Improvement of Civilian Oversight of Internal Security Sector Project II

İç Güvenlik Sektörünün Sivil Gözetiminin Geliştirilmesi Projesi II

Improvement of Civilian Oversight of Internal Security Sector Project

ICOISS Phase II

TR 2011/0324.02

DATA PROTECTION AND CCTV'S IN TURKEY

1.07.2013

Local Short Term Expert: ELİF KÜZECİ

Reference to the Description to the Action	
Component	A. Legislative Framework
Activity	A.7 Benchmarking and review of the video surveillance regulatory framework and mechanisms in selected EU countries and Turkey (Mobil Elektronik Sistem Entegrasyonu - MOBESE) with a view to enhanced civilian oversight
Output	A.7 Gap analysis of the video surveillance regulatory framework and mechanisms in selected EU countries and Turkey
Description	• A contribution to activity A.7, description of Data Protection and CCTV's in Turkey

"Improvement of Civilian Oversight of Internal Security Sector Project Phase II (ICOISS II) is funded by the European Union.The beneficiary of the Project is the Republic of Turkey Ministry of Interior.Technical assistance for the implementation of the Project is provided by the United Nations Development Programme."

AS TO THE FINAL REPORT OF DR. ELİF KÜZECİ CONCERNING VIDEO SURVEILLANCE LAW IN TURKEY

Project: Improvement Of Civilian Oversight Of Internal Security Sector In Turkey Phase II

Component A: Lagislative Framework

Activity A7: Benchmarking and review of the video surveillance regulatory framework and mechanisms in selected EU countries and Turkey (Mobil Elektronik Sistem Entegrasyonu - MOBESE) with a view to enhanced civilian oversight *(Output: gap analysis of the video surveillance regulatory framework and mechanisms in selected EU countries and Turkey).*

The meeting that the local short-term expert participated: 11 June 2013-Ankara.

Dr. Elif Küzeci's report consists of the following titles:

- **I.** INTRODUCTION
- **II.** THE NEED FOR DATA PROTECTION
- **III.** DATA PROTECTION LEGISLATION IN TURKEY
- **IV.** CONCLUSION

The following points can be derived from Dr. Küzeci's final report:

1-The key aspect regarding the need for data protection which is developments in computer and new communication technologies having a significant function on increasing the power of state. Thus, having the knowledge is a major component of power.

2-Answers to these questions in terms of law are really important: Where and by whom are the information which the state and private enterprises gather via tools developing and becoming widespread day by day recorded, for what purposes and how long are they used, what processes are made on data, and whom are they transferred to?

3-The answers to these questions will show how much “personal integrity”, the inseparable part of human dignity, is protected.

4-The main related legal provisions in Turkey are the articles 20 and 90 of the Turkish Constitution, the latter obliging the state to act in accordance with the human rights conventions. Turkish Civil Code art.24 provides that disclosure or misuse of personal data can be considered as an infringement of personal rights. Turkish Criminal Code art. 135,136 prohibits the unlawful recording and delivery of personal data and art. 138 provides penalty in case of failure to destroy personal data after the expiry of the legal period.

5-The measures taken by the authorities may breach the "right to privacy". An important European Court Of Human Right's decision in the case of P.G. and J.H. v. United Kingdom can be a good example in which the court draws the line between "monitoring" and "recording" of personal data the latter to be regarded as interference to right to privacy.

As a local legal expert of the UNDP I approve Dr. Küzeci's report.

Dr. Ahmet Yayla
Local Legal Expert For UNDP
University Of Bahcesehir Istanbul

Assist. Prof. Dr. Elif Küzeci
Bahcesehir University, Faculty of Law

DATA PROTECTION AND CCTV'S IN TURKEY

I. INTRODUCTION

Personal information has been important for "others" throughout history. Even though the reasons and target information types change, other persons (-for instance- spouses, relatives, friends, neighbors, etc.), certain communities (-such as- companies, religious communities, associations etc.), administrators (either pre-modern or modern) have always wanted to know us more inclusively.

Certainly, this has been due to very different reasons. The most basic reason is curiosity, which may assume as a human instinct. In this respect, people's desire to know more about each other has been the subject of substantial researches in the area of psychology. However, in addition to this, there is a variety of needs, which can be evaluated in sociological, political, and legal manners. The governments keep track of their citizens in order to ensure a rationalistic regime and security; enterprises monitor their clients for increasing profitability, whereas employers watch their employees to get a better performance. Of course the examples and their motives can be multiplied.

Nevertheless, in every respect, gaze from several actors, raises various questions concerning basic rights and freedoms. Necessity of replying these questions in the legal area and founding a balance between conflicting interests historically falls in a recent time. Even though keeping records about individuals is as old as the civilization itself, legislation on data protection had begun to be discussed in the 1960s. In this context, it should be noted that the first legislative regulation pertaining to protection of personal data had been accepted in this land, in the Hesse state of Germany in 1970. After this first legislation, it had been spread all over the Western Europe.

Of course speaking in terms of space and time, this is not a coincidence. In this period, the state's will of surveillance that has a long history as well as other novelties have enabled a more comprehensive scope of implementation for efforts of surveillance, which resulted in concerns of personal freedom.

Governmental bodies as well as private enterprises both have an increasing demand for personal data and they are in a certain sense "digitalizing" individuals to ensure more proficient use of these data. Therefore, they are improving surveillance

technologies with tremendous desire and pace. In this sense, rapidly widespread of usage of the CCTV's can be evaluated as a significant example. Especially for security reasons, both the governments and private entities use CCTV's. The Urban Security Management System (MOBESE) is the most significant example of CCTV usage in Turkey.

II. THE NEED FOR DATA PROTECTION

Surveillance may, in its most general sense, be defined as systematic investigation or monitoring of movements or communication of a single individuals or several persons. Collecting data about persons, monitoring them, and, in the general sense, surveillance as well as various instruments developed to serve this aim are not new. However, we should underline that, modernity and relevant emergence of the modern state has been a turning point. Consequently, current understanding of surveillance is a concept of modern ages. Discussing reasons behind this, is significant for us to understand the basic reason for existence of surveillance tools that surround us today.

Modernization process has both contributed in development of the right of privacy and also resulted in rapid increase of threats targeting the right in question. Modern state resembles a machine and needs data on citizens to function properly. Therefore, data on citizens are collected from various sources. Collected data are recorded according to present opportunities and it is attempted to derive rationalistic results. This is main reason of why the modern state depends on personal data. Because the bond between the ruler and the ruled has been deprived of the personal aspect of medivel times. Modern state should provide an objective base for its relations with citizens. Such necessity is manifestly observed at issues such as financial relationships, obtaining security, and drafting the state budget.

It is possible to examine state-held records in three basic categories as administrative records, intelligence records, and statistical records. One of the most significant rules for creating these records is surveillance. Local, domestic or religion based surveillance of the pre-modern era's fractured society has now been recessed and central surveillance has become solid and widespread.

Works of Foucault are important when we tring to define why we need data protection. Indeed, Foucault assesses surveillance not only that is created by organizations but in the context of "discipline" scattered in the whole society. He points at the structure of surveillance that surpasses borders of bureaucratic organization. Foucault explains his views particularly depending on panopticon, a prison architecture planned by J.Bentham. This structure's outer periphery has a building shaped as a ring and a tower stands in the center. This structure, as explained in detail by Bentham, has provided such an order that prisoners cannot know when they are monitored by guardians. The strength of the panoptic penitentiary lies in this aspect. Foucault considered panopticon as the fundamental logic of the modern state's target of disciplining the society. According to him, the modern society is a disciplinary society. In order to ensure submission of people to

social norms, people get increasingly monitored. Without their knowing, people's movements are monitored, documented, and classified. All these data are essentially related to the power.

It is clear: developments in computer and new communication technologies have a significant function on increasing the power of state or private enterprises. Thusly, having the knowledge is a major component of power. No matter with what expression it is called – "The Information Society", "Third Wave" or "Post-Industry Society" etc.- in this new era, the main emphasis is on "information". Protecting personal data is of key importance in consideration concerning the information society. The complex structure of a powerful state and capitalist enterprises along with it and developments in information technologies express processes which are bounded up and proceed parallel.

Significant technological developments, which are closely associated with data protection, may be analyzed by dividing into three periods. The first of these is the emerging of computers and establishing of data banks. Computers, when first emerged in the 1950's and 60's, were quite different than today's computers. These big, complex and hard-to-use machines were only used by large companies and the state, due to their high cost. In other words, these not widely-used machines were in the hands of central authorities. This caused an avoidance of power concentration in the establishments using computers. Making it possible to gather data in centralized data banks has also an effect on this concern. In the 1960's and 70's, with bureaucrats' seeing the benefits of gathering the dispersed data in central data banks and, of course, the information technologies making it possible, most states made an attempt to establish central data banks. Setting an ID number for each citizen, which was debated and started to be applied in the same period, caused debates on protecting data to be blazed. Another application bringing many questions along with it is using automatic systems in population census. Public susceptibility is raised from the potential of these progresses to attack on main values, such as the right of privacy and personal integrity, and the fear of the structure of pluralistic democratic society's collapsing. From now on, personal data have started to be transferred from the memories of relatives or from the files in the dusty archives of various establishments into electronic environment at a fast pace. It is the reason that society, philosophers, lawyers and writers closely approach to the impact of usage of computers becoming widespread on private life from the beginning of the 1960's. It may be said that the most important surveillance devices in the present day are the databases and the computers enabling to keep, to match, to process and to market the gathered data. It has been possible to create integrated profiles of citizens by using commercial databases, such as credit card or telephone databases, besides the databases of the state. Whether we are aware of it or not, personalities formulized with various numbers within the networks compose more detailed pictures in the corridors of computers day by day.

So when we review the impact of technology, in the aspect of gathering and processing personal data, we must emphasize that the first important milestone occurred after the emerging of computers and databases. The second big change

was created by the Internet becoming improved and widespread. Internet, “The network of the networks”, walked into our lives in the 20th century, and become, unquestionably, a part of our lives in the 21st century. By interconnecting computers, sharing, associating and integrating between completely different databases have been enabled. It is not surprising that the youngest members in the list of dollar millionaires of Forbes’ February issue are the owners of companies providing services via the Internet. E-mail, search engines, social networking websites, online banking, e-commerce, e-shopping, smart phones with 3G connection are musts for most people. But, in this point, it must not be forgotten that every action on the internet leaves a trace and the information concerning this action is recorded and held somewhere. Internet is not only a window to the world; also numerous agents can reach our private lives through that window. While reviewing the relationship between the developments in technology and protection of personal data, advancements in new information technologies must be said. Besides computers and the Internet, some other methods closely associated with them are also in use, and their using rate is rising. CCTV, RFID, biometric methods, DNA analyses, GPS are examples to them. It should not be missed that new methods are added to these example every passing day and expressions such as “ubiquitous computing”, “cloud computing” are becoming widespread indicate developments in technology.

The question which must be asked but is ignored most of the time is: where and by whom are the information which the state and private enterprises gather via tools developing and becoming widespread day by day recorded, for what purposes and how long are they used, what processes are made on data, and whom are they transferred to? The answer to that question will show how much “personal integrity”, the inseparable part of human dignity, is protected. Above all, constant monitoring and surveillance hinder oneself to develop their “personality” – which is the unique characteristic of him / herself. Thusly, this concern has mainly been effective in accepting legal regulations concerning protecting personal data in democratic states. It must be stated that what has been aimed by protecting personal data is not setting barriers in front of the technological developments, nor banning data processes, many of which can be indeed useful. What have been aimed are these processes to be carried out by only authorized people and only for legal purposes. Besides that, it is important that one must not sever all ties with self and be aware of “informational self determination” (Informationelle Selbstbestimmung) as described in the famous decision by German Constitutional Court in 1983.

We can find in literary works vivid depictions of what kind of environment we can find when these requirements are not met. The “Big Brother”, depicted in George Orwell’s 1984, is the most referred metaphor on this matter. However, the present situation, I suppose, can amaze even Orwell himself. First of all, as I’ve mentioned before, who monitors us in the present time is not only the “Big Brother”, the ruler who is willing to observe and discipline all his citizens. Private enterprises, which can be named as “Little Sisters”, improve their skills on surveillance and manipulate people in order to materialize their economic interests. Another point Orwell misses is that although surveillance is associated with totalitarism, it can be performed under democratic regime, and in other words, a velvet glove can hide the iron fist. Lastly, in the

environment described in the novel, those who are monitored know by which device they are monitored. In present day, this monitoring is applied without our awareness. This brings obscurity and indefiniteness, a dark depiction of which Kafka did in his work, “The Trial”. It will be quite difficult to improve moral and material existence freely in such an environment. Besides that, the novels “1984” by Orwell, “Brave New World” by Huxley and “We” by Zamyatin depict how the government, which is ever-monitoring the people, can destroy human values. In an absolutely-planned world of mathematical exactness, there is no place for much needed creativity, accidentalness and a value that is peculiar to humans: individual autonomy.

Because of all these reasons, today data protection legislation is a necessity. Although legal regulations concerning protection of personal data are not capable of providing a complete protection against fast-growing technology and rising flow of information, as we describe above, it is the most important of the few assurances we have, which can avoid curios agents who are waiting in front of our doors.

III. DATA PROTECTION LEGISLATION IN TURKEY

The first legislative regulation pertaining to protection of personal data had been adopted in the Hesse state of Germany in 1970. After this first legislation, it had been spread all over the Western Europe and in a short time data protection regulations have adopted both national and international level. These are the most important international instruments on the subject:

- OECD-Guidelines on the protection of privacy and trans border data flows of personal data (1980)
- Council of Europe- Convention for the protection of individuals with regard to the automatic processing of personal data (1981)
- United Nations-Guidelines concerning computerized personal data files(1990)
- APEC-Privacy Framework (2004)

If we look at the legal texts developed in order to protect personal data since 1970, it is possible to ascertain some changes regarding new technological products and contemporary requirements, like wide spreading use of cloud computing, social networks, RFIDs or CCTVs. It does not seem too easy to solve all the problems related to data protection. In recent period, reviewing the efficiency of provisions under EU regulations and ongoing discussions signify that the development of legal provisions in this area has not come to an end.

We need to define the situation in Turkey in this respect. Although, in Turkey, systems collecting personal data spreads rapidly, other side of the issue, namely the legal protection of personal data is falling short when we compare it with the other democratic states. Furthermore, we can say that effective public debate regarding the problem does not take place.

The most important legal provision on data protection in Turkey is stated in the Article 20 of the constitution. Protection of personal data has been a subject of a

constitutional amendment after the referendum held on 12 September 2010. The provision amended to the Article 20 of the Constitution states personal data protection as a constitutional right and also guarantees some basic principles of data protection. This article stimulates that:

“Everyone has the right to demand the protection of his/her personal data. This right comprises the right to be informed about the personal data concerning himself/herself, access to such data, right to request correction or deletion of them as well as the right to be informed if such data is used in accordance with the purposes for which it was collected. Personal data can be processes only in cases regulated in a law and upon express consent of the subject individual. Principles and procedures regarding the protection of personal data shall be regulated by a law”.

We can state that it is not possible any more to neglect effective protection of personal data in Turkey due to this provision. Hereinafter adopting new provisions and reviewing the current ones is a constitutional requirement. While adopting new laws in the light of the provision amended to the article 20 of the constitution, European Convention on Human Rights must be also taken into consideration. Hence, it is a constitutional obligation. Indeed, duly adopted international conventions have the force of law pursuant to the Article 90 of the Turkish Constitution. Besides that, this Article also requires to prevail the provisions of international agreements in the area of fundamental rights and freedoms, when they conflict with the domestic laws. Article 90/5 states that:

“International agreements duly put into effect bear the force of law. No appeal to the Constitutional Court shall be made with regard to these agreements, on the grounds that they are unconstitutional. In the case of a conflict between international agreements in the area of fundamental rights and freedoms duly put into effect and the domestic laws due to differences in provisions on the same matter, the provisions of international agreements shall prevail”.

Turkey has ratified European Convention on Human Rights (ECHR) in 1954. According to Article 90/5 of Turkish Constitution, provisions of the Convention are also part of Turkish legal system.

Data protection is not an independent right in ECHR. However, the European Court of Human Rights (ECtHR) applies Article 8 of the Convention as basic principle of data protection in its judgments. As it may seen in many decisions of ECtHR, the objective of the Convention is to secure the rights in effective and practical way and not through imaginary or theoretical measures. This approach constitutes a basic but significant principle to bear in mind, not only for the Convention, but also implementing provisions concerning data protection in Turkey.

Despite the constitutional provision and the decisions of ECHR, the most important problem is the legal shortcomings. The clear sign of this fact is that we do not have a legal framework that constitutes basic principles regarding the protection of personal data. Draft law on data protection is pending and the entry into force is still shrouded in mystery. It is also need to be mentioned that, the draft law, if it is adopted in its

present form, would be lacking of full and inclusive protection. It is a necessity to update and reevaluate it before the date of entry into force. It should be noted that there is some promising efforts to make changes on some provisions, but it is so hard to be optimistic about the possible revisions.

The lack of framework law causes some significant consequences. For instance, Convention for the protection of individuals with regard to automatic processing of personal data, has been signed by Turkey in 1981, but the process of adoption has not been completed due to the lack of a framework law. Besides that, more importantly, the absence of a framework which constitutes basic principles, jeopardizing the enforcement of legal provisions on data protection and they may provide just a limited protection. This can be seen clearly in evaluating the application of the related provisions of Turkish Penal Code, Civil Code, Code of Obligations or other legal instruments.

For instance, disclosing or misuse of personal data can be considered as an infringement of personal rights to these general rules of the Civil Code. Indeed Article 24 of the Civil Code states that:

“The person subject to assault on his/her personal rights may claim protection from the judge against the individuals who made the assault. Each assault against personal rights is considered contrary to the laws unless the assent of the person whose personal right is damaged is based on any one of the reasons related to private or public interest and use of authorization conferred upon by the laws”.

Besides Civil Code, Turkish Criminal Code also states some provisions directly aim to protect personal data. In this sense, Article 135 regulates unlawful recording of personal data and it states that:

“Any person who unlawfully records the personal data is punished with imprisonment from six months to three years.
Any person who records the political, philosophical or religious concepts of individuals, or personal information relating to their racial origins, ethical tendencies, health conditions or connections with syndicates is punished according to the provisions of the above subsection”.

Moreover Article 136 states that:

“Any person who unlawfully delivers data to another person, or publishes or acquires the same through illegal means is punished with imprisonment from one year to four years”.

Article 138 of the Turkish Criminal Code is on destruction of personal data and it stimulates:

“In case of failure to destroy the data within a defined system despite expiry of legally prescribed period, the persons responsible from this failure are sentenced to imprisonment from six months to one year”.

However they can just serve a limited protection since the lack of a framework code which describes:

- The meaning of personal data,
- Grounds for the protection of personal data,
- Principles to provide the protection,
- Responsibilities of data processors and
- The rights of data subjects.

Unfortunately in practice we are facing with this fact: our private life and personal data is almost not a subject of a legal protection. Judges may have some problems to determine whether there is an issue regarding “personal data” and besides that Turkish citizens generally do not apply to the courts based on these regulations. The second aspect of the problem appears at this point: We do not have the awareness for the problems that may arise from absence of protection.

We need to determine the rapidly evolving usage of CCTV’s in this sense. Monitoring public spheres by CCTV’s, namely MOBESE systems in Turkey, is a substantial issue related to data protection. Indeed, the imagery data records mostly cause identification of an individual in direct or indirect way. That is why the principles of personal data protection should be forceful in this subject. Thus we need to point the real and potential problems related to the usage of CCTV’s.

These systems can be used for maintaining specific objects, like security and controlling the traffic flow. Besides that they can be used either monitoring a specific person who is accused or suspected for a crime, or preventing crimes through recording public spheres such as stadiums, bus terminals etc.

According to ECtHR decisions, it is stated that monitoring of public spheres is not a violation of privacy only if they are not recorded. But imagery data recording and doing this systematically and permanently, changes the situation. At his point, we need to remember objectivity and proportionately principle. In this sense, the reason of the monitoring of the person should always be taken into consideration. If the anonymous data is enough to reach the aim, then the data should not be linked to an identified person. In P.G. and J.H. v. United Kingdom (application no. 44787/98) case ECtHR stated that:

“There are a number of elements relevant to a consideration of whether a person’s private life is concerned by measures effected outside a person’s home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person’s reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be

visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method" (par.57).

III. DATA PROTECTION LEGISLATION IN TURKEY

I.

As a conclusion, it is quite obvious that there is a necessity of a framework law regarding protection of personal data in Turkey. It has become more obvious when we think on solicit examples, like usage of MOBESE cameras. Under the explicit regulation in the Article 20 of the Constitution, regulating CCTV usage in Turkey, has become an essential requirement. In this potential regulation and its implementation, basic principles of data protection will provide a guideline for us. Furthermore, it must be taken into account that necessity of awareness about protection of personal data and demanding its realization are of utmost importance.

It must not be forgotten that one of the most powerful weapons we have, are legal regulations concerning protection of personal data in an era in which as some authors call "the end of the privacy". Thus, our space protecting in the scope of "the right of privacy" is consisted of unique features which differ us from each other. Unlimited access to our names, preferences, likes and thoughts may render "being us" impossible. This is an assault aimed at human dignity.