



National Security Exceptions to the Processing of Personal Data under the new Turkish law on protection of personal data and the EU data protection regime

[Itır Çetinkaya \(u1277366/ANR 883532\)](#)

Master thesis Faculty of Law

LL.M. Law and Technology

Tilburg Institute for Law, Technology, and Society (TILT)

Supervisor: Emre Bayamlıoğlu

Second Reader: Colette Cuijpers

Tilburg 2017

Table of Contents

1. INTRODUCTION	4
1.1 BACKGROUND	4
1.2 SIGNIFICANCE	10
1.3 RESEARCH QUESTION	12
1.4 METHODOLOGY	13
1.5 STRUCTURE OF THE THESIS	13
2. GENERAL REVIEW OF THE LAW AND THE TURKISH LEGISLATION BEFORE THE LAW	15
2.1 TURKISH LEGAL LANDSCAPE BEFORE THE LAW	15
2.1.1 CONSTITUTION	16
2.1.2 CIVIL CODE	19
2.1.3 CRIMINAL CODE	19
2.1.4 CODE OF OBLIGATIONS	20
2.1.5. OTHER GENERAL PROVISIONS	20
2.1.6 SECTOR-SPECIFIC LAWS	21
2.1.7 THE LAW ON DUTIES AND POWERS OF POLICE	22
2.2 THE LAW ON PROTECTION OF PERSONAL DATA	23
3. NATIONAL SECURITY AND NATIONAL SECURITY EXCEPTION	32
3.1 NATIONAL SECURITY AND NATIONAL SECURITY EXCEPTIONS IN TURKEY	33

3.2 THE SCOPE OF NATIONAL SECURITY IN THE EU	36
3.3 BALANCING THE NATIONAL SECURITY INTEREST AND RIGHT TO PROTECTION OF PERSONAL DATA WITHIN THE EU AND TURKEY	38
4. ANALYSIS	43
5. CONCLUSION	50
BIBLIOGRAPHY	53

1. Introduction

1.1 Background

Last year, Turkey took a new step to catch up the European Union by passing a data protection legislation. The Law on Protection of Personal Data (hereafter: Law), enacted on 24 March 2016, came into force on 7 April 2016. There are number of motives that triggered the legislation process. First, Turkey was an unsafe country regarding data protection, and the lack of adequate data protection caused difficulties in cooperation between Turkey and foreign agencies. Second, Turkish companies had also suffered difficulties in their business relations with Europe for the same reason. Last, Turkey is a candidate country for the European Union, and data protection legislation is a part of the required criteria for the EU harmonization process.¹

“The European Union launched the Visa Liberalization Dialogue with Turkey on 16 December 2013, in parallel with the signature of the EU-Turkey Readmission Agreement.”² The Readmission Agreement concerns the resettlement of refugees from the European Union states to Turkey.³ Visa Liberalization Dialogue is based on 72 requirements that Turkey must fulfill, in order that Turkish citizens can travel to Schengen area without a visa for maximum of 90 days.⁴ Ratifying and implementing international data protection conventions and implementing a legislation on the protection of personal data were two of these requirements. Also, cooperation with European Union agencies, such as EUROPOL, EUROJUST, and OLAF, was set as a

¹ 'New Data Protection Law In Turkey - Edri' (*EDRi*, 2016) <<https://edri.org/new-data-protection-law-in-turkey/>> accessed 25 February 2017.

² European Commission, 'European Commission Opens Way for Decision by June on Visa-Free Travel for Citizens of Turkey' (2016) <http://europa.eu/rapid/press-release_IP-16-1622_en.htm> accessed 25 February 2017.

³ “The Europeans agreed to give \$3.3bn to Turkey and in return asked the Turks to take back and resettle refugees coming from Turkey, and prevent more refugees from entering the EU via Turkey. Additionally, they pretended to revitalize Turkey's EU membership bid, and promised Turkish citizens visa-free travel within the Schengen area in the unspecified future” Cengiz Aktar, 'EU-Turkey: Is Refugee Issue A New Membership Criterion?' *Al Jazeera* (2016) <<http://www.aljazeera.com/indepth/opinion/2016/03/eu-turkey-refugee-issue-membership-criterion-160310093315328.html>> accessed 25 February 2017.

⁴ *ibid*

requirement as well.⁵ A proper data protection law was needed since “with the current scale of the refugee problem, the Turkish Police coordination with EUROPOL is more crucial than ever, especially with regard to data sharing on data processing of refugees”⁶. As an outcome of the visa liberalization requirements, especially the cooperation with EUROPOL, the Law came into force after many years of waiting. This is a keen development, which should have been completed long before for the citizens own good, not only for the sake of cooperation with the EU.

Prior to the approval of the Law, Turkey did not have a specific data protection law. The Turkish Parliament started working on the draft of the Law in 2003. The second draft was prepared in 2008; however, none of the drafts were enacted. In 2015, the third draft was finalized and enacted as the Law in 2016.⁷ Also, Turkey signed the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (hereafter: Convention 108) on 28 February 1981; however, Turkey did not ratify it for 35 years, until 29 February 2016. Although the country lacked a harmonized data protection law before 2016, some general provisions were found in various statutes to regulate data protection.⁸ Primarily, following the constitutional amendments of 2010, protection of personal data became a fundamental right, and as a result, restrictions on recording and processing of personal data were introduced to the Turkish Constitution. Other general provisions were formed under Civil Code, Code of Obligations, Criminal Code, and Law on the Right to Access Information. Also, sectorial laws applied to the protection of personal data. In today's technology and data-driven world, a general legislation for the protection of personal data was needed rather than the dispersed general and sector-specific provisions.

⁵ European Commission, 'Turkey's Progress on the Visa Liberalization Roadmap - Factsheet' (2016) <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-migration/background-information/docs/20160504/turkey_progress_visa_liberalisation_roadmap_en.pdf> accessed 25 February 2017.

⁶ Akın Ünver and Grace Kim, 'Data Privacy and Surveillance in Turkey: An Assessment of the Draft Law on the Protection of Personal Data', (2016) EDAM Cyber Policy Paper Series 2, p. 18

⁷ Hande Hançar Çelik and Ozan Karaduman, 'The New Personal Data Protection Law in Turkey - Gün + Partners' (*Gün + Partners*, 2016) <<http://gun.av.tr/the-new-personal-data-protection-law-in-turkey/>> accessed 26 February 2017.

⁸ Fevzi Toksoy, Bahadır Balki and Sera Erzene Yıldız, 'Data Protection in Turkey: Overview' (*Practical Law*) <<http://uk.practicallaw.com/7-520-1896#a897047>> accessed 19 February 2016.

The Law is based on Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereafter: Directive 95/46/EC). Directive 95/46/EC was taken as an example to form the Law; however, there are several differences, as well. While Directive 95/46/EC focuses on the act of processing personal data, the Law provides rights and set obligations on the data processing parties.⁹ Sensitive data, data protection board and authority, and the exemptions to the right to protection of personal data are a few of the other critical differences between the two legal tools.

Protection of "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and health or sex life" of the individuals is set out as special categories of personal data in Directive 95/46/EC. The Law embodies those data with the addition of "appearance and clothing, data relating to criminal records and biometric and genetic data" under the title of sensitive data.¹⁰ The general rule for processing sensitive data in both Directive 95/46/EC and the Law is the explicit consent of the data subject.¹¹ The remarkable difference,

⁹ Gönenç Gürkaynak, İlay Yılmaz and Nazlı Pinar Taskiran, 'Comparison of Turkish Data Protection Law with EU Directive 95/46/EC' (*Mondaq.com*, 2016) <<http://www.mondaq.com/turkey/x/486152/data+protection/Comparison+Of+Turkish+Data+Protection+Law+With+EU+Directive+9546EC>> accessed 26 February 2017.

¹⁰ *ibid*

¹¹ Çelik and Karaduman (n 7)

which can cause concerns, is that while the Directive formed detailed provisions for processing sensitive data without consent, the Law does not ask for consent where it is stipulated by laws¹².¹³

Another difference is the formation, structure and in particular the independence of the DPA of. Directive 95/46/EC obliges Member States to provide independent supervisory authorities. Member States shall provide certain margin of discretion to the supervisory authorities to function with complete independence as one of the main elements for effective protection of personal data.

¹⁴ ¹⁵ The Data Protection Board (hereafter: Board) is, under the Law, composed of nine members. Two members of the Board will be appointed by the Council of Minister, two members will be appointed by the President, and five members will be appointed by quorum of decision by *Türkiye Büyük Millet Meclisi* (Turkish Grand National Assembly, hereafter: TGNA). The Board is entrusted with critical duties, such as ensuring that personal data is processed in accordance with fundamental rights and freedoms, resolving the complaints of data subjects who claim their rights

¹² *In the current political situation in Turkey, the state of emergency was extended and delegated legislations are keep enacted by the Turkish Parliament. So, now it is easier than before to enact a delegated legislation to process sensitive data without the consent of data subject. Also, an official document penned by the Istanbul Provincial Education Directorate has revealed that Turkey's population administration system has been recording minorities in Turkey, who have Armenian, Jewish or Anatolian Greek (Rum) origins with race codes without any reason. Hürriyet Daily News, 'Minorities in Turkey Tagged By 'Race Codes,' Official Document Reveals' (2013) <<http://www.hurriyetdailynews.com/minorities-in-turkey-tagged-by-race-codes-official-document-reveals.aspx?pageID=238&nID=51849>> accessed 9 June 2016. and 'Turkish Court Issues an Injunction Against*

The Ministry of Education's Refusal to Enroll a Child to an Armenian School' (ochrance.cz, 2014) <http://www.ochrance.cz/fileadmin/user_upload/DISKRIMINACE/aktuality/TR-40-Turkish_court_issues_injunction_against_the_Ministry_of_Education_s_refusal_to_enroll_a_child_to_an_Armenian_school.pdf> accessed 9 June 2016.)

Recording those sensitive data of the citizens without reason can raise the question of what can happen during the state of emergency period.

¹³ Gürkaynak, Yılmaz, Taşkıran (n 9)

¹⁴ *ibid*

¹⁵ The Court stressed in *European Commission v. Federal Republic of Germany* case that "the supervisory authorities are 'the guardians' of rights related to personal data processing ensured in the directive and that their establishment in the Member States is thus considered "as an essential component of the protection of individuals with regard to the processing of personal data".¹⁵ The CJEU also found that the meaning of 'complete independence' should be interpreted in light of the independence of the EDPS as defined in the EU Institutions Data Protection Regulation. As underlined by the Court, Article 44 (2) thereof clarifies the concept of independence by adding that, in the performance of its duties, the EDPS may neither seek nor take instructions from anybody. This rules out state supervision of an independent data protection supervisory authority. (Case C – 518/07 *European Commission v. Federal Republic of Germany* [2010])

have been violated, or determining adequate safeguards to process sensitive data. The obligations of the Board are critical because they should work like an oversight mechanism to ensure the data subjects enjoy their right to protection of personal data. Therefore, there are concerns on the formation of the Board. The formation may create a political dependency, and this may undermine principles of fairness and transparency.¹⁶ Also in the report on Turkey of the European Commission, the need for “an independent data protection authority in line with European standards” was underlined.¹⁷

Another significant concern about the Law is the exception with regard to “the issue of ‘preventive, protective and intelligence-related activities’ and cases of ‘national security’”¹⁸. None of the provisions of the Law shall apply if the processing of personal data by a public institution or organization is carried out within the scope of preventive, protective, and intelligence-related activities for providing national security. There is no limit to the exception, such as restricting the data subject’s right to access to his/her own data with regard to national security. Contrarily, the exemption is broad and ambiguous. The identity, type and nature of the public institution or organization is not determined. Moreover, the Law provides no description with regard to national security. The vagueness of the national security description and the general structure of the exemption may cause a broad scope of application and abuse of the national security exception.¹⁹

The national security topic is not in within the scope of Directive 95/46/EC; model legal tool for the Law makes an exception in cases of national security and preventive actions by giving room to Member States to adopt legal measures to restrict the right to protection of personal data to safeguard national security.²⁰ However, it also sets a limit for the Member States’ interference

¹⁶ Akin Ünver and Grace Kim, ‘Data Privacy and Surveillance in Turkey: An Assessment of the Draft Law on the Protection of Personal Data’, (2016) EDAM Cyber Policy Paper Series 2

¹⁷ Commission, ‘Turkey 2015 Report’ (Communication) COM (2015) 611 Final, 62

¹⁸ *ibid*

¹⁹ Ünver and Kim (n 16)

²⁰ Directive 95/46/EC Article 13

to the right to protection of personal data, while giving them the permission to restrict the right. Additionally, Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (hereafter: GDPR) which will abolish Directive 95/46/EC on May 2018, also empowers the Member States to restrict the right on such grounds as well.²¹ As an important point, both legislations, the Directive 95/46/EC and GDPR, seek the restriction to the right to protection of personal data to be proportionate and necessary in a democratic society.

Privacy and data protection started to become more visible after information technologies started to enter lives of individuals'.²² Data are commonly understood to be the raw material produced by abstracting the world into categories, measures, and other representational forms—numbers, characters, symbols, images, sounds, electromagnetic waves, bits—that constitute the building blocks from which information and knowledge are created.²³ When data protection first came to light, the baseline risk was the State. When technology, and computers, brought in the bureaucratic process, public authorities begin to proceed with surveillance of citizens. During the 1980s, when technology was more developed and became affordable, the private sector began to use personal data for commercial purposes, which caused massive processing of personal data. Furthermore, terms such as profiling and data mining were acknowledged in this period.²⁴

After the terror actions, which started with and increased after 9/11, focus on the private sector shifted again to the State. Because of the attacks, the State began to use data processing to combat terrorism, and since then, personal data have been intensively processed by public

²¹ GDPR Article 23

²² Paul de Hert and Serge Gutwirth, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in E. CLAES, A. DUFF & S. GUTWIRTH (eds.), *Privacy and the criminal law*, Antwerp/Oxford, Intersentia, 2006, 61-104

²³ Rob Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences* (1st edn, Sage Publications 2014) 1.

²⁴ Paul de Hert and Vagelis Papakonstantinou, 'The Data Protection Framework Decision of 27 November 2008 Regarding Police and Judicial Cooperation In Criminal Matters – A Modest Achievement However Not The Improvement Some Have Hoped For' (2009) 25 *Computer Law & Security Review*.

authorities due to security purposes.²⁵ Moreover, public and national security policies have been extended and put privacy under pressure.²⁶ Governments usually show a tendency to put national security interest of the countries in front of the fundamental rights of their citizens. The provisions on the restrictions to the protection of personal data with regard to the national security in the Law, Directive 95/46/EC, and GDPR are examples of such tendency. Furthermore, “terrorism and the threat of terrorism is increasingly being used as a reason to justify intrusions and limit privacy. States are using terrorism to justify the limitation and, at times, the total restriction or abrogation of fundamental rights.”²⁷ However, if there is interference to the fundamental rights of the individuals regarding the national security, the interference should be balanced with the human rights. Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (hereafter: ECHR), legislates the right to respect private and family life, and the European Court of Human Rights regards the protection of personal data as a fundamental human right in its jurisdiction.²⁸ This article underlines, everyone has the right to respect his/her private and family lives, and public authorities shall not interfere in the right, unless it is in accordance with law and necessary in a democratic society in the interest of national security, public safety, etc. Thus, the scope of application of the national security exception in the Law should have a limit as well. Since the right of protection of personal data and the right to privacy of the citizens are fundamental human rights, not only they should be taken into consideration, but also they should be balanced with the national security interest.

1.2 Significance

In recent years, Turkey has been dealing with both politically and socially difficult issues, such as terror attacks and explosions that caused the death of many civilians in addition to

²⁵ de Hert and Papakonstantinou (n 24)

²⁶ de Hert and Gutwirth (n 22)

²⁷ Jeremy Sarkin, 'balancing National Security and Human Rights: International and Domestic Standards Applying to Terrorism and Freedom of Speech' (southernafiralitigationcentre.org) <<http://www.southernafiralitigationcentre.org/1/wp-content/uploads/2017/01/GOAL-16-Book-Sarkin.pdf>> accessed 28 February 2017.

²⁸ *Handbook On European Data Protection Law (1st edn, Publications Office of the European Union 2014)*

significant number security personnel.^{29 30} As a result, combating terrorism, and national security in general, has become more sensitive than ever.³¹ With the ongoing terror attacks and lastly, with the coup attempt of summer 2016, the Turkish government set the alarm bells ringing with regard to the national security defense. The Parliament gave broad authority to the police and National Intelligence Agency to processing personal data, backed by the suspension of constitutional fundamental rights with the deceleration of state of emergency.

Protection of privacy and personal data, as a human right, is in the middle of the on-going national security measures of Turkey. Processing data has serious ties with providing national security in the case of terror attacks. Since the Law on Protection of Personal Data came into force recently, national security is a hot topic and data is gaining importance day by day, it is important to pay attention to the topic. The lack of a specific description of the national security as a legal term is a problem. Additionally, it should be taken into consideration that the Turkish government may use the ongoing terror problem as an excuse for interpreting the national security exception in a wide extent.³² Since the Law was enacted, how the private sector can comply with the Law is mostly being discussed. According to this thesis, how to redress the balance between the right to protection of personal data interest of the citizens and national security interest of the state should be discussed as well.

²⁹ “Two powerful bombs exploded at a peace rally near the main train station in Ankara on Saturday morning, killing at least 95 people and wounding 246 others in the deadliest attack in the Turkish capital in recent memory.” Don Melvin, ‘At least 95 killed in twin bombings near train station in Turkey’s capital’ *CNN* (2015) <<http://edition.cnn.com/2015/10/10/middleeast/turkey-ankara-bomb-blast/>> accessed 29 April 2016.

³⁰ “An explosion believed to have been caused by a suicide bomber has hit the popular Istiklal Street in central Istanbul’s Taksim square area. Government officials said at least five people were killed and 36 were injured – seven seriously – in Saturday morning’s explosion.” Aljazeera, ‘Istanbul Bombing: At Least Five Killed in Turkish City’ (2016) <<http://www.aljazeera.com/news/2016/03/istanbul-taksim-square-area-hit-explosion-160319091702737.html>> accessed 29 April 2016.

³¹ Zygmunt Bauman and others, ‘After Snowden: Rethinking the Impact of Surveillance’ (2014) 8 *International Political Sociology*.

³² Barçın Yinanç, ‘Turkey’s Data Protection Draft Law Open to Abuse: Expert’ *Hürriyet Daily News* (2016) <<http://www.hurriyetdailynews.com/turkeys-data-protection-draft-law-open-to-abuse-expert.aspx?pageID=238&nID=95796&NewsCatID=341>> accessed 29 April 2016.

On the other hand, the EU already has a reform on data protection rules. The sample legal tool for the Law, Directive 95/46/EC, will be annulled by a more comprehensive document, GDPR, and there will be a separate legal tool, a directive, for the field of police and criminal justice. As a result, the Law will fall short and be outdated considering the new provisions within the EU. Therefore, the government should start working on reforms on the data protection law and should find the balance between right to protection of personal data and national security.

1.3 Research Question

The lack of legal analysis of the Law on Protection of Personal Data from the right to protection of personal data—as a human right—point of view with regard to national security exceptions, considering the Turkish government’s way of use of personal data by public institutions without ensuring the security of data, encouraged me to research this topic in light of EU data protection regime on the basis of the following research questions:

How could Turkish law be improved to better balance the right to protection of personal data against national security? Furthermore, how shall exception for the purposes of national security be brought more in compliance with EU regulations to prevent the abuse of such exceptions?

Accordingly, the sub-questions are as follows:

1. How did Turkish legislation handle data protection issues before the new Law? Were there any legal tools that regulated protection of personal data before the Law?
2. What are the general provisions in the Law? How is the national security exception formed in the Law? What is the scope of the exception?
3. What may be the true—and data protection-compatible— meaning of the term national security? What does national security mean for Turkey and the EU? How is the national security exception formed in Directive 95/46/EC?
4. What are the measures of the ECtHR and the Turkish Constitutional Court for balancing fundamental rights and freedoms against the State?

1.4 Methodology

To answer the questions above, general desk research was conducted based on specific case law both in Turkey and ECtHR. Journals, books, working papers, etc. were consulted to gain a deeper understanding of the new data protection law of Turkey, the concept of the national security in both Turkey and the EU, and how they treat the right to protection of data against a national security threat. The Law on the Personal Data Protection was used as the main source of Turkish legislation. For the EU legislation, Directive 95/46/EC was mainly used as the law of origin. Also, Directive on the Protection of Natural Persons with Regard to Processing of Personal Data (hereafter: Police and Criminal Justice Data Protection Directive) and GDPR were considered since they are the upcoming legislative tools in the EU with regard to the protection of personal data. In addition, ECHR, the Charter of Fundamental Rights of the European Union (hereafter: Charter), and Convention 108 were other sources used in the research. Furthermore, European Commission communications, opinions of two important actors in the European Union with regard to data protection, European Union Data Protection Supervisor, and Article 29 Working Party were used. To explain the situation to an audience without a background in Turkish politics, news articles are used introduce and explain certain events and issues. Lastly, cases of ECtHR and Turkish Constitutional Court were analyzed.

1.5 Structure of the Thesis

This thesis consists of five chapters. The current chapter is an introduction to the new Turkish Law on protection of personal data. The reasons triggering the process of enacting the Law were explained. General background information on the legal condition before the Law with regard to the protection of personal data was given. Further, the significant differences according to the writer of the thesis, between the Law and Directive 95/46/EC—the model legal source of the Law—were explained. The reason for concerns about the national security exception to the right to protection of personal data, was elaborated to give the reader a clear understanding on the significance of the topic. Additionally, how personal data started to be used and for what reasons personal data is used by the States was briefly addressed. The second chapter will start with the analysis of the Turkish law before 2016 in the absence of a proper Data Protection law. The general

and sector-specific statutes will be mentioned. After explaining the Turkish legal landscape before the Law, the provisions in the Law will be explained, and on certain points, brief comparisons with Directive 95/46/EC will be provided. Further, the national security clause will be explained, and the scope of the national security exception will be discussed. Thereafter, the third chapter will further elaborate on the topic of national security. The national security definition will be analyzed. After that, significance of the national security in Turkey will be explained, and the provisions with regard to national security in the Turkish Constitution will be analyzed. Within this context, two judgments of the Turkish Constitutional Court will be used to explain the different approaches to national security and, therefore, the different approaches to restricting the fundamental rights and freedoms against the national security concerns. Following, the national security concept and the national security exception in the EU will be analyzed. Disparities with regard to the national security exception between Directive 95/46/EC and the Law will be mentioned. Lastly, the ECtHR and the Turkish Constitutional Court approaches to redressing the balance between the national security interest of the state and the right to protection of personal data of the individual will be compared. The fourth chapter is reserved for further analysis and synthesis. The findings of the previous chapters, will be evaluated to assess whether there exists a solution to balance right to protection of personal data and national security, or can improvements be made in the Law to balance right to protection of personal data and national security. Lastly, the fifth chapter will provide an overall conclusion and an answer to the overall research question.

2. General Review of the Law and the Turkish Legislation before the Law

2.1 Turkish Legal Landscape before the Law

As mentioned in the first chapter, before the Law dated 2016 on the Protection of Personal Data, there was no specific and harmonized data protection law in the Turkish legal system. Even the term of personal data was not described under any Turkish laws. The jurisprudence of ECtHR was taken as a basis for the definition of personal data.³³ In the absence of a specific legal tool for data protection, the Constitution of Republic of Turkey (hereafter: Constitution)³⁴ and a few other laws contained general provisions with regard to the protection of personal data. In addition, sector-specific provisions were applied to the topic as well.³⁵ The right to protection of personal data is protected under the Constitution as a fundamental right. Civil Code³⁶, Criminal Code³⁷, Code of Obligations³⁸, Labor Law³⁹, and Law on the Right to Access Information⁴⁰ are the general

³³ Hande Hamevi and Gary Lachman, 'Data Protection Laws in Turkey' (*Mondaq.com*, 2014) <<http://www.mondaq.com/turkey/x/308428/Data+Protection+Privacy/Data+Protection+Laws+In+Turkey>> accessed 22 May 2016. More citation, in particular, the sources I have mentioned.

³⁴ The Turkish Constitution date 7 November 1982 and numbered 2709 <https://global.tbmm.gov.tr/docs/constitution_en.pdf> accessed 23 May 2016

³⁵ Naz Değirmenci, 'Turkey's First Comprehensive Data Protection Law Comes into Force' (*Inside Privacy*, 2016) <<https://www.insideprivacy.com/data-security/turkeys-first-comprehensive-data-protection-law-comes-into-force/>> accessed 1 March 2017.

³⁶ Civil Code dated 22 November 2001 and numbered 4721, <http://www.tusev.org.tr/usrfiles/files/Turkish_Civil_Code.pdf> accessed 23 May 2016

³⁷ Criminal Code dated 26 September 2004 and numbered 5237, <https://www.unodc.org/res/cld/document/tur/2004/criminal_code_law_no__5237_html/Turkey_Criminal_Code_Law_No._5237_2004.pdf> accessed 23 May 2016

³⁸ Code of Obligations dated 1 January 2011 and numbered 6098

³⁹ Labor Law dated 22 May 2003 and numbered 4857

'Turkish Labor Law' (*Turkishlaborlaw.com*) <<http://turkishlaborlaw.com/turkish-labor-law-no-4857/19-4857-labor-law-english-by-article#2>> accessed 2 March 2017.

⁴⁰ Law on Right to Access Information dated 9 October 2003 and numbered 4982

'Legislation on the Right to Information' (*Bedk.gov.tr*) <http://www.bedk.gov.tr/Yayinlar/LEGISLATION_ON_THE_RIGHT_TO_INFORMATION/index.html> accessed 2 March 2017.

legal tools other than the Constitution that were used for protection of personal data before the new data protection Law of Turkey. Banking Law⁴¹, Debit Cards and Credit Cards Law⁴², Regulation on Internal Systems of Banks⁴³, Electronic Communications Law⁴⁴, Electronic Commerce Law⁴⁵ Basic Law on Health Services, and Statutory Decree on Establishment and Duties of the Ministry of Health and Associated Authorities are the sector-specific provisions on the protection of personal data.⁴⁶

2.1.1 Constitution

Privacy of private life is protected by Article 20 of the Constitution numbered 2709. According to the first paragraph of the Article, everyone has the right to ask for respect for their private and family lives.⁴⁷ The privacy concept begins with The Right to Privacy article of the American scholars Warren and Brandeis, in which they define privacy as the right to be left alone.⁴⁸ This definition identifies privacy as non-interference. Ruth Gavinson identified privacy as a condition of limited accessibility, and this condition is comprised of three elements: secrecy, solitude, and anonymity.⁴⁹ According to Alan Westin's definition, "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others".⁵⁰ This definition is framed in terms of information control. The final and unpopular definition makes a connection between privacy and sensitive or intimate personal information. According to this definition, privacy loss occurs when

⁴¹ Banking Law dated 1 November 2005 and numbered 5411

⁴² Bank Cards and Credit Cards Law dated 22 February 2006 and numbered 5464

⁴³ Regulation on Internal Systems of Banks dated 1 November 2006 and numbered 26333 Official Gazette

⁴⁴ Electronic Communications Law dated 10 November 2008 and numbered 5809

⁴⁵ Electronic Commerce Law dated 5 November 2014 and numbered 6563

⁴⁶ Toksoy, Balkı and Yıldız (n 8)

⁴⁷ Hamevi and Lachman (n 33)

⁴⁸ De Hert and Gutwirth (n 22)

⁴⁹ Lee A Bygrave, 'The Place of Privacy in Data Protection Law' (2001) 24 University of New South Wales Law Journal.

⁵⁰ *ibid* 279

there is a breach of sensitive or intimate personal information.⁵¹ To put it more simply, privacy is a fundamental human right affiliated with autonomy and protection of human dignity.⁵² “It is found in the UN Universal Declarations of Human Rights, 1948 and its legal form is found in the UN International Covenant on Civil and Political Rights, 1966”⁵³; while it is also protected in Article 8 of ECHR. Therefore, it is important to provide a protection to the privacy under the Constitution.

The second paragraph of Article 20 underlines that it is not possible to perform a body search or search and seize private papers and belongings of an individual unless there is a decision duly granted by a judge on the grounds of national security or public order.⁵⁴

With the constitutional amendment of 2010, the right to protection of personal data was included as a fundamental constitutional right. The third paragraph of Article 20, which regulates the protection of personal data, states that the individual has the “right to be informed of, having access to and requesting the correction and deletion of his/her personal data, and to be informed whether these are used in consistency with envisaged objectives”.⁵⁵ According to the paragraph, “Personal data can be processed only in cases envisaged by law or by the person’s explicit consent. The principles and procedures regarding the protection of personal data shall be laid down in law”.

⁵⁶

⁵¹ *ibid* 280

⁵² 'What Is Privacy | Privacy International' (*Privacyinternational.org*)
<<https://www.privacyinternational.org/node/54>> accessed 19 June 2016.

⁵³ Bauman and others (n 31)

⁵⁴ Mehtap Yıldırım Öztürk and Çağdaş Evrim Ergun, 'Data Privacy in Turkish Law | White & Case LLP International Law Firm, Global Law Practice' (*Whitecase.com*, 2011)
<<https://www.whitecase.com/publications/article/data-privacy-turkish-law>> accessed 2 March 2017.

⁵⁵ Amended on 12 September 2010, Act No. 5982

⁵⁶ the Constitution Article 20 (3)

The right to protection of personal data is the right for the person who has concerns about his/her data to decide which data will be shared.⁵⁷ Although there is no article in ECHR to protect the right, ECtHR acknowledges protection of personal data falls under the scope of Article 8 ECHR in its decisions.⁵⁸ Data protection is an extensive term.⁵⁹ Although having a constitutional safeguard is important, a statutory framework on the subject is necessary.

Furthermore, within the scope of Article 21, no domicile may be entered or searched or the property seized therein. These immunities are, including the privacy of private life and the protection of personal data, protected under the Constitution, unless there is a decision duly given by a judge on one or several of the grounds of national security, public order, prevention of crime, protection of public health and public morals, or protection of the rights and freedoms of others, or unless there is a written order of an agency authorized by law in cases where delay is prejudicial, again on these grounds.⁶⁰ However, there is no definition of national security, public order etc. in the Constitution.

Article 90 (6) of the Constitution stresses the importance of lawful application of the international agreements by stating: “international agreements duly put into effect have the force of law.” The paragraph continuous; no appeals to the Constitutional Court by claiming that the international agreements are unconstitutional; and if there is a conflict between international agreements and laws with regard to the same topic, provisions of the international agreements shall be taken into consideration. This article is important to ensure the compliance with Article 8 of the ECHR and the decisions of ECtHR.⁶¹

⁵⁷Yves Poulet, 'Data Protection Legislation: What Is At Stake for Our Society and Democracy?' (2009) 25 Computer Law & Security Review.

⁵⁸ De Hert and Gutwirth (n 22)

⁵⁹ Poulet (n 57)

⁶⁰ Nilgün Başalp, *Kişisel Verilerin Korunması Ve Saklanması* [Protection and Storage of Personal Data] (1st edn, Yetkin Yayınları 2004) 100.

⁶¹ Turkey Henkoğlu, *Bilgi Güvenliği ve Kişisel Verilerin Korunması* [Information security and Protection of Personal Data] (1st edn, 2015).

2.1.2 Civil Code

Turkish Civil Code (hereafter: Civil Code) covers protection of personal data under the title of Protection of Personality in a general manner:⁶² “[Article] does not provide either a comprehensive or *numerous clausus* list in respect of [personality rights] and leaves the matter to the discretion of the courts.”⁶³ The question of whether personal data would be included as an integral part of personality and the ensuing rights as provided under the Civil Code in articles will depend on the judicial precedents on the matter.⁶⁴ Article 23 of the Civil Code states that no person may waive his/her rights and neither the person nor anyone may impose restrictions on his/her freedom contrary to the laws and ethics/morality. Article 24 states that every violation on personal rights is considered unlawful unless the consent of the person whose rights are violated is based on any one of the reasons related to private or public interest and use of authorization conferred upon by the laws. On the other hand, Article 25 addresses civil remedies against the violation of the right.

2.1.3 Criminal Code

Turkish Criminal Code (hereafter: Criminal Code), in its ninth section, under the title of Offences against Private Life and Privacy regulates the protection of privacy and defines the violation of privacy as a crime. Criminal code has a specific provision for protection of personal data. According to Article 135, “Any person who illegally records personal data shall be subject to a penalty of imprisonment for a term of one to three years”. The article also punishes any illegal/unauthorized recording of personal data on “political, philosophical or religious opinions, racial origins; sex lives, health or relations to trade unions” with imprisonment.⁶⁵ Article 136 declares that obtaining, disseminating and giving away an individual’s data through unlawful means is punishable by imprisonment. While Article 137 regulates qualified forms of offense, such

⁶² Hamevi and Lachman (n 33)

⁶³ Gönenç Gürkaynak and İlay Yılmaz, *The privacy, data protection and cybersecurity law review* (1st edn, Gideon Robertson 2014) 242.

⁶⁴ *ibid*

⁶⁵ Criminal Code Article 135

as the offenses defined in the above articles committed by a public officer or due influence based on public office or by exploiting the advantages of a performed profession and art, Article 138 punishes the person who failed to destroy the data after the expiry of legally prescribed period. There is no definition for the term of “illegal recording” in the Criminal Code or in another law, but the term usually is interpreted as any record of personal data without the consent of the data subject.⁶⁶ Also, the Criminal Code does not define what constitutes personal data, so it is necessary to fill this terminological gap. When the preamble of Article 135 is checked, any information related to a natural person is accepted as personal data.⁶⁷

In addition to the explanations above, the Law addresses the Articles 135 to 140 of the Criminal Code with regard to crimes relating to personal data.

2.1.4 Code of Obligations

Article 27, Article 58, and Article 419 of the Code of Obligations⁶⁸ also concern personal data.⁶⁹ Article 27 states that an agreement contrary to personal rights is invalid, and Article 58 regulates civil remedies in case of a violation of a personal right. Article 419 obliges an employer to only use his/her employees’ data with regard to job-related situations.⁷⁰

2.1.5. Other General Provisions

Law on the Right to Access Information, which is applicable to the activities of public authorities, aims to promote the convenient access to information for a natural and legal person.

⁶⁶ Öztürk and Ergun (n 54)

⁶⁷ Rezzan İtişgen 'Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme Suçu' (Offence of Unlawfully Giving or Obtaining of Personal Data in Turkish Criminal Law) (2015) 6 Türkiye Adalet Akademisi Dergisi <<http://www.taa.gov.tr/yayin/turkiye-adalet-akademisi-dergisi-sayi-23/>> accessed 6 February 2017.

⁶⁸ Code of Obligations dated 1 January 2011 and Law no. 6098,

⁶⁹ Toksoy, Balki and Yıldız (n 8)

⁷⁰ *ibid*

Article 21 of the law sets out that personal data and documents can be disclosed only if there is a public interest and the relevant person's written consent exists.

Labor Law, which has a purpose “to regulate the working conditions and work-related rights and obligations of employers and employees working under an employment contract, has a provision on personal data”⁷¹. Article 75 of the law provides that employers are obliged not to disclose information belonging to their employees where employees’ interests require for the information to remain confidential. This provision also sets out that employers should use their employees' personal data in good faith and in accordance with other applicable laws.⁷²

2.1.6 Sector-specific Laws

Banking Law, Debit Cards and Credit Cards Law, and Regulation on Internal Systems of Banks have provisions about protection of personal data, which provides for prison sentences. In addition to these laws and regulations, Electronic Communications Law has a broad scope regarding the processing of personal data and protection of privacy in electronic communications and data traffic. Finally, Electronic Commerce Law holds the Internet Service Provider liable for storing and providing the security of the data, transfer of the data to third parties and use of the data for other purposes without consent of that person.⁷³

“Banking Law Article 73 provides that customers' personal data must be protected and kept confidential by banking personnel. Article 159 states that an administrative fine, as well as a prison sentence (of one to three years), will apply to those who are in breach of this obligation.”⁷⁴

“Pursuant to Article 23 of the [Debit] Cards and Credit Cards Law, member merchants cannot use, store or copy the personal data regarding their customers, which they obtain during the utilization of credit cards or [debit] cards in their [workplace], without written consent of the

⁷¹ Labor Law Article 1 (1)

⁷² *ibid*

⁷³ Toksoy, Balkı and Yıldız (n 8)

⁷⁴ *ibid*

customer. Card issuing institutions are also required to keep such information confidential other than for the purposes of marketing [and provision of] their services. Article 39 of Law on the Debit Cards and Credit Cards provides that violation of such requirements is subject to imprisonment from one to three years as well as an administrative fine.”⁷⁵ Since banks substantially work with customer’s personal data, the need of a statutory framework in the personal data protection scheme alongside of the laws governing the specific subject matter was significant.

“Regulation on Internal Systems of Banks contains the principles that need to be followed by the internal systems of banks, which, among others, concern the infrastructure/software allowing the safe electronic registration, access and use of data. The banks' systems must aim to ensure the compliance of banks with the obligations under both banking legislation and any other laws. The "primary system" refers to the whole system whereas the "secondary system" is a back-up to the primary system. Article 11 provides that Turkish banks are required to maintain their primary and secondary data systems in Turkey. Finally, Article 42 sets out that a data management process must be formed in a way to ensure the data quality, and the consistent and trustworthy supply of such data, as well as its security.”⁷⁶

2.1.7 The Law on Duties and Powers of Police⁷⁷

As a public legal tool, the Law on the Duties and Powers of Police regulates the duties and powers of the law enforcement authorities. Article 5 set rules on registration of fingerprints and photographs. The Article states “Fingerprints and photos stored on the system are deleted from the system after ten years from the date of death of the person and after eighty years from the date of registration.” Additionally, Annex-7 gives police the power to carry out intelligence activities within the country and in the online environment to take preventive and protective measures with regard to the national security.

⁷⁵ Öztürk and Ergun (n 54)

⁷⁶ Toksoy, Balkı and Yıldız (n 8)

⁷⁷ Law on the Duties and Powers of Police dated 14/7/1934 and numbered 2559

Although data protection was formed under constitution, general, and sector-specific provisions, those provisions were inadequate because the background of the laws were not technically sufficient for data protection.⁷⁸ At its simplest, there was not a personal data definition in any of the laws. Therefore, a framework law on the subject was needed.

2.2 The Law on Protection of Personal Data

After a long period of waiting and several drafts, the Law was published in the Official Gazette on 7 April 2016. As mentioned, the EU harmonization process was the main motivation behind this process. The Law is modeled on Directive 95/46/EC, which is the principle legislation on protection of personal data regarding the subjects falling within the scope of Union Law⁷⁹, the Treaty on European Union; it is not applicable to a large extent in the Area of Freedom, Security and Justice, but, according to Article 29 Working Party, its principles are generally applicable in the area of data protection.^{80 81} However, with the reform on data protection in the EU, the new legal tool with regard to the protection of personal data, GDPR, will abolish Directive 95/46/EC and enforce, on 25 May 2018, the harmonization of data privacy law across the EU.⁸² Hence, the Law will fall behind the EU data protection tools, and Turkey will fail to harmonize with the EU with regard to data protection.

⁷⁸ Gökhan Uğur Bağcı, '14 Soruda Kişisel Verilerin Korunması Kanunu – E-Ticaret Ve İnternet Hukuku' (*Eticarethukuku.com*, 2016) <<http://www.eticarethukuku.com/14-soruda-kisisel-verilerin-korunmasi-kanunu>> accessed 3 March 2017.

⁷⁹ Franziska Boehm, 'Confusing Fundamental Rights Protection in Europe: Loopholes in European Fundamental Rights Protection Exemplified On European Data Protection Rules' [2009] SSRN Electronic Journal.

⁸⁰ Article 29 Working Party WP 211 Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector [2104] 2

⁸¹ *The European Union was composed of three pillars from 1993 to 2009. This pattern was introduced by the Treaty of Maastricht on 1 November 1993 and abolished when the Treaty of Lisbon came into operation on 1 December 2009. First, so-called, "Community Pillar" conducted economic, social and environmental politics. The second pillar, the Common Foreign and Security Policy, handled in foreign policy and military issues. Third Pillar, Police and Judicial Co-operation in Criminal Matters, was concerned about fight against the crime. Although the pillar system abolished with the Treaty of Lisbon, the legislations about data protection still distinguish by the pillar system.* Boehm (n 79)

⁸² 'Home Page of EU GDPR' (*EU GDPR Portal*) <<http://www.eugdpr.org/>> accessed 3 March 2017.

“The Law will be implemented during a two-year transitional period; whereby various provisions will enter into force at different times.”⁸³ According to the temporary Article 1, “Personal data that is processed before the date of publication of this Law shall be rendered compliant within two years following the date of publication of this Law.”⁸⁴ The articles on the transfer of personal data to third parties and abroad, the rights of the data subject, application to data controller, complaint to the Board, procedures and principles of inspection, data controllers registry, and crimes and misdemeanors will be effective after six months following the date of publication. Other articles enter into force on the date of publication.

The purpose of the Law is stated in Article 1: “to protect the fundamental rights and freedoms of persons, privacy of personal life in particular, while personal data are processed, and to set forth obligations of natural and legal persons who process personal data and procedures and principles to comply with for the same.” The scope of the Law is stated in Article 2: “natural persons whose personal data are processed and natural or legal persons who process such data wholly or partly by automatic means or otherwise than by automatic means which form part of a filing system.”

The Law introduces definitions of four key players in the Code: “Data Subject”, “Data Controller”, “Data Processor”, and “Data Protection Authority and Data Protection Board” alongside, “Personal Data” and “Special Quality of Personal Data”.⁸⁵ According to Article (3) (1) (ç), a data subject is a natural person whose personal data is processed. The following clause of the Article defines personal data as any information relating to an identified or identifiable natural person. The term Data Controller, defined in the clause (ı) of the Article, is natural or legal person who sets the purpose and means of processing personal data and is responsible for constituting and

⁸³ Değirmenci (n 35)

⁸⁴ Translation by Yusuf Mansur Özer 'Turkish Law on the Protection of Personal Data No. 6698' (*Kişisel Verilerin Korunması*) <<http://www.kisiselverilerinkorunmasi.org/ingilizce-ceviri/#Purpose-Scope-and-Definitions>> accessed 3 March 2017.

⁸⁵ Yusuf Mansur Özer, 'Turkey: A New Era for Data Protection in Turkey - The Law on the Protection of Personal Data Enters into Force' (*mondaq.com*, 2016) <<http://www.mondaq.com/turkey/x/483272/Data+Protection+Privacy/A+New+Era+for+Data+Protection+in+Turkey+The+Law+on+the+Protection+of+Personal+Data+Enters+into+Force>> accessed 24 May 2016.

managing the data recording system. The Data Processor is a natural or legal person who processes the personal data in regard to the authorization given by the Data Controller and on behalf of him/her, as well.⁸⁶ In addition, Data Protection Authority, is a public legal entity which has administrative and financial autonomy, has been established to perform the tasks assigned by the Law on Protection of Personal Data; and its decision making body is Data Protection Board.

While personal data is defined as any information related to an identified or identifiable natural person in Article 3 (d), a special quality of personal data or sensitive data is defined as “Information related to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dressing, membership of association, foundation or trade-union, health, sexual life, criminal conviction and security measures, and biometrics and genetics”⁸⁷ in Article 6. The Law differentiates from Directive 95/46/EC with regard to sensitive data. Article 8 of Directive /95/46/EC states “data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life” are sensitive data. The Law added “appearance and clothing, data relating to criminal records and biometric and genetic data” as sensitive data to the list enumerated in Directive 95/46/EC. By taking into account the requirements of the current technological developments, biometric and genetic data was added to GDPR as sensitive data. Furthermore, the rules on processing personal data relating to criminal convictions was formed in a separate article in GDPR. These improvements in the EU data protection legislation show that the Law may be outdated by taking Directive 95/46/EC as a model. While in the second paragraph of Article 8 of Directive 95/46/EC there are exceptions to the prohibition of processing sensitive data listed in detail, in the Law on the Protection of Personal Data processing can be done in the cases provided by other laws.⁸⁸ The Law does not elaborate what are the other laws, or it does not give a detailed list. The

⁸⁶ *ibid*

⁸⁷ *ibid* (para 15) translation

⁸⁸ To make the term clear, “provided by law” refers to a provision formed in other various laws. For some people, the provided by law term is vague and may give a blank check to the controllers and to the government authorities for profiling citizens. Başalp (n 60)

only requirement for processing of sensitive data is, adequate precautions must be taken by the Board.

The protective measures in the Law are similar to the ones in Directive 95/46/EC.⁸⁹ Article 4 of the Law sets out the principles of data processing. According to the Article, “personal data shall be processed in conformity with the law and in good faith; be accurate and, if necessary, up to date; be processed for specified, explicit, and legitimate purposes; be relevant, limited, and proportionate to the purposes for which data are processed; be stored only for the time designated by relevant legislation or necessitated by the purpose for which data are collected”⁹⁰. The principles set out in Article 6 of Directive 95/46/EC are similar to those in the Law; however, Directive 95/46/EC explained them more in detail.⁹¹

According to the Article 5 of the Law the general condition for processing of personal data is the explicit consent of the data subject. The conditions for processing personal data without explicit consent are regulated in the same article. According to Article 5, processing has to be expressly permitted by the laws, some of which were mentioned in this chapter of the thesis such as the Constitution, the Criminal Code, Banking Law or Electronic Commerce Law etc.⁹² As a result of a criminal investigation by the law enforcement, taking the fingerprints of the suspects in accordance with Article 5 of the Law on the Duties and the Powers of the Police can be shown as an example to processing – without explicit consent – permitted by law. Other conditions for processing personal data without explicit consent are as follows: “processing has to be necessary in order to protect the life or physical integrity of the data subject or another person where the data subject is physically or legally incapable of giving consent; it is necessary to process the personal data of parties of a contract, provided that the processing is directly related to the execution or performance of the contract; it is necessary for compliance with a legal obligation to which the

⁸⁹ Eda Uludere, 'Personal Data Protection under Turkish and European Legislation - Erdem & Erdem' (*Erdem-erdem.av.tr*, 2015) <<http://www.erdem-erdem.av.tr/publications/law-post/personal-data-protection-under-turkish-and-european-legislation/>> accessed 5 March 2017.

⁹⁰ Translation by Özer (n 84)

⁹¹ Uludere (n 89)

⁹² The complete list can be found here: <http://www.kisiselverilerinkorunmasi.org/mevzuat/>

controller is subject; the relevant information is revealed to the public by the data subject herself/himself; it is necessary for the institution, usage, or protection of a right; it is necessary for the legitimate interests of the data controller, provided that the fundamental rights and freedoms of the data subject are not harmed.”⁹³ These conditions for processing are also similar to the criteria for making data processing legitimate, set out in Article 7 of Directive 95/46/EC.

The relationship between Article 6 and Article 7 is strong. One cannot be without the other. In other words, processing of personal data should be done in compliance with processing principles (Article 6) and with a lawful ground (Article 7).⁹⁴ This inference is applicable for the Law, as well. The controllers should apply both articles to their operations.⁹⁵

According to Article 7 of the Law, if the reason(s) for processing the data is eliminated, the personal data must be deleted, destroyed, or anonymized automatically by the data controller or on request by a related person. Therefore, data controllers must use an infrastructure where the reasons for processing data can be regularly monitored and assessed.⁹⁶

The Law also regulates transfer of personal data to third parties or abroad. The general rule for transferring data to third parties or abroad is obtaining the explicit consent of the data subject.⁹⁷ Personal data can be transferred abroad without obtaining the explicit consent of the data subject if additional requirements are present. The additional requirements are the destination country must have an adequate level of protection or both sides of the transfer must commit, in writing, to provide an adequate level of protection, and the approval of the Data Protection Board_must be obtained.⁹⁸

⁹³ Directive 95/46/EC

⁹⁴ Paul de Hert and Vagelis Papakonstantinou, 'The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?' (2016) 32 Computer Law & Security Review 185.

⁹⁵ *ibid*

⁹⁶ Çelik and Karaduman (n 7)

⁹⁷ *ibid*

⁹⁸ Zihni Bilgehan and Yusuf Mansur Ozer, 'ICLG: Data Protection 2016 - Turkey - International Comparative Legal Guides' (*Turkey - Data Protection 2016 - ICLG - International Comparative Legal Guides*,

‘Article [11] fills an important gap in the personal data protection scheme by regulating the rights of a data subject, including the right to request information on whether his/her personal data exists, has been subject to processing, transferred, or correction requested of any personal data, etc.’⁹⁹ The Law also imposes obligation on the controllers. Article 10 obliges the controller to inform the data subject with regard to processing his/her data, such as the information on the controller or processor. Article 12 obliges to the controller and the processor to take all necessary technical and organizational measures for providing an appropriate level of security in order to provide data security.

The sixth chapter of the Code is allocated for Data Protection Authority (hereafter: the Authority) whose decision making body is the Board of Protection of Personal Data.¹⁰⁰ The composition of the Board had changed several times before the Law was enacted by the parliament. It was provided by the first draft on 3 November 2014 that the Board is composed of seven members and the members were appointed by the Cabinet. The Board members of the 2014 version, had been chosen with respect to their technical expertise: two lawyers or judges who had at least ten years of professional experience, one academic member who had at least ten years of experience in higher education institutions, four people who had at least ten years of professional experience in public or private sectors. The period of office of members was two years, and the members whose period of office expired could be reappointed for one more term. In comparison with the first draft, the second draft, dated 4 January 2016, stated the Board also had seven members, but division of the members was different. The Draft provided that four members were to be appointed by the Council of Ministers, three members were to be appointed by the President among the people who had at least ten years of working experience in a public or private sector. The second draft not prescribe any technical expertise while designating the members. Duration of period of office grew from two years to four years and 2nd draft stated that members could be re-elected but did not set a specific term as he did in the first draft. When draft came before the

2016) <<http://iclg.com/practice-areas/data-protection/data-protection-2016/turkey#chaptercontent10>> accessed 5 March 2017.

⁹⁹ Uludere (n 89)

¹⁰⁰ Özer (n 85)

Parliament, changes were made once again before it was enacted. The legislator increased the number of members to nine. Two are appointed by the Cabinet, two by the President, and five by TBMM by simple majority ¹⁰¹. Similar to the second draft, there is no prescribed technical distinction within the designation of the members. In addition, right of re-election is the same as in the second draft. Structure and duties of the Authority and the Board are widely addressed in the sixth chapter of the Law.

Article 28 is the general exception rule of the Law. In the cases of exceptions stated in the Article, the provisions of the Law shall not apply. One of the exceptions is the subject of this thesis: national security exception. Clause (ç¹⁰²) of the Article states “Processing of personal data by the public institutions and organizations authorized by law in terms of preventive, protective and intelligence activities to ensure national defense, national security, public safety, public order, economic security are excluded from the law.” The scope of the national security exception, explained in the preamble of the Law, is as follows:

“The activities of National Intelligence Organization and other intelligence units with regard to the national defense, national security, public security, public order, and economic security are excluded from the scope of the Law. Likewise, activities carried out by the competent authority on the laundering of crime incidents, prevention of terrorist financing and investigation of financial crimes are within the scope of this exemption. [...] Furthermore, the processing of personal data by investigation, prosecution, trial and execution authorities and disciplinary investigation and prosecution authorities in accordance with the provisions of the relevant law is also excluded.”¹⁰³

¹⁰¹ *TGNA is formed from 550 members. Majority party (Adalet ve Kalkınma Partisi/AKP) has 317 members, while other 233 people are divided into other parties.*
<https://www.tbmm.gov.tr/develop/owa/milletvekillerimiz_sd.dagilim> accessed 13 February 2017.

¹⁰² The 4th letter of the Turkish alphabet before after c and before d

¹⁰³ *Kişisel Verilerin Korunması Kanunu Tasarısı (1/541) ve Adalet Komisyonu Raporu No: 117 (The Draft Law on the Protection of Personal Data (1/541) and the Justice Commission Report No: 117)*

As mentioned, the scope of the Law is “natural persons whose personal data are processed and natural or legal persons who process such data wholly or partly by automatic means or otherwise than by automatic means which form part of a filing system”. The preamble states, “There is no distinction between the private sector and the public sector and it is accepted that the envisaged principles and procedures are applied in both sectors”.¹⁰⁴ However, it does not specify whether police and intelligence agency activities are in the scope of the Law. As security and police cooperation matters are outside of the scope of Directive 95/46/EC, model legislation for the Law, what public sector means in the Law is not clear. Since the subject is national security, the National Intelligence Organization or other intelligence units, such as police intelligence, are the authorities that process personal data, as is also mentioned in the preamble of the Law. Therefore, the language of the scope needs to be clearer.

Furthermore, neither national security nor national security exception definitions were given in the Law. The limit of the authorization given to public institutions and organizations by the Law is also vague. National security exception provision in the Law is a general exception clause. Without defining a limit and mentioning which rights are restricted to secure the national security, public institutions and organizations may use the exception in a wide range, which can cause the abuse of the national security exception. For example, in Article 4 of the Law on State Intelligence Services and National Intelligence Organization of Turkey¹⁰⁵, the obligations of the National Intelligence Organization were determined. Clause (i) of the Article states one of the obligations of the NIO is “To collect, record and analyze information, documents, news and data by using all kinds of technical intelligence and human intelligence procedures, tools and systems in foreign intelligence, national security defense, combat against terrorism and international crimes and cyber security issues and to deliver the produced intelligence to necessary institutions”. In addition, the NIO may obtain information, documents, data, and records from the institutions and organizations within the scope of the Banking Law, as well as other legal entities and entities that do not have legal personality and may utilize and make contact with archives, electronic data

¹⁰⁴ *ibid*

¹⁰⁵ Law on State Intelligence Services and National Intelligence Organization 3 November 1983 dated and numbered 2937

processing centers, and communication infrastructure. The provision authorizes the NIO a wide range of tools to work on its duties, and of course, national security defense is one of those duties. Since NIO already has had a limitless authorization to use all kinds of technical intelligence and human intelligence procedures to defend national security, not limiting the national security exceptions in the Law could cause a broad practice of processing personal data by NIO. Another example of the topic is the current amendments to the Law on the Duties and Powers of the Police. As of January 2017, some amendments were made in Annex-6 and Annex-7 of the Law on the Duties and Powers of the Police with the Decree Law 680 within the extraordinary period. This is a current example of the “authorized by law” term of Clause (ç). According to the amendment in Annex-6, police were given the authority to access the identity information of the internet subscriptions and research in the virtual environment during the crimes committed in the virtual environment. Furthermore, police can detect and intercept data transmitted between telecommunication or internet connection and internet resources, and also they can record the signal information with regard to the determined crimes by the amendment of Annex-7. Crimes against the state’s security and crimes against national defense are two of the determined crime categories.¹⁰⁶ With the decree, it was also allowed to monitor the data traffic without the consent of the judge to inform crimes. Everything can be defined as a crime against the state’s security or a crime against national defense without a general and well-defined national security understanding. Therefore, the vague terminology and wide exception of national security in the Law cause concerns with regard to the authorizations given to the public institutions and organizations by other laws.

¹⁰⁶ Hüseyin Gönüllü, 'Kişisel Verilerin Koruması Kanunu Polisi Bağlar Mı? - Xtrlarge' (*xTRlarge*, 2017) <<https://www.xtrlarge.com/2017/01/17/kisisel-verilerin-korumasi-kanunu-polisi-baglar-mi/>> accessed 17 March 2017.

3. National Security and National Security Exception

It is difficult to create a legal definition for the term national security. Although it reminiscent of a purely militaristic concept; it involves political-legal aspects, too.¹⁰⁷ On one hand, the term is political because the scope of national security may change according to the political circumstances of a country and the ideological setting of the regime; on the other hand, the term is legal because it is somehow included in the constitution and in other legal documents such as statutes, governmental decrees, ministerial regulations and etc.¹⁰⁸

“From the academic debate on its definition, two elements of national security can be drawn out. First, in the context of military defense, several academics have highlighted the importance of territorial sovereignty – as monitored internally within a state’s jurisdiction and externally, beyond the state’s borders. [...] The other element [...] is the protection of democratic constitutional values. As will be seen in states’ interpretations, national security has been construed so as to include political and economic ‘interests’ (another ambiguous term) – not only domestically, but worldwide.”¹⁰⁹ Wide interpretation and strict application of national security may harm human rights.

Obviously ‘security’ can cover just about anything: at its broadest, including threats to anything we value as individuals, from our physical survival and wellbeing to our economic welfare, personal relationships and sense of self-worth, and then extends to our collective values as part of a society or group. To have any use for the national security concept, we must reduce the definition to a significant extent and determine how much of the "security" concept should be covered by the "national security idea". While ‘security’ can legitimately contain someone’s

¹⁰⁷ Tayfun Akgüner (1985) 6 İdare Hukuku ve İlimleri Dergisi
<<http://www.journals.istanbul.edu.tr/iuihid/article/view/1023002682>> accessed 7 March 2017.

¹⁰⁸ Rona Aybay, 'Milli Güvenlik Kavramı Ve Milli Güvenlik Kurulu' (1978) 33 Ankara Üniversitesi SBF Dergisi [Concept of National Security and National Security Council (1978) 33 Ankara University Faculty of Political Science Journal].

¹⁰⁹ Donal Kearney, 'What Does “National Security” Actually Mean?' (*Rightsni.org*, 2013)
<http://rightsni.org/2013/05/national-security/#_ftn3> accessed 8 March 2017.

individual emotional wellbeing, ‘national security’ naturally restricts the features of security for which the state might take responsibility.

3.1 National Security and National Security Exceptions in Turkey

Since Turkey has a long history of terror events and separatist conflicts, territorial integrity of the state is crucial; thus, national security has always been on the top of country’s agenda. National security in Turkey, is understood as an immune and inarguable term.¹¹⁰ Domestic terrorism was in the center of attraction of Turkey until the 9/11.¹¹¹ Kurdish segregation and radical Islam was the core reasons of the terrorism in Turkey.¹¹² Kurdistan Worker’s Party (PKK) has been operating its terrorist activities in the eastern and southeastern part of Turkey to demand a separate Kurdish state.¹¹³ In the last years, the terror actions have been hauled to major cities such as the capital, Ankara, and Istanbul. As a radical Islamic terrorist group, Hizballah took action against the secular structure of Turkey. The 9/11 did not influenced Turkey deeply. However, terrorism became a major international problem Currently, the Islamic State of Iraq and al-Shak (ISIS) is an international terror threat for Turkey, along with domestic terror threat, PKK and Kurdistan Freedom Falcons (TAK) a terrorist group which left PKK. Therefore, national security is significant in the political scheme of Turkey.

The endeavor for the national security and the integrity of the community has had a significant role in the constitutional tradition of Turkey.¹¹⁴ “A product of the 12 September 1980 military coup, the 1982 Constitution – nourished with the power generated by the coup; empowered by the legacy of political and administrative structures in Turkey [...] towered over a system of legislation marked by a distinct national security culture. This distinct national security

¹¹⁰ Akgüner (n 107)

¹¹¹ Necla Güney, 'Country Report On Turkey', *Terrorism as a Challenge for National and International Law: Security versus Liberty?* (1st edn, Springer 2004)

¹¹² Ulkumen Rodoplu, Jeffrey Arnold and Gurkan Ersoy, 'Terrorism In Turkey' (2003) 18 *Prehospital and Disaster Medicine*.

¹¹³ *ibid*

¹¹⁴ Güney (n 111)

culture formed the basis of the institutional structures of the state and was further embedded in the administrative system [...].”¹¹⁵ In the 1982 Constitution, national security was a reason to restrict all constitutional human rights. With the 2001 constitutional amendments, the general restriction to the fundamental rights and freedoms were abolished, and a new system was created. In the new system, every right and freedom has a specific and differentiated restriction according to its characteristic. However, restrictions with regard to national security are still preserved in their initial form under some of the articles, and Article 20 privacy of private life is one of them, so restrictions were shifted from general to specific.^{116 117} The issue of how to provide a balance between national security and fundamental rights and freedoms is one of the main points of the national security subject. However, balancing them has usually failed.¹¹⁸

Different dissenting opinions on the *Erdem Gul and Can Dundar* case of the Turkish Constitutional Court, two journalist who reported on the weapons which had been delivering to the rebels in Syria by Turkish National Intelligence Organization¹¹⁹, mentioned that the term national security is a subjective topic by its very nature. The meaning that the country imposes on the concept of security is under the influence of different circumstances unique to that country. For this reason, according to the constitutional court, the ECtHR does not take the concept of national security absolutely into consideration and does not ignore the countries' own positions, leaving a wide margin of appreciation to the national authorities. However, in doing so, it sets a minimum limit and imposes on the state the proving of the right to intervene in the fundamental

¹¹⁵Hale Akay, *Security Sector In Turkey* (1st edn, TESEV Publications 2010).

¹¹⁶ Bulut Gürpınar, '1982 Anayasası'na Göre Milli Güvenlik Kavramı' [2012] Hasan Kalyoncu Üniversitesi Hukuk Fakültesi Dergisi. (National Security Concept according to 1982 Constitution)

¹¹⁷ *Other constitutional rights which have national security restrictions: Inviolability of the domicile (Article 21) Freedom of communication (Article 22), freedom of expression and dissemination of thought (Article 26), Freedom of the press (Article 28), Right to use media other than the press owned by public corporations (Article 31), the freedom to establish associations (Article 33), Right to hold meetings and demonstration marches (Article 34), Right to organize unions (Article 51) Professional organizations having the characteristics of public institutions (Article 135)*

¹¹⁸ Akgüner (n 107)

¹¹⁹ 'The Case Of Journalists Can Dünder and Erdem Gül - Global Freedom Of Expression' (*Global Freedom of Expression*) <<https://globalfreedomofexpression.columbia.edu/cases/case-journalists-can-dunder-erdem-gul/>> accessed 23 March 2017.

rights and freedoms by reason of national security.¹²⁰ Giving a broad discretion to the state to interfere in the rights and freedoms for the national security may not be a neutral approach. It goes without saying that national security is an increasingly sensitive topic for Turkey, considering its historical background and geographic location and the recent terror events. However, “human rights might become a collateral damage of the war against [national security threats]”¹²¹, and this should be prevented. The Constitutional Court has other judgments, which place importance on the sensibility of the fundamental rights and puts them prior to national security. In the judgments the Court asserted the contrary of the dissenting opinions mentioned above. It stated the term national security is a general concept that will lead to diverse and gradual applications, which can be expanded according to the personal opinions and understandings of the administration, open to subjective interpretations and, therefore, reaching arbitrariness.¹²² Exercise of a fundamental right, in order to be seen as a threat to national security, must reveal serious threats to the state and the state's security. For example, if the exercise of the right to access data subject's own data would disclose critical information on an ongoing investigation regarding to a terror issue, it can be seen as a threat to national security.¹²³

The law on Protection of Personal Data has an ambiguous national security exception clause. The legislator did not draw a framework for the exception. To what extent the authorized public institutions and organizations can process personal data is not clear. This vagueness may cause “subjective interpretations” of the concept as it underlined by the Constitutional Court, as well. Since the increasing terror attacks over the last years and the coup attempt of summer 2016, national security is more important than ever. Mentioned before, with the amendments to the Law on the Duties and Powers of the Police, police can access the identity information of internet subscriptions and can monitor the data traffic without the consent of a judge. This practice may disclose sensitive data of the individuals and harm their right to protection of personal data and the

¹²⁰ Anayasa Mahkemesi (Constitutional Court) 27/2/2016 T. Application no: 2015/18567

¹²¹ Güney (n 111) 51

¹²² Anayasa Mahkemesi (Constitutional Court) 25/4/1974 T. 1973/41 E. 1974/13 K.

¹²³ Anayasa Mahkemesi (Constitutional Court) Kristal-İş Sendikası Başvurusu 2/7/2015 T. Application No 2014/12166

right to privacy. There is no guarantee of the authorization to access identity information of people and to watch their data traffic will not be abused by the police. Processing the data of the whole population based on criminal suspicion about certain individuals is not a balanced and fair procedure. European Commission report on Turkey explains principle of separation of powers and human rights is not always respected in Turkey, while national security interest of the state is deemed high.¹²⁴ Therefore, the national security exception clause in the Law should be reshaped to avoid any broad interpretations and applications.

3.2 The Scope of National Security in the EU

There are two different opinions on the missions of the European Union. First opinion declares, there is no separation between the missions of the EU, such as military missions and civilian missions.¹²⁵ These military elements and civilian elements are combined in the EU missions. On the other hand, according to second opinion, the EU's attitude toward political issues "is based on civilian power rather than military, which uses soft security rather than hard security."¹²⁶ "European security includes the strengthening of democracy, respect for human rights and the rights of national minorities, socio-economic welfare, and environmental protection. In relation to these values, the EU has emerged as a civilian actor in domestic and external policies."

¹²⁷

Prior to the 9/11, the EU did not have significant attitude towards counter-terrorism. The 9/11 was a wake-up call for the EU states to be aware of the external terrorism threats. After the bombings in Madrid in 2004 and in London in 2005, the EU started to take the threat of terrorism

¹²⁴ *In the report, it is said that Turkey has failed to respect the principle of separation of powers, the protection of human rights, and fundamental freedoms and independence of judicial system; therefore, judges and prosecutors deal with strong political pressure. The report continued, "In the absence of progress in this field, the existing legislation on the National Intelligence Service and the amended internet law, which grant wide powers to the National Intelligence Service and the Telecommunications Communication Presidency, continue to raise concerns".* Commission (n 17)

¹²⁵ Jolyon Howorth, *Security and Defense Policy in the European Union* (1st edn, Palgrave Macmillan 2014).

¹²⁶ Çiğdem Üstün, *Turkey And European Security Defence Policy* (1st edn, IB Tauris 2014).

¹²⁷ *ibid*

serious, and counter-terrorism has become one of the critical topics for the EU. For example, on March 2004, the European Council adopted the Declaration on Combating Terrorism which focused on cooperation between the national authorities of Member States, and Justice and Home Affairs bodies.¹²⁸ In the recent years, ISIS bombings in Brussels and Paris has kept the tension of terror threat alive. As a consequence of the unique approaches on national security, decisions on national security and defense of the states is left to Member States.¹²⁹ “Member states are the pillars of European counter-terrorism and national authorities still do the lion’s share of the counter-terror work in practice.”¹³⁰

The term of national security and the limits of national security exception are also unclear in the EU. “There is no uniform understanding of ‘national security’ across the EU. The concept is not further defined in EU legislation or in CJEU case law, although the CJEU has stated that exceptions to fundamental rights must be interpreted narrowly and justified.”¹³¹ Article 4 (2) of the Treaty on European Union states that the Union shall respect Member States’ safeguarding national security. Hence, processing of personal data for national security reasons is left outside from the scope of Directive 95/46/EC and from the other data protection legislations of the EU. Since the national security subject has a natural connection with police, there is a debate with regard to the scope of the Police and Criminal Justice Data Protection Directive, which worth mentioning.

The background of the Police and Criminal Justice Data Protection Directive is the Council Framework Decision 2008/977/JHA. Its aim is extending the application limits of the Council Framework Decision, increasing the level of data protection safeguards and harmonizing provisions of EU Member States of personal data processing in the field of police and criminal

¹²⁸ Javier Argomaniz, ‘Post 9/11 Institutionalization of European Union Counter-terrorism: Emergence, Acceleration and Inertia’ (2009) 18 *European Security*

¹²⁹ Howorth (n 125)

¹³⁰ Argomaniz (n 128)

¹³¹ FRA (European Union Agency for Fundamental Rights), ‘Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU’ (2015)

justice.¹³² Article 2 (3) (a) states the Police and Criminal Justice Data Protection Directive does not apply to the processing of personal data in the course of an activity that falls outside of the scope of Union law; by the Union institutions, bodies, offices and agencies. Recital 14 enumerates the activities that fall outside of the scope of Union law: activities concerning national security, activities of agencies or units dealing with national security issues, and the processing of personal data by the Member States when carrying out activities that fall within the scope of Chapter 2 of Title V of the Treaty on European Union (TEU).¹³³ Practices in these areas parts are left to the Member States. However, “the safeguarding against and the prevention of threats to public security” counts as the objectives of the Police and Criminal Justice Data Protection Directive in the Article (1) (1), which is contrary to activities counted in Recital 14. The idea of activities concerning national security can be easily interpreted as it contains the safeguards against and the prevention of threats to public security.¹³⁴ Briefly, there is no common ground for national security in the EU, as the EU has a civilian and moderate policy, and every Member State has its own approach to the term national security. Therefore, lack of a specific national security definition in the EU can cause interpretation problems; however, CJEU determined national security exceptions should be interpreted narrowly and justified.

3.3 Balancing the National Security Interest and Right to Protection of Personal Data within the EU and Turkey

National security exemption under the Law on Protection of Personal Data differs from Directive 95/46/EC, as the processing of personal data does not come within the scope of the Directive if it is carried out for the purposes of public security, defense, or national security.¹³⁵

These topics are responsibility of Member

¹³² Paul de Hert and Vagelis Papakonstantinou, 'The New Police and Criminal Justice Data Protection Directive a First Analysis' (2016) 7 New Journal of Criminal Law 8-10.

¹³³ The Police and Criminal Justice Data Protection Directive Recital 14

¹³⁴ Costanza Di Francesco Maesa, 'Balance Between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for Data Protection in the Police and Justice Sectors and the Directive 2016/681 on the Use of Passenger Name Record (PNR)' [2016] 3(2) Eurojus.it 5

¹³⁵ Preamble 16 of the Directive 95/46/EC

States according to the TEU Article 4 (2). Article 13 of Directive 95/46/EC permits Member States, regarding the legislative measures they adopt, to restrict the scope of obligations and right to protection of personal data in their national law to safeguard national security.¹³⁶ Another difference between Turkish Law and Directive 95/46/EC is the limits that were set in Article 13. The Article limits the restriction of the obligations and rights in two ways. First, the rights and obligations which Member States can restrict are designated in the Directive. The restriction to the scope of rights and obligations does not contain the entire provisions of the Directive. Those designated rights and obligations are the principles of processing data, information to be given to the data subject, data subject's right of access to his/her own data, and publicizing or processing operations. Second, the article underlines the scope of obligations and rights can only be restricted when such restriction constitutes necessary measures to safeguard national security, so Directive 95/46/EC does not grant a broad and ambiguous grounds for limiting the right to protection of personal data with regard to national security, to the Member States. Briefly, the extent of the restriction to the protection of personal data is, necessary to safeguard national security. Directive 95/46/EC balances the national security exception with the necessity. On the contrary, the national security exception contains the entire obligations and rights regarding protection of personal data in the Law, and there is no such a limit to the restriction as it is in Directive 95/46/EC. National security exception in the Law is broad and open to any kind of interpretation.

Balancing the national security interest of the States and right to protection of personal data interest of the citizens is made through a proportionality test in the EU. The proportionality test is performed in the light of the EU Charter and ECHR. As mentioned in previous chapters. ECHR regulates the right to respect private and family life, and ECtHR accepts personal data as a part of privacy in its jurisprudence. Alongside the unity of the internal market in the EU, to provide unity from social aspects, the charter was issued in the EU in 2000. It became legally binding after the Lisbon Treaty entered into force.¹³⁷ The right to respect privacy and family life and right to

¹³⁶ *Handbook On European Data Protection Law* (n 28)

¹³⁷ Elena Butti, 'The Roles and Relationship between the Two European Courts in Post-Lisbon EU Human Rights Protection' (*Jurist.org*, 2013) <<http://www.jurist.org/dataline/2013/09/elena-butti-lisbon-treaty.php>> accessed 6 September 2016.

protection of personal data is separated in the Charter. In Article 8 of the Charter, a definition for personal data was formed.¹³⁸ Lawful limitations and justified interferences under the EU Charter Article 52(1) and requirements of justified interference under ECHR Article 8(2) state criteria for interfering in the right. The interference is lawful only if it is in accordance with law, pursues a legitimate purpose, and is necessary in a democratic society in order to achieve the legitimate purpose.¹³⁹ The proportionality test can be seen in the *Rotaru v Romania* judgment of ECtHR. The Court found that the Romanian law rules providing that information affecting national security may be gathered, recorded, and archived in secret files did not afford a sufficient degree of foreseeability. The holding and use by Romanian Intelligence Service of information on the applicant's private life were, therefore, not in accordance with the law, so that Article 8 was violated. The court also stated that the interference with the applicants right did not pursued a legitimate aim, and also, the interference was not necessary in a democratic society. The court concluded “the interest of a State in protecting its national security must be balanced against the seriousness of the interference with an applicant's right to respect for his or her private life. Our Court has repeatedly stressed the risk that a system of secret surveillance for the protection of national security poses of undermining or even destroying democracy on the ground of defending it.”¹⁴⁰ In particular, the “necessary in a democratic society” aspect is crucial in the three criteria. Article 29 Working Party stressed that ECtHR found violation of Article 8 due to the interference does not meet the criteria “necessary in a democratic society”, even though the interference pursues a legitimate purpose.¹⁴¹ The proportionality test became a standard of the ECtHR jurisprudence; the scope of the national security term was narrowed in the light of the standards, and the CJEU reminds Member States that they have international obligations under the ECHR.¹⁴²

The Council of Europe’s legal tool on protection of personal data, Convention 108, of which Turkey is one of the signatories, has a provision on exceptions to protection of personal

¹³⁸ Handbook on European Data Protection Law (n 28) 20

¹³⁹ *ibid*

¹⁴⁰ [*Rotaru v Romania*](#) App no 28341/95 (ECtHR, 4 May 2000)

¹⁴¹ Article 29 Working Party WP 211 (n 80)

¹⁴² FRA (n 131) 9-11

data. The Convention is applied to both private and public sectors and both offline and online worlds.¹⁴³ Article 9 of the Convention states that processing of personal data be permitted by the national law of the Party, and it should be necessary in democratic society in the interest of protecting State security, public safety, the monetary interests of the State, or the suppression of criminal offences or protecting the data subject or the rights and freedoms of others. So, “necessary in the democratic society” is the limit of interference to right to protection of personal data. The Convention 108 redresses the balance between national security interest of the state and right to protection of personal data of the individual with the necessary in the democratic society requirement.

Article 13 of the Turkish Constitution forms restrictions of fundamental rights and freedoms. According to the Article, fundamental rights and freedoms may be restricted only by law and in conformity with the reasons mentioned in the relevant articles of the Constitution, and the restrictions have to be necessary in a democratic society and in conformity with the principle of proportionality. Reasons to restrict right to protection of personal data is set in Article 20 (3) of the Constitution, which was mentioned before.

In a dissenting opinion of the Turkish Constitutional Court regarding an objection to the processing of biometric data to benefit from healthcare services, processing of biometric data was not provided as proportionate measure and necessary in a democratic society.¹⁴⁴ The necessary in a democratic society principle should be understood as pluralism, tolerance, and open mindedness. The principle of proportionality reflects the relationship between the purpose of restriction (to the right) and the means used to achieve this purpose. Principle of proportionality is comprised of sub-principles, such as convenience, necessity, and proportionality.¹⁴⁵ As a result of developments in information technologies, the capability to gather and store large numbers of data, requires a higher

¹⁴³ Jörg Polakiewicz, 'International Data Protection Conference Convention 108 As A Global Privacy Standard?' (*coe.int*, 2011)
<<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806b294e>> accessed 7 October 2016.

¹⁴⁴ Anayasa Mahkemesi (Constitutional Court) 19/3/2015 T. 2014/180 E. 2015/30 K.

¹⁴⁵ Anayasa Mahkemesi (Constitutional Court) 27/5/2015 T. 2014/176 E. 2015/53 K.

level of protection of personal data. Thus, protection of personal data is provided as a fundamental right under the Constitution, and the right to protection of personal data is protected against discretionary interventions by public authorities.¹⁴⁶ This protection is ensured by the proportionality principle and the necessary in a democratic society measure. Indeed, processing personal data for national security and healthcare services has considerable disparity. National security is a legitimate reason to interfere the the right to protection of personal data, however the right should be restricted proportionately and when it is necessary in a democratic society, as it declared in the opinion.

The intervention to the right has to be in accordance with law, pursue a legitimate purpose, and be necessary in a democratic society in order to be lawful. To be necessary in a democratic society is the most important point both in the EU and in Turkish jurisdiction. Directive 95/46/EC states that interference has to be necessary, as does the Turkish Constitution. To interfere to a fundamental right, in the case of the thesis protection of personal data, with regard to national security, there should be a serious threat against the state and the country. Also, the interference has to be proportionate, and reasonable measures have to be chosen against the threat. The Law does not provide requirements to justify the interference to the right to protection of personal data in its national security exception clause. However, necessary in a democratic society requirement should be taken as a minimum limit to the interference, proportionality should always be taken into consideration, and readjustment should be done to the Data protection and national security in Turkish law, which is the core of the thesis is very brief.

¹⁴⁶ Constitutional Court (n 144)

4. Analysis

The importance of national security for the countries is undeniable. It is understandable that countries want to use every method to keep themselves safe against national security threats. However, there should be a logical balance between human rights and the countries' perception of national security interests. Since national security is a special and delicate subject also on the European level, bringing a straightforward answer to the main question of this thesis—which is to find a solution to balance national security interest and the right to protection of data in the Turkish data protection law— is difficult. To create the balance, one should be able to understand what national security is, as well as the limit of national security exceptions.

A national security definition is missing from the data protection related legislations, including the Law. The term national security is prone to subjective interpretation and could expand according to political opinions and the ideological underpinnings. Lack of a legal definition may give ample discretion to an administration while interpreting national security exceptions. According to the Working Party, the national security exemption should be used to the extent of the legal and necessary purposes.¹⁴⁷ Lack of a clear definition should not be interpreted as a pretext for a wide scope of application. Since national security is used as a legitimate ground for restricting the right to protection of personal data, a framework definition should be created to avoid the abuses arise from the vagueness of the term.

In the Law, no limits are set for the extent of interference of the exception to the right to protection of personal data. The exception provision of the Law, Article 28, states “provisions of this Law shall not be applied in the following cases” and then enumerates those cases in which processing of personal data for providing national security is included. This article is a general exemption rule. National security and national defense are actually legitimate grounds for exempting the protection of personal data. However, taking into account the former administrative and judiciary practice of turkey together with increased perception of threat, the term national

¹⁴⁷ Article 29 Working Party WP 215 Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes [2014]

security does not have a specific definition and is open to interpretation; processing of personal information using the national security reason may be overused, may be abused, and may not always have legitimate grounds. Therefore, the limitations of processing personal data for national security purposes should be defined in detail and be clarified in the Article 28, as it was in Directive 95/46/EC. The Directive set the “necessary in a democratic society” notion as the limit of restrictions of the right to process of personal data. Moreover, exceptions should only restrict specific rights, such as a data subject’s right to access his/her own data.¹⁴⁸ Otherwise, “If the scope of exemptions remains broad, it could result in violations of Article 20 of the Constitution and Constitutional Court decisions where privacy and the protection of personal data are protected as basic human rights.”¹⁴⁹

The Constitutional Court follows the ECtHR proportionality test, expects the interference to the right to protection of personal data to be in accordance with law, to pursue a legitimate aim and to be necessary in a democratic society. According to the Constitutional Court, proportionality means an equitable balance between purpose and means. It contains the concepts of the legal measure to be suitable for the purpose of the restriction, the purpose and the means to be proportionate, and the restrictive measure to be necessary in the democratic society. According to the proportionality principle, it is not the right choice, when there is a minor tool to achieve the purpose of restriction, to choose a serious tool. With the proportionality principle, the state is obliged to maintain a fair balance between the public interest and the fundamental rights and freedoms of the individual and protect this balance.¹⁵⁰ Therefore, even though there are different national security perceptions among the judges of the Constitutional Court, the mechanism to redress balance for national security and protection of personal data is the proportionality test in the Turkish Jurisdiction. However, the proportionality test is not enough to guarantee the data subject enjoys his/her right to protection of personal data. As mentioned, the European

¹⁴⁸ Unver and Kim (n 16), Gönenç Gürkaynak and İlay Yılmaz, 'Exemptions under Data Protection Law' (*International Law Office*, 2016) <<http://www.internationallawoffice.com/Newsletters/IT-Internet/Turkey/ELIG-Attorneys-at-Law/Exemptions-under-Data-Protection-Law>> accessed 12 March 2017.

¹⁴⁹ Gürkaynak and Yılmaz (n 148)

¹⁵⁰ Application no: 2014/176 The Constitutional Court

Commission underlined, in its report on Turkey, that judges and prosecutors are not free; they have political pressure on them, and the judicial system is not independent. Judges should be independent, and there should not be governmental pressure on them to allow for free and transparent decisions. For example, in Turkey's current situation, after the coup, 2,745 judges and prosecutors were laid off from their positions.¹⁵¹

Public institutions and intelligence organization assigned and authorized to process personal data for national security purposes should be transparent about their processing activities.

¹⁵² The right to be informed and to access information are crucial tools for data subjects to use against public institutions who process their data. However, ECtHR has acknowledged that these rights can be restricted.¹⁵³ Since the “preventive, protective and intelligence-related activities” are mostly confidential, the public institutions, such as an intelligence agency or the police, may not want to disclose their processing actions. However, for transparency, at least, they should inform the Board to let them review the restrictions on the data subject's rights. The Board should be able to assess the reasonability and proportionality of the national security threat and the measures to avoid it.¹⁵⁴ Also, the Working Party prescribes more transparency for the surveillance programs of the States. Such transparency would help restore trust between citizens, the State, and private entities by providing better information to the citizens when their data has been given to intelligence services, according to the opinion of the Working Party.¹⁵⁵

The significance of an “independent” supervisory authority is mentioned in the Important European legal texts. Other than Directive 95/46/EC, GDPR, Police and Criminal Justice Data Protection Directive, OECD Privacy Guidelines, Additional Protocol to Convention 108, the

¹⁵¹ Sozcu, 'Türkiye'Deki Hakim Ve Savcıların 5'Te Biri Gözaltında' (2016) <<http://www.sozcu.com.tr/2016/gundem/turkiyedeki-hakim-ve-savcilarin-5te-biri-gozaltinda-1319405/>> accessed 12 March 2017.

¹⁵² FRA (n 131) 48

¹⁵³ *ibid*

¹⁵⁴ *ibid*

¹⁵⁵ Article 29 Working Party WP 215 (n 147)

Charter and TFEU drove attention to the independence of the supervisory authorities.¹⁵⁶ Existence of an independent data protection authority is important to ensure that processing is lawful. Data protection authorities can form expert bodies to oversee the public institutions, organizations, and private parties authorized to process personal data. To perform their duties, effective and efficient investigative power and tools should be provided for supervisory authorities. Independence is important for the Board to perform its duties freely. Just as the judicial system should be, the Board--as an oversight body—should not feel the political pressure. If the Board feels the pressure of the government, it could be difficult to act freely. The structuring of the Turkish Data Protection Board seems not so much legal, but instead political, which may cause failure to fulfil its obligations. In this context, to ensure full independence of the Board, it would be appropriate to establish a structure in which the members are elected by the public sector, the private sector, academicians, and judicial authorities instead of being formed as a structure elected only by the Council of Ministers and the President. In the Law, duties and powers of the Board are not mentioned attentive and elaborately. The duties and powers of the Board should be explained in details and should be amplified. A power to “issue non-binding recommendations on general matters related to national intelligence services’ surveillance”¹⁵⁷ or control the processing of a law enforcement authority or the intelligence agency should be given.¹⁵⁸ Additionally, when a data subject wants to access his/her own data, the Board, at least, ought to be permitted to inform the data subject that the necessary examination has been made. Also, the Board ought to have power to handle complaints of individuals with regard to data processing activities of the intelligence agency.¹⁵⁹

Legislators copied the key points of Directive 95/46/EC, such as the principles, the rule of lawful processing, sensitive data, rights of the data subject, data security, and supervisory authority

¹⁵⁶ Handbook on European Data Protection Law (n 28) 114-116

¹⁵⁷ FRA (n 131) 47

¹⁵⁸ Article 29 Working Party WP 233 Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data [2015] 15

¹⁵⁹ FRA (n 131) 48

to the Law. As Article 29 Working Party recalls Directive 95/46/EC as a general legal tool for data protection¹⁶⁰, the Law could be accepted as a general legal tool as well. However, with the current EU data protection reform, on one hand, the Directive 95/46/EC will be annulled by more comprehensive document, GDPR, and on the other hand, there will be a separate legal tool for the field of police and criminal justice, the Police and Criminal Justice Data Protection Directive. As a result, the Law falls short considering the new provisions within the EU.

In the General Data Protection Regulation, which will replace Directive 95/46/EC, the Commission, on one hand, enforces new measures to data protection legislation, and on the other hand, keeps some provisions of Directive 95/46/EC and implements them into the GDPR. Attention should be drawn to GDPR's scope, which will be applicable to both public and private sectors.¹⁶¹ As a positive move, transparency and accountability are added to the principles of data processing. Also, the right to be forgotten¹⁶² and the right to data portability¹⁶³ are defined as new rights in GDPR. The differentiation between non-sensitive data and sensitive data keeps its place in GDPR. The definition of personal¹⁶⁴ data remains the same as in Directive 95/46/EC. As a change, genetic data, biometric data, sex life, and sexual orientation are added as sensitive data, which also can be found in the Law. The Law is, on one hand, modelled on an outdated legal tool—Directive 95/46/EC—and, on the other hand, acknowledges today's technological developments and makes an addition to sensitive data provision as it is regulated in the GDPR. Therefore, the Law should be updated with regard to the current technological needs and also meet the EU standard.

The other part of the EU data protection reform, the Police and Criminal Justice Data Protection Directive, is limited to “the processing of personal data by competent authorities for the

¹⁶⁰ Article 29 Working Party WP 211 (n 80)

¹⁶¹ Peter Hustinx, 'EU Data Protection Law: The Review Of Directive 95/46/EC And The Proposed General Data Protection Regulation' (*statewatch.org*) <<http://www.statewatch.org/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf>> accessed 9 September 2016.

¹⁶² The GDPR Article 17

¹⁶³ The GDPR Article 18

¹⁶⁴ The GDPR Article 4(1)

purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security”.¹⁶⁵ Although there are arguments on the extent of the scope of the Police and Criminal Justice Data Protection Directive, activities fall outside the scope of the Union law, one of which is national security, are not the subject of the Directive. However, there are some provisions which can help the balance the national security and protection of personal data. These provisions are distinction between different categories of data subject and distinction between personal data and verification of quality of personal data. The Police and Criminal Justice Data Protection Directive separates different categories of data and data subjects.¹⁶⁶ Article 7(1) of the Police and Criminal Justice Data Protection Directive obliges Member States to make distinctions between personal data based on facts and personal data based on assessments. This distinction is important to ensure the accuracy and reliability of data in regard to verification of data quality¹⁶⁷, in other words data accuracy principle. Additionally, Article 6 obliges Member States to make a distinction between the different categories of data subjects. According to the Article, the categories are “persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence; persons convicted of a criminal offence; victims of a criminal offence or persons with regard to whom certain facts give rise to reasons for believing that he or she could be the victim of a criminal offence; and other parties to a criminal offence, such as persons who might be called on to testify in investigations”. Article 29 Working Party stresses the necessity of this distinction to assure the proper implementation of data protection principles.¹⁶⁸ As the police and criminal justice authorities connect different pieces of data and interpret to create evidence, making a distinction between categories of data is a positive move. Both these articles would ensure data added in the

¹⁶⁵ The Police and Criminal Justice Data Protection Directive Article 1 (1)

¹⁶⁶ Liane Colonna, 'The New EU Proposal to Regulate Data Protection in the Law Enforcement Sector: Raises the Bar but Not High Enough' (*Juridicumsuse*, 2012) <<http://www.juridicum.su.se/iri/docs/IRI-PM/2012-02.pdf>> accessed 19 November 2016, 5.

¹⁶⁷ *ibid*

¹⁶⁸ Article 29 Working Party WP 233 (n 158)

police database is accurate and regularly updated with regard to categorization.¹⁶⁹ Also, this may avoid mass surveillance of the authorities. Processing personal data of a country's whole population to reach a couple of suspects clashes with the protection of personal data interest of the citizens. In the case of processing personal data with a national security purpose, having different categories of data subjects and distinguishing data based on facts and data based on assessments??? may force the competent authorities to be more careful with the data they collect. By this means, personal data of a suspect and personal data of a law-abiding citizen may be treated differently. Thus, adding two articles, distinction between different categories of data subjects and distinction between personal data and verification of quality of personal data, to the Turkish Criminal Code may help to redress the balance between national security interests of the state and the protection of personal data right of the citizen.

¹⁶⁹ ibid 8

5. Conclusion

Fighting against terrorism and preventing crime is one of the leading subjects in the states' agenda, thus national security is crucial more than ever. In the era of information technology, using personal data as one of the tools to fight against national security threats is inevitable. The terror attacks, the explosions in the crowded cities and the last incident, , caused Turkey to take repressive measures against national security threats. For example, currently, an authorization was given to the police to detect and to intercept the data transmitted between telecommunication or internet connection and internet resources, and to record and evaluate the signal information with regard to specific crimes, such as crimes against the state's security and crimes against national defense. While the broad authorizations have been given to the public institutions with regard to collect and record data, a legal tool for protecting personal data, the Law on the Protection of Personal Data came into force on April 2016.

Prior to the Law, there was a lack of a framework statute for the protection of personal data. There were provisions regarding personal data in several statutes, and those dispersed provisions were insufficient. The absence of clear and understandable legal arrangements and applicable written policies cause the difficulty in drawing boundaries of the responsibilities of the personnel who process data. Through lack of definitions in regard to protection of personal data, principles relating to data quality, an independent supervisory authority that can control whether processing of personal data is legal, an individual cannot fully enjoy his/her constitutional right to protection of personal data. In addition, before the Law came into force, Turkey was regarded as an insecure country. For this reasons, the legislative organ enacted a provision to comply with EU legislation regarding the protection of personal data. Furthermore, in the same period Convention 108 was ratified after 35 years, as well.

Since the main reason of enacting the Law was the harmonization with the EU, the Directive 95/46/EC was taken as a model for the structure and for the content of the Law. The Law mostly have similarities with the Directive 95/46/EC, such as the definitions, the principles relating the data quality. On the other hand, there are different points, as well, such as the provisions on the sensitive data, the data protection board/authority and the exemptions and restrictions. The

Law has major differences from the Directive 95/46/EC regarding the provision on exemptions, especially the broad exception to the right to protection of personal data with regard to the national security. As it mentioned before, the Law mainly assessed from the private parties point of view, such as how the companies can comply with the Law, since it was enacted. However, since the right to protection of personal data is a fundamental human right, and the national security exception which completely restricts the right should be discussed, as well.

Fundamental rights and freedoms of an individual are not untouchable, as well as the right to protection of personal data. Thus, the right can be restricted by the reason of national security. However, the interference to the right is lawful only if it is in accordance with the law, pursues a legitimate purpose and necessary in a democratic society in order to achieve the legitimate purpose according to the ECHR and the Charter. The ECtHR seeks these three steps in its jurisdiction. Otherwise, restriction may cause the violation of the right. In the opinion of the thesis, these three steps proportionality test is the mechanism for redress balance between the national security and the right to protection of personal data. However, there is no guaranty that the state or the public institutions will apply the proportionality test to their actions in practice. Therefore, rules should be set in the data protection legislations.

Since the national security of the state is crucial, balancing national security interest of the state with the right to protection of personal data of the citizens is a controversial topic. The countries have their own background and identity, so their approach towards national security differs. As a result, the national security issue is the Member States' responsibility in the EU. The Directive 95/46/EC, the model legislation of the Law, leaves national security topic to the national legislations of the Member States. When doing so, it permits the Member States to restrict only few rights such as the data subject's right of access his/her own data rights and it demands for the interference to be 'necessary'.

The national security exception in the Law is very broad, and if the limit will not be drawn, the exception will be abused by the public institutions, and this will cause the violation of the right to protection of personal data, which is a Constitutional right. Also the definition of national security is missing in the legislations of Turkey. The Constitutional Court interprets the term in its

judgments, however there is a lack of general definition. In addition, the Constitutional Court underlined the subjectivity of the term national security, too. Hence, without a generally accepted and objective definition on the national security, forming a very broad national security exception provision is dangerous. Considering the public institutions have already broad authorizations such as the police example given above, the exception should be limited to some specific rights, and the necessity of the restriction should be demanded, like it was done in the Directive 95/46/EC.

As another measure to keep the balance between the national security and the right to protection of personal data, the independence of the Data Protection Board should be strengthened by structural adjustment of the Board. In the opinion of the thesis, the Board works like an oversight mechanism to the rights of the data subjects. It is one of the corner stones for data subjects to enjoy their rights. Therefore, it has an important role on balancing the right to data protection and the national security. Thus, the structure should be changed to be more independent from the political influence, and the authorization to check whether the interference to the right to protection of personal data with the purpose of national security is proportionate and necessary in a democratic society should be provided to the Board.

Briefly, the national security exception clause in the Law should be improved by modifying the current general character of the exception clause and by limiting the scope of application of the national security restrictions to specific cases/rules in order to redress the balance. These specific obligations and rights could be designated as: Article 5 the principles of processing data, Article 10 data controller's obligation to inform and Article 11 rights of data subject. The structure of the Board should be changed to create a less dependent organization. The members of the Board should be elected amongst the people nominated by the public sector, the private sector, academicians and judicial authorities instead of being formed as a structure elected only by the Council of Ministers and the President. After this pre-selection, the candidates should be elected by the Parliament. Lastly, other than these suggested improvements, it should always be kept in mind that the right to protection of personal data is a fundamental human right, it has to be always taken into consideration, even if it comes up against the national security interest of the state.

Bibliography

All links were checked on 24 March 2017.

Cases

19/3/2015 T. 2014/180 E. 2015/30 K. (Constitutional Court)

27/5/2015 T. 2014/176 E. 2015/53 K. (Constitutional Court)

25/4/1974 T. 1973/41 E. 1974/13 K. (Constitutional Court)

Case C – 518/07 *Commission v. Federal Republic of Germany* [2010]

Erdem Gül ve Can Dündar Başvurusu 27/2/2016 T. Application no: 2015/18567 (Constitutional Court)

Kristal-İş Sendikası Başvurusu 2/7/2015 T. Application No 2014/12166 (Constitutional Court)

Rotaru v Romania App no 28341/95 (ECtHR, 4 May 2000)

Statutes and statutory instruments

Banking Law dated 1 November 2005 and numbered 5411

Bank Cards and Credit Cards Law dated 22 February 2006 and numbered 5464

Civil Code dated 22 November 2001 and numbered 4721

Code of Obligations dated 1 January 2011 and numbered 6098

Convention 108

Criminal Code dated 26 September 2004 and numbered 5237

Data Protection Directive 95/46/EC

Electronic Communications Law dated 10 November 2008 and numbered 5809

Electronic Commerce Law dated 5 November 2014 and numbered 6563 Charter of Fundamental Rights

European Convention on Human Rights

General Data Protection Regulation (EU) 2016/679

Labor Law dated 22 May 2003 and numbered 4857

Law on the Duties and Powers of Police dated 14/7/1934 and numbered 2559

Law on Right to Access Information dated 9 October 2003 and numbered 4982

Law on State Intelligence Services and National Intelligence Organization 3 November 1983 dated and numbered 2937

Police and Criminal Justice Directive (EU) 2016/680

Regulation on Internal Systems of Banks dated 1 November 2006 and numbered 26333 Official Gazette

Turkish Constitution date 7 November 1982 and numbered 2709

Official Documents

Article 29 Working Party WP 211 Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector 27 February 2014

Article 29 Working Party WP 215 Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes 10 April 2014

Article 29 Working Party WP 233 Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data 01 December 2015

Commission, 'Turkey 2015 Report' (Communication) COM (2015) 611 Final

European Commission, 'European Commission Opens Way for Decision by June On Visa-Free Travel For Citizens Of Turkey' (2016) <http://europa.eu/rapid/press-release_IP-16-1622_en.htm> accessed 25 February 2017

European Commission, 'Turkey's Progress on the Visa Liberalization Roadmap - Factsheet' (2016) <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-migration/background-information/docs/20160504/turkey_progress_visa_liberalisation_roadmap_en.pdf> accessed 25 February 2017

European Commission, 'The EU Data Protection Reform and Big Data - Factsheet' (2016) <http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf> accessed 26 February 2017

FRA (European Union Agency for Fundamental Rights), 'Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU' (2015)

The Draft Law on the Protection of Personal Data (1/541) and the Justice Commission Report No: 117

Books

Akay H, *Security Sector in Turkey* (1st edn, TESEV Publications 2010)

Başalp N, *Kişisel Verilerin Korunması Ve Saklanması* (1st edn, Yetkin Yayınları 2004)

Handbook On European Data Protection Law (1st edn, Publications Office of the European Union 2014)

Henkoğlu T, *Bilgi Güvenliği Ve Kişisel Verilerin Korunması* (1st edn, 2015)

Howorth J, *Security and Defense Policy in the European Union* (1st edn, Palgrave Macmillan 2014)

Kitchin R, *The Data Revolution: Big Data, Open Data, Data Infrastructures And Their Consequences* (1st edn, Sage Publications 2014)

Ustun C, *Turkey and European Security Defence Policy* (1st edn, IB Tauris 2014)

White H, *The Idea of National Security* (1st edn, National Security College 2012)

Book chapters

De Hert P. and S. Gutwirth, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power', *Privacy and the criminal law*, (1st edn, Intersentia 2006)

Güney N, 'Country Report On Turkey', *Terrorism as a Challenge for National and International Law: Security versus Liberty?* (1st edn, Springer 2004)

Gürkaynak G and Yılmaz İ, *the privacy, data protection and cybersecurity law review* (1st edn, Gideon Robertson 2014)

Journal articles

Akguner T (1985) 6 *Idare Hukuku ve İlimleri Dergisi*
<<http://www.journals.istanbul.edu.tr/iuihid/article/view/1023002682>> accessed 7 March 2017

Argomaniz J, 'Post-9/11 Institutionalisation Of European Union Counter-Terrorism: Emergence, Acceleration And Inertia' (2009) 18 *European Security*

Aybay R, 'Milli Güvenlik Kavramı Ve Milli Güvenlik Kurulu' (1978) 33 *Ankara Üniversitesi SBF Dergisi* (Ankara University Faculty of Political Science Journal)

Bauman Z and others, 'After Snowden: Rethinking the Impact of Surveillance' (2014) 8 *International Political Sociology*

Bertota J and others, 'Big Data, Open Government And E-Government: Issues, Policies And Recommendations' (2014) 19 *Information Polity*
<<http://content.iospress.com/download/information-polity/ip000328?id=information-polity%2Fip000328>> accessed 19 February 2016

Boehm F, 'Confusing Fundamental Rights Protection in Europe: Loopholes In European Fundamental Rights Protection Exemplified On European Data Protection Rules' [2009] *SSRN Electronic Journal*

Bygrave L, 'The Place of Privacy in Data Protection Law' (2001) 24 University of New South Wales Law Journal

De Hert P and Papakonstantinou V, 'The Data Protection Framework Decision Of 27 November 2008 Regarding Police And Judicial Cooperation In Criminal Matters – A Modest Achievement However Not The Improvement Some Have Hoped For' (2009) 25 Computer Law & Security Review

De Hert P and Papakonstantinou V, 'The New General Data Protection Regulation: Still A Sound System for The Protection Of Individuals?' (2016) 32 Computer Law & Security Review

De Hert P and Papakonstantinou V, 'The New Police And Criminal Justice Data Protection Directive A First Analysis' (2016) 7 New Journal of Criminal Law

Gurpinar B, '1982 Anayasası'na Göre Milli Güvenlik Kavramı' [2012] Hasan Kalyoncu Üniversitesi Hukuk Fakültesi Dergisi

İtisgen R, 'Türk Ceza Hukukunda Kişisel Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme Suçu' (2015) 6 Türkiye Adalet Akademisi Dergisi <<http://www.taa.gov.tr/yayin/turkiye-adalet-akademisi-dergisi-sayi-23/>> accessed 6 February 2017

Kim G, Trimi S and Chung J, 'Big-Data Applications in the Government Sector' (2014) 57 Communications of the ACM

Poullet Y, 'Data Protection Legislation: What Is at Stake for Our Society and Democracy?' (2009) 25 Computer Law & Security Review

Rodoplu U, Arnold J and Ersoy G, 'Terrorism in Turkey' (2003) 18 Prehospital and Disaster Medicine

Ünver A and Kim G, 'Data Privacy And Surveillance In Turkey: An Assessment Of The Draft Law On The Protection Of Personal Data' (2016) 2 EDAM Cyber Policy Paper Series

Websites and blogs

'4857 Labor Law English by Article - Turkish Labor Law' (*Turkishlaborlaw.com*, 2017) <<http://turkishlaborlaw.com/turkish-labor-law-no-4857/19-4857-labor-law-english-by-article#2>> accessed 2 March 2017

Bagci G, '14 Soruda Kişisel Verilerin Korunması Kanunu – E-Ticaret Ve İnternet Hukuku' (*Eticarethukuku.com*, 2016) <<http://www.eticaret hukuku.com/14-soruda-kisisel-verilerin-korunmasi-kanunu>> accessed 3 March 2017

Bilgehan Z and Ozer Y, 'ICLG: Data Protection 2016 - Turkey - International Comparative Legal Guides' (*Turkey - Data Protection 2016 - ICLG - International Comparative Legal Guides*, 2016) <<http://iclg.com/practice-areas/data-protection/data-protection-2016/turkey#chaptercontent10>> accessed 5 March 2017

Butti E, 'The Roles and Relationship between the Two European Courts in Post-Lisbon EU Human Rights Protection' (*Jurist.org*, 2013) <<http://www.jurist.org/deline/2013/09/elena-butti-lisbon-treaty.php>> accessed 6 September 2016

Colonna L, 'The New EU Proposal to Regulate Data Protection in the Law Enforcement Sector: Raises the Bar but Not High Enough' (*Juridicumsuse*, 2012) <<http://www.juridicum.su.se/iri/docs/IRI-PM/2012-02.pdf>> accessed 19 November 2016

Degirmenci N, 'Turkey's First Comprehensive Data Protection Law Comes into Force' (*Inside Privacy*, 2016) <<https://www.insideprivacy.com/data-security/turkeys-first-comprehensive-data-protection-law-comes-into-force/>> accessed 1 March 2017

Gurkaynak G and Yilmaz I, 'Exemptions under Data Protection Law' (*International Law Office*, 2016) <<http://www.international lawoffice.com/Newsletters/IT-Internet/Turkey/ELIG-Attorneys-at-Law/Exemptions-under-Data-Protection-Law>> accessed 12 March 2017

Gurkaynak G, 'Comparison of Turkish Data Protection Law with EU Directive 95/46/EC' (*Mondaq.com*, 2016) <<http://www.mondaq.com/turkey/x/486152/data+protection/Comparison+Of+Turkish+Data+Protection+Law+With+EU+Directive+9546EC>> accessed 26 February 2017

Hamevi H and Lachman G, 'Data Protection Laws in Turkey' (*Mondaq.com*, 2014) <<http://www.mondaq.com/turkey/x/308428/Data+Protection+Privacy/Data+Protection+Laws+In+Turkey>> accessed 22 May 2016

Hançar Çelik H and Karaduman O, 'The New Personal Data Protection Law in Turkey - Gün + Partners' (*Gün + Partners*, 2016) <<http://gun.av.tr/the-new-personal-data-protection-law-in-turkey/>> accessed 26 February 2017

'Home Page of EU GDPR' (*EU GDPR Portal*) <<http://www.eugdpr.org/>> accessed 3 March 2017

Hustinx P, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation' (*statewatch.org*) <<http://www.statewatch.org/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf>> accessed 9 September 2016

Kearney D, 'What Does “National Security” Actually Mean?' (*Rightsni.org*, 2013) <http://rightsni.org/2013/05/national-security/#_ftn3> accessed 8 March 2017

'LEGISLATION ON THE RIGHT TO INFORMATION' (*Bedk.gov.tr*) <http://www.bedk.gov.tr/Yayinlar/LEGISLATION_ON_THE_RIGHT_TO_INFORMATION/index.html> accessed 2 March 2017

'New Data Protection Law In Turkey - Edri' (*EDRi*, 2016) <<https://edri.org/new-data-protection-law-in-turkey/>> accessed 25 February 2017

Özer Y, 'Kişisel Verilerin Korunması Mevzuatı' (*Kişisel Verilerin Korunması*) <<http://www.kisiselverilerinkorunmasi.org/mevzuat/>> accessed 6 March 2017

Özer Y, 'Turkey: A New Era for Data Protection in Turkey - The Law on the Protection of Personal Data Enters into Force' (*mondaq.com*, 2016) <<http://www.mondaq.com/turkey/x/483272/Data+Protection+Privacy/A+New+Era+for+Data+Protection+in+Turkey+The+Law+on+the+Protection+of+Personal+Data+Enters+into+Force>> accessed 24 May 2016

Sarkin J, 'Human Rights: International and Domestic Standards Applying to Terrorism and Freedom of Speech' (*southernafiralitigationcentre.org*) <<http://www.southernafiralitigationcentre.org/1/wp-content/uploads/2017/01/GOAL-16-Book-Sarkin.pdf>> accessed 28 February 2017

'The Case Of Journalists Can Dündar And Erdem Gül - Global Freedom Of Expression' (*Global Freedom of Expression*) <<https://globalfreedomofexpression.columbia.edu/cases/case-journalists-can-dundar-erdem-gul/>> accessed 23 March 2017.

Toksoy F, Balki B and Erzene Yıldız S, 'Data Protection in Turkey: Overview' (*Practical Law*) <<http://uk.practicallaw.com/7-520-1896>>accessed 19 February 2016

'Turkish Court Issues An Injunction Against The Ministry Of Education's Refusal To Enroll A Child To An Armenian School' (*ochrance.cz*, 2014) <http://www.ochrance.cz/fileadmin/user_upload/DISKRIMINACE/aktuality/TR-40-Turkish_court_issues_injunction_against_the_Ministry_of_Education_s_refusal_to_enroll_a_child_to_an_Armenian_school.pdf> accessed 9 June 2016

'Turkish Law on the Protection of Personal Data No. 6698' (*Kişisel Verilerin Korunması*) <<http://www.kisiselverilerinkorunmasi.org/ingilizce-ceviri/#Purpose-Scope-and-Definitions>> accessed 3 March 2017

'Türkiye Büyük Millet Meclisi' (*Tbmm.gov.tr*) <https://www.tbmm.gov.tr/develop/owa/milletvekillerimiz_sd.dagilim> accessed 13 February 2017

Uludere E, 'Personal Data Protection under Turkish and European Legislation - Erdem & Erdem' (*Erdem-erdem.av.tr*, 2015) <<http://www.erdem-erdem.av.tr/publications/law-post/personal-data-protection-under-turkish-and-european-legislation/>> accessed 5 March 2017

'What Is Privacy | Privacy International' (*Privacyinternational.org*) <<https://www.privacyinternational.org/node/54>> accessed 19 June 2016

Yildirim Ozturk M and Ergun C, 'Data Privacy in Turkish Law | White & Case LLP International Law Firm, Global Law Practice' (*Whitecase.com*, 2011) <<https://www.whitecase.com/publications/article/data-privacy-turkish-law>> accessed 2 March 2017

Newspapers

Aktar C, 'EU-Turkey: Is Refugee Issue a New Membership Criterion?' *Al Jazeera* (2016) <<http://www.aljazeera.com/indepth/opinion/2016/03/eu-turkey-refugee-issue-membership-criterion-160310093315328.html>> accessed 25 February 2017

Aljazeera, 'Istanbul Bombing: At Least Five Killed In Turkish City' (2016) <<http://www.aljazeera.com/news/2016/03/istanbul-taksim-square-area-hit-explosion-160319091702737.html>> accessed 29 April 2016

Çetingüleç T, 'CHP Report Exposes Turkey's High Poverty Levels' (2015) <http://www.al-monitor.com/pulse/tr/originals/2015/03/turkish-opposition-draws-up-alarming-poverty-map.html> accessed 7 June 2016

Hürriyet Daily News, 'Minorities In Turkey Tagged By 'Race Codes,' Official Document Reveals' (2013) <<http://www.hurriyetdailynews.com/minorities-in-turkey-tagged-by-race-codes-official-document-reveals.aspx?pageID=238&nID=51849>> accessed 9 June 2016

İdiz S, 'Is Turkey Becoming A Police State?' *Al Monitor* (2015) <<http://www.al-monitor.com/pulse/originals/2015/02/turkey-becoming-police-state.html#>> accessed 21 June 2016

Melvin D, 'At Least 95 Killed in Twin Bombings near Train Station In Turkey's Capital' *CNN* (2015) <<http://edition.cnn.com/2015/10/10/middleeast/turkey-ankara-bomb-blast/>> accessed 29 April 2016

Murdock J, 'Anonymous: Hacker Unleashes 17.8GB Trove of Data from a Turkish National Police Server,' *International Business Times* (2016) <<http://www.ibtimes.co.uk/anonymous-hacker-unleashes-17-8gb-trove-data-turkish-national-police-server-1544131>> accessed 19 February 2016

Sozcu, 'Türkiye'Deki Hakim ve Savcıların 5'Te Biri Gözaltında' (2016) <http://www.sozcu.com.tr/2016/gundem/turkiyedeki-hakim-ve-savcilarin-5te-biri-gozaltinda-1319405/> accessed 12 March 2017

Sözeri E, 'Turkey Paid Hacking Team \$600K to Spy on Civilians' *The Daily Dot* (2015) <<http://www.dailydot.com/layer8/hacking-team-turkey/>> accessed 19 February 2016

Yinanç B, 'Turkey'S Data Protection Draft Law Open to Abuse: Expert' *Hürriyet Daily News* (2016) <<http://www.hurriyetdailynews.com/turkeys-data-protection-draft-law-open-to-abuse-expert.aspx?pageID=238&nID=95796&NewsCatID=341>> accessed 29 April 2016