University of Westminster
School of Media, Arts & Design
Department of Journalism & Mass Communication

MA Communications Policy

2MED7H1

Advanced Independent Study

Dissertation:

"Privacy and the Role of Regulations Regarding Data Protection in Telecommunications Sector: A case Study on Turkey"

Submitted by

Ulku Davutoglu*

1351186

Submitted to

Dr. Maria Michalis

August 2010, University of Westminster, London

* ulku.davutoglu@my.westminster.ac.uk

ABSTRACT

Privacy is a basic human need which should be protected legally. Right to privacy provides individuals capability of determining to what extent their personal information shall be communicated to others. Due to its importance on creating dignity and liberty of individuals in society, privacy has been subject to regulations in both national and international level via setting principals and rules.

Owing to the development and fast spread of new telecommunications (electronic communications) technologies, new threats to privacy have emerged. Those technologies introduced new types of data providing personal information about users who benefits from telecommunications services and networks. Each transaction in telecommunications generates new set of data about users' habits, relations, whereabouts etc. thus users are threatened by their own data. Since telecommunication technologies are widely used in society, almost all individuals of society have the risk of facing those threats. As a result, states and international bodies make regulations regarding data protection in telecommunications in order to prevent mentioned threats

This study intends to analyse the relationship between privacy and the data generated in connection with telecommunications services and/or networks and role of regulations regarding data protection in telecommunications sector in protecting privacy.

Key words : privacy, data protection, personal data, traffic data, location data, unsolicited communication.

Supervisor : Dr. Maria Michalis

Content

List of Tables

List of Figures

1. INTRODUCTION

Privacy is a basic human need which is crucial for the development of individuals (Busch, 2010:1). Since privacy is a basic human need, right to privacy is accepted as one of human rights. Most countries accept right of privacy as an institutional right and have set legislations to protect privacy.

Protection of privacy is not a new issue, since individuals' information has been being gathered and merged for long, for different purposes. Marketers, lenders, insurers, private investigators and governments has had efforts to collect personal information such as names, addresses of individuals and information regarding activities of them throughout the twentieth century (O'Harrow, 2006: 39). Although notion of privacy has been introduced by Warren and Brandeis (1890) as "the right of the individual to be alone" (cited in Penders, 2005: 247) in last few decades privacy has been subject to discussions and regulations more. The increasing trend of discussions on regulations regarding protection of privacy is due to increasing threats to privacy resulted from technological developments in telecommunications (electronic communications). Since the fast spread of internet and mobile communications, new regulations on privacy in information and communication technology has emerged.

Although telecommunication technologies facilitate the life and contribute to public interest, they have some "side effects" which may not be seen in the first step of technological diffusion. The most significant side effect of telecommunication technologies is the fact that each telecommunication transaction produces data which may have high privacy and may be personal (Kuzeci, 2011:142).

With the help of telecommunication technologies personal data of individuals can be collected, stored and transmitted easily. Namely, the privacy of users who benefit from telecommunication services are threatened by the information generated with use of these services. Owing to the fact that electronic communications is widely used in every aspect of the life by almost everyone in society, all people may face with this threat regardless of where they live and who they are.

Telecommunications sector is subject to intervention of governments due to its distinctive features and challenges. Governments intervene in this sector with the help of regulations to ensure that the players of the sector act in accordance with public interests. Like other issues of telecommunications, privacy of personal data generated or processed in connection with the provision of electronic communications services are also subject to government intervention. This intervention is accomplished by the tools which are called regulations. The issue of data protection in telecommunications is directly related to privacy of private life and freedom of communication which are basic human rights. Thus, telecommunications regulations regarding protection of data play a big role in both protecting privacy and freedom of communication.

Depending upon the rapid changes and new technologies in telecommunications; new issues, new challenges and shortcomings regarding the protection personal data emerge.

In this study it is aimed to research regulatory issues regarding data protection in telecommunications and their role in overall privacy. Besides, current situation is discussed with the help of political analysis as a case study.

1.1 RESEARCH QUESTIONS

This study particularly seeks to answer the main questions such as:

(i) Why do governments need to make regulations about privacy in telecommunications?

(ii) How can the right of privacy be achieved in telecommunications and what are the current challenges?

(iii) How is policy regarding privacy in telecommunications sector made and what are the current challenges in Turkey?

1.2 SCOPE AND FOCUS

Technological development in the last decades has changed many things in our lives. The usage of telecommunications (electronic communications) technologies such as the Internet and mobile phones is increasing day by day. Many people benefit from telecommunication technologies in terms of not only communication but also socializing, researching, economic transactions and entertainment. Governments also take the advantages of electronic communications introducing e-government applications, using telecommunications systems for national security, public security etc. In addition, with the increasing use of the Internet and decreasing prices of mobile communication, they are accepted to be one of the most efficient ways to reach customers. Therefore, businesses have started to use the means of electronic communications heavily for their marketing purposes.

The scope of privacy in information and communication systems is very wide, including privacy in social networks, cloud computing, closed circuit television (CCTV), Internet banking radio frequency identification (RFID) and telecommunications services.

This study focuses on the protection of data generated or processed in connection with the provision of telecommunications services which are subject to regulatory framework of electronic communications services and networks. Therefore, this study does not cover the privacy issues arised from many applications and services which are actually not electronic communications networks/services but usually confused since they are provided over electronic communications networks/services.

Two basic questions help to define the scope of this work:

(i) Which activities/services/applications are included in electronic communications (What is an electronic communication service)?

(ii) Which personal data are produced while providing electronic communication services?

Financial services on line, privacy on e-trade, e-government applications, privacy regarding google applications and social networks, cloud computing, CCTV and RFID are not accepted as telecommunications services. They are the applications created or delivered over telecommunications services or networks. Privacy issues regarding to them are dealt in information society service regulations or cyber crime regulations not in telecommunications regulations. With this regard privacy concerns resulting from cybercrime or information society services, on-line financial services, e-trade, e-government applications, google applications, social networks, cloud computing, CCTV, RFID etc. fall outside of the scope of this work.

1.3 METHODOLOGY

Researches play important role for social sciences by providing means for enhancement of intellectual development of them (May, 1999: 1). According to May (1999), "*the social sciences status as 'science' are often justified by alluding to the technical aspects of research methods, while the very term 'science' carries with it ideas of areas of study which are accessible only to those who have undergone a lengthy training process in order to understand their inner workings* (p: 1)". Deciding on the right research method for the specified working title and questions then applying the method properly is crucial for social sciences thereby crucial for this research project.

This research study seeks to answer its questions above by the so-called policy and archival research (Hansen et al., 1998: 66-90) and a case study. Policy and archival research constitutes the main method for the studies which require reviewing different kinds of literature and archives (Hansen et al., 1998: 66-90). Within the frame work of this study, for the policy and archival research, main references are:

(i) Literature on related topics such as privacy, data protection, telecommunications regulations and policies regarding privacy,

(ii) Related reports, publications and archives of international agencies

(iii) Related legislations

Case studies are functional because they provide detailed and specific information about one situation or event, and then they exhibit the relationship between the cases and wider issues. On the other hand, one of the strengths of the case study approach is that it allows the researcher a variety of research methods (Denscombe, 2003: 31). Within this study the title 'Regulatory Issues Regarding Data Protection in Telecommunications in Turkey" is dealt as a case study in order to submit a specific instance for the issue.

Bryman (2001) defines the research method as "*a simply a technique for collecting data. The method can involve a specific instrument such as self completion questionnaire, interview schedule, participation observation or content analysis*" (p:29). Interview is the most convenient option for the case study of this study because the aim of the case study is to gather deeper information about regulations regarding data protection in Turkish telecommunications sector. It is evident that participant observation naturally can not apply to the topic. Similarly, content analysis seems to be incompetent to collect sufficient amount of data because in earlier stages of searching research it has been determined that there has been a lack of data in about data protection in Turkish media and lack of awareness of rights regarding privacy in public. Questionnaire does not allow flexibility to the respondents and also results in low response rate (Frankfort & Nachmias, 1996: 237) so that it is not appropriate option as well.

According to Denscombe (2003) "*it is appropriate to use interviews if the research would be better served by getting material which provides more of an in-depth insight into the topic, drawing on information provided by fewer informants*" (p: 164). In this project, with the help of interview, information regarding policy of regulator and other political issues which is not found in literature, can be obtained by interview

Interviews can be categorized as three : (i) structured, (ii) unstructured and (iii)semi structured. Structured ones follow a set form. The questions are all decided before the interview, interviewer has no flexibility he follows pre-designed sequence and

questions. The interview mainly includes closed and directed questions. (May, 1997: 110; Allison et al, 1996: 104)

On the other hand, unstructured interviews provide interviewer flexibility and freedom to modify the sequence of questions. Interviewer can go deeper and obtain more detailed information. There are no set questions planned topics that are raised at appropriate moments. This style of interview enables the researchers to see more complete picture (May, 1997: 112; Allison et al, 1996: 106).

Semi structured interviews are somewhere between structured and unstructured ones, they benefit the advantages of both. Questions are pre determined and specified but the interviewer is more flexible to probe beyond the answers. The answers are the mixture of close and open ended (May, 1997: 111; .Gray, 2004: 215,216).

On the other hand, there is still need for predesigned questions. In this study semi-structured interview is used. The interview has pre designed questions to get the advantage of time and to lead interviewees and it is flexible enough to let the interviewees express their opinions deeper knowledge about policy of regulatory body on data protection in telecommunications

The interviews are conducted on face-to-face basis in Ankara, Turkey. The list of interviewees is given below.

(i) Osman Sahin, ICT Expert in Information and Communications Technologies Authority (ICTA), working on data protection in telecommunications,

(ii) Meltem Turhan, ICT Expert, Legal Consultancy Department, ICTA, working on data protection in telecommunications,

(iii) Leyla Keser Berber, (Dr. Leyla Keser Berber, Director of IT Law Institute, İstanbul Bilgi University), specialized on privacy legislation.

2. POLICIES OF DATA PROTECTION

2.1 PRIVACY, RIGHT TO PRIVACY AND DATA PROTECTION

The issue of privacy and right to privacy have been discussed since late 1800s. The notion of privacy was introduced by Warren and Brandeis as "*right to be let alone*"(1890: 193). According to them right to privacy makes individuals be capable to determine "*to what extent his thoughts, sentiments, and emotions shall be communicated to others*"(1890: 198) namely, "*whether that which is [theirs] shall be given to the public*" (1890:199).

Gavison (1980) defines right to privacy as the right of a person *"to determine what information about is communicated to others, person's measure of control over personal information and over who has sensory access to him or her, and a state or condition of limited access to the person"* (cited in Chandler, 2009: 121). Westin's (1967) definition of privacy addresses that it is "*a basic need shared by all individuals, the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about themselves is communicated to others*"(cited in Costello). Altman (1976) states that privacy is "*selective control of access to the self or to one's group*" (cited in Costello).

For a deeper analysis it is necessary to take a step further to answer the questions; why is privacy important and why should it be protected?

For individuals, privacy is necessary for both creating and promoting dignity, individuality, liberty, and social intimacy in the society. Individuals who think they are tracked or whose personal data are subject to public scrutiny loose autonomy and feel pressure to confirm public expectations. Besides freedom from pressure to conform, privacy also protects individuals from other parties' use of their information (Schoeman, 1984: 8,19). In other words, privacy provides individuals "***autonomy"*** which is the ability to make one's own decision and "*limited and protected communication"* which ensures individuals to express themselves according to their context and aids them for developing and maintaining of their relationships with society (Costello).

The concept of data protection and privacy are not identical. They can be referred as twins but have slight differences. Data protection is related to the rights of individuals to protect the data which identifies them (Kurner, 2009: 307). Regulations of data protection seek to create safeguards to protect data which provide information about identification of individuals as well as information about their whereabouts, habits and other certain situations.

On the other hand, the concept of privacy is wider. Privacy covers issues relating to the protection of an individual's 'personal space' in addition to the issues relating to data protection. Basing on the European Convention on Human Rights, Kuner (2009) lists the issues that privacy deals with as "*private, family and home life, physical and moral integrity, honour and reputation, avoidance of being placed in a false light, non-revelation of irrelevant and embarrassing facts, unauthorised publication of private photographs, protection against misuse of private communications, protection from disclosure of information given or received by the individual confidentially*"(p.309).

Since the improvements in and spread of computers and telecommunication technologies (such as mobile phones and the Internet), privacy has been threatened by person-related information which can be created and transmitted easily in digital area. Such information can be stored, compressed, manipulated and interpreted easily as never before. Besides, they can be transformed into useful knowledge more easily compared to before (Busch, 2010:2; Nisseanbaum, 2009: 37).

To sum up, issues regarding data protection can be assumed as a subset of those regarding privacy. Data protection deals with establishing safeguards against threats to privacy resulting from modern technology which enables easy ways to obtain and process personal data of individuals. Since the scope is the role of telecommunication regulations in privacy, privacy is handled through the perspective of data protection within this study.

2.2 THE RATIONALE OF REGULATING DATA PROTECTION

Governments, actors in private sectors and other individuals can reach individuals' data easily with the help of improving, pervading and diversifying technology.

Tracking and monitoring threat individuals in improving their 'personality'. Thus, democratic governments have to make regulations in order to prevent such threat (Kuzeci, 2011: 143).

Although tracking and monitoring are not new issues, in the last few decades modernity introduced a new term, 'surveillance society'. Nissenbaum (2009) defines surveillance as a term which *"covers much of monitoring and tracking. It is usually associated with a set political assumptions, monitoring is performed 'from above' as subjects of surveillance are monitored by those in authority or more powerful than them" (p.22).* Accordingly, regulations regarding privacy and data protection should ensure to create safeguards against the threats of surveillance society.

According to Gavison (1980), the notion of privacy can only be functional if it is protected legally (cited in Yuksel, 2009: 277). Hustinx (2008) states that "*the right to privacy and personal data protection can only be made effective in practice, and this certainly includes situations where the need for protection is greatest*"(p:31). Hence, personal data can be protected by proper regulations which base on legal basis.

While forming legal solutions to protect privacy, regulators should concern who, for whom and for what purposes are collecting and processing personal data of individuals.

2.3 POLICIES REGARDING DATA PROTECTION REGULATIONS

To begin, it must be mentioned that there is no unique description of policy but it can be summarized as; a process of determining agenda, follows making consultations, decision making, enforcement and decision making and eventually product of politics, economics and culture (Papathanassoppoulos and Negirne, 2011:3) Analysing the policy making process in communications, several interest groups (actors) must be considered to see the whole picture. Within the framework of data protection, those actors having influence on policy making process can be given as (this is not an exhaustive list) international bodies, other states, governments, public, nongovernmental organizations and other parties who use data.

Here it must be noted that international affairs (that is policies, strategies and regulations of international bodies and dominant states) are the most influential matter that shapen states' domestic policies. There are two main rationales of this; (i) need for harmonization and (ii) increasing number of databases which are accessible globally.

Firstly, with the effect of globalization, personal data have been subject to flow among states. The disaccord among states about data protection level prevents appropriate protection of data all around the world. To ensure the free flow of data among states, the standards should be harmonized. To illustrate, the EU has set adequate level of protection with its Data Protection Directive – 95/46/EC and has prohibited its Member States to transfer personal data to states which do not have sufficient regulation to meet that level (95/46/EC, recital 20 of preamble).

The EU has become the most influential international body by its Data Protection Directive which has determined minimum standards and has suggested high level of data protection. Besides, first experiments related to data protection has emerged in 1970's due to governments' widespread usage of computers and centralized data bases in order to collect and process information about their citizens in Western Europe, especially in Germany, first regulations regarding data protection has emerged in this region and they began to affect other regions. Being first in data protection regulation has made Europe be followed by other states (Kuzeci, 2011: 14).

Secondly, globally accessible databases lead same data be subject to different standards for protection. International businesses face with economic difficulties because of the uncertainty resulting from incoherent standards in data protection (Kuner, 2009;307).

The trade off between security and privacy is another issue which affects policy of data protection. Regulations of data protection cover not only the measures of protecting data but also exemptions for collecting and processing of them in order to provide security. Chandler (2009) defines that the debate on that trade off as a contest between national security and privacy which has been shut down in favour of

security (p.122). In this day and age, the tendency of governments to impose duties on organizations to collect and report data of individuals for national security reasons is increasing. Financial instuitions, airline companies and especially telecommunication operators are the examples of those who are involved by governments in data collection being far from their own interests (Hustinx, 2008:28).

In addition to governments, commercial firms benefit from the access to personal data. They take the advantage of knowing their customers and become more competitive and profitable by decreasing their costs, establishing strategies for meeting the needs of their target market and advertising effectively with the help of that knowledge.

Despite states go for harmonization in that field in order not to be excluded from free flow of information and utilize international trade; level of data protection still differs from one society to another. The desire for privacy, which is high in more modern societies (Busch, 2010:.3), and awareness of public about privacy are the other factors that shape such policy. .

As a consequence, data protection policies are mainly influenced by international regulations especially those of the EU. Besides, policy makers take the debates on security and privacy, businesses needs and public demands into consideration while regulating the field.

3. INTERNATIONAL POLICIES OF REGULATING PRIVACY ON TELECOMMUNICATIONS

Since telecommunication services/networks has eased the move of digital data across national borders and around the globe, international level has become the right place for regulation of privacy. Thus, several international bodies have attempted to establish guidelines and common frameworks of privacy regulation for nations (Busch, 2010:5). The political agendas and agencies has varied over time but the most leading agencies and organizations in privacy field who put main points, framework and principles are European Union, Organization of Economic Cooperation and Development (OECD) and the International Conferences of Data Protection and Privacy Commissioners.

3.1 THE RATIONALE BEHIND INTERNATIONAL FRAMEWORK

The first generation regulations regarding data protection were born in a period where computers were used by few. The regulations were set up in national level and policy of privacy was state-centric (Jori, 2007: 3.1). However, globalization gave rise the need for regulation in international level. According to Jori "*The need for harmonizing national legislations occurred inevitably after the adoption of the first data protection acts, in order to ensure that these national legislations are not boundaries to the trans-border flow of personal data*" (2007:3.3).

The main aim of international studies is to create harmonization among countries about data protection because the regulations regarding data protection in electronic communication provides provisions concerning not only protection of data but also free flow data. The cooperation of non-European members of OECD and European states for forming the draft of "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" is an instance of harmonizing studies. Afterwards, OECD introduced its own guidelines about data protection which has been influential for both European Countries and Europe ones. Its principles inspired European Council's Data Protection Directive (95/46/EC).

The need for unique regulations within the European Union (EU) arised from the differences among the national data protection regulations of Member States and the consequent obstacles to the creation of a single internal market (Jori, 2007: 3.3). EU introduced Data Protection Directive for defining general rules of data protection and free flow of data in all sectors. Data Protection Directive requires member states to harmonize and ensure an equivalent level of data protection, besides it prohibits the transfer of data to any third country that does not have adequate privacy legislation competent with the provisions of Data Protection Directive (Civelek, 2011:77). Hence, it has been influential all over the world because of the willingness of the third countries to harmonize their legislation with EU in order to get the benefits of free flow of data. Namely, Data Protection Directive affected the regulations of not only EU Member States but also non-European Countries. Its impact on international area was significant. It affected data protection regulations of South Africa, Argentina, New Zealand, Hong Kong, Canada (Jori, 2007:3.3). Data Protection Directive was followed by Directive 97/66/EC which was replaced by Directive E-Privacy Directive (2002/58/EC) which provides rules for data protection in electronic communications sector and suggests Member States harmonize their national legislations on data protection in the sector. Data Retention Directive (2006/24/EC) is another regulation for data protection in electronic communications which also illustrates harmonization studies within EU. Before Data Retention Directive, Member States had introduced different legislations on data retention relying on some provisions of Data Protection Directive and E- Privacy Directive. This disharmony has been suppressed by European Council introducing Data Retention Directive.

3.2 INTERNATIONAL DISPUTES ON DATA PROTECTION

Despite the harmonization studies in the field, regulation of data protection has been subject to disputes between two approaches: The European Approach and the United States (US)' Approach.

Although it seems that the differences between approaches are resulting mainly from colliding economic interests which became evident because of the massive growth of electronic commerce and different security strategies which were formed after 09 September 2011 to fight against terrorism, the emergence of differences comes up to

1960s and 1970s. The US used to have advantage of early introduction of information technologies and stayed out of European moves towards data protection in 1970s (Busch, 2010: 6). Busch summarizes the difference of the approaches as "*Europeans saw the American championing of freedom of information and free flows of data across national borders primarily as designed to protect the advantage of the US data processing industry, while Americans suspected Europeans of erecting protectionist barriers to trade in the name of protecting privacy*" (2010:6). Furthermore, in 1978, when OECD initiated studies for construction of its guidelines to harmonize different national data protection legislations, difficulties in negotiations occurred because the US which had dominant data industry was one of the parties (Bennett, 1992: 136).

Owing to the influence of European Commision's Data Protection Directive, states around the world went for policy harmonization in data protection which means they started to follow a similar data protection policy with one significant exception, that of the United States[1] (Jori, 2007: 3.3).

After terrorist attack on 11 September, the focus of the disputes shifted from economic sphere to security sphere making the US became more controller and more interfering on personal data (Civelek, 2010:82). The new policy of the US which is primarily focusing on decreasing protection of personal data was not compatible with the concept of "adequate level of protection" which makes Data Protection Directive, thus the more protective European Approach, more effective and influential in international level (Jori, 3.3:10). Consequently, the EU and the US went on negotiation and agreed on "Safe Harbour Privacy-Principles" in 2000 and still valid between parties. By Safe Harbour Privacy-Principles, US moved towards meeting the adequate level of protection of European Union (Civelek, 2010: 83-84) which exhibits that European Approach influenced even the US to some extent.

[1] Bennett (1997) called this manner as "American exceptionalism"(113).

3.3 INTERNATIONAL REGULATIONS REGARDING DATA PROTECTION

3.3.1 Convention 108

The right to privacy was first held as an issue at international level by The Council of Europe. The Council declared "the right to respect for private and family life" in 8th Article of its European Convention of Human Rights (ECHR) in 1950. ECHR was followed by Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No: 108 (Convention 108) which was adopted in 1980 and opened to countries for signature on 28th January of 1981. Convention 108 mentions basic principles for data protection which address that; personal data should be obtained and processed fairly and lawfully, be stored only for legitimate and specified purposes, be accurate and kept up to a date. Besides, the Convention includes regulations regarding trans-border data flows in relation with free flow of data. Although it has some weaknesses such as it has no mechanism for enforcing compliance with its rules and many of its terms are left undefined; Convention 108 is a key reference point for following instruments of privacy and data protection debate in Europe (Busch, 2010: 6; Bygrave, 2008: 26)

3.3.2 OECD Guidelines

OECD which had been invited to cooperate for the Convention 108 had already taken interest in privacy issue before. The draft of Convention 108 had been formed also with the help of non-European members[2] of OECD (Busch, 2010:6). In 1978, OECD set up its own group to handle the issue and agreed on certain principles by adopting "Guidelines Governing the Protection of Privacy and Trans border Flows of Personal Data". The Guideline suggests eight specific principles for national applications which are in connection with Convention 108 of Council of Europe and four principles for international applications for international applications regarding free flow and legitimate restrictions.(Bennett, 1992: 136; Bush, 2010: 6; OECD, 1980). The principles are categorized such as national level and international level.

[2] Australia, Canada, Japan and United States

Basic principles for national application and their explanations are the ones as follows (OECD,1980: Articles 7-14):

(i) Collection Limitation Principle suggests limits for collecting personal data. According to this principle personal data can only be obtained by lawful and fair means where appropriate, with the knowledge or consent of the data subject.

(ii) Data Quality Principle seeks for relevance of the personal data with the purpose of their usage. According to this principle, data should be necessary for the specified purpose, should be accurate, complete and kept up-to-date.

(iii) Purpose Specification Principle addresses the features of the purpose for which the personal data is collected. The purpose should be specified not later than at the time of data collection. The collection and usage of personal data should be limited by the fulfilment of the specified purposes and the data which are incompatible with those purposes should not be collected or used.

(iv) Use Limitation Principle limits the usage, disclosure of personal data and access to those. Personal data should not be disclosed, made available or used for other than specified purposes which are in accordance with "Purpose Specification Principle". But the principles has exceptions such as; personal data might be used for other purposes only with the consent of the data subject or by the authority of law.

(v) Security Safeguards Principle sets rules related to protection of data against some risks. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data

(vi) Openness Principle mentions a general policy of application, principles and developments regarding the privacy issue. Within this principle, OECD

states that "*Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.*"

(vii) Individual Participation Principle lists the rights of individuals regarding privacy. According to this principle an individual has the right;

- to obtain information whether his personal data is collected or not by data controller who officially has the authority or by anyone other than data controller,

- to regain his own data within a reasonable time, in an easily understandable way, at a charge, if any, that is not excessive and in reasonable manor,

- to be informed about the reasons of denial if a request of information regarding collection or usage of the data is denied and to be able to challenge such denial,

- to challenge his personal data. If the challenge is successful the data relating to him should be erased, rectified, completed or amended.

(viii) Accountability Principle declares that a data controller should be responsible for complying with measures which give effect to the other principles of the Guideline.

The Guideline of OECD has been influential for both inside and outside of Europe because it (Sahin, 2011: 19);

(i) had wide scope, which means it does not address either government or private sector,

(ii) focused on data controller exhibiting only guidelines and general rules (thus it is not binding),

(iii) was written in technology neutral terms,

(iv) added accountability principle,

(v) mentioned the significance of trans border flow.

It has influenced the data protection regulations of non- European countries such as: Japan, Australia, New Zealand, Canada and Hong Kong (Bygrave 2008:28). Furthermore, it also has formed a basis for European Council's 95/46/EC Data Protection Directive (Sahin, 2011:19).

3.3.3 Data Protection Directive (95/46/EC)

Data Protection Directive, composed of 7 chapters and 34 articles, was a consequence of the EU's single Internet market in goods and services which emerged in 1992 and increasing use of the Internet (Busch, 2010: 7). In addition to main principles mentioned in the Guideline of OECD, Data Protection Directive includes special provisions about sensitive data such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and those concerning health or sex life. It also covers provisions for data protection related to direct marketing and conditions for disclosure of personal data.

Data Protection Directive proposes establishment of independent national authorities which are responsible for data protection. Furthermore, it aims to provide a balance between high protection for personal privacy and free flow of information. Within this context; it not only provides free flow of information regarding personal data, whenever necessary, but also determines the methods and principles about conditions and necessities for which personal data can be collected, stored, used or processed (Civelek, 2011:72).

The protection intended by Data Protection Directive is preventive which means the Directive aims to construct a structure which can prevent attacks to privacy rather than to suggest solutions for possible attacks (Basalp, 2004: 31).

Data Protection Directive is technology neutral (Civelek, 2011: 75) which means this Directive can be applied to any situation in which personal data are processed regardless of technology used.

The Directive has main principles regarding processing of personal data and the responsibilities of Member States and controllers which are as follow:

Member States can collect and process data only in fairfull and lawfull ways. Besides, collected or processed data can be kept up to a date (95/46/EC, Article 6a, 6d)..

Member States can collect data for only specified purposes. The purpose should be explicit and legitimate and must be determined at the time of collection of the data. Data collected previously cannot be used or processed for any further incompatible purpose other than the purpose which was originally specified. Personal data can be processed for historical, statistical or scientific purposes which are compatible with the original purpose provided that Member States generate suitable safeguards (95/46/EC, Article 6b, 6c).

The data may be processed only with the consent of the data subject [3] (95/46/EC, Article 7.1)

Member States should prohibit to process personal data disclosing special information about data subject such as ethnic origin, religions, religious or philosophical beliefs, political opinions, trade union membership and the data concerning health or sex life. (95/46/EC, Article 8.1)

Member States should ensure that, controllers will provide sufficient information to data subject about himself/herself. For instance, the controller should inform the data subject about the purpose of collecting end processing data (95/46/EC, Article 10).

[3] The definition of data subject consent in 95/46/EC is "*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*" (95/46/EC, Article 2h).

Member States should promote for subjects right to access data. Every data subject should be able to obtain information about whether data relating to him/her are processed, the purpose of the controllers for collecting data. They should also be capable of being informed before personal data are disclosed to third parties for the purpose of direct marketing (95/46/EC, Article 11).

Member States should provide for the data subject right to object so that, data subjects may object to processing of his/her data on legitimate grounds (95/46/EC, Article 14).

In addition to rights of data subject, obligations of controllers and the responsibilities of Member States in order to protect privacy, Data Protection Directive also includes exemptions and restrictions. Accordingly, the scope of the principles regarding data quality[4], right to access and publicising of processing may be restricted by Member States for certain purposes such as national security, public security, defence, the prosecution of criminal offences, significant financial or economic interests of Member State or of the EU or protection of data subject (95/46/EC, Article 13). Data processing activities concerning national and public security and state wellbeing are excluded from the scope. According to the same article, data processed by a natural person in the course of a purely personal or household activity are also excluded (95/46/EC, Article 3). Personal data can be processed only if the data subject gives his/her consent, processing can be done under only reasonable necessities such as (95/46/EC, Article 7.2);

(i) for the performance of a contract in which the data subject is a party,

(ii) for accomplishment of a purpose resulted from a legal obligation which is pursued by the controller

(iii) for the performance of a task carried out in public interest

[4] The principle which expresses that data should be processed fairly, lawfully and they should be accurate and kept up to date (95/46/EC, Article 6a).

(iv) for protecting the vital interests of data subject

Furthermore, although article 8.1 includes provisions which prohibits processing special categories of data, it declares that this kind of data can be processed if (95/46/EC, Article 8.2);

(i) the subject data gives explicit consent for processing,

(ii) processing is necessary for the purposes of carrying out the legal obligations

(iii) processing is necessary to protect data subject or vital interests of another person where the data subject is legally or physically incapable of giving consent.

Data Protection Directive suggests Member States provide a supervisor authority/authorities to monitor the applications of the provisions of the Directive, contact with relevant regulators in their regulatory activities regarding data protection and consult independent advisory Working Parties to handle the issues regarding protection of individuals with regard to the processing of personal data (95/46/EC, Article 29). Article 29 Data Protection Working Party, an independent European advisory body on data protection, is one of those working parties set up under Article 29 of Data Protection Directive (Civelek, 2011: 72)

As a consequence, 95/46/EC provides general rules for protection of privacy in the EU. Following the main principles of OECD Guideline, it has set up new principles which OECD has not covered. Data Protection Directive is binding for all Member States. Citizens, relying on it, can claim their rights related to data protection issues in all Member States including even those, if there is any, which have not harmonized their legislation with the Directive yet (Civelek, 2011: 73).

3.3.4 E-Privacy Directive (2002/58/EC)

As mentioned before, OECD's Guidelines has set general principles related to data protection. Afterwards, European Council has widen the scope of the issue covering new measures to protect personal data and put the general rules for data protection for all sectors in the EU by its Data Protection Directive.

However, specific requirements concerning protection of privacy and personal data emerged as a result of introduction of advanced technologies in electronic communications sector. Need for specific rules covering data produced by electronic communications services/networks caused introduction of the new regulation which focuses only on protection of data originated telecommunications services/networks. This was the Directive 97/66/EC was then replaced by the E-Privacy Directive (2002/58/EC)

Kroes (2009) states that E-Privacy Directive aims to put provisions independent of technology, to apply data protection rules of Data Protection Directive in electronic communications sector and enhance the level of data protection in telecommunications. With this regard, E- Privacy Directive supplies solutions to problems related to cookie issues and data protection issues emerging in mobile networks such as defining locations (cited in Sahin, 2011: 36).

E- privacy Directive complement Data Protection Directive and provide for protection of the legitimate interests of subscribers who are legal persons. It covers, in particular, the right to privacy with respect to the processing of personal data in electronic communications. Although Article 1 restricts the scope of protection to subscribers, the whole text contains provisions for both subscribers[5] and users[6], thus E – Privacy Directive aims to protect the interests of both subscribers and users.

As well as Data Protection Directive, E-Privacy Directive includes provisions regarding consent of data subject. The use of data generated in electronic

[5] *natural persons or legal entities whoor which is party to a contract with the provider of publicly available electronic communications services for the supply of such services* (2002/21/EC, Article 2k).

[6] *a legal entities or natural persons using or requesting a publicly available electronic communications service* (2002/21/EC, Article 2h).

communications is subject to data subject's consent. The basic principle is to prohibit processing those data without consent of data subject.

E-privacy Directive defines basic concepts related to data protection in electronic communications. The directive gives place to the definitions of traffic data, location data, value added service and electronic mail in its Article 2.

E-Privacy Directive provides detailed and explicit rules for data protection in electronic communications such as regulating issues regarding confidentiality of communications, protection of traffic data and location data, unsolicited communication, itemised billing, line identification, automatic call forwarding directories of subscribers. The general principle of the Directive is based on the rights of users and subscribers to privacy and to be informed. To illustrate, the Directive suggests Member States to ensure that subscribers and users be informed about unsolicited communications and inclusion of their personal data in directories of subscribers and have the right to reject. The rules for traffic and location data are set in accordance with Data Protection Directive which means those data should not be processed without the consent of user or subscriber. Furthermore according to E-Privacy Directive, traffic data relating to subscribers and users, except where they are needed for billing purposes, must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. On the otherhand, for the purpose of marketing electronic communications services or for the provision of value added services, traffic data may be processed to the extent and for the duration necessary for such services or marketing, if the related subscriber or user has given his/her consent (2002/58/EC, Article 6). Similarly, location data other than traffic data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service (2002/58/EC, Article 6).

In general, E-Privacy Directive proposes measures for providing data security in the operations of electronic communications service and network providers. The Directive obliges the providers of publicly available telecommunications service and networks to take suitable solutions to safeguard security for personal data. In case of

a particular risk of a service or network, the provider should inform users and subscribers concerning such risk (2002/58/EC, Article 4)

E-privacy Directive also emphasizes confidentiality of communications[7]. Member States should ensure such confidentiality which means they should make appropriate regulation which prohibits tapping, listening, storage or other kinds of interception or surveillance of communications of users and the related traffic and location data without the consent of the users (2002/58/EC Article 5.1).

3.3.5 Data Retention Directive (2006/24/EC)

Although E-Privacy Directive has strict rules for processing and retention of traffic and location data, it excludes some activities such as defence, state security, the EU security and the activities of states in criminal areas. It allows restricting privacy rights and obligations through the retention of data for a limited period, where it is *"necessary, appropriate and proportionate in a democratic society to safeguard national security (i.e. state security), defence, public security and the prevention, investigation, detection and prosecution of criminal offences or of the unauthorised use of the electronic communication system as referred to in Article 13(1) of Directive 95/46/EC."* (2002/58/EC, Article 15.1)

Before the introduction of Data Protection Directive, retention of traffic and location data for prevention, investigation, detection, and prosecution of criminal offences were discussed extensively in Europe. Some Member States used to have legislation regarding data retention. For instance, Ireland used to have legislation which obliged retention of traffic data for 3 years. For another instance, all electronic communication providers in Italy used to be obliged to keep the traffic data for 4 years (Sahin, 2011: 43).

[7] The meaning of communication here is defined by the Directive as "*naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication*" (2002/58/EC recital 15 of preamble).

Mentioned provisions of E-Privacy Directive permit Member States adopt their legislation on data retention. As a consequence, while some service and network providers in some Member States were retaining data on behalf of law enforcement authorities, in other Member States there were no such a practice. These differences among Member States regarding data retention leaded to distortions in the EU internal market. Besides, the terrorist attacks in Madrid in 2004 and in London in 2005 added urgency to the discussions on how to regulate the issue and harmonize the regulations of Member States (EC, 2011a:4).

As a result of discussions, the EU introduced Data Retention Directive (2006/24/EC) which aims to harmonise the regulations about obligations for providers of electronic communications services, publicly available services and public communications networks with regard to data retention for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law (2006/24/EC, Article 1.1).

The scope Data Retention Directive covers traffic and location data of both legal entities and natural persons and the related data necessary to identify the subscriber or registered user.

Data Retention Directive defines the categories of data to be retained, obligations to retain data, periods of retention, protection and security of data. Data to be retained are divided into 6 categories as follows (2006/24/EC, Article 1.2; Article 5.2):

(i) Data necessary to trace and identify the source of a communication,

(ii) Data necessary to identify the destination of a communication,

(iii) Data necessary to identify the date, time and duration of a communication,

(iv) Data necessary to identify the type of communication,

(v) Data necessary to identify users' communication equipment or what purports to be their equipment,

1. Data necessary to identify the location of mobile communication equipment.

Details of such data are exhibited in Table 2 in Annex 1. It can be concluded that they are generally related to name or address of the subscriber or registered user, calling and called telephone number, user ID of internet users, Internet Protocol (IP) addresses, start and end times of the communication and log in and log off times of the internet access, the international mobile subscriber identity (IMSI), the international mobile equipment identity (IMEI), digital subscriber line (DSL), location label, geographic location,etc.

According to Data Retention Directive, Member States should adopt measures to ensure that data listed above are retained in accordance with the provisions of Articles 5, 6 and 9 of E-Privacy Directive (2006/24/EC, Article 3.1). Obligation to retention also covers the unsuccessful call attempts (2006/24/EC, Article 3.2). Retained data should be provided only to the competent national authorities in specific cases and in accordance with each Member's national law. The procedures and conditions for accessing retained data should be defined by each Member State in accordance with European Union law or public international law and European Court of Human Rights (2006/24/EC Article 4). The data should be retained for not less than six months and not more than two years from the date of the communication (2006/24/EC, Article 6). Their security and protection should be the same as those on network and they should be protected against destruction, loss or alteration ((2006/24/EC, Article 7).

3.3.6 London Initiative

In addition to the Directives and the Guidelines, we must also mention about International Conferences of Data Protection and Privacy Commissioners which are international events that bring together all parties (including representatives of non governmental organizations and academicians) related with regulations regarding privacy and personal data protection since 1978. The main objective of these conferences is to establish an environment for exchanging and sharing knowledge

and to support cooperation among nations for global regulations regarding the issue (EDPS, 2006).

The 28th Conference, which offered significant suggestions about making more effective regulations, was held in November 2006 in London. It was the first conference of the commissioners which provided a platform to discuss privacy issues regarding telecommunications (EDPS, 2006). In the conference, surveillance was discussed as purposeful, routine and systematic recording of individuals' movements and it was concluded that people were living in a surveillance society all around the world (Hustinx, 2008: 28).

The conference in London not only provided a platform to discuss related issues and to increase the awareness of data protection but also launched an initiative of "Communicating Data Protection and Making It More Effective" which is named as "London Initiative" in short. The initiative has emphasised on "better communication" and "effective data protection" and received general support of the authorities who are responsible for making regulations, all around the world (EDPS, 2006)

The initiative implies the main points of data protection as folows (EDPS, 2006):

The protection of data is vital for any democratic society,

(i) New communication strategies should be developed by data protection and privacy commissioners in order to make public and relevant parties more aware of the right to privacy and its importance. The strategies should be powerful enough to create long term awareness.

(ii) The effectiveness and efficiency of the practices of data protection authorities should be assessed.

(iii) The capacity of data protection authorities in technological areas should be reinforced by producing advanced studies, expert opinions and

interventions, interacting sharing and working with the new technology industries.

(iv) The involvement of all parties related to data protection including civil society and NGOs at national and international level should be promoted in order to develop strategic partnership where appropriate and to make the data protection regulation process more effective.

(v) The London Initiative was followed by other conferences of the Data Protection and Privacy Commissioners. It has a very influential guiding role for national and international regulatory authorities of electronic communications when making regulations.

4. TELECOMMUNICATIONS REGULATIONS AND PRIVACY

Regulations are the intervention tools of states to restrict the actions of real persons juridical persons and governmental entities. Telecommunications sector is one of the sectors which require highly intervention of government. Data protection is one of the issues subject to regulation in the sector. Related regulations form legal basis to ensure protection of data in connection with telecommunications service and networks.

4.1 RELATIONSHIP BETWEEN TELECOMMUNICATIONS SERVICES/NETWORKS AND DATA PROTECTION

Technological developments, especially the ones in telecommunications services and networks, have generated new threats to privacy owing to the fact that with the help of new telecommunications technologies new sorts of data has emerged.

Telecommunications technologies provide convenience for communication and also "*perpetual contact"* (Katz and Aakhus, 2002: 305-309). However, it must be noted that almost each transaction in telecommunications services and networks generates personal data making the issue of privacy in electronic communication sector very vulnerable.

With the help of telecommunication technologies personal data of individuals can be collected, stored and transmitted easily. Namely, the privacy of users, who benefit from suitable signaling systems of telecommunication services/networks, are threatened by the information about themselves which are generated with use of these services.

Telecommunications services and networks creates threats to the right to be alone since the data generated in telecommunications provide information regarding the users' habits, relations, whereabouts etc.

4.2 DATA TYPES GENERATED IN CONNECTION WITH TELECOMMUNICATIONS SERVICES AND NETWORKS

The question what kind of data is produced/obtained in connection with the provision of publicly available electronic communications services in public communications networks is very important as it defines the scope of privacy in electronic communications (and that of this work as well).

As mentioned in the Introduction there are two main questions:

i. Which activities/services/applications are included in electronic communications (What is an electronic communication service)?

ii. Which personal data are produced while providing electronic communication services?

Framework Directive (Directive 2002/21/EC) sets two basic definitions for the first question above:

> *"Electronic communications service means a service, normally provided for remuneration, which consists in the conveyance of signals on electronic communications networks. Services providing, or exercising editorial control over, content transmitted using electronic communications networks and services are excluded"* (2002/21/EC, Article 2c).

> *"Public communications network means an electronic communications network*[8] *used wholly or mainly for the provision of publicly available electronic communications services"* (2002/58/EC, Article 2d).

[8] *"Electronic communications networks means transmission systems which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed and mobile terrestrial networks, networks used for radio and television broadcasting and cable television networks"* (2002/21/EC, Article 2a)

To answer the second question, data regarding telecommunications services and networks can be classified into 3 main groups being; (i) personal data, (ii) traffic data and (iii) location data.

Because of influence on the states all around the world, Data Protection Directive can be said to be the general regulation with regard to the processing of personal data. It defines personal data as *"(a) any information relating to an identified or identifiable natural person*[9] (95/46/EC, Article 2a). This definition of personal data was needed to be clarified since there was some uncertainty and some diversity in practice among Member States, thus, Article 29 Data Protection Working Party was charged to form an opinion on the concept of personal data. In its opinion submitted in June 2007, the Working Party -noting that European Lawmakers seemed to adopt a broad notion of personal data intentionally- defined a very broad scope of personal data emphasizing the four main building blocks clearly stated in the definition above; *(i)"any information", (ii)"relating to", (iii)"an identified or identifiable", (iv)"natural person"* (Working Party 29, 2007: 6-25).

E-Privacy Directive defines traffic data as *"any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof"* (2002/58/EC, Article 2b).

According to E-Privacy Directive "*a communication may include any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication. Traffic data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission. Traffic data may consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning,*

[9] *An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"* (95/46/EC, Article 2a)

end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network" (2002/58/EC, recital 15 of preamble).

Traffic data are generated beyond the users' control and they exhibit with whom when and how long we contact. Accordingly they reveal our habits and relations (Warren and Brandeis, 1890;p195).

Telecommunications service is a two way point to point connection, end points should be known by the service providers in order to supply service. Knowledge about the end points provides information about the users' whereabouts which is called location data.

E-Privacy Directive defines location data as *"any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service"* (2002/58/EC, Article 2c).

According to E-Privacy Directive, "*location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded*" ((2002/58/EC, recital 15 of preamble).

4.3 APPLICABLE REGULATIONS TO DATA TYPES REGARDING TELECOMMUNICATIONS AND SERVICES

However, due to overlaps, a clear distinction between the groups is hard to achieve as there are many possible combinations, e.g., personal data can be location data as well or a traffic data may also fall into the group of personal data (FIDIS, 2007: 24).

On the following pages, the different possible combinations of personal, traffic, and location data giving examples of the combinations after evaluating the interpretations of relative Directives on data are we schematically illustrated.

However, the definition of Working Party is considered too sweeping by some other parties including Future Identity in the Information Society (FIDIS). For instance; while Working Party's definition includes all location data that can be produced in electronic communication services/networks, FIDIS states that location data that are not personal data do exist although this category is probably quite small (FIDIS, 2007: 27-28).

As mentioned before, Data Protection Directive is a general Directive applicable to all sectors. On the other hand, since the general Data Protection Directive may not provide sufficient legal protection for some sectors considering specific vulnerabilities or particularities of those sectors, EU has some sector-specific data-protection regulations including E-Privacy Directive (2002/58/EC) of electronic communications sector.

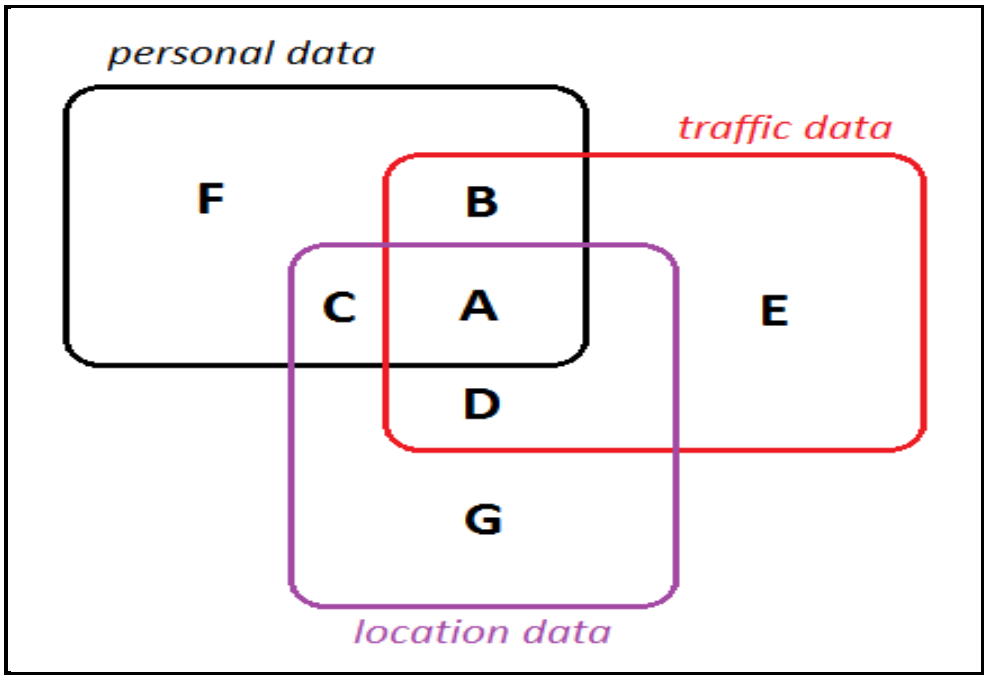
Here, Data Protection Directive must be viewed as the *lex generalis*[10]while E-Privacy Directive as *lex specialis*[11]. *Lex specialis*, in legal theory and practice, is a doctrine relating to the interpretation of laws, and can apply in both domestic and international law contexts. The doctrine states that where two laws govern the same factual situation, a law governing a specific subject matter (*lex specialis*) overrides a law which only governs general matters (*lex generalis*).So that; only the situations regarding processing of personal data that are not covered by the E-Privacy Directive fall within the scope of Data Protection Directive(FIDIS, 2007: 26).

To understand the relation between the data groups (personal, traffic and location), it may be better to use a drawing showing the overlaps (combinations of data groups: zones A to F in the drawing) between them. The drawing is followed by some examples for the clarification.

[10] Law which only governs general matters

[11] Law governing a specific subject matter

Figure 1: Relation Between Personal, Traffic and Location Data



Source: FIDIS, 2007: 27

It must be noted that the size of the zones in the drawing does not represent the size of the categories in reality. Category A includes the traffic data that are personal and location data, as well (Example: The cell-ID of a mobile phone used for a voice call by an individual subscriber). Category B includes those that are both traffic and personal data at the same time but not location data (Example: The date and time of an SMS sent by an individual with a GSM subscription). Category C includes those that are both personal and location data at the same time, but not traffic data (Example: address of an individual's fixed telephone). Category D includes those that are both traffic and location data at the same time, but not personal data (Example: Address of a public pay-phone where someone made a call). Category E includes those that are traffic data, but not personal or location data (Example: The date and time when an Internet user accessed a business website using an anonymising service). Category F includes those that are personal data, but not location or traffic data (Example: ID number or birthday of an individual subscriber). Category G includes those that are location data, but not personal or traffic data (Example: Location of a company mobile phone which is in stand-by position, if that phone is not registered to one employee and used by several employers). (FIDIS, 2007.28)

E-Privacy Directive declares the personal data to which it shall apply as *"This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community"* (2002/58/EC, Article 3.1.)

Therefore whether or not certain data (it may be traffic data, location data or something else) are considered as the personal data in the scope of E-Privacy Directive mainly depends on the question: Has it been produced or obtained in connection with the provision of publicly available electronic communications services in public communications networks?

The question whether the data has been produced/obtained in connection with the provision of publicly available electronic communications services in public communications networks is very important as it defines the scope of privacy in electronic communications (and that of this work as well).

Regarding which regulation shall apply to which data group, we must note again that; generally E-Privacy Directive takes precedence over the Data Protection Directive, but the latter supplements the protection of traffic and location data when they are not covered by prior one. E-Privacy Directive provisions only apply to data generated/obtained in connection with electronic communications[12]. Data generated in other services are not covered by E-Privacy Directive; however, if they relate to individuals, the Data Protection Directive applies.

To illustrate the complex picture of applicability of Directives, we split the each field of data category into two sub-categories (see Figure 2); (1) white part representing the data generated/obtained in connection with electronic communications and (2) grey part data generated in other services (For instance white part of category B, Category White-B, represents the traffic data generated/obtained in connection with an

[12] In some cases some provisions of Data Protection Directive applies together with E-Privacy Directive provisions.

electronic communications service which are also personal data but not location data).

Figure 2: Applicability of Directives to Data Categories

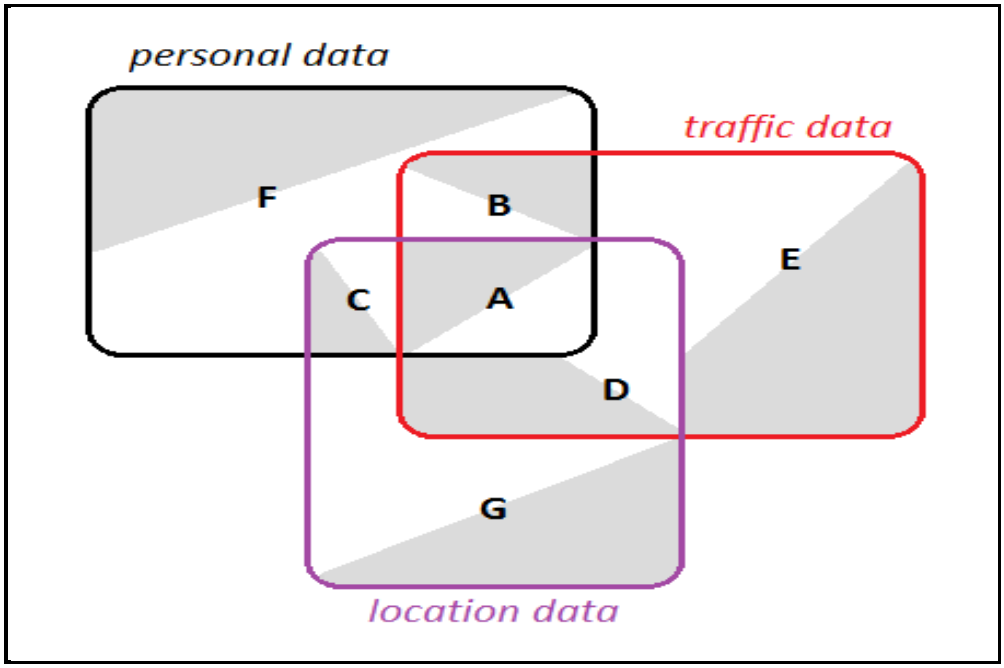


Table 1 summarizes the issue of which regulation should be applied for which kind of data:

Table1: Applicable Directives/Provisions According to Data Categories

Data Category	**Applicable Directive/Provisions**
White-A	Art. 5 and Art. 6 of E-Privacy Directive apply, indicating requirements such as confidentiality, the legal grounds for processing, storing, and erasure. Other requirements from Data Protection Directive (Art. 6 and 17) also apply, when related to personal data and not specifically covered by E-Privacy Directive, such as several aspects of data quality and data security.
Grey-A	Data Protection Directive applies.
White-B	The same as Category White-A.
Grey-B	The same as Category Grey-A.
White-C	Art. 9 of E-Privacy Directive applies, as well as other requirements

	from Data Protection Directive not covered by the E-Privacy Directive.
Grey-C	Data Protection Directive applies.
White-D	Art. 5 and Art. 6 of E-Privacy Directive apply.
Grey-D	Not covered by any legal data-protection instrument.
White-E	The same as Category White-D.
Grey-E	The same as Category Grey-D.
White-F	Data Protection Privacy Directive applies.
Grey-F	Data Protection Privacy Directive applies.
White-G	Art. 9 of E-Privacy Directive applies.
Grey-G	Not covered by any legal data-protection instrument.

Derived from FIDIS, 2007: 34-35

4.4 CHALLENGES REGARDING DATA PROTECTION IN TELECOMMUNICATIONS

The regulatory concept of data protection in telecommunications is related to two parties: (i) data subject[13] (ii) parties benefit from others' data.

Owing to the fact that main principle of data protection is ensuring prevention of illegal collection and processing of data, in telecommunication sector, regulators should set rules to make telecommunications service and network providers (operators) take measures to safeguard their users' data. Operators also should inform its users for the possible risks and threats to their data.

The parties benefiting from data generated in telecommunications are government and commercial firms. Governments may need traffic data and/or location data certain purposes such as national security, public security, defence, the prosecution of criminal offences. To solve the challenge of Governments to protect data in some circumstances where threats exist for the above purposes, EU adopted Data Retention Directive which allows Member States make regulations for ensuring

[13] An individual to whom personal data relates.

operators retain certain data for a certain time. Table 2 presents data to be retained by operators.

Commercial firms use telecommunications services to be close to their customers by unsolicited communication. Commercial firms use telecommunication technologies for direct marketing purposes such as SMS, fax, telephony or email. However, that kind of advertisement is incompatible data protection and may disturb users resulting in infringement of right to be alone. Unsolicited communication may be resulted from the illegal transmission of users' details from operators to third parties as well. Regulators should take measures to prohibit operators leak the personal data (name, address, number) to third parties such as commercial firms. There are two solution systems for unsolicited communication: opt-in, opt out. Opt in system suggests that users should be informed clearly about the further use of their details for direct marketing while making agreements for getting telecommunications service and should given the opportunity to refuse. Accordingly, operators should add a special provision for approval of unsolicited communication. Whereas opt in system prohibits communication for direct marketing without consent of user, opt out system allows usage of unsolicited communicated unless the user declares his objection. Namely, operators can send SMS or make telephone calls to its user and continue until the user expresses his disapproval (Sahin, 2011: 62). According to E-Privacy Directive, unsolicited communication can only be allowed if subscribers or users give their prior consent namely, opt in system is obliged for that kind of communication (2002/58/EC, Article 3.1)

Value added services are the other challenge for data protection in telecommunications. Some services, by their nature, requires processing of the users traffic and location data. To illustrate location data can be used by a GSM operator for providing its subscribers value added services such as traffic road support, weather forecast, emergent health, tracing children etc. If traffic and location data were not allowed to be processed, it would be impossible for operators to provide that kind of services. E-Privacy Directive offers solutions for value added services. Directive states that traffic data and location data may be processed if necessary for the provision of value added services (2002/58/EC, Articles 6.3, 9.3). However, it is

possible to adopt opt in system by adding an option to subscription agreements for value added services to ensure data subject’s consent.

5. CASE STUDY: ANALYSIS OF REGULATIONS REGARDING DATA PROTECTION IN TELECOMMUNICATIONS IN TURKEY

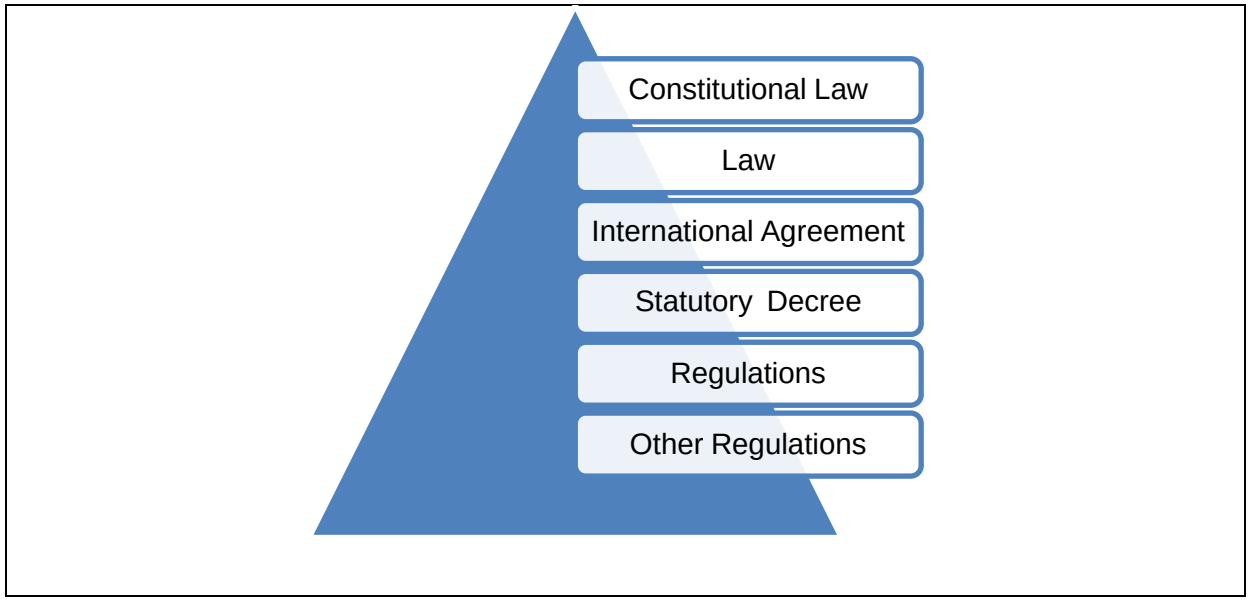
In this part of the study, regulations regarding data protection in telecommunications in Turkey are dealt in order to illustrate the role of telecommunications regulations in privacy with the help of literature review and interviews with experts from ICTA and an academician studying on data protection.

5.1 REGULATIONS REGARDING DATA PROTECTION

As mentioned in part 2.2 of the study, to ensure the effectiveness of data protection in practise and make the protection functional, the issue should be regulated legally.

In fact legislation is strictly hierarchical in nature, which is called “hierarchy of legislation”. According to ‘hierarchy of legislation’ inferior legislations derive its force from its superior ones. Any legal rule of an inferior legislation, which is incompatible with the rules of superior ones, is invalid and not applicable. Figure 3 represents the hierarchy in Turkey.

Figure 3: Hierarchy of Legislation in Turkey



Accordingly, any legislation should not be incompatible with Constitutional Law in Turkey. With the revision in 2010, a provision for data protection was added in

Constitutional Law. Article 20 states that each citizen in Turkey has right to demand for protection of his/her personal data. That article also gives citizens rights to access to their personal data collected, to demand for deletion or correction of the data and to be informed about the use and purpose of the usage the data. Personal data can only be processed with consent of the individual only under certain circumstances which any law foresees. Thus data protection is defined as a basic human right and secured by Constitutional Law which stands at the top in the hierarchy.

Another point of Turkish legislation system is that Turkey follows '*lex specialis*' doctrine[14]. Hence, regulations regarding data protection specified on telecommunications override general ones when the subject is the data in telecommunications.

Besides, Turkey is negotiating for membership with the EU, both the negotiations and the EU's high influence on data protection al around the world make Turkey follow European Directives while regulating the field.

5.2 GENERAL REGULATIONS REGARDING DATA PROTECTION

In Turkey, defining data protection as a constitutional and basic right provides the main framework of legal regulation. All provisions of inferior law about data protection base on the mentioned article of Constitutional Law due to hierarchy of legislation.

Turkey gave start to its studies to make a specific law regarding data protection under the frame of EU harmonization process in 1995. A commission was formed to construct a law regarding data protection. The commission finished its studies in 2003 by submitting the Draft Law Regarding Data Protection. However, the draft has not been transformed into a law yet.

Despite the fact that, there is still lack of specific law on data protection, the issue is dealt in some articles of a few laws as, Turkish Penal Code, Turkish Civil Code, Code of Obligations, Law Regarding Electronic Signature, Law on Right to Information (Sahin, 2011: 120-124).

[14] The doctrine is explained in part 4.3 in details.

The punishments for illegal storage, process or transmission of personal data occur in Turkish Penal Code (Article 135, 136). The Code also declares punishments to impose to those who do not erase personal data which are no longer needed for any purpose defined in any law (Article 138).

As well as processing data illegally is defined as a crime in Turkish Penal Code, individuals whose data are processed (and/or kept) have right to apply to the court (Turkish Penal Code, Article 25) to demand for compensation of pecuniary and non pecuniary damages (Code of Obligations, Article 58)

Law Regarding Electronic Signature includes provisions related to the obligations of electronic certificate service providers. According to the Law, service providers can collect only necessary data of the candidates for e- certificate. Unrelated data should not be collected. Service provider has obligations to ensure the security of data (Article 12). Additionally, Law on Right to Information, which provides individuals to access information, excludes disclosure of personal data. If public security is the matter, personal data can only be collected with the consent of data subject (Article 21).

5.3 SPECIFIC REGULATIONS REGARDING DATA PROTECTION IN TELECOMMUNICATIONS

The specific regulations on data protection in telecommunications are as follows:

(i) Electronic Communications Law,

(ii) By Law on Consumer Rights in Electronic Communications Sector ,

(iii) By Law on Authorization in Electronic Communications Sector,

(iv) By Law on Processing and Protection of Privacy of Personal Data in Electronic Communications Sector.

In Turkey, Electronic Communications Law is the framework legislation which provides general provisions regarding electronic communications sector. The Law charges ICTA with making regulations and carrying out necessary supervisions on processing and privacy of personal data (Article 6.1.c). According to the Law, ICTA can impose obligations to operators for maintaining security of their subscribers' data (Article 12.2.d). Unsolicited communication is the only issue regarding data protection which is dealt in details in the law. Although Data Protection and E-Pricacy Directives of the EU obligate for opt in system, opt out system is proposed in Electronic Communication Law (Article 50). By Law on Consumer Rights in Electronic Communications Sector adopts opt out, too (Article 15.2).

The law leaves other issues regarding data protection to be held by inferior legislations. In this regard, By Law on Authorization in Electronic Communications Sector which includes the provisions of the overall rights and obligations of operators has a general provision for data protection as well. According to it, operators are obliged to obey the regulations regarding protection of personal data (Article 19.2.ç).

By Law on Processing and Protection of Privacy of Personal Data in Electronic Communications Sector is the main secondary legislation that concern provisions for data protection in electronic communications. It includes detailed provisions regarding data retention, traffic data, location data and sanctions for infringements. According to it, operators are obliged to provide network security and to inform their subscribers about the risks. They cannot process traffic and location data for the purposes other than their service purposes. They should erase such data as soon as the specified purpose is achieved. They should take the approval of subscribers for and inform the subscribers about the processing of traffic and location data in case of value added services. Subscribers and users have right to cancel their approval (Articles 5-12). Furthermore data categories to be retained are listed, operators are obliged to provide security of retained data and the time for retention is limited to 1 year (Articles 13,15). By Law does not include any provisions for unsolicited communication.

5.4 POLITICAL ANALYSIS OF DATA PROTECTION IN TELECOMMUNICATIONS

It can be said that Turkish national policy for data protection is not state centric and intensely affected by the EU regulations. On the other hand national affairs such as politicians' interventions, demand of operators and public, attitude of media influence the policy to a certain extent. Turkish policy relies on the EU policy because of two reasons: (i) As a candidate member of the EU, Turkey has been struggling to harmonize its regulations with those of the EU and (ii) the EU has the highest protection level which influences the rest of the world including Turkey, for the reasons mentioned in the previous parts.

It must be also noted that Turkey signed Convention 108, however it has not been approved because there is still no specific national law on data regulation (Civelek, 2011:64). As understood from the interviews, this absence of specific law is the most important challenge of Turkey regarding the issue. The Draft Law was prepared in 2003 but has not come into force yet. Although the Draft was compatible with EU Directives, some politicians and media launched it as "tracking, monitoring and tagging instrument of the government". Furthermore, Data Protection Directive suggests to form an independent supervisory authority to control and consult for data protection (Article 28). Establishment of such an authority has been subject to discussions among related commissioners. Some commissioners have been in favour of establishment of that supervisory authority while some are against, indicating that a fully independent institution is not compatible with Turkish domestic legislation and costly to Government. Here it must be remembered that in its 2011 Progress Report about Turkey, EC (2011) emphasizes on the lack of independent supervisory authority and law in particular Data Protection Law (p.89).

The government has accelerated the process of putting the Draft Law into force since 2010. Provisions for data protection were added to Constitutional Law after the referendum held in September 2010. Thus, the amendments in Constitutional Law have contributed to the motivation of the Government to align the legislation sufficiently with the EU's. Besides, to achieve its economic development targets, Government should ensure foreign investors that data protection is harmonized with

the world. In recent years, some events about data leaking, including disclosure of personal data of the Prime Minister (about the state of his health), occurred. Those events have accelerated the speed of the studies as well.

Data protection in telecommunications sector is dealt by Information and Communications Technologies Authority (ICTA). ICTA opens its all regulations (when they are draft) to public opinion, so it can be said that ICTA's policy in data protection is also affected by public at some extent. The main parties in telecommunications are users and operators[15]. For operators, the issues regarding data retention and unsolicited communication create challenge. They, naturally, have commercial concerns. Interviews exhibit that in the public opinion process of Draft Regulation on Data Protection, operators mainly emphasized on the related provisions for data subject consent for value added services. They opposed to opt in solutions for unsolicited communication and demanded for opt out. They stated that if they asked the consent of their subscribers by opt in, subscribers would get confused and would not approve. Thus the volume of value added services provided would decline. As a consequence of the objections from operators, unsolicited communication has been removed from regulation. The other main concern of the operators was the costs of data retention. In this regard, some operators were not in favour of data retention. Removal of unsolicited communication form Draft Regulation for data protection in telecommunications is an instance for the impression of service providers on regulation process.

As mentioned before, the more awareness of the public is the more protective the legislation are. Public awareness and desire for data protection is rather low in Turkey. According to the interviews only a few people, individuals interested in telecommunications, interested in telecommunications, have knowledge about the issue. The only aware sector is telecommunications being the sole sector which has specific regulations for data protection. The complaints to ICTA from users are mainly related to unsolicited communication. There are almost no complaints regarding data leaking.

[15] Providers of service and/or networks in telecommunications sector.

There is no regular and systematized control system of ICTA. Controls are made due to complaints or the events appearing in the media. Therefore, it can be said that lack of public awareness affects the control mechanisms and keeps the amount of controls low. For an instance, 2011 is a milestone for data protection in telecommunications. Until 2011 no operator was punished depending upon infringement of data protection. The number of the cases is only 3 which is very low. Although it can easily be anticipated that more than 3 infringements occur during a year. Additionally, due to lack of framework Law, there is no proper sanction to impose for general issues in data protection which also affects the effectiveness of controls.

In 2011, ICTA has made 3 audits and the Board of ICTA decided for punishments. The events and the punishments can be briefly summarized as:

i. ICTA punished TTNet AS, the biggest internet service provider in Turkey, to administrative fine (0.02% of its net sales of 2010) because of sharing the personal data of its subscribers with one of its retailers (ICTA, 2011a: DK-14/659).

ii Turkcell AS, the biggest mobile operator in Turkey in terms of number of subscribers, was punished to administrative fine (0.015 % of its net sales in 2010) because one of its personnel had leaked personal data belonging subscribers (ICTA, 2011b: DK-10/198).

iii ICTA imposed administrative fine (0.05% of its net sales of 2010) to Vodafone AS due to a security gap in its system where data of subscribers are held (ICTA, 2011c: DK-10/83).

Briefly, it can be said that the biggest challenge is the absence of specific law which undermines the protection of personal data in all sectors. However it must be also noted that, electronic communications sector, despite the scarcity of proper legal tools in its field, is relatively in a good situation comparing to other sectors. Although ICTA awarded some punishments for the infringements of data protection rules in

2011, as given above, there are concerns regarding the dissuasiveness of the sanctions.

6. CONCLUSIONS

- Privacy is a basic human right. It is crucial for both development of society and self improvement of individuals. Lack of privacy threatens dignity, individuality, liberty and social intimacy of individuals. Governments develop policies to take measures to prevent attacks on privacy.

- The coverage of the notion of privacy is very wide including also data protection. Data protection, which is the focus of this study, covers data that provide certain knowledge to identify individuals.

- The first generation data protection regulations emerged as a result of increasing use of computers at national level and they were state centric. However, globalization and new telecommunication technologies has eased the movement of data across the national borders. Consequently, several international bodies attempted to regulate data protection globally. Nowadays, the state policies regarding data protection are mainly being affected from international affairs. States harmonize their legislations with international framework in order to benefit from free flow of data. OECD and EU are the leading bodies in the field with their guidelines and regulations.

- OECD introduced guidelines for data protection, afterwards, with its Data Protection Directive, EU introduced basic principles in connection with the guidelines. In brief, the guidelines of OECD (i) limit collection, usage and disclosure of personal data (ii) seek for relevant, specified purposes for collection, processing and usage of personal data, (iii) suggest regulators take necessary measures to safeguard personal data, (iv) provide for individuals right to be informed about the purpose and usage of their data and right to reject collection of their data and (v) mention the necessity of data subjects' consent.

- In addition to the requirements which are in line with OECD guidelines, the EU, by its Data Protection Directive, suggests Member States form an

independent supervisory authority to regulate data protection. In the Directive EU has set ‘adequate level of protection’ and has prohibited its Member States from transferring personal data to states which do not have sufficient regulation to meet that level.

- Despite harmonization studies for data protection, the issue is subject to disputes between two approaches. First one is European approach targeting high protection of data. Second one is US approach suggesting more freedom for collection and processing of individual data and less protection. Since Data Protection Directive provides high protection and does not allow free flow of data to third countries with inadequate protection, EU approach is more influential on other states compared US approach. In fact, EU’s highly protective policy is the most influential factor all around the world.

- Public awareness and desire for privacy, which are high in modern societies, are the other factors which are influential on national level of protection. However their effects are low compared to international regulations.

- Telecommunications technologies have revealed new threats to privacy. Each transaction in telecommunications networks generates personal data. Users of telecommunication services are threatened by their own data generated in connection with telecommunication services and networks. Those data are traffic data and location data.

- E-Privacy Directive and Data Retention Directive are the sector specific regulations for telecommunications of EU in data protection field. E-Privacy Directive has provisions regarding protection of traffic and location data and unsolicited communication.

- Unsolicited communication is mainly used for the purposes of direct marketing. It can be the result of data leakage of operators to third parties and can disturb users. Namely, in case of non existence of users’ consent, unsolicited communication infringes right to be let alone. Hence, regulators should take

measures. There are two methods of solution for unsolicited marketing: opt in and opt out. EU directives proposes for opt in system. However, operators tend to prefer opt out because of their commercial concerns.

- Value added services create challenge for protecting traffic and location data. Operators process such kind of data in order to supply value added services. Opt in system is an effective measure to ensure data subject's consent.

- Despite E-Privacy Directive has strict rules for retention of traffic and location data, it permits data retention for some certain purposes such as defence, state security, public security and criminal prosecution. In this regard, Data Retention Directive was adopted in order to achieve harmonization of the regulations regarding data retention among Member States. The Directive provides provisions related to obligations of operators to retain users' data and conditions under which data can be retained.

- Telecommunications Regulations regarding data protection obliges operators to safeguard location, traffic and personal data of users benefiting from electronic communication services and networks. They also limit access of third parties to such data. In EU level, the provisions of Data Protection Directive, E-Privacy Directive and Data Retention Directive are applied to such data depending on the type.

- Telecommunications regulations regarding data protection play big role in ensuring privacy. Traffic data and location data offer significant knowledge about users. Other sectors like finance, insurance are also open data leakage yet their services are not got by whole society. However, in this day and age telecommunications services are got by almost everyone in society, all people may face with the threat regardless of where they live and who they are. Therefore protecting data in telecommunications affect all society.

- Case study of this work illustrates the influence of international and national affairs on states' data protection policies. Turkey focuses on harmonising its all

levels of legislation regarding data protection with EU but harmonization in terms of data protection is achieved only in telecommunications sector. There is still an absence of framework law. Draft law was prepared in connection with EU Data Protection Directive, yet national factors such as politicians and media affected the time table. Thus, it can be concluded that national factors do not affect the direction of policy but still have some effects like determining the time table.

- Public awareness in Turkey is very low. There is no pressure from the public on the Government to put framework Law into force. However, Turkish Government is working for constructing a framework compatible to EU legislation in order to accomplish its economic goals.

- Telecommunications regulations are the most effective ones in general data protection issue in Turkey. Nonetheless there are still shortcomings. Absence of framework law affects data protection in telecommunications as well. Sanctions are not well defined. Control mechanism is weak and no regular controls are done. Controls are done due to complaints but owing to lack of public awareness ICTA does not receive as many complaints as the number of infringements.

REFERENCES

- Allison, B., O' Sullivan, T., Owen A., Rice, J., Rothwell A., Saunders C., (1996) 'Research Skills for Students', De Monfort University, London

- Altman, I., (1976) 'Privacy: A Conceptual Analysis' in *Environment and Behavior*, *8*(1), 7–29

- Baslap, N., (2004) 'Kisisel Verilerin Korunmasi ve Saklanmasi [Protection and Retention of Personal Data] *,* Yetkin Yayınları [Yetkin Press] , Ankara

- Bennett, Colin J. (1992) 'Regulating Privacy: Data Protection and Public Policy in Europe and the United States'*,* Ithaca: Cornell University Press.

- Bryman, A., (2001) 'Social Research Methods', Oxford University Press, Oxford

- Busch, A., (2010) 'The Regulation of Privacy', in *Jerusalem Papers in Regulation and Governance, Working Paper*, No. 26, September: 1-22.

- Bygrave, Lee A. (2008) 'International agreements to protect personal data', in James B. Rule and Graham Greenleaf (eds) (2008), *Global Privacy*

- *Protection*, Northampton, MA: Edward Elgar, 15-49.

- Chandler J. A. (2009) 'Personal Privacy versus National Security: Clarifying and Reframing the Trade-off' in Kerr, Lucock and Steeves, eds. *On the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, Oxford Univ. Press, 121-138.

- Civelek, D. Y. (2011) 'Kisisel Verilerin Korunmasi ve Bir Kurumsal Yapılanma Onerisi [Protection of Personal Data and a Corporate Structuring Proposal], TC Kalkinma Bakanligi [Ministry of Development of Turkish Rebublic], Ankara

- Costello, L. K., 'Privacy and Disclosure' available at http://k8lin.com/2012/08/07/privacy-and-disclosure/ retrieved on 19 August 2012

- Council of Europe (1981) 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*'*, (ETS 108), Strasbourg

- Denscombe, M., (2003) 'The Good Research Guide', Open University Press, Buckingham, Philadelphia

- Drake, W. J. (2000) 'The Rise and Decline of the International Telecommunications Regime' in Marsden, C.T., (ed.) *Regulating the Global Information Society*, London, Routledge

- EC (1980) 'Convention for the Protection of Individuals with regard to

Automatic Processing of Personal Data No: 108' Brussels

- EC (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', in *Official Journal of the European Communities*, L 281/31, 23 November 1995

- EC (2002a) 'Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a Common Regulatory Framework for Electronic Communications Networks And Services (Framework Directive)', in *Official Journal of the European Communities*, L 108/33, 24 April 2002.

- EC (2002b) 'Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on Concerning the Processing of Personal Data and the Protection Of Privacy in the Electronic Communications Sector', in *Official Journal of the European Communities*, L 201/37, 31 July 2002.

- EC (2006) 'Directive 2006/24/EC of The European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection With The Provision of Publicly Available Electronic Communications Services or of Public Communications Networks And Amending Directive 2002/58/EC' in *Official Journal of the European Communities*, L 105/54, 13 April 2006

- EC (2011a) 'Report from The Commission to the Council and the European Parliament Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)', Brussels

- EC (2011b) 'Commission Staff Working Paper Turkey 2011 Progress Report Enlargement Strategy and Main Challenges 2011-2012', Brussels

- EDPS (2006) 'Communicating Data Protection and Making It More Effective' available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/06-11-03_London_initiative_EN.pdf retrieved on 17 June 2012.

- European Commission's Directorate General for Justice, 'Article 29 Working Party', avaliable at http://ec.europa.eu/justice/data-protection/article-29/index_en.htm, retrieved on 12 August 2012.

- Frankfort, C., Nachmias, D., (1996), 'Research Methods in the Social Sciences', London

- FIDIS No: 507512, (2007) *D11.5: The Legal Framework for Location-Based Services in Europe*

- GAVISON, Ruth (1980), 'Privacy and the Limits of Law', in *The Yale Law Journal,* 89/3: 421-471.

- Gray, E., G., (2004) 'Doing Research in The Real World', Sage Publications, London

- Hansen, A., Cottle, S., Negrine, R. and Newbold, C. (1998) 'Mass Communication Research Method', London: Macmillan.

- Hustinx, P.J., (2008) 'The Surveillance Society:Trends and Implications for Data Protection' in *Challenge Europe*, Issue 18, December: 28-33

- ICTA (2011a) 'Board Decision DK-14/659' Ankara

- ICTA (2011b) 'Board Decision DK-10/198' Ankara

- ICTA (2011c) 'Board Decision DK-10/83' Ankara

- Katz, J., E., Aakhus, M., (2002) 'Perpetual Contact: Mobile Communication Private Talk Public Performance' Cambridge, Newyork

- Jori A., (2007) 'Data Protection Law: An Introduction' available at http://www.dataprotection.eu/ retieved on 01 August 2012.

- Kroes Q. R., 2009, E-Business Law of the European Union, Netherlands.

- Kuner, C., (2009) 'An International Legal Framework For Data Protection: Issues And Prospects' in *Computer Law and Security Review: The International Journal of Technology and Practice*, Vol.25(4), 307-317

- Kuzeci, E., (2011) 'Anayasal Bir Hak, Kisisel Verilerin Korunmasi [A Constitutional Right, Protecting Personal Data]', in *Aylık Bilisim Kulturu Dergisi [Journal of Informatics Culture],* Ocak (January)

- May, T., (1997), 'Social Research Issues Methods and Process', Open University Press, Buckingham, Philadelphia

- Nissenbaum, H.,(2009) 'Privacy in Context: Technology, Policy and the Integrity of Social Life', Stanford University Press, Palo Alto, USA

- OECD, (1980) 'Guidelines Governing the Protection of Privacy and Trans border Flows of Personal Data' avaliable at http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part2 retrieved on 01 August 2012.

- O'Harrow, R., (2006) 'No Place To Hide: The Terrifying Truth About The People Who Are Watching Our Every Move' Penguin Books, London, UK

- Papathanassoppoulos S., Negirne R., (2011) ‘Approaches to Communications Policy: An Introduction’ in Papathanassoppoulos S., Negirne R., *Communications Policy: Theories and Issues*, Palgrave

- Penders, J., (2004) ‘Privacy in Mobile Telecommunications Services’ in *Ethics and Information Technolgy, 6:247-260.*

- Sahin O., (2011) ‘Elektronik Haberlesme Sektorunde Kisisel Verilerin Islenmesi, Saklanmasi ve Gizliliginin Korunmasi [Processing, Retention and Protection Personal Data in Electronic Communications Sector], BTK [ICTA], Ankara

- Schoeman, F., (2007) ‘Privacy: Philosophical Dimensions of the Literature’ in Schoeman, F., (ed.) *Philosophical Dimensions of Privacy: An Anthology, Cambridge UniversityPress, New York: 1-33.*

- Warren, S.; Brandeis, L.,(1890) ‘The Right to Privacy’, Harvard Law Review, 4: 193-220.

- Westin, A. (1967) ‘Privacy and Freedom’ New York: Atheneum

- Working Party 29, (2007) ‘Opinion 4/2007 on the Concept of Personal Data’, 01248/07/EN WP 136

- Yüksel, M., (2003) ‘Mahremiyet Hakki ve Sosyo-Tarihsel Gelisimi [Right to Privacy and Its Socio-historical Development], in *Ankara Universitesi SBF Dergisi [SBF Journal of Ankara University* , C:58/1:181-213.

ANNEX 1

Interview (1) with Osman SAHİN

(ICT Expert, Sectoral Competition and Consumer Rights Department, ICTA)

1) Apart from the EU framework, is there any other factor affecting policy of data protection in electronic communications in Turkey?

Turkey has been negotiating with the EU for membership and signed Convention 108 of the European Council. So, all regulations in telecommunications are done with the aim of harmonising EU legislations. The national policies are affected by the EU as well.

2) Are the opinions of public, operators or nongovernmental organizations taken into consideration while making regulations? For example, was the draft of new regulation on data protection opened to public opinion?

Yes. The draft regulation was opened to public opinion.

The attendance of public was low however operators' attendance was high. Operators expressed their commercial concerns. Operators mainly emphasized on the related provisions for data subject prior consent necessary for provision of value added services. They stated that some applications, for example advice on least expensive tariff packages, are in favour of consumers but if prior consent was necessary and consumers did not consent for data processing, it would be disadvantageous to consumers. They also opposed opt in method for unsolicited communication. They demanded for opt out. They stated that if they asked the prior consent of their subscribers for direct marketing, subscribers would get confused and would not approve and consequently they would not be informed of advantageous tariffs and packages.The other concern of the operators was the costs of data retention. Some operators were not in favour of data retention and they stated that the minimum retention period should be applied.

Draft regulation used to include provisions for unsolicited communication, however as a result of the Draft E-Trade Law, those provisions were removed.

Electronic Communication Law suggests opt out for unsolicited communication thus it is incompatible with EU legislation. However, E-Trade Law includes opt in and soft opt in methods for unsolicited communications which is compatible with EU legislation.

3) How is the control mechanism of ICTA regarding data protection? Does ICTA control operators regularly or control when a complaint occurs?

There is no regular control system of ICTA. We do control operators basically due to consumer complaints but sometimes take action according to the events appearing in media. The level of public awareness is not sufficient yet. There have been no complaints regarding data leaking but the consumer complaints are mainly related to unsolicited communication. So, only a few controls have taken place so far.

4) Are the obligations effective enough to prevent illegal data processing? Are there any examples for ICTA's punishment due to illegal data processing or leaking of data?

There is a lack of provision for sanction to impose to data leakers in sectors other than electronic communications. ICTA cannot intervene in other sectors in terms of data protection. So, if a frame law about data protection which is compatible with 95/46/EC Directive enter into force, it will not only complement the deficiencies in data protection but also increase the level of public awareness in this area.

Until 2011 no operator was punished depending upon infringement of data protection.

There are three examples:

- ICTA Board Decision No: 2011/DK-14/659
- ICTA Board Decision No: 2011/DK-10/198

- ICTA Board Decision No: 2011/DK-10/83

It is important to mention that telecommunications is the only sector in Turkey which is regulated in terms of data protection.

5) Is there any supervisory authority suggested by Data Protection Directive (95/46/EC)?

No. ICTA makes its regulations regarding data protection only basing on the provisions of related Directives of the EU.

Interview (2) with Meltem Turhan

(ICT Expert, Legal Consultancy Department, ICTA)

1) What is the role of ICTA in studies of Data Protection Law?

ICTA plays a big role attending to the workshops and submits its opinions regarding the issue.

2) What are the suggestions of ICTA for Data Protection Law?

ICTA informs about provisions for data retention and data protection in telecommunications and leads the provisions of Draft Law in connection with ICTA regulations. Besides, ICTA suggests being more active in preparing provisions of confidentiality of communication.

3) Who determine data protection policy in Turkey?

Ministry of Development and Ministry of Justice

4) Who is responsible for preparing Data Protection Law?

Ministry of Justice

5) Is the Draft Law opened to public opinion?

Partially. It has not been opened to public yet, but it is planned to be. So far, it has been opened only to state institutions and organizations.

6) Why has the data protection law not come into force yet?

The main discussion on the Law is about the supervisory authority to be formed. The EU suggests independent supervisory authority but the issue of independency is incompatible with Turkish domestic law. Besides, it is costly for government to form such an authority.

Interview (3) with Leyla Keser Berber

(Dr. Leyla Keser Berber, Director of IT Law Institute, İstanbul Bilgi University)

1) What is the policy of government in data protection?

The policy of the government is in connection with the EU policies. After 2010 studies has speed up.

2) Why has studies speeded up since 2010?

In 2010, provisions for data protection have been added to Constitutional Law after referendum. Constitutional Law has required government to prepare legislation for data protection. In other words, government has made a change in constitutional law which binds itself. Thus, studies for data protection law have speeded up.

Furthermore, the government published a report about its targets for 2023. Lack of Law on Data Protection is a burden for the Government achieving those goals.

In recent years, some events about data leaking, including disclosure of personal data of the Prime Minister (data regarding his health), has occurred. Those events have accelerated the speed of studies as well.

3) Why has the data protection law not come into force yet?

Some politicians in the Parliament and media have reflected the Law as “tracking, monitoring and tagging instrument of government”. However the fact is different. Law is fully compatible with the EU Directives.

4) What are the shortcomings in regulating data protection in Turkey?

Most important shortcoming is lack of a framework Law. But the draft is planned to be submitted to Parliament on October 2012.

5) What is the level of desire for privacy and public awareness?

Public awareness is almost zero. Only a few people, interested in telecommunications, have knowledge about the issue. The only aware sector is telecommunications.

ANNEX 2

Table 2: Data to be Retained Under the Provisions of Data Retention Directive

<table>
<tr><td colspan="5">DATA NECESSARY TO TRACE AND İDENTİFY THE SOURCE OF ACOMMUNİCATİON</td></tr>
<tr><td colspan="2">concerning fixed network telephony and mobile telephony</td><td colspan="3">concerning Internet access, Internet e-mail and Internet telephony</td></tr>
<tr><td>the calling telephone number</td><td>the name and the address of the subscriber or registered user</td><td>the user ID allocated</td><td>the user ID and telephone number allocated to any communication entering the public telephone network</td><td>the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication</td></tr>
<tr><td colspan="5">DATA NECESSARY TO İDENTİFY THE DESTİNATİON OF ACOMMUNİCATİON</td></tr>
<tr><td colspan="2">concerning fixed network telephony and mobile telephony</td><td colspan="3">concerning Internet e-mail and Internet telephony</td></tr>
<tr><td>the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is</td><td>the name(s) and address(es) of the subscriber(s) or registered user(s)</td><td>the user ID or telephone number of the intended recipient(s) of an Internet telephony call</td><td colspan="2">the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication</td></tr>
</table>

routed			
DATA NECESSARY TO İDENTİFY THE DATE, TİME AND DURATİON OF A COMMUNİCATİON			
concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication	concerning Internet access, Internet e-mail and Internet telephony		
	the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic orstatic, allocated by the Internet access service providerto a communication, and the user ID of thesubscriber or registered user	the date and time of the log-in and log-off of theInternet e-mail service or Internet telephony service,based on a certain time zone	
DATA NECESSARY TO İDENTİFY THE TYPE OF COMMUNİCATİON			
concerning fixed network telephony and mobile telephony: the telephone service used	concerning Internet e-mail and Internet telephony: the Internet service used		
DATA NECESSARY TO IDENTIFY USERS' COMMUNICATION EQUIPMENT OR WHAT PURPORTS TO BE THEIR EQUIPMENT			
concerning fixed network telephony, the calling and called telephone numbers	concerning mobile telephony		

	the calling and called telephone numbers	the International Mobile Subscriber Identity (IMSI) of the calling party	the International Mobile Equipment Identity (IMEI) of the calling party	the IMSI of the called party	in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated	the IMEI of the called party
DATA CONCERNİNG INTERNET ACCESS, INTERNET EMAİL AND INTERNET TELEPHONY TO İDENTİFY COMMUNİCATİON EQUİPMENT.						
the calling telephone number for dial-up access			the digital subscriber line (DSL) or other end point of the originator of the communication			
DATA NECESSARY TO IDENTIFY THE LOCATION OF MOBILE COMMUNICATION EQUIPMENT:						
the location label (Cell ID) at the start of the communication			data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained			

Derived from Data Retention Directive 2006/24/EC Article 5.