351.74:004-049.7 Original scientific article

CHALLENGES OF USING INFORMATION TECHNOLOGIES IN POLICING

Bogdancho Gogov, PhD
Faculty of Security-Skopje,
Email: bgogov@t.mk

Abstract:

Crime is perceived as symbolic as well as a real threat to human security. Hence a growing number of different institutions take part in crime control. At the same time, due to greater security needs, public and private organizations increasingly cooperate in building a multi-agency partnership. It creates a situation in which by implementing the partnership projects for crime control and public order, they put individuals in position of being subjected to control, but at the same time to participate in the implementation of the control of others and of themselves.

Relatively new technical means such as digital video cameras and audio systems, an analysis of genetic material are introduced in the police and policing for the purpose of better control of the various forms of criminal behavior. It is interesting that these new forms of criminal control do not replace the old ones, but only complement them. Continuous and comprehensive control is established as an explicit function in many areas of social life, and it is explained as a result of the situation with crime and the associated phenomenon of fear of crime.

The opportunities that are offered by information technology to monitor various segments of private and public life sharpen the relationship between the need of security and privacy protection. Obviously, the monitoring and surveillance will increase in use along the future development of science and technology, and will develop from routine in regular investigative measure in the criminal and legal events.

In this paper we consider the possibilities of new technologies and their use in policing, as well as the dangers of violation of human rights and freedoms, and especially the right to privacy.

Key words: Information technology, policing, ambient intelligence and privacy.

Introduction

Contemporary society develops in a complex manner, where the individual behavior becomes a subject of interest for many different forms of social control. We live in a historical period in which the control mechanisms are reshaping, and they involve several governmental, private and public-private agencies that apply numerous techniques and strategies which lead towards a more systematic and more intense control (Clegg and Courpasson, 2006). The sense of an increased control and its expansion can be attributed to the fact that certain technologies have become more sophisticated, providing facilitated insight in what we consider to be a private sphere. The contemporary technological development assists and continues the long-lasting trend of practicing social control where the differences in the techniques and methods create new possibilities. This development carries the risk every our activity to be controlled. As a matter of fact, the possibilities offered by the modern information and communication technology are great and their implementation is limited only by the financial recourses that are at disposal of the control agencies.

Some basic social structures, institutional and organizational establishments are subject of in-depth revision regarding the manner in which we understand both, who we are and the world around us. In this context, first of all we think about the transformation of the capitalist paradigm, about the changes in the role of the state and its institutions, about the speed and development of the network forms of social organization, about the expandable and fluid sense of the identity and, at last, about the changes in daily exchange and interpretation of information through the media for interpersonal and mass communication.

The traditional stratification system has broken down and the traditional moral (norms) are less compulsory than they used to be. People become more mobile, which have increased the feeling of mutual connection, but, at the same time lots of people feel unprotected and look for a sense of security (Giddens, 1991). Giddens calls this a diffused insecurity and it constrains significant changes in the logic and practice of social control.

Contemporary crime and changes in policing

The presence of fear and insecurity is the primary incentive for articulation of the demands for a better and greater control. The numerous forms of risk allow a specific way of considering the potential problems, for which, state control is required. It is revealed that the risk is a very important element of the social control transformation (Stern and Fienberg, 1996).

Because the crime is perceived as a symbolic, as well as a real threat for the human security, the number of different institutions which take part in crime control has increased. For example, the changes in architecture and the new designs have accepted the idea of natural monitoring in order to detect crime. Social welfare institutions nowadays have more legal authority to reveal false requests for social protection, and their function is more focused on detecting false requests than on real protection (Cohen, 1985). Public and private organizations are mutually connecting in order to establish multi-organizational partnership that often goes beyond the already established mutual scopes and legal activities. Introducing a model of policing, in which, the police and other public and private institutions would participate (such as banks, hospitals, trade associations, etc.) creates a situation in which by conducting partner projects for crime control, put the people in situation of both, to be subject of control and to control the others. Video cameras, audio systems, genetic material analysis were introduced to provide a better control of the different types of deviant behavior. It is typical that the new forms of control do not substitute the previous ones, they only supplement and amplify them. The control is established as an explicit function in many areas of society, with an explanation that it is a result of the dark figure of crime, as well as with the fear of crime, as a consequence. .

When the crime rates increase, the government usually takes intensive repressive measures, which, if they are not conducted in accordance with the law, become a serious threat for the human rights and freedoms. Threats, mostly private threats are proportional to the seriousness of the crime because in such cases the police dispose of intrusive measures and techniques. Governmental activities that are undertaken for protection of the inherent right to life, property and other aspects must be restricted and to respect other rights and freedoms. The application of military rhetoric as a tool for fighting against terrorism, against organized crime, corruption and similar activities do not deter criminals or terrorists from their intentions, but it can increase the fear among citizens. One of the most common paradoxes nowadays is the constant disrespect of the human rights (for example, the right to clean water and sanitation, health care, elementary existence) and at the same time, as never before, the existence of international and national legal documents, strategies and debates about the human rights and freedoms. Numerous wars have been waged and are still going on in 'defense' of the human rights (in Iraq, Afghanistan, Syria, Mali, the Balkans...), peace corps (aside from the military corps) are engaged in order to help the establishment of democratic societies, while the United Nations as a body for resolution of conflicts and problems is avoided. We can get an impression that the Clausewitz's belief, according to which, war is continuation of politics by other means is abandon, and that Foucault is right by saying that 'War is

probably the continuation of politics". However, we should not forget that 'politics' is perceived as continuation, if not directly to the war, then to the military model as the most common method to prevent civil rebellions (Foucault, 2004).

New technologies and their influence on policing

As a result of the almost limitless possibilities of the information technologies, especially delicate is their application in observing different aspects of the private and public life as well. Video camera surveillance is more frequently being used in public areas. It has become impossible for people in the cities across the Western world to move without being monitored every step they make. It can be expected that this type of surveillance and monitoring would develop with the expansion of technology, surveillance centralization and with the widespread but unproven belief that surveillance (with video cameras) leads to a greater security. The closed-circuit television (CCTV) or video surveillance market constantly develop, furthermore, it easily integrates with other technologies such as the internet, the face recognition software, the fingerprint databases and other bases which are at disposal of the police and other public institutions. The video camera's abilities are essentially improved with the upgrade of the night vision equipment, the motion sensor etc. Other similar technologies that can easily track the location and motion of the people (Global Positioning System-GPS), access control systems, record of presence, mass motion software and systems are also being developed.

All these and other similar technologies make possible for the police to have a documentation of the everyday behavior and normal activities of the people. The police stores the data in big 'depositories' called data warehouse, and its value i.e. helpfulness is evaluated when needed. These technologies can help in analyzing the past behavior of the individual and to determine their habits and choices in the everyday life. The above mentioned, as well as many other methods and techniques (such as the profiling) are very useful for analyzing different manifestations. But their excessive and illegal use, mostly in the police work causes a well-founded concern regarding possible malpractice in the surveillance process of the majority of citizens and disruption invasion of the privacy caused by the presumption that every individual can be suspect until the opposite is not proven.

The police in their duties rely more and more on the information technologies neglecting the contact with the citizens, its presence in public spaces, preventive activities in different institutions such as schools, local administration, and citizens associations. The possible benefits of using video surveillance and global positioning system (GPS) in policing will not show better results if the police made distance from citizens and from their daily, sometimes even banal problems related to their safety.

Video surveillance, Global Positioning System (GPS) and Radio-frequency identification

Video surveillance conducted with the help of video cameras is more frequently used in public spaces. It has become almost impossible for people in all cities in the Western world to move without being located and kept under surveillance almost every step they make. It can be expected that this type of surveillance will increase, with the development of the technology, with the centralization of the surveillance, and with the common belief that surveillance (with video cameras) leads to a greater security. In some countries, video cameras are inseparable part of the urban life, similarly to the electrical grid and water supply network in the beginning of the previous century. The video surveillance market, or close-circuit television (CCTV) is constantly developing, and what is more important, it easily integrates with other technologies such as the internet, the face recognitions systems, the fingerprint identification database and other databases which are at the disposal of the police and other governmental institutions. The capacity of the surveillance cameras is significantly expanded with the upgrade of the night vision options, the devices for monitoring of the movement, and other technological gadgets.

The governments and the science are, for a longer period of time, trying to determine the real effect of the video surveillance in the public spaces upon crime reduction. Apart from the numerous research and studies on this topic, there are no results which would indisputably confirm the effect of prevention. In our country, in my opinion, no similar studies have been conducted, but there are numerous studies around the world, more or less relevant. We will mention some of them.

In 2001, the Interdepartmental Committee on Closed Circuit Television of New South Wales in Australia published a Final report about the evaluation of closed circuit television (CCTV) in public places. The committee concluded that certain reports and statistics (which are not completely accurate) show that video surveillance can be effective in certain situations and has a high level of support. However, the committee also noticed that their assessments can be considered as systematic evaluation of the technology.

The University of Ottawa, for the needs of the Canadian police, made an evaluation (Wade, 2003) which showed that 'the effects of the video surveillance upon the crime are inconsistent and can change, and to a great extent are unpredictable' and that the preventive dimension of the video surveillance can vary in different periods of time and among different types of criminal activities. It was determined that video surveillance systems have the smallest effect on crimes against public order. The magnitudes of the preventive effect of video surveillance on criminal activities depend on the location, and the car-parking places have most benefit from this system. The study also determined

that there was preventive effect even when the surveillance cameras were off. The best preventive effect was noticed in cases when video surveillance was combined with other methods of crime prevention even in cases when it was adjusted to the local conditions. After the implementation of the video surveillance system, no evidence was found about increased crime rates.

The Home Office of UK published a report about the crime prevention effects of closed- circuit television (Welsh and David, 2002). The report is an analysis of 22 studies which were done in Britain and USA and which were selected according to rigorous and strict methodological criteria. According to these studies, it can be concluded that the closed-circuit television, also known as video surveillance, reduces, to a small extent, criminal activities, and it is the most efficient in preventing motor vehicle theft from parking places. It was determined that the video surveillance has small or no effect in the public transport or in the city centers.

The results of these studies do not answer completely the questions about the level of influence which the video surveillance has on crime reduction. This is, mainly as a result of the influence of other criminogenic factors that are inconsistent and is difficult to separate them. However, the studies show that this method of crime control should be neither rejected nor given too much significance, but to be carefully analyzed and designed in accordance with every individual case and location.

The Global Positioning System (GPS) is a space-based radio navigation system, which, 24 hours of the day covers the space with satellites that circle around the earth and provide information about the geographic location of people and other objects. When these objects are owned by a certain individual, his or her locations can be easily discovered (most frequently, the GPS equipment determines the location of the individual in a range of 10 to 100 meters) and the direction of movement. For example, when the individual uses a mobile phone, from the moment he/she turns the phone on, bidirectional connection is established between the phone and the location of the mobile network operator, which provides constant observance of the phone's user.

Radio Frequency Identification (RFID) is a technolgy which which uses a detector of electromagnetic waves (antenna) on one side, and an object which radiate (respond) on the other side. The detector emitts radio waves to one or more sides or more frequencies, while the "tag" (transponder) or the sign of the item 'dismisses' by sending collected information. The RFID tags can be passive RFID (can be read-only) or active RFID (can be read-write), and it is not necessary to be 'visible' for the detector. Also, more than one can be read simoultaneously.

Nowadays, RFID are successfully used in admission control, information about presence, information about mass motion (motorways, ski centers), information about animals, and is widely applied in production processes and in the store activities. RFID devices can be easily integrated and even hidden in different items, mostly due to their miniature size. The miniaturization of electronic technologies is one of the prerequisites that provide the feasibility of the RFID devices. For example, in 2009, researchers from the University of Bristol successfully attached RFID micro-transponder to the live ants in order to analyze their behavior. This tendency towards even greater miniaturization of the RFID devices will most probably continue with the technological development. For example, in 2007 the company Hitachi designed the smallest RFID chip with dimensions 0.05 mm × 0.05 mm. Nowadays, the chips are dust-sized and therefore they are called dust chips. The RFID technology is also used in the production of biometric passports, in other words, tags (smartcards) are being embedded in the passports, in which, biometric data about the owner are inscribed and this data can be read by the electronic passport control even at a distance from 10 cm to a few meters away. Furthermore, all information about the time and location of the entrance and exit of the country by the individual are inscribed in the tag. The danger seams to appear when those who want to steal the data are able to do it from the same distance. As a result of this, different technologies for protection of the e-passports are part of the standards for designing biometric or e-passports, but, however, complete security of the e-passports is still not possible.

Due to the constant innovations and unlimited possibilities of the information technologies, especially delicate is their application and usage in the process of monitoring different aspects of the private, as well as the public life. Therefore, data collection via technical observation and other automatic devices shall be regulated by special legal provisions[2]. Such specific regulations for conducting video surveillance are included in the last part of the Law on Personal Data Protection, more precisely, in the articles 9-a, 9-b и 9-v. The Law on Police also contains provisions about video surveillance. According to article 65, from the Law on Police, under recording in public places can be understood permanent audio and video surveillance in public places where crimes and other offences occur more frequently, in order to prevent such activities.

Nevertheless, if we take into consideration the fact that the video bases of the cameras which are located in different institutions (companies, banks, governmental institutions, public spaces,) might be connected soon in our country, and that the police can use and compare these data, than the current legal provisions are not a sufficient protection. Therefore, there is a need to develop further procedures and mechanisms that will guarantee the protection of the personal data which can be revealed and used.

[2] Principle 2.3 ofrom the Recommendation (87)15

Moreover, in order to use the surveillance in accordance to the real needs without being unnecessarily intrusive and invasive, we should consult the studies and best practices which will scientifically determine the positive impact of the video surveillance upon crime prevention and community safety. This refers to the data collected from the GPS systems and RFID devices, as well.

Smart Environment and Internet of Things

In the past decade, the development of technologies, particularly their speed, power, networking capacity and physical minimization of machines, have aroused the interest of researchers and scientists for a new way of using profiling which, it is almost certain, will be all-encompassing in the future and will hardly have any visible consequences. This is Ambient Intelligence. Apart from science, the concept of smart environment was dealt with by the European Commission as well. It is upon its request that in 2001 the Information Society Technologies Advisory Group – ISTAG published a Report titled "Scenarios for Ambient Intelligence" where a team of scientists and experts elaborately examined this issue and prepared several scenarios or examples on its future operation. The 2001 ISTAG Report placed this future in 2010. From today's perspective we see that technologies are already here, are completely developed and accessible, and their all-encompassing application is on the verge of becoming a reality.

The concept of ambient intelligence creates a vision of an information society where the focus of interest is on the simple use of technologies, on more efficient supplementary services and support of human interaction. People are surrounded by an intelligent intuitive interface incorporated in all kinds of possible objects and environments which are capable of recognizing and responding to the presence of various individuals in a concealed, non-invasive and often invisible manner.

How exactly will these technologies influence police work in the near future is still unknown, but there's no doubt that they lend a possibility to observe all details of the personal life of an individual as well as psychological features which sometimes even the person in question is not aware of. They will be able to provide police intelligence databases with an enormous amount of data. There is no doubt that the police will take advantage of those possibilities. The question is: to which extent and in which limits? Protective mechanisms drawing necessary boundaries need to be incorporated into the respective technologies and that needs to be done even in the process of designing them. Dilemmas particularly arise in the direction of automatic decisions made without the human factor, which are a feature of the very operation of ambient intelligence. Responding to those challenges will take time, practice and interdisciplinary scientific and technical solutions.

Ambient intelligence is defined by its key elements: 1) integration, meaning networked machines are integrated in the environment; 2) awareness of context, because machines can recognize both us and the context of our current situation; 3) personalization, because they can be tailored according to our needs; adaptability, which means they can modify the environment as a response to our behavior; and 5) anticipation, because they need to anticipate our priorities without our deliberate request and influence (Hildebrandt, 2008).

Smart environment technologies available are sensor technologies, RFID systems used for radio-frequency identification, nanotechnologies and miniaturization. Together, they compose the "Internet of things" which is supposed to put the real world online. The internet of things consists of small devices tags) built into objects, people, animals being constantly monitored and exchanging data through the network connecting them (Aarts and Marzano, 2003).

All those technologies generate an enormous amount of data, however they will not reveal any knowledge until profiling techniques are applied on those data. Profiling technologies are the essential connection between the excessively trivial data of our movement, temperature, interaction with other people or things and the applicable knowledge of our habits, needs and the state of our environment (Gubbi,, Buyya, Marusic, and Palaniswami, 2013). Only after identification techniques are applied on models through mutually connected data bases, the things in our environment can become smart and start acting on our behalf as our agents in the multi-agent network. Thus, profiling creates an added value to the mass of data.

In our country, such technologies are still not available in practice, and in the rest of the world we can see them only in the richest countries and even there they still seem largely futuristic. In order to make the abstract terms of ambient intelligence clearer, we are going to explain them through an example. In the future, people are going to carry in them a small, inconspicuous communication device – part of a network which through profiling will know all of the habits and needs of its owner. When the device detects, according to the model of behavior and schedule of the owner, that he is at a meeting, it will lower the level of incoming phone calls and limit it only to the necessary ones. The device will further "negotiate" with the devices of people calling its owner in order to establish the level of emergency of the phone call. This "negotiation" is in fact profiling of the future needs of the owner in view of his device, based on databases on his behavior in the past and data of past behavior of other people trying to reach him for the purpose of evaluating the necessity or emergency of contact. In that manner, the device acts as a representative, an agent of its owner (Ja¨rventausta, Repo, Rautiainen, Partanen, (2010)

The vision of ambience intelligence depends on its imperceptible adaptation, modification of the environment of our conditioned habits and needs. The idea is not for us to give a deliberate, conscious signal, but for the environment monitoring our behavior to be able to "predict" what it needs to do and what the change is that it needs to make. It envisages a proactive instead an interactive use of computers, putting human intelligence as further possible. Supporters of the development and application of these technologies point out that we need to conform the environment according to our needs, "we cannot afford to wait for a human interpreter but need profiling machines that draw their own conclusions about what we prefer when and where, hoping we can thus solve the problem of endless choice and deliberation"(Hildebrandt 2008).

Conclusion

The information technologies are widely applied in policing. They, however, bring certain positive and negative aspects, mostly related to the privacy of citizens. The possible gains and advantages of the application of video surveillance and global positioning system (GPS) in policing will not show better results if the police keep away from the citizens and from their daily problems related to security. On the other hand, a constant reassessment and amendments of the legal framework regarding the application of information technologies is crucial in order to achieve balance between greater security and protection of human rights and freedoms.

Ambient intelligence is exceptionally complex, but its complexity is hidden, without monitors and keyboards which is why the environment itself becomes interface. Particularly significant is its ability to perform surveillance in real time. Due to the fact that the environment will always be one step ahead of us, the concept of intelligent environments poses many questions and maybe the biggest challenges so far regarding privacy as a basic human right, indispensable to sustaining democracy and the rule of law.

Bibliography:

1. Aarts E, Marzano S (eds.) (2003), The New Everyday: Views on Ambient Intelligence, Rotterdam: 010 Publishers.
2. Budapest Declaration on Machine Readable Travel Documents (MRTDs), 2006, available at: http://www.fidis.net/press-events/press-releases/budapest-declaration/
3. Clegg S.R., Courpasson, Phillips, (2006), Power and Organizations, SAGE Publications, London

4. Clegg Stewart R., David Courpasson, Nelson Phillips (2006), Power and Organizations, London: Sage Publications.
5. Cohen, S. (1985) Visions of Social Control, во Martin Innes, Understanding social control Deviance, crime and social order, Open University Press, 2003
6. Dilemmas Of Privacy And Surveillance, Challenges Of Technological Change (2007) The Royal Academy of Engineering, London
7. Final report Evaluation of the NSW government policy statement & guidelines for closed circuit television (CCTV) in public places, (2001) prepared for the Inter-Departmental Committee on CCTV c/o Crime Prevention Division, Attorney General's Department, accessed on: www.dlg.nsw.gov.au/dlg/dlghome/documents/Information/CCTV%20final%20reportPDF available on 18.02.2015tp://
8. Geradts Zeno and Sommer, Peter (2008), " D6.7c: Forensic Profiling", Future of Identity in the Information Society (FIDIS), accessed on: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.7c.Forensic_Profiling.pdf.
9. Innes Martin (2003), Understanding social control deviance, crime and social order, Open University Press.
10. Gubbi J et al. (2013), Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29 (7).
11. Hildebrandt Mireille (2008), Profiling and the rule of law, Identity in the Information Society, vol. 1, no. 1.
12. Järventausta P. et al. (2010), "Smart grid power system control in distributed generation environment", Annual Reviews in Control, 34(2).
13. Petersen, Julie K. (2007), Understanding surveillance technologies: spy devices, privacy, history & applications, 2nd ed., New York: Auerbach Publications, Taylor & Francis Group.
14. Scenarios for Ambient Intelligence in 2010, (2001), Information Society Technology Advisory Group; ISTAG.
15. Stern Paul C. and Harvey V. Fineberg (eds.) (1996), Understanding Risk, Informing Decisions in a Democratic Society, Washington: National academy press.
16. Wade Deisman, (2003),"CCTV: literature review and bibliography", Research and Evaluation Branch, Community, Contract amd Aboriginal Policing Services Directorate, Royal Canadian Mounted Police, accessed on: http://publications.gc.ca/collections/Collection/JS62-108-2003E.pdf
17. Welsh, Brandon C. and Farrington, David P. (2010) "Crime prevention effects of closed circuit television: a systematic review", Home Office Research Study 252, accessed on: http://www.chs.ubc.ca/archives/?q=node/655