UDK 336.5, 004.738.5:658.8, Pregledni rad

Differences in Legislation of Data Privacy Protection in Internet Marketing in USA, EU and Serbia

Jasmina Markov, Biljana Lazić

Abstract: There is a growing number of companies that are, in its operations and dealings with consumers, turning to the Internet and using huge opportunities that it provides. Therefore, Internet marketing is now experiencing extreme expansion and it is considered to be the marketing segment that is vulnerable to intensive and continuous change. Along with the positive effects brought to both businesses and consumers, there are some negatives associated with this form of marketing, and one of them is the insufficient protection of privacy. The fact is that we must raise the level of data protection, and improve its quality. Intense changes have to be taken on the normative level, because there are still plenty of reasons for the dissatisfaction of consumers when it comes to protecting their privacy. Thus, the legislation must play a key role in building consumer confidence as well as in the establishment of a positive relationship with marketers. The aim of this paper is to show the importance of the construction of such levels of private data protection which will establish long-term partnerships between consumers, marketers and other participants in the market, since only the aforementioned relations can bring prosperity to all parties. The paper will make a comparative analysis of the legislative framework in this field in the United States, the European Union and Serbia, as well as stress still present significant backlog of Serbia in relation to the aforementioned developed countries.

Key words: Internet marketing; Consumer protection; Privacy protection; Legislation

1. INTRODUCTION

Problems and open issues related to data privacy and consumers' rights have always existed, as well as attempts to regulate them through numerous laws and regulations. Contemporary information and communication technologies have rapidly shifted the boundaries of privacy. However, the fact that all has its limits is confirmed by frequent public debates on this topic, as well as the latest data which show that around 80% of American citizens believe that the right for privacy comes immediately after the right to live and be free.

We can safely conclude that, from consumers' perspective, data protection is certainly the most important. But, while in the protection of these rights in traditional commerce one could use developed case law and numerous legal provisions, the position of consumers in internet marketing is uncertain. Infinite ease is a characteristic of electronic data handling rather than traditional paperwork. Copying books in the middle Ages lasted for years, and until recently the same procedure had been carried out quickly only by using rare devices available to a small number of people. Currently, the situation is completely different. With just one mouse-click on a personal computer, one can access a large number of data and information. These challenges require that the legislation in the field of data protection provides adequate solutions and ensures maintenance of consumers' confidence in internet marketing. The main problem for consumers is collecting sensitive personal data, and the possibility of their abuse in order to create consumer profiles, as well as complete dossiers about their purchasing habits, interests and the like. Therefore it is necessary to mobilize the public and raise awareness among people about the need for privacy protection. One of the possible solutions is to outline unique, global laws that would ensure effective control over data and information collection, as well as transparency of their further use.

The aim of this paper is to emphasize the exceptional role of legal norms in regulating the problem of consumers' data privacy protection, and to highlight their contribution to the development and dissemination of trust in internet marketing activities. Also, special attention will be paid to the legislation of the mentioned field in the European Union and the United States, with reference to the current circumstances and future prospects of data protection in Serbia.

2. NEED FOR DEFINING LEGAL NORMS TO REGULATE DATA PRIVACY PROTECTION

One of the most controversial topics that not only intensely involve governments around the world, but also many non-governmental organizations is related to privacy and protection of personal information of consumers. Currently, due to the widespread use of the Internet and direct marketing, privacy issues are becoming increasingly important. "Online business" uses demographic information (for example, personal information of credit card numbers), giving the consumer a fear of performing "online shopping activities." According to some estimates, as many as 77% of Internet users have never purchased a product online, and nearly 86% showed a fear that other users could use their credit card numbers, which is private information according to them (Končar, 2003, p. 269-270). All this suggests that the issue of protection of consumer privacy in one of the most important issues of internet marketing. Of course, the problem lies not in the fact that internet marketing has become one of the key selling strategies, but in the unauthorized use and sharing of personal information of consumers. Even in the first European directives dealing with this issue it was well known that data collected for one purpose cannot be used for any other purpose without the consent of the individual whose data were in question. This meant that the individual actively brought decisions on any new use or sharing of information. However, experts in Internet marketing, and legislative authorities as well, were prone to liberal interpretation of this provision. They believed that the consent of the consumer to use his or her personal data for marketing purposes would also permit them to trade with a third party if it would use the data for marketing purposes.

Although it seems that the right to privacy came into the focus of public interest along with the expansion of new technologies, legal science has been dealing with it for more than a century. One of the earliest definitions is that it is „the right to be left alone," but today it is much more discussed from the standpoint of property rights over the information and their use. Moreover, a recent survey in the US showed that respondents are more concerned about the disclosure of information held by various agencies and companies rather than environmental control. The reason lies in the fact that the data collected through internet marketing are so valuable that the FBI and tax services have been interested in them lately.

Privacy issues include the right to be free from unreasonable personal intrusions and so we can safely say that it has been a legal and social issue of a large number of countries for many years. Today the right of privacy is recognized in its virtual form and it is closely related to the following characteristics (Salai, Končar, 2007, p. 268):

- The right of privacy is not an absolute right and it balances in relation with the needs of the society.
- The right of publicity is superior to the right of individual privacy.

According to this, we can conclude that the right of privacy and its protection are a very sensitive issue and therefore it is very difficult to identify and define specific legislation.

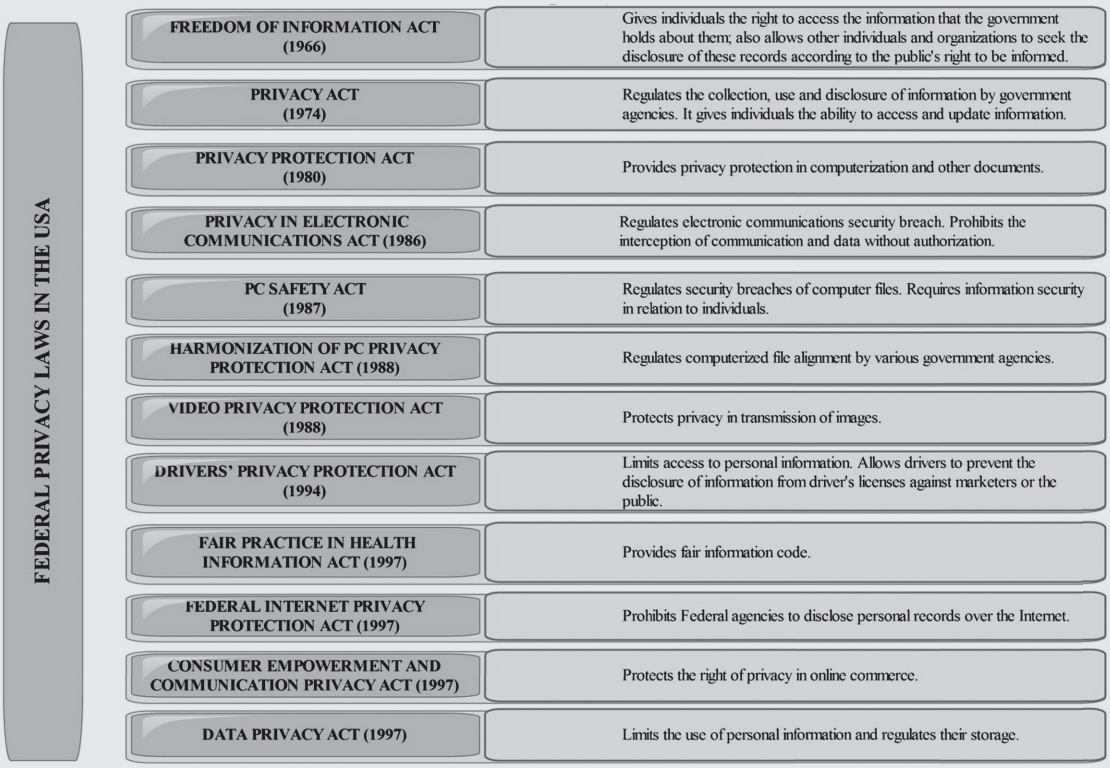
3. LEGISLATION IN THE FIELD OF DATA PRIVACY PROTECTION

Every individual has a right to know which personal information about him or her are collected, how they are processed and for what purposes they are used. Consumers must be given the possibility of checking personal data stored in various databases and registries to decide independently whether these data can be used in internet marketing. One of the basic principles of protection of data confidentiality is the principle of ownership over stored data that clearly defines who is responsible for ensuring the protection of data and who determines the possibility to access the data (ISO/IEC 17799 norm). There are many situations in which the data must not be available to the general public because their general availability could be misused for any reason and in any manner. Some information must be kept secret due to the need to protect the general, common and business interests, and some for the protection of individual privacy. Therefore, concrete measures to protect the insight and access to confidential information against unauthorized persons must be taken. In the case law of many countries, this issue is approached in different ways, which we will to explain through the examples of the US, the European Union and Serbia.

3.1. Data privacy protection in the USA

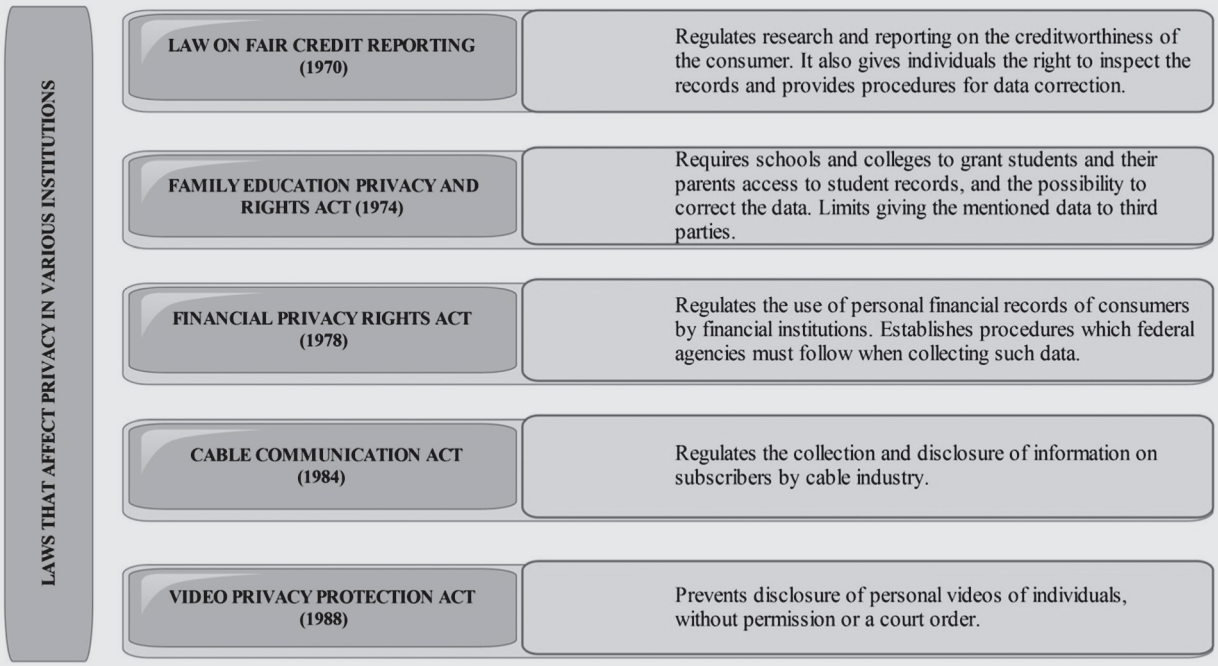
In the United States, Canada and Germany, the right of privacy is expressly guaranteed or can be derived from the Constitution or the Statute of the country. In the UK and the US, there is also protection of privacy

ILLUSTRATION 1. Federal privacy laws in the USA



SOURCE: Laudon, Traver, 2002, E – commerce, Business Tehnology Society, Addison Wesley, Boston, p. 471

ILLUSTRATION 2. Laws that affect privacy in various institutions



SOURCE: Laudon, Traver, 2002, E – commerce, Business Tehnology Society, Addison Wesley, Boston, p. 471

in the common law, whereas court decisions involve personality injuries of individuals. For example, in the United States, four forms of privacy violations have been defined by court decisions involving violations of individuals by other persons:

1. Unreasonable personal imposition.
2. Public disclosure of private information and facts.
3. Public presentation of an individual in an unfavorable light.
4. Acquiring somebody else's name for commercial purposes (mainly related to celebrities).

In the US it is argued that the privacy of individuals is provided by the First Amendment that guarantees freedom of speech and association, Fourth Amendment, which provides protection against unreasonable collection of personal information, as well as the Fourteenth Amendment which guarantees that all individual rights guaranteed by law will be respected (Laudon, Traver, 2002, p. 470). Except by the Constitution and the common law, individual privacy is guaranteed and presented through federal and state laws.

Governments around the world are responding to the growing public concern about online privacy and extending well-developed concepts of privacy and offline business to online business as well. In the US, the Federal Trade Commission (FTC) has taken the lead in conducting research about online privacy and making recommendations of legislative framework to the Congress. The Commission seeks to ensure efficient functioning of markets by protecting consumers from unfair practices and fraud, providing them at the same time with a larger choice as a result of encouraging competition. In 1995, the Federal Trade Commission started a series of online privacy researches, with regard to their attitude that online invasion of privacy could involve fraudulent and unfair conduct. In 1998, the Commission published the principles of fair information practices (FIP) on which it based its assessments and recommendations for online privacy.

These principles are continually striving to develop a form that is suitable for solving the problems of online privacy. They represent the basic rules on the protection of privacy in direct, internet marketing. The most important law on privacy which is directly influenced the formulation of the abovementioned principles is the Law on Protection of Children on the Internet, which implies the granting of permission by the parents to collect information regarding children under the age of 13 (Laudon, Traver, 2002, p. 471). Currently, the principles of the Federal Trade Commission are only guidelines, not laws. However, they are used as a basis for the development of new legislation on the protection of data privacy in the USA.

Illustration 3. FTC principles of fair information practices (FIP principles)

AWARENESS *(Basic principle)*	Consumers must be notified prior to data collection. The principle involves the identification of the person who collects information, the use of data, data users, the consequences of refusal to provide information, as well as ways to protect the confidentiality, integrity and quality of the data collected.
CHOICE/CONSENT *(Basic principle)*	Consumers must have the possibility to choose how to use their personal data, including their own internal use, or transfer to third parties.
ACCESS/ PARTICIPATION	Consumers need to have an insight into the accuracy and completeness of personal information.
SAFETY	Consumers' personal information must be secured against unauthorized use.
IMPLEMENTATION	There must be a mechanism for the implementation of FIP principles. This may include self-regulation, legislation, federal statutes, and others.

Source: Laudon, Traver,C.G. 2002, E – commerce, Business Tehnology Society, Addison Wesley, Boston, p. 472

3.2. Data privacy protection in the European Union

In Europe, privacy is regulated much more strictly than in the US. In the US, private companies and organizations are permitted to use personal information collected in commercial transactions for other business purposes, without prior consent of the consumers (Marković, 2003). In the US there is no federal agency responsible for enforcing the Law on Privacy, but instead the Law on Privacy is being implemented mainly through self-regulation by companies or individuals. The European approach to privacy protection has a more comprehensive and regulatory nature. European countries do not allow companies to use personal information collected from consumers without their prior consent. Privacy laws are implemented through establishing data protection agencies that take care of consumer complaints and enforcement of the laws in practice (Laudon, Traver, 2002, p.476).

The Directive on Data Protection (DPA), a decision made by the European Commission in 1998, provides standardization and extension of the protection of privacy in all EU countries. The Directive is based on the principle of Fair Information Practices (FIP principles) with the extension regarding giving consumers control over their personal information. The Directive requires companies to inform consumers when collecting information about them, and about the ways the collected information are stored and used. Consumers must give their consent before the companies begin to use the data about them. They also have the right to access the information, the possibility of their correction, as well as to prohibit the collection of further information for marketing and other purposes. The Directive prohibits the transfer of personal data to those companies or countries that do not have a similar privacy policy. This means that the data collected in Europe by US companies may not be transferred or processed in the United States (which has less severe privacy laws). However, the Ministry of Commerce of the EU in cooperation with the European Commission has developed a security policy, the so-called „Safe harbor“ principle for American companies. The companies that decide to participate in this program must develop a privacy policy that meets the European standards and enroll in the Web Registry kept by the Ministry of Trade of the EU (Laudon, Traver, 2002, p.476-477).

In essence, the DPA operates in two directions: on the one hand it grants certain rights to individuals, and on the other it forces those who collect personal information on consumers to inform them about the purpose and manner of their use, as well as to follow the proper guidelines. The Directive requires companies to provide detailed descriptions of (Bandypadhyay, 2002, p.247):

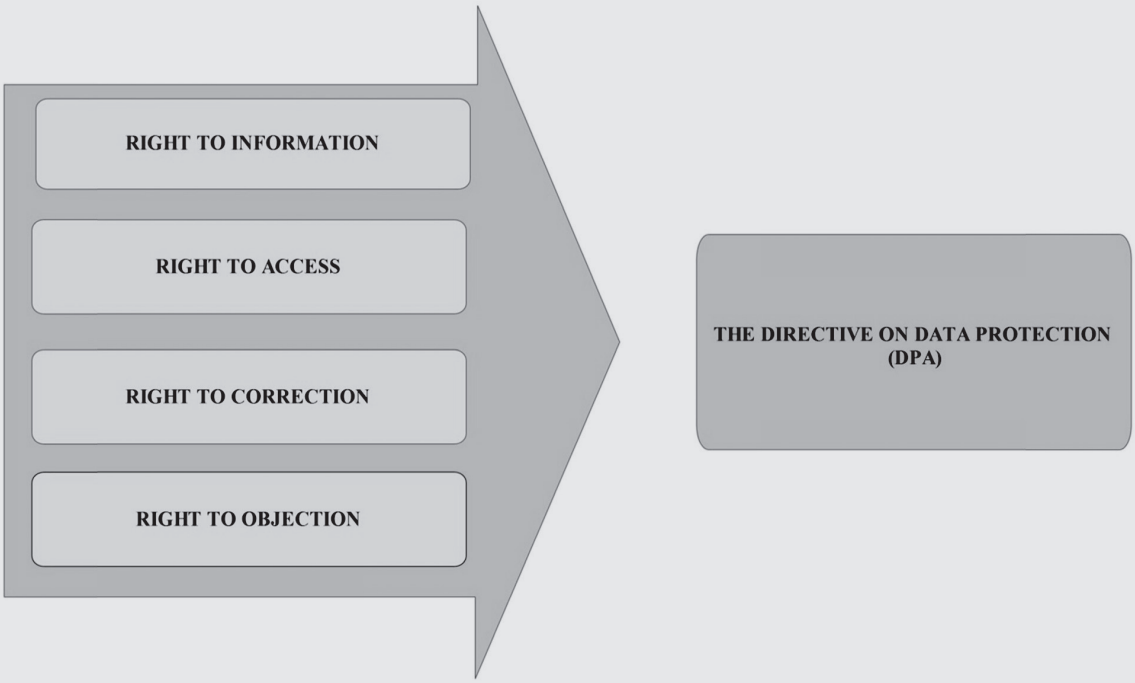
- data stored,
- the purposes for which the data may be used,
- sources from which the information are collected,
- third parties to which the information may be passed,
- countries or companies to which the information can be transferred.

The Directive includes eight principles which represent obligations for those companies that collect and use personal information on consumers. Basic principles of data manipulation are as follows (Bandypadhyay, 2002, p.247):

1. Handling data must be fair and lawful.
2. Data can be collected and used only for specific, clear and legitimate objectives.
3. Only those data that are relevant for mentioned purpose may be collected, and the availability of data should be granted only to those who are registered.
4. Provide accurate and updated information.
5. Take all necessary steps to correct or delete inaccurate information.
6. Data storage time should not be longer than required for the purpose for which the data are collected.
7. Ensure security of data against accidental or unauthorized access or manipulation. However, the data must be available to the data subject (the person whose personal data is processed) who, if necessary, shall be entitled to correct or delete any information about him/her.
8. Guarantee the implementation of safety measures in the event of data transfer abroad.

According to Bandypadhyay (2002) the Directive also provides the following rights to data subjects:

ILLUSTRATION 4. Rights which are provided by Directive to data subject



SOURCE: Bandypadhyay, 2002, E – commerce: Context, Concepts and Consequences, Mc Graw – Hill Education, UK, p.247

The right to information means that the data subject must always know when the data about him is collected, whereas the right of access provides secure access to the data in whatever form they are (text, images, etc.). Respecting the correction right, the subject has the possibility of correction or deletion of certain data. His/her last right leaves space for giving comments on certain data and information collected about him/her.

The abovementioned data protection principles apply to information regarding individuals, not organizations. If the data subject believes that there is a violation of one of the principles (or any other provision of the Law), but is unable to independently solve the problem, he/she can complain to the Commissioner for Information. If the Commissioner finds that the complaint is justified, and that it cannot be resolved informally, then he may decide to send a notification to the user of the data. On the other hand, the user of the data can appeal to an independent court for data protection. If it gets proven that a crime was committed, the Commissioner may pursue the user in court. However, the abovementioned principles of privacy are extremely broadly and vaguely defined, so it is very difficult to determine how much information is "relevant" or what constitutes "reasonable" activities, and as a result, to prove a criminal offense is very difficult as well. It is important to emphasize that there is a large number of exemptions from the DPA, which enables companies and other organizations to collect and keep personal data under certain circumstances. Also, this does not make it easier for consumers to understand and exercise their rights. As a result, the public is aware of a very small number of cases of data abuse and there are an even smaller number of achieved successes in proving the guilt of companies. Another reason for such a low rate of prosecution results from the fact that although the Information Commissioner is obliged to consider all objections, he does not have the authority to initiate an investigation against the registered users of data or the power to compel the companies to pay compensations to data subjects (Bandypadhyay, 2002, p. 249). However, the legislation provides a useful framework that companies must follow, and provides an opportunity for individuals in the EU, who are concerned about their privacy, to obtain the necessary information and support.

With the increase in the number of international consumer transactions, international transfer of data has increased significantly as well. It became necessary to regulate such cases, mainly because some

countries do not guarantee unconditional protection of data transfer. It is the eighth principle of the EU Directive on Data Protection that prohibits the transfer of personal data outside the European Economic Area (EEA) unless that country provides adequate protection for the rights and freedom of data subjects. This causes some problems because of the difficulties in adequate assessment of the level of protection, and requires the execution of certain checks (Bandypadhyay, 2002, p.251):

- If the data intended for transmission, they can be accessed from Web sites in the destination country.
- If the destination country is within the EEA then the transfer will not affect the eighth principle of the Directive on Data Protection, but there are other regulations that must be followed.
- There are certain exceptions to this rule, for example, if the company uses a Web site for selling goods abroad, it can take the names and addresses of customers for delivery.
- When it comes to countries outside the EEA, the European Union publishes a list of countries with the appropriate level of protection.
- For countries that are not on the list of "safe countries", adequacy tests are performed.

The last Directive on Privacy and Electronic Communications from 2002 (the Directive 2002-58 EC-Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications) requires the provision of basic rights and freedoms to natural persons in relation to the processing of personal data, especially when it comes to privacy rights, to ensure the free flow of personal data (Surčulija, 2004, p.50). The goal of this directive is to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy, as well as legitimate interests of legal persons in relation to the processing of personal data.

3.3. Data privacy protection in the Republic of Serbia

The protection of personal data is guaranteed by the Serbian Constitution and the Charter of Human and Minority Rights. The Law on Personal Data Protection regulates the conditions for collecting and processing of personal data, the rights of individuals and the protection of rights of persons whose data are collected and processed, restrictions on personal data protection, the procedure before the competent authority for personal data protection, data security, records, the transfer of data outside the Republic of Serbia and supervision over the implementation of this law. The protection of personal data is performed by the Commissioner for Information of Public Importance and Personal Data Protection, as an autonomous state body, independent in the exercise of its jurisdiction.

The objective of this Law is to, with regard to the processing of personal data; provide each natural person with the protection of privacy rights, and other rights and freedoms. According to the Law on Protection of Personal Data in the Republic of Serbia, data processing is prohibited if:

1. the individual has not given his/her consent to the treatment, or if the processing is done without lawful authorization,
2. it is done for a purpose other than that for which it was intended, regardless of whether it is done on the basis of consent or legal authorization for treatment without consent,
3. the purpose of treatment is not clearly defined, if it is altered, unauthorized, or already accomplished,
4. the person to whom the data relate to is specific or identifiable after reaching the purpose of processing,
5. such manner of processing is not permitted,
6. the data being processed are unnecessary or unsuitable for realizing the purpose of processing,
7. the amount and type of data to be processed is disproportionate to the purpose of processing and
8. the data are false and incomplete, i.e. not based on a credible source or are outdated.

According to the mentioned law the operator that collects information from the persons concerned, or from another person, shall inform the person to whom the information relates, or any other person, prior to collection, about:

- his/her identity and the name and address or company, or the identity of any other person responsible for processing data in accordance with the law,
- the purpose of collecting and further processing,
- the manner of data use,
- the identity of the persons or categories of persons using the information,
- obligation and legal basis regarding voluntary data provision and processing,
- the right to revoke consent to processing, and legal consequences in the case of revocation,

- rights of data subject in the event of unlawful processing and
- other circumstances who's withholding against the data subject or another person would be contrary to good faith actions.

The data related to nationality, race, gender, language, religion, political party affiliation, union membership, health, victims of violence, criminal charges and sex life may be processed based on the freely given consent of the person, except when the law prohibits the processing of such data even with consent. Processing of sensitive data is prohibited, except in certain cases (e.g. with consent given by the data subject). Consent to the processing of particularly sensitive information is given in writing, including the designation of the data being processed, the processing purpose and manner of their use. The Law on Protection of Personal data in our country states that the individual has the right to request that the operator accurately and fully informs him/her about:

1. whether the operator is processing data about him/her, and what kind of processing operations will be performed,
2. which data about him/her are being processed,
3. from whom the data were collected, i.e. who is the source of data,
4. for what purpose and on what legal basis are the data being processed,
5. which data collections contain information about him/her,
6. who are the recipients of data,
7. which data, i.e. what kind of data are being used,
8. what are the purposes of using data about him/her,
9. on what legal grounds are the data being used,
10. to whom are data transferred to, and which data,
11. purposes for which the data are transmitted,
12. on what legal basis the data are transmitted and
13. during which period of time the data will be processed.

According to the Law, the individual has the right to request from the operator to have insight into the data relating to him. The abovementioned includes the right to review, read and hear the data and to make notes. Also, the individual has the right to terminate and suspend processing, if he doubts the punctuality, completeness and accuracy of data, as well as the right to mark such information as disputed, until their punctuality, completeness and accuracy are confirmed.

In our country, there is a present and developing awareness of the need to regulate the issue of privacy in internet marketing, by developing legal practices and other measures, by inclusion of consumers' interests in the formulation of legislation, amending consumer policy, strengthening consumer associations and their active participation in the decision-making process. However, the Law on the protection of personal data is inaccurate and inconsistent with international standards, and deficiencies are such that it is impossible to upgrade, so it is desirable to make a new one as soon as possible. Of course, modern international standards do not guarantee an absolute right of privacy, because there are always areas in which those rights are significantly restricted, such as government and public safety, criminal prosecution, and all the situations where the public interest outweighs the individual.

4. CONCLUSION

We live in an information society, in which power and wealth largely depend on information and knowledge as a central asset. The controversies that arise around the collection and use of information are the result of companies' battles to increase their strength, power and influence on the market in such a manner. Therefore, the protection of data and information is one of the most important issues from the consumers' point of view. Governments of most developed countries are intensely trying to keep under control, through laws or unwritten rules, the protection of all data related to existing and potential customers. Generally speaking, in the future we should expect the emphasizing of importance of laws that directly or indirectly relate to this issue in an effort to increase consumer confidence in Internet marketing activities. Internet marketing is an activity that is in the growth phase and every day it gets more and more important, especially because of the great impact it has on the creation and maintenance of partnerships between companies and users, i.e. consumers. Since Serbia has recently become a candidate for membership in the European Union, it is necessary to commence on time the process of adapting our own laws on privacy and data protection of Internet users. The European Commission has defined new rules which guarantee greater control over personal information on the Internet, and that should start to be applied by the end of 2013 after being ratified by all member states of the European Union. According to these rules, the responsibility of society to protect user data would be much larger; each

user would be entitled to remove their data from the network, as well as profiles and e-mail accounts if he wants to. This would resolve some of the current issues about who retains user data, whether the companies use them properly, are they allowed to keep them at all, and in what time frame. New measures aim to provide Internet users with the ability to be the owners of their own data, not a web page, social network, or the company to which the data were made available for a particular purpose.

References:

1. Bandypadhyay, N. (2002), *E – commerce: Context, Concepts and Consequences*, Mc Graw – Hill Education, UK
2. Končar, J. (2003), *Elektronska trgovina*, Ekonomski fakultet Subotica, Subotica
3. Laudon, K.C., Traver, C.G. (2002), *E – commerce*, Business Tehnology Society, Addison Wesley, Boston
4. Marković, A. (2003), „Zakonska regulativa i Internet", *Zbornik radova III Međunarodnog simpozijuma o E-trgovini i E-poslovanju, Agencija «E-trgovina»*, Palić
5. Salai, S., Končar, J. (2007), *Direktni marketing*, Ekonomski fakultet Subotica, Subotica
6. Surčulija, J. (2004), *Evropski pravni okvir za elektronske komunikacije: osnov za izgradnju informacionog društva u Srbiji*, Centar za razvoj Interneta, Beograd
7. Zakon o zaštiti podataka o ličnosti Republike Srbije, www.zakon.co.rs/zakon-o-zastiti-podataka-o-licnosti.html, pristupljeno: 12.11.2012.

Rezime:

Razlike u zakonskoj regulativi zaštite privatnosti podataka u internet marketingu u SAD, Evropskoj Uniji i Srbiji

Jasmina Markov, Biljana Lazić

Sve je veći broj preduzeća koja se u svom poslovanju i kontaktima sa potrošačima okreću Internetu i koriste ogromne mogućnosti koje on pruža. Stoga, Internet marketing danas doživljava izuzetnu ekpanziju i smatra se segmentom marketinga podložnim intenzivnim i kontinuiranim promenama. Uporedo sa pozitivnim efektima koje donosi kako preduzećima tako i potrošačima, javljaju se i negativnosti koje prate ovaj oblik marketinga, a jedna od njih je nedovoljna zaštita privatnosti podataka. Činjenica je da se mora podići nivo zaštite podataka i unaprediti njen kvalitet. Intenzivne promene se moraju preduzeti na normativnom planu, jer još uvek postoji dosta razloga za nezadovoljstvo potrošača kada je u pitanju zaštita njihove privatnosti. Dakle, zakonodavstvo mora da odigra jednu od ključnih uloga u izgradnji poverenja potrošača i uspostavljanu pozitivnih odnosa sa marketarima. Cilj ovog rada jeste ukazivanje na značaj izgradnje takvog nivoa zašitite privatnosti podataka koji će omogućiti uspostavljanje dugoročnih i partnerskih odnosa između potrošača, marketara i ostalih učesnika na tržištu, s obzirom da samo pomenuti odnosi mogu doneti prosperitet svim stranama. U radu će se izvršiti uporedna analiza zakonodavnih okvira u ovoj oblasti u SAD, zemljama Evropske unije i Srbiji i istaći i dalje prisutan značajan zaostatak Srbije u odnosu na pomenute razvijene zemlje.

Ključne reči: Internet marketing, zaštita potrošača, zaštita privatnosti, zakonodavstvo

Kontakt:

Jasmina Markov, Asistent
jasmina.markov@gmail.com
Visoka poslovna škola strukovnih studija Novi Sad

Biljana Lazić, Asistent
vps.biljalazic@gmail.com
Visoka poslovna škola strukovnih studija Novi Sad