ANNALS OF THE "CONSTANTIN BRÂNCUȘI" UNIVERSITY OF TÂRGU JIU
LETTER AND SOCIAL SCIENCE SERIES

ISSN-P: 1844-6051 ~ ISSN-E: 2344-3677

2/2020 ***https://alss.utgjiu.ro***

THE SOCIAL NETWORKS: RISKS AND BENEFITS FOR NATIONAL SECURITY

Elena DAJU

PhD student, University of Craiova, Doctoral School of Social Sciences and Humanities

Abstract: *SCIENTIFIC STUDIES AND THEORIZING HAVE ESTABLISHED TWO DISTINCT PERSPECTIVES ON THE INTERNET PHENOMENON: THE INTERNET AS A MEANS OF COMMUNICATION AND INFORMATION AND THE INTERNET AS A MEANS OF SOCIAL MANIFESTATION, THE SOCIAL COMPONENT OF THE INTERNET BEING AN INCONTESTABLE REALITY.*
THE ACT OF PRODUCING, ESPECIALLY IN THE CASE OF SOCIAL NETWORKS, CREATES A SITUATION IN WHICH PRIVATE INFORMATION BECOMES OPEN AND ACCESSIBLE TO ALL THOSE CONNECTED TO THE INTERNET.
THOUGHTS, OPINIONS, INFORMATION ABOUT STUDIES, HEALTH OR JOB, PERSONAL PHOTOS, ALL BECOME ACCESSIBLE BECAUSE PRIVATE INFORMATION IS POSTED ON A PUBLIC DOMAIN. OF COURSE, THIS RAISES A LARGE NUMBER OF QUESTIONS ABOUT SURVEILLANCE. WHO ACCESSES OR, MOREOVER, WHO STORES THIS INFORMATION? WHAT IS THE USE IN THIS ERA OF "KNOWLEDGE CAPITALISM", IN WHICH THE SEARCH FOR INFORMATION AND FORECASTING TECHNOLOGIES ARE PROMINENT?

Keywords: *SOCIAL MEDIA, INTERNET, INFORMATION COMMUNITIES, TECHNOLOGY, RISK, INFORMATION*

Contact details of the author(s): Email: elena.alimona.daju@gmail.com

WHAT ARE SOCIAL NETWORKS?

All online communication tools whose purpose is to facilitate the dialogue among users, Social Media, integrates technology, social interaction and creation through words, photography, video and audio. New Media, in a broad sense, encompasses all the innovative forms of digital technology and the ways in which these technologies and people interact. It is a virtual globalization that unifies domains and people with different nationalities, traditions and visions, what matters being what defines you in the interaction with others.

ISSN-P: 1844-6051 ~ ISSN-E: 2344-3677

2/2020 ***https://alss.utgjiu.ro***

If the inclusion of the Internet in the media area was done naturally, continuing the initial direction for which it was designed, its transformation into an environment of social manifestation, but, especially its involvement into the virtual reality has caused much controversy. From computer simulations and virtual environments developed in the 1980s for various technical applications, it has moved fast enough to postulating a new dimension of humanity: cybersociety.

Social media has changed the way we live, from the way we receive the news to the way we interact. Currently, social media is an inevitable, strong and constantly evolving environment - according to Emarsys, quoted by businessdays.ro, there are 3.2 billion social media users who are active every day, which means about 42% of the population world.

According to Business Days also, which on 23.10.2020 presents 25 statistics on social media this year, the most accessed social platform in Romania is Facebook for all ages, 61% of the online population aged between 16 and 74 years representing daily users. Almost all Facebook users in Romania access the platform through mobile devices. Instagram is more used by the 16-34 age groups, which also applies to Snapchat and Pinterest.

Social accounts are accessed several times a day, in an analysis made by the Global World Index concluding that individuals spend an average of 2 hours and 22 minutes on social networks.

According to HubSpot research, out of a total of 2.6 billion Facebook accounts, 3 billion profiles are fake; applications and websites use Facebook 53.1% of the time for social connection opportunities; since April 2020, 29% of adults between the ages of 18 and 29 use Instagram; 2 billion YouTube users watch an average of about 5 billion videos every day, and since January 2020, 93% of the most viewed videos were music videos.

THE NEED FOR INSTITUTIONAL ADAPTATION OF SECRET SERVICES TO THE EVOLUTION OF SOCIAL NETWORKS

In the early 2000s, none of the CIA analysts still had an Internet connection. Spreading the attention of the secret services to the web has not been without obstacles, as the old guard of analysts looked at the Internet with distrust. That is why the agencies have called on young recruits from universities and the private sector to make this adaptation. On the occasion of this rejuvenation, the information work was computerized, investing in specialized startups.

Information communities have begun to valorify the social networks, such as Facebook, to allow staff, divided into several geographically remoted agencies, to collaborate in real time.

Currently, information agencies have their own social networks, which ensure real-time communication, multimedia content broadcasting to many users on very specific topics and quickly contact of a specialist located at the other end of the world in order to use his/her skills. Used in the analytical field, it facilitates the maintenance of a certain cohesion in the information community, the initiation of some debates, the stimulation of the reflection among the analysts, but also the presentation for analysis of some complex subjects.

Social networks also favor the rapid establishment of teams of experts in a crisis situation.

The call on the open sources is an old practice for information services, and the appearence of the Internet has been fully exploited by agencies. In search of sensitive information, structures are created inside the agencies through which social networks and blogs are monitored.

The world of information services has evolved from the concept that every soldier is a prisoner, to the fact that every Internet user is a prisoner, a state generated by the way the technique has been assimilated in human terms. The mobile phone, for example, has become indispensable for most people. Even since 2008, the mobile Internet has brought record traffic to social networking sites (during that period, the mobile phone company Orange announced that 640 thousand of its customers accessed social network sites using mobile phones, thus generating over 166 million posts each

month.The total number of monthly checks or updates of the pages of these sites, generated by a single user, averaged rises up to 260, with an average daily of eight hits).

The following years have accentuated these trends, especially due to the so-called "user generated content", content created by users (blog, music, fims). Mobile phones are made with a focus on blogging. Not only that people can write directly on their personal diary pages, but they can take photos or videos that can be added directly to their personal website in the correct format.

APPROACHES AND OPPORTUNITIES FOR INTELLIGENCE

Thanks to the multitude of information made available to the public, social networks can prove to be the basic tools of the secret services.

Like any community, these networks allow the collection of information from areas of interest for Intelligence, they are used as a recruitment tool - both in the sense of attracting new agents (networking sites giving candidates the advantage of getting acquainted with aspects of the life of the organization), as well as attracting to collaboration of the human resources, can be a favorable framework for operational games. They, thus, represent an operations theatre, where one can intervene through complex, combinate measures, where one can resort to intoxications, manipulations in order to generate reactions or to penetrate the intimacy of hermetic organizations.

The launch of institutions in the field of national security and public order on social networks is also seen as a means of communication with the civil society, by the virtue of the principle of improving the relationship between citizens and institutions but also strengthening inter-agency cooperation with the private sector and the academic environment.

The recruitment and management of the agency, the correspondence interception, the surveillance of media and backgrounds, the inter-agency information exchange, geolocation of some persons, documentation takes place in the virtual space too - as methods, means and procedures specific to the secret services, according to the same rules of conspiracy , the great advantage being an even better conspiracy but also ensuring a high degree of efficiency (especially in the case of inter-institutional cooperation).

Fearing possible repercussions, in real life there is much reluctance of citizens to complain about antisocial facts or to say that they have witnessed such facts and they have clues that could help investigators. On the Internet, however, anonymity inspires courage, with users being more willing to cooperate.

Another opportunity offered by social networks is the possibility of launching some topics for discussion and reflection, action through which currents of opinion are identified and experts in extremely precised issues are located, who can be, subsequently, the object of some recruited and / or protection activities. The proposed topics of discussion and reflection can also represent test balloons, by evaluating the reactions of the population to which government policies and strategies can be oriented towards.

Last but not least, the secret services have set up virtual closed-circuit networks, which facilitate the communication among agents, spread in all corners of the globe, the dissemination of multimedia content, the rapid creation, in crisis situations, of some teams of experts to evaluate facts and identify optimal intervention measures. It has been shown that such virtual communities increase the cohesion of professional groups and improve internal communication.

RISKS FOR THE NATIONAL SECURITY

It is well known that any secret service community has a double goal: achieving national security and espionage. It turns out, of course, that in espionage actions any information service can use the algorithms listed above to gathering the information from the social networks. At the same

ISSN-P: 1844-6051 ~ ISSN-E: 2344-3677

time, it is clear that the sources and generators of information in a given country are also in the attention of adverse services or criminal, terrorist groups. Hence, the imperative of avoiding sensitive information leakage, that could reach the enemies, endangering thus the national security.

Although allies in combating crime and achieving professional goals, social media and the Internet in general can harm the secret services, the main risk being the uncovering of some actions and facilitating the actions of criminal organizations.

Social networks have opened unprecedented gates of interpersonal communication, offering new ways to share information about oneselves and own lives to others, bringing new marketing methods to companies, offering new means of belonging to groups that share the same ideals, regardless of physical distance between people. In a word, they formed new territories in the real world, based on the affinities of individuals.

Like any technological innovation, they have brought with them new ways of manifesting of criminal groups and new tools for committing crimes, as they have generated new types of crimes, and for the authorities in charge with fighting crime have put and continue to put countless new problems.

Among the most common ways of using these networks for criminal purposes are:

- Recruitment and promotion activities: in the case of terrorism, we can already talk about a history of using these networks to recruit new members and followers and their indoctrination.

Authorities in some states, for example, have been put in a position to try to close Facebook pages opened by local criminal groups, pages in which they apologize for antisocial acts by promoting a certain attitude towards the influential youth in order to identify new recruits. The same type of activity applies to terrorism too.

- planning criminal activities through the social media, coordinating them or even carrying them out on social media.

The area of monitoring that is far too wide for the real capacity of the law enforcement has made social media an ideal environment for planning and coordinating criminal activities when it comes to crimes that have a transposition in real life as well as a favourable environment of masking the crimes committed even in the digital environment, such as the spread of child pornography.

- new forms of classic crimes and new types of crimes: in this category we could include a wide range of activities, starting with the types of fraud based on the carelessness or the insufficient information of the Internet users in case of phishing attacks, carried out through the social media in which the criminals manage to obtain the important data, such as the passwords of these users or access to the bank accounts; crimes based on the users credulity in the case of scams based on, for example, marriage vows, with the selection of the victims on the social networking sites following the so-called sentimental relationships via the Internet and the subsequent obtaining of large sums of money from them; other types of aggression against people or their own representatives in the digital environment (this category includes an extreme side of complaints, made at the police of people who accused the aggression of their avatar in the game of Second Life or even theft of items bought by them in the game using real money);

- collecting personal information about the potential victims: publishing of personal information on the Internet, about the daily leisure or company activities, listing the close friends, publishing personal photos with oneself and children and many other similar elements, made from social media an inexhaustible source of information for criminals, of studying the lives of the next victims and planning crimes.

- the spread of botnets and Trojans to obtain confidential information and access to company networks: the use of social networks in the workplace in the absence of a strict company policy on Internet access or accessing the company network on the same computer we use in the free time to access other sites on the Internet, may run the risk of leaking confidential information such as access

ISSN-P: 1844-6051 ~ ISSN-E: 2344-3677

2/2020 ***https://alss.utgjiu.ro***

passwords to the company network or email accounts when that computer is infected with one of thousands of Trojans capable of registering the data entered from the keyboard, data including access passwords too. Once in the hands of criminals, those data open the criminals the door to access confidential company information.

We've all heard of viruses that take over our personal online accounts and send messages on our behalf to all our friends. The common feature of these messages is to provide entry to an Internet address under the pretext that it is recommended by a friend, an address that, once visited, infects friends' computers with the same Trojan capable of stealing personal data. How to access criminals' own accounts? By the fact that these viruses registered and provided to the criminals the password and account data that the victim typed in order to access the email or social media pages.

The enumeration can continue, daily discovering new ways in which social media is used for planning or committing of reprehensible or punishable acts by criminal law.

The most important common features of this environment and the most favorable features for crimes in the digital environment are:

- the huge territory that should be investigated to gather evidence for incrimination;
- the lack of education of the population regarding the providing of personal data and details about privacy in these environments and the false impression that some personal data once provided on the Internet can be deleted at any time;
- lack of discipline in companies regarding the policy of using the Internet at work;
- insufficient protection of the personal computer and the use of public terminals in order to access important personal accounts.

The information services, in their efforts of achieving the national security, using as a source and a theatre of operation the social networks must never omit that the same territory is targeted, monitored and used by the adverse services, the latter approach being predominantly offensive. Therefore, the level of exposure on social networks to sensitive issues for national security must be constantly assessed, and at the same time the access of adverse services to such content must be blocked.

CONCLUSIONS

Social networks have developed and expanded at the same time as the interest of the secret services towards them and with the improvement of the monitoring methods and tools. By researching the social networks, the secret services obtain valuable information, with a high degree of veracity, which they can compare /verify with those from the effective social communities, while being able to act operatively.

Paradoxically, over time it has been possible to see the increased artificialization of the interpersonal relationships developed in classical environments, in effective social communities, simultaneously with the progressive humanization of the connections mediated by social networks. On the social networks, people are more and more open, restraintless, sociable and, more and more, more present. Or, where there are people, special services must be present too, first of all to protect their fundamental rights and freedoms.

For more than 10 years now, social networks have been anticipated to become the main points of influence on the Internet; that interconnection and socialization will be achieved by logging in with a username and password everywhere; to achieve the decentralization of the information and the transfer of power from sites to users (active users, opinion leaders in social networks to become the next celebrities of the Internet pages, surpassing bloggers, journalists or online celebrities); that economic life should powerfully adapt to the online environment (that brands should change their promotion strategy, investing more time and money in the online presence); for new media to provide

ISSN-P: 1844-6051 ~ ISSN-E: 2344-3677

real-time information when the event happens; as the number of Internet users on the mobile phone increases, so does the phone of the future be all-in-one devices, so that the Internet of the future is a mobile one.

All these developments in social media are accompanied by transformations within the information communities, which are forced to respond synchronously and capitalize on the optimal level of opportunities offered by the social networks.

Currently, a hot topic for both the simple user and for the intelligence service is represented by the appearence of the latest 5G technology, event overlaid somehow over the pandemic event generated by the new coronavirus and the threats that such health risks will be frequent in the future.

With the advent of a new era of the Internet, it is not possible to accurately predict its effects on lives in general - how significantly the inter-human relationships will be transformed, the dangers to stability (how strong or weak the criminal organizations will become), the approach towards trust, freedom, the willingness to accept the risk of an increasing monitoring.

About 5G technology, which is the fifth generation of technology for wireless cellular networks, the industry service providers claim that it will mainly lead to faster Internet browsing, to a better video call quality, to a great stability of the connection in crowded places, to a new experience in playing Virtual Reality content or high-resolution games, applications, websites and smart home devices that can be accessed almost instantly. It will also lead to the facilitation of teleworking, a way of approaching the indispensable professional activity during the pandemic.

According to the results of a study conducted in November, the current year by Motorola and the research company Cult Market Research, 48% of Romanians intend to buy a new phone next year, in order to have access to 5G technology.

There were reports in the media that secret services in several countries, such as New Zealand in 2108, rejected the offers of the local operators to provide 5G services using Huawei equipment, motivating with the risks for the national security. It has been accused that unlike the previous networks, 3G and 4G, in the case of 5G each component of the network can be accessed, being vulnerable to espionage, existing suspicions that the Chinese government is using Huawei for espionage activities, being known the fact that Ren Zhengfei, the founder of the company, had worked in the past as an engineer in the Chinese army.

ISSN-P: 1844-6051 ~ ISSN-E: 2344-3677

2/2020 ***https://alss.utgjiu.ro***

REFERENCES

Troncotă, C., (1999). The history of the Romanian secret services. From Cuza to Ceausescu. Bucharest. Ion Cristoiu SA Publishing House

Dâncu, V., S., (1999). Symbolic communication. Advertising discourse architecture. Cluj-Napoca. Dacia Publishing House.

Nitu, I. (2012). Bucharest intelligence analysis. RAO International Publishing Company Johnson, L., K. (editor). (2012). Handbook of National Security and Intelligence. Oxford. Oxford University Press

Troncotă, C. (2008). Security studies. Sibiu, "Lucian Blaga" University

Klador, M. (2007). Human Security. Reflections on globalization and intervention. Cluj Napoca, CA Publishing Publishing

http://www.dictsociologie.netfirms.com/

http://www.euractiv.ro/uniunea-europeana/articles|displayArticle/articleID_16453/eTwinning projects-Creativity-Innovation-and-socialisation-in-schools.html

http://www.zdnet.fr/actualites/reseaux-sociaux-la-formation-des-salaries-est-strategique-pour-limiter-les-risques-en-entreprise-39750681.htm

25 statistics regarding the social media în 2020 (businessdays.ro);

(New Zealand rejects use of 5G services provided by Huawei due to security risks natiziare.)