EUROPEAN COURT OF HUMAN RIGHTS CASE LAW ON PROTECTION OF PERSONAL DATA: REASSESSMENT OF REPUBLIC OF TURKEY CASES IN LIGHT OF TURKEY'S DATA PROTECTION LAW

VÁRKONYI GÜLTEKİN, GIZEM*

Abstract: Protection of Personal Data is one of the newest right developed within the Right to Privacy. This fundamental right has been perceieved mostly as a European value giving as a reason that it has been continuesly develop-ing under the European legal framework. Turkey also follows European heritage of human rights as one of the member of the Council of Europe and European Union candidate country. Recognition of personal data pro-tection as a single fundamental right was a late action of Turkey. For this reason, some of the data potection cases could not solved in Turkey's jurisdiction, but were referred to the European Court of Human Right. If there was well-grounded data protection law before, the cases could be solved quicker and more in favor of Plaintiffs.

Keywords: European Court of Human Rights, data protection, human rights, Turkey.

1. Introduction

Republic of Turkey is one of the largest and most populated country in Europe. Its special geopolitic position gives many advantages to the country. Many neighbors around the country from the European continent gives opportunities to Turkey to follow global legal developments in the field of human rights protection. European Union is an important organization as a matter of fact that it makes globally leading developments in certain areas especially protection of human rights. Although, Turkey's European Union accession turned to be a sort of "soap opera" by more than 30 years now, it is impossible to refuse the efforts of Turkey on the road to the EU accession. Many legal developments boosted the country to adopt better human rights protection legislation. One of these efforts is surely is on the data protection field. Turkey is one of the oldest member of Council of Europe. Although she is one of the first signatory[1] of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108),[2] she waited so many years to ratify it. Only very recently, in 2016, Turkey could enact a law on Protection of Personal Data. For years, Turkish courts were interpreting the personal data protection cases in frame of separate laws such as Turkish Code Civil, Turkish Criminal Code and sector focused regulations. In Europe, however, protection of personal data was defined as a fundamental right that should be protected in the single legislation. In this paper, we will re-interpret the ECHR Case Law in light of the new Turkish Data Protection Law. Moreover, new law brought many developments but still there is a need for further improvements.

* University of Szeged, Faculty of Law and Political Sciences, gizemgultekin@windowslive.com.

[1] The Convention was opened for signatories in 1981 and Turkey signed it at that time.

[2] Full text version of the Convention is accessible at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37.

1.1. Development of Right to Protect Personal Data

Protection of personal data is one of the newest third generation rights and increasingly receiving attention in the legal concept. This right firstly developed under the right to privacy before 90's, when the mass technologic developments had not been started yet. Since then, such developments change people's daily life as well as confront them with new threats.

The technologic developments change people's life style as well as their private life. One touch is enough to share any personal information with billions of people nearly with speed of light. Either willingly, mistakenly or out of knowledge, information related to our personal life "fly somewhere on the virtual space" where whomever can access it. For this reason first of all, the perception and then the understanding of privacy has changed. Privacy basically referred to the physical privacy such as border of someone's home or some space that can be definable with physical borders. Vast amount of virtual services and transactions eliminated this tangible border, sometimes by people's their own will sometimes by forcing them to use such virtual services. Hence, not just services such as internet banking, health information systems or online shops, but communication facilities and social media attractions also receive many users. Using such services require sometimes people's financial information, sometimes age indication or sometimes addresses, phone numbers, nationalities, in short, information belong to people. Millions of data somehow transmitted to the virtual space where people do not exactly know what happens to them and do not have control over it. The virtuality has changed the privacy in a way that it got new dimensions which is intangible and other than physical privacy such as information privacy or spiritual (decisional privacy).[3] It brought a new type of privacy, information privacy, which generally refers to personal data protection. However, there are claims[4] that even information privacy is not enough to involve the personal data protection issues. For these reasons, even newer right, right to protect personal data has shaped in different philosophical and legal basement. Still, there is a connection existed between privacy and personal data protection. Data protection right developed with privacy and been separate right but never has lost its connection. This connection was described best in one of the research[5] as follows: "Data protection is both broader and more specific than the right to privacy. It is broader because data protection also protects other fundamental rights such as the freedom of expression, the freedom of religion and conscience, the free flow of information, the principle of non-discrimination, next to individual liberty and self-determination. But data protection is also more specific than privacy since it simply and only applies when personal data are processed". It is

[3] SAVOIU, ALINA – BASARABESCU, C. CATALIN: The Right to Privacy, in *Annals of the Constantin Brancusi University of Targu Jiu Juridical Sciences Series,* 2013, 1, 90.

[4] WRIGHT, DAVID – RAAB, CHARLES: Privacy principles, risks and harms, in *International Review of Law, Computers & Technology,* 2014, 3, 28, 278.

[5] GUTWIRTH, SERGE – POULLET, YVES – HERT, PAUL DE: *Data Protection in a Profiled World,* 2010, Springer, Dordrecht-New York http://search.ebscohost.com/login.aspx?direct=true&db=edshlc&AN=edshlc.012582268-5&lang=tr&site=eds-live&authtype=ip,uid.

clear that neither data protection nor privacy is not an equivalence of each other. From the legal point of view also differentiation between the two rights were needed and occurred by many national and international legal documents.

Data protection as a fundamental right was adopted by many European countries as well as Council of Europe (CoE) members. Some of the members already had basement of such right in their domestic legislation while some of them had to modify it in order to comply with the Convention. Most of the members ratified the Convention in the early 2000. However, Turkey waited 36 years for the ratification and currently it holds the latest ratified country among the members of the CoE.

In this work, we assume that if there was Personal Data Protection Law in Turkey from the day that the Convention 108 was signed, and then if it was ratified quickly, there would not be any cases related to this topic in the European Court of Human Rights' (ECtHR) agenda. Although there were not much cases already, because of the country's bad reputation in the ECtHR as a second most defendant country, it could be possible to decrease some amount of the case load there. Also, it would be better for the plaintiffs to get quicker result, and solve the case in the national remedies. We choose one of the case which is directly related to personal data protection, apart from the privacy for the first sight. The case is important and worth to examine to show how Personal Data Protection Law in Turkey will affect the country's fundamental rights efforts in a positive way.

1.2. Protection of Personal Data in the International Context

Right to protect personal data had been interpreted under the privacy protection national sphere as well as international one. First personal data protection placed under the privacy rules in the global approach. The most known and the first most comprehensive human rights document, the United Nations Universal Declaration of Human Rights (UDHR) signed and declared in 1948, can be accepted also as the first legal document that ensures right to privacy. Article 12 of the UDHR indicates that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Although the UN take the first step towards protection of human rights, right now it is the European continent where the human rights researches and legislation has been predominantly and continuously developing. It is clear in the international documents also; CoE European Convention on Human Rights (ECHR) is one of the comprehensive international human rights legal document that is very effective in Europe as well as countries from other continents that are willing to join. Article 8 of the ECHR stresses out the "Right to respect for private and family life."[6]

[6] The article stresses out that "Everyone has the right to respect for his private and family life, his home and his correspondence" and "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

There is no doubt that ECHR brought many basic norms in order to protect political and civil rights but the Convention adopted almost any single human rights in frame of its protection. Hence, as we will mention below, the first and only international legal document protecting personal data has been developed within the ECHR. We think that ECHR affected domestic will and development on protection of personal data and privacy in Europe. When we review the legal developments about personal data protection, one can easily realize that the right to protect personal data is actually a European value. Until the Convention 108 was enacted, there were many development occurred in the European countries. For example, the first domestic legal regulations were done for data protection in 1970 Länd of Hessen, Germany. The reason why behind this need was the idea of creating a central federal database for storing the data and realization of the risk of protection of the database. Later on in 1977, the legal improvements affected the federal level and federal level legislation was adopted. Sweden was the second country where data protection legislation was adopted and then other European countries except from Ireland, UK and Italy developed its domestic legislation either at the constitutional level or constitutional studies2. United States is the only non-European country where personal data protection legislation has developed earlier than 1980.

Automatic systems surely easiness the world of manual works but in a world where the value of data protection was realized, it would not pushed out of concept. Organization for Economic Cooperation and Development (OECD) has realized the danger on transferring "vast quantities of within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data" and where there is no unique approach to the issue from the countries, it will cause breaches on people's basic rights. For this reason, OECD released its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980, as the first document that deals with transmission of personal data abroad. Later on the UN would follow the OECD with its the Guidelines for the Regulation of Computerized Personal Data Files in 1990 which was updated in 2013 last. The Asia-Pacific Economic Cooperation, similarly to the OECD, adopted APEC Privacy Framework in 2004 in order to handle regional data transfers without causing breaches on people's fundamental rights. The document focuses on the data protection in the field of economy foresees the rules for "electronic commerce to expand business opportunities, reduce costs, increase efficiency, improve the quality of life, and facilitate the greater participation of small business in global commerce". APEC information privacy principles are presented as "Preventing Harm, Notice, Collection, Limitations, Usages, Choice, Integrity of Personal Information, Security Safeguards, Access and Correction, Accountability" which are in the framework with the Directive 95. The last part of the document presents separate approach to Domestic and International Implementations. These documents are not binding "how to..." documents where the basic principles for data protection is drawn, not deeper.

Table 1.: Development of personal data protection timeline

National		International	
1970	Hessen	1948	United Nations
1970-1974	United States	1950	Council of Europe
1973	Sweden	1980	OECD

1976	Portugal	1981	Council of Europe Convention 108
1977	Germany	1995	European Union Directive 95
2016	Turkey	2004	Asia-Pasific Economic Cooperation

Source: KÜZECI, ELIF: *Personal Data Protection*, 2010, Unpublished doctoral thesis, Ankara, Ankara University Institution of Social Sciences, Ankara, 117-119.

Another international legal document that is very important for data protection legislation is the Directive 95 of the European Union. The importance of the Directive is, it is multidimensional. First of all, it aims to take over difficult interpretation of direct data breach issues based only on privacy. The Directive also brings stronger protection than the other legislations, because it introduces many rights that can be counted new in this field. Right to obtain the source of the information, modification, remedies, rules for transferring the personal data abroad even though the transferee country does not have an adequate level of protection can be present with some examples.[7] In 2000 Charter of Fundamental Rights adopted right to protect personal data as a human right. Since then, the EU institutions also follow the same rules of personal data protection as the Directive reflects.

We should point out that although the Directive was released later than the Convention, the Convention was affected from this newer approach to the data protection and later it was modified mostly based on the Directive. It should not be wrong to say the Directive is globally influential document in this field. However, the EU authorities even did not think that the Directive meets with the developments and the needs of EU citizens furthermore. In order to adopt single approach and elimination differences between the EU members, the EU introduced European Data Protection Regulation in 2016, and it will be enforced in May 2018. The new Regulation brings stricter rules that will be directly applicable in the Member States, even more it will be bind cross-border sense and it introduces new rights such as "right to be forgotten". There is no doubt that legal developments are trying to catch the daily developments and for now EU seems more adopted to the change.

Based on the ECHR of CoE, privacy started not to meet with the needs of European people. For this reason, stressing the personal data protection separately as a single right at the international level has adopted in Europe lead by CoE. By this way, the restricted interpretation caused by only privacy right targeted to be eliminated. Also, lack of being standard legal basement for everyone in Europe could be ensured. Convention 108 opened for signatory in 1981.

2. Basıcs of the conventıon 108

Convention 108 is the first international legal document protects individuals' data. It is accepted as the basement of the Directive 95 and a model for many countries' national personal data protection legislation. Currently, all the 47 members of the CoE ratified the Convention, 5 non-CoE member countries signed (Cabo Verde, Mauritius,

[7] KÜZECI: *op. cit.* 176.

Morocco, Senegal, Tunisia, Uruguay) and 3 of them (Mauritius, Senegal, Uruguay) ratified the Convention.[8] For this reason, it worths to review the Convention 108 deeply.

It is important to see what does personal data mean according to the Convention. Personal data is "any information relating to an identified or identifiable individual" who is actually defined as the data subject. Whomever, either in the public or the private sector, collects, stores and processes the data subject's information is called as data controller. Scope of the Convention was limited with the automated personal data files and processes but some of the countries, such as Serbia, adopted national legislation that covers the non-automated files containing personal data either. This Convention is the basic and it brings the minimum standards for protection of personal data so the countries should be free to adopt more or better solutions in their jurisdiction. For this reason, the Convention explicitly indicates that the countries should give a notice if they extend or limited the scope of it. This would definitely help improving the Convention as well as to see the different implementations so that the CoE may recommend to the countries to ensure standard level of protection.

The basic principles for data protection in the Convention are as following:

Duties of the Data Controllers; to adopt the rules of the Convention at the national level, and make it as soon as possible.

Quality of data; should be determined while processing whether it is fair and lawful, in frame of its purpose, accurate and updated, and is stored for no longer than is needed.

Special (sensitive) data; is a data that should not be processed automatically if there is no separate protection rules at the national level. These data is the data related to racial origin, political opinions or religious or other beliefs, health or sexual life and most importantly for our case, criminal convictions of the data subjects.

Data security; any kind of security measure against illegal accession of the personal data.

Additional safeguards for the data subject; is a right to know whether the data is stored, where it is store and who is the controller, ask for erasure or rectification if it is illegally stored, and have a remedy if it is stored illegally.

Exceptions and restrictions; are based on the fact that there can be issues to restrict such protection. These issues can be related to state and public security, state's monetary interests, suppression of crime, and protection of others' rights and freedoms besides the data subject.

Sanctions and remedies; should be adopted in the domestic law against violations.

Trans-border data flows: Before the Additional Protocol on the Convention 108 was accepted in 1999 which we will mention below,, it was very open ended for interpretation to transfer the personal data outside of the jurisdiction, without in knowledge whether tansferee country would protect the data same way as the

[8] The Chart of the signatory countries and the ratifications can be found here: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=QraCFokWs

transferer. Within the amendment, it was modified in favor of the persons as well as the countries to not to put them in a confusion and missing protection.

Cooperation between parties; is important to share information and practices either with the CoE or parties of the Convention.

Consultative Committee; which consists of representative from contractor parties and open for non-contractors' representative. The Committee's duties are to make proposals to improve the Convention, propose amendment and give its opinion as well as advices. It is an independent body to watch over the application of the Convention.

The Convention 108 was adopted by many member states of the CoE in the 90's but when the internet based activities developed and integrated into people's daily life, there appeared another problems. There are several technologically leading companies in different countries. Electronic world is not very much independent from the hardware, which means that such services actually served from certain points where the hardware is located. When a person takes an activity on the web, it leaves nearly a fingerprint alike sign on such hardwares. In addition, many services run better with the data from the user of the service; the data is stored and processed on the hardware where might be at the jurisdiction of abroad. While such cases appear and were looking like to appear more, CoE amended the Convention 108 in 2001 with the Additional Protocol which regulates the rules of data transmission abroad to the countries that is not a party of the Convention 108. The Protocol brought the obligation for the transferee country to ensure "adequate level" or safeguards to protect personal data at their domestic law. Level of adequacy which placed in nearly any national or international personal data protection documents, has criticized many times by the scholars. This is because firstly, not every country perceive privacy in a same way. It was the case of transmission of the air plane ticket Personal Name Records from European Union to the United States. When the US obliged the air carriers to share wide range of such information with the US law enforcement authorities, regardless of where they come from, it was the EU that delivered its privacy concerns. Actually, such "adequacy" concept was performed in this issue. Still, there are debates about the adequacy understanding. Because there is a need to agree clearly on whether prior approval to the data transmission is enough or transmission with no ex ante control should be adopted.[9] Apart from this discussion, Additional Protocol brought an obligation to the contractor countries to establish a national supervision mechanism to be watch-dog of the data controllers whether they are compatible with the Convention.

The Court had received numerous cases regarding to the right privacy. Indeed, there are many cases related received directly or indirectly related to personal data protection. According to the ECtHR Factsheet published in November 2016, the Court groups the cases related to personal data according to the titles of the rights as they are in the Convention. According to that, the main rights of the people as well as the violation areas are grouped as "Collection, storage and use, disclosure, accession,

[9] KIERKEGAARD, SYLVIA – WATERS, NIGEL – GREENLEAF, GRAHAM – BYGRAVE LEE A. – LLOYD, IAN – SAXBY, STEVE: 30 years on-The review of the Council of Europe Data Protection Convention 108, in *Computer Law&Security Review* (2011), 27, 231, doi:10.1016/j.clsr.2011.03.007.

erasure or destruction of personal data". After this grouping, the type of data must be important for the Court as a first step for the judgement. Health related data, employees' data, DNA data, data gained from surveillance technologies such as CCTVs or telephones, social insurance data and many more types of data have been subject of the Court's judgement. The cases lodged by the individuals against one or more member states, and found eligible to be judged generally resulted as fine or just satisfaction. The cases that did not violated the ECHR or the Convention generally interpreted as "legitimately aimed and necessary for the national security, public safety and the rights of the victims, and of preventing crime". As the Member States of the CoE can ask for preliminary ruling from the judges of the ECtHR, many cases were interpreted under the principle of proportionality or margin of appreciation. Surely, there are cases that the judges made the ruling in favor of the Member State to not to breach the Conventions.

However, in the 21st century the technology has gain an unstoppable speed. Mobile usage as well as social media boomed. Developments required once again changes on the Convention. In order to make the Convention better, more effective and more clear for everyone, so called globalization[10] or modernization of the Convention had finalized in 2013, but not enforced yet. The modernization includes major developments such as obligation of the parties, data protection standards, additional obligations, data export restrictions and new roles for the CoE Consultative Committee. We will not discuss the planned developments in frame of this article, however, it is important to stress out that data protection legislation is a dynamic process in Europe where global leading developments occur in the field.

3. Protection of personal data in the turkish jurisdiction

Turkey was lack of a single personal data protection law until 2016. The Law was enacted upon the constitutional amendment referendum held in 2010, that brought many legal developments in human rights protection, as expressing the personal data protection as a single right. During the preparation and after the enactment, it immediately interpreted as harmonization of the 108 Convention and 95 Direction. Although the 95 Direction will be replaced as a Regulation next year, this seems very important step for the country to follow updated and European developments in this field.

Prior to the Law, there were many sector based regulations for protection of personal data. These sectors were mainly the ones that the technologic developments that affected very quickly. E-communication, e-banking, e-commerce and anything contains "e" was regulated with a personal data protection. However, different implementations and lack of a Law guidance and power was creating a disadvantageous situation for the country. Staying out of these global developments created obstacles for the country, for example, Turkey could not collaborate with the EU agencies such as

[10] GREENLEAF, GRAHAM: 'Modernising' data protection Convention 108: A safe basis for a global privacy treaty?, in *Computer Law&Security Review* (2013), 29, 431, http://dx.doi.org/10.1016/j.clsr.2013.05.015.

Europol for intelligence exchange. This missing point was always expressed in the EU-Turkey Progress reports from the year that Turkey was announced as a candidate country, since 1999[11] until the adoption of Personal Data Protection Law, 2016. This created political pressure on the country which may be assumed as a boosting effect for the country's legal development in this field. Although sectoral data protection steps taken, sectoral regulations swelled up the legislation with no comprehensive interpretation possibility. Turkey took a huge step with enactment of Personal Data Protection Law.

The Law consists of 7 Chapters and 33 Articles. Basic principles in the law are found very similar to the EU Directive by most of the Turkish scholars.[12] The definition of personal data is as comprehensive as the other international legislation and expressed as "any information belongs to natural person(s) who is identified or identifiable". In compliance with the other examples, Turkish Personal Data Protection Law also differ the sensitive or special categories of personal data, data related to ethnicity, political opinion, religion, appearance (clothes), health, and sexual life. As a general rule, both data types cannot be processed without an explicit consent of the data subject. The explicit consent is defined as "freely given consent based on pre-given information on a specific subject". This may certainly cause wrong implementation of the Law, because it does not stress the form of the consent whether it is written or oral declaration or just putting a sign on the check-box on the virtual world could be enough.

The processing activity should be restricted with the purpose and scope of the processing. In the Law, processing principles are base on the data subject's consent which means that there can be processing activity without a consent of the data subjects. Out of consent cases are generally referring to the fact that the activity only can be done in a legitimate basis such as, if the data is already made public by the data subject, it is necessary for the public safety and security, or if processing is necessary to fulfill a legal obligation of the data controller. While the data controllers are bind with the processing rules, they also must ensure transparency, accession and erasure rules. They also must not transfer the personal data neither inside the country nor outside of the country, without a legitimate basement.

The Law clarifies the basic principles of data processing, the circumstances, and exceptions for data processing, responsibilities of the data controllers, legal remedies, and sanctions. Establishment, competences, working principles, personnel and the budget of the Personal Data Protection Authority and the Board for Data Protection thoroughly explained. The Board would be established 6 months later the Law was enacted, which was in April 2016. Unfortunately, there is no formal information

[11] All the reports are available at: https://ec.europa.eu/neighbourhood-enlargement/countries/package_en.

[12] KORKMAZ, IBRAHIM: An Assessment of The Law on Protection of Personal Data, in *Turkish Bar Association Journal* (2016) 124, 81–152., BAĞCI, GÖKHAN UĞUR: *14 Soruda Kişisel Verilerin Korunması Kanunu. E-ticaret ve internet hukuku,* http://www.eticarethukuku.com/14-soruda-kisisel-verilerin-korunmasi-kanunu#more-176 [2016-11-10], TOKSOY, FEVZI – BALKI, BAHADIR – YILDIZ, SERA ERZENE: *Data Protection in Turkey: overview. Practical Law Multi-Jurisdictional Guide,* http://us.practicallaw.com/7-520-1896?q=turkey [2016-11-11].

verifying the establishment of the Institution while we publish this work. Some of the news websites quoted from each other that the Head of the Institution and the members were elected in the Parliament, but the Institution is still not ready. Current political issues in Turkey such as terrorist attacks, 15th of July military coup attempt and adopting state of emergency after it, and constitutional amendment which will result with switching the parliamentary system to the presidential system might be effective for this slow development, we guess.

The data controllers' responsibilities and duties according to the Law are closely related to the legal collection, storage and processing activities. For this reason, data controller should inform the data subjects during the collection. Informing activities should at least consist of the purpose, transfer, method and legal basement of the collection, and the rights of the data subjects finally. In frame of their rights, the data subjects have a right to learn whether their data is being processed, if yes, ask for information about the process, ask for the purpose of the process and whether the processing complying with this purpose, ask for rectification, erasure or destroying if the processing is not complying with the purpose, and ask for the data controller to inform if the data is transmitted to third parties. As it is already seen in the Law, all the rights and rules are closely related to the processing activity. During the processing, besides legal basement, there are principles for the data controllers to follow. These principles are:

- The data should be accurate and kept updated if necessary,
- Should be processed for certain, explicit and legitimate purposes,
- Processing should be limited, related and restrained with its scope,
- Should be stored in a limited time within its scope.

The rest and the most of the Law is about the needed supervisory body, so we can dismiss this part due to its irrelevance with our case. In frame of the basic rules and principles, now we can review the present case.

4. Cemalettın canlı vs. Republıc of turkey case[13]

Although Turkey's personal data protection framework had been developed slower than European practices, there were not much cases carried to the ECHR. We do not interpret it negatively, instead, the reason behind could be the national mechanisms were found enough for protection of such right. As we already indicated before, lack of data protection law was found an obstacle for international collaboration in the certain fields but there were no cases stayed unsolved in Turkish jurisdiction related to personal data protection. Still, the Personal Data Protection Law was necessary for Turkey and adopting such law ensures better protection for the fundamental rights.

[13] Judgment of the European Court of Justice of 6 October 2009. Cemalettin Canli vs. Belgium. Case C-6/09 available at: http://hudoc.echr.coe.int/eng?i=001-89623.

4.1. Merits of the Case

The Plaintiff, Cemalettin Canli is a known sociologist with number of publications. In 1990, he was prosecuted to be involved with an illegal organization known as left-communist group of people named "Revolutionary Youth" and "Revolutionary Path". It should be noted here that in Turkey, sadly, some of the organizations used these kind of "fancy" titles to cover themselves because they generally do not purely target to stress out what do they think democratically, but serve to some other purposes, like terrorist activities. Unfortunately, these kind of groups generally contain also "bad guys" besides the innocent believers. As we can see in this case also, not all the members of such organizations are treated as bad guys; hence Mr.Canli was neither arrested, nor punished after the interrogation. He was released right after his investigation. Later on, in August 2003, while he was going to a demonstration organized by the Confederation of Public Workers' Unions in Ankara, which is totally legal organization, he was arrested by the police after a brawl between policeman and a group of demonstrators including him. While 26 policemen injured, Mr.Canli claimed that he was beaten by the police. At the same day, the police prepared a report which describes this issue. The report had an addition information related to the Plaintiff's background that he was previously convicted. The report clearly contained that "he had a previous record for terrorist related activity". The report was presented to the Prosecutor's office in Ankara. The Prosecutor decided according to the Demonstrations Act of Turkey, accusing Mr.Canli and others from the group for damaging state property and resisting arrest by using force. Upon this decision, the case devolved to the Ankara Criminal Court of First Instance. There, a police presented a new report to the court called "Records of Guilt", which includes his fingerprints, address and birth information, also his past involvements in 1990 in accordance with Police Regulations on Fingerprinting. He was in a position that he was found guilty in the past and it should be known by the Prosecutor.

Mr. Canli became a Plaintiff starting from this point, from January 2004. He first lodged a complaint to the Public Prosecutor showing that he was acquitted from this case and this case should not be presented again here by the police. He pointed out that the above-mentioned Regulation should contain the rule of exclusion of such information from the police records. By this way, the policeman who prepared the report against him breached the Regulation according to him. While the case is running, one of the press released a news including the following information: one of the captured is a member of an illegal organization, Revolutionary Youth. Upon that, he claimed that this report damage the presumption of innocence because he is a known person and his reputation damaged with the news.

In February 2004, the Public Prosecutor refused his claims giving as a reason that the police "just" informed the court about the past of him. The Plaintiff claimed that the Public Prosecutor made his/her decision based on a missing information because he or she did not even mention about the Regulation, which the plaintiff referred to be reviewed in his application. The applications were refused giving as a reason that the policeman only informed the prosecutors. He extended his application as claiming that some of his rights in the European Convention of Human Rights were violated starting from fair hearing to respect to family life. His this application was also refused and on December 2005, he was acquitted from the case.

Aftermath, the case was closed in Turkey not in favor of the Plaintiff's claims. However, once his fame and family was damaged, he kept seeking his rights in the ECtHR. He lodged his complaint to the Court, claiming that there is a violation of the Article 8, entitle "Right to respect for private and family life". The ECtHR judges analyzed the application step by step. The basement of the judgement was the Article 8 of the ECHR, but Convention 108 was interpreted widely because of the merits of the case fit exactly to the Convention. Whenever the ECtHR receives a case, it always starts from evaluating it according to admissibility criteria of the Court. The ECtHR admissibility criteria is very clear and simple.

Firstly, the Government of Republic of Turkey draw the attention of the Court on the application must be counted as inadmissible because the Plaintiff were not exhausted the domestic remedies. The judges agreed on the fact that the Plaintiff's efforts were not taken serious and would not have been taken neither even if he kept trying. The Government claimed that keeping the records has a legitimate basis; but the Government did accept that it should have been amended with the right information. The Government also argued that the Plaintiff should have seek his right against the newspaper. However, the newspaper company did not make anything lawful; the news was released as it was received by the Prosecutor. The Plaintiff did not have chance to ask for correction of his data because he did not know that his records are kept wrong and also he already complained about it to the court.

The ECtHR judges agreed that the information that the Prosecutor gained from the policeman under the title of "Records of Guilt" report mentioned about him as he is still a member of an illegal organization which breaches protection of his reputation. Passing such inaccurate information to Public Prosecutor against him also breach his right to privacy. It was not a necessity for public security nor the public to know this record; so here the judges decided that this information was related to his private life. The most important part of the judgement is the fact that the Police Regulations on Fingerprinting orders to the law enforcement agencies to keep all information up to date by attaching all related information about the individuals. So, Turkey was fined with 5.000Euro for pecuniary damage plus 1.500Euro for costs and expenses of the Plaintiff.

4.2. Result

If Turkish Personal Data Law was enacted prior to this case, the interpretations as well as the fine would be different. Article 4 of the Law is drawing the general principles for data processing rules, which oblige the data controller (related Police Department, in our case) to keep personal data (Mr.Canli's records) updated and accurate. Article 5 of the Law shows the rule for data processing; the personal data cannot be processed without an explicit consent of the data subject (Mr.Canli). Because the Plaintiff was under the investigation procedure and this procedure regulated with another law which makes the data controller not to require the consent of the data controller, he would not get much advantage of this article. However, it is the Plaintiff's right to know what records are kept about him especially at the law enforcement agencies archives. The Plaintiff did not even know that his records are kept and it is kept inaccurately. Article 6 of the Law prevents persons from processing their sensitive data without their consent, which is in this case, his political opinions and philosophical beliefs and more

importantly, his criminal records. The news released about him was showing him as criminal as well as it was possible to guess his political opinions from the organizations' names that he was member of. The policemen caused actually more damage to his private life than the ECHR interpreted.

As the Section 5 of the Law orders, both the policemen and the police department would be punished. Because the Plaintiff was not informed that his records are being kept, the police department would be punished from 5.000 to 100.000Turkish Lira (TL) (approx. 1.000Euro to 25.000Euro). Because the data was acquired and released by the newspaper, there could be another punishment for the department. This data is not a public data and it should have kept secure by the department, so there could be fine from 15.000TL to 1.000.000TL (approx. 4.000Euro to 250.000Euro). The most importantly, apart from the fine, there would be disciplinary proceedings against the policeman who shared these information with the Prosecutors. If this Law was enacted, there would be significant timeframe to keep such information. If the policeman kept these data more than it is necessary, there could be other punishments according to Turkish Criminal Code. Finally, if this Law and the Board was active prior to the case, may be the Plaintiff could apply to the Board. The Board probably would decide in favor of the Plaintiff, so there would not be any harm for the both Parties. So, if the Law was enacted before;

- There would not be need for going until the ECtHR and loose time,
- There would be more compensation gained by the Plaintiff,
- There would not even be need for such complicated procedures, because the Plaintiff could access to the Board and the Board would decide in favor of the Plaintiff.

List of References

[1] BAĞCI, GÖKHAN UĞUR: *14 Soruda Kişisel Verilerin Korunması Kanunu. E-ticaret ve internet hukuku,* http://www.eticarethukuku.com/14-soruda-kisisel-verilerin-korunmasi-kanunu#more-176 [2016-11-10].

[2] GREENLEAF, GRAHAM: 'Modernising' data protection Convention 108: A safe basis for a global privacy treaty?, in *Computer Law&Security Review* (2013).

[3] GUTWIRTH, SERGE – POULLET, YVES – HERT, PAUL DE: *Data Protection in a Profiled World,* 2010, Springer, Dordrecht-New York. http://search.ebscohost.com/login.aspx?direct=true&db=edshlc&AN=edshlc.012582268-5&lang=tr&site=eds-live&authtype=ip,uid.

[4] KIERKEGAARD, SYLVIA – WATERS, NIGEL – GREENLEAF, GRAHAM – BYGRAVE LEE A. – LLOYD, IAN – SAXBY, STEVE: 30 years on-The review of the Council of Europe Data Protection Convention 108, in *Computer Law&Security Review* (2011), 27, 231, doi:10.1016/j.clsr.2011.03.007.

[5] KORKMAZ, IBRAHIM: An Assessment of The Law on Protection of Personal Data, in *Turkish Bar Association Journal* (2016).

[6] KÜZECI, ELIF: *Personal Data Protection*, 2010, Unpublished doctoral thesis, Ankara, Ankara University Institution of Social Sciences, Ankara.

[7] SAVOIU, ALINA – BASARABESCU, C. CATALIN: The Right to Privacy, in *Annals of the Constantin Brancusi University of Targu Jiu Juridical Sciences Series,* 2013.

[8] TOKSOY, FEVZI – BALKI, BAHADIR – YILDIZ, SERA ERZENE: *Data Protection in Turkey: overview. Practical Law Multi-Jurisdictional Guide,* http://us.practicallaw.com/7-520-1896?q=turkey [2016-11-11].

[9] WRIGHT, DAVID – RAAB, CHARLES: Privacy principles, risks and harms, in *International Review of Law, Computers & Technology,* 2014, 3, 28, 278.