

TOWARDS A SURVEILLANCE SOCIETY

Abstract

The paper deals with the issues of data gathering, surveillance and intense use of targeted messages in contemporary living space shaped by technology and by the capitalist view of the world. Those who possess a relevant knowledge about others, possess a power over them, and they can use and abuse this power in various ways. Intense data gathering, observations and surveillance facilitate the manipulation of people and allow the real holders of power to shape the social reality in the ways that serve their interests, but which can easily lead to a totalitarian society. Totalitarian systems used to be imposed by states and by religious organizations, and they were based on political ideologies or religious dogmas. Using the power of technology, contemporary capitalism has been creating a new business civilization which nominally promotes openness and freedom, but which shows clear totalitarian tendencies. The paper puts forward a series of critical reflections related to these issues.

Key words: *data gathering, consumer profiles, observation, privacy, surveillance, targeting, business civilization, totalitarian society*

1. Observing and gathering

Information technology makes possible for ordinary people to record and make public various events, and to provide evidence of various abuses to which they have been exposed; in this way information technology helps the weaker to protect themselves from the oppression of the stronger. However, at the same time, information technology helps the stronger - holders of economic power and various institutions - to introduce efficient systems of a complete surveillance and control of the weaker. In other words, the Information Society shows a tendency to move towards the Surveillance Society, which actually means towards a *totalitarian society*. Data gathering and surveillance tend to be secretive, so that the professionals in this field could be the only one who know exactly what means and methods are used in these activities. However, technical details are not essential here because this discourse deals primarily with the *psychological and social effects* of the intense observation of the people and of their intrusive targeting with specific messages, regardless of the means and methods used, by whom and for what purposes it is done.

Holders of power and various institutions have always gathered data about their subjects and observed their behaviour. However, contemporary information technology has radically increased the possibilities of observation and data gathering, as well as of processing of the data gathered in various ways, places, times, and forms. People are increasingly observed at their workplace; companies normally observe the Internet and telephone communication of their employees (cf. Castells 2001; Barney 2000). However, information technology allows observation of the people virtually at every step. Every gate that a person

* University of Rijeka, Faculty of Philosophy, Dept. of Informatics, Omladinska 14, 51000 Rijeka, Croatia

mradovan@mapef.ffri.hr

Članak primljen u uredništvo: 3.06.2006.

passes through and all spaces she enters can register some data about her and about her activities. Various devices we use or pass by can do the same. A device can take fingerprints of the one who uses it; another can check the presence of various ingredients in his breath, such as alcohol or drugs. Cameras that record passers by can send the images directly to a central system which checks in its database if some of the recorded faces is a suspected criminal, a terrorist, or wanted for some other reason. These possibilities are not only hypothetical; according to various reports, all these methods of observation and data gathering, as well as many others, have been tried or practiced. There are probably numerous activities of that kind going on around us, which are not known to ordinary citizens.

Data gathering, observation and surveillance are nominally practiced mainly for business and security purposes, but the data and knowledge acquired for these purposes can be used and abused for various other purposes. These activities and their results can be used for manipulation and exploitation of the people; they can allow the holders of power to shape people and social reality in the ways that serve the aims of the holders of power. It has been said that knowledge is power, and that power corrupts people. Those who can know virtually everything about others, possess power over them and they can use this power in many ways, some of which may be abusive, harmful and destructive.

Issues related to data gathering, observation and surveillance of the people have been given a notable attention in academic research as well as in public discourse (cf. Regan 2002; Ball 2002; Ploeg 2003; Koops 2003; Viseu, Clement, Aspinall 2004). However, these analyses and discussions deal primarily with the issue of privacy; in the present paper we argue that *mistakes* in the processes of data gathering, observation and surveillance, and *abuses* of the results of these processes, can have much wider and more dramatic social consequences than the (mere) loss of privacy normally has.

2. Profiling the people

By our daily activities we constantly create data which can be recorded by various devices. For example, when we pay with a credit card, we create data which show on what we spend our money, and what amount of money we spend. Each such piece of data by itself does usually not tell much; however, on the basis of a collection of such pieces of data gathered together, it is possible to form a "portrait" of a person; such portraits are usually called "profiles". In the techno-economically stronger countries, data gathering for commercial purposes has become a normal business activity. There are companies which collect commercially relevant data about individuals and communities; they obtain such data from various sources such as shops, agencies, and other services. On the basis of these data, companies form consumer profiles of the individuals and of communities. Companies which produce such profiles, sell them to businesses which are interested in contacting people with some specific interests. On the basis of such consumer profiles, marketing and service companies can offer their commodities and services to those people whose profiles show that they could be interested in their offers.

Political profiles have also been produced for individuals and communities, and sold to electoral candidates who use them in their electoral campaign. For example, Castells reports that on occasion of the 2000 elections in the USA, political profiles were created for 150 millions USA citizens, and sold to the campaign offices of the candidates (cf. Castells 2001, p. 176). On the basis of such profiles, candidates can tell each community precisely what that community wants to hear, with an aim to win the support of its members. Such practice compels candidates to advocate opposite positions on different occasions, but in the

present age of noisy disinfotainment, nobody notices such inconsistencies. And even if rare individuals do notice them, this does not have much effect.

The Internet has opened new opportunities for data gathering. There are companies which copy and elaborate every message posted on the Usenet newsgroups; such messages normally contain some personal data, email addresses, and a content relevant for the profiles of their authors (written by themselves). The Usenet newsgroups are suitable for profiling as well as for targeting customers, since each of the newsgroups normally deals with a specific issue which shows a specific interest of the members of a specific newsgroup. Offers related to that subject of interest can be posted to the newsgroup, or sent as individual messages to the members of the newsgroup. Web sites also collect data about those who visit them, implicitly (by software means), and often also explicitly, especially from the less skilled or less cautious users. This data can also be used for various purposes, not all of which are innocuous.

In sum, various forms of data gathering allow creating various kinds of profiles of the individuals and communities, which can then be used for various purposes. The basic problem related to massive data gathering and observation of the people is that the results of these activities can be used not only for commercial, security and political purposes (which are considered acceptable), but also for abusing and harming people in various ways. A larger problem is that also the accepted and legal practice of observation of the people, data gathering, and targeting of the people with specific messages, can have bad psychological effects and lead to a totalitarian society if practiced in excessive forms and extensions. More about these perils will be said later.

3. Following and recording

It has been said that virtually all the Internet communication has been recorded for security reasons. These records can be stored for years, searched and processed in many ways and for various purposes. For example, it is possible to gather together all the activities of a specific person or all the communication in which some specific words appear. Data can be searched and elaborated in many ways. The huge quantity of data may pose a problem, but with the present data storing devices of incredibly large capacities and with processors of incredible speeds, this is probably not a big problem. A bigger problem may be the understanding of the recorded contents. Very many languages are used in communication, messages can be encrypted in various ways, and they can be hidden (encoded) in digital records of pictures and sounds. There is no need to deal with these problems here; I wanted only to point out how pervasive the surveillance has become and how incredibly large amount of data have been constantly recorded and stored. I cannot tell how useful this endless mass of data actually is from the security point of view; professionals in the field of security could tell us more about this, but they will probably not do it, for security reasons, of course.

Regardless of the real use and effects of the massive recording of the Internet activities, I am impressed with two basic things in this regard. Firstly, with the incredibly large amount of data that have been stored with this kind of surveillance of the Internet activities. Secondly, with the fact that my innocuous email messages are stored and kept in some obscure place, possibly for many years. This latter fact has spoiled for me the pleasure of writing emails. The fact that my emails are recorded by somebody (just in case) and that they can be retrieved and processed in a way that uses their content out of the context in which they were written, has changed the way I write emails. The awareness that whatever personal thing or a stupidity I wrote to a friend in some moment, could later be used by a third side, whoever it be, out of the original context and possibly with an aim to harm me, have

spoiled for me the satisfaction of writing in an open, vigorous, and sincere way; and I do not feel a satisfaction in writing private messages in a diplomatic way.

When they are turned on, mobile telephones are connected to an antenna (access point), normally the closest one which they can hear the best. When a mobile telephone moves away from the antenna to which it is connected, and approaches another one from which it can hear stronger signal than from the one to which it is connected, the mobile telephone switches from the previous antenna to the new one. It has been said that mobile telephone companies permanently keep records for all antennas about all connections of mobile telephones to them and about their leaving the antennas; in this way mobile telephone companies create (and possess) the evidence about the movements of all mobile telephones, and with this also of their owners. Such data are made available to the police and to various security agencies when they ask them, but they can be used also for other purposes. In any event, the very existence of a database which contains data about the movement of almost all the citizens (or of their mobile telephones) during the last few years, is amazing. It has been said that people could regard *invasive* such a systematic gathering and storing of data about their movement (cf. May 2002, p. 110). They could, indeed; but this is only one of the forms of invasiveness which people will be compelled to get used to; other forms could be much more invasive. One could turn the mobile telephone off sometimes and in this way escape the monitoring; but this would make him suspicious. The fact that a mobile telephone was not connected to any antenna for a certain period of time, would raise the question why was the telephone turned off, and where had its owner been during that time; why was he hiding, and so on. When the Big Eye watches you, an attempt to hide even for a moment makes you suspicious!

Regarding the issue of recording the *contents* of telephone conversations, the situation is rather secretive and less clear. However, there are indications that telephone conversations are massively recorded. For example, on 11 May 2006, the BBC television reported that telephone calls of "tens of millions of ordinary citizens" in the USA were recorded for security purposes. It was also said that the National Security Agency "asked" telephone companies to record *every* telephone call made in the USA. Since some senators expressed concern about such practice, the President of the USA addressed the nation by a statement in which he said that the recording of telephone conversations does not mean invading privacy, and that "the privacy of ordinary Americans is fiercely protected" in all the activities related to data gathering and surveillance. He should know the best.

Will such a pervasive observation and data gathering turn out to be more beneficent than detrimental for the common citizens, only time will tell. Or perhaps it will not, because people get used to everything; new generations are replacing the old ones, so that the old times are gradually being forgotten, and with time everything new becomes normal.

4. A global Panopticon

Jeremy Bentham proposed a design of a building called Panopticon in which all the inmates can be observed all the time by a supervisor whom they cannot see. This structure consisted of the central tower and of many cells situated around it; the doors of the cells were such that a supervisor could see inside every cell from the tower; on the other hand, the windows of the tower were such that the inmates could not see the supervisor in the tower from their cells, so that they could not know if and when the supervisor was watching them. The impossibility of the supervised to see their supervisors is especially important, because this creates a sense of powerlessness in the supervised and gives an additional power to the supervisor. The basic aim of the specific design of the Panopticon was to "induce" in the

inmates the awareness of the "permanent visibility that assures the automatic functioning of power". In other words, the system of surveillance was designed and organized in the way that "the surveillance is permanent in its effects, even if it is discontinuous in action". The invisibility of the supervisors makes the Panopticon "a machine for creating and sustaining a power relation independent of the person who exercises it" (cf. Rheingold 2002, p. 189)

Bentham considered his Panopticon an appropriate architectural structure for prisons, asylums, schools, hospitals and factories. In the present age, the entire world has been transformed into a global Panopticon. It remains to be seen if this global Panopticon will turn out to be a perfect prison, a global insane asylum, a much needed compulsory school, a hospital for incurable diseases, or a total factory from which there is no escape. In any event, a system of total and invisible surveillance empowers the supervisors and intimidates the supervised. Even if people get used to the unpleasant feeling which surveillance creates, the "power relation" will remain and it could get increasingly problematic. Because power tends to corrupt, and absolute power tends to corrupt absolutely.

Information technology offers countless possibilities of surveillance. For example, according to a BBC television report (2001), in some cities, cameras have been installed into driver's cabs of the trucks that clean the streets and collect garbage. These cameras record the streets through which the trucks are moving, and send records directly to a central office. In this way, drivers are kept under a constant surveillance so that they cannot park their vehicles and go for a drink, or they cannot do it too often. Another way of observing people in their work environment is to require of them to carry devices which register their movement; such devices can register their passage through certain points (doors). Similar systems have been used in some hospitals with an aim to control the movements and the activities of the staff. However, it is possible to implement such a system also in a wider space, and to use it for the constant observation of all those who are considered suspicious by the holders of political and spiritual power in a society. For example, to observe those who warn of the oppressive power of information technology and who speak about the perils of the increasing observation and surveillance of the people.

A person who lives in a city, passes in front of a few hundreds cameras every day. These cameras record people and events and often also send records directly to various monitoring centres. There are systems that record faces of people who pass in front of them and check for every face if it is contained in the database of wanted persons. Such systems were allegedly installed long ago at the entrances of stadiums and probably also in other places (cf. Rheingold 2002, p. 185). The use of such systems can be considered a necessary form of protection of the citizens and of the self-protection of a society. However, such kind of surveillance is risky and it will probably lead to mistakes which will create troubles to innocent people. Computer processing of images can lead to mistakes. I do currently not follow the activities in this field, but I know that a few years ago software systems for image recognition were not very successful. A change of the position of head or of the expression of face were able to confuse such a system. Things may have improved in recent years but I am not sure they have, because many methods were tried long ago, with a rather modest success.

In any event, cameras are around us and satellites are above us, and their eyes and ears are getting increasingly sharp. I do not have anything to hide, but I hate the fact that I *can* be watched by an Invisible and Unknown Somebody virtually at every step. I feel uneasy when I think that I am constantly watched, listened and fingered by invisible eyes, ears and fingers in front of which everybody is suspicious, possibly a criminal or a terrorist, and which observe and process him or her as such. Indeed, a prospective of the Surveillance Society seems almost equally frightening as the evils from which the system of total surveillance is supposed to protect us.

It is right to be known who is doing what, and to award or punish each individual according to his or her merits. However, if people are unreliable creatures, the same holds for the supervisors, whom a system of surveillance could give excessive power upon those whom they supervise. They could abuse this power. Gods used to be the only ones who had the ability and right to keep under surveillance everybody and everything. Those among the people who gain this capacity could start to consider themselves gods and to behave like this.

5. Privacy and business

One of the important issues related to data gathering and observation regards the question of privacy. There are claims that in the Information Age privacy has been lost and that there is nothing to be talked about in this regard. On the other hand, there are claims that privacy belongs among the basic human rights, and that society must protect this basic right of its citizens (cf. Radovan 2000; 2001; 2003). Some constructive proposals regarding this issue have been put forward long ago, but it is not sure if they can ever be successfully implemented. These proposals are based on some basic principles like the following ones. (1) Activities related to data gathering must not be secret. (2) A person must have a possibility to know what data are gathered and kept about her, and for what purposes are they used. (3) Data obtained for one purpose must not be used for other purposes without the consent of the persons they regard. (4) A person must have a possibility to correct erroneous data records about her. (5) Subjects dealing with gathering, processing and using data must prevent the misuse of these data (cf. Shenk 1997, p. 209; Rheingold 2000, pp. 314-315).

These principles are general but they could serve as a basis for the development of a legislative regulation which would protect citizens from various kinds of abuses to which data gathering can lead. However, in the present techno-economic society - called also the *business civilization* - business interests have priority and for the sake of them everything else is easily sacrificed. This makes virtually impossible to implement an efficient legislative regulation which protects the privacy and other rights of the citizens related to gathering and use of data, since such protection could obstruct some business activities. The other supreme priority regards national security; this is an argument which a state administration can use whenever it wants, and which easily prevails over everything else. There are also technical and organizational problems which make difficult the implementation of an efficient system of legislative control of the activities related to data gathering and the use of these data. The activities related to data gathering are dispersed and difficult to control; the ways that the gathered data are processed and used is even more difficult to control. Companies involved in data gathering and their use, are smart enough to formally satisfy some specific legal request in some tricky ways which do not limit their activities. A basic trick consists in offering to an individual a possibility to *forbid* some things related to gathering and using data about him or her; however, people do normally not notice such possibilities (options), and their omission to forbid something, is then interpreted as their consent that this can be done. Finally, people have learned that it is hopeless to resist business interests and administrative power, so that they simply accept whatever these two supreme gods bestow upon them. This is nothing new in the history of the relationships between the mighty and the weak. What is peculiar to contemporary age is that the weak are being told that with the development of technology they are getting stronger, while in reality they might be getting weaker, possibly much weaker.

There are claims that the complaints about the loss of privacy are exaggerated and not justified, because people have actually never had much privacy. Life in a traditional family and community did not offer virtually any privacy. All regimes and rulers throughout history

supervised people and usually destroyed those whom they did not like. In other words, there is no sense to complain that people have lost something they have hardly ever had. Such claims are largely correct; however, the issue of the present data gathering and surveillance nevertheless do deserve a special attention for a few reasons. First of all, it is bad to justify some dubious present practice by the fact that in the past ages the situation was not better. Secondly, data gathering has become a business activity which uses people and their privacy as a raw material; this is a relevant novelty in comparison with the past ages. Thirdly, contemporary information technology has such operative capacities that uncontrolled practicing of data gathering and surveillance could turn the world into such a madhouse that is difficult to imagine.

A society could not function successfully without gathering certain data about its members and without a certain forms of surveillance. However, social institutions should do their best to keep these activities under a strict control and inside some limits. It may be that the intense spread and use of information technology has actually not brought about a really new age; however, an intense data gathering, profiling of the people and aggressive targeting them for various purposes, together with an ubiquitous surveillance, could do it. This would probably be an age of fear and persecution, corruption and stupidity.

In the business civilization, data gathering and surveillance serve the aims of those who have the power, so that the attempts to limit this practice could hardly achieve much. Struggles against the interests of the holders of power are seldom won, but they keep the awareness of an issue and of its relevance. Also lost battles are sometimes worth fighting. In any event, the right to privacy should be considered one of the basic human rights, not only because privacy is a value by itself, but also because the lack of it is the first step to other forms of devaluation, abuse and oppression.

6. Processing the people

Technology by itself does not determine the way of man and history; it creates possibilities of the realisation of various individual and collective inclinations, but it does not determine which of the possibilities will be chosen by an individual, a community or the humankind. People are the ones that chose and decide. Data gathering and aggressive targeting of the people with specific messages, as well as massive surveillance of the people, do not mean that *technology* has run out of control, as it has often been said. It rather shows that *corporate business* has run out of social control, and that the *state administration* normally tends to do the same. These two dominant social forces normally struggle with each other for prevalence, but they also need and support each other. Both of them aim to keep people under control and to shape them in accordance with the needs and aims of these forces. The increase of technological power strengthens such tendencies as well as the possibilities of their realization. Although technology does not determine the aims and tendencies of corporate business and state administration, it offers them increasingly efficient means by which they mould people and their reality according to the aims of these two supreme forces. In the capitalist society, business shapes public discourse and dominates politics; this then means that the growing power of technology gives an increasing power to the present ruthless capitalism to shape the world on its own image. This image may not be nice; it may be frightening and repulsive.

Data gathering, observation and targeting of the people should be practiced in reasonable ways and to a reasonable extent. Excessive practicing of these activities should be considered disturbing and harmful. Except for some peculiar people, it is unpleasant to feel constantly observed, and even more unpleasant to be constantly targeted. The awareness that

people are (or may be) constantly observed, may radically change the feeling and behaviour of the people. The awareness that every my activity creates data which somebody may be recording and processing, and which will then be used for *targeting* me for whatever purposes, makes me feel like a rat moving along a maze of a proverbial mad scientist. An excessive scrutinizing of the people and of their behaviour, for whatever purposes, is actually insane and unpleasant. A constant exposure to data gathering, surveillance and targeting is not only irritating and exhaustive, but is also humiliating and dehumanising. Data gathering and profiling turns a person into an object of observation and processing the aim of which is to compel her to buy some commodities or services. The process of data gathering, of profiling the people and of targeting them with specific messages, reduces people to raw material which is elaborated, shaped and used for business purposes. The very idea of making consumer profiles is repulsive to me. I do not want to be watched by tradesmen and mad scientists who study me with an aim to compel me to "consume" something or to think and behave in a certain way. I do not want anybody to gather data about me, to profile me, and especially not to target me. I know what I need and what I want, and what I can afford, and I do not want to be imposed anything by anybody.

Regarding the targeting of the individuals, practiced by marketing and service companies, but also by many others, various proposals have been put forward with an aim to keep this intrusive practice inside certain limits. Firstly, all kinds of automated massive sending of messages to targeted consumers (based on addresses obtained by data gathering) should be forbidden. Secondly, the state administration should establish a registry of addresses and numbers of the people who do *not* want to be targeted by anybody and for whatever reason. Such a registry should be mandatory and all marketing and advertising subjects should be legally obliged to respect it (cf. Shenk 1997, p. 207). I support such proposals the aim of which is to provide citizens a protection from the aggressive targeted advertising and manipulation; but it does not seem that such proposals have much chance to be successfully implemented. Intense targeted advertising makes people confused and neurotic. However, this practice could hardly be stopped, because in the techno-economic world, everything that is technically feasible and that may favour business, has the absolute right to exist. People have been made *tool-serving consumers*, and they have been treated as such.

In the disputes about privacy and business interests, there is not much discourse about the *mental profile of the society* which is so obsessed by data gathering and by targeting of the people reduced to consumers. I hold that the situation in this regard is getting repulsive and insane. I do not care much about my privacy; but I am frustrated with the fact that I am compelled to live in a world in which people are constantly observed like rats in an experimental maze, and targeted by various advertisers and tradesmen like hares chased by a pack of wild dogs. *Not individual privacy but collective madness is the basic issue regarding the excessive data gathering, observation and targeting of the people.*

7. Risks and threats

Complex systems are normally not perfect; they contain some errors in design and production; elements of such systems sometimes fail, and those who work with these systems make mistakes. Errors, failures and mistakes related to a system of data gathering and surveillance can have tragic consequences for innocent people, and they can cause harm to a community. There are disturbing reports in this regard, although the holders of power have good reasons to cover up the existence of such problems as much as they can. Since I am not involved in criminal activities, I hope that the systems of data gathering and surveillance have

been designed well, produced well, and used well. Generally speaking, technological systems are getting better and more reliable, and they are also operated rather well, so that we have good reasons to hope that technical difficulties will not be happening often and that they will not have too bad consequences.

Regarding possible abuses of the of data gathering and surveillance, the situation is quite different. Data gathered for whatever purposes can be abused, and with the increase of intensity of data gathering and surveillance, increases also the plausibility that the results of these activities will be abused. Data can be abused by those who collect them legally, as well as by those who come in their possession in an illegal way. Data may be abused with an aim to gain some profit for their possessor, to harm somebody, and for subversive activities against a society. Many problems do not have a perfect solutions; but they can be solved in very bad ways. One such problem related to data gathering and surveillance regards the issue of who is to *supervise the supervisors*, and how. The other regards the question of who can *protect the data* gathered in various processes of data gathering and surveillance, and how. None of the two problems have a perfect solution, but they can both be solved very badly. Those who are in position to supervise other people, have a power over those whom they supervise. This power grows with the levels of hierarchy of the system. At each of the levels people can abuse in various ways the power that the system gives them. A perfect system of extensive data gathering and surveillance may lead to a perfectly totalitarian society. An imperfect such system may lead to a highly corrupted society in which everybody abuses others in accordance with his or her power.

Extensive data gathering and surveillance may not bring much good, and they always bring various risks. The assumption that more intense data gathering and surveillance bring more useful knowledge and better security, is dubious. First of all, the gathered data may not be processed and used in optimal ways. Secondly, these data can come into the hands of those who will use them for illegal or subversive purposes. In sum, if business forces and social institutions overstep a certain measure in data gathering and surveillance, this will create many difficulties to the citizens and it will gradually lead to a totalitarian society. It is difficult to say what exactly should be considered the right measure in the space of data gathering and surveillance; in any event, in this space of activities, more does not mean better.

The advance of science and technology have always served holders of power rather than common people. Various *scientific societies* which started to emerge in the seventeenth century, treated ordinary people in ways that were profitable for the elites, and deflected them from the political and religious ideas which could have called into question the existing authorities and structures of power. For example, the immutability of natural laws that physicists started to discover at that time, was used as the basis for the claims that the social narrative (of that time) and the existing structure of social power, were also immutable and that they could not be changed (cf. Noble 1997, pp. 203-204). During the twentieth century, as well as today, scientists have served existing powers even more directly than their predecessors were doing it. The development of information technology has been closely related to military and governmental purposes. These technologies are now used for many purposes, but they have also created vast possibilities of surveillance, manipulation and control of the people.

Figuratively speaking, information technology facilitates shaping and control of the people at the *software level*. On the other hand, biotechnology facilitate shaping and control of the living beings, including people, at the *hardware level*. This can have much more radical consequences than the software shaping has. "Genetic engineers, supported by the state, have laid the technological foundations for an Orwellian future", concludes Noble (p. 206). It remains to be seen to what extent will the present holders of social power use the means that science and technology has bestowed upon them, for the development of a truly totalitarian

(Orwellian) society. If there will still be anybody able to see anything. In any event, for a totalitarian society, one does not need the monsters of the past, such as Fascism, Nazism or Stalinism; a complete dominance of the ruthless capitalism is enough to transform a formally democratic and free society into a factually totalitarian society. Totalitarian should be considered every society in which a narrative and practice have a status of absolute truth, a criticism of which is condemned and punished, formally or informally the same. In the ruthless capitalism, corporate interests and profit are treated as absolute values; whatever promotes them is accepted and practiced, regardless of the harm it brings to the people and to the nature; whatever obstructs the pursuing of these supreme aims of capitalism, is overridden by it. Corporate business controls the space of public discourse and moulds the mind of people by its disinfotainment industry. It gathers data about everything and targets people in intrusive ways with the aim to compel them to behave in the way it wants them to behave. All these elements together create a totalitarian social environment.

Finally, there have always been people who adored power and supported rigid ideologies as well as a totalitarian social environment. A totalitarian system is an ideal social environment for sadists: by serving the power in such a system, they gain the possibility to practice their sadism without any risk (cf. Fromm 1992). A society that practices intense data gathering, surveillance and targeting of the people, has good chances to become a truly totalitarian society, and then also a sadistic society. It used to be considered entertaining to watch people being torn apart by wild animals as well as being tortured and killed. We may not want to admit it, but such kinds of entertainment are still appealing to many among us. It has been noticed that many people enjoyed watching scenes of military attacks of a technologically far superior military power against a technologically inferior one. How many of these people who enjoyed watching such scenes, tried to imagine the horrors of those small people who were hit by these attacks? Not many, I am afraid. Technological advance may be changing the forms of our barbarism, but the essence seems to remain the same. A brief view on television screens that surround us indicates that contemporary audience is not less interested in the spectacles of violence and destruction than the audience in the Roman amphitheatres had been. Indeed, the monster of destructiveness is always close to us and it may be hidden in us. Hence, the increase of technological power and efficiency always carries a risk of creating such technological and social conditions which could lead to the submission of the entire humankind to the worst inclinations of the worst among its members.

8. Concluding remarks

Intrusive observation and aggressive targeting of the people, for business purposes and security reasons as well as for other purposes create a totalitarian living space. Totalitarian societies used to be imposed by states and religious institutions, and they were based on political ideologies and religious dogmas. The danger of such kind of totalitarianisms always exist, and it will exist as long as there are states and religions. In the present age, the capitalist narrative has imposed a new global techno-economic ideology which is very intrusive and aggressive towards people and nature. Relying on its technological power, the ruthless capitalism has been creating a new business civilization which nominally promotes freedom, but which could turn out even more totalitarian than the old ideologies, dogmas and regimes have been. The powerful trinity Technology, Business and Security has sized the world; this trinity can bring to people a lot of good, but also a lot of evil. This trinity tends to create a new kind of society, the Surveillance Society, in which extensive data gathering, intrusive observation and surveillance, and aggressive targeting of the people by specific messages, have an essential role and pervade the entire space of human activities and life.

This will be an unhappy society of confused and neurotic people, and it will be totalitarian almost by definition.

What can the common people do to prevent the creation of such a surveillance society towards which the present techno-economic paradigm, the business civilization and its disinfotainment have been heading? Not much, I am afraid. We can only hope that the movement towards the totalitarian society will not succeed, and that data gathering, observation and targeting will not manage to transform people and their living space into rats in a maze of a mad scientist. We can base this hope on three elements; the first of them is weak, the second is stronger and defiant, and the third is slightly cynical and its power is hard to estimate. Firstly, our hope relies on the common sense of the holders of power; we hope that they will not allow the totalitarian tendencies of the techno-economic society to go too far. This is the weak element because modesty and power rarely go long way together; the totalitarian tendencies of the present techno-economic system can also run out of control of the holders of power. A stronger reason for hope comes from the present techno-economic system itself. This system produces everything that can be sold, so that there is a hope that it will produce also some means which protect people of its totalitarian behaviour. This sounds like a vicious circle, and it may also seem ridiculous, but this should not discourage us. The idea of large anti-virus systems, firewalls, and similar miracles could have also sounded ridiculously a few decades ago, and yet it has become an essential element of our reality, and a huge business, of course. It may be insane to produce various technological systems and at the same time also the means that obstruct their activities, but that is what people have normally been doing. Finally, a cynic or an optimist, let us say, could argue that the techno-economic world is getting too complex to be kept under an efficient control. A thorough system of data gathering and surveillance will produce an incredibly large quantity of all sorts of data by which it will congest itself so that it will not work well. This may be a sane approach to the problem in a situation when nothing better can be done.

Despite our three reasons for hope that the things will not get too bad, the totalitarian tendencies of the present techno-economic world remain a real threat with which people will have to live and cope as they can. Data gathering, observation, surveillance and targeting of the people do not regard only the issue of privacy. The problem is much wider and more essential: *people are observed and targeted with an aim to be mastered*. This is a much more important fact than the loss of privacy. Information technology allows employers a thorough surveillance of the activities and movement of employees; it allows government administration to monitor citizens at every step; and it allows business forces to shape the living space as well as the mind and behaviour of the people in ways that serves their aims. Information technology has created the means by which a truly totalitarian society can be created for the first time in history. A new tyranny may not come, but it may also be approaching and rather close.

Information technology is an extremely efficient means which has brought to people wondrous powers in the space of communication, knowledge, and control. It has brought new opportunities and freedoms to billions of people. However, this same technology can be used by the holders of economic, political and spiritual power in ways that steadily increase their power over the common people, and lead towards a totalitarian and oppressive society, or to a new mental and physical slavery. The feeling that one has been constantly watched by invisible eyes, listened by invisible ears, and fingered by invisible fingers, is unpleasant. Being constantly targeted and manipulated makes this situation even worse. A society must practice data gathering to learn those basic facts which are necessary for its optimal functioning; it must practice observation and surveillance to be able to prevent irresponsible and criminal behaviour and subversive activities; it must also target people with various messages to achieve some positive aims. However, no data gathering, surveillance and

targeting can make people and world better without a constructive and benevolent behaviour of the people themselves. Hence, humankind must reshape its narratives, its socio-economic systems and its behaviour at all levels in the ways that protect human dignity and promote a global solidarity. Because without this, no advance of technology, data gathering and surveillance can make the life of people more safe and more pleasant.

REFERENCES

- Ball, Christine (2002) "Elements of surveillance: a new framework and future directions", *Information, Communication & Society*, Vol. 5 (4): 573-590.
- Barney, D. Darin (2000) *Prometheus Wired: The Hope for Democracy in the Age of Network Technology*, Chicago: University of Chicago Press.
- Castells, Manuel (2001) *The Internet Galaxy: Reflections on the Internet, Business, and Society*, Oxford: Oxford University Press.
- Fromm, Erich (1992) *The Anatomy of Human Destructiveness*, New York: Henry Holt and Co.
- Koops, Bert-Jaap (2003) "The shifting 'ballance' between criminal investigation and privacy", *Information, Communication & Society*, 6 (3): 380-403.
- May, Christopher (2002) *The Information Society: A Sceptical View*, Cambridge: Polity Press.
- Noble, David (1997) *The Religion of Technology*, New York: Penguin Books Ltd.
- Ploeg, Irma, van der (2003) "Biometrics and privacy", *Information, Communication & Society*, 6 (1): 85-104.
- Radovan, Mario (2000) "Twelve Theses on the Information Age", *Informatica*, Vol. 24 (2000) pp. 445-448.
- Radovan, Mario (2001) "Information Technology and the Character of Contemporary Life", *Information, Communication & Society*, 4 (2): 230-246.
- Radovan, Mario (2003) "Waiting for Hermes", *Synthesis Philosophica*, Vol. 18 (2003), No. 1-2, pp. 393-408.
- Regan, M. Priscilla (2002) "Privacy as a common good in the digital world", *Information, Communication & Society*, Vol. 5 (3): 382-405.
- Rheingold, Howard (2000) *The Virtual Community (revised edition)*, Cambridge, MA: The MIT Press
- Rheingold, Howard (2002) *Smart Mobs; The Next Social Revolution*, Cambridge, MA: Perseus Publishing.
- Shenk, David (1997) *Data Smog: Surviving the Information Glut*, New York: HarperCollins Publishers, Inc.
- Viseu, Ana; Clement, Andrew; Aspinall, Jane (2004) "Situating privacy online", *Information, Communication & Society*, 7 (1): 92-114.

PREMA DRUŠTVU NADZIRANJA

SAŽETAK

Članak se bavi pitanjima prikupljanja podataka, nadziranja i intenzivne upotrebe ciljanih poruka u suvremenom životnom prostoru koji je oblikovan tehnologijom i kapitalističkim svjetonazorom. Oni koji posjeduju relevantna znanja o drugima, posjeduju moć nad njima, i oni mogu tu moć rabiti i zlorabiti na razne načine. Intenzivno prikupljanje podataka, promatranje i nadziranje olakšavaju manipuliranje ljudima i omogućavaju stvarnim nosiocima moći da oblikuju društvenu stvarnost na načine koji služe njihovim interesima, ali koji mogu lako voditi prema totalitarnom društvu. Totalitarne sustave su obično nametale države ili vjerske organizacije, i oni su se zasnivali na političkim ideologijama ili religijskim dogmama. Rabeći moć tehnologije, suvremeni kapitalizam stvara jednu novu poslovnu civilizaciju koja nominalno promiče otvorenost i slobodu, ali koja pokazuje jasne totalitarne tendencije. Članak iznosi niz kritičkih promišljanja vezanih uz ta pitanja.

Ključne riječi: prikupljanje podataka, potrošački profili, promatranje, privatnost, nadziranje, ciljanje, poslovna civilizacija, totalitarno društvo