Akademik Hassasiyetler **The Academic Elegance**
Yıl/Year: 2020 **Sayı/Issue: 13**
Cilt/Volume: 7 **Sayfa/Page: 449-472**
Araştırma Makalesi
Makale Gönderim Tarihi: 05/09/2019 **Makale Kabul Tarihi: 29/05/2020**

A REVIEW ON THE PERSONAL DATA PROTECTION AUTHORITY OF TURKEY [*]

İsmail SEVİNÇ[**] & Niyazi KARABULUT[***]

Abstract

The Personal Data Protection Authority which has administrative and financial autonomy and public legal personality was established in order to perform the duties stipulated by Law No. 6698 in February 2016. In this study, the power of sanction and the capacity to impact of the authority are examined over its missions and visions. By examining the authority, this study tries to find the answers of the questions of why it is needed, how it protects personal data, and to what extent it is successful. Eventually, this study aims to analyze how this authority can be more efficient and accordingly to give suggestions of implementation for future studies in the light of a swot analysis. As a result of the study, it was found that the Authority's operational capacity is not in a satisfying level and it is not known by public enough. The number of applications and complaints are also not in a satisfying level. In return, it is recommended in this study that, the authority should develop its operational capacity, act more independently, and propagate and extend its functions by taking good examples from the world.

Keywords*: personal data, protection, personal data protection authority, the right of personality*

KİŞİSEL VERİLERİ KORUMA KURUMU ÜZERİNE BİR İNCELEME

Öz

Kişisel Verileri Koruma Kurumu 2016 yılı şubat ayında 6698 sayılı kanunun verdiği yetkileri ugulamak üzere kurulmuş idari ve finansal otonomiye sahip bir kurumdur. Bu çalışmada kurumun misyonları ve vizyonu üzerinden etki ve cezalandırma kapasiteleri incelenmektedir. Kurumun incelenmesi ile kuruma neden ihtiyaç duyulduğu, kurumun kişisel verilerin korunmasında nasıl rol aldığı ve ne ölçüde başarılı olduğu sorularına cevap aranmaktadır. Bu soruların cevaplarından yola çıkılarak bu çalışmada temel olarak kurumun nasıl daha etkili ve başarılı olabileceğinin analiz edilmesi ve buna yönelik olarak önerilerde bulunulması

[*] Bu çalışma 18-20 Nisan 2019 tarihlerinde düzenlenen KAYSEM13 konferansında sunulan "A Review on the Personal Data Protection Authority of Turkey" başlıklı bildirinin genişletilerek makale formatına dönüştürülmüş halidir.

[**] Doç. Dr., Necmettin Erbakan Universitesi Siyaset Bilimi ve Kamu Yönetimi Bölümü, isevinc@erbakan.edu.tr, https://orcid.org/0000-0002-4229-8760

[***] Arş. Gör., Necmettin Erbakan Universitesi Siyaset Bilimi ve Kamu Yönetimi Bölümü, nkarabulut@erbakan.edu.tr, https://orcid.org/0000-0002-6175-2025

hedeflenmektedir. Bu kapsamda kurumun güçlü,ve zayıf yönleri ile sunduğu fırsatlar ve karlıaştığı tehditler ele alınmıştır. Çalışmanın sonucunda ise kurumun operasyonel açıdan eksikliklerinin olduğu ve toplum tarafından henüz yeterince tanunmamasından dolayı kuruma yapılan başvuru sayısının düşük bir seviyede kaldığı saptanmıştır. Bu sonuçlara yönelik olarak kurumun gelişmiş ülke örneklerinden yola çıkarak bağımsız hareket etme kapasitesini geliştirmesi, tanıtım faaliyetlerine ağırlık vermesi ve kurumsal ve işlevsel kapasitesini artırması üzerine önerilerde bulunulmuştur.

Anahtar Kelimeler: *Kişisel veri, kişilik hakları, kişisel verileri koruma kurumu*

Introduction

In today's world, individuals have become more and more challenging in protecting their personal rights and space because of rapid developments in technology. Technological progress in recent years has created some security problems about the protection of personal data. Discussions on this issue have also attracted a new field of study that has named as "protection of personal data". The driving impetus in the conduct of these discussions has been the concern of protecting personal spaces that has become more and more transparent with technical and technological developments such as the unrestrainable expansion of social media. As an example, individuals need to share some of their personal data in order to create specific social media accounts and they need to authorize them to use their personal data. With the impact of globalization, there have been many serious changes in the political, economic, social, and cultural structures in the world. The main factor affecting this change is the incessant developments in information and communication technologies. In the twentieth century, there have been rapid developments in political, economic, social, and technological fields. Indeed, very rapid developments have been observed especially in information and communication technologies in this century. These developments, along with many conveniences, have brought some serious problems (Chua et al., 2017).

Due to the developments in information and communication technologies, it has become easier for personal data to be compiled, classified, stored and easily presented when requested, and as a result, some risks have been occurred on illegal use of this information related to private life. These technologies enable the disclosure of personal data to others without the consent of the person and the transfer of the information from their location to other places. Moreover, the Internet plays a leading role in the spread of information and communication technologies and thus personal data. Especially with the developments in the Web 2.0 technologies and social networks, information flow has been fastened (Wu, 2014). Social networks are an obvious example for the observation of concerns about the protection of personal data (Caudill and Murphy, 2000). Social networks have emerged as a social and economic phenomenon that has changed the usual ways of communication between people. They brought people together

regardless of the distance between them, and they enabled people to communicate with each other on the Internet. Therefore, social media allows users to access all the information, images, videos, and other documents downloaded to their profiles on the social network and to be seen by anyone using those platforms (Dinev and Hart, 2005). In other words, many personal data are shared in these environments. Therefore, these shares create certain risks for the protection of personal data.

For the protection of personal data; right to privacy and right to personality are guaranteed in international conventions on human rights and in constitutions of democratic countries. After the developments in the information and communication technologies, the Internet, and social networks; many new measures have been taken. New legal regulations have been enacted in many countries around the world on the protection of personal data. Also internationally accepted conventions have been regulated on this issue. As a result of these regulations, some certain measures have also been taken such as establishments of personal data protection authorities, complaint and request platforms and so through.

In Turkey, Personal Data Protection Law no. 6698 was enacted in March 24 of 2016 and the Convention on the Protection of Individuals against Automatic Processing of Personal Data No. 108 prepared by the Council of Europe put into force in January 30 of 2016. As an output, Personal Data Protection Authority (KVKK), which has administrative and financial autonomy and public legal personality, established in order to perform the duties stipulated by Law No. 6698. Later in this study, the power of sanction and the capacity to impact of the authority will be examined over its missions and visions. Past works of the authority will be evaluated and some comparisons will be made with other examples from the world while doing this examination. By examining the authority, this study tries to find the answers of the questions of why it is needed, how it protects personal data, and to what extent it is successful. Eventually, this study aims to analyze how this authority can be more efficient and accordingly to give suggestions of implementation for future works of it.

1. PERSONAL DATA

Personal data is a concept that is controversial and cannot be described precisely; however, it is possible to define it as any kind of information that can define the individual (Dülger, 2016:101). In General Data Protection Regulation (GDPR) of EU (1995), personal data defined as "any information relating to an identified or identifiable natural person". Personal data is also defined as "any kind of information relating to an identified or identifiable real person" in the Turkish Personal Data Protection Law no. 6698 (2016:1). Identity information, age, marital status, phone numbers, address information, health information, passport information can be given as examples of personal data. However, it is actually a more comprehensive concept that contains personal rights like right to privacy and

right to personality. Therefore, the person's religious belief, conscience, thoughts and opinions, physical characteristics, information about health, education, employment status and family life, and communication with others are evaluated within the scope of personal data. There are four elements in the definitions of the concept of personal data are need to be analyzed which were "identified and identifiable", "real person", "relating", and "any kind of information" (EU, 1995; Purtova, 2018; KVKP, 2019).

Firstly, in the definition of the concept of personal data, the person must at least be identifiable. A person can be defined as identified when he or she distinguished from the other members of the community they live in (Fuster, 2014:2). Although the most common form of identification of a person is specifying his or her name and surname, this information may not always be required for the identity of a person to be specific. For example, it is possible to categorize individuals in socio-economic, psychological, or other contexts without the need for information such as name, surname or address, and attributed to the behaviors they act via the device to which they connect to the internet. Secondly, according to the definition in the law, the data must be related to the real person in order to evaluate it as personal data. Thirdly, the data should be about the person and related with his or her life (Long and Quek, 2002:331). Finally, any kind of information about the person which has mentioned features can be evaluated in the scope of personal data. The statement of "any kinds of information" in the law express the will of the lawmaker to keep the limits of the concept of personal data as wide as possible (KVKP, 2019).

The developments in science and technology and its reflection on the components of society and social life, especially in the last century, have included many types of information into personal data (Lee et al., 2019). For example, bank account numbers, social security numbers, id numbers, and passwords of the e-mail addresses can be shown as the new forms of personal data (Dülger, 2016:102). Thus, from a broader perspective, it is possible to separate personal data into two categories. Personal data that people have because of being human can be specified as the first category and data that is given to people as a result of the reforms which have come from information society can be specified as the second category. In order to understand this distinction, the historical background of the personal data and the need for protection of personal data should be known.

2. HISTORICAL BACKGROUND AND LEGAL STRUCTURE

The use of personal data has a historical background began with World War II. In World War II, Dutch local government, under German occupation, collected personal data files in order to identify individuals who were transported to concentration camps (Shaw, 2013). In the 1960s, it was widely argued that the collection of personal data by governments and private companies increased. The spread of computers and communication technologies during the 1970s had increased the collection and processing of

personal data. After the 1970s, governments and international organizations were forced to take measures.

The record, storage, and use of personal data are important for both state institutions and private sector organizations (Bainbridge, 1997: 17). Nowadays, transfer and storage of personal data is quite easy. Since the 1990s, with the widespread use of internet networks and the rapid development of mobile technologies, collecting, storing, sharing, and analyzing personal data have made it necessary to take some security measures (Kutlu and Kahraman, 2017:47). The increase in the number of devices used via the Internet and the increase in the number of recording devices have made it easy to record personal data, and thus the scale of data compiled has increased by the time. Personal data on the Internet is derived from written materials, audio recordings, visual files, videos, animations, presentations, and any kind of information shared on social media networks (Tavani, 1999). As a result of this wide-ranging sharing of personal data, many types of problems have come to sight. Because, personal data, which was previously filed in the hands of a small number of people or institutions, were transferred to the digital environment with the technological developments, and as a result of the widespread use of the Internet, have been made available to everyone by legal or illegal ways (Dülger, 2016:102).

The right of privacy and the right of personality, whether real or unrealized, should be protected against any attack. For this reason, legislators have strengthened the opportunities offered by private law in terms of protection before the attack in the face of possible attacks by new technologies. Since modern law order accepted the person as the highest value, legislators from all around the world have built the legal structure in order to protect the right of privacy and personality both nationally and internationally. Protection of personal data is directly related to privacy and protection of private life (Kılınç, 2012:1095).

The first data protection law was enacted by Germany in 1970 (Long and Quek, 2002:330). Then, during 1970s, many countries from all over the world began to enact data protection legislations. Germany was followed by Sweden in 1973, the USA in 1974, and France in 1978. Therefore, two prominent international regulations were also regulated in 1981. "Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data" was created by Council of Europe (COE) and "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" was created by the Organization for Economic Co-operation and Development (OECD). These international texts had a significant impact on the enactments of personal data protection laws around the world (Rudraswamy and Vance, 2001:128).

The privacy of private life is one of the most important human rights and has been subject to many international regulations. In this context, as the first internationally accepted legal text on the protection of personal data, the Convention on the Protection of Individuals against Automatic Processing of

Personal Data No. 108, prepared by the Council of Europe and signed by its members in 1981 and entered into force in 1985. However, before the Convention no. 108, there were some documents which mentioned the protection of personal data (Van Loenen et al., 2016). International organizations such as the United Nations, the Organization for Economic Development and Cooperation (OECD), the Council of Europe and the European Union (EU) have various arrangements for the protection of personal data (Regan, 2003:264). At very first, according to Article 12 of the Universal Declaration of Human Rights published in 1948: "Everyone has the right to the protection of the law against such interference or attacks." (UN, 1948). As a second example, according to Article 8 of the European Convention on Human Rights published in 1950: "Everyone has the right to respect for his private and family life, his home and his correspondence." (ECHR, 1950). As a last example, Turkish Constitution of 1982 mentioned protection of personal data in Article 8 as: "Everyone has the right to demand respect for his private and family life. Privacy of individual and family life may not be violated." (The Constitution of Turkey, 1982). As can be seen, the protection of personal data had generally been evaluated in terms of the privacy of private life in the texts before 1985.

The Convention on the Protection of Individuals against Automatic Processing of Personal Data No. 108 consists of 27 articles. The purpose of this Convention is to guarantee the rights of private life in the Member States in respect of the fundamental rights and freedoms of natural persons regardless of nationality or domicile and the automatic data information processing of personal data which is of particular interest to them (Kılınç, 2012:1113). The automatic processing is defined as the operation of all or part of the automated data recording, the application of biological or arithmetic operations to this data, the modification, removal, or dissemination of the data (COE, 1981). Convention covers personal data in both the public and private sectors. However, the contracting parties may, if they so wish, notify the other entities that benefit from the legal entity for applying the Convention on communities, associations, foundations, and corporations which directly or indirectly convene natural persons (Cate, 1994).

The other international document on the protection of personal data is the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted by the Organization for Economic Cooperation and Development (OECD) in 1981. These Guidelines "apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties" (OECD, 2013).

As another document, Guidelines for the Regulation of Computerized Personal Data Files was adopted by United Nations General Assembly in 1990. It has ten principles to provide guarantees for protection for personal

data which are principle of lawfulness and fairness, principle of accuracy, principle of the purpose-specification, principle of interested-person access, principle of non-discrimination, principle of power to make exceptions, principle of security, supervision and sanctions, transborder data flows, and field of application (UN, 1990).

As a last example of documents, the European Union, in 1995, adopted European Community Data Protection Directive 1995/46 on the protection of personal data which full name was "Direction on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data". This Directive seeks to take measures against any attack to personal data such as public or private violations and to provide systematic protection before violations (EU, 1995).

In Turkey, many studies have been carried out to create a legislation on the protection of personal data. Turkey signed European Council Convention No. 108 together with other Member States in 1981. However, Turkey was the only country that approved the convention but did not put into force until January 30 of 2016. Indeed, at first, a commission formed by the Ministry of Justice prepared a draft law on the Protection of Personal Data in 2003 (Dülger, 2016:107). The draft is generally based on the European Council Convention No. 108 and the European Community Data Protection Directive. Also, as second, with the Law No. 5982 Amending Certain Provisions of the Constitution, Article 20 of the Turkish Constitution was amended. With this amendment, a clause related with protection of personal data was added to Article 20 of the Constitution as (TBMM, 2010):

> All individuals have the right to request the protection of their personal data. This right includes being informed of, having access to and requesting the correction and deletion of their personal data and to be informed whether these are used in consistency with envisaged objectives. Personal data can be processed only in cases envisaged by law or by the individual's own consent. The principles and procedures regarding the protection of personal data are laid down in law.

The right to protection of personal data has reached a positive ground in the constitutional plane with the amendment in 2010. Then finally, as a result of the re-negotiation process of Turkey's accession to the European Union, which included the protection of personal data, the drafts were negotiated in the TGNA. The draft law submitted to the TGNA was adopted by the Assembly on 24.3.2016 with the number 6698 and was published in the Official Gazette dated 7.4.2016 and numbered 29677 and came into force (Official Gazette, 2016). Moreover, there are articles on protection of personal data in different laws like Turkish Civil Code, Turkish Penal Code, Criminal Procedure Code, Labor Law, and so through.

In Article 19 of the law no. 6698, it is stated that "Personal Data Protection Authority which has administrative and financial autonomy and public legal personality established in order to perform the duties stipulated

by this law" (KVKP, 2019). With this article, Personal Data Protection Authority was established. This study aims to analyze missions and visions of the authority and by analyzing the authority, tries to find the answers of the questions of why it is needed, how it protects personal data, and to what extent it is successful.

3. GENERAL PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA

The general principles for the processing of personal data were regulated in line with the Council of Europe Convention No. 108 and the principles on the quality of the data contained in the Directive (Oğuz, 2013:23). There is no generally accepted principles for the processing of personal data. However, when above mentioned international regulations examined, it can be found that there are six important principles for the processing of personal data.

First of all, personal data should be processed in accordance with the law and honesty since principles of law and honesty address the models of behaviors which everyone should demonstrate. As a requirement of honesty and lawfulness, the data processor should clearly and precisely determine the purpose of the data processing. That is, the data processor must inform the data owner before contacting the personal data about why they are collected, how they are collected, for what purposes and in what form they are collected (Purtova, 2018). As the second principle, it is necessary to verify that the relevant data is correct while personal data is processed. Incorrect data may be harmful for both the data processor and data owner, especially where the data is passed on to third parties (Oğuz, 2013:24). The third principle for the processing of personal data is being up-to-date. This principle is directly linked to the second principle. Because if a personal data is out of date or outdated, it cannot be mentioned that it is correct. Thus, an outdated personal data is likewise likely to expose the personal data owner to the risk of being harmed. Processing for specific, clear and legitimate purposes is the fourth principle. The use of the data collected in accordance with the law and the rules of honesty cannot be considered unlawful. In this respect, the purposes for which personal data will be processed should be clear and unambiguous (Fuster, 2014). As the fifth principle, personal data should be collected or processed within the boundaries set by its objectives with the general rule of proportionality. In connection with clearly defined objectives, it should be limited and measured (Van Loenen et al., 2016). As the sixth and the final principle, personal data should not be stored forever. They must be kept for the time required for the purpose for which they were collected or processed. Once its objective is achieved, the data must be made anonymous or deleted.

In general, as a rule, personal data cannot be processed without the consent of the person concerned. Unauthorized consent is unlawful. The consent of the person concerned is a reason for compliance with the law.

Consent is a unilateral legal transaction and as such the transaction must have validity requirements. However, consent of a person does not always indicate that it is legal to process data. Therefore, that's why an institution is needed for the protection of personal data.

4. PERSONAL DATA PROTECTION AUTHORITY

Turkish Personal Data Protection Law no. 6698 stipulates crimes and faults related to the processing of personal data, the operations of the data officer responsible for the establishment and management of the data recording system, and the rights of persons and the protection of personal data (Kağıtçıoğlu, 2016:78). In order to fulfill the duties assigned by this Law, the Personal Data Protection Authority was established by Article 19 of the law. There are some reasons of the establishment of this authority. Actually, these reasons are almost the same with the reasons of legal regulations for the protection of personal data. Moreover, the driving force in the establishment of the institution is international documents on the personal data protection. Because almost all of the documents stipulated the establishment of an authority that guarantees the protection of personal data.

In this study; the general framework, organizational structure, operational structure, actions, applications, and decisions of the KVKK are explained and analyzed respectively. The methodology of the study is "systematic review" (Kitchenham, 2004; Moher et al., 2009). That is, a systematic review is done on the Authority's legal and organizational structures, actions, applications, and decisions. Its decisions are analyzed by making comparisons with other personal data protection authorities from the world such as ICO from UK. Finally, recommendations on its operational development are done by doing a swot analysis.

4.1. General Framework and the Organizational Structure

The reasons for the establishment of the Authority emerged as the necessity of being a state that respects human rights (Kağıtçıoğlu, 2016:80). In Turkey, administrative bodies have experienced many problems in terms of the issue of protection of personal data in the applications of collecting health data, keeping archive records of public, fingerprint collection, keeping telephone records, doing security investigations, and so through. In order to eliminate these problems coming with the technological developments and to protect the personal data against them, personal data protection authority was established with the law no. 6698. As a matter of fact, in the lawsuits filed with the Council of State regarding the leakage of personal information prior to the establishment of the authority, it was stated that there is a need for an Authority which would fight against these problems (Akgül, 2013). On the other hand, as a requirement of the harmonization of the administrative bodies and legal structure of Turkey to the EU charter in the EU candidacy process, a supervisory authority in the context of the protection of personal data was needed.

The purpose of Personal Data Protection Law no. 6698 stated in Article 1 is to protect the fundamental rights and freedoms of persons, particularly the privacy of private life, and to regulate the procedures and principles to be followed by the obligations of natural and legal persons who process personal data. In order to fulfill this aim, Personal Data Protection Authority has been established as authorized and commissioned to fulfill this purpose. Administrative and financial autonomy has been emphasized by the legislator in its institutional structure in the law (Law No. 6698, 2016).

Within the scope of the protection of private life and the protection of basic rights and freedoms envisaged in the Constitution, mission of the Authority is stated as ensuring the protection of personal data and raising awareness on this issue. Also it has the mission of creating an environment that enhances the competitive capacity of private and public actors internationally. Accordingly, its vision is stated as to be an effective and internationally competent authority in the protection of personal data and the formation of citizenship awareness (KVKK, 2019). Then, in accordance with its mission and vision, it has the basic principles and values of protecting the privacy of private life, respect for fundamental rights and freedoms, impartiality, independence, reliability, compliance with law and ethical principles, transparency and accountability, accurate and objective decision making, cooperation and participation, and serving at national and international level as stated in the website of the Authority.

The duties of the Authority are stated in the law as (Law no. 6698, 2016):

- Following the practices and the developments in the legislation, giving evaluations and recommendations, carrying out researches and inspections or having them carried out in this regard, according to its scope of authority.
- Cooperating with public institutions and organizations, nongovernmental organizations, professional organizations or universities, when necessary, regarding the issues which fall within the scope of its authority.
- Following and evaluating the international developments concerning personal data, cooperating with international organizations on the matters which fall within the scope of its authority, attending the meetings.
- Presenting the annual activity report to the Presidency, the Committee on Human Rights Inquiry of the Grand National Assembly of Turkey and to the Prime Minister's Office.
- Performing the other duties assigned by laws.

In the 2001 meeting of the International Conference of Data Protection Commissioners (ICDPPC) on “Decision on the Principles of Accreditation of Data Protection Authorities”, it was foreseen that personal data protection authorities should have four basic principles as legal basis,

autonomy and independence, consistency with international documents, and appropriate functions. In short, Generally, in the resolution paper of the meeting, various standards have been introduced for data protection authorities such as the establishment of a public institution in the framework of a law, appointment of members for certain periods, dismissal of members under certain conditions such as neglect of duty, inadequacy, abuse of office, and direct reporting to legislation or government (ICDPPC, 2001). Personal Data Protection Authority of Turkey was established according to these basic principles in 2016 with the law no. 6698.

Personal Data Protection Authority of Turkey has a public legal entity and it is composed of two bodies defined by the law as the Personal Data Protection Board and the Personal Data Protection Presidency. Personal Data Protection Board is the decision making body of the Authority located in Ankara. On the other hand, The Presidency is responsible for the general management and representation of the Authority and has the duties and authorities to regulate, execute, audit, evaluate, and publicly announce the work of the Authority. In the law no. 6698, the duties and powers of the Authority, the Board, and the Presidency are separated from each other and the working areas of these three administrative units are determined in detail; accordingly, articles 19-20 are about the Authority, articles 21-23 are about the Board, and articles number 24-25 are about the Presidency.

According to the law, Personal Data Protection Board consist of nine members and five members are elected by the Grand National Assembly of Turkey, two by the President of the Republic, and two by the Council of Ministers. The President and the Vice-President are elected among the members by the Board. The President of the KVK Board is also the president of the Authority. The term of office of the Board members is four years and the member whose term has expired can be re-elected (Law no. 6698, 2016). As it is seen, the election procedure is included in the appointment of the members of the KVK Board and the election of the members is divided between the legislative and the executive and the members are elected for a certain period of time.

The Authority is responsible for ensuring that personal data is processed in accordance with the fundamental rights and freedoms, together with the decisions taken by the Board. Nowadays, technology has penetrated many social areas and personal data is processed by different people and institutions such as public administrations, banks, hospitals, payment institutions, social networks, and so through by collecting, recording, changing, correcting, explaining, merging, deleting personal information (KVKK, 2019). Hence, the fact that in some cases, even without the information and permissions of individuals, these data are processed, the protection of personal data and the effective enforcement of violations and the implementation of sanctions are increased the role of the State (Kağıtçıoğlu, 2016: 86). Within this framework, the Board implements the administrative sanctions and administrative measures provided for in the

Law while using its regulatory authority. Moreover, as in the duties and powers of the Board, the complaints of those who claim that their rights regarding personal data have been violated are also evaluated by the Authority.

4.2. Operational Structure

Elements of the operational structure of the Authority are defined in the Article 3 of the law no. 6698 as (2016):

- *Data subject*: Natural person whose personal data are processed
- *Data processor*: Natural or legal person who processes personal data based on the authority granted by and on behalf of the data controller
- *Filing system*: Any recording system through which personal data are processed by structuring according to specific criteria
- *Data controller*: Natural or legal person who determines the purposes and means of the processing of personal data, and who is responsible for establishment and management of the filing system
- *Explicit Consent*: Freely given specific and informed consent
- *Anonymization*: Rendering personal data by no means identified or identifiable with a natural person even by linking with other data

Before explaining the functioning of the Authority, the relationship between these elements is needed to be explained. At first, according to Article 10 of the Law, data controller has the obligation to inform the data subjects in terms of the purpose for which personal data will be processed, to whom and for what purpose personal data can be transferred, and the method and the legal reason for collecting personal data. Then, as stated in Article 12, data subjects have the rights to learn whether their personal data has been processed or not, to request information if their personal data is processed, to learn the purpose of processing personal data and whether they are used appropriately, to request correction of personal data in case of incomplete or incorrect processing, to object to the emergence of a result against the individual by analyzing the processed data exclusively through automated systems, to request their loss if it is damaged due to unlawful processing of personal data by applying data controller. Within this framework, data controller and data subject are the main actors of the process. In the functioning of the Authority, the other elements defined above are shaped according to the relationship between the two.

Personal Data Protection Authority functions in two different ways as on complaint and as in its own. The complaint way has also two different stages as “application to data controller” and “complaint to the board”. Application to data controller is the first stage and no complaint can be lodged without having to exhaust the way of application. In the stage of application, firstly, data subjects convey their requests regarding the implementation of the Law to the data controller. Secondly, data controller

finalized the application within 30 days at the latest according to the nature of the request, that is, if the transaction requires an additional cost, the fee determined by the Board may be charged. Finally, data controller accepts or rejects the request and notifies the person. In the stage of complaint, data subject may lodge a complaint within 30 days from the date when he or she learn the decision of data controller in cases of refusal of the application, inadequate response, or failure to respond to the application.

After application or complaint is approved, it is send to related department of the Authority in order for negotiating. There are seven departments under the body of the Authority as the departments of data management, inspection, legal affairs, human resources and support services, data security and information systems, strategy development, and guidance, research and corporate communications. These departments carry out their own tasks within the framework of a specific division of labor and make the applications available to be resolved by the Board (Regulation no. 6951, 2018).

According to Article 15 of the law no. 6698, Board also has the authority to review allegations of violation in its own, ex officio, if it learns them without any application or complaint (Law no. 6698, 2016). It means that the Board may initiate an inspection in the event of a violation in which it is notified. In other words, the Board does not need to be lodged in order to initiate an investigation. This allows the Board to prevent violations of rights, even if data subjects do not make a complaint or even do not know about the violation. Therefore, the rights of the data subjects can be protected more effectively. It is an important result of the Board being authorized to initiate reviews in its own is that it has the authority to evaluate the notifications received and to decide to initiate an investigation if necessary (KVKK, 2018a:34).

4.3. Actions and Applications

As a newly-established body, Personal Data Protection Authority of Turkey has done a lot of work in a short time. Since March 2016, a lot of events have been organized by the Authority to present and promote their works and applications. They organize "Wednesday Seminars" in every Wednesday on specific topics about the protection of personal data and problematic areas of applications. Moreover, they organized "Personal Data Protection Symposium" annually with the participation of academicians, lawyers, and public officials in order for discussing on the problems and solutions of the issues about personal data in Turkey. Besides, they held awareness conferences in universities and "KVKK Awareness Meetings" in different cities of Turkey. They held 18 awareness meetings in 2018 in different cities of Turkey with the participation of President of the Authority in order to inform people, organizations and public institutions about the Authority. At the meetings, attended by the Board members and executives, representatives of public institutions and organizations and private sector

were informed about the Personal Data Protection Authority. They also have announced all of their events via their official website as well as their decisions and actions.

The Authority published an annual report on its activities and applications in 2017. As a newly-established institution, general information about legal, organizational, and operational structure of the Authority and its departments shortly explained in the first chapters of the report. Then, its activities were reported supported by statistical data. According to the report, in 2017, a total of 59 applications were submitted to the institution, 48 of which were complaints and 11 of them were denunciations (KVKK, 2018a: 35). By the end of 2017, 31 from those 48 applications were completed by the Board. An administrative fine of 125.000 TL was imposed in 4 applications concluded by the Board it was given instructions to the data controller, in 3 applications, disciplinary investigations were carried out on the relevant public personnel within the framework of a violation made by the public institution in 2 applications, and the data controller's personal data processing activity was stopped in 1 application. On the other hand, it has been decided by the Board that there is no transaction to be made by the Authority within the scope of the Law regarding 3 applications. Other 9 of the applications were rejected on the grounds that they not included in the mandate of the Authority, and the remaining 9 were rejected by the Authority due to the failure to meet the procedural requirements in the Law (KVKK, 2018a:37).

As another action that was stated in the report, the Authority has been establishing a Data Controllers' Registry Information System (VERBIS). According to the Article 16 of the Law no. 6698, it is necessary to keep the Data Controllers' Registry, which is open to the public under the supervision of the Board. In this context, the procedures and principles of the obligation of registering, managing, and supervising the Data Controllers' Registry are regulated by the Regulation on the Registration of Data Controllers' published in the Official Gazette dated 30.12.2017. For this purpose, Data Controllers' Registry Information System (VERBIS) was established by the Authority for the fast and efficient registration of the registry processes, development of the established systems in accordance with the technological developments, carrying out the necessary information activities, providing the management by creating an institutional database, and presenting the data in the database to the use of the relevant units and public. VERBIS has designed as a system in which the data and responsibility of the data controllers who are obliged to register in the Registry can be entered into the technical and administrative measures they take in order to ensure the protection of the personal data.

4.4. Decisions

In order to make a review on the Authority, decisions taken by the Board are needed to be examined. Some of its decisions have been published

in the Authority's website after they're taken. In this context, firstly, some of the announced decisions will be examined in this part of the study, then, it will be analyzed that if mentioned decisions becomes influential or not.

As the first example, Decision dated 16.10.2018 and numbered 119 on "Preventing advertising notifications forwarded to data subjects' e-mail addresses or mobile phones via SMS or calls" can be examined. It is thought that this decision is a good example because it is a decision on a problem that is commonly encountered in society by many people. In this context, it is stated that a great number of applications submitted to the Authority in this issue. As a result, the Board stated in the decision that the data controller shall take all necessary technical and administrative measures to prevent the unlawful processing of personal data, to prevent unlawful access to personal data and to ensure the appropriate level of security in order to ensure the protection of personal data. Therefore, it was decided that data controllers who forwarded the advertising messages should immediately stop the data processing activities by sending SMS to the phone numbers, making calls or sending mails to e-mail addresses without obtaining the consents of the data subjects and ensuring the data processing conditions (KVKK, 2018b).

As the second example, Decision dated 21.12.2017 and numbered 61 "Personal Data Protection Board's Decision on the Protection of Personal Data on Websites and Applications Providing Guidance Services" can be examined due to the fact that it is related to an excessively encountered problem by many people in society. It is stated in the decision that as a result of the evaluations made within the scope of the notifications and complaints submitted to the Personal Data Protection Authority regarding the websites and applications that provide guidance services such as the phone number of the person whose name is written or the telephone number of the person whose name is written without taking the explicit consent of the him or her, it is found that there are many mobile applications and websites that share personal data on various websites or social media accounts, by collecting personal data, providing phone number information when the name is queried, providing name information when the phone number is queried, and providing how they are registered in the phone books of others. In this context, it was decided by the Board that the data processing activities carried out by these websites and mobile applications sharing the contact information of the data subjects without complying with the Law and the related legislation should be stopped immediately. In addition, it is also stated in the Decision that in case of acquiring information that the websites and mobile applications involved in such activities do not end their activities, the Authority is going to apply to the authorized institutions in order to prevent access to these websites and applications (KVKK, 2018c).

As the last example, Decision dated 26.07.2018 and numbered 91 "Personal Data Protection Board's Decision on the data controller who cannot fulfill the obligation to prevent unlawful access to personal data" can be examined as an example of a decision taken over an individual

application. It is stated that the application was made because of the fact that the personal data such as the delivery address, name, surname, address and telephone number of the person who made purchases via the website of a ready-to-wear clothing company were made accessible by the third parties who make purchases via this website of the company. In this context, it is stated that the data subject applied to Authority because of the unsatisfying response of the company on the demand from the company to delete personal data from the company's systems, to destroy them, and to make them inaccessible and to be deleted from the systems of other institutions shared in Turkey and abroad. In this context, the Board decided to impose administrative fines on the company as it was concluded that the necessary technical and administrative measures were not taken to ensure the appropriate level of security in order to protect personal data and prevent unlawful access to personal data prior to the above mentioned unjust treatment. In addition, regarding the request of the complainant, it was decided that the explanations of the transactions made by the parties need to be forwarded to the Complainant by the company within 30 days with the documents of the company regarding the deletion, destruction, and inaccessibility of all kinds of personal data of the complainant from the systems of the company and the other institutions shared in the country and abroad (KVKK, 2018d).

5. A REVIEW ON THE AUTHORITY

It can be seen from the examples that the applications to the Board include the important problems encountered by the majority of the society. Accordingly, it is thought that decisions and sanctions of the Board are also satisfactory for both applicants and society. Because, when the decisions analyzed in general, it is seen that the Board pays a great regard to data controller’s obligation on taking all necessary technical and administrative measures to prevent the unlawful processing of personal data based on the law and the regulations. However, the problems mentioned in the decisions are still frequently encountered problems in the society. Although laws and regulations on the protection of personal data foreseen and the Authority takes the monitoring actions on these unlawful activities, it is known that many online platforms still use, store and share personal data. It is thought that the most important reason that they can still continue their unlawful activities is that the people still do not know their rights on the protection of personal data and their right to apply to Personal Data Protection Authority when they faced a problem on the issue. This inference can be made by considering the number of applications made to the institution and the number of decisions that the Board made in a year.

When a small-scaled comparison is made between the Personal Data Protection Authority of Turkey and the other examples of personal data protection authorities from the World, it can be observed that the

organizational and operational structures and applications of Turkish authority are at a satisfactory level as a newly-established body. However, the Authority need some reforms in order to be more effective. In order for making a clearer comparison, the UK's independent authority on personal data protection, Information Commissioner's Office (ICO) is chosen as a good example for this study. When the activities of the ICO analyzed from its website, it is seen that there are several differences from the activities of the Authority Turkey.

ICO have carried out advisory visits, data protection audits, researches, monitoring activities and have been publishing overview reports, annual reports, policy views for parliamentarians and legislators, and research publishes. It is seen in the comparison that the ICO have more actions and applications than the KVKK. Especially, as it is seen as the most important difference, the ICO operates more on its own while the KVKK takes action more on complaints. For example, in its overview report on 16 universities in the UK between April 2017 and March 2018, it was made observations, follow up researches, physical visits, and telephone conferences by the ICO (2019). As a result of these actions, areas of good practice, areas of improvement, and areas of development were explained in detail and recommendations on these issues were given in-text. Moreover, the ICO have been doing monitoring activities which they monitor public authorities, and private organizations in order to make recommendations on their applications. Finally, it is seen from the comparison that there have been many more applications and complaints have been taken from the ICO when compared with the KVKK. Therefore, the ICO has a greater enforcement power. For example, the ICO has fined ride sharing company Uber £385,000 for failing to protect customers' personal information during a cyber-attack (ICO, 2018a) and has issued maximum £500,000 fine to Facebook for failing to protect users' personal information (ICO, 2018b).

Result

In today's conjuncture, almost all of the websites, social media platforms, mobile applications and online interactive platforms demand personal data for membership or usage for their services. In this situation, people who want to use these platforms need to share their personal information by approving an online contract that includes terms and conditions about the storage and share of their personal data. In the context of these contracts, those platforms easily take the permission for processing personal data. Thus, there is a great need for an authority to protect personal data from unlawful actions. The Personal Data Protection Authority of Turkey was established in the context of these need.

As a newly-established authority, the KVKK has made significant progress in a short time. However, a swot analysis should be made on the Authority in order to see its competitiveness by identifying its strengths,

weaknesses, opportunities and threats as a result of this study. Actually, the Authority's swot analysis was also briefly made in its annual report (KVKK, 2018a:64). Nevertheless, it seen from the report that there is a need for a comprehensive comparison to make a swot analysis.

The Personal Data Protection Authority has significant strengths in its field of work. These strengths can be explained as:

- Firstly, it is the one and only authority in Turkey that protects personal data from unlawful actions. Therefore, when people need to demand their right on personal data, there is only one authority they can apply to.
- Secondly, it can act independently based on the regulations in the law. That is, it is an independent body that people can trust.
- Thirdly, it has the power of administrative sanction and supervisory. These powers have brought a great strength to the Authority over public and private organizations.
- Fourth and finally, it is open to innovations and reforms as an Authority in the process of organizational structuring, so it has the possibility to detect its incomplete and insufficient aspects while go to structuring.

The Authority has also some weaknesses in addition to its strengths. It is thought that they also can be listed as:

- Firstly, it needs qualified human resource in the field of protection of personal data. Because, as a new field of study, there is not much people who interested in this issue.
- Secondly, the Authority does not have enough experience in the processes of investigation and decision. Therefore, it needs time and exercise for gaining experience as a newly-established body.
- Thirdly, it needs to improve its actions and applications by implementing new practices which can be observed from the examples of the other countries in the world. In this context, the Authority should firstly develop its operational structure by adding new practices to monitor. For example, as seen from the comparison with ICO, the Authority needs to do monitoring activities by its own without an application or complaint.
- Fourth and finally, the right to protection of personal data has recently been subject to a constitutional basis and a basic law in Turkey. In this context, the culture of protecting personal data needs to be improved and people are need to be informed about the law and the Authority.

The Authority has also some threads and, in return, opportunities as a newly-established body. These threads and opportunities can be explained as follows:

- As the first thread for the Authority, as mentioned earlier, there is a huge development in information and communication technologies which increase the flow of the personal data. Therefore, spread of the personal data is increasing day by day.
- As the second thread, the inaccessible flow of the information should be mentioned. That is, although there are legal regulations and sanctions on unlawful share of personal data, there are many anonymous platforms in the world of web which can easily store and share personal data. This situation makes the functioning of the Authority very hard.
- In return to the mentioned threads, depending on the developments in information and communication technologies, the need for an authority to protect personal data is also increasing day by day on the global bases.
- Finally, as the second opportunity for the Authority, it is thought that the international developments in the field of personal data protection should be mentioned. Because of the process of transition to the data- based economy, there is a process of international integration in the field. Therefore, the KVKK has the opportunity to reach other personal data protection authorities from the world and to work in coordination with them.

As a consequence of this study, it is thought that the KVKK is an important authority for Turkey in terms of the implementation of the envisaged practices in the legal regulations and also for the updating of the legal arrangements as a result of the gained experiences thanks to its practices. Thus, some recommendations have been prepared as a result of this study with respect to observations, researches, and comparisons done on the KVKK. At the very end, these recommendations are:

- It is firstly recommended in this study that the Personal Data Protection Authority of Turkey has to catch people's attention. The number of applications and complaints have not been in a satisfying level. In addition to symposiums and meetings held in different places, it should be more attention getting and active in online platforms. As of February 2019, the Authority's social media accounts do not have enough followers. For example, it has just 981 likes in Facebook, 4556 followers in Twitter, and 1010 followers in Instagram. The Authority should become more visible and catchy in social media.

- It is also recommended that the Authority should develop its capacity to act independently and capacity to act by its own without an application of violence. By taking from the good examples of the world, it should begin to make monitoring visits, to prepare follow up reports, and to make independent data protection audits. These actions may increase its capacity to protect.
- It is thirdly recommended that the Authority should open local offices, conduct projects in coordination with universities, and choose local representatives in order to propagate and extend its function.
- It is finally recommended in this study that the Authority should participate more in decision making processes by sharing their experiences and thoughts. In this context, involvement of lawyers, academicians, and public officials in the scope of the Authority becomes significant. Because, issues on how the Authority can become more efficient, active, and satisfying should be studied; then necessary reforms can be detected.

All in all, as a newly developing institution, there are important points that it should learn from data protection institutions of EU countries, which operate in accordance with GDPR. However, although it is a newly established institution, it also has some aspects that should be taken as an example by other countries, especially in the context of "awareness meetings", "Wednesday seminars", and academic publications. It is an example in terms of its establishment process, structure, and activities for countries where data protection has not yet been institutionalized. Under today's conditions, where the protection of personal data is very difficult, it is clear that it will become a more functional body with an increased capacity and expanded powers.

References

Akgül, A. (2013). Danıştay Kararları Işığında Kişisel Sağlık Verilerinin Korunması, *Danıştay Dergisi*, 133, 21-50.

Akgül, A. (2015). Kişisel Verilerin Korunmasında Yeni Bir Hak: 'Unutulma Hakkı ve AB Adalet Divanı'nın 'Google Kararı', *TBB Dergisi*, 116, 11-38.

Bainbridge, D. I. (1997). "Processing Personal Data and The Data Protection Directive", *Journal of Information & Communications Technology Law*, 6(1), 17-40.

Cate, F. H. (1994). The EU data protection directive, information privacy, and the public interest. Iowa L. Rev., 80(3), 431-443.

Caudill, E. M., & Murphy, P. E. (2000). Consumer online privacy: Legal and ethical issues. Journal of Public Policy & Marketing, 19(1), 7–19.

CoE (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Retrieved from https://rm.coe.int/1680078b37 (February 10, 2019)

Chua, H.N., et al. (2017). Unveiling the coverage patterns of newspapers on the personal data protection act, Government Information Quarterly, 34(2), 296-306, DOI: 10.1016/j.giq.2017.02.006

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. International Journal of Electronic Commerce, 10(2), 7–29.

Dülger, M. (2016). Kişisel Verilerin Korunması Kanunu Ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması, *Istanbul Medipol University School of Law Journal*, 3(2), 101-167. Available at: https://ssrn.com/abstract=2942230 (February 10, 2019).

ECHR (1950). European Convention on Human Rights, Retrieved from https://www.echr.coe.int/Documents/Convention_ENG.pdf (February 9, 2019)

EU (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046 (February 11, 2019)

Fuster, G. G. (2014). The emergence of personal data protection as a fundamental right of the EU, Springer Science & Business.

ICDPPC (2001). Accreditation Features of Data Protection Authorities, *23rd International Conference of Data Protection Commissioners*, 25 September 2001, Paris, Retrieved from https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Accreditation-Features-of-Data-Protection-Authorities.pdf (February 14, 2019)

ICO (2018a). ICO fines Uber £385,000 over data protection failings, Retrieved from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-fines-uber-385-000-over-data-protection-failings/ (February 19, 2019)

ICO (2018b). ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information, Retrieved from https://ico.org.uk/about-the-ico/news-and-events/news-and-

blogs/2018/10/facebook-issued-with-maximum-500-000-fine/ (February 19, 2019)

ICO (2019). Findings from ICO information risk reviews of information security in the higher education sector, Retrieved from https://ico.org.uk/media/2614196/20190124-information-risk-review-report-higher-education-sectorpdf.pdf (February 19, 2019)

Kağıtcıoğlu, M. (2016). Kişisel Verileri Koruma Kurumu'na İdare Hukuku Çerçevesinden Bir Bakış, *Aurum Sosyal Bilimler Dergisi*, 1(2), 77-99. Retrieved from http://dergipark.gov.tr/aurum/issue/27138/289543 (February 12, 2019)

Kılınç, D. (2012). Anayasal Bir Hak Olarak Kişisel Verilerin Korunması, *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 61(3), 1089-1169.

Kitchenham, B. (2004). Procedures for performing systematic reviews. Keele, UK, Keele University, (33), 1-26.

KVKK (2018a). Kişisel Verileri Koruma Kurumu 2017 Yılı Faaliyet Raporu, Retrieved from https://www.kisiselverilerinkorunmasi.org/wp-content/uploads/2017/09/2017-Faaliyet-Raporu.pdf (February 17, 2019)

KVKK (2018b). Kişisel Verileri Koruma Kurulunun 16/10/2018 Tarihli ve 2018/119 Sayılı İlke Kararı, Retrieved from https://kvkk.gov.tr/Icerik/5299/2018-119 (February 17, 2019)

KVKK (2018c). Rehberlik Hizmeti Veren İnternet Sitelerinde/Uygulamalarda Kişisel Verilerin Korunmasına Yönelik Kişisel Verileri Koruma Kurulunun 21/12/2017 Tarihli ve 2017/61 Sayılı İlke Kararı, Retrieved from https://kvkk.gov.tr/Icerik/4113/2017-61 (February 17, 2019)

KVKK (2018d). Kişisel verilere hukuka aykırı erişilmesini önleme yükümlülüğünü yerine getiremeyen veri sorumlusu hakkında Kişisel Verileri Koruma Kurulunun 26/07/2018 Tarihli ve 2018/91 Sayılı Kararı, Retrieved from https://kvkk.gov.tr/Icerik/5365/2018-91 (February 17, 2019)

KVKK (2019). Misyon ve Vizyon, Retrieved from https://www.kvkk.gov.tr/Icerik/2074/Misyon---Vizyon (February 16, 2019)

KVKP (2019). Turkish Personal Data Protection Law no. 6698, Retrieved from https://www.kisiselverilerinkorunmasi.org/kanunu-ingilizce-ceviri/ (February 9, 2019)

KVKP (2019). Kişisel Veri, Retrieved from https://www.kisiselverilerinkorunmasi.org/kisisel-veri-nedir-ne-demektir/ (February 8, 2019)

Kutlu, Ö., & Kahraman, S. (2017). Türkiye'de kişisel verilerin korunması politikasının analizi. *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi*, 5(4), 45-62.

Lee, H., Wong, S. F., Oh, J., & Chang, Y. (2019). Information privacy concerns and demographic characteristics: Data from a Korean media panel survey. Government Information Quarterly, 36(2), 294-303, DOI: 10.1016/j.giq.2019.01.002

Long, W. J., & Quek, M. P. (2002). Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise. Journal of European Public Policy, 9(3), 325-344.

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. Annals of internal medicine, 151(4), 264-269.

OECD (2013). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Retrieved from http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (February 14, 2019).

Oğuz, H. (2013). Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları Ve Ülkemizdeki Durum. Uyuşmazlık Mahkemesi Dergisi, (3), 1-38.

Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. Law, Innovation and Technology, 10(1), 40-81.

Regan, P. M. (2003). Safe harbors or free frontiers? Privacy and transborder data flows. Journal of Social Issues, 59(2), 263-282.

Regulation no. 6951 (2018). Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği, http://www.mevzuat.gov.tr/MevzuatMetin/3.5.201811296.pdf (February 15, 2019)

Resmi Gazete (2016). 7 Nisan 2016 Tarihli ve 29677 Sayılı Resmî Gazete, Retrieved from http://www.resmigazete.gov.tr/eskiler/2016/04/20160407.htm (February 11, 2019)

Resmi Gazete (2017). 30 Aralık 2017 Tarihli ve 30286 Sayılı Resmî Gazete, Retrieved from http://www.resmigazete.gov.tr/eskiler/2017/12/20171230.htm (February 11, 2019)

Rudraswamy, V., & Vance, D. A. (2001). Transborder data flows: adoption and diffusion of protective legislation in the global electronic commerce environment. Logistics Information Management, 14(1/2), 127-137.

Shaw T. J. (2013). World War II Law and Lawyers: Issues, Cases, and Characters. American Bar Association Press.

Tavani, H. T. (1999). Informational privacy, data mining, and the internet. Ethics and Information Technology, 1(2), 137-145.

TBMM (2010). Türkiye Cumhuriyeti Anayasasinin Bazi Maddelerinde Değişiklik Yapilmasi Hakkinda Kanun No. 5982, Retrieved from https://www.tbmm.gov.tr/kanunlar/k5982.html (February 10, 2019)

The Constitution of Turkey, (1982). The Constitution of The Republic of Turkey, Available at: http://www.anayasa.gen.tr/1982Constitution-1995-1.pdf (February 11, 2019)

UN (1948). The Universal Declaration of Human Rights, Available at: http://www.un.org/en/universal-declaration-human-rights/ (February 10, 2019)

UN (1990). Guidelines for the Regulation of Computerized Personal Data Files, Retrieved from https://www.refworld.org/pdfid/3ddcafaac.pdf (February 11, 2019)

Van Loenen, B., Kulk, S., & Ploegar, H. (2016). Data protection legislation: A very hungry caterpillar, Government Information Quarterly, 33(2), 338-345, DOI: 10.1016/j.giq.2016.04.002

Wu, Y. (2014). Protecting personal data in E-government: A cross-country study. Government Information Quarterly, 31(1), 150–159. DOI: 10.1016/j.giq.2013.07.003