BILETA

15th BILETA Conference: "ELECTRONIC DATASETS AND ACCESS TO LEGAL INFORMATION".

Friday 14th April 2000.
University of Warwick, Coventry, England.

Privacy in the Yugoslav Cyberspace - Problems and Protection

Mirjana Drakulic, Ph.D.* **and Ratimir Drakulic, M.S.****
*Associated Professor of Computer Law and Business Law
**Assistant of Introduction to Information Systems
Faculty of Organizational Sciences, University of Belgrade
Belgrade, YUGOSLAVIA

Abstract: *With the current expansion of the Internet, privacy is once again becoming a hot issue. This global computer network has become the arena in which an individual is trying to fight for his/her privacy. Numerous 'evil enemies' are pursuing him, be he simply a user, visitor, or consumer of information, or just a record on a database. The mere act of collecting, memorizing and distributing this data about a person jeopardizes the individual's privacy, and this in turn opens up the debate about protection issues. The primary ways in which computer networks' threaten personal privacy are discussed in this paper. Yugoslav cyberspace brings so many new questions, especially in the field of the law. The paper presents the Yugoslav legal solutions in solving this attractive problem.*

Key words: privacy, rights, Internet, aggressors, Yugoslav cyberspace and legal protection.

1. WHAT IS HAPPENING ON THE INTERNET?

Internet has become the space in which an individual is trying to fight for his privacy. Numerous `evil enemies' are chasing after him, especially if he/she has the role of a user, visitor, consumer or `ordinary' individual about who databases are created. Jeopardizing privacy related primarily to collecting, memorizing and distribution of data and information about the person.

Meanwhile their detecting (gathering and disclosing) is not less dangerous, neither likes appliance specific methods for their gathering (spying, recruiting, watching or disturbing). All of Internet hasn't same value of risk for individual and her/his privacy. Specific Internet service is appropriate instrument of this.

Also conducting business transactions on Internet also requires a great number of participants. Each business operation opens numerous controversies, for example, the requirements for openness, accessibility, easiness of communication, advertisement, negotiations, contracting, distribution and realisation of certain business transaction, opposite of secrecy, privacy and confidentiality. Especial exactly pawn for secrecy, privacy and trustworthiness was orientated primarily on individual and their right to be protected from: interference into private and family life, physical and psychological integrity, attacks on moral, intellectual life; honour and dignity; unauthorised use of name, identity or person; abuses of private communications. All participants who are conducting business

electronically, because they are the focus of attention of numerous interested and often unauthorised controllers experience such interference and invasions to privacy.

Messages related to e-mail and e-conferences are also threatened by dangers in **public and private communication systems**. Providers must not overview neither audio nor other types of messages. However, it is often needed that they are controlled for the purpose of protection from criminal and that is deviation from the rule. Situation is far more delicate when private systems are at stake, where according to their `*rules of conducting operations*' it is allowed. Privacy of e-mail and dialogs via e-conferences is seriously endangered because of `**property rights**'.

There is more and more involvement in the field of `**information about the person tied to telecommunications**' which is collected about the `*potential consumers*' for different `*providers*'. In rendering telecommunication services there have to be limitations in respect to individuals - users, who have to be informed that certain data about them are placed in databases related to these services. Here, there are problems of control and responsibility of their logging and `spreading' in telecommunication infrastructure and networks, as well as collecting and aggregating for market needs. Browsing such sites and over viewing data that they contain represents serious problem.

Attractive and interesting sites also challenge numerous visitors, who, navigating through information super highway, `hang' on them, often more than one time. Particularly interesting and attractive are unlawful and damaging contents whose browsing and visiting, especially by minors, has caused the need for monitoring and control.

However, it is even greater problem to follow the paths which **surfers and/or users of video or other on-line services** went through in searching for relevant data. These problems are twofold: they with their activities jeopardise privacy of others, while providers or services and other surfers jeopardise their privacy. Thus, the circle is closed.

Certainly that collection and distribution of data about the personalities of `ordinary' individuals is conducted for many other purposes, and one of more significant is their sale. That is big and profitable business. It is growing into powerful industry. Many of these data are used for marketing and advertising because they are necessary for attracting buyers, in order to know what, when, how often and for how much they obtain certain goods, where and in which way. Thus, specialised agencies often motivated by the reasons of political nature keep data on individuals, which can be easily, connected. `The book of clients' becomes ever more detailed and complex proportionally with increase of number of competitors and volumes and types of goods that are offered. That is also the case with the `lists of political counterparts' which appeared in some countries.

Of course, these are only some of dilemmas which are part of privacy issues in the Internet environment and which open even more numerous and more complex controversies than it was the case before. Appearance of anonymous virtual personalities, which are, raises a question whether virtual or real aggressors conduct invasion on privacy? Separate problem is providing for legal protection of privacy in circumstances where the role of national states in its regulation has become minor, when the state borders are being eliminated, on one hand and where global consensus is being developed, on the other. This has caused the changes in the approach, as well as emergence of the new concept that would be more acceptable than the traditional one.

2. WHO ARE THE ASSAILANTS?

If something is not disputed that is that privacy is under attack of real enemy. Although sometimes their aggression is hidden, silent, secret, and sometimes open and direct, it is real one. Most often aggressors are **states** (their bodies and agencies), `**private sector**' and other **individuals**.

2.1. States

States often `consider' that it is their natural right to have access to all data on individuals (regardless of whether they are its citizens or not) who are on its territory or on its citizens out of the state. There is twofold problem here: **on one side**, an excessive involvement of the state and its bodies into data about persons under the claim that in `the contemporary conditions processing of data and information is the basic function of state' and, **on the other side**, that in these activities the state (administration), its bodies and agencies may (ab)use data which they collected, processed and memorised on the basis of official and other evidences. The danger is even greater when the individual is more helpless in relation to aggressor. This is becoming more actual issue with increasing number of secret bases, which contain many data on numerous individuals.

Sometimes these invasions are undertaken in order to solve `clashes' among different levels within the same authority, different bodies or agencies, administration and parliament or political counterparts (governing or these in opposition). This offence is undertaken and used for retribution with civilians.

In any case, the state represents one have the most often and most cruel aggressors to privacy. Along with that, vested with power and force, it in the same time represents such aggressor against whom the individual can hardly fight, and even more hardly can get out as a winner.

2.2. `Private Sector'

Preoccupation of lawyers with attacks to privacy conducted by states, their bodies and agencies, at the beginning covered the increasing danger from `private sector' and from existence of private databases. A little number of countries put under control these data basis and these entities. However, with the time when the number of this basis was growing progressively, as well as number of different data obtained in different ways, it was growing uneasiness because they were `exempted' from control. Researches show that there is increased fear of individuals because of totally losing control over transactions related to data about them. Data show that concern for possible attack to privacy by state is negligently decreasing, while it is increasing when the companies - `private sector' - are at stake. Also, there is growing concern of consumers because of to make impossible of control on how data about them are being used in companies or how they circulate among them. There is also increased number of persons who refused to give their data because they considered `that they are not needed for the companies or that they are too private'. Great number of examined consumers consider that their right to privacy is not properly secured and that it will not get better until 2000, it will even be worse.

There are numerous attack conducted by: **sellers of telecommunication, video and information services** (control accesses of users); **Internet service providers** (keeping data about their assets, electronic address, numbers of business and private telephones, addresses, credit reports, etc. and which collect directly from user or from on-line registry, mailing lists, etc.); **competitor companies** (collect data, for instance, on managers, researches of the competitor company); **`look up' services** (review and use, and even further send sensitive identifiable information such as social insurance number, identification number, maiden name, address, data of birth, etc.); and other **information users** (who collect adequate and relevant data about person directly from the individual). Appearance of all these entities draw the attention to loophole that was widening with growing use of information technology, especially, with computer networks.

2.3. Individuals

Individual is not only jeopardized by publishing and manipulating personal data without permission and control, but is in the same time aggressor to privacy of others. There are many reasons why they do that, but most often are:

a. Curiosity;

b. Malicious intentions (for conducting criminal acts, acquiring unlawfully material funds, misrepresentation);

c. Solving financial (alcoholism, drugs, gambling or betting, etc.) or **personal and family problems** (health care, education, etc.);

d. Mercy;

e. Blackmails and extortion for secure a benefit;

f. Political and ideological reasons (discrimination and discreditation of political counterparts, their family members or close associates, etc.);

g. Religious reasons;

h. Illness, mental or physical which causes unadjusted behaviours in relation to another familiar or not familiar individual;

i. Characteristics of persons (malicious, envious and jealous persons);

j. Revenge;

k. Irresponsibility, and negligence - in conducting activities related to data about persons;

l. Proving themselves; and many others.

Without a doubt, each of these motives is equally dangerous regarding privacy, but it seems that appearance of computer and cyber criminals has made more dangerous many of them. These individuals have certain characteristic, as well as particular specific forms of behaviour (Icove D., Seger K., VonStrch W., 1995). Their ways for reaching needed data can be entirely innocent; but always followed by different methods and techniques. It is frequent the case that their application is consequence of thorough preparations and well-planned action. They gather all possible data, even those which they consider useless for protection (brochures, catalogues, web pages about products, trash). Breaking-in, attacks, stealing, vandalism, sabotage, spying, frauds and many other manipulations with data about person represent only tip of an iceberg of invasions to privacy of individuals by other individuals.

3. PRIVACY IN YUGOSLAV CYBER SPACE

3.1 Yugoslav Internet environment

Yugoslav cyberspace is not enough developed, inside of it are approximately 150 thousand electronic, virtual, addresses in reference to 10 millions citizens. But, there is full of contrary especially in last year. Many activities are on the edge of permission or even on the other side of the law. The most expressive is **hacking** and the most widespread is **stealing of Internet time**. **Illegal and harmful contents** are also present.

Hackers, alone or in groups, are sliding inside of this, and specially in foreign cyberspaces. There are a tenth of attack attempts per day on computers of main Yugoslav Internet providers, but not only from Yugoslavia. Results are `knocked down' sites, interrupted connections, slowed down access, and numerous spam messages, with attached viruses, which strangle normal flow of Internet contents, because some of them ends successfully. This are often causes for interrupting the privacy `in the name of security'.

For example, in January 2000 site of one of the best Yugoslav news provider, www.inet.co.yu, was demolished [Picture 1]. This site which simultaneously gives news in Serbian and English became a referent source of current information during the NATO intervention on Yugoslavia in a spring 1999. In a period from March to July 1999 every 5 minutes was a change of contents. Today, this dynamic is every half an hour [Picture 2]. Very soon, the link to this site was on many sites of world news agencies, for example CNN or BBC. Unknown hacker deleted all usual contents and put illiterate note `Pleas, stop to poison yourself and especially children!!!!!!' After this on the bottom of the page was written `we pillaged this with BRE-BRE!!!!!!!!' (BRE- is insulting expression originally Turkish word which has been in use in Serbian since the period of Turkish occupation).

Besides this, other sites were knocked down. That is only logical extension of reinforced hacker activities that have been going since the NATO aggression on Yugoslavia, when the situation began to be particular very critical. At that moment Yugoslav cyberspace was for the first time in the centre of attention of all Internet users in the world because the often attacks which have been spreading to others, especially the NATO countries. It was specific war, the Internet war. This cyberspace war is characterised by (Drakulic M., Drakulic R., 1999):

* National homogenisation and parallel activities of Serbian hackers-individuals and groups regardless of geographical and political disposition;

* Making the `antiNATO hacking alliance' of Russian, Ukrainian, Chinese and Serbian hackers while pro-NATO hackers are `freelance', and by some opinions they do not work because of political reasons but rather to attract attention;

* Shapes of hacking activities, no matter if they are individual or by groups, include mail bombing, with or without attached viruses, manipulations with contents, manipulations with sites log, manipulations with navigation or manipulations with related links, examining the IP addresses; and

* Attacks on Yugoslav servers and sites, according to inquiry, the most of them from Germany, Holland, Croatia, Bosnia and Herzegovina, Great Britain, USA, Poland, Island and some other countries. Most servers with Microsoft operative system were attacked, mainly the mail and log procedures. These attacks were not synchronised. There were more attempts (depending on providers from 3 per 78 days, up to 10 times a day) than real attacks. Some of Yugoslav sites were closed for a few hours.

To these activities proceeded fights between Serbian and hacker of ex Yugoslav Republics, especially of Croatia. In these fights were damaged many sites in Serbia and Croatia, and threating of possibility to outgrow in larger. In March, already known Serbia hacker group `**The Black Hand**' attacked world famous browser Yahoo. A virus was inputted, so Yahoo was blocked. Few seconds before the virus was inputted hackers warned compatriots to turn off their computers. The ones who did not listen had a real computer attack. There was no picture on the screens but a note `LIVE SERBIA-THE BLACK HAND'. After a few minutes everything turned back to normal. Isn't that similar to the activities that happened on January and February of 2000 (www.epic.org) with the same browser but also with other sites in USA (E-trade, Datek, ZDNet, Amazon, CNN, eBay, Buy.com) and in another countries [Picture 3]?

Two months after International troops entrance to Kosovo, exactly on 27th August of 1999 hacker once again subvert one of NATO sites, www.nato.int, and put on a picture of Serbian general Draza Mihajlovic [Picture 4] who was commander of `Chetnic' units in II World war (during the 19$^{th}$ century and at the beginning of the 20$^{th}$ century `Chetnic' were fighters for free Serbian contras against Turks, but in II World war they accede on German side. Today some of nationalistic politic parties try to rehabilitate general Mihajlovic into a fighter for liberation of Serbia against communism). Picture stayed on about 30 minute instead of original content. Also, on site stayed text of salutation: `Greetings from Serbia', also and `Stop violence to Kosovo... and help us against

Milosevic. Serbs have children, too'. Responsibility for this took `Serbian Hackers'. Who really stayed behind of this act, it is still unknown. However, attacked and disturbed is one of the most and best-protected sites on Web.

About of 10% of Yugoslav Internet time is stolen. One of illustration examples happened in Belgrade in the middle of January of 2000 when actuated public investigation against young man who stole user password files on the way that he sent greetings cards like as small .exe files. Provider had to stop business on a few days to determinate a problem. But, **stealing Internet time** isn't preferred only for individuals. In the last time organized groups also frequently use it. In the middle of 1999 one case animated many subjects. Namely, one provider at south of Serbia already a long time has a problem with permanent attacks. After a regional investigation, it was discovered that to this group also helped employees from phone central because they have access to Web. With phone numbers they detected a subscribers from whose private apartments they performed an invasion. Also, attackers have access of all segments of Web and permanently watching e-mail jeopardizing privacy of this. This group on one free site publicised list of all e-mail and password users of that provider which is usual to bring up to date. Also, group sent an invitation to all interested for the list, to use it when they surf on Internet. Interesting in this case is that the group gave an offer to provider that they will give up of their activities if provider give them some services for compensation.

Situating **specific contents** and access to these contents, also is appropriate terrain for conflict of privacy and needed for regulation. Presentation of pornography and children pornography, terrorist contents, religious sects, narcotics, prostitution and escort, virtual gambling, sport-gambling, is only a part of fan interesting and attractive contents, which could be found. To this it should be added homepage of individuals who propagate specific ideas and attitudes. All of them begin to be very interesting for various controllers who under false decency only restrict privacy.

All of that are reason who shall animate provider but also and other subject that with more serious action does something against protection and safety on Internet. In this protection and safety, absolutely can't be endangered privacy.

3.2. What is jeopardised?

E-mail began especially attractive for many eyes. In middle of 90s happened first raid in privacy of e-mail in Yugoslavia. Raid has done by one student and harmed side was his professor. Student, without authorisation reviewed at professor's international correspondence, and about that left him a note as suggestion that he should accept a job.

Other side of this problem is that large parts of **employers inspect in e-mail of employees**, with or without their knowledge. Until now in Yugoslavia hasn't been any investigation about reasonable control of Internet and their parts neither any data about dimension of monitoring. Extreme situations only warn about its appearance and damages in domain rights of privacy and privacy on information. Some part of academic Web became problematic because some users don't use it anymore since existed malversation of e-mail which finance state (www.internodium.org.yu). First suspicion about controlling e-mail was born in *Students' protest* time in 96/97. Students after 7 days of protest made decision about Internet presentation of all their activities. They showed reasons of protest and several times during the day the news were changed because they were in connection with students activities and actual happenings in Serbia. Web has done its basic function - permanent informing and connecting of users. Web pages of *Students' protest* were very visited (during four months there were over 80.000 visitors) and over e-mail thousands of messages had been changed. These messages were monitoring, but their authors in that time didn't have troubles (Drakulic M., Drakulic R., 1998). Second wave of suspicion was in 1999 during the intervention of NATO - in the Yugoslav ether circulated `a breeze' that all electronic messages, even e-mail is under control institution of NATO countries. Both suspicions doesn't exact affirm or unconfirmed.

News which appeared on 17th March 2000 in Yugoslav cyberspace (www.inet.co.yu) agitated souls: *Yugoslav Constitutional Court today acclaimed as unconstitutional the regulation of federal Law of state security, according to which functionaries of security services are allowed, on their own decision, to eavesdrop phones, take-over electronic massages, faxes and open letters `in case that is necessary for FRJ security'* [Picture 5]. The public in Yugoslavia didn't know that will agitate a motion for actuate process, neither such regulation like this. Similar case is with identical regulation in republic act; against whose illegal act is also actuating a process seven years ago and lay to deadlock.

To this also should be added growing numbers of Web addresses in which could be found data about individuals gated on the different ways [Picture 6, Picture 7], even that registration in appropriate on-line form from unauthorised person. So, for example, on site www.mse.cg.yu [Picture 8] is possible in addresses entering data of any person without permission. Data is put on web and can be used without any limit.

Having this on mind it could be made **conclusion**:

* Jeopardizing e-mail is present, but without enough data about size and from whom;

* A small number of cases and information of these is accessible for majority of public;

* Most usual forms of interruption are related to infiltrate (especially during NATO intervention in Yugoslavia that surely didn't begin and also didn't stop with it); reading from unknown person (provider, hacker, etc); leaking of data from users databases of providers (addresses, path, etc.); making (by play) addresses, such as e-mail [Picture 9], etc; chain letters (invitation for solidarity, propagation of love or cursing, blackmails, threatens). Data about these modalities distribute by the same e-mail or by chat rooms.

Chat rooms and new groups also are very interesting for everybody who wishes to know what is happening in that part of Internet (www.internodium.org.yu). Often, specific data leak in public. That provocateur reciprocal protests, but until today has no clear vision about what strictly personal data it is? In meantime in one of e-mail address existed panic because of some personal data needed for work of ISP, became easy accessible for everybody. Some providers disassociated themselves from responsibility for privacy of data of its users. Still, in contract of one them exists a regulation: provider is not responsible for violation of justice on user privacy and safety, which on Internet makes third person. Yet render of these services shall not be responsible only if he attempts all adequate measure. If they stay-away or if they insufficient, responsibility can't be recalled. To this should add answers on questions: Does the Internet provider must take care about category of data, which he collected? When, to whom and why he can put data on disposal?

4. YUGOSLAV LAW IN GAP

Yugoslav law during many years is trying to successfully finish fight with problem of protected privacy and information privacy. Preparing lasted too long. The most developed countries it's first acts brought in the beginning of 70s. Almost five years after them began preparing to make appropriate regulation in Yugoslavia, but *The Law on Protection of Personal Data* brought, in 1998. Fundamental for its restitution there is *The Constitution of the Federal Republic of Yugoslavia*. Nevertheless, *The Constitution* in Section II: Freedoms, Rights and Duties of Man and the Citizen anticipate `The inviolability of the physical and psychological integrity of the individual, his privacy and personal rights shall be guaranteed. The personal dignity and security of individuals shall be guaranteed' (article 22.). So, it precise `Privacy of the mail and of other means of communication shall be inviolable. Federal statute may prescribe that, under a court decision, the principle of inviolability of privacy of the mail and other means of communication may be put in abeyance if so required for the purposes of criminal proceedings, or for the defence of the Federal Republic of

Yugoslavia' (article 32). Especially important is article 33, which says, `Protection of the secrecy of personal data shall be guaranteed. The use of personal data for purposes other than those for which they were compiled shall be prohibited. Everyone shall have the right of access to personal data concerning him as well as the right of court protection in the event of their abuse. The collection, processing, utilisation and protection of personal data shall be regulated by federal statute'. The same year Yugoslav Parliament has ratified *European Convention for the Protection of Individuals with Regard to Automatic Processing in Personal Data*. Although there were made legal terms for passing a special law for protection privacy and information privacy, it could pass a long time, to really happen.

The Law on Protection of Personal Data protection is for data about personality of citizens. These data are gathered, processed and used only if they are in concord with purpose which is affirmed by the law, or if exists an agreement of citizen. Interesting is that in Federal and Republic acts is provided obligation to compose certain data of personality. Also, to this must be added numerous data, which with citizens agree, but still today haven't sure fact.

Citizen has next rights:

a. The right to the access of information, respectively the right to find out **1)** which collections of personal data contain data referring to him/her, **2)** which data on him/her are being processes, for which purpose and on what grounds, and **3)** who are the users of personal data referring to him/her, and on which grounds (article 11);

b. The right to demand from the body supervising the collection of personal data **1)** the information concerning the existence of a collection of personal data and a written proof (certificate) on the personal data kept on him/her, **2)** a review of the data referring to him/her, **3)** correction of wrong data, **4)** deletion of data referring to him/her if the processing thereof is not in accordance with the law, respectively the contract, **5)** ban on use of wrong, outdated and incomplete data referring to him/her, **6)** ban on use of data from collections of data and similar databases if they are not used in accordance with the law, respectively the contract (article 12);

c. The right on remedy in case of the breach of the individual's right and injury resulting in the use got in the way or for the purposes not pursuant to the corresponding provisions of the law. A citizen whose rights set forth in this Law have been violated, or suffered damages as a result of use of gathered data in a way or for purposes contrary to the provisions of this Law may bring a lawsuit for damages before the court in charge (article 15).

Simultaneously, it is **requested specific quality of data**, which means that have to be correct, up-to-date and based on credible sources, and, bearing in mind the purpose they are gathered for, complete. Of course, they must be gathered in a manner that does not offend the dignity of man, even that they must be gathered from other citizens or taken over from the existing collections of personal data in cases set forth in the law, or under a written consent from the citizen.

Still that, it must be pointed out that under **`the citizen'** isconsidered `everybody, the physical person to whom the data refer'.`**The personal data'** is `the information contained in the collection of such data, and refer to the privacy, personal integrity, private and family life and other personal rights related to the identified person or an identifiable person'.

Something, which is specifically anticipated is the appropriate federal law administration body supervises the observance of this law. **Federal ministry of Justas**, who jurisdiction is entitled to review:

a. The contents of the register of collections of personal data and the contents of collections of personal data;

b. The documents referring to gathering, processing, keeping, transfer and use of collections of personal data;

c. General documents issued by the body supervising the collection of personal data related to measures and procedures of protection of personal data;

d. Premises and equipment of importance for realisation of protection of collections of personal data.

It also can prohibit the gathering, processing, use and transfer of personal data if it finds out that the conditions set forth in this Law have not been **provided or order**:

* Elimination of irregularities in protection of personal data within a certain period of time;

* Deletion of the entire collection of data if it has not been created, or is not used, in accordance with the law;

* Change or ban on use, or deletion of personal data, if it finds that personal rights of citizens have been violated.

Beside regulation about right of individuals, especially important is regulation about of rights and obligations of **body supervising the collection of personal d**ata, as a legal entity or an entrepreneur, authorised by the Law or a written consent from the citizen to gather, process, keep and transfer personal data and establish, maintain and use the collection of personal data. This body can, or must to:

a. Founds such collection solely for the needs set forth in the law or based on a written consent from the citizen;

b. Establishes and keeps the catalogue of collections of personal data;

c. Process and keep personal data;

d. Cede the collection or a part thereof to users empowered by the law or under a written consent from the citizen;

e. Entrust the duties or part of the duties related to establishing and keeping the collection, respectively gathering, processing, keeping and revealing the personal data from the collection, to other legal entities or entrepreneurs registered for such activities;

f. Defines the measures of safekeeping and protection of the data from destruction, loss, unauthorised use, changes or disclosure; measures aimed against unauthorised access to premises, equipment and technique used for processing the personal data; measures and procedures in cases of emergencies; and persons responsible for the collection of personal data;

g. Keeps the register of the collection.

Also it should be added providing of **principle of reciprocity** for personal data if the state the data are taken to has established the protection of personal data which encompasses foreign citizens on a level which may not be below that provided by this Law.

If exists infringement of the Law an enterprise or another legal entity or entrepreneur or responsible person shall be fined.

Regulation of the Law, still, is not enough to determinate problem of protecting privacy in specific condition and surrounding such as Internet. Solution for specific Internet problem requests a new way out.

Self - regulation is one of the answers to the `glove' which the Internet has thrown to the Yugoslav arena of privacy protection. In the same time there appear some misunderstandings between proponents and opponents of this solution. This conception has many followers in many countries. Its proponents are louder in their requirements that these rules must necessarily be. They consider that self - regulation should replace or in some instances be added to the state regulation, because the requirements which are imposed by the market are more realistic then the state ones. Along with that, they emphasise that their advantages are in creation of rules on the basis of collective experience based on ethic principals of participants, in reduction of common norms in compliance with demonstrated practice and in easier establishment of rules which participants can better build together than individually. Of course, this concept also has its opponents or at least those who doubt in its efficiency in replacing existing regulation (may be as useful experience can serve the example of social agreements and self-management arrangements which was dominant in Yugoslavia during the period of self-management socialism). They also object `forgetting' that the central place is the interest of the user and not of the individuals who are margined in the evasion of market values. The separate problem is control over implementation of such created rules, as well as penalties for those who break them. Still it is the question whether the self - regulation is safe gateway for privacy and information privacy to electronic highway? On the other side, such approach should not be a priori refused, moreover because many countries re-examine the efficiency of existing legal frameworks.

5. CONCLUSION

Yugoslavian cyberspace obviously is beginning to pile a many problems in the protection of privacy and information privacy. Formation of act regulation continues so long, with inappropriate use. Also, existed rules are to enlarger because of lower `lawyers culture', on the one side, and not existing `habit' of respect for human rights, on the other. Still, something which is for more attention is that `legal veil' of protected rights to privacy and information privacy is not big enough to cover Internet surrounding. Others word speaking, right like a veil should wrap up privacy and information privacy. That who is under the veil must see what is going on in the surrounding, but anybody from surrounding should not see what is under the veil. That veil could be proper protection it must be big and dense enough. A long time veil of Yugoslav Law didn't exist, and now it became too small.

REFERENCES

Drakulic M., Drakulic R., Balkan Hackers War in Cyberspace, Bileta, 14th Annual Conference, Cyberspace 1999: Crime, Criminal Justice and the Internet, March 1999, CyberLaw Research Unit, Centre for Criminal Justice Studies, University of Leeds, http://www.leeds.ac.uk/law/ccjs.

Drakulic M., Drakulic R., Yugoslav Legal, Ethical and Social Dilemmas of Information Technology, Information Society: Looking ahead, Promises and Achievements, CREIS, 11th European Colloquium on IT and Society, Strasbourg, 1998, pp. 75 - 83.

Icove D., Seger K., VonStrch W., Computer Crime, A Crimefighter's Handbook, Sebastopol, O'Reilly & Associates, Inc., 1995, pp. 65 - 69.

Savezni zakon o ratifikaciji Konvencije o zastiti pojedinaca s obzirom na automatsku obradu licnih podataka (*Act of Ratification of European Convention for the Protection of Individuals with Regard to Automatic Processing in Personal Data),* Sluzbeni list br. 1/92.

Ustav Savezne Republike Jugoslavije (*The Constitution of the Federal Republic of Yugoslavia),* Sluzbeni list br. 2/92.

Zakon o zastiti podataka o licnosti (*The Law on Protection of Personal Data),* Sluzbeni list br. 24/98.

[Pictures were not available at the time of printing.]