JEL O31,32,33,34

PhD Dariusz Prokopowicz

Institute of Sociology, Faculty of History and Social Sciences,
Cardinal Stefan Wyszynski University in Warsaw
(Warsaw, Poland)
darprokop@poczta.onet.pl

THE QUESTION OF THE SECURITY OF FACILITATING, COLLECTING AND PROCESSING INFORMATION IN DATA BASES OF SOCIAL NETWORKING

KWESTIA BEZPIECZEŃSTWA UDOSTĘPNIANIA, GROMADZENIA I PRZETWARZANIA INFORMACJI W BAZACH DANYCH PORTALI SPOŁECZNOŚCIOWYCH

ВОПРОС О БЕЗОПАСНОСТИ ОБМЕНА, КОЛЛЕКЦИИ И ОБРАБОТКИ ИНФОРМАЦИИ В ОСНОВЕ ДАННЫХ СОЦИАЛЬНЫХ ПОРТАЛОВ

Abstracts

In recent years, The number of companies that have been collecting personal information for marketing purposes has grown. Then, they have been reselling it to other companies, banks, institutions. In this way, enterprises, financial and public institutions create huge collections of nonpublic data that are valuable information for taking marketing enterpises. By targetting appropriately profiled product and service offer at a selected group of receivers; trading partners and potential clients, a greater effectiveness used in the marketing strategy is achieved suitably Thereupon, multifaceted and informational personal data base, which are built in institutions, enterpises and social networking sites, become a valuable source of informaton used for the marketing purposes. The development of information processing and dissemination techniques through the Internet is determined by the many conveniences for beneficiaries, customers and users of services offered by the Internet. On the other hand, the development of information technologies on the Internet carries the risk of loss or theft of information by an unauthorized entities. The process of facilitating information online generates a number of threats related to identity theft, capturing nonpublic data by hackers, and accomplishing conversion of funds in the electronic system banking. In response to these threats, specific entities expand security systems for remote facilitating of information and making transactions via the Internet.

Keywords: *Internet, social networking sites, internet companies, technology companies, information facilitating, website, internet server, information service, cyberspace.*

Streszczenie

W ostatnich latach rośnie liczba firm, które zbierają dane osobowe w celach marketingowych a następnie je odsprzedają innym firmom, bankom, instytucjom. W ten sposób przedsiębiorstwa, instytucje finansowe i publiczne tworzą ogromne zbiory danych niejawnych stanowiące wartościową informację na potrzeby podejmowanych przedsięwzięć marketingowych. Poprzez kierowanie stosownie sprofilowanej oferty produktowej lub usługowej do ściśle wyselekcjonowanej grupy odbiorców, kontrahentów, segmentu docelowego potencjalnych klientów uzyskuje się większą skuteczność zastosowanej strategii marketingowej podczas kampanii reklamowych. W związku z tym budowane w instytucjach, przedsiębiorstwach, w tym także w internetowych portalach społecznościowych rozbudowane wieloaspektowo i informacyjnie bazy danych osobowych stają się cennym zasobem informacji wykorzystywanej na potrzeby marketingu. Rozwój technik przetwarzania i udostępniania informacji poprzez Internet zdeterminowany jest wieloma udogodnieniami dla beneficjentów, klientów i osób korzystających z oferowanych przez Internet usług informacyjnych. Z drugiej strony z rozwojem technologii informacyjnych funkcjonujących w Internecie wiąże się także ryzyko utraty bądź kradzieży informacji przez podmioty nieuprawnione. Proces udostępniania informacji poprzez Internet generuje wiele zagrożeń związanych z przestępstwami kradzieży tożsamości, przechwytywania przez hakerów danych niejawnych oraz dokonywania malwersacji środków pieniężnych w systemach elektronicznej bankowości. W odpowiedzi na te zagrożenia poszczególne podmioty rozbudowują systemy bezpieczeństwa zdalnego udostępniania informacji oraz dokonywanych transakcji realizowanych za pośrednictwem Internetu.

Słowa kluczowe: *Internet, portale społecznościowe, firmy internetowe, firmy technologiczne, udostępnianie informacji, strona internetowa, serwer internetowy, serwis informacyjny, bezpieczeństwo w cyberprzestrzeni.*

Аннотация

В последние годы растет число компаний, которые собирают персональные данные в маркетинговых целях, а затем продают их другим компаниям, банкам и учреждениям. Таким образом, предприятия, финансовые и государственные учреждения создают огромные коллекции секретных данных, предоставляя ценную информацию для нужд маркетинговых предприятий. Получая надлежащим образом профилированный продукт или предложение услуг тщательно отобранной группе получателей, подрядчиков, целевого сегмента потенциальных клиентов, повышается эффективность маркетинговой стратегии, применяемой во время рекламных кампаний. В связи с этим базы данных, созданные в учреждениях, предприятиях, включая сайты социальных сетей, многогранную и информативную базу данных, становятся ценным ресурсом информации, используемой в маркетинговых целях. Разработка методов обработки и обмена информацией через Интернет определяется многими возможностями для бенефициаров, клиентов и людей, использующих информационные услуги, предлагаемые Интернетом. С другой стороны, развитие информационных технологий, функционирующих в Интернете, также сопряжено с риском потери или кражи информации со стороны несанкционированных лиц.

PhD Dariusz Prokopowicz
Opublikowany: 2017-12-30
DOI: 10.5604/01.3001.0010.7645
Wydanie: International Journal of New Economics and Social Sciences 2017; 2 (6): 319-330

Процесс предоставления информации через Интернет создает множество угроз, связанных с кражей личных данных, хакеров, загроможденных секретными данными, и денежных растрат в электронных банковских системах. В ответ на эти угрозы отдельные организации разрабатывают системы безопасности для удаленного обмена информацией и транзакциями, осуществляемыми через Интернет.

Ключевые слова: *Интернет, социальные сети, интернет-компании, технологические компании, обмен информацией, веб-сайт, веб-сервер, информационный сервис, безопасность в киберпространстве.*

Introduction

In recent years, the role of improving the logistics and security of information systems have been increasing together with the development of acquisition techniques, and the multicriterial processing of information accumulated in the constantly growing online data bases of social networking sites, where citizens share information sometimes even very personal. In addition, the number of companies that collect personal information for marketing purposes and then resell it to other companies, banks, institutions is increasing. Increasingly, the collection of personal data is not limited to basic information such as name, gender and age, but also refers to other categories of private information pertaining to particular citizens such as shopping preferences, interests, place of work, income level etc. [S. Gwoździewicz 2014, s. 73]. This way companies, financial and public institutions create huge collections of nonpublic data composing valuable information for the need of marketing enterprises. By directing an appropriately defunct product or service offer at a strictly targeted audience, trading partners and at the segment of potential customers, it is more effective to achieve the greater effectiveness used in strategy marketing during advertising campaigns. Advertising campaigns conducted in this way generate a significant reduction of the costs of necessary marketing activities, in the situation of targeting this offer at a strictly defined segment of prospective purchasers [J. Sarnowski, D. Prokopowicz 2015, s. 137].

Therefore, expanded multiperspectively and informationally data bases, built in institutions, enterprises and also in social networking sites, become a valuable resources of information used marketing. Data bases of personal details, which grows informatively and measurably valuably, enforce sustaining their expenditures on entities to ensure the required level of security. In case of Internet companies, including social networking sites, Internet- hosting companies, web sites and e-mail services, telecoms, public institutions with an electronic access to profiled services and electronic agencies of banks and other financial institutions, there is a significant risk of an unauthorized access to personal data by hackers working on commission of companies and competing institutions [S. Gwoździewicz, D. Prokopowicz 2016a, s. 229-230]. The growing number of these types of nonpublic databases created by entities also active on the Internet and the ever-expanding range of information collected in data bases may generate an increase of the risk of announcing citizen's personal data on the Internet [D. Prokopowicz 2009, s. 65]. Thereupon, entities maintaining and extending this type of databases, are forced to spend more on improving the technical security of nonpublic data in order to reduce the potential of appearing categories named above such as: the risk of loss, theft or announcing of personal data on the Internet.

PhD Dariusz Prokopowicz
Opublikowany: 2017-12-30
DOI: 10.5604/01.3001.0010.7645
Wydanie: International Journal of New Economics and Social Sciences 2017; 2 (6): 319-330

1. Information security in the context of developing social networking sites

In economic systems of highly developed and developing countries, both business entities and the sector of public institutions play a particularly important role in meeting the needs of the society and indirectly the whole economy. After more than a quarter-century of the development of the Polish economy in the market conditions and processes of adapting to the European Union system standards, one of the spheres of public services offered in Poland is fulfilling the information needs of citizens [D. Wociór red. 2016, s. 48]. Decision-making processes indirectly influence on the pace of the socio-economic development of the country in enterprises and in the sector of public institutions such as financial management [M. Muchacki 2014, s. 27].

As a result, in recent years, new categories of the ITC system's risk on the Internet have emerged as a derivative of the rapidly growing and continuously growing large collections of the nonpublic data generated by companies offering specific products or services to Internet users. For several years, this type of data warehouse have functioned as a collection of information defined as Big Data and so called. Clouds computing. Facebook, Twitter, Instagram, YouTube, and other networking sites are currently having the largest data collection of this type about the Internet users. Because each of these commercial entities creates their own database about the Internet users, hence so called sensitive data bases about users are being stored now in many places in the global network [M. Górka red. 2014, s. 93]. Internet corporations acting globally, offer Internet users free use of their services, including social networking platforms [S. Gwoździewicz, D. Prokopowicz 2016c, s. 82-83]. They also create special software programs called robots that analyze available information about particular users and collect personal information for marketing purposes. Probably a small fraction of the Internet users know how far this commercialized surveillance carried by the Internet companies has taken place. The activity of these entities increases the potential scale of risk associated with the possible decrease of the security of nonpublic information collected in electronic databases and transferred via ICT systems [M. Matosek 2015, s. 112].

Unfortunately, under Polish conditions, there are not so much verified and confirmed quantitive data in terms of effective hackers attacks performing on other's entities IT systems via the Internet [A. Dmowski, D. Prokopowicz 2006, s. 77-78]. Wróbel quotes that the question of the legal responsibility is related to the issues of the security information systems and the information resources are included in these systems. It has already been significantly described by American researchers. On the other hand, in Poland, this issues is not still undertaken in researches, what is connected with a limited resource of analytic data [P. Wróbel 2014, s. 186-187]. On the basis of researches done in Western countries, a relatively high level of information leakiness of ICT systems has been demonstrated. According to the 2011 Websense Research report drawn up on the basis of 2,000 different types of economic entities and institutions operating in the US, Canada, Britain, and Australia employing at least 250 computer users in the period of one year, there have been many worrying events that may suggest many gaps in security systems and in procedures developed erroneously. In 37% of the surveyed entities, the employee contributed to the loss of certain nonpublic information and data that could result or resulted in advert events for some entity. In

PhD Dariusz Prokopowicz
Opublikowany: 2017-12-30
DOI: 10.5604/01.3001.0010.7645
Wydanie: International Journal of New Economics and Social Sciences 2017; 2 (6): 319-330

20% of the surveyed organizations nonpublic information was consciously and illegally copied and stolen by employees. They were also stolen from internal IT systems of companies and institutions. Also in 20% of the surveyed entities nonpublic data was sent to social networking sites. Besides, in internal IT systems of 35% surveyed entities there appeared Trojan horses, malicious programs like malware or other types of viruses [*Websense Research Raport,* 2011, s. 11].

2. Global tendency in terms of the security conducted in social networking sites processing and transfer of data

The dynamic development of Internet services accelerated the process of the informational globalization but also created a wider field for hackers and terrorist organizations. Everyday, globally, there arise many new viruses, that are repeatedly capable of attacking the IT systems of many companies, public institutions, banks, and home computers. On the other hand, new securities measures are also created for attacked information systems every day. This type of rivalry does not always take the form of a zero-scoring game [D. Prokopowicz 2016, s. 21-22]. Currently, the legal norms functioning in UE are not fully adequate to the prevailing standards of digitization of offices and enterprises, and the infrastructure of the sensitive branches in the national economy. Energetics , transport, crisis management centers, offices and financial system belong to branches in the economy that are threatened by cyberterrorists attack [A. Dmowski, D. Prokopowicz 2010, s. 326].

In connection with the immigration crisis in Europe and the war in Syria, the media in Europe are dominated by reports suggesting that Islamic fundamentalists are currently responsible for attacks. However, globally, the sources of terrorist attacks are more diverse, taking into account the nationality, culture and religion that is the culprit of the attacks . As terrorism is more and more concerned with the global medium of the Internet and the phenomenon of cyberterrorism can cause not less negative effects than "traditional" acts of terror, so the global spin of this issues is also important [A. Suchorzewska 2010, s. 19-20]. Analyzes refering to the global approach to terrorism show that Islamic fundamentalism can only be linked to every fifth terrorist attack in recent months. Apart from Islamic fundamentalism, terrorist attacks are still assassinated by different types of neo-Nazi and leftists organizations, groups of separatist and fundamentalist associated with different religious currents. Krzysztof Cieślak, who is an expert of the research centre on Collegium Civitas terrorism, indicated that cyberterrorism took a shot at financial sector ,which doesn't need to restrict to hacking on bank accounts. It was during Bank Security Forum that held on 10th May 2016 in Warsaw. The threat of cyberterrorism in regard of bank may be different. So far in the structures of the right public services, teams constituted for the current monitoring of potential threats, including crisis management teams, have changed the nature of the process of controlling and managing potential threats in recent years. Current threats caused by the forces of nature, failures of energy installations and water pipes and other facilities give way to potential terrorist or even cyber terrorist threats [K. Machowski 2016, s. 14].

Therefore, in recent years, new categories of cybersecurity risk of IT systems have emerged as a derivative of the rapidly growing and ever-expanding large data sets about users, customers that are created by economic entities on the Internet. Recently, these large data sets have functioned in the

PhD Dariusz Prokopowicz
Opublikowany: 2017-12-30
DOI: 10.5604/01.3001.0010.7645
Wydanie: International Journal of New Economics and Social Sciences 2017; 2 (6): 319-330

so-called data cloud developed on a data warehouse of a given entity. The analysts of this issue predict that the largest collections of data on Internet users are currently had and persistently developed by online companies like Google, Facebook, Twitter, Instagram, YouTube and others. In connection with it, the data of Internet users, including so-called sensitive personal details are currently stored in many locations, on servers of different companies and institutions [M. Górka red. 2014, s. 93]. The largest Internet companies, that offer a free use of social networking sites, create special programs called robots, with the help of which they analyze online data sets and then copy, convert and collect it in their own data warehouses. Probably still, most people on Earth do not know how far this commercialized surveillance of Internet companies has taken place [S. Gwoździewicz, D. Prokopowicz 2016c, s. 81].

Internet users are generally unaware of the scale of potential use of their personal data by online companies that do marketing business on behalf of other entities. Online companies such as Google, Facebook, Twitter, Instagram, YouTube get the most part of their revenues from advertisings on their social networking sites. On the user's accounts of these social networking sites, there are displayed advertisings appropriately profiled according to the preferences of the user and his personal characteristic [T. Trejderowski 2013, s. 165]. These preferences are sometimes defined by the user at the stage of setting up an account on a given social networking site. Later, while using a particular account, specially created robots will scan preferences of a given user about the areas of interest and the type of content ad they would like to receive [J. Kos-Łabędowicz 2015, s. 52].

In addition, the robots that work on these portals collect certain data about the user and create multi-faceted personal profiles in databases of the mentioned online concerns. Because the number of users of these portals is not even millions, and even billions are data warehouses secured with the possible latest security techniques and with encryption of data sent on the Internet, including personal data [J. Kosiński 2015, s. 146]. These warehouses are created for the huge resources of information. Most online companies that run a commercial and advertising business , collect data about user's websites by installing in their browsers so called Cookies, ie background programs, that collect data about users of some webpage [S. Gwoździewicz, D. Prokopowicz 2016c, s. 83-84].

3. The need to improve risk management systems and adjust the legal regulations to the technological progress of online information technologies

In accordance with current legal regulations, Internet users generally know about this trade to be possible, they may or may not have to agree to it at the beginning of the website of the company or institution [K. Machowski 2016, s. 14]. Theoretically, because of the prevalence of this solution, Internet users are more likely to forget or ignore this possibility of deciding on how these cookies work. Consequently, each web user of a global village, more or less consciously, consent to build their digital profile in warehouses of online concerns, other companies and institutions [B. Szaruga-Domańska, D. Prokopowicz 2016].

The most extended personal profiles, also known as avatars of particular online users, are built in data warehouses of online concerns mentioned above. Other important parameters affecting the scope of information generated by an avatar ,are the frequency of use of the global network, the scope of information provided, and the

PhD Dariusz Prokopowicz
Opublikowany: 2017-12-30
DOI: 10.5604/01.3001.0010.7645
Wydanie: International Journal of New Economics and Social Sciences 2017; 2 (6): 319-330

number and type of browsed pages. It is now assumed that each user of the Internet and in particular a user browsing a wide variety of sites and having an account on social networking sites, has an Internet equivalent- an avatar, whose characteristic is found in databases of the mentioned examples of Internet concerns [A. Gałach, S. Hoc, A. Jędruszczak, P. Kowalik i inni 2015, s. 243].

It is also widely acknowledged that Internet users and users of other news media care for the protection of their privacy, intimacy that is important in everyday existence and in the use of these dynamically developing media. However, the scale of progress made in ICT and in the offer of online companies has depreciated the real opportunities of user privacy of certain online information services available on the Internet. Progress in this area has significantly outrun the technique that should provide privacy protection. The awareness of Internet users is in this respect still negligible. This is because it is in the interest of these Internet concerns who bother to build the most informationally well-formed personal profiles in the form of avatars in their data warehouses [J. Grzywacz 2016, s. 81].

In recent years, collecting information about Internet users for developing information avatars has been facilitated by the next stage of technological development. This next stage of progress in the development of global Internet media is determined by the widespread technology of platforms built in the clouds computing [C. M. Olszak 2014, s. 47], that is data warehouses accumulating huge collections of data with the possibility to process them and with an access to mobile devices. Sometimes there is also the issue of physical distribution of data warehouses in different places of a given country, continent or in a global view. The issue of distributing the components of the data warehouse system is determined by the security of data storage, the need for data backup and by the mirroring of data warehouses physically located in different parts of the globe. Internet users, thanks to the widespread cloud computing technology, have the convenience of an access to their social networking sites accounts from various mobile devices with the Internet access [A. Krasuski 2012, s. 127].

It is commonly assumed that, in keeping with the needs of most Internet users, the protection of personal data is this domain of human existence in the current digital revolution, which should be also provided by online companies. According to the Basic Law, that is the Constitution, the protection of personal data is one of the fundamental rights of every citizen and also the Internet user. The dynamic advance in technology and In the range of an offer of Internet services have caused a partial erosion of the real operation of this law. This is because either Internet users are not fully aware of avatars built in the warehouses of the Internet concerns or new ICTs no longer allow to reserve the full privacy of citizens in information societies. The Internet companies such as Google, Facebook, Twitter, Instagram, and YouTube collect other data about users of their social networking sites every day [S. Gwoździewicz, D. Prokopowicz 2016c, s. 84-85]. They constantly develop avatars that already existed, this is electronic equivalents of individual citizens and Internet users. How and when will these data be used, except for the current advertising activities of these corporations, unfortunately Internet users do not know [Ł. Libuda 2016, s. 95]. They cannot even know it even if these companies, online companies that own social networking sites, do not know how these constantly growing information collected in data warehouses will be used for 10 years.

As a result, technological advances change the relationships between Internet

users and personal data owners about individual citizens. When the disclosure of a violation of citizens' right to privacy and to the issue of the institutional protection of personal data, Internet users generally regard it as a lack of action guaranteed in the Constitution. Internet companies justify their collection of personal data about Internet users by consenting citizens to this practice [S. Gwoździewicz, D. Prokopowicz 2016b, s. 65]. Besides, another institutional element that is to provide the required level of protection of personal data is the adaptation of regulation by law to the normative standards of the European Union, that Poland is a member. Accordingly, the legal norms that exist in Poland concerning the protection of personal data should be adjusted to the regulation of European Union Law and also to the regulation of international law [P. Hołyst, J. Pomykała 2011, s. 13]. So there is the question whether these institutional and legal solutions that currently exist do not contribute to lulling into a false sense of security of Internet users in analyzing the security of nonpublic information, including the personal data collected and used by the Internet companies in a specific way?

Internet users should not forget that the legal protection of personal data as a part of the institutional electronic security system for the collection and transmission of nonpublic information cannot always provide real full protection of information that citizens transmit to individual commercial companies and institutions that are in operation on the Internet. Citizens usually assume that providing security to information is the responsibility of companies and institutions [A. Gałach, A. Jędruszczak, B. Nowakowski 2013, s. 116]. These entities should be obliged to do so, as they control most of the information resources stored in national ICT systems and networks. In addition, domestic and foreign operators offer their services and products to consumers, so they should provide customers with the protection of their personal data for the purposes of the transaction. The legal norms that should oblige those entities to protect nonpublic data is for example the Law of 16 July 2004,Telecommunication Law and the Law of 18 July 2002 on providing services by electronic means [D. Prokopowicz 2017, s. 94-95].

According to the text of Article 10 (1) of this Act, Internet companies and institutions may not send commercial communication that has not been ordered to individuals with the help of any electronic means of communications . On the basis of legal norms in Poland, it is also forbidden to use teleinformatic systems, techniques and devices without the consent of the user of these systems for marketing purposes [D. Wociór red. 2016, s. 68]. The ban also applies to the use by commercial operators of automatic calling systems created for the purposes of doing direct marketing business if the final user hasn't agreed with it. These regulations provide the most elementary level of protection for nonpublic data while realizing certain commercial and financial transactions, but they may be insufficient towards the perpetual advance in teleinformatic technology used by Internet service providers, and especially those that usually offer cost-free usage of social networking services [A. Buss 2008, s. 74].

Therefore, in the dozen or so years, significant progress has been made in electronic data transmission systems, which has been determined mainly by the development of information and communication technology. Technological advance in the fields described above, have also led to the implementation of modern IT solutions in the processes of enterprise management to improve their economic efficiency. Companies operating in Poland in the pursuit of market and business success try to build

their competitive advantage by implementing new IT solutions to their business. More and more companies and financial institutions use business analysis conducted on their IT platforms for Business Intelligence Solutions.

On these platforms, the information needed for management decision-making processes is constantly updated, archived, categorized and used to develop Business Intelligence analytics reports. Research has shown that Business Intelligence analyses make it easier for managers to perform analysis of large collections of business-related data in real time. Consequently, the opinion that Business Intelligence solutions are becoming more and more useful in the processes of organization management [J. Grzegorek, D. Prokopowicz 2017, s. 224]. In recent years, global Internet corporations, such as Google and Facebook, have been trying to combine Big Data technology, computing data in the cloud computing, creating business intelligence platforms and doing researches and implementation for the creation of an artificial intelligence.

4. Summary

The reconstruction of the SME sector in Poland in the 1990s was an important factor in the context of the effective development of the market economy in Poland. On the other hand, the development of information technology determines the need of tweaking the rules forming the security of electronic transfer of data on the Internet. When the number of Internet users grows quickly, the importance is in improvement of IT systems in the security of transactions, the risk analysis and bearing the costs of the system solutions. It has to maintain the high level of security and the protection of nonpublic data. The issue of improving system security solutions is particularly important in the case of the most common hacker attacks on online banking systems [B. Domańska-Szaruga 2013, s. 269-270].

In addition, as a result of the growth of transnational capital flows and trade, the share of financial transactions settled electronically also has increased. In addition, as Poland is a member of the European Union, Polish regulations on the security of electronic data transfer and protection of nonpublic information are adapted to the normative EU standards. This process is also part of the improvement of external regulations by law and is linked to the progressive globalization of financial systems [J. Kosiński 2015, s. 141].

Accordingly, the progressive economic globalization and, therefore, the growing link between the Polish economy and the world, means that the improvement of national regulations concerning the maintenance of a certain level of security of information systems and protection of nonpublic data takes place, among other things, as a process of adapting Polish legislation to European Union regulation [D. Prokopowicz 2012, s. 27]. On the other hand, this is not a factor ensuring a full adequacy of legal norms in relation to the dynamically developing electronic banking offering of financial institutions and services provided by online companies. Currently, it is assumed that the current legal regulations only provide the most elementary level of protection of nonpublic data while processing specific commercial and financial transactions, but may be insufficient with the ever-evolving technology of information and communication technology used by Internet service providers, especially those who usually offer the usage of social networking services without any costs.

In the context of the ongoing digitization of companies, offices and institutions, it is now accepted that, as most Internet users need, the protection of personal data is the domain of human existence that should

PhD Dariusz Prokopowicz
Opublikowany: 2017-12-30
DOI: 10.5604/01.3001.0010.7645
Wydanie: International Journal of New Economics and Social Sciences 2017; 2 (6): 319-330

be ensured by the Internet. According to the provisions of the Constitution, the protection of personal data is one of the basic rights of every citizen, and therefore also the right of the Internet user. Perpetual technological advance and services offered by Internet companies have caused a partial eradication of the real operation of this law on Internet users' side [A. Gałach, A. Jędruszczak, B. Nowakowski 2013, s. 121]. This is because either Internet users are not fully aware of avatars built in data warehouses or the new IT technologies no longer allow to keep the full privacy of citizens in information societies.

The above mentioned Internet companies such as Google, Facebook, Twitter, Instagram and YouTube collect data about users of their social networking sites every day. They are constantly developing informative avatars, this is electronic equivalents of individual citizens and Internet users. Unfortunately, the Internet users do not know in what way and when these data will be used except for the current advertising of these companies. They cannot know it even if these companies, online companies that own social networking sites also do not know in what way they will use these constantly growing information collected in data warehouses.

References

1. Buss A., (2008), *Internet Marketing*, Warszawa: Wydawnictwo Longman Pearson Education.
2. Dmowski A., Prokopowicz D., (2006), *Przestępczość elektroniczna i kradzież poufnych informacji – dynamicznie rozwijająca się gałąź szarej strefy* (w:) „Szara strefa gospodarcza w dobie globalizacji" - monografia naukowa, Seria wydawnicza: Konferencje i seminaria nr 19, Publikacja pokonferencyjna dla Konferencji naukowej pt.: „Szara strefa gospodarcza w dobie globalizacji", Konferencja naukowa w PWSBiA w dniu 06.10.2006 r., Prywatna Wyższa Szkoła Businessu i Administracji w Warszawie, Warszawa 2006, s. 76-96.
3. Dmowski A., Prokopowicz D., (2010), *Rynki finansowe*, Warszawa: Wydawnictwo Centrum Doradztwa i Informacji Difin sp. z o.o.
4. Domańska-Szaruga B., (2013), *Common banking supervision within the financial safety net*, (w:) Raczkowski K., Schneider F. (red.), *The Economic Security of Business Transactions. Management in business*, Oxford: Wydawnictwo Chartridge Books Oxford.
5. Gałach A., Jędruszczak A., Nowakowski B., (2013), *Ochrona danych osobowych, informacji niejawnych i systemów teleinformatycznych w sektorze publicznym*, Warszawa: Wydawnictwo C.H. Beck.
6. Gałach A., Hoc S., Jędruszczak A., Kowalik P., i inni (2015), *Ochrona danych osobowych i informacji niejawnych w sektorze publicznym*, Warszawa: Wydawnictwo C.H. Beck.
7. Górka M., red. (2014), *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Warszawa: Wydawnictwo Difin.
8. Grzegorek J.,, Prokopowicz (2017), *The Application Of The MS EXCEL Program And The Informalized Business Intelligence Analytics Platforms In The Management Of The Enterprises* (w:) "Czasopismo Międzynarodowe Nowa Ekonomia i Nauki Społeczne" – "International Journal of New Economics and Social Sciences" (IJONESS), Międzynarodowy Instytut Innowacji Nauka - Edukacja - Rozwój w Warszawie, nr 1 (5) 2017, s. 222-237.
9. Grzywacz J., (2016), *Bankowość elektroniczna w przedsiębiorstwie*, Warszawa: Wydawnictwo SGH.

PhD Dariusz Prokopowicz
Opublikowany: 2017-12-30
DOI: 10.5604/01.3001.0010.7645
Wydanie: International Journal of New Economics and Social Sciences 2017; 2 (6): 319-330

10. Gwoździewicz S., Jakubowski J., (2017), The tasks of the national administration within the protection of the Polish Cyberspace [in] PUBLIC MAMAGEMENT - "ПУБЛІЧНЕ УРЯДУВАННЯ" - Collection is trained in scientific partnership with the Ukrainian Technological Academy - № 2 (7) – May 2017; KB 21596-11496 P; ISSN 2414-0562. Kijów 2017 r. („Public management" - czasopismo naukowe Ukraińskiej Akademii Technologicznej), Kijów 2017 r. str.65.
11. Gwoździewicz S., Prokopowicz D., (2016a), *Bezpieczeństwo bankowości internetowej i uwarunkowania elektronicznego transferu danych w technologii Big Data w Polsce* (w:) V. Vlastimil (red.), "Međunarodni naučni zbornik. Pravo Ekonomija Menadžment I" /Międzynarodowe zeszyty naukowe. Zarządzanie Prawo Gospodarka I/ International scientific books. Right, Economy and Management I/, Wydawnictwo [Izdavač:] Srpsko Razvojno Udruženje /Stowarzyszenie Rozwoju Serbii/ Bački Petrovac 2016, s. 228-252.
12. Gwoździewicz S., Prokopowicz D., (2016b), *Globalization and the process of the system and normative adaptation of the financial system in Poland to the European Union standards* (w:) *Globalization, the State and the Individual*, "International Scientific Journal", Free University of Varna "Chernorizets Hrabar", Chayka, Varna, Bułgaria 9007, Varna 2016, nr 1(9) 2016: 63-75.
13. Gwoździewicz S., Prokopowicz D., (2016c), *Prawno-społeczne determinanty bezpieczeństwa gromadzenia i transferu danych niejawnych w internetowych portalach społecznościowych* (w:) V. Vlastimil (red.), "Međunarodni naučni zbornik. Pravo Ekonomija Menadžment I" /Międzynarodowe zeszyty naukowe. Zarządzanie Prawo Gospodarka I/ International scientific books. Right, Economy and Management I/, Wydawnictwo [Izdavač:] Srpsko Razvojno Udruženje /Stowarzyszenie Rozwoju Serbii/ Bački Petrovac 2016, s. 80-107.
14. Hołyst P., Pomykała J., (2011), *Cyberprzestępczość, ochrona informacji i kryptologii*, (w:) „Prokuratura i Prawo", nr 1, 2011.
15. Kos-Łabędowicz J.,(2015), *Internet jako źródło informacji w decyzjach nabywczych konsumenta*, Warszawa: Wydawnictwo C.H. Beck.
16. Kosiński J.,(2015), *Paradygmaty cyberprzestępczości*, Warszawa: Wydawnictwo Difin.
17. Krasuski A.,(2012), *Dane osobowe w obrocie tradycyjnym i elektronicznym. Praktyczne problemy*, Warszawa: Wydawnictwo Wolters Kluwer.
18. Libuda Ł., (2016), *Era Big Data - zarządzanie ryzykiem z dopalaczem* (w:) "Bank. Miesięcznik Finansowy", nr 6 (278), czerwiec.
19. Machowski K.,(2016), *Hakerzy i terroryści czyli kto zagraża współczesnym bankom* (w:) "Bank. Miesięcznik Finansowy", nr 6 (278), czerwiec 2016.
20. Matosek M.,(2015), *Marketing partnerski w obliczu wielokulturowości* (w:) J. Wróblewski, „Zarządzanie w czasach kryzysu", Dąbrowa Górnicza: Wydawnictwo WSBI w Dąbrowie Górniczej, rozdział. X.
21. Muchacki M.,(2014), *Cywilizacja informatyczna i Internet. Konteksty współczesnego konsumenta TI*, Warszawa: Wydawnictwo Impuls.
22. Olszak C. M. ,(2014), *Business Intelligence in cloud*, (w:) "Polish Journal of Management Studies", (10) 2014.
23. Prokopowicz D., (2009), *Zagrożenia rozwoju i bezpieczeństwo bankowości elektronicznej* (w:) Zeszyty Naukowe Wyższa Szkoła Zarządzania i Prawa im. Heleny Chodkowskiej w Warszawie. Rok XIV. Nr 1 (30)/2009, s. 60–73.
24. Prokopowicz D., (2012), *Na tle struktur rynkowych Unii Europejskiej* (w:) "Przedsiębiorstwo przyszłości". Kwartalnik Wyższej Szkoły Zarządzania i Prawa im. Heleny Chodkowskiej. Warszawa, Nr 2 (11) 2012, kwiecień 2012, Rok wyd. IV, s. 25-34.
25. Prokopowicz D., (2016), *Social and economic determinants of the processes of economic globalization that shape the development of the banking system in Poland* (w:) *Globalization, the State and the Individual*, "International Scientific Journal", Free University of Varna "Chernorizets Hrabar", Chayka, Varna, Bułgaria 9007, Varna 2016, nr 2(10) 2016, s. 21-22.

PhD Dariusz Prokopowicz
Opublikowany: 2017-12-30
DOI: 10.5604/01.3001.0010.7645
Wydanie: International Journal of New Economics and Social Sciences 2017; 2 (6): 319-330

26. Prokopowicz D., (2017), *Bezpieczeństwo udostępniania informacji przez instytucje sektora publicznego oraz transferu danych niejawnych poprzez sieć Internet* (w:) A. Gołębiowska, B. Zientarski (red.), „Ponowne wykorzystywanie informacji sektora publicznego w administracji", Senat Rzeczypospolitej Polskiej, Kancelaria Senatu, Warszawa 2017, s. 91-114.
27. Sarnowski J., Prokopowicz D., (2015), *Zastosowanie innowacji marketingowych w przedsiębiorstwach w Polsce* (w:) M. Sitek, T. Graca (red.), "Nowe wyzwania dla Europy XXI wieku w dziedzinie zarządzania i edukacji", wydanie pokonferencyjne, Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie, Józefów 2015, s. 135-156.
28. Suchorzewska A., (2010), *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa: Wydawnictwo Wolters Kluwer Polska Sp. z o.o.
29. Szaruga-Domańska B., Prokopowicz D., (2016), *Ochrona transferu danych osobowych w cyberprzestrzeni* (w:) „Secretum. Służby specjalne, bezpieczeństwo i informacja", Instytut Nauk Społecznych i Bezpieczeństwa Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach, Oficyna Wydawnicza RYTM w Warszawie, nr 2 (2016).
30. Trejderowski T., (2013), *Kradzież tożsamości. Terroryzm informatyczny*, Warszawa: Wydawnictwo Eneteia.
31. *Websense Research Raport*, (2011), s. 11, (www.websense.com).
32. Wociór D., red. (2016), *Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego*, Warszawa: Wydawnictwo C.H. Beck.
33. Wróbel P., (2014), *Komunikacja elektroniczna. Zagrożenia i ich skutki dla organizacji,* Gdańsk: Wydawnictwo Uniwersytetu Gdańskiego.