional roundness and to some extent normative. Institutional capacity for critical infrastructure has been strengthened and "institutionalized" with the formation of a new sector for the coordination and protection of critical infrastructure in the Ministry of Interior. The Law on Critical Infrastructure was adopted, which prescribes the criteria for defining critical infrastructure, a disaster risk assessment study was done with a clear operational plan and clear institutional responsibilities, the Cyber Security Strategy of Montenegro from 2022 to 2026 was adopted, etc.

Also, after signing an arrangement with the EU in November 2019 for the implementation of the Joint Action Plan for the fight against terrorism in the Western Balkans, Montenegro continued to implement the planned measures and submitted its second and third reports in January and August 2021. years.

4. CONCLUSION

Based on what has been said, we can conclude that the consequences of cybercrime, which does not bypass Montenegro, are severe and far-reaching. Based on experience, we see that global cyber threats are very present in Montenegro. The statistics of the biggest global cyber threats do not differ to a great extent about Montenegrin cyberspace. Bearing in mind the results of this work, it is clear that in the future it is necessary to pay more attention to this topic, Government of Montenegro - Ministry of Information Society and Telecommunications "Analysis of threats in the cyberspace of Montenegro", 2014 (see website www.gov.me).

In the following, I will list some of the activities that must be implemented to increase the level of cyber security as well as the need for stronger protection of critical infrastructure in the ICT sector;

- Web portals of state institutions and companies from the private sector are a frequent target of hacktivists, so it is necessary to pay more attention to the proper creation of web pages and protection against possible attacks,
- One of the biggest global threats is spam, which is why it is necessary to implement antispam solutions,

- Configure the mail server to block attachments that are most often used to spread viruses,
- Tools for monitoring, updating software, removing vulnerabilities, protecting against DDoS and targeted attacks, as well as protecting mobile devices used for business purposes (see the website www.gov.me),
- Force a complex password policy,
- Create and maintain regular backups of critical systems (see website www.gov.me)
- The development and implementation of safety regulations is another key part of overall safety,
- Educate employees about the basics of cyber security and the critical infrastructure sector,
- Strengthen institutional cooperation and training regarding cyber threats and protection of critical infrastructure, etc.

When comparing the current situation regarding cyber security in Montenegro and the protection of critical infrastructure with the practice of EU countries, it is evident that there is a gap that needs to be overcome. Montenegrin society is still in the process of transition, therefore all public and private organizations are making a significant effort to quickly meet EU standards in terms of raising awareness among the population about risks and the consequences of those risks, Tempus project under the auspices of the European Commission: 544088-TEMPUS-1 -2013-1-SI-TEMPUS-JPHES, Outcomes of the project task "Comparison of practice in Montenegro with European Union standards" (see website https://ecesm.net/sites/default/files/DEV_1.3_ME.pdf).

5. LITERATURE

Mujevic, Mersad., & Korac, Safet (2020). Development of the concept of critical infrastructure protection in Montenegro - roads, experiences, roles, and responsibilities. Knowledge International Journal, 41(4), 711 - 718;
Ana-Maria, Kezerić, "Analysis of threats and risks to the cyber security of the Republic of Croatia: vulnerability of the information infrastructure", graduate thesis, University of Zagreb, 2017;
Hadjin (2009) Protection and security of information systems (teaching materials with a collection of tasks). Zagreb: Faculty of Electrical Engineering and Computing;
Brnetić, Damir, et al (2013) Criminal law-forensic protection of critical national infrastructure from IT (cyber) threats. In: Antoliš, Krunoslav (ed) New security threats and critical national infrastructure (pp. 34-45). Zagreb: Ministry of the Interior, Police Academy;
Nađ, Ivan and Adelsberger, Zdenko (2016) Information security in the context of crisis management. In: Nađ, Ivan (ed.) Days of crisis management (116-126). Velika Gorica: University of Velika Gorica;
Juran, Ana (2014) Security of information systems. Graduate work. Rijeka: Maritime Faculty in Rijeka;
Singer, Peter Warren, and Friedman, Allan (2014) Cybersecurity and Cyberwar: what everyone needs to know. New York: Oxford University Press;
Vuković, Hrvoje (2012) Cyber security and the system of combating cyber threats in the Republic of Croatia. Final specialist thesis. Zagreb: Faculty of Political Sciences;
Košutić, Dejan (2012) 9 Steps to Cybersecurity: The Manager's Information Security Strategy Manual. Zagreb: EPPS Services Ltd;
Klaić, Aleksandar (2010) Overview of the state and trends in contemporary information security policy and information security management methods. Doctoral qualification exam. Zagreb: Faculty of Electrical Engineering and Computing;
Kovačević, Božo (2014) Cyberwar – American pretext for a new cold war? Polemos: journal for interdisciplinary studies of war and peace 16(32): 91-110;
Matika, Dario (2009) Energy security, and critical infrastructure - an overview of research results. In: Matika, Dario, and Poljanec-Borić, Saša (eds) Critical infrastructure in Croatia: Towards a new system of security and protection (45-59). Zagreb: Institute for Research and Development of Defense Systems of the Ministry of Defense, Institute of Social Sciences Ivo Pilar;
Tofan, Dan; Nikolakopoulos, Theodoros; Darra, Eleni (2016) The cost of incidents affecting CIIs. Ennis.

Legal acts and norms

Cyber Security Strategy of Montenegro 2022-2026;
Law on Information Security ("Official Gazette of Montenegro", no. 14/10, 40/16, 74/20, 67/21);
Law on Designation and Protection of Critical Infrastructure ("Official Gazette of Montenegro", No. 72/2019);
Defense Strategy of Montenegro;
Disaster Risk Reduction Strategy 2018-2023;
Digital Transformation Strategy of Montenegro 2022-2026;
Disaster recovery implementation strategy (strategy for securing data in the event of a disaster for the needs of state and administrative bodies in Montenegro);
The strategy of using Open source technology;
Program for the development of information and communication technologies of the judiciary 2021-2023.

Other Internet sources

https://ccdcoe.org/cyber-security-strategy-documents. HTML
https://cert.europa.eu / static/SecurityAdvisories/2017/CERT-EU-SA2017-012.pdf
https://securelist.com /files/ 2016/11/ KL_Q3_Malware_Report_ENG.pdf
HTTPS:// securityevaluator HTTPS /hospitalhack /
www.iso27001 security.com /ISO27k_ISMS_Mandatory_documentation_checklist_release_1.docx
HTTPSHTTPSdvisera.com/27001 academy/knowledgebase/iso-27001-gap-analysis-vs-risk-assessment
www.nato.int/cps/en/natohq/official_texts_133169.htm
https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade
www.cirt.me
www.isme.me
www.yumpu.com/xx/document/view/38655723/1-pojam-information-sistema-itrevizijaba
www.zastita.info/hr/casopis/clanak/granice-kibernetícke-bojisnice-nije-lako-repoznati,22946.html
www.slobodnaevropa.org/a/crna-gora-vlada-istraga-sajber-napadi/32002798.html
https://avaz.ba/globus/region/781786/dfc-razotkrio-opasne-aktivnosti-ruske-tajne-sluzbe
www.antenam.net/politika/263510-dfc-crna-gora-u-mrezi-aktivnosti-gru
www.slobodnabosna.ba/vijest/273215/uzbuna_u_crnoj_gori_dfc_razotkrio_opasne_aktivnosti_ruske_tajne_sluzbe.html
www.scribd.com/document/580304186/strategija-sajber-bezbednosti-crne-gore-2022-2026-spredlogom-akcionog-plana-za-period-2022-2023-1
https://pubdocs.worldbank.org/en/384771604613506147/3-Energetski-sektor.pdf
https://docplayer.rs/211233602-Analiza-prietnji-i-rizika-cyber-sigurnosti-republike-hrvatske vulnerability of information - infrastructure.html
https://ne-np.facebook.com/102994798278482/posts/hakeri-blokirili-i-crnogorski-nacionalni-centar-zaodgovar-na-sajber-incidente/585724080005549
www.baltictimes.com/ega_strengthens_cyber_resilience_of_the_western_balkans_countries
www.scribd.com/document/486514599/15-94-18-12-2014-pdf

Borisov, B. (2022). Planning through a cloud-based software platform, *SCIENCE International journal, 1*(1), 13-20. doi: 10.35120/sciencej010113b
UDK: sss

PLANNING THROUGH A CLOUD-BASED SOFTWARE PLATFORM

Borislav Borisov[1*]

[1]University of National and World Economy, Bulgaria, e-mail: b.borisov@unwe.bg

Abstract: The purpose of the research is to identify the main challenges to the development of planning science, to emphasize how the development of information and communication technologies can help planners to develop quality planning documents, to review existing planning software applications and to present the possibilities of the Bulgarian prototype of a cloud-based platform for planning and budgeting - CPPB. The methods of comparative analysis and visualization were used. The article discusses the advantages and disadvantages of popular autonomous and cloud-based software solutions and argues that planning software should enable the development of strategic and business plans as an integrated and interrelated process. It also defines the benefits of introducing specialized cloud-based planning software for businesses, public administrations, credit institutions and the society as a whole.

Keywords: *strategic planning, business planning, planning software.*

1. INTRODUCTION

Planning science is constantly evolving, offering new concepts, models and solutions that are approbated and applied or rejected in practice, which selects the most feasible of them. As the economic environment becomes increasingly dynamic, planning strives to be adequate to these challenges and meet the requirements to achieve competitive advantages. Planning, in fact, has its critics. Some economists from economically developed countries doubt that planning can respond to rapid changes in a turbulent economic environment and some of their colleagues from the former socialist countries believe that the centrally planned economy is to blame for the economic backwardness of this group of countries compared to their economically developed counterparts. They all probably have their reasons to be disappointed with planning, but a deeper insight into the specific problems can suggest that the reason for them is not the essence of planning as a management tool but its application in different countries and by different governance bodies. For example, Zach Taylor from the University of Toronto, points out that scholars of planning have long grappled with the dilemma of how to explain variation among places' traditions, modes or styles of planning practice (Taylor, 2013) and introduces the concept of 'planning culture'. Newman and Thornley, in their 1996 book Urban Planning in Europe, also attempt to explain the differences in planning patterns across countries, identifying five European families of planning which they defines as British, Napoleonic, Germanic, Nordic and East European (Newman & Thornley, 1996), which differ as to whether control is directive or regulatory, whether authorities are centralized or decentralized, to what extent public-private partnership is conflictual or cooperative, and whether land use is integrated or separated.

Planning models can be classified in terms of various criteria. Scientific literature abounds with different classification schemes, which categorize planning as directive, adaptive, synoptic, incremental and situational planning, goal-based planning also known as Strategic Planning System (SPS), problem-oriented planning known as Strategic Issue Management System (SIMS), planning based on of principles, scenario planning, etc., but it seems that the most significant difference between the types of planning and the planning documents created is that some of them are strategic and aim to determine the long-term policy of an organization in order to provide it with competitive advantages while others are focused on its day-to-day activities that must ensure the achievement of its short-term and long-term goals. This is the difference between strategic planning, the outputs of which are concepts, strategies, strategic plans and programs, and operational planning, the outputs of which are business plans, work plans, road maps, scenarios, timelines, projects, etc.

[*]Corresponding author: b.borisov@unwe.bg

2. PLANNING METHODS AND SOFTWARE APPLICATIONS

Although the differences between strategic and operational planning are obvious, in many methodologies and scientific works in the field of planning they are mixed in an unacceptable way. Thirty years ago Camillus and Datta (Camllus & Datta, 1991) proposed a model, which considered the process of developing strategic and operational plans as a whole but with a clear distinction between the stages of strategic and operational planning. The model was entitled Integrated Planning Systems Framework (IPSF) and includes the following steps (stages):

- environmental analysis;
- defining goals and objectives;
- internal analysis (evaluating strengths and weaknesses);
- formulation and evaluation of alternative strategies;
- strategy selection;
- operational plans and implementation;
- performance evaluation and feedback.

In other words, one of the constant challenges for planning science has always been to specify what content to put into the understanding of the individual concepts related to planning science and what planning methodologies to propose as most appropriate. However, this is a rhetorical question, since the content of planning documents, methodologies and techniques is constantly modified and supplemented according to changes in the environment and circumstances.

Another important aspect of the requirement for planning effectiveness is the way planning documents are made. Long gone are the days when plans were developed for months and were valid for years - in the turbulent and dynamic environment such a “luxury” is impossible. Practice needs quick solutions to specific problems, which, however, must be consistent with the general policy and goals of the organization. The development of ICT provides an opportunity to support planning specialists. Planning has always been based on collecting and processing certain information, but now it is possible to handle a large amount of data and search for optimal solutions. It can be said that “information-based planning” is moving to “database planning”. It is a fact that data provides information, but the idea here is that planning solutions would be more adequate when based on the processing of large databases. This means that new planning systems must be built on the principle of Database management systems (DBMS).

Recently, Internet sites which provide strategic analyses and forecasts and solve planning tasks have become very popular. Such an application for developing business plans is the Business Plan Maker Professional (see the site http://www.individualsoftware.com/?product=business-planmaker-professional-12). LivePlan (https://www.liveplan.com) is another WEB-based application that provides over 500 sample business plans. BizPlanBuilder, on the other hand, contains plan templates for construction, service, manufacturing, non-governmental, and other organisations (http://www.toptenreviews.com/business/software/best-business-plan-software/bizplan-builder-review/) It has a “what-if” feature that allows you to experiment with different options for plan solutions, such as the final result tracking. There is a Cloud version and a Windows App version. Business Plan Pro is a business plan development program designed for budding entrepreneurs. The application comes with detailed instructions on what information is needed and why. (http://www.paloalto.com/business_plan_software/features/premier). Business Resource Software, Inc. offer online business plan development, marketing plans, sales plans, internet business plans, pricing strategies, etc. through Plan Write for Businesses cloud-based technology. Another program - Business in a Box - offers 1800 document templates for developing business plans for different types of business. There are versions for Windows XP, Vista, 7, 8 and 10, as well as Mac OS X 10.5 and later versions. The application is updated via the Internet. (http://www.paloalto.com/business_plan_software/features/premier).

A closer look at the electronic and software solutions intended to support the development of business plans shows that they all fall in in of the following categories:

- Sites with descriptions and methodological guidelines of the steps to be followed to develop plans;
- Business plan template sites with fillable forms with tables, forms and various applications;
- Video lessons on planning;
- Scheduling applications;
- Spreadsheet solutions for various planning tasks;
- Software applications for planning scenarios;
- WEB-based software solutions for strategic analyses and business plan development.

The available software products and web platforms for developing strategic and business plans

could be used in our country as well but there are some limitations that make them convenient for solving individual planning tasks rather than for developing complete strategic and business plans. Another limitation is that they do not allow for drawing up plans in different languages and, with few exceptions, are only in English (we found one application that has a Spanish language pack), which is why they are not fully applicable to Bulgarian conditions and requirements. Although some of them have what-if functions, there are no true optimization models. More importantly, most software products, while assisting professionals in applying any of the popular strategic analysis techniques such as SWOT, PEST and other similar methods, or in making forecasts and various calculations, do not have functions to bind the strategic decisions with the technical calculations of the business plans. Software applications would be more useful if they offered guidance on the most appropriate strategies to determine the strategic and operational objectives and sequentially solve interrelated planning tasks in order to reach the desired end result by means of optimization models.

Therefore, it is clear that there are some software products that assist planners in developing simple business plans but none that are suitable for developing comprehensive strategic plans. This is due mainly to the fact that, unlike business plans, which are generally reduced to solving tasks related to solving technical, personnel and financial operational issues and the expected performance, strategic plans are oriented towards development goals and are components of the company's policy based on its senior management expertise. Strategic planning is a creative activity that cannot be reduced to pushing buttons to get results. The challenge of creating such a product adapted to the Bulgarian conditions was answered by creating a prototype of a cloud-based platform for strategic planning. It was developed by a team led by the author under the project "Prototype of a cloud-based software application for planning and budgeting", in implementation of the Project Financing Agreement under the Tenth Session of the National Innovation Fund No. 10IF-02-21/28.11.2019 The prototype software application has the working title of Cloud Platform for Planning and Budgeting (CPPB).

3. PLANNING VIA A CLOUD-BASED PLATFORM

The pilot application Cloud Platform for Planning and Budgeting (CPPB) developed by a Bulgarian team of specialists largely meets the requirements for a dynamic relationship between strategic analysis, strategy development and goal setting and business planning. The idea of cloud-based software with a web interface is not to offer a software product that users will have to buy a license for but a service accessible at an affordable price.

Figure 1. CPPB's Start Screen

The application suggests development strategies based on the results of analyses:

Figure 2. Recommended Development Strategies screen

Next is the development of the so-called “objective tree” incorporating the vision, mission, strategic and operational objectives of the recommended strategies:

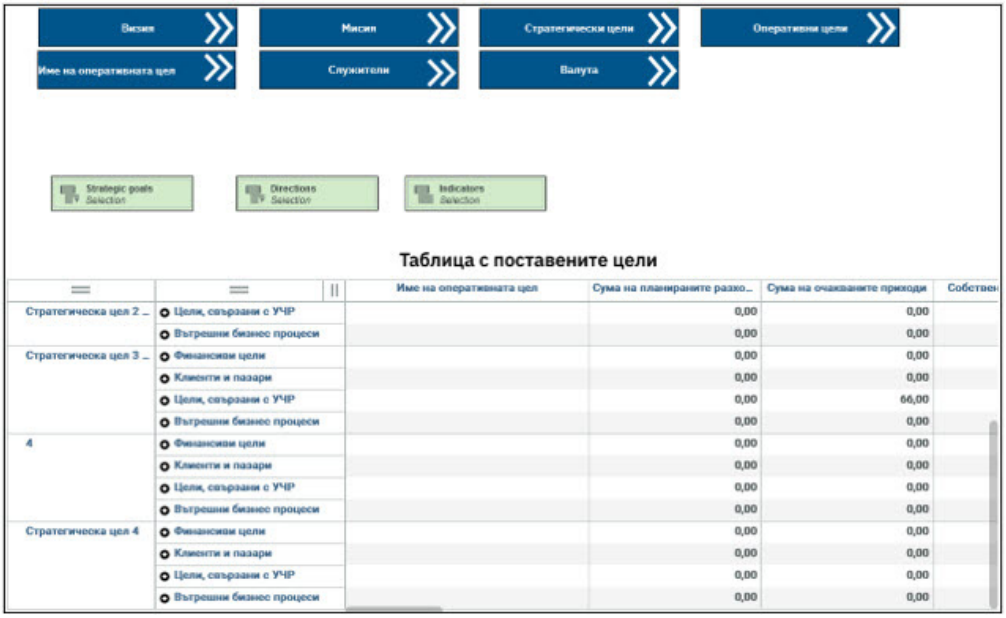


Figure 3.

The Business Planning module includes several sections related to the phases of the business planning process:

Figure 4. Business Planning Steps screen

Sales revenue is projected using several methods for greater reliability. On this basis, a production program and the necessary costs are determined.

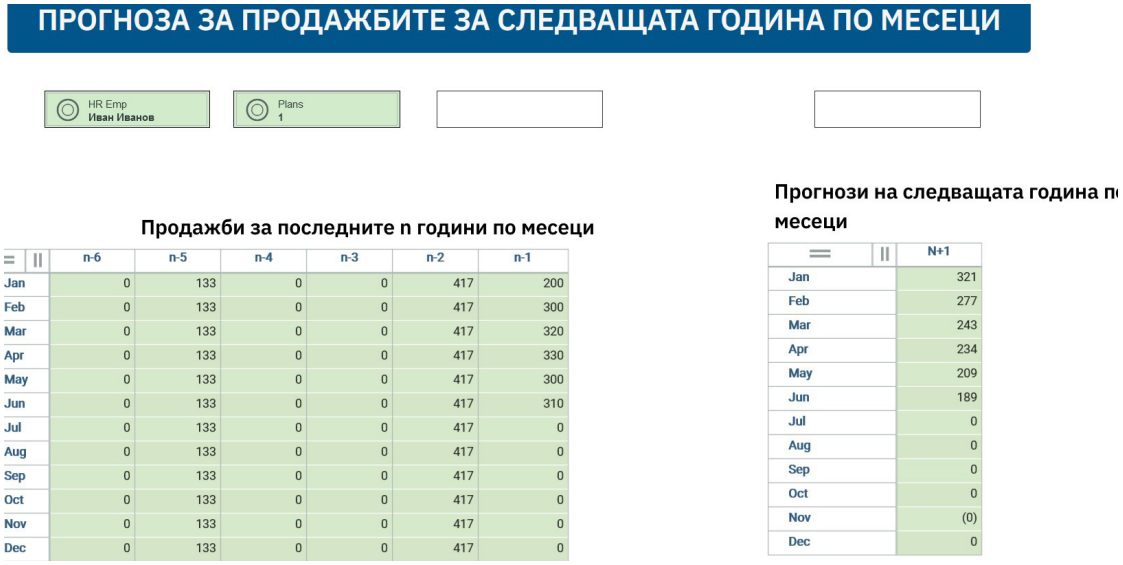


Figure 5. Sales Forecast screen

Figure 6. Production Costing screen

Обобщени стойности

	2020							
	Total Year	Q1	Jan	Feb	Mar	Q2	Q3	Q4
Брутна печалба	808 400,00	376 100,00	98 300,00	135 400,00	142 400,00	432 300,00	0,00	0,(
Лихви	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,(
ДДС	1650,00	1650,00	1650,00	0,00	0,00	0,00	0,00	0,(
Амортизация	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,(
Печалба/Загуба от продажба на акти...	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,(
Общо разходи	6550,00	6550,00	3350,00	1600,00	1600,00	0,00	0,00	0,(
Нетна печалба преди корп. данък	806750,00	374450,00	96650,00	135400,00	142400,00	432300,00	0,00	0,(
Корпоративен данък	9665,00	9665,00	9665,00	0,00	0,00	0,00	0,00	0,(
Нетна печалба след Корп. данък	797085,00	364785,00	86985,00	135400,00	142400,00	432300,00	0,00	0,(

Figure 7. Total Income and Expenses Table

The automated income and expenses calculation provides a projected accounting balance as well as a forecast of the net cash flows and the net present value of the investment, which is indicative for the overall economic effect of the investment.

Share

Прогнозен баланс

	2021									
	02	03	Q2	04	05	06	Q3	07	08	09
Активи	366566,11	410022,50	1421665,83	441895,55	473215,28	506555,00	1803423,33	534394,72	601034,45	667994,17
Краткотрайни активи	436899,44	515522,50	1949165,83	582562,22	649048,61	717555,00	2647423,33	780561,39	882367,78	984494,17
Парични средства	436899,44	515522,50	1949165,83	582562,22	649048,61	717555,00	2647423,33	780561,39	882367,78	984494,17
Краткосрочни вземания	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Текущи активи	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Материални запаси	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Дълготрайни активи	-70333,33	-105500,00	-527500,00	-140666,67	-175833,33	-211000,00	-844000,00	-246166,67	-281333,33	-316500,00
ДМА	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Амортизации с натрупване	-70333,33	-105500,00	-527500,00	-140666,67	-175833,33	-211000,00	-844000,00	-246166,67	-281333,33	-316500,00
Пасиви	173791,11	118927,78	298125,67	103214,44	98521,11	96390,11	325579,33	86728,11	121357,11	117494,11
Краткосрочни задължения	64289,86	69081,53	186221,92	64693,19	61559,86	59968,86	142155,58	54806,86	45785,86	41562,86
Задължения към доставч...	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Данъчни задължения (КПО)	-12166,81	-5538,47	-12433,75	-4280,14	-4106,81	-4046,81	-20380,42	-3546,81	-8396,81	-8436,81
Данъчни разлики (ДДС)	30566,67	32850,00	98166,67	31333,33	32166,67	34666,67	99500,00	33166,67	33166,67	33166,67
Задължения към финансо...	45890,00	41770,00	100489,00	37640,00	33500,00	29349,00	63036,00	25187,00	21016,00	16833,00
Дългосрочни пасиви	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Дългосрочни кредити	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Собствен капитал	109501,25	49846,25	111903,75	38521,25	36961,25	36421,25	183423,75	31921,25	75571,25	75931,25
Неразпределена печалба/...	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00

Figure 8. Projected Financial Position screen

4. CONCLUSIONS

The development of ICT affects all aspects of our life - from our individual workplaces and pastimes to the general culture and public education. Planning systems follow this trend as well. Today there is a plethora of software products to aid planners in developing quality strategies, plans and programs. In Bulgaria, there is already a prototype of such a product developed by Bulgarian specialists, which has some advantages that other known products do not possess. One of these advantages is that it is cloud-based and easily accessible. Another one is that it combines the development of strategic and business plans into one continuous process.

The specialized Bulgarian software application for automated business planning provides various benefits to:

1. Businesses - they will be able to independently, without the help of external experts, develop better, realistic and justified business plans;
2. Public sector organizations - the managing bodies of the operational programs can be sure that their business plans (which are an integral part of most project proposals) are justified in terms of finance, staff and resource allocation, and the expected effects are realistic;

3. Credit institutions – banks will be able to compare the results of business plans with their estimates with greater confidence and thus mitigate their credit risk exposure;

4. The general public or society – the application raises the public awareness of ICT advantages and is a step towards popularization of electronic services.

REFERENCES

Борисов, Б. и др. (2020). Нови парадигми в планирането. Колективна монография. Русе, 2020.

МРРБ. (2020). Методически указания за разработване и прилагане на плановете за интегрирано развитие на общините (ПИРО) за периода 2021-2027 г.

Newman, P., & Thornley, A. (1996). Urban Planning in Europe: International Competition, National Systems, and Planning Projects. Routledge Camllus & Datta, 1991

Taylor, Z. (2013). Rethinking Planning Culture: A New Institutionalist Approach. Town Planning Review, 2013, 84(6). Town Planning Review, 2013, 84(6).

Camllus, J. C., & Datta, D. K. (1991). Managing Strategic Issues in a Turbulent Environment. Long Range Planning 24, 67– 74.

Mirković. Dj. (2022). The impact of Instagram in the process of improving English vocabulary at "c" levels, *SCIENCE International journal, 1*(1), 21-26. doi: 10.35120/sciencej010121d
UDK: sss

THE IMPACT OF INSTAGRAM IN THE PROCESS OF IMPROVING ENGLISH VOCABULARY AT "C" LEVELS

Djukica Mirković[1*]

[1]Self-employed, The Republic of Serbia, e-mail: djukica2509@gmail.com

Abstract: The Internet revolution stems from a rapid development of Information Technology which considerably determines human`s lives. The necessity for new jobs appears, there is a demand for new life skills that might not have been developed in the past, people connect on global level, businesses are established and run in this virtual world, but the access to gaining knowledge is one of the Internet benefits as well. The result of this digital revolution is the creation of social media, initially invented for amusement. Little is known about how many benefits social networks can bring to the sense of learning foreign languages. The aim of this paper is to discover the impact of Instagram in improving English vocabulary at "C" levels on its users in 2022. Furthermore, it will also elaborate on the means used for improvement of, allegedly, the most demanding segment of English. The development of technology in 21st century and its discoveries revolutionised approach to education. While popularity of the Internet grew considerably, it commenced to predominantly affect society, in general. Nevertheless, at the same time, it offered such possibilities which enabled all the Internet population to do jobs or learn from their homes. Accordingly, this invention generated social media which has transcended traditional education in classrooms. The application that proved supremacy of this phenomenon is Instagram. The primary goal of this social network was entertainment; however, the fact that even students can learn English vocabulary, aimed at "C" levels in a spontaneous and natural way, transformed this application into the leading learning tool. As a result, it appears that the major purpose of social media nowadays, including Instagram, is educating. People tend to regard it as an extremely important discovery particularly in 2020 and 2021, when online learning was the only possible alternative to traditional classroom education due to COVID-19. In addition, even after the pandemic, students occupied this space for learning principally foreign languages, as classroom education was considered time-consuming. This paper will deal with the effects which Instagram has on advancing English vocabulary at "C" levels in 2022. Besides, it will also provide the examples of how posting on Instagram helps, explaining various options available for practising and mentioning skills that might be developed. The method used in the paper is quantitative and is associated with the previous research corresponding to the topic. Similarly, the corpus for this paper is based on the Instagram profile @english,exams.with.djukica. The questionnaire used in the research was created in the Instagram story on the aforementioned profile and it collected the votes from its followers. The insight into the results prove the theory that Instagram significantly influences enhancing English vocabulary at "C" levels. In the conclusion, the author recommends that offline English teachers should include social networks in their curriculum to complement the material in the form of extra resources. Not only will the social media be an exceptional asset to education, but it will connect students worldwide and encourage their communication in English.

Keywords: *English vocabulary, social media, Instagram, learning.*

1. INTRODUCTION - DIGITAL LITERACY IN 21st CENTURY

As David crystal states, the development of modern information technology occurs simultaneously with the development of globalisation. The Internet, as an exceptional innovation, plays an important role in all spheres of human lives in 21st century. It is known to serve as good source of any information. "Social networks are not only entertaining means of communication between people but also a powerful component of the information and educational environment that has considerable educational potential" (Aleksandrova et al., 2021; Tolmachev et al., 2021; Zenin et al., 2021). With respect to education, the approach to learning foreign languages has almost changed beyond recognition. In this domain, Instagram became increasingly powerful on global level, spanning entertainment and learning. As lingua franca, English is dominant among all foreign languages. "Emails, chatgroups, instant messages, and the Web have one thing in common: they are all electronic interactions where the subject-matter comprises – apart from the occasional aberration – real thing in the real world." (Crystal, 2012). Some scholars claim that Instagram provides its users with certain tools and options valuable for specific linguistic units such as vocabulary. "A wide range of vocabulary is the key to learning a foreign language successfully and confidently. The more vocabulary you know, the easier you will find it to understand the language, whether written or spoken." (Mirkovic, 2022).

*Corresponding author: djukica2509@gmail.com

2. MATERIALS AND METHODS

2.1. SOCIAL MEDIA

Social media is the matter of the utmost importance which gives new momentum to education. In spite of the fact that these applications such as Facebook, Instagram, YouTube and TikTok liken to each other in terms of learning, they are all different and suitable for various types of people and their objectives. "Recent investigations have pointed out that Facebook can have a positive effect on the student-to-student and student-to-teacher relationship" (Mazer et al, 2007). Furthermore, users acknowledge social networks as a resourceful capacity which enables them to advance language skills, including grammar, vocabulary and pronunciation as well. This appeared to be pivotal during the pandemic in 2020 and 2021, when Instagram became a life-altering tool for learning foreign languages. It is noticeable that interaction and learning are inextricable to the extent that this process reinforces the scientific theories which are based on the presumption that online learning has a tendency to suppress classroom learning. Taking into account the fact that the topic is wide, our focus in this paper will be on enhancing English vocabulary at "C" levels.

2.2. INSTAGRAM

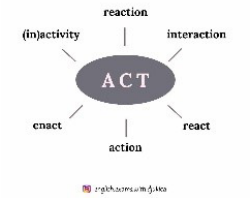
Instagram is a visual social network, which implies that aesthetics is momentous. "Instagram allows the users to express themselves, as in writing a caption below the photos or videos, share information, interact with others, spend their free time, and even for entertainment (Alhabash & Ma, 2017; Handayani, 2016). Seemingly, this trend attracted numerous users on global level, bridging entertainment and education. Conversely, entertainment is seen to have been diminished, perhaps even repressed substantially. The rise of various businesses is a further manifestation of new Instagram; education is no exception. Besides, it was upgraded and comprised long videos but now, short video forms, called reels, are the most recognised ones. This platform connects people in the way that they gain knowledge unwittingly, through entertainment, yet spontaneity. Regardless of the fact that Instagram is a social network, the nature of some accounts is highly professional. The capacity of "market" is immense – paid or free programmes, courses, e-books, videos in which teachers give explanations, and then invite followers to comment or ask questions, stimulating interaction. Subscription to the newsletter may be rewarding for the reason that it enables subscribers to get engaged more and they may receive a free e-book on a certain topic. In actual fact those who pay for programmes, earn extra privilege. Students have a chance to be taught by native speakers or non-native teachers who are qualified. One of the implemented options in demand on Instagram is so called "live" where a host invites a guest and they discuss a certain topic. Followers are informed about the time of the live and may directly participate in the discussion or be answered the questions thoroughly. Instagram predominantly plays an important role regarding exchanging DM messages (direct messages) which are private. Hence, the sense of confidence to require a further explanation or any information arises. One argument in favour of Instagram is that the content is condensed, giving rise to new optimism that learning is possible. As it excludes the climate of fear, communication is intensified. Practising English and regular interaction lead to the closer relationship with teacher; therefore, this mechanism affects learning positively. "Besides being used as a tool of communication, institutions have integrated social media such as Instagram as learning tools to deliver new information and connect with students." (https://deejournal.org/index.php/dee/article/view/26/22). Instagram undeniably has a beneficial effect on both – teachers and students. Accounts are created in the way that it is emphasised in the form of a short biography on the profile what service is offered, disclosing crucial information. Such standards facilitate the process of selection of the teacher and the content. It is usually the case that the followers can participate in commenting on the given topic and, thus, discussion or interaction with the teacher and other followers spontaneously develops. Interacting on a regular basis makes progress. While fears of the students subside, confidence simultaneously rises. Not only does Instagram contribute to learning, but it also encourages connecting with people worldwide. Users have an opportunity to make friendships and increase interpersonal intelligence. "Instagram is not only for sharing photos and videos, but also to create a community in any field, where the people involved may widen their networking as well as exchanging ideas, knowledge, or information (Soviyah & Etikaningsih, 2018). Moreover, being a member of a community triggers the sense of trust and the members do not hesitate to express their personal opinion on something to practise English. For instance, in closed groups, all the users who have the access exchange useful information, help each other, promote or ask a question, as they feel comfortable in that surroundings. Psychologists have argued that these positive characteristics create an intrinsically rewarding reason to continue participation in such a group (Kuo, 2003; Whitworth & De Moor, 2003). Mazer and his colleagues who conducted the research claim that, by joining these

groups and becoming a member of a community, students connect with the other peers and discover similarities. Not only does this relate to the peers, but to the teacher as well, since they learn what their life values are. This leads to a productive outcome which initiates a clear demonstration of the need to belong to a community. Furthermore, all the members become supportive and motivate each other. This implies that all the factors entailed will undoubtedly have a positive impact on the students` learning.

2.3. VOCABULARY

"It is true that knowing effective vocabulary learning strategies is important, yet applying the strategies, exploring new strategies, making the commitment to learn new words, using them in speaking and especially in writing, and having a strong desire to increase one's vocabulary size are even more crucial" (www.researchgate.net/publication/343252325_Effective_English_vocabulary_learning_strategies_A_research_summary). Definition of the word vocabulary in the Cambridge Dictionary is: "All the words that exist in a particular language or subject". Vocabulary is considered one of the most demanding segments of the English language, although new words can be found everywhere, for instance, in movies, in songs, or generally, on the Internet, even when users are in pursuit of entertainment. "Given the significance of having extensive vocabulary knowledge, that is, knowing a lot of English words, particularly high frequency ones, many, if not all, English as a second or foreign language learners from all over the world may have a strong interest in knowing and understanding how English vocabulary can be learned in an effective way" (www.researchgate.net/publication/343252325_Effective_English_vocabulary_learning_strategies_A_research_summary). Appropriateness of "C" level vocabulary should correspond to the complexity required at the highest levels – advanced and proficiency. The central challenge that Instagram users face is to recognise the professional account run by a qualified teacher. It is of a paramount importance to understand and apply the techniques which help vocabulary acquisition. However, at this stage, when students have already levelled up overall knowledge, their capacity is expected to be greater than "A" and "B" level simple words used on a regular basis, principally for the purpose of the English exams. This category entails collocations, idioms (in speaking), phrasal verbs, two-word adjectives, and such language segments, which are critical for the English exams - IELTS and Cambridge. Additionally, these aspects are taught and presented on the Instagram account @english.exams.with.djukica together with various techniques which have been proven to foster acquiring new high-level vocabulary. One of the objectives of this Instagram account, which is exclusively aimed at "C" levels, is to provide its followers with different techniques and strategies, considering learning vocabulary, for instance, Word Families or Grouping Vocabulary. The Word Families technique is defined as "words with similar roots and meanings" (Puchta, Stranks and Lewis-Jones, 2012).

The photo exemplifies Word Families technique posted on the Instagram account @english.exams.with.djukica.



Another technique, Grouping Vocabulary, covers the strategy which promotes creating different groups, such as organising words in topics, and this encompasses sets of links between the items.

The picture illustrating Grouping Vocabulary was taken from the E-book "Boost Your Vocabulary".

2.4. METHODS

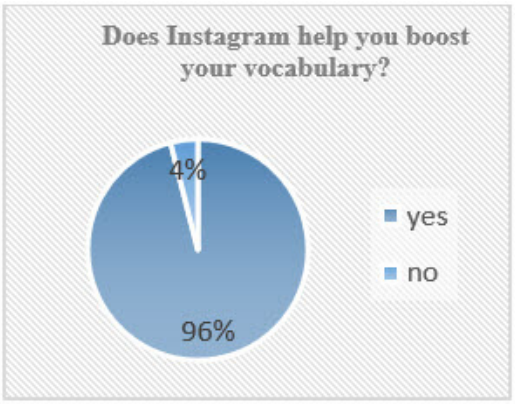
The prior studies are based on the premise that the role of Instagram is manifested through variety of accounts which provide its followers with the content for learning English vocabulary. The previous research "The Effect of Instagram on learning English Vocabulary" conducted in 2021 proved high effectiveness of Instagram on learning English Vocabulary. The data in this research was collected through survey, studying the effect of Instagram in learning Vocabulary of third semester students at English Tadris Study Program in IAIN Palu academic year 2020/2021. Relying on this research and the questionnaire created in the Instagram story on the account @english.exams.with.djukica, this paper will answer the following questions:

1. Is it possible to enhance and adopt English vocabulary at "C" levels on Instagram?
2. How does Instagram contribute to learning and improving English vocabulary at "C" levels?

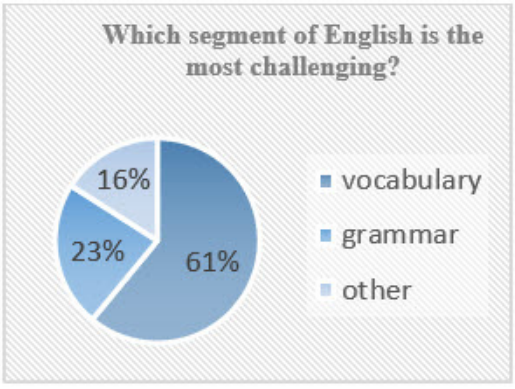
Hence, the paper will contextualise the use of Instagram for improving English vocabulary at advanced and proficiency levels. 57 followers who are at one of these two levels participated. The questionnaire, which was posted in Instagram stories, contained several questions with given options. After the followers had voted, the Instagram immediately calculated the percentage. Here, it will be explained what the option "story" is. "The photos and videos will disappear after 24 hours and won't appear on your profile grid or in feed." (https://about.instagram.com/blog/announcements/introducing-instagram-stories).

3. RESULTS

The first bar chart shows how useful Instagram is for improving English vocabulary at "C" levels. The percentage of those who consider it beneficial (96%) overweighs the ones who assume that Instagram is not helpful (4%). In support of this, there is a positive view that they understand and recognise complexity of the process of improving vocabulary, since at this level, they need both formal and informal register.



The second bar chart illustrates the percentage of the most demanding segments of English. It is obvious that vocabulary is considered the most difficult one. Albeit different techniques, for instance, Word Formation or Grouping Vocabulary, are applicable, demonstration of "C" level vocabulary is exceptionally challenging. Students are expected to have a wide range of vocabulary and awareness that simplifying sentences through the use of basic words will lead to failure in English exams, which are the main goal of the followers.



The third bar chart shows the options which the followers use to improve their vocabulary at "C" levels. 74% voted for stories, as these are not exposed to everyone; it is the teacher who has the insight into them. 21% approve of comments, which confirms their degree of confidence, given that this option is revealed to anyone. Only 5% supported chatgroups. This indicates that they are prone to the lack of confidence and it is the sense of community which stimulates them to participate.

4. DISCUSSION

It is obvious that the research corroborates prior study which proved high effectiveness of Instagram on learning English vocabulary. Likewise, the premise that Instagram has an influence on improving vocabulary at "C" levels is confirmed in this conducted research. The results reveal an enormous interest in enhancing vocabulary at "C" levels on Instagram. The students interact relying on numerous tools, use various techniques and adopt new words and expressions, practising them through the context that is meaningful for them. However, they have a different approach to learning considering the fact that they are aware of the complexity of vocabulary required at these two highest levels. Therefore, the majority of them are confident to do the tasks solely in stories, as the teacher is the only one who has the access to the answers. The second commonly used space for interaction is comments. The followers belonging to this group have confidence to share their ideas with others, not exclusively with teachers. Finally, there is a small number of those who voted for "other", which is usually DM (direct message) or closed groups. They evidently have a tendency to prioritise the sense of community in the process of acquiring vocabulary at advanced and proficiency levels.

5. CONCLUSION

Opportunities offered on social media are immense and invaluable, particularly taking into consideration the fact that majority of content is free. In this modernised era social networks have become an indispensable asset regarding education, and the amount of heterogeneity in the opportunities given is massive. Not only do people entertain, but they also develop social skills, connect worldwide, run businesses and learn. However, Instagram among other platforms, has been elevated to the degree which reinforces its new task – educating its users. As "C" level requires complexity, in general, an impediment to improving vocabulary can be an erroneous belief that cognitive approach is not fundamental. Accordingly, selection of the Instagram accounts should come under close scrutiny in order to avoid discrepancy between necessary techniques for improving vocabulary at "C" levels and the wish to rapidly acquire new words. The influence of Instagram is undiminished and this phenomenon is presumed to thrive in the future. It is obvious that as a consequence of digital revolution, teaching methods have dramatically changed and online learning dominantly replaced traditional classrooms. Therefore, the recommendation of the author is that offline English teachers should include learning on social media in curriculum and introduce it in their classrooms. This can serve as extra material for practising English and strengthening communication skills.

6. REFERENCES

Alhabash, S., & Ma, M. (2017). A Tale of Four Platforms: Motivations and Uses of Facebook, Twitter, Instagram, and Snapchat Among College Students? Social Media and Society. https://doi.org/10.1177/2056305117691544
Crystal, D. (1997). English as a Global Language. Cambridge University Press.
Crystal, D. (2012). Language and the Internet. Cambridge University Press.
Handayani, F. (2016). Instagram As a Teaching Tool? Really? Proceedings of the Fourth International. (https://www.researchgate.net/publication/335241024_INSTAGRAM_AS_A_TEACHING_TOOL_REALLY)
Kuo, Y.-F. (2003). A study on service quality of virtual community websites. Total Quality Management. Published online.
Mazer, J.P., Murphy, R.E., & Simmonds, CJ. (2007). I'll see you on "Facebook": The effects of computer-mediated teacher self-disclosure on student motivation, affective learning, and classroom climate. Communication Education. Published online.
Mirkovic, DJ. (2022). Boost Your Vocabulary. E-book. https://drive.google.com/file/d/1eewsZOozZG6NRcT6G4DHnP8ebOV9HyJ-/view?usp=share_link
Paolillo, J. (1999). The virtual speech community: social network and language variation on IRC. Journal of Computer-Mediated Communication.
Puchta, H., Stranks, J. & Lewis-Jones, P. (20120). English in Mind 5, Workbook, second edition. Cambridge University Press.
Shih, C. (2010). The Facebook Era - Tapping Online Social Networks to Market, Sell and Innovate Pearson Education, Inc.
Soviyah, & Etikaningsih, D. R. (2018). Instagram Use To Enhance Ability in Writing Descriptive Text. Published online.
Whitworth, B., & De Moor, A. (2003). Legitimate by design: Towards trusted socio technical systems. Behaviour and Information Technology. Published online.

DICTIONARIES:
https://dictionary.cambridge.org/dictionary/english/vocabulary
https://www.collinsdictionary.com/
CAMBRIDGE Academic Content Dictionary. (2009). Cambridge: Cambridge University Press.
Longman Dictionary of Contemporary English. (2008). Longman
https://www.thesaurus.com/browse/impede

WEBSITES:
www.frontiersin.org/articles/10.3389/feduc.2022.923507/full
www.deejournal.org/index.php/dee/article/view/26/22
www.researchgate.net/publication/343252325_Effective_English_vocabulary_learning_strategies_A_research_summary
www.about.instagram.com/blog/announcements/introducing-instagram-stories
www.doi.org/10.25134/ieflj.v4i2.1373.

Blazhevski, I. (2022). Ethical considertions in usage of Twitter data, *SCIENCE International journal, 1*(1), 27-32.
doi: 10.35120/sciencej010127i
UDK: sss

ETHICAL CONSIDERTIONS IN USAGE OF TWITTER DATA

Ivan Blazhevski[1*]

[1]Institute for Sociological, Political and Juridical Research, Ss. Cyril and Methodius University Skopje, Republic of North Macedonia, e-mail: ivan.blazevski@isppi.ukim.edu.mk

Abstract: Internet-based data, especially the ability to extract and analyze data from social media such as Twitter, is becoming more prevalent in providing data in empirical research. The public nature of Twitter and its more open access to data, compared to other social media, as well as the approval to use that data in accordance with the Twitter's Terms of Service were considered a sufficiently ethical justification for the use of Twitter data in research. This tendency to collect data from the Internet, that is from social networks, in social research, has prompted a number of scientific societies to develop ethical guidelines for Internet research.

This paper provides an overview of the recommendations contained in the ethical guidelines, compared to the requirements set out in the Twitter's Terms of Service. Additionally, research on social media users' perceptions regarding the use and publication of their data is analyzed. The tendency to apply the principle of situational ethics is evident in the ethical guidelines, starting from the existing collision between the established ethical principles for scientific research and the privacy policy on Twitter. However, there is a lack of consensus among ethical guidelines in determining the appropriate way of collecting, processing and presenting data in research and scientific publications. Also, in research on the perception of social media users, there is a significantly lower concern about the use of data by Twitter users, compared to users of other platforms. But in spite of that, the prevailing opinion among them is the need for prior consent for the use of their data in research and scientific publications, with a special emphasis on the request for anonymity. Given the complexity of this debate, which ultimately aims to preserve the academic integrity of research, the conclusion points to the need to summarize the various ethical aspects in establishing a methodological approach in studies that use Twitter data.

Key words: ethics, research, data, social media

INTRODUCTION

Modern technological advances, which enabled wide availability of information, as well as the possibility to conduct certain research in a shorter time and with less financial resources, have led to the widespread use of the Internet. Given that the traditional survey methods have long faced difficulties from increasing costs and declining responses rates, the great interest in web surveys was quite expected. For the first time, an alternative was offered, which made data collection much easier, especially the collection of more sensitive data (Woodfield and Iphofen, 2018). But with increasing public interest and access to the Internet during the early 1990s, ethical questions about practices and outcomes also arose. Thereby, the public was rightfully concerned about the practices such as the widespread collection, archiving, and selling of one's personal information; the loss of privacy from surveillance technologies; the rise in cut and paste plagiarism in education; questions of authorship and credibility in the publication of information and layperson journalism; and copyright issues raised by the easy sharing of music over the Internet (Markham, 2006).

After the first social media appeared on the Internet, 25 years ago, the interest of scientific researchers was immediately attracted by the unprecedented opportunities for research endeavors. Their interest was particularly driven by the opportunities for recruiting participants and collecting data. At that stage of social media development, the activity of the participants in the communication through social media was significantly lower, while the research role was not clearly defined. The first social media surveys took place during this period, dominated by online interviews, participant observations, online surveys and focus groups. In doing so, the first ethical issues were raised, whether social media data should be considered human subjects research or text, how these deliberations influence practices of consent, and whether social media users have perceived expectations of privacy when using social media platforms (Samuel and Buchanan, 2020).

Twitter as one of the most widespread social media platform across the world, has gained popularity among researchers due to its open access. Additionally, researchers can relatively easily collect

*Corresponding author: ivan.blazevski@isppi.ukim.edu.mk

large amounts of data in a short period of time as well as process it through the platform's Application Programming Interface (API). When collecting data, in many cases, the researcher is not required to their oversight or informed consent practices. In doing this, most researches who collect tweets do not gain consent from each user whose tweet is collected, nor do researchers inform those users. However, it should be noted that Twitter's Privacy Policy mentions that academics may use tweets as part of research, but this update was not included until revisions were made to the policy in 2014. Moreover, Internet users rarely read or could fully understand website terms and conditions (Webb et al., 2017).

RESEARCH ETHICS IN SOCIAL AND e-RESEARCH

Discussions on ethical issues are often perceived as pre-imposed constraints and activities. But in academic research contexts, ethical debates focus on how researchers treat humans within their studies. That is, according to Markham, in the context of:" policy-making, laws and regulations - which have probably developed in particularly cultural contexts over long periods of time - predetermine ethical parameters" (Markham, 2015). According to Bryman (2012), discussions about ethical principles in social research, or more precisely – the ethical transgressions, tend to revolve around certain issues that recur in different guises, which Diener and Crandall (1978) have broken down into four main areas: whether there is harm to participants; whether there is a lack of informed consent; whether there is an invasion of privacy; and whether deception is involved. Although these four principles overlap in part, Brayman points out that there is no doubt that these four areas form an appropriate classification of ethical principles in and for social research.

The advent of the Internet and its use in social research has raised new dimensions of ethical decision-making for social researchers. The biggest challenge in conducting research in the internet community is the issue of informed consent, that is the risk of violating ethical principles of privacy and confidentiality. As a starting point in such an ethical dilemma, Essaybach and Till (2001) suggest that it should be the determination of the material, posted by the internet community, as public or private. In addition, Bryman (2012) points out that the more the website is recognized as public, the less the researcher's obligation to protect the confidentiality and anonymity of the website users, or the less the respondent's obligation to seek informed consent. But very often, the difference between the public and private sphere of the Internet is vague and disputable. Also, complete protection of anonymity is almost impossible in internet surveys, which arises from the difficulty of knowing who has access to the information. This, according to Bryman, places special ethical concerns on quality researchers, because a message posted on the social networking websites may be available for anyone with a computer and internet connection. Here I would list Pace and Livingston's (2005) point of view, according to whom such electronic communications should be used for research only if: the information is publically archived and readily available; no password is required to access the information; the material is not sensitive in nature; and no stated site policy prohibits the use of the materia. Moreover, they suggest that if these circumstances do not pertain, informed consent should be provided and it should be provided without disrupting the ongoing online activity. They also point out that identities and confidentiality must be protected.

According to another point of view (Jouhki et al., 2015) research ethics in any academic research can be seen as balancing between two classic moral philosophical stances – utilitarianism and deontology. Utilitarianism attempts to calculate the morality of an act by estimating the total amount of happiness or suffering produced by the act, while deontology views certain actions as immoral or moral per se, regardless of their consequences. In this regard, the Jouhki et al. (2015) indicate that:" in social media research when scholars contemplate the effect of their study on the subjects' privacy: the utilitarian view of privacy might allow certain incursions into privacy if the result is the greater good, whereas deontological ethics holds that a certain level of privacy is a right that should not be violated by, for example, conducting a study without receiving the informed consent of the subjects of the study". Ultimately, they emphasize that the utilitarian emphasis on avoidance of harm and the more deontological value of receiving informed consent from research subjects are the two most crucial imperatives of research ethics in studies with human participants.

EMERGE OF ETHICAL ISSUES IN SOCIAL MEDIA SURVEYS

The representation and importance of social media can best be shown through the statistics according to which in April 2022 there were five billion internet users worldwide, which is 63 percent of

the world's population. At the same time, 4.65 billion of them were social media users (Statista, 2022). Social networking is the most common online activity, which resulted in global average penetration rate of 58.4 percent (Statista, 2022). This presence of social media resulted in their positioning as the most influential media on public opinion. The ability to access via smartphones has increased the speed of initiating any kind of public debate, thus establishing the undisputed position of social media on public opinion. This technological advancement has introduced social media platforms in the areas of Facebook, Twitter, YouTube and others, and thus their presence on the Internet. First ethical issues that emerged at the beginning of usage od social media in scientific surveys, like issues of identifiability of participants, vulnerability, potential harm, intrusiveness, and confidentiality, were developed into the first and second Association of Internet Researchers ethics guidance for researchers using social media data (Ess and the AoIR ethics working committee, 2002; Markham and Buchanan, 2012). But with the further technological advancement of social media platforms, social media research methodologies have also evolved, as they have progressed to more analytical and autonomous processes based on large quantitative analyzes and "data models". Consequently, debates, which initially revolved around consent and privacy for social media data use as an isolated source, were reshaped by large-scale "big data" surveillance, and scraping and mining research employing artificial intelligence and data modeling methods (Samuel and Buchanan, 2020).

In addition to the research benefits of social media development, in recent years, there have also been a number of research ethics controversies that gained public attention such as Facebook Emotional Contagion study that studied Facebook users without their consent; OkCupid, a social media dating service, public release of non-anonymized data scraped by a researcher against the site's Terms of Service; and perhaps the most media-covered case of this kind – Cambridge Analytica scandal – misuse of data of an estimated 87 million Facebook users by data firm Cambridge Analytica to build voter profiles (Markham, 2015). Therefore, Whiteman (2012) points out that the public/private distinction has specific implications for social science research. According to her:" it plays a key role in academic discussion of the legitimacy of certain methods and, in particular, the contested acceptability of covert methods of data collection. This is because, despite a 'nearly universal' understanding of the need to protect the private sphere, there is a tradition of observational research in which 'it has been accepted that behaviour that is performed within the public domain may be observed and researched without consent'. In raising questions of privacy, the public/private distinction therefore raises fundamental 'questions about the necessity of consent." Finally,Williams, Burnap and Sloan (2017) emphasize that a principal ethical consideration in most learned society guidelines for social research is to ensure the maximum benefit from findings while minimising the risk of actual or potential harm during data collection, analysis and publication. They also point out that potential for harm in social media research increases when sensitive data are estimated and published along with the content of identifiable communications without consent. These data usually include sensitive personal demographic information (ethnicity and sexual orientation), information on associations (memberships to particular groups or links to other individuals known to belong to such groups) and communications of an overly personal or harmful nature (details on morally ambiguous or illegal activity and expressions of extreme opinion).

ETHICAL GUIDELINES AND PRIVACY POLICY (LEGAL OBLIGATIONS)

Twitter was launched in 2006, as a online social networking and micro blogging service, as of January 2022 were registered 436 million monthly active users (Statista, 2022). Communication on Twitter is enabled through statements called 'tweets', which can contain up to 140 characters. Users are not obliged to state their real names and location, and are usually identified by their unique usernames. When creating an account, each user is referred to the terms and conditions of Twitter, where the open character of this platform is especially emphasized. The Privacy policy also highlights the privacy settings in which the character of the user account can be determined, that is the setting up of an open access account, or closed account, whose activities are visible only to the users that are registered as 'followers'. Additionally, due to the open nature of Twitter, users are informed that according to the Twitter's Terms of Service and Privacy Policy, their information may be collected and used by third parties (Twitter, 2022).

The growing popularity of Twitter as the primary online space for public expression of citizens' reactions to certain events has made it one of the most widely used data sources in social science research. One of the most significant features that drives such popularity of Twitter, as well as the influence of the Twitter audience on various topics of social life, according to Stephen Dann (2015), arises from the default public nature od Twitter versus the default private nature of other social networks. According to him, this

perception stems from the fact that Twitter users post content on the public timeline, which can be viewed from a public website, thus creating a source of secondary published data. This perception has also been reflected in the view of a number of researchers who believe that the ethical and legal justification for using data without informed consent stems precisely from Twitter's privacy policy. Specifically, the Twitter's Developer policy states that:" academic researchers are permitted to distribute an unlimited number of Tweet IDs and / or User IDs if they are doing so on behalf of an academic institution and for the sole purpose of non-commercial research" (Developer policy, 2022). However, Twitter imposes certain additional conditions on this permission of the researchers, so that when distributing the tweets, the user ID must be provided. Also, if certain content has been deleted, or given protected status, or otherwise been suspended or removed from Twitter, the developers should delete or modify that content as soon as possible (Developer policy, 2022). This Twitter privacy policy allows researchers to collect tweets, which they use for analysis through the API (Application Programming Interface) platform, without the prior informed consent of the users whose tweets have been collected. Based on this, users, in most cases, are not approached directly to obtain their informed consent to participate in a specific survey, as Twitter's Developer policy is considered to allow this. But social media users' interest in using their posts is also complementing this trend. This situation was determined in a survey conducted in 2011, regarding the legal implications of the posts of users of various social media, and it was found that only 18 percent of respondents read the terms and conditions for posting on the social media they use (Zimmer and Proferes, 2012). However, in most cases, the research is conducted within universities or is funded by institutions that impose certain ethical standards. The principles and rules deriving from these standards often go beyond just binding legal standards. Also, violations of the ethical principles of universities, that is institutions entail sanctions which in certain cases may result in job loss or further and future funding of research.

Facing a growing number of ethical dilemmas that have arisen from the use of the benefits of digital technology and the Internet in social research, a number of scientific societies have developed specific ethical guidelines for research in digital environment. So in the past years such guides have been introduced by the British Sociological Association, the British Psychological Society, the European Society for Opinion and Market Research, the International Visual Sociology Association and others. However, the Association of Internet Researchers (AoIR) was the first to developed ethical guidelines for internet research in 2002, designed as recommendations for researchers, students, developers, that is all those who face ethical concerns during their Internet research (Ess and the AoIR ethics working committee, 2002). Following this initial version, two more ethical guidelines were introduced in 2012 and 2020, which are upgraded versions of this guideline (Markham and Buchanan, 2012; franzke et al., 2020). What these guidelines have in common, according to Williams et al. (2017), is that they generally adopt the principle of situational ethics: "that each research situation is unique and it is not possible simply to apply a standard template in order to guarantee ethical practice". Furthermore, these ethical guidelines on the issue of informed consent indicate that in cases where it is not possible to obtain, the analysis must be conducted on depersonalized data. This position, to a large extent, prevails in the later acts and documents introduced by various institutions and universities, so in the US a 2015 amendment to the 'Common Rule' Federal Policy for the Protection of Human Subjects it is stated that certain forms of online behaviors can be classed as public behavior, hence there is no need to require additional ethical review. Whereas it is stated that:" Any research involving standardized testing, surveys, interviews, or observations, including audio and video recording, of public behavior, including behavior online, will be able to proceed without further review" (HHS, 2015). The British Psychological Association and the Association of Internet Researchers also point to the need for careful consideration of ethical issues when using social media as a source of research data, particularly in relation to privacy breaches. It is also important to cite the University of Aberdeen recommendations from a project funded by the Economic and Social Research Council, which states that in the case of sensitive social media content, researchers should either consider using paraphrased / composite data instead of reproducing the actual posts or use an informed consent approach (Webb et al., 2017). Webb et al. (2017) also cites the updated 2016 Oxford University web-based research guidance, which states that when providing data from Twitter, researchers do not need to seek informed consent from participants/users, unless they plan to publish individual posts in a specific report or scientific paper.

PUBLIC ATTITUDES ON TWITTER DATA USAGE

The lack of consensus in the academic community, as well as some controversy regarding the use of data from social networks, initiated research on users' perceptions regarding the use of data. In one of the first such studies, conducted by Beninger et al. (2014), it was found that for social media users, the need for informed consent or anonymity guarantees depends on the following factors: mode and content of the posts; social media website being used; the expectations the user had when posting, and; the nature of the research. In addition, the participants in this research clearly stated that they are particularly concerned about posting their pictures, the publication of sensitive or personal posts, as well as the publication of their usernames in research papers. What is particularly noticeable is the perception of content posted on social media websites for fun purpose as much more "personal" compared to content posted on social media websites for "professional" purpose. Respondents also expressed less concern about the use of their tweets in research without prior consent, compared to their Facebook posts, which the authors said stemmed from Twitter being understood as a public network, as well as its more open privacy settings. In 2015, Evans et al. (2015) conducted research in the UK on users' attitudes regarding ethical principles for social media research. According to their findings, 38% of the respondents believe that the sharing of their data from social media with third parties for research purposes is carried out according to the terms and conditions that were indicated to them on the social media sites. Nevertheless, 60% of them think that their data on social media sites should not be shared with third parties for research purposes. However, this attitude varies among the respondents depending on whether that data was already publicly available (as is the case with Twitter posts), the level of anonymity, as well as the purpose of the research and how much personal data is contained in the data used in the research.

A 2017 study by Williams et al. (2017), conducted on Twitter users in the UK, found that respondents had the lowest level of concern about using their data in scientific research (84% of respondents were not at all or only slightly concerned). While, users' concern about the use of their data by other actors is significantly higher, with 49% being quite or very concerned about the use of data by the government, and 51% being quite or very concerned about commercial settings. However, despite the low level of concern of the respondents about the use of their data in scientific research, still almost 80% of them expect their consent to be requested before publishing their data in scientific research, while 90% of the respondents expect to remain anonymous in scientific publications.

CONCLUSION

The wide range of possibilities that have emerged with the advent of the Internet have also been reflected in scientific research. Online surveys have made it possible to reduce the cost of research, which was one of the main difficulties, as well as to increase the range of respondents. Additionally, with the advent of social media, scientific researchers have recognized the potential for simpler provision of participants, as well as significantly facilitated communication and data collection. However, the increased use of social media, that is Internet platforms and applications in data collection in research, has resulted in increased confrontation of researchers with the conditions of use, that is ethical principles that dictate the conditions under which such research activities can take place.

Twitter data is more openly accessible than other social media platforms, and in web research, it is standard practice to collect tweets for analysis through the platform's API. In doing so, users are usually not approached to seek their informed consent to participate in the research, instead it is assumed that the approval arises from the Twitter's Terms of Service and Privacy Policy, that is their acceptance by the user. However, the emergence of numerous ethical controversies regarding the use of data from social media, as well as the manipulation of users for various researches, has attracted the attention of the public. Public pressure has sparked debate over the applicability of established ethical principles in the use of social media data in scientific research. This has resulted in the development of specific ethical guidelines for scientific research in the digital environment by a number of scientific societies. In the analysis of such ethical guides, that is the use of data from Twitter in scientific research, it was observed that there is no consensus among the academic community in determining the appropriate way of collecting and using data from social media, including Twitter. The most obvious are the disagreements about relying solely on the Terms of Use of Twitter when collecting data. According to certain guidelines and many studies it is a standard practice, but it is problematic, especially in terms of the already established ethical principles in scientific research. In such a debate, researchers are brought into a position of constantly negotiating ethical positions, as well as their interpretation and introduction of alternative ethical positions.

According to certain authors, the views of the public, that the users whose data are used in research, must also be taken into account. Analyzing their findings, it was found that although, compared to other platforms, Twitter users are much less concerned about the use of their data in research, they are still particularly concerned about the amount of personal data contained in data that will be used in the research. In doing so, users emphasize the publication of their usernames, as well as the publication of their posts with sensitive content in research papers. Also, most of the respondents, that is users expect their consent to be previously requested for the use and publication of their data in research, especially emphasizing the request for their anonymity in research publications.

Given all this, we could conclude that from an ethical perspective, the practices established in the use of Twitter data are to some extent in collision with the ethical guidelines and attitudes of users. Hence, in order to maintain scientific credibility, it is necessary to summarize the different views and aspects when conceptualizing the methodological approach for research that uses Twitter data.

REFERENCES

Beninger, K., Fry, A., Jago, N., Lepps, H., Nass, L. & Silvester, H. (2014). Research using Social Media; Users' Views. NatCen Social Research Retrieved from: https://www.bl.uk/collection-items/research-using-social-media-users-views (October 30, 2022)

Bryman, A. (2012). Social Research Methods, 4th edn. Oxford University Press

Dann, S. (2015). Twitter Data Acquisition and Analysis: Methodology and Best Practice. In Burhalter, J. & Wood, N. (eds) Maximizing Commerce and Marketing Strategies through Micro-Blogging. Business Science Reference

Developer policy [website]. (2022, August 27) Content redistribution Retrieved from: https://developer.twitter.com/en/developer-terms/policy

Diener, E. & Crandall, R. (1978). Ethics in Social and Behavioral Research. Chicago: University of Chicago Press

Ess, C. & the AoIR ethics working committee (2002). Ethical decision-making and Internet research: Recommendations from the aoir ethics working committee. Retrieved from: https://www.aoir.org/reports/ethics.pdf (September 12, 2022)

Evans, H., Ginnis, S. & Bartlett, J. (2015). #SocialEthics: A Guide to Embedding Ethics in Social Media Research. London: IpsosMORI Retrieved from: https://www.ipsos.com/sites/default/files/migrations/en-uk/files/Assets/Docs/Publications/im-demos-social-ethics-in-social-media-research-summary.pdf (September 10, 2022)

Eysenbach, G. & Till, J. E. (2001). Ethical issues in qualitative research on internet communities. British Medical Journal, 323 (7321)

franzke, a. s., Bechmann, A., Zimmer, M., Ess, C. & the Association of Internet Researchers (2020). Internet Research: Ethical Guidelines 3.0. Retrieved from: https://www.aoir.org/reports/ethics3.pdf (September 12, 2022)

Jouhki, J., Lauk, E., Penttinen, M., Rohila, J., Sormanen, N. & Uskali, T. (2015). Social media personhood as a challenge to research ethics: Exploring the case of the Facebook experiment. Social Media Research Symposium "Successed and failures in studying social media: issues of methods and ethics", University of Jyväskylä, Finland

Markham, A. (2006). Ethic as Method, Method as Ethic: A Case for Reflexivity in Qualitative ICT Research. Journal of Information Ethics 15 (2)

Markham, A. & Buchanan, E. (2012). Ethical decision-making and Internet research 2.0: Recommendations from the AoIR ethics working committee. Retrieved from: https://www.aoir.org/reports/ethics2.pdf (September 12, 2022)

Markham, A. (2015). Produsing ethics [for the digital near future]. In Lind, R. (Ed.). Produsing theory in a digital world 2.0: The intersection of audiences and production in contemporary theory Vol.2. Peter Lang Inc.

Pace, L. A. & Livingston, M. M. (2005). Protecting Human Subjects in Internet Research, International Journal of Business Ethics and Organization Studies, Vol.10

Samuel, G. & Buchanan, E. (2020). Ethical Issues in Social Media Research. Journal of Empirical Research on Human Research Ethics 15(1-2)

Statista.com [website]. (2022, May 20) Worldwide digital population as of April 2022, Retrieved from: https://www.statista.com/statistics/617136/digital-population-worldwide/

Statista.com [website]. (2022, May 20) Social media: global penetration rate 2022, Retrieved from: https://www.statista.com/statistics/269615/social-network-penetration-by-region/

Statista.com [website]. (2022, May 20) Most popular social networks worldwide as of January 2022, ranked by number of monthly active users Retrieved from: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Twitter Terms of Service [website]. (2022, August 25) Retrieved from: https://twitter.com/en/tos

U.S. Department of Health and Human Services: Office for Human Research Protections. (2022, October 03). Code of Federal Regulations (Pre-2018 Requirements). Retrieved from: http://www.hhs.gov/ohrp/regulations-and-policy/regulations/nprmhome/index.html

Webb, H., Jirotka, M., Procter, R., Stahl, B.C., Rana, O., Burnap, P., Housley, W., Edwards, A. & Williams, M. (2017). The Ethical Challenges of Publishing Twitter Data for Research Dissemination. ACM Web Science

Whiteman, N. (2012). Undoing Ethics: Rethinking Practice in Online Research.Springer

Williams, M.L., Burnap, P. & Sloan, L. (2017). Towards an Ethical Framework for Publishing Twitter Data in Social Research: Taking into Account Users' Views, Online Context and Algorithmic Estimation. Sociology, 51(6)

Woodfield, K. & Iphofen, R. (2018). The Ethics of Online Research. In Woodfield, K. (ed.), The Ethics of Online Research (Advances in Research Ethics and Integrity, Vol. 2). Emerald Publishing Limited

Zimmer, M. & Proferes, N. (2012). Privacy on Twitter, Twitter on Privacy. In Weller et al. (Eds.) Twitter and Society. Peter Lang Publishing

Risteski, T. (2022). The principle of responsibility as the supreme legal principle in the work of public organs, *SCIENCE International journal, 1*(1), 33-39. doi: 10.35120/sciencej010133t

THE PRINCIPLE OF RESPONSIBILITY AS THE SUPREME LEGAL PRINCIPLE IN THE WORK OF PUBLIC ORGANS

Temelko Risteski[1*]

[1]American University of Europe – FON, Skopje, RN. Macedonia, e-mail: temelko_mkd@yahoo.com

Abstract: PURPOSE: The purpose of the research is to prove that the principle of responsibility is the supreme (primary) principle in the work of public organs (ministries, other state administration organs, organizations established by law, other state organs, legal and natural persons to whom, by law, is entrusted to exercise public powers, as well as the organs of the municipalities, the city of Skopje and the municipalities in the city of Skopje). RESEARCH METHODOLOGY: The research used the method of analysis of the provisions of the state constitutions for public administration and human rights; on the laws on public administration and on the procedural provisions that lead public organs, on the international legal acts on human rights and on the relevant literature on the organs of public administration. RESEARCH RESULTS: The research imposed the following basic ideas: Public organs are composed by people. Those people are organized by special acts for the organization and systematization of jobs. These acts are adopted on the basis of special laws that regulate social relations in various areas of social life. In the jobs to which people are assigned, they have precisely prescribed tasks that they are obliged to perform. The duty to perform them entails responsibility for non-performance or for low-quality and untimely performance. A democratic society is a society of responsible individuals and responsible public organs. There are no responsible public organs without responsible individuals. CONCLUSIONS: Public service in public organs is performed by officials. The responsibility of officials is manifested as a three-dimensional social phenomenon. The first dimension covers the responsibility of the official to himself as a person to whom the international legal acts on human rights and the Constitutions of the states guarantee respect and protection of honor, dignity and reputation. The second dimension of responsibility covers the responsibility of the officials, as public servants, in relation to the citizens, as clients. The third dimension of responsibility covers the responsibility of the officials to the public organs in which they works and his responsibility to the public service, as a service to the citizens within the state, as an organized community of citizens. The general conclusion is that the principle of responsibility is the supreme principle, the consistent implementation of which in the work of public organs directly depends on the implementation of other principles in their work. RECOMMENDATIONS: Throughout the process of education and upbringing, one should, first of all, work on developing the autonomous responsibility of officials. In addition to the autonomous responsibility with the activity of the control protection services and institutions of society: the system of internal control in public organs, inspections, internal affairs organs, the State Commission for the Prevention of Corruption, the Commission for Protection against Discrimination, the Ombudsman, prosecutors' offices and courts should be developed the heteronomous responsibility. ADDITIONAL INFORMATION: The autonomous morality, and thus the autonomous responsibility of public officials, in the public organs of the Republic of North Macedonia, is not at a satisfactory level. To the principle of accountability of public officials is not given enough attention. This is supported by the fact that it is attributed to a very small number of laws, and it is not found in procedural laws. This imposes the need to prescribe this principle in the laws for the regulation of social relations and for the work of public organs in all areas of social life, and this, as the first in order of rank, because the implementation of the other principles in the work of public organs directly depends on its implementation in the work of these organs.

Keywords: principle, responsibility, public authority, public service, official.

INTRODUCTION

Responsibility is a basic assumption for the efficient functioning of the state as an organized community of citizens and as a legal and political system. The character and form of the political system depends on the existence or non-existence of responsibility. The democratic political system starts from the assumption that citizens consciously and conscientiously perform their duties towards society and, thereby, create the basis and conditions for the harmonious development of mutual relations, and at the same time, conditions for the proper functioning of the democratic political system, as a whole.

The feeling of personal responsibility is one of the basic prerequisites for the efficient functioning of the institutions of the socio-political system of the state. Accordingly, every citizen bears responsibility for his actions in the sphere of social action. He also bears a certain degree of responsibility for his passive

*Corresponding author: temelko_mkd@yahoo.com

attitude towards the mistakes and violations of social rules of other citizens, because he is part of society made up of people who live, work, and satisfy their personal and common needs in conditions of mutual coexistence and solidarity. In such conditions, the omissions and violations of social norms, by certain citizens, have a negative impact on the realization of the rights and interests of other citizens.

Citizens, as members of a social community, also perform public functions or services, or participate in their performance. It is their right guaranteed by the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the Constitution of the Republic of North Macedonia*.

Citizens perform or participate in the performance of public functions in public organs. Public organs are ministries, other state administration organs, organizations established by law, other state organs, legal and natural persons entrusted by law with exercising public powers, as well as the organs of the municipalities, the city of Skopje and the municipalities in the city of Skopje**.

Citizens who perform or participate in the performance of public functions in public organs have the status of authorized officials.

Every participant in the performance of a public office should be aware that he is participating in the service of citizens in the area of social life in which the public organ was established. Accordingly, the performance of public office must be human in nature and humane in purpose. To be such, it must be based on the respect of the person as a citizen - client in the procedure and on the trust towards him. The performance of a public function is human, which starts from the sense of responsibility of everyone who performs it. Filled with that feeling, the public official becomes aware that he is not "all-powerful," that he is not a man who knows all and that his word means "law."*** Otherwise, the public official takes on the psychology of an official - the bureaucrat. With such a psychology he turns into a blind follower of his superior and as such, seeking himself in the hierarchy of public service, he forgets his basic duties and waits for orders from his superiors. In that way, he is alienated from the service function of its performance of the public service. Thus alienated and bureaucratized, the public servant is subject to the use of public office for personal purposes, which in turn is the basis for the emergence of corruption in the ranks of public services.

In order to eliminate this sociopathological phenomenon in public organs, it is necessary, first of all, to work towards developing a sense of personal, ie autonomous responsibility among public officials. Autonomous responsibility is the basis of any institutional responsibility. Without autonomous responsibility there is no real responsibility. Institutional accountability is therefore a superstructure of autonomous accountability. That is why the developed sense of autonomous responsibility is a guarantee for the legal and efficient performance of public services by public authorities, and the principle of responsibility, as a legal principle, is a guarantee for the implementation of other principles in their action: the principle of constitutionality and legality, the principle of objectivity, the principle of service orientation, the principle of efficiency, the principle of economy and rationality and other principles.

RESPONSIBILITY OF OFFICIAL PERSONS FOR THEIR REPUTATION AND DIGNITY

The Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights guarantee every citizen of the Planet the right to protect his honor and reputation****. According to Article 1 of the Declaration, "All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should treat each other in the spirit of common humanity."

The Constitution of the Republic of North Macedonia, in Article 25, guarantees the citizens of the Republic, among other things, respect and protection of dignity and reputation. Honor, dignity and

* Everyone has the right to equal access to public services in their country (Article 21, paragraph 2 of the Universal Declaration of Human Rights). Every citizen has the right and the opportunity, without any discrimination and without unreasonable restrictions, to participate in the management of public affairs and to be accepted, under general equal conditions, in the public services of his country (Article 25 under a) and c) from the International Covenant on Civil and Political Rights). Every citizen has the right to participate in the performance of public functions (Article 23 of the Constitution of the RNM).

** See: Article 4, paragraph 1, of the Law on General Administrative Procedure ("Official Gazette of RSM", number 124/2015).

*** See: Hristov A., (1981), Administrative Law, Institute for the Advancement of the Economy of SRM, Skopje, p. 224.

**** See Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights.

reputation, as legal and moral values, imply a person with integrity, with a built system of moral values aligned with the moral values of the social environment.

When it comes to the officials of the public organs, the principle of responsibility requires them to act conscientiously towards the performance of their official duties. Reason, as a natural characteristic of man, as homo sapiens, should be in the function of conscience as a set of moral judgments of the person about his desires and actions. The conscience based on reason and in the spirit of common human belonging, to which the Universal Declaration of Human Rights refers, should create and maintain a person whose character will be distinguished by the following moral values: independence in work, sacrifice, caring, conscientiousness, etc. These moral values are the basis of the autonomous responsibility of the person as a moral category. A person whose autonomous morality relies on these moral values is characterized by strongly developed feelings of duty and responsibility for quality and timely performance of work duties. Such a person does not run away from tasks that entail responsibility before the community, but gladly accepts them as an opportunity for self-affirmation in the eyes of the members of the community, as an organized human system. When she accepted these values, she works seriously, with a critical attitude towards herself, and towards other members of the community who directly or indirectly participate or have an influence on the performance of the tasks. Such a person is alien to frivolity, uncriticalness, lack of a sense of duty, indifference, negligence and irresponsibility of others, ignoring work obligations which, unfortunately, is a characteristic of many public servants whose main concern is earning and advancing in the service with poltergeist attitude towards the superiors and the powerful, leaving aside the quality and efficiency of the work, as something secondary.

If the international legal acts and the provisions of the constitutions of the states on human rights and freedoms, based on them, guarantee the person the right to honor, reputation and dignity, that right should be protected. It will be most effectively protected with reason aimed at achieving as much efficiency and quality as possible in the performance of the public service, the basis of which is the conscience of the public servant as the basis of his autonomous morality and, therefore, of his moral responsibility on which, in turn, relies on his legal responsibility. Honor, reputation and dignity are best acquired by responsible work in the service of the citizens of one's own country who are part of humanity on Planet Earth. Only with such work will they confirm and prove the true belonging to their national community - a state in the spirit of the general human belonging spoken of by the Universal Declaration of Human Right.

RESPONSIBILITY OF OFFICIAL PERSONS IN RELATION TO CITIZENS AS CLIENTS

The state, as an organized community of people, is formed in order to provide order in society. By ensuring order in the society, it enables or rather should enable its citizens a safe life, freedom and security. It enables this through numerous organs and institutions established in all areas of social life. Those organs and institutions are formed to serve the citizens within the goals of the state as an organized community of people. They perform their function within the framework of their public powers prescribed by the laws of the state that regulate social relations in those areas. That is why they are public organs. In them work people - public servants and support staff (typists, hygienist drivers and others). The quality of the organs and institutions directly depends on the quality of the people. There is no organ, no institution is better than the people who make it up. Many experts in the field of constitutional and administrative law, and other public persons, make a mistake when they criticize the work of the organs and institutions of the state, forgetting the people, the public officials and employees who work in them. There is no responsibility of the public organs without the responsibility of the public officials and employees who manage them or work in them.

Officials employed in public organs, as public servants, should be aware that they work in the service of citizens; that the security of their life, their freedom and security within the state, depend, more or less, on their work. If they are aware of this, they will be in solidarity with the citizens as clients and will have an understanding for their problems and difficulties that life imposes on them. Solidarity is the essential basis of autonomous morality, and thus of the autonomous responsibility of public officials.

Solidary public servant places himself in the position of the client. Thus placed, he acts and decides with consistent respect for the principle of responsibility in the work of public organs.

In this connection, it is not out of place to mention the Old Testament principle that reads: "Do not do unto others what you do not want them to do to you." or the New Testament principle contained in the Gospel according to Matthew that reads: "Do unto people as you would have them do unto you."*****

***** See: Holy Scripture – Bible, Matt. 7/12.

These millennial moral principles are the foundation of autonomous morality, and thus of the autonomous responsibility of every person, and especially of the person - a public servant.

The laws, some directly and some indirectly, prescribe or have this principle in mind. Thus, the Law on the Organization and Work of the State Administration Organs prescribes that the state administration organs perform their responsibilities, in addition to others, on the base of the principle of responsibility.******

As for the attitude of officials towards the clients, this principle, although unfortunately not specifically prescribed, derives from the principles of the Law on General Administrative Procedure, and especially from the principle of service orientation of public organs, and from the principle of active assistance the client by the public organs. According to this principle, "The public organ is obliged to enable all clients in the procedure to exercise and protect their rights and legal interests in the most possible effective and easy way." The public authority informs the clients about the legal provisions that are important for solving the administrative work, about their rights and obligations, including all the information related to the procedure and warns them about the legal consequences of their actions or omissions.

The public organ allows the client to access him electronically. The absence of knowledge of the client participating in the procedure should not be to the detriment of his legal rights and interests."*******

This principle prescribed in this way, at least legally, excludes carelessness, recklessness and irresponsibility in the action of public organs, that is, ie in the work of officials who work in administrative procedures for the realization of the rights and legal interests of citizens.******** But, in practice, this principle is insufficiently applied, even though it is insisted on, a lot. It is natural that many clients in administrative proceedings do not know the path they should follow in order to exercise their rights and legal interests. If the organ conducting the procedure does not help such a client and does not instruct it, then the right of the client to active assistance by the organ remains only a legal declaration. This right enables a responsible and correct attitude towards the client. However, in order to realize that attitude, the official who conducts the procedure should help the client as much as it is necessary for him to exercise his rights and legal interests without difficulties and obstacles, and not only in the procedure until the adoption of the first instance solution, but also during the entire administrative procedure.********

RESPONSIBILITY OF OFFICIAL PERSONS TO THE PUBLIC ORGANS IN WHICH THEY WORK AND TO THE PUBLIC SERVICE

Man is a social being. He, from the beginning of his formation, as homo sapiens, throughout the many millennia of evolution, lives and acts in community with other people. Public organs are organized communities of people - public officials and support staff who work and act in accordance with the rules established by the laws and by-laws that regulate the performance of the public service. Knowledge and consistent adherence to those rules by public officials is a basic requirement for harmonious, and therefore, efficient and effective functioning of public organs in serving citizens in the areas of social life for which they were established.

The responsible public servant, as a member of the working community of the public organ in which he works, should be adorned with the following moral values: loyalty to the public organ, adaptability, collegiality, democracy and social maturity. Loyalty is, of course, the most important among these values. It is also a condition for nurturing and developing other moral values. Loyalty implies a developed sense of belonging to the public organ, solidarity and reciprocity in the relations with the rest of its members, unconditional acceptance of the duties and obligations arising from the competences of the public organ, especially those defined by the act on the organization and systematization of jobs in the organ, protecting the interests of the organ and subordinating their official interests to the interests of the organ.

The public servant should be proud of the fact that he belongs to the public organ and that, as its member, he contributes, with his work, to the efficient and legal realization of the constitutional freedoms and rights of the citizens as clients.******** The exercise of some of those freedoms and rights is often of

****** See: Article 3 of the Law on Organization and Work of State Administration Organs.

******* Law on the General Administrative Procedure, ("Official Gazette of the Republic of Macedonia", number 124/2015).

******** This can be concluded from the frequent debates about the work of the public administration and information in the media, where the service role of its bodies is invariably emphasized.

******** See: Marković B. (1977), Position and Role of the Client in Administrative Proceedings. Privredni pregled, Belgrade, p. 39.

******** According to Article 4 of the Law on the Organization and Work of State Administration Bodies, these bodies are obliged to provide citizens with the efficient and lawful exercise of their constitutional freedoms and

vital importance to the citizen. A public servant should not be proud by his position in the public organ, but by the works he creates in the performance of public service. He is tied to his organ not because of the position he occupies in it, but because of the service he performs in serving the citizens within the competences of the organ. The moment when the public servant will not be able to contribute to the performance of the tasks of the public organ, the performance of his public service automatically ceases. Understood in this sense, public service cannot and must not become a privilege followed by a feeling of irreplaceability of the public servant who performs it. From this nature of the public service and from this knowledge about its nature, every public servant, as an official, should strive to improve his work by acquiring new knowledge and thereby creates prerequisites for more efficient and effective performance of his works tasks, which, in turn, is a function of the efficient and effective realization of the rights and legal interests of the citizens, for which public organ decides within its competences. Only in this way the public servant will contribute to the efficient and effective performance of the tasks of the public organ and to raising his reputation, and thus also to raising the reputation of the public service in the state as an organized community of citizens and as their social environment.

CONCLUSIONS

Man's responsibility for his personality, as a purely psychological category and for his character as a moral psychological category, enters the sphere of the personal as part of his psychophysical structure.

Man's responsibility to himself and to his conscience, as a moral category, is a personal relationship. His responsibility towards other people and towards the community, in which he lives, is a social relationship. If it, as a social relationship, is regulated by legal norms, the very act of regulation creates it a legal relationship.

Officials, as public servants, are special within the framework of people, as general. As homo sapiens, they belong to the general - people, inhabitants of Planet Earth, and as public servants they belong to the special - officials employed in public organs. As people and as officials they have guaranteed rights to respect, reputation and dignity. These rights are guaranteed to them by the international legal acts on human rights and by the provisions of the constitutions of the states that comply with those acts.

The honor, reputation and dignity of officials do not have the same weight as those of ordinary citizens, but more. They are given the honor to serve the rest of the citizens and, by serving them, to decide or participate in the decision-making about their rights and obligations, some of which are of vital importance for the citizens. From that honor comes a higher degree of reputation and dignity. A higher degree of reputation and dignity requires a higher degree of responsibility before conscience as part of a person's autonomous morality.

Responsibility before the conscience as a set of moral attitudes and judgments of the social environment, accepted by the public servant, is his autonomous responsibility. Autonomous responsibility is a reliable guarantee for conscientious, high-quality, efficient and effective performance of official duties.

The quality performance of official duties implies consistent adherence to the other principles of the work of public organs, such as the principle of constitutionality and legality, the principle of objectivity, the principle of service orientation, the principle of efficiency, the principle of economy and rationality and other principles.

Autonomous morality, and within it, autonomous responsibility is established and developed through the processes of upbringing and education, first, within the family, and then, through education in educational institutions and through the process of socialization in the social environment.

But, unfortunately, a significant number of officials in public organs do not have, or do not have in sufficient degree, autonomous morality. This is supported by the frequent occurrences of bad attitudes of officials towards the clients, the large number of low-quality decisions in administrative proceedings against which the clients are forced to file complaints, and against those final, and lawsuits for initiating an administrative dispute, the almost regular occurrence of decisions for the requests and complaints of the clients after the expiration of the legal deadlines, the long waiting time for the issuance of the so-called real documents (certificates, extracts from the registers, etc.), as well as personal identification documents (identity cards, driver's licenses, travel documents, etc.).

This problem is solved by activating and intensifying the work of the control and protection services and institutions of society: the system of internal control in public organs, inspections, internal affairs organs, the State Commission for the Prevention of Corruption, the Commission for Protection against

rights. They, within their competence, ensure efficient and legal realization of the rights and interests established by law for all participants in the administrative procedure.

Discrimination, the Ombudsman, the prosecutor's offices and the courts.

These institutions initiate and conduct procedures for compensation of damage, disciplinary, misdemeanor and criminal procedures against the officials who violated the regulations that ensure high-quality, efficient and effective execution of the work of the public organs.

Officials who violated the regulations can bear material, disciplinary, misdemeanor and criminal liability. Appropriate sanctions can be imposed in the proceedings: an obligation to compensate the public authority or third parties for the damage done, then disciplinary, misdemeanor and criminal sanctions.

No one wants a procedure for material, disciplinary, misdemeanor or criminal responsibility to be initiated against him and to be sanctioned with an appropriate sanction. Officials in public bodies especially do not like that, because it damages their reputation and dignity, and even worse, by sanctioning, certain rights are taken away and limited. That is why officials try to avoid situations in which they can be subject to material, disciplinary and criminal responsibility. They fear such situations. Fearing and avoiding those situations, they work in accordance with the regulations that ensure quality, efficient and effective work of public organs. By this, actually, is achieved a heteronomous morality, and thus also a heteronomous responsibility based on the fear of sanction for wrongdoing.

From the above, it can be concluded, without a doubt, that the responsibility of officials, as public servants, is a supreme principle in the work of public organs. That is why this principle should be found prescribed in all laws that regulate social relations in all areas of social life in which public organs are responsible for serving citizens. Then, it should be found in all laws on procedural proceedings and in all by-laws: decrees, regulations and others, that elaborate separate provisions of the laws for the purpose of their execution. In the Macedonian legislation, the number of laws in which this principle is prescribed is small. In addition to the Law on the Organization and Work of State Administration Organs, it is found in the Law on Internal Affairs, the Draft Law on Ministry of Defense Employees, and it can rarely be found in other laws.

This principle, as a supreme principle, should be found in legal texts before other principles, because it is a condition for their implementation. Without responsibility, there is no service orientation of the public organs, no legality in their work, no objectivity, no efficiency, no economy and rationality, or, in short, no quality, efficient and effective service to the citizens by the public organs.

REFERENCES:

1. Alder J.,(2007), Constitutional and Administrative Law, Palgrave Macmillan, New York.
2. Constitution of the RNM,(2001), Special Edition, Fenix, Skopje.
3. Davitkovski B., Pavlovska – Daneva A.,(2018) Administrative Law, First Part – Material Law, Skopje.
4. Draft Law for Employees of the Ministry of Defense (2022), Ministry of Defense, Skopje.
5. Hristov A., (1981), Administrative Law, Institute for the Advancement of the Economy of SRM, Skopje.
6. Jovanovski Z., (2020), Administrative Law, Military Academy, Skopje.
7. Karadjoski M., (2020), Public - administrative cooperation in Europe, Faculty of Law, Kicevo.
8. Law on Internal Affairs (2022), Unofficial Revised Text, Ministry of the Interior, Skopje.
9. Law on the Organization and Work of State Administration Bodies ("Official Gazette of RM," No. 58/00).
10. Law on the general administrative procedure, ("Official Gazette of the Republic of Macedonia", No. 124/2015).
11. Law on Administrative Officers ("Official Gazette of the Republic of Macedonia," No. 27/14).
12. Marković B. (1977), Position and role of the party in administrative proceedings, Privredni pregled, Belgrade.
13. Thompson D., (2007), Political ethics and civil service, Službeni glasnik, Belgrade.
14. United Nation Basic Documents (1995), NIP "Nova Makedonija," Skopje.
15. Vitanski D.,(2020), Public and States Administration, University "St. Clement of Ohrid", Bitola.