

Отже, складна ситуація зі збереженням прайвесі в соціальних мережах і при користуванні Інтернет-пошуковиками, а також інтерактивними мультимедійними додатками ставить складні запитання як перед творцями Інтернету, так і перед глобальною Інтернет-спільнотою: як зберегти право на свободу слова, право на комунікацію в глобальній громадській комунікаційній сфері, уособленням якої сьогодні великою мірою є Інтернет, як не перетворитися на об'єкт для стеження, аналізу та використання різними інституціями – від спецслужб до маркетологів і рекламодавців.

Можна підсумувати, що введення механізмів стеження в серцевину глобальних диджитальних комунікацій серйозно загрожує правам людини в диджитальному еру. **Всі нові форми децентралізованої влади відбивають фундаментальні зсуви структури інформаційних систем у модерних суспільствах.** І кожен крок у цьому напрямі повинен бути розглянутий і широко, і глибоко, і транспарентно.

Global Social Network and Cybersecurity of an Individual

At the beginning of the XX century social networks became very popular. People use them to keep in touch with their families and friends. These are such global social networks as *MySpace*, *FriendWise*, *FriendFinder*, *Yahoo! 360*, *Facebook*, *Orkut*, *Classmates*, etc. There are also own social network services in every country. In the United States, for example, many users have *LinkedIn* to have different business contacts and to follow the possibilities in their career developments.

But not all understand that using the Internet in the times of social media, or like it is already called *Web 2.0* (*blogs*, *wikis*, *file sharing*, *social networking sites*, *microblogs*), carries in itself many threats for the users of the Internet. "During the recent years it has transformed from the system, which was oriented foremost on the supply of information, to the medium for communication and development of communication" [1].

Concept *Web 2.0*, social software, sites of social web such as *Facebook*, *Twitter*, *MySpace*, appeared in this context. Together with these platforms the enormous amount of personal information was formed and is stored, and which is systematically estimated and used by advertisers to look for their target users.

In the world of global economic competition, crisis and fear of terrorism and corporations, the state institutions have all greater interest to this personal data as well. Therefore the following questions become of great importance:

- how the environment changes in this sphere;
- how the gathering of commercial personal data for advertising is done;
- how the sites for users and interactive medias are correlated;
- how self-revelation is done in social networks;
- how those who make exchange of the files are watched;
- how privacy is interpreted in the time of the Internet;
- what the civil surveillance after the sites of social networks and the network surveillance in the transnational space mean.

Site "What is social network?" [2] acquaints the users in an intelligible form with the dangers that are waiting for imprudent users in the social networks. It is felt that its target audience is the youth. The conversation goes from the first person: "I am sure that you all are well-informed about the presence of dangers related to the social networks, including the theft of information and viruses. The most dangerous are on-line predators or individuals

Список використаних джерел:

1. Internet and Surveillance / Ed. by C. Funch, K. Boersma, A. Albrechtslund and M. Sandoval. – New York: Routledge, 2011. – 332 p.
2. What is Social Networking? [Електронний ресурс]. – Режим доступу: <http://www.whatissocialnetworking.com>
3. Как повысить безопасность ваших фоторафий в «облаке»? [Електронний ресурс]. – Режим доступу: <http://www.inosmi.ru/world/20140904/222797438.html>
4. Федеральные власти и *Yahoo* [Електронний ресурс]. – Режим доступу: <http://www.russian-bazar.com/ru/mnews/156958.htm>
5. Кіркпатрік Д. Ефект *Facebook*. Внутрішня історія компанії, що об'єднує світ / Д. Кіркпатрік. – К.: Темпора, 2013. – 488 с.
6. *Gillmor D.* The New Editors of the Internet / D. Gillmore // *The Atlantic*. – 2014. – 24 August.

who pretend to be someone whoever they are not in actual fact. Exactly the same pieces of advice as those which relate to the situations when you meet a stranger in a club or bar, at school or at work, will be useful in order to feel safe online". Further you will find the concrete rules on how you should behave in the cyberspace:

- create your personal media-privacy space so that only your friends could see your profile and content;
- do not accept invitations to become friends from the strangers;
- do not make your daily curriculum of businesses public;
- do not give people the possibility to know when you are not at home;
- do not use the locally based services as *Facebook Places* and *Foursquare* which show your place of stay automatically;
- do not show the pictures of your family (especially kids) or expensive things which you have in your house;
- ask *Google Maps* to make the vague photos of your house, car or anything that is private for you in order to be shown in public.

It's clear that these pieces of advice are written for the young generation but they concern everyone. But the pieces of advice published by the American influential newspaper *Washington Post* are foremost for solid audience. After the scandal in 2014, when hackers made public the intimate pictures of the Hollywood stars which were stored in *iCloud* service, the *Washington Post* newspaper published on its site a few pieces of advice how to protect the information [3]:

1. Make sure that any of your photos did not get in iCloud without your consent.

The thing is that some companies like *Apple*, *Microsoft*, *Dropbox* offer to store the pictures from your telephones or tablets in "cloud" automatically.

2. Use two level auto identification.

This procedure will help you to protect your accounts better with the help of additional short code, in addition to the password at the entrance.

3. Avoid the traps of hackers.

Hacker attacks often become successful not due to high technologies but due to cheating the victims who finally give the necessary data to abusers.

But not only hackers pave the way to disclose the data of Americans. It is also done by the federal institutions of the USA. They compelled the known Internet-searcher *Yahoo* to give them access to the confidential data of its users,

threatening to penalize the company by 250 thousand US dollars on daily basis. It was published by the administration of *Yahoo* in the Internet-blog of the company.

The company, once it had received the leave of the court, published 1.5 thousand pages of documents related to the court claim against the National Security Agency (NSA). Legal adviser of *Yahoo* Ron Bell added the proper comments to this publication. From the documents it is clear that the attempt of the National Security Agency to get access to the personal information became possible only in 2007 when the amendments to the legislation of the USA were made, which enabled the power to require from the Internet companies information about the users.

At the very beginning *Yahoo*, as R. Bell asserts, refused to execute the orders of the National Security Agency, considering them to be against the Constitution. The company brought the case against the Agency before the court law which carries the observant activity over the secret services, and asked to cancel such unconstitutional requirement. But this court mostly takes the side of the power, that is why the company defeated after a year and half fight.

The requirement of the National Security Agency was to get meta-data about the users of its e-mail from the company. These data enable to see between whom and when the exchange of messages takes place. At this the special services have never had a permit to have access to the letters, as asserted in *Yahoo*. In summer 2013 most Internet companies of the USA, which took part in transferring data to the National Security Agency, appealed to the court with a requirement to allow them to publish the statistical information about the queries of the special services. The first publication of such information took place in February 2014. Presently the Internet companies try to approve at the Congress the law which would protect confidentiality of private correspondence [4].

In summer 2013 the letter from the organizations of the civil society of the world to the Congress of the United States about the Internet and telecommunication surveillance was published in the Internet. This concerned: "We write as a coalition of organizations of the civil society from the whole world in order to express our serious concern about the numerous examples of surveillance after the American and non-American citizens. We concern greatly that the data, which are gathered during the surveillance in the United States, is then passed to other states, in particular to Great Britain, Netherlands, Canada, Belgium, Australia and New Zealand. Many American companies of a global significance do the same".

As we can see, the group of mighty global Internet companies, which are all around the world, co-operates with the special services, although, when they only entered the market of information and communication services, they promised complete privacy to its users. What it can transform into we can see on the example of the biggest in the world social network *Facebook*.

Social network *Facebook* crossed the limits of the country, the region, and reached the global scales. What is the secret of its success in the world? *Facebook* essentially differs from all other Internet companies which preceded it, at least that in theory and practice it is based on the real information about a person. "It is important to be yourself here. In the Internet all long time ago got used to anonymity, roles, pseudonyms, nicknames... But here all this is needless. If you invent some image for yourself or behave too artificially, there is nothing to do for you in *Facebook*. Be yourself, otherwise your friends will not recognize you or will not accept you as a friend. Here one can quickly understand who you are in actual fact through only checking up the list of your friends. Exactly they are your certificate of identity", – Donald Kirkpatrick, who wrote a book about this company, marks [5]. He reflects about social and psychological changes caused by the effect of *Facebook*. He understands that there is still not enough scientific information to talk with confidence about such changes, but he marks that for many people

Facebook is a source of a false sense of unity (5000 persons – maximum amount of friends) which in the course of time degenerates into deep loneliness. Besides, he raises a question: don't young people who days and nights stay in *Facebook* lose their ability to be glad and surprised with what takes place in the real world and surrounds them every day?

In the course of time the euphoria from finding the old friends and acquisition of new ones disappears, and publishing in *Facebook* of "funny" pictures from parties, where the tricks of students were often captured by their friends without consent (that is, the pictures where friends keep bottles or glasses in their hands, where there are people with drunk faces, where there are moments when young people took light drugs, and other compromising photos got into the social network), not only start to irritate those who found themselves in them but also became a serious obstacle in their career development. In fact, many companies, public institutions and firms, before hiring the applicants, watch their life and behavior in the cyberspace, in particular in social network *Facebook*, where they are presented in different posing under their real name and last name.

The questioning conducted among the American employers in 2009 showed that 35% companies refused to employ the applicants because of the information found about them in the social networks. First reason for the refuse: placing of edgy pictures or unworthy information [5, p. 276]. The universities started to do the same because the age of those who can have access to *Facebook* was reduced to 13 years old. Now during the introductory campaigns, the members of the registering administration at the universities and colleges also check the social networks.

Mark Zuckerberg is a convinced adherent of the "open and transparent world". He considers that while acknowledging openly our essence and treating all friends the same way, "we create a healthy society". But the amount of people, who think that making private information public in *Facebook* becomes surplus, grows in course of time. In actual fact, as D. Kirkpatrick testifies, "Zuckerberg does not believe in total openness as well. He does not write about his confidential meetings in his profile" [5, p. 274].

The real policy of his company proves that *Facebook* makes users share their own information, although the reason for that is innocent enough aspiration "to create more safe, more reliable version of the Internet, where people are aware of the consequences of their acts, where they use their real names".

External experts do not support these thoughts of Zuckerberg. Here is the opinion of one of them – Mark Rotenberg, acting Head of Electronic Privacy Information Center (EPIC) and experienced "watch-dog of the Internet", who writes that every year *Facebook* creates all more obstacles on the way to protect the privacy of its users. They are simply deprived of the ability to control the privacy of information, and *Facebook* itself, without regard to the persuasion and adherence to transparency, does not show transparently enough what it does with our data.

Violation of confidentiality from the side of *Facebook* has impact not only on the university entrants and graduating students of the universities. It is also a great threat for politicians and officials of higher grade, as it can ruin their careers. Political candidate from Canadian Vancouver withdrew his candidacy when there appeared a picture in the newspaper where two people put on his underpants. Jon Favreau, a speechwriter of Barrack Obama, was condemned in public when the picture appeared in some blog where he at one of the parties touches the breasts of cardboard Hillary Clinton. The picture was published by one of his friends in *Facebook*... Possibly, B. Obama thought exactly about the incident with Favreau, when he was coming forward before senior pupils in Virginia in spring 2009: "Be careful with what you publish



in *Facebook*, – he warned, – because in the era of *Youtube* everything can one day unexpectedly come out. And being young, you do many dumb things”.

With the development of social networks the problems of confidentiality appear to be of more importance. People whose work requires secrecy suffered from its transparency. For example, after it was announced in Great Britain in the middle of 2009 that Sir John Soars would be the Head of the Center of Counterintelligence – Secret Reconnaissance Service (once known as *M16*), the newspaper *Daily Mail* found public pictures of him with his wife, published by his wife in *Facebook*. There were pictures from holidays, photos of friends of the family and the details of where he lived and what he did.

The example of a celebrity of the world caliber, who violated the model of *Facebook*, is Bill Gates, who closed his personal profile in the social network at the beginning of 2008.

Consequently, there is a dilemma: people want to spread their personal information everywhere, to be popular, but at that they would like to be protected from an unexpected disclosure which can have a negative impact on them. The problem is that a negative impact can be caused by the undesirable disclosure of information made by a person who was added as “a friend” of a user – so it turns out to be a friendly violation of privacy. In order to prevent the publication of edgy pictures in the social network, in the United States during the recent years it has been forbidden to use a camera at the university parties, and there are even special dark rooms in some establishments where nobody will be able to capture someone drinking alcohol or smoking weed. From the other side, such preventive measures make us think: does *Facebook* really help to develop “transparent and open society”, if dark rooms appear in order to hide not the best human displays? Does not it lead to the appearance of double standards of morality?

Initial assignment of *Facebook* as of a place where one could find the friends from the real world was constantly moved aside to a back seat. Important event in the development of the site was the appearance of pages of the companies (not friends). Now their updates appear in the news feed next to the news from friends. No matter how marketing specialists of *Facebook* tried to characterize positively this step, it is obvious that the company becomes commercial and monetized. It gets enormous revenues exactly due to advertising – to only one way to become a real business-company. Due to that *Facebook* turned into one of the best advertising environment of nowadays. Besides, the information which it has about its users is “a pot of gold” for market researches, for the creation of target advertisement. Exactly these strategies helped *Facebook* to cope quietly with the global financial and economic crisis of 2008 and to become a public company.

Power of *Facebook*, its potential and ambitions in relation to the control over users and the platform are at least the same as *Microsoft* used to have, but *Facebook* controls its own platform more than *Microsoft*. “*Facebook* can push the button and turn you off. All of you. Whenever” [5, p. 446]. The author marks, if to think drastically, *Facebook* can take the key functions of the governments. He quotes I. Milner, Russian investor of the company: “*Facebook Connect* is in general your passport, your on-line passport. Passports are issued by the government. One more institution, which deals with that, appeared. That is how competition appears. But who said that only the government can issue the passports? We will simply get to a global citizenship”. The question is whether all users of *Facebook* want to have a global citizenship? Is it an ultimate goal of M. Zuckerberg who from the beginning of the start of the site was more interested in the growth of the amount of users than in the growth of revenues? Are the governments of the world countries interested in delegating their plenary powers to *Facebook*? And after all, when one private company of a global scale has information about

the majority of population of the Earth, does not this mean that it has a soft domination (monopoly) in the modern world, the domination many effects of which are unknown to anybody, except for Zuckerberg, but, probably, they are unknown for him as well?

Most probably, Mark Zuckerberg knows about these global effects very well. As of 2015 his financial position was USD 33.4 milliard. The changes which took place during one year added USD 3.4 milliard more for him. According to Forbes rating, he occupies the 16th place among the richest people of the planet. Well, the founder and Director General of *Facebook* continues to manage his company up to the market records, except that the social network gradually becomes an anachronism for part of young audience. In 2014 the profit of Zuckerberg increased by 58% due to the best payout from the mobile advertising. The audience of the company is about 1.4 milliard people in the whole world who watch 3 milliard videos every day. 300 million users accumulate their photos in *Instagram* which belongs to this network, and 700 million people use messenger *WhatsApp* which was purchased in 2014 for record USD 19 milliard.

Where is young Mark who dreamed about the transparent Internet and the absence of advertisement in to the social network created by him? Cruel laws of market competition brought him over to the pool of a small group of big Internet companies where he appeared to be a leader.

Dan Gillmor in the article “The New Editors of the Internet” asks: “Who gave them this power? We did. And if we don’t take back what we’ve given away—and what’s being taken away—we’ll deserve what we get: a concentration of media power that will damage, if not eviscerate, our tradition of free expression” [6].

Consequently, the difficult situation with the maintenance of privacy in the social network services and while using the Internet-searchers and also interactive multimedia applications puts complicated questions to both the creators of the Internet and the global Internet-association: how to protect the right to freedom of speech, right to communication in a global public communication sphere, personification of which today to a great extent is the Internet, how not to become a marked man, how to avoid being analyzed and being used by different institutions – from the secret services to marketing experts and advertisers.

We can summarize that the introduction of mechanisms of surveillance to the core of global digital communications really threatens the human rights in a digital era. **All new forms of the decentralized power reflect the fundamental changes of the structure of the informative systems in the modern societies.** And every step in this direction must be considered intensively, deeply and transparently.

References

1. Internet and Surveillance / Ed. by C. Funch, K. Boersma, A. Albrechtslund and M. Sandoval. – New York: Routledge, 2011. – 332 p.
2. What is Social Networking? – Available at: <http://www.whatissocialnetworking.com>
3. Kak povysit bezopasnost vashykh fotografii v “oblake” [How to Further Safety of your Photos in iCloud?]. – Available at: <http://www.inosmi.ru/world/20140904/222797438.html>
4. Federalnyie vlasti i Yahoo [Federal Authorities and Yahoo]. – Available at: <http://www.russian-bazar.com/ru/mnews/156958.htm>
5. Kirkpatrick D. (2013) “Efekt Facebook. Vnutrishnia istoria kompanii, shcho obiednuie svit” [Effect of Facebook. Internal History of the Company which United the Whole World]. Tempora
6. Gillmor D. The New Editors of the Internet / D. Gillmore // The Atlantic. – 2014. – 24 August.