Protection of Personal Data in Turkish Law

YILDIZ Sevil[1]

[1] *Selcuk University (TURKEY)*
Email: syildiz@selcuk.edu.tr

DOI: 10.26352/CJ02F5017

Abstract

The rapid development of information and communication technologies has caused personal data to be shared and spread more easily. Consequently; protection of personal data has become an important need. Personal data is defined as; any data about a real person whose identity is identified or can be identified. Within this context, not only the basic personal identification information such as the person's name, surname, date and place of birth, but any other personal data that can be directly or indirectly make such person identifiable, such as phone number, motor vehicle plate number, social security number, passport number, personal background, photo, video or audio records, fingerprints, genetics data, IP address, e-mail address, equipment identities, hobbies, preferences, contact persons, group memberships, family information etc. are included within the scope of personal data.

The right of the protection of personal data is included among the basic personal rights and freedoms. It is vital for the protection of the person's privacy and for the empowerment of democracy and the principle of the state of law. The basic reason for the protection of private life, including personal data, through constitutional guarantee is to allow for the free development of personality and to provide the person with a free environment where the person can be alone with himself/herself and his/her acquaintances without being disturbed by the state or by other people.

Many legal arrangements have been made particularly on the international arena for the protection of personal data, which is one of the rights of personality. Among these, the Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data is the most significant one. This paper aims to analyze the Turkish law and legislation with regard to the protection of personal data. The current situation will be assessed with regard to conformance to international legislations.

Keywords: Information technologies, Protection of personal data, Turkish Law

1. Introduction

As information and communication technologies began to be part of our daily lives as they widespread, "information" began to gain value when compared with previous periods. Increased usage of "Information" in all kinds of economic and social activities of the community, made it necessary for this information to be transmitted in a fast and reliable way with reasonable costs and this change being lived through in economic and social ground began to be expressed with the concept of "information community" (Murray, 1998, p.112). Increase in the alternatives regarding the transmission, storage, alteration, classification, and searching of said information has brought up the question as how to protect the personal data defining and specifying an individual without giving any harm to the fundamental rights and freedoms.

Protection of personal data aims to protect the individual rights and freedoms during the processing of these data. In this frame, right to protect personal data aims not only to protect the data itself as being independent of the rights and freedoms of the individual but it also aims to protect the freedoms of the individual. Therefore, protection of individual data serves to protect the fundamental rights and freedoms of individual against unlimited collection, recording, usage, and transfer of personal data by the public bodies. The adjustments made for this purpose, define the principles of having access to these personal data, using these data and processing them in general meaning and they provide various rights to the individual in cases where they are used by violating these principles (Kong, 2010, p. 443).

Threats developing against personal data which can be defined as all kinds of information suitable for specifying the identities of individuals, has made it necessary to develop a defense mechanism against the surveillance technologies and it was seen that it was required to have law for the protection of personal data. Adjustments aiming to inspect the person being related with personal data, has first come out in 1970s in Europe as the computers developed fast and central data banks were established and in time they spread around the world (Kaya, 2011, p. 331).

Even though our country, being a state of law that is democratic and respectful to human rights as being stated in 2nd article of Constitution dated 1982, is a member of organizations like United Nations, European Council and OECD, it could not transfer the principles accepted by international institutions in this area to its national law for a long time as there was no private law protecting personal data. By adding a sub clause to the 20th article of Constitution in 2010 for the regulation of private life which stated: "*Everyone has the right to request the protection of his personal data.*

This right also comprises notification of the person about his personal data, having access to these data, requesting them to be corrected or erased, and learning whether they are used in line with their purpose or not. Personal data can only be processed in situations where permitted by law or as per the explicit consent of the person. Basis and procedures as regards to the protection of personal data are regulated by law.", protection of personal data of individuals was openly secured by the constitution. This regulation was criticized in that the conditions under which the protection of personal data could be restricted was not specified in the doctrine and that an independent organ to inspect the processing of personal data was not stipulated (Cengiz, 2016, p. 85).

"Contract for protecting the individuals against personal data's being made subject to automatic processing" with no.108 which was prepared within the body of European Council as being opened for signature on the 28th of January,1981 and being put in effect on the 1th of October,1985, was not approved for a long time although it was signed by our country on the 28th of January,1981 and finally as it was approved according to the law regarding 'Contract for protecting the individuals against personal data's being made subject to automatic processing" with no. 6669, and it was put in effect on the 18th of February, 2016.

In the regulations of many states in Europe, laws regarding the protection of personal data are present for more than forty years (Kong, 2010, p. 442). Almost all of the modern states have introduced fundamental laws regarding this subject. It can be stated that for certain reasons there is an increasing pressure on the states not having made any adjustments regarding this subject, for the protection of personal data by the fundamental laws in national regulation. The first reason for this tendency is that importance was given for the protection of fundamental rights and freedoms in countries where there used to be authoritarian regimes before, in order to avoid experiencing similar cases. Another reason is the desire to eliminate the obstacles in front of commerce that develops through technology and mainly electronic trading. Third reason is realization of required

amendments in the regulations of countries which would like to have trade with European countries as per the reason that the transfer of personal data to countries not providing sufficient protection of personal data has been prohibited according to European Union Directive with no 95/46/EC (Korkmaz, 2016, p. 221).

Although there are scattered provisions regarding the protection of personal data in our regulation, lack of a private law defining fundamental principles as being integrating, was seen as an important deficiency for a long time. All of the reasons stated above are present for having a fundamental law to protect the personal data in our country. Firstly, the outcomes of unjust interference to the individual rights and freedoms like unlawful tagging and security investigations at various periods in our country, reveal the damages that could occur in cases where personal data are not protected sufficiently. In case the required and sufficient measures are not taken, the probability for these kinds of unjust applications to occur in democratic managements always exists besides the authoritarian regimes. Having a private law in Turkey as regards to the protection of personal data is a requirement first of all as it is a fundamental human right. Furthermore, it is required to protect personal data in order to avoid our country to remain behind in economic activities like electronic trading that advances. Besides, as it is prohibited to make the transfer of personal data to countries which do not provide sufficient protection as per 25th and 26th articles of European Directive with no 95/46/EC, in order to enable effective trading to be realized with these countries and to avoid experiencing various problems due to the specified provisions, it is important to make an adjustment in our country in this direction. Furthermore, an adjustment to be made in this subject is also required as regards to the candidacy process of Turkey in European Union. The first committee to prepare a private law for protecting personal data in our country was established in 1989 but they could not complete their studies (Johnson, 2007, p. 46).

Law draft prepared for the protection of personal data was sent to Presidency of the Grand National Assembly of Turkey on the date of 18.01.2016 by the Presidency. Committee of Justice has presented their report about the proposal on the date of 12.02.2016. The law for the Protection of Personal Data with no.6698 was finally accepted at the Grand National Assembly of Turkey of the 24th of March, 2016 and it became a law.

2. The Concept of Personal Data the Purpose of Law

The concept of personal data has been defined on the 3rd article of the law. Accordingly, all kinds of information relating to a real person whose identity is specified or could be specified, is being considered as personal data. A person's being specific or being specifiable has been defined in the justification as making that person definable by associating the existing data with the real person somehow. This definition complies with the definition of personal data made both in the European Council Agreement with no. 108 and in the European Union Directive with no. 95/46 (Cengiz, 2016, p. 88).

In the first article of the Law for the Protection of Personal Data with no.6698 with the heading of "Purpose", the purpose aimed to be attained by the law has been defined. Accordingly, the purpose of Law for the Protection of Personal Data is: "*To protect the fundamental rights and obligations of real and legal entities and mainly the confidentiality of private life while processing personal data and to regulate the liabilities of real and legal entities processing personal data and the rules and procedures which they shall comply with*."

In the justification of article, it was stated that with the article the purpose of Law was defined and that this purpose was to discipline the processing of personal data and to protect the

fundamental rights and obligations stipulated in the Constitution, mainly being related with the confidentiality of private life. In the justification it was also stated that with the law it was aimed to protect the right of privacy of people which gained importance recently and to regulate the liabilities of real and legal entities and the rules and procedures they must comply with. As the article text is reviewed, we can see that the purpose of law has been adjusted within the frame of 20th article of the Constitution. The article is in parallel with the 1th article of European Union Directive with no 95/46 (Korkmaz, 2016, p. 48).

2.1. Processing of Personal Data

Processing of personal data has been defined in the 3rd article of Law as: "All kinds of processes realized on the data like obtaining personal data through partially or completely automatic paths or through non automated paths on condition that they are part of a data recording system, their being recorded, stored, maintained, amended, readjusted, disclosed, transferred, taken over, being made attainable, being classified, or being avoided.". Therefore, all kinds of transactions realized on data starting from the point where personal data is attained for the first time, have been evaluated as processing of personal data. Apart from these, combining personal data, correlating them with other data, their being erased, and other processes realized for this purpose as covering a wide range of area, are also considered within the definition of processing of personal data (Kaya, 2011, p. 329).

In the 4th article of Law for the processing of personal data, the principles have been adopted.

These are compliance with law and rules of honesty, being correct and updated as required, being processed for specific, clear, and legitimate purposes, being related, limited and restrained as per the purpose for which they are processed, and being stored for a period required for the purpose of their being processed and as being stipulated by the related legislation.

Processing of personal data has been linked with certain conditions. First of all, general rule for the transaction of processing is to obtain explicit consent of the related person. Or else, the processing of personal data has been prohibited. The concept of explicit consent has been defined in the law as consent that is based on being informed about a specific subject and which is expressed as per free will. In the articles 2/h and 7/a of the Directive with no.95/46, the consent of relevant person has been considered among the cases which legitimates the processing of data (Kılınç, 2012, p. 1093).

As regards to the processing of data, there are certain cases when having the consent of data owner is not required. These cases are (Tekin,2014, p. 249):

- Having an explicit provision in law relating with the processing of data,
- Inability of relevant person to express his consent or its being required to protect the life and body integrity of relevant person, for whose consent no legal validity is attached, or some other person,
- The requirement for the processing of personal data of the parties on condition that they are directly related with the formation or realization of a contract,
- It's being required for the data responsible to execute his duties
- In cases where the data have been made overt by the relevant person,
- It's being obligatory for a right to be established, used, or maintained,
- It's being required for the data to be processed as regards to the legitimate interests of data responsible on condition that no damage is given to the fundamental rights and freedoms of relevant person.

In the 6th article of the Law, data of people relating with their race, ethical origin, political view, philosophic beliefs, religion, sectarian, or other beliefs, dressing, membership in unions,

foundations, or associations, health, sexual life, penal sentence, and security measures as well as their biometric and genetic data have been considered as personal data having private quality. In the 3rd sub clause of the article, personal data relating with health and sexual lives have been regulated privately in a different way than the others. Accordingly, all of the personal data other than those relating with health and sexual lives, could be processed in cases specified by the law without getting the explicit consent of the relevant person. But processing of these two types of data having private quality, could be possible if they are realized by people or authorized institutions having confidentiality obligation with the purpose to protect public health, preventive medicine, medical diagnosis, execution of treatment and care services, planning and management of health services and financing. Law requires for the measures being specified by the Council of Protecting the Personal Data to be taken in order for personal data with private quality to be processed (Ayözger, 2016, p. 188).

2.2. Transfer of Data

Transfer of data has been divided as domestic and foreign transfer as per the law. Transfer of personal data to other people within the country is subject to the rules stipulated for the processing of data. In this respect, for the realization of transfer process, first of all the consent of relevant person should be obtained. For realizing transfer to foreign countries, in addition to these conditions mentioned, it was stated that it is required for sufficient protection to be provided in the related foreign country (Küzeci, 2010, p. 76). Countries where there is sufficient protection will be determined and announced by the Council. In case the country to where data transfer will be realized does not provide sufficient level of protection, it is required for the data responsibly in both countries to undertake this protection as written and permit should be obtained from the council. As regards to the transfer of data to foreign countries, similar adjustments exist in the directive with no. 95/46. In the Directive, a system has been adopted which prohibits the transfer of data to third countries where there is not sufficient level of protection (Ayözger, 2016, p.188).

2.3. The Tasks of Data Responsible

Data responsible has been defined in the 3rd article of Law as: "Real or legal entity specifying purposes and tools for the processing of personal data as being responsible for the establishment and management of data recording system." This person is responsible from all kinds of processes realized as relating with the data. It is required for data responsible to enlighten the data owner about his identity and the identity of his representative, if any, about the purpose of processing data, about the people to whom the data will be transferred and the purpose of transfer, the method of collecting data, and its legal reason (Kılınç, 2012, p. 1096).

Acting in contradictory to the obligation to enlighten, to provide data security, and to realize the decisions taken by the council, as including the liability to unregister and to make notification, has been adopted as being a crime according to the law.

As within the scope of obligation to enlighten, data owner has the right to learn whether any processing has been done on his data or not, to obtain information about the purpose and method in case such processing is done, to be notified about third parties to whom his personal data has been transferred within or outside the country, to ask for the correction of any possible deficiencies or mistakes as relating with processing of personal data, to make objection to analysis outcomes of processed data being obtained through automatic systems, to request for the data to be erased or destroyed, and to ask to be indemnified due to the losses incurred as a result of unlawful acts (Tekin, 2014, p. 256).

Institution for the Protection of Personal Data, being responsible from the implementation of law, has been established. The decision-making body of the institution being composed of council and presidency, is the Council of Protection of Personal Data. The tasks of the instruction are to follow up the applications and legal developments in national and international ground, to make research and investigation regarding this subject, to cooperate with the relevant institutions and associations, and to make proposals as regards to the subject matters required (Kaya, 2011, s. 329).

3. Conclusions

All kinds of information belonging to a person which makes a person defined or definable are considered as personal data. Protection of these data is a fundamental human right. Obtaining and processing of personal data in an uncontrolled way, is threatening many fundamental rights and freedoms, and mainly the confidentiality of private life. In our country with the addition of provision with no. 20/2 to the Constitution in year 2010, the required legal basis for the protection of personal data has been established. Thus, individuals began to be protected at Constitutional level. But it has taken a long time to complete this regulation, being important as regards to the data protection law, with a special law of implementation as relating with the subject. Turkey has remained as the only country which has signed the Contract of European Council with no.108 but which could not approve it since a private law being specified as obligatory in the contract could not be introduced. This situation has given rise to a problem as European countries did not transfer personal data to countries where there was not sufficient protection. As a result of the studies carried out, the Law for the Protection of Personal Data was accepted on the 24th of March, 2016.

As the law is investigated, it is seen that adjustments being parallel with Contract with no.108 and the Directive with no.95/46, have been made. Accordingly, it was adopted as the fundamental principle to process personal data according to the conditions specified in the law, to enlighten the data owners, to establish an authority for inspecting and regulating this area, and to take the necessary measures as relating with data security.

Furthermore, with the Law that was prepared by considering current and future requirements, it was aimed to catch up with the contemporary standards and to provide protection in this direction.

In order to minimize the problems that could arise as relating with this subject, it is especially important to inform the individuals and relevant institutions about data security and to improve their consciousness.

REFERENCES

1. Ayozger,C. (2016). *Kişisel Verilerin Korunması*. Turkey: Beta
2. Boz, A. (2014). *Kişisel Verilerin Korunması: Türkiye, ABD ve AB Örnekleri* (Master's thesis), Polis Akademisi Güvenlik Bilimleri Akademisi.
3. Cengiz,T. (2016). Uluslararası Düzenlemelerde ve Türkiye'de Kişisel Verilerin Korunması. In Selda Güneş Peschke, Lutz Peschke. *New Media and Law: A Comparative Study.* Ankara: Yetkin.
4. Johnson, E.H. (2007). Data Protection Law in the European Union, *The Federal Lawyer*. USA
5. Kaya, C. (2011). Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi. *İÜHFM*. 69 (1-2). İstanbul
6. Kılınç,D. (2012). Anayasal Bir Hak Olarak Kişisel Verilerin Korunması. *AÜHFD*. 61(3). Ankara: Adalet.
7. Kong, L. (2010). Data Protection and Transborder Data Flow in the European and Global Context. *European Journal of International Law*. 21(2).
8. Korkmaz, I. (2016). Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme. *TBB Dergisi*. 124. Ankara: Adalet.
9. Küzeci,E. (2010). *Kişisel Verilerin Korunması*. Ankara: Turhan

10. Murray, J.P. (1998). The Adequacy Standart Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standart? Fordham International Law Journal, 21 (932).
11. Tekin, N. (2014). Kişisel Verilerin Korunması İle İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma DirektifiIşığında Değerlendirilmesi . *Uyuşmazlık Mahkemesi Dergisi*. 78(1). Ankara.