SELÇUK ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ

S.Ü. Müh. Bilim ve Tekn. Derg., c.6, Özel Sayı, ss. 798-809, 2018
Selcuk Univ. J. Eng. Sci. Tech., v.6, Special Issue, pp. 798-809, 2018
ISSN: 2147-9364 (Electronic)
DOI: 10.15317/Scitech.2018.169
EURASIAN GIS CONGRESS 2018

PROTECTION OF PERSONAL DATA: EXAMPLE OF GEOGRAPHIC INFORMATION SYSTEMS

[1]Sevil YILDIZ

[1] *Selcuk University, Communication Faculty, Department of Radio, Television and Cinema, 42075 Konya, Turkey*
[1] syildiz@selcuk.edu.tr

(Geliş/Received: 08.11.2018.; Kabul/Accepted in Revised Form: 06.12.2018)

ABSTRACT: Right of protection of personal data is among the fundamental human rights and freedoms and it bears significant importance legal state principle and democracy to gain depth. Protection of personal data has gained great importance in the last forty years time. An important factor relating with this is that privacy area of private lives of people has become more defenceless as information and communication technologies developed and capacities to collect data and to process them automatically increased. Depending on technological and democratic development levels, countries have began to take important steps to establish legal arrangements and institutional structures with the aim to protect personal data starting from 1970s onward. In Turkey with the provision which is added to the Constitution in 2010, the necessary legal basis relating with protection of personal data has been established. In 2016, the law about the protection of personal data has been accepted and the legal arrangement deficiency in this area has been eliminated. In our study, the provisions of law relating with the protection of personal data will be investigated and afterwards measures which are required to be taken for the protection of existing personal data will be examined in the Geographic Information System, being a database processing system with private computer support which is used with the aim to collect, preserve, process, analyze, and display geographical data, within the context of international law and national regulations.

Key Words: *Data, Geographic information systems, Protection of personal data*

Kişisel Verilerin Korunması: Coğrafi Bilgi Sistemleri Örneği

ÖZ: Kişisel verilerin korunması hakkı, temel insan hak ve özgürlükleri arasında yer almakta olup, insanın şahsiyetinin korunması, hukuk devleti ilkesi ve demokrasinin derinlik kazanması acısından hayati öneme sahiptir. Kişisel verilerin korunması hakkı son kırk yılda büyük önem kazanmıştır. Bunda, bilgi ve iletişim teknolojilerinin gelişmesiyle birlikte veri toplama ve bunları otomatik olarak işleme kapasitelerindeki artış ile bu artışa dayalı olarak kişilerin özel hayat mahremiyet alanının daha savunmasız hale gelmesi önemli bir etkendir. Teknolojik ve demokratik gelişmişlik seviyelerine bağlı olarak ülkeler, 1970'lerden itibaren kişisel verilerin korunmasına yönelik kanuni düzenleme ve kurumsal yapıları oluşturma yönünde önemli adımlar atmaya başlamışlardır. Türkiye'de 2010 yılında Anayasa'ya eklenen hüküm ile kişisel verilerin korunmasına ilişkin gerekli hukuki temel oluşturulmuştur. 2016 tarihinde ise, Kişisel Verilerin Korunması Hakkında Kanun kabul edilmiş ve bu alandaki hukuki düzenleme eksiği giderilmiştir. Bu çalışmamızda kişisel verilerin korunmasına ilişkin Kanunun hükümleri incelenecek ve sonrasında coğrafi verileri toplamak, saklamak, işlemek, analiz etmek ve görüntülemek amacıyla kullanılan özel bilgisayar destekli veritabanı işletme sistemi olan Coğrafi Bilgi Sisteminde mevcut kişisel verilerin korunmasına yönelik alınması gereken önlemler, uluslararası hukuk ve ulusal düzenlemeler kapsamında irdelenecektir.

Anahtar Kelimeler: *Veri, Coğrafi bilgi sistemleri, Kişisel verilerin korunması*

INTRODUCTION

Data is the series of facts which gain meaning when they are correlated with similar ones (Ayözger, 2016: 40). Information is composed of data which are classified and interpreted, meaning that they are conceptually processed (Ayözger, 2016: 43). Data can transform into information only when they are correlated with a special problem. In order to reach to information, it is required to select, integrate, and interpret appropriate data within a specific data cluster.

Diversification of data sources and increasing the volume of data being established necessitates classification of data in order for legal frame to be established and for the arrangements to be made. Data originating from different sources can be qualified as personal or impersonal data depending on the quality of data. Examples of personal data are given below (Kılınç, 2012: 1099):

- Blogs, interpretations, photos, and videos being created by people,
- Information about internet activity of a person, researches he has made,
- Data in social platform, friends and environment of a person,
- Location information of a person,
- Demographic information of a person,
- Financial data, account details, health records, security records which bear official quality and which can be used to define a person.

As a result of unavoidable increase in the usage of computers, giving their name to the epoch, collection, storage, and sharing of information being named as personal data, has reached to significant levels. A government or private company and even a private person can learn about shopping habits of a person by collecting and comparing personal data and for example by following up his credit card expenses, and they can learn about their areas of interest by using the cookies left during their usage of internet and by means of the information in their mobile phones, they can easily learn about who their relatives are. Information given by an internet user only to get an e-mail address or to use internet banking or to do shopping in internet and information given by a person to become a member of a sports hall, to participate in a lottery, to get credit from a bank and to realize various other processes in daily life without requiring to use internet, are all personal data (Develioğlu, 2017: 59).

There are three basic methods of gathering personal data(Ayözger,2016: 57):

* Person/institution about whom data is requested to be gathered, may give them voluntarily,
* Personal data can be legally followed up and gathered,
* New data sets can be established by processing personal data. The process that takes place from the stage of gathering data to their being used, can be possible by a value chain of four stages being composed of collection, storage, analysis, and usage.

As a result of advancing technologies, the opinion came out that individuals can not freely develop their personalities and participate in democratic life against data processing activities of public organs, unless there are legal arrangements. It can be stated that there are basically three factors in the coming out of law of protection of personal data (Develioğlu, 2017: 66):

- The requirement of various organizations for personal data;
- Technological advancements;
- Worry felt due to the developments lived through in inspection technologies.

Various information such as names, birth dates, genders, professions of people, which define people and which differentiate them from others, are being kept recorded by public authorities for different purposes for a long time. As informatics technologies began to develop in 1970s and as private people

and institutions also began to record these data, besides public authorities, and as it became easier to store these data and especially to transmit them to others, the need to protect personal data emerged.

The law which was accepted in 1970 in Hessen Federated State in Germany has been the first arrangement being accepted in this area in the world. Laws relating with protection of personal data have been accepted in 1973 in Sweden, in 1976 in Germany, and in 1978 in France (Cengiz, 2016: 188).

With said arrangements, states try to keep control of the situation where especially the data of their citizens are taken out of their borders and circulate in international ground and they only permit for data to be transmitted to countries which provide sufficient legal security. Certain institutions which consider that these legal arrangements would limit data flows beyond borders and that they would limit international trade in return, try to determine minimum level of protection required to be provided by states, with the regulations they make since 1980s (Johnson, 2007: 113).

First example of international studies relating with law of protection of personal data is OECD Principles. Purpose of Principles of Guideline relating with Protection of personal area and flow of personal data beyond borders is to enable free circulation of data in free market economy and to regulate protection of interests of data owners. Said principles are presented as recommendations and they don't bear any binding effect (Johnson, 2007: 118).

In 1981 European Council of Ministers Committee has opened Contract of European Council About protection of individuals with regards to automatic processing of personal data, for signature. This contract evaluates the right of protection of personal data within the context of principle of protection of private lives as being stated in 8th article of European Human Rights Agreement and it provides detailed regulations. Turkey has approved this contract on the date of 30.01.2016 (Kılınç, 2012: 1128).

The most effective regulation regarding the protection of personal data is European Parliament and European Council Directive with no 95/46/EC regarding the protection of individuals with respect to free circulation of personal data, which was put in effect on the date of 24.10.1995. In the month of November in 2010, although fundamental principles of EU Directive remained valid, European Union has decided for European Union to conduct studies relating with the protection of personal data against rapid technological developments and globalization. As a result of these studies, on 4th of May, 2016 EU General Data Protection Code has been published (15). This code will become effective on the date of 25th of May, 2018 and on this date, application of EU Directive with no 95/46/EC will be ended (Develioğlu, 2017: 129).

The code primarily increases the liabilities of data responsibles and data processors. Obligation to keep record of processes being realized, providing details of liability for taking measures relating with data security, foreseeing preliminary inspection mechanisms regarding the processing of personal data, requiring for the assignment of information security official are the important developments (Atak, 2010: 101).

Right of protection of personal data was first specified in the Constitution in year 2010. "Law About making amendments in certain articles of Constitution of Turkish Republic" with no.5982 has been published on official gazette dated 13th of May, 2010 with no 27580 with the aim to present it to public opinion as per fourth paraphrase of 175th article of the Constitution and it was accepted with the majority of votes as a result of public opinion on the date of 12th of September, 2010 (Ayözger, 2016: 68). The following paraphrase has been added to 2nd article of this law with no. 5982 and to 20th article of Constitution of Turkish Republic: "Everyone has the right to request protection of personal data relating with himself. This right also includes notification of a person about his personal data, his having access to these data, requesting for them to be corrected or erased, and to learn whether they are used in line with the purposes or not. Personal data can only be processed in cases which are foreseen by the law or as per explicit consent of the person. Rules and principles relating with protection of personal data are regulated by the law." Afterwards on the date of 24.03.2016, Law for the protection of personal data has been accepted. Nowadays, national arrangement of law of protection for personal data is this law. However, the law which is accepted with the aim to follow up the developments in the area of law of

protection for personal data, assumes Directive with no 95/46/EC as basis and it does not contain the renewals brought up by EU General Data Protection Code (Korkmaz, 2016: 89; Çayır, 2016: 12).

The purpose of this law is defined as: "Protection of fundamental rights and freedoms of people with regards to the processing of personal data and regulation of rules and principles which legal entities processing personal data shall comply with". This law is the application law of the right of protection of personal data which is stated in 20th article of the Constitution (Ayözger, 216: 188; Korkmaz, 2016: 69). Therefore, disciplining the processing of personal data and protection of fundamental rights and freedoms are among the basic purposes of the law.

It is a known fact that personal data are collected by many institutions for various reasons. The law with no.6698 was prepared with the reasoning that these data shall be gathered at a certain center in a controlled way and that it shall be avoided for them to be misuse them. Accordingly, in the law the rules and principles which are required to be complied with and which are related with protection of personal data which are obtained by public or private institutions or by real people from people getting services or not, either by getting their consent or by force, are specified (Develioğlu, 2017: 121).

CONCEPT of PERSONAL DATA

In many national and international texts, personal data is defined as: "All kinds of information relating with a specific person or a person who can be determined". Starting from this opinion on, in order for an information to be considered as personal data, first of all it is required for it to belong to a real person and it is necessary for the identity of person to be defined with these data.

Personal data also covers information about a person's financial, professional, and communal life as not being limited with his private life. For example data such as a person's name, address, photo, education details, institution registry and tax numbers, phone messages, social sharing messages sent through Twitter/Facebook/Whatsapp etc., aural and visual records, finger prints, e-mail address, biometrical and medical information which we can see in each area of our lives are considered within the context of personal data. In this respect we can state that personal data are "Data which reveal the identity of an individual, which determine a person and which characterize him" (Ayözger, 2016: 51).

Part of personal data are separated from the others as private personal data. According to 6th article of law with no.6698, "Data relating with people's race, ethnic root, political opinion, philosophical beliefs, religion, sectarian, other beliefs, dressing, memberships in associations, unions and foundations, health, sexual life, criminal sentences, and security measures, and their biometrical and genetic data" are considered as private personal data (Develioğlu, 2017: 203).

Processing of Personal Data

Processing of personal data is defined as "All kinds of processes such as obtaining, recording, storing, keeping, changing, modifying, explaining, transferring, receiving, providing, classification, and avoiding the usage of personal data either partially or completely through partially automated paths or through ways which are part of a data recording system but which are not automated" (Ayözger, 2016: 44).

All kinds of processes starting from obtaining personal data for the first time as including all processes which are realized on the data are considered as processing of data. Apart from this, it is possible to state that processes realized for combining personal data, correlating them with other data, erasing them or other processes being realized for such purposes are within the context of definition of processing the personal data (Kılınç, 2012:1099; Korkmaz,2016: 109).

With regards to processing activity, it is required for the rules and principles in law to be foreseen. Compliance of processes being realized with respect to personal data with the human honor and values is a particular that should be paid attention to. Besides, general principles that should be complied with in the processing of personal data are being in conformity with law and rules of honesty, being correct

and updated when required, processing for specific, clear and legitimate purposes and to be related with the purpose of processing (Korkmaz, 2016: 110).

Processing of personal data has been connected with certain conditions. First of all the general rule for the process of processing is obtaining the explicit consent of relevant person. The concept of explicit consent has been defined in law as: "Consent which is based on notification and which is explained with free will". There are no provisions relating with the form of explicit consent. As it can be understood from the definition in law, it is possible for the consent to be given in any oral or written way.

With respect to the processing of data, there are certain cases when it is not needed for the consent of data owner to be taken. These situations have been specified in 5th article of law with no. 6698. Such that, these are as stated below (Ayözger, 2016:48; Develioğlu, 2016: 193):

* There is explicit provision i the laws regarding the processing of data,
* It is not possible for the relevant person to declare his consent or the person, to whose consent legal validity is not provided, is obliged for the protection of life or physical integrity of someone else,
* It is required for personal data to be processed on condition that it is directly related with the establishment or execution of a contract,
* It is required for the data responsible to execute his duties,
* It is required for establishing, using or reserving a certain right,
* It is required for the data to be processed with respect to legitimate interests of data responsible on condition that it does not damage the fundamental rights and freedoms of relevant person.

In 28th article of law relating with processing of personal data, a general provision for exceptions has been specified. Such that, in below cases, provisions of law shall not be applied (Ayözger, 2016: 48; Develioğlu, 2017: 194):

a) Processing of personal data by real people within the context of activities relating with themselves or with their family members they are living with in the same residence on condition that they are not given to third parties and that provisions relating with data security are complied with,

b)Processing of data for purposes such as making research, planning and statistics by making them become anonymous with official statistics,

c) Processing of personal data for purposes relating with art, history, literature, or science or within context of freedom of expression on condition not to violate national defense, national security, public order, economic safety, privacy of private life or personal rights or not to constitute any crimes,

d) Processing of personal data within the context of preventive, protective, and informative activities with the aim to provide national defense, national security, public order, or economic safety,

e) Processing of personal data by judicial authorities or execution authorities as relating with investigation, prosecution, judgment, or execution processes.

Erasing, Destroying Personal Data and Making Them Become Anonymous

In the 7th article of Law for the protection of personal data, erasure of personal data, their being destroyed or their being made anonymous have been regulated. Accordingly if the reasons requiring for the processing of personal data which are processed as complying with the law, are eliminated, these personal data will be erased, destroyed or made anonymous with the request of relevant person or as ex officio by the data processor.

As it is specified in the reasoning erasure of personal data means erasure of data from recording environments such as document, file, CD, disk or hard disk in a way that it can not be used or obtained again.

Destroying the data means destroying recording materials such as document, CD, disk, hard disk on which data are recorded in a way that they can not be used and obtained again (Develioğlu, 2017: 209).

Making data become anonymous means making it impossible for them to be correlated with a real person, the identity of whom is specific or which can be determined, even if personal data are matched with other data. As with anonymous data, by disconnecting the bond between the individual whose identity can be determined as a result of the processes being done and the data, it can not be possible to reach to the person by means of data. For this reason anonymous data are not personal data (Millard and Hon, 2012: 66). But since at the beginning of process of making anonymous, the situation of personal data's being determined does not vanish and this process is protected within the context of European Union Directive with no 95/46/AT. According to European Council Contract with no 108, if relevant people have processed data as violating the provisions of Contract, they have the right to request for these data to be erased or if their request is rejected, they have the right to apply for legal remedies (Başalp, 2015: 88).

At the end of process of making personal data become anonymous, it is required for it to be impossible to determine the person to whom data belongs to by realizing follow up as per the data and by matching with other data or by enabling support. Another issue that needs to be investigated with respect to a data's making a person identifiable or not is related with data in which nick names are used, encrypted data and anonymous data. Data in which nick names are used are those data which are formed especially when more than one data needs to be collected as relating with more than one person for statistical purposes and as the names of these people are changed with other names to avoid these people from being identified. In encrypted data, a code number is written in place of names of people and this code number is stored in a separate place (Korkmaz, 2016: 128). As it can be possible for a person to learn about the identity of a person as he gets access to these code numbers by using them or as he learns nick names by using these nick names, data with nick names and encrypted data are under the protection of data protection laws. Data with nick names have not been defined in Law of protection of personal data. In anonymous data as a result of processes being conducted by disconnecting the bond between a person whose identity can be determined and data, it is made impossible for the identity of individual to be determined and it becomes impossible to reach to people who own these data. For this reason anonymous data are not personal data(Cengiz,2016: 97).

In the reasoning of law it is stated that starting from the stage of obtaining data for the first time all the processes being realized are deemed as processing of personal data. Accordingly transfer of personal data being arranged in 8th and 9th articles of law are within this context. Transfer of data has been divided to two sections which are domestic and foreign transferring. This differentiation bears meaning with respect to conditions required for said processes. Hence different rules and principles have been determined especially for transfers which are made to abroad (Çayır, 2016: 6).

Transfer of personal data to other people within domestic country is subject to the rules foreseen for processing of data. In that respect for the transfer process first of all consent of relevant person should be taken. For the transfers which are made to abroad, besides these conditions it is specified that it is required for adequate protection to be established in the relevant foreign country. Countries having adequate level of protection will be determined and announced by the council (Başalp, 2015: 92). If the country to which data transfer will be made does not provide adequate level of protection, it is required for data processors of both countries to undertake this protection as written and to get permission from the council.

Data Responsible and His Liabilities

Data responsible is defined in the 3rd article of law as "Real or legal person who determines tools and purposes of data processing and who is responsible from the establishment and management of data recording system. This person is responsible from all kinds of processes which are realized as relating with the data. 16th article of law has arranged "Registry of data responsibles" in which people being responsible from data will be recorded. Before starting with data processing, it is absolutely required to make recording at this registry.

10th article of law of protection of personal data arranges the liability of data responsible to clarify the relevant person as being stated in the reasoning and being parallel to European Union Directive with no 95/46/AT. According to the law, data responsible or the person authorized by him will inform the relevant person within the context of his liability to clarify the person about his other rights being stated in 11th article with respect to identity of data responsible and his representative, if any, purpose of data processing, people to whom data can be transferred and the relevant reasons, method of data collection and legal reasoning (Başalp, 2015: 93; Atak, 2010: 521).

Data owners who can provide evidence about their identity with relevant documents have the right to request being notified whether data relating to him have been processed or not, for the data to be given back to him in a reasonable way without any unnecessary delays and costs, to request for appropriate corrections and erasures if these data have been recorded in a illegal, unnecessary and wrong way and to be notified if they are transferred to third parties (Atak, 2010: 529).

Notification of the relevant person about the processing of his personal data is important from two respects which are usage of an individual's personal data in an effective way and ensuring transparency of administration.

Furthermore, notification of relevant person is also related with the rule of honesty. For these reasons notification of an individual about the processing of his personal data has an important place in the protection of personal data.

Liabilities of data responsible with regards to the protection of personal data are arranged in 12th article of Law about the protection of personal data. According to this article, data responsible is obliged to take all kinds of technical and administrative measures in order to avoid illegal processing of personal data and having illegal access to the data and to maintain appropriate level of security for storing the data.

In the second paraphrase of the article is is stated that if personal data are processed in his name by other real or legal people, data responsible shall be liable from taking the measures which are stated in the first paraphrase of this article jointly with these people (Korkmaz, 2016: 107).

In the third paraphrase of the article it is stated that data responsible is obliged to make necessary inspections or cause them to be made with the aim to ensure application of provisions of law about the protection of personal data in his own institution or association.

Fourth paraphrase arranges liability of data responsible and data processes to keep secrets and accordingly, data responsibles and data processors can not disclose personal data which they have learned to others by violating the law and they can not use them for their personal benefits. This liability shall continue even if data responsibles and data processors resign from their jobs. In the fifth paraphrase of 12th article of the law it is specified that if the processed data are obtained illegally by others, data responsible will notify the relevant person and the institution at the soonest time. If required, institution will announce this situation from their internet site or by other ways they deem appropriate (Kılınç, 2012: 1128).

In data security, it was aimed to directly secure data and not people. If people relating with data are being protected with the measures that are taken to provide data security, data protection will be provided as well. For this reason in many legal arrangements relating with the protection of personal data, data security has been among the fundamental principles.

Data security and protection of personal data are not particulars having same meaning. Data security which mainly considers technical particulars as basis considers compliance with certain standards as basis. However, data security serves for the protection of personal data. Thus, data security and protection of personal data come in front of us as two integral particulars (Develioğlu,2017: 268).

Technical and administrative measures can be understood as all the measures to be taken by data responsible to fulfill his liabilities. These measures can be related with the infrastructure, organization, personal, software or transmission methods of data responsible. This type of measures can come out as taking necessary measures against cyber attacks, notifying the employees, being continuously subject to

training, avoiding unauthorized access with current and variable ciphers, conducting necessary inspections, and defining inter-company data usage policies (Develioğlu, 2017: 268).

In order for data security to be provided and continued in a sustainable way, it is required for data responsible to establish a data management system as per the quality and scope of data being processed (Millard and Hon, 2012: 69).

Law About the Protection of Personal Data

In the 19th article of law with no.6698, it is arranged that a new and autonomous institution being responsible from the application of law will be established. Name of this institution which has newly become part of the state organization is Institution for the Protection of Personal Data. Decision organ of institution being composed of council and presidencies is the Council of Protection of Personal Data.

Tasks of the institution are to follow up implementations and legal developments in national and international ground, to realize research and investigations regarding this subject, to collaborate with relevant institutions and associations, and to make proposals in the areas needed. Organization structure and manner of work of this institution having public legal entity bear similarity to the features of other autonomous institutions. Independence of council, being the decision organ of institution bears significant importance. In the law it is stated that the council will fulfill their tasks and authorizations given to them in an independent way under the responsibility given to them. Regarding these issues, it is absolutely forbidden for the council to take orders and instructions from any authorities, organs, or people (Develioğlu, 2017, 271).

EVALUATION of GEOGRAPHİCAL INFORMATION SYSTEMS with RESPECT to the PROTECTION of PERSONAL DATA

Basic reason for establishment of Geographical Information Systems is the requirement for planning. If it is required to evaluated very different data in planning, showing very different data on a single map can be very difficult and even impossible. Because many of the data overlap with each other. Obtaining the information being required for planning from these data that are stored as different layers in computer environment can be possible by screening them, querying those requested and bu analyzing them. This opportunity is provided to us with Geographical Information Systems. While software of Geographic Information Systems that will realize processes needed such as investigating and analyzing can be used, Geographical Information Systems aiming for the relevant purposes can be developed. There are various advantages of Geographical Information Systems.

When investigated quantitatively, advantages of Geographical Information Systems can be listed as below (Şehsuvaroğlu et al., 2017, 190);

- There are no data repetitions in CBS technology,
- Updating numerical geographic data is easier and cheaper,
- It is more correct and fast to produce information as based on data,
- It is cheaper to transfer data from another CBS with an appropriate data standard instead of producing them again,
- It helps with increasing the production,
- It provides savings from time, money and

Advantages of CBS with regards to qualitative aspects can be listed as below (Şeremet and Alaeddinoğlu, 2017: 189):

- Sharing of information: By enabling for sharing of locational information between different divisions, institutions and associations, it enables for them to use each other's locational information.

- Avoidance of abundance, complexity and inconsistency of information: Rapid changes in locational information and the need for updating as being parallel to this, gives rise to inconsistencies between locational information being stored in different places. CBS avoids abundance, complexity, and inconsistency of information.

- Gathering information together: An important advantage of CBS is that it promotes integral effectiveness being required for different divisions, institutions and associations to approach positional problems in a more systematic way.

- Classification of information: By means of CBS, data can be classified as per specific features. Classifications can help divisions that are in need of various information to solve their certain problems.

General Directorate of Geographical Information Systems being within the body of Ministry of Environment and Urbanization is assigned to conduct works and processes (or cause them to be realized) for establishing, using, and developing International Geographical Information System, to determine standards of relevant urban information systems regarding activities of local managements relating with planning, mapping, infrastructure and superstructure, to promote their being widely used, and to operate National Geographical Information Portal (Şehsuvaroğlu et al., 2017: 192). For this purpose, Regulation About Establishment and Management of National Geographical Information Systems has been published on the date of 20th of March,2015.

Main source of these studies is INSPIRE project which is created to enable access to spatial data being required for the policies and activities and especially for the environmental ones and those relating with environment in Europe. Basic principles of this project were revealed with the directive with number of 2007/E/AT. The directive which emphasizes the importance of free submission of minimum level of infrastructure to users for spatial data infrastructures to be successfully processed, requests for member countries to investigate spatial data sets and to prepare minimum level of data to be submitted as free, by also considering specific private conditions. Said directive emphasizes the necessity of network services for sharing of data between different levels of authorized public institutions and they enable for network services to reveal spatial data, to transform them, to screen them, to load them and to enable spatial data e-commerce requests (Uyan and Akçin, 2017: 44).

Provisions relating with these network services, emphasizes for the fulfillment of obligations as fully complying with relevant principles relating with protection of personal data as per European Parliament Directive with no 95/46/EC and Council directive being dated 24th of October 1995. In the 13th article of directive, it is stated that if having access to spatial data clusters and services influences international relations, public security and national defense in a negative way, it could be restricted (Millard and Hon, 2012: 69). Regarding these particulars in (f) paraphrase it is stated that confidentiality is provided with national law or communal law and that regarding notification of public, if the relevant person has not given his consent, it is required for the confidentiality of data and/or files belonging to the person to be provided. With regards to national law, the institution being assigned to fulfill this liability is General Directorate of Geographical Information Systems. Legal study which is a guide for the protection of existing personal data in Geographical Information Systems is Law about the protection of personal data with no. 6698. It comprises issues that should be paid attention to for the protection of personal data being present in Geographical Information Systems (Johnson, 2017: 4). In order for the necessary measures to be taken with regards to information security and protection of personal data and for the necessary efforts to be shown, first of all awareness should be created in this subject and level of consciousness should be improved (Gürleyen, 2016: 78).

In the law about the protection of personal data, liability to take necessary administrative and technical measures has been laid on the data responsible. For this reason, especially security, back-up, patching, reviewing the chipper policies bear importance. It is required for crisis management centers to be established and for confidentiality contracts to be signed between companies providing informatics services while having access to most critical information, and their employees (Çayır, 2016: 48). In the informatics systems, it is required for fundamental security measures to be improved. Besides these

measures, it is required for administrative arrangement and organization structures to be shaped by considering the particular of information security.

It is required to attach importance to restrictions regarding capturing of geographical data, analyzing them, processing them and making them become anonymous which form the main topics of Geographical Information Systems (Gürleyen, 2016: 77). As being examples to these restrictions, legal and security restrictions relating with data, restrictions relating with having access to data/capturing data, restrictions in using data, legal restrictions, security classification of data, and restrictions relating with security could be listed.

Security is a concept which bears the particulars such as what to be protected, the value being important, threats against this value, existing weaknesses, and measures that can be taken. In the protection of personal data, the value to be protected in "data" and "information" and it bears importance to conduct inventory study to define the content of particular that needs to be protected primarily (Civelek, 2011: 25). With the information systems and data inventory study which is part of these systems, data assets which are required to be protected and their qualities will be determined and accordingly, by considering qualities of data such as those being sensitive data, critical infrastructure data, and confidential data, security measures could be applied as fitting to these qualities (Uyan and Akçin, 2007: 49).

Important particular is for this type of measures not to be fixed but to be continuously updated, to be in conformity with the solid event, and for the process to be continuously reviewed (Civelek, 2011: 25). Within this frame it is required for data responsible to establish a data management system in accordance with the quality and scope of data being processed. In order for data management system to be established, it is primarily required for data security concept to be determined and then it should be tested to see whether this concept is actually operating or not and to determine how functional it is (Uyan and Akçin, 2007: 49). Besides it is required for data management system to be organized in a way to avoid for data to be used for reasons other than those being intended. Data responsible who is obliged to take administrative and technical measures for the data to be processed as per the conditions being foreseen in the law, should take measures such as notifying his personal who process data, training them, avoiding having access to those other than the authorized people, following up data processing activities, and keeping record of them.

By considering that any problems that may be experienced in information systems could influence the efficiency and quality of service provision negatively in the long term and that they could cause delays in daily service provisions, it could be thought that security of information systems should be considered starting from the design stage onwards and that balance should be established between functionality and security within this context (Civelek, 2011: 26-27).

CONCLUSIONS

Information is one of the most important values of modern life. Each day state institutions and private associations gather, store, process, and transfer important amount of information about individuals. Furthermore, technology develops in a way to permit sharing of personal information and their being spread worldwide. All of these cause for people to lose control of their information and for dangerous situations to arise such us their being used against them. Protection of personal data is a right owned by people against their individual data's being used by other people or institutions in an unauthorized way. By adding the following paraphrase to the law about the protection of this right with no 5982 and to 20th article of Constitution regulating confidentiality of private life, protection of personal data has been explicitly taken under constitutional security. Law about the protection of personal data has been accepted and legalized in Grand National Assembly of Turkey on 24th of March, 2016.

It is required for explicit consent of data owner to be taken for conducting processes such as defining personal data, processing personal data, erasing them, destroying them, or making them become

anonymous. Personal data responsible has legal, administrative, and technical liabilities which he is obliged to fulfill within the context of law. Furthermore, in 19th article of law for the protection of personal data, constitution of Institution for protection of personal data, having public legal entity, as being established to fulfill the tasks that are defined in the law, as also having administrative and financial autonomy is being arranged.

The system being composed of software, hardware and users with the aim to obtain information about geographical assets, storing them, processing them, and analyzing them is named as Geographical Information System (CBS). According to various sources, CBS is being defined as follows: It is a system dealing with management and analysis of big volume of geographical data relating with complex social, economical and environmental problems on the globe and the solutions being created for them. CBS, is a series of software and methods consisting of hardware, map module and database, which is designed for solving complex planning and method problems and which enables for spatial data being dependent on location to be stored, modeled, processed, analyzed and submitted. In Geographical Information Systems, besides existing spatial data, it is especially required for data bearing personal qualities to be protected. Among the international texts being accepted as relating with this subject, it is important that reference has been made to the protection of personal data while limitations are brought to having access to spatial data in European Parliament directive with no 2007/2/EC and Council directive being dated 2007. In this regard, measures which should be taken with respect to national law and especially creating awareness for the right about protection of personal data bear importance.

Since data responsible has the liability to take all kinds of technical and administrative measures for the protection of personal data, it is required for him to improve security measures in informatics system. With the information systems and data inventory study which is part of these systems, data assets to be protected and their qualities should be determined and by considering qualities of data such as their being personal data, sensitive data, critical infrastructure data or confidential data, appropriate security measures should be implemented. It is required for data responsible to establish data management system as per the quality and context of data being processed. In order for data management system to be established, it is first required to define data security concept and then to test whether this concept is actually operating or not and to determine how functional it is.

KAYNAKLAR (REFERENCES)

Atak, S., 2010, "Avrupa Konseyinin Kişisel Veriler Açısından Sağladığı Güvenceler", *TBBD*, Sayı 87. pp. 54- 72.

Atak, S., 2010, "Avrupa Konseyi'nin Kişisel Veriler Açısından Sağladığı Temel Güvenceler", *TBB Dergisi*, Sayı 87, pp.90-120.

Aygözer, C., 2016, *Kişisel Verilerin Korunması*, İstanbul, Beta.

Başalp, N., 2015, "Avrupa Birliği Veri Koruması Genel Regulasyonu'nun Temel Yenilikleri", MÜHF-HAD. c.21. s.1. pp. 77-105.

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.

Civelek, D., 2011, "Kamu Sektörü Bilgisinin Paylaşımı ve Yeniden Kullanımı", *Devlet Planlama Teşkilatı Bilgi Toplumu Dairesi Başkanlığı, Çalışma Raporu* 2. Şubat.

Çayır, F., 2016, "Kişisel Verilerin Korunması Kanunu ve OHAL Kanun Hükmünde Kararnamesi ile Kurulan Coğrafi Veri Merkezine İlişkin Değerlendirme", *21. Türkiye'de İnternet Konferansı.*

Develioğlu, H.M., 2017, *6698 Sayılı Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Olarak Avrupa Birliği Genel Veri Koruma Tüzüğü Uyarınca Kişisel Verilerin Korunması Hukuku*, On İki Levha Yayıncılık, İstanbul.

Gürleyen, S.B., 2016, "Coğrafi Bilgi Erişim ve Türkiye'deki Açık Coğrafi veri Hazırlıkları Üzerine Bir Değerlendirme", *Academia Journal of Social Sciences*, Vol. 1, Issue. 2, pp.70-89.

Johnson, E. H., 2007, *Data Protection Law in the European Union,* The Federal Lawyer, USA.

Kılınç, D., 2012, "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması", *AÜHFD*, Vol. 61(3), pp. 1089-1169.

Korkmaz, İ., 2016, "Kişisel Verilerin Korunması Hakkında bir Değerlendirme", *TBBD*, Sayı 124, pp. 82-156.

Millard, C. Hon, W.K., 2012, "Defining Personal Data in e- Social Science", *Information*, *Communication and Society*, Vol. 15, No. 1, pp. 66.

Şehsuvaroğlu, M.S., Araz, A., Koç,İ., Selderesi, N.,2017, Harita Genel Komutanlığı, "Coğrafi Veri Bilgi Kapısı", *AKÜ FEMÜBİD*, 17. Özel Sayı pp. 190- 203.

Şeremet, M.F., Alaeddinoğlu, F., 2017, "Coğrafi Bilgi Sistemlerinde Farklı Bir Perspektif: Eleştirel CBS'ye Yönelik Bir Literatür Analizi", *Batman University Journal of Life Sciences*, Vol. 7, No. 1, pp. 187-194.

Uyan, C. Akçin, H., 2007, "Türkiye'de Konumsal Verinin e-Devlet Yapısı İçinde Satışına Yönelik Bir Uygulama", *Harita Genel Komutanlığı- Harita Dergisi*, Yıl 73, Sayı 137, Ocak. pp. 43-57.