UNIVERSITY OF TARTU

SCHOOL OF LAW

Department of Public Law

Aykut Özgürsoy

COMPATIBILITY OF EMPLOYEES' PERSONAL DATA PROTECTION IN TURKEY WITH INTERNATIONAL LEGAL AND *DE FACTO* STANDARDS

Master's Thesis

Supervisor

Prof. Aleksei Kelli

Tallinn

2021

TABLE OF CONTENTS

INTRODUCTION

Throughout history, the right to privacy has been always one of the most important and debated human rights mainly because of its fragility, the obscurity of its limitation and potentiality to clash with other human rights. It has been debated mostly traditionally however with the rapid development of technology especially the invention of technology, like other human rights and whole law areas, the right to privacy sure was affected to a large extent.

Set aside other reasons, the main reason for the change of the right to privacy is that internet has connected almost all people all around the world. With this way, all types of data belonging to individuals have been gathered into one place and stored. Dataflow is now beyond measure. Data of individuals thus became much easily reachable and the right to privacy became much vulnerable compared to former times. There have been and still are serious concerns regarding this issue. For example, Scott McNealy one of the most known businessmen and the back then the CEO of Sun Microsystems answered these kinds of concerns as "You have zero privacy anyway, get over it."[1] as if it is impossible to prevent interventions directed to the data.

These righteous concerns have opened a road for legislations throughout the world with intense disputes. For a long time, data protection had been evaluated under the topic of the right to privacy in terms of human rights law. Because of the different technicality and more complex nature, data protection during recent years has been defined as an independent topic. It is now in a transition stage and will become a completely separate topic in human rights law for certain. However, it is undeniable to refuse the fact that data protection and the right to privacy are related with each other significantly.

With the establishment of the protection system of data, sub-titles have been started to be debated. One of the most controversial areas for data protection has been the one between employers and employees. This is because this type of relationship has always been conflicting and constantly creates novel problems for all legal areas. This relationship by nature is clashing due to the fact that both parties have critical interests and contradictory rights. Additionally, most times of their lives, both parties are in workplaces and affect each other constantly.

[1] Sprenger, P. Sun on Privacy: 'Get Over It'. 1999. Accessible at: https://www.wired.com/1999/01/sun-on-privacy-get-over-it/

Former times, this relationship was still problematic mostly because of the frequent contradiction between the right to property and right to govern of employers and the right to privacy of employees. This issue has evolved with the rapid development of technology. Employers with the new technologies and devices now have much easier ways to collect data of their employees, monitor correspondences, make surveillance of workplaces, record working times and so on and so forth.

It is the fact that with the boundaries of the law, employers have a right to process data of their employees and premises, however, processing must be limited with some conditions given by regulations and judicial decisions. Otherwise, the rights of employees concerning privacy would be in jeopardy. Because, by the urges of employers and the nature of this relationship, employers always want more control over their employees, premises and businesses due to the fact that they always want their business is working smoothly as possible as it is. Hence, employees in terms of data privacy should be protected intensely.

In addition to the reasons given above, it should be also said that in this relationship, there is an obvious imbalance in terms of power over each other thus it should not be evaluated in terms of data protection like in the relationship between businesses and customers. Because in the latter one there is a comparatively equal relationship. However, employees are so much vulnerable when it comes to their relationship with employers. That is to say, the general rules of data protection in some circumstances may not be effective as it is normally in the relationship between employees and employers. Given the fact that everyone is vulnerable whether they are customers, citizens, students and so on, it must be accepted the fact that employees are in worse conditions.

The first stage should be taken is defining the term personal data and determining the limits thereof to understand the content and the scope of the protection of personal data by the law in a broad sense. Afterwards, it would be easier to detect what are the deficiencies when it comes to the protection of personal data and what needs to be done for further protection. However, before defining the personal data which is more related with the legal sphere and this work, the concept of data should be briefly evaluated. Data can be said is sounded both technical and legal concept often being used by almost everyone attracted by it excessively without knowing its meaning. Apart from its more technical definition, it is more important to realize the meaning within the realm of law.

Firstly, the lexical meaning of the data should be set forth. Etymologically, data as a word is the plural form of the Latin word "datum"[2] and may refer to the meaning of "a given."[3] Data can be described comprehensively as the "symbols that represent properties of objects, events and their environments."[4] In addition to the etymological approach of the term data, it should also be put out that the "meaning of data, information and knowledge can be used interchangeably"[5], hence relations with the other concepts such as information and knowledge should be examined as well.

Regarding those three concepts, it can be said that they have different meanings even if they are used on behalf of each others' place. Where data has no meaningful content by itself, when it is processed with various methods then it can acquire some meaningful content thus can be called information. That is to say, data is often used as raw or unrefined data where information is used for refined, useable data with meaningful content and whole.[6]

When it comes to knowledge, it can differ as per meaning from the former two mainly because it defines the third level comes after the information. It can be defined as "learnt and comprehended information."[7] It somehow includes the answer to the question of how rather than what or who as in information level.[8] After the knowledge level, other concepts are being reached respectively understanding and wisdom. The whole system is called as Data-Information-Knowledge-Wisdom Hierarchy (The DIKW Hierarchy[9]) and it defines the vertical relationships between those terms which are used as "the blocks of library and

[2] Accessible at: https://www.oxfordlearnersdictionaries.com/definition/english/data?q=data
[3] Wilkinson, L. The Grammar of Graphics. (Statistics and Computing). Second Edition, 2005, Springer, Page 42.
[4] Ackoff, R. L. From Data to Wisdom. - Journal of Applies Systems Analysis, Vol 16, 1989, p 3. Accessible at: http://www-public.imtbs-tsp.eu/~gibson/Teaching/Teaching-ReadingMaterial/Ackoff89.pdf
[5] Sander, J.D. Terms: Data, Information and Knowledge. - SAI Computing Conference, London, 2016, Page 1. Accessible at: https://www.researchgate.net/publication/305474792_Defining_Terms_Data_Information_and_Knowledge
[6] Liew, A. Understanding Data, Information, Knowledge and Their Inter-Relationships. - Journal of Knowledge Management Practice, Vol. 7, No. 2, 2007, Page 2.
Accessible at: https://www.researchgate.net/publication/224937037_Understanding_Data_Information_Knowledge_And_Their_Inter-Relationships
[7] Wang, Y. Formal Cognitive Models of Data, Information, Knowledge, and Intelligence. - WSEAS Transactions on Computers, 2015, Page 775.
Accessible at: http://www.wseas.us/journal/pdf/computers/2015/b5072610-109.pdf
[8] Ackoff, R. L. From Data to Wisdom -Journal of Applies Systems Analysis, Vol 16, 1989, Page 4.
[9] Baskarada, S., Koronios, A. Data, Information, Knowledge, Wisdom (DIKW): A Semiotic Theoretical and Empirical Exploration of the Hierarchy and its Quality Dimension. - Australasian Journal of Information Systems. 18(1), 2013, Page 6.
Accessible at: https://www.researchgate.net/publication/279942958_Data_Information_Knowledge_Wisdom_DIKW_A_Semiotic_Theoretical_and_Empirical_Exploration_of_the_Hierarchy_and_its_Quality_Dimension

information science".[10] All in all, when it comes to information science, data, information, knowledge and wisdom are the layers of a whole system.

Apart from the distinction between data, information and knowledge, in terms of legal approach, it is much more important to focus on the varieties of data groups, definitions and limitations thereof. Because the law implemented is used as per the types of data in the present case. Additionally, case law can be differentiated. Hence, it should be looked at the definitions in the international and regional instruments with the national legislation in Turkey by force of the scope of the work.

Human rights instruments such as the ICCPR, the ECHR, the CFREU and so on do not include a specific definition of personal data. In fact, aside from the CFREU, other instruments do not include a provision regarding personal data let alone defining it. However, regional legislation such as the General Data Protection Regulation of the European Union("GDPR") and national legislations such as Turkish Personal Data Protection Law ("Law no. 6698") have the exact provision involving the definition of personal data.

The GDPR art. 4 and the Law no. 6698 art. 3 define personal data as "any information relating to an identified or identifiable natural person."[11] Thus, as per these legislations, the most important thing to determine the personal data is whether that data can relate to a natural person. It should be also noted that Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention no. 108") art. 2 has the same provision. Therefore, although the central and technical meaning may be varied from time to time and person to person, regarding the definition of the concept of personal data, it can be said that there is widely acknowledged consensus within the legal sphere.

It should be said that only processed data can be subject to data protection law. If data is not processed which means that it is raw, then it is not within the scope of the protection system. Likewise, even if data is processed, if it is not "concerning identified or identifiable natural person"[12] then it cannot be protected by law. Such data is called anonymous data and it is "the

[10] Bernstein, J.H. The Data-Information-Knowledge-Wisdom Hierarchy and its Antithesis. City University of New York Academic Works Publications and Research, 2009, Page 68. Accessible at: https://academicworks.cuny.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=1011&context=kb_pubs

[11] General Data Protection Regulation. Strasbourg, 27.04.2016, e.i.f.25.05.2018, Article 4.
Turkish Personal Data Protection Law ("Law no. 6698"). Ankara, 24.03.2016, e.i.f.24.03.2016, Article 3.

[12] General Data Protection Regulation, op.cit., Recital 26.

opposite of personal data."[13] The problem of which data is personal and which are not should be looked at case by case. Hence, it can be said that case law is highly important when it comes to solving this problem.

One case of the CJEU can be given to this situation as an example. The decision was made for joined cases of Rechnungshof and others. Cases are mainly regarding the employees' income as personal data. Even though the questions from the national courts are formulated differently, evaluations of the CJEU are important for this work are that "the monies paid by certain bodies and the recipients, constitute personal data" and "the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights".[14] It also states the fact that collection of information of income as personal data "falls within the scope of Article 8 of the Convention of The European Court of Human Rights."[15] In this decision, the CJEU has underlined the importance of the main principles of proportionality, lawfulness and so on when it comes for states to legitimize their interference of the right to privacy.

All in all, when data is processed and can be defined as some information regarding a natural person, it should be protected against possible infringements and violations. Some types of personal data are under more specific protection because of their fragility such as health data. Nonetheless, whether it is sensitive data or not, if the conditions are met mentioned above, it should be protected by the data protection law.

Regarding this work, it can be said that by nature, employees are natural persons and their data which is in the hand of the employers by a majority are personal data hence their personal data fall into the realm of data protection law.

The other concept which is important in terms of the scope of this work is "employee". The right to privacy and more specifically data protection rights are such rights that belong to all people regardless of their race, social status, gender etc. This is the main principle of human rights however for the sake of this work, the topic should be limited to a specific group of

[13] Purtova, N. The law of everything. Broad concept of personal data and future of EU data protection law. - Law, Innovation and Technology, 10:1, 2018, Page 43.
Accessible at: https://www.tandfonline.com/doi/pdf/10.1080/17579961.2018.1452176?needAccess=true
[14]The Joined Cases C-465/00, C-138/01 and C-139/01, CJEU, 20.05.2003, para. 68. Accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62000CJ0465&from=EN
[15] Ibid, para.73

people and special circumstances thereof. The threat for violation of the data protection rights of the employees is much higher and their conditions should be evaluated carefully.

ILO, when it established its only instrument regarding this issue called the Code of Practice on the Protection of Workers' Personal Data, it used the term "worker" instead of employee or laborer. In this document, the term worker is defined in the art. 3.4 as "any current or former worker or applicant for employment."[16] This definition simply comprises three main groups which are current workers, former workers or applicants. Why it counted applicants in the definition is that when applications for employment have been made, there are plenty of personal data given by applicants to expectant employers thus their personal data should be evaluated as if they are already employees. Because, employers need those kinds of personal data from applicants for various reasons such as complying with the law, selecting the best candidate in addition to that general reasons like "protecting the assets of the company and providing security."[17] However, it can also cause discrimination such as that applicant may not be employed not because of lack of skills but because of something related to applicant's private life that is learned by employer while collecting data.[18] Hence, this area should also be evaluated by legislation or case laws and applicants should be protected compatible with their situations under the data protection law system.

In the GDPR, on the contrary of the Code of Practice of ILO, the term employee has been used in art. 88 and Recital 155 instead of worker however the content and the meaning remained the same. Additionally, European Data Protection Board is generally using the term employee. For example in one of its guidelines regarding consent, it used the term employee to state this group of people.[19] ECtHR and CJEU are also using the term employee for this topic. They also look at cases regarding these issues whether employer is public or private entities. Hence, it can be said that in terms of personal data protection, employees are not divided into two separate branches as public or private employees.[20]

---

[16] Code of Practice on the Protection of Workers' Personal Data, ILO, Geneva, 1997, Article 3.4.
Accessible at: https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf

[17] Abdurrahimli, F. Big Boss is Watching You! The Right to Privacy of Employees in the Context of Workplace Surveillance. Master Thesis. Lund University, 2020, Page 9.
Accessible at: https://www.researchgate.net/publication/342040621_Big_Boss_is_Watching_You_The_Right_to_Privacy_of_Employees_in_the_Context_of_Workplace_surveillance

[18] Bronstein, A. International and Comparative Labour Law. Current Challenges. ILO, 2009, Page 184.

[19] Guidelines on consent under Regulation 2016/679, The EDPB, 04.05.2020, para.20.
Accessible at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[20] Recommendation No. R (89) 2, Coe, 18.01.1989.
Accessible at: https://www.coe.int/t/dg3/healthbioethic/texts_and_documents/Rec(89)2E.pdf

The subsequent questions will assist to verify the hypothesis;

- Is Turkish legislation compatible with various international and regional instruments especially with the Convention no. 108, the GDPR and ECHR regarding the protection of employees' personal data?

- Is Turkish case law comprehensive enough and in accord with the case law of ECtHR in terms of protection of employees' personal data especially in terms of common types such as video surveillance, monitoring correspondence and monitoring by facial recognition and fingerprints systems?

Some legislations have been established all around the world regarding data protection. Most famous and the one that created de facto standards for data protection is the GDPR. After the establishment of the GDPR, Turkey instituted its own data protection regulation not by looking at the GDPR but by making the former directive an example. One of the main reasons for the establishment of the GDPR was the deficiencies of the former directive hence it can be said that just looking at this fact the data protection law of Turkey is not compatible with the GDPR and has deficiencies that will be given in this work.

It should be also said that, although the GDPR is not directly applicable in Turkey, it is becoming a *de facto* standard for personal data protection. Therefore the author evaluates the compatibility of Turkish law in the field of employment with the GDPR.

Data protection in combination with technological development continuously remains to pose complex problems which have to be studied and discussed. The discussions are not limited to Europe but take place throughout the world, including Turkey. The discussion is reinforced with the adoption of the GDPR just before the GDPR entered into force; Turkey published its new law no. 6698 which is mostly the translation of the former directive 95/46/EC regulating the area of personal data protection. The law has some inefficient provisions with regards to the protection of personal data of employees and general inefficiencies concerning the concept of consent, basic principles and so on.

Besides the Law no. 6698, there are other regulations regarding this issue but they are not so effective to protect the employees' personal data rights. For example, the labour legal law includes just one provision regulating the area of personal file. The provision is wide, vague

in terms of meaning and outdated. The author argues that Turkish legislation concerning employees' personal data protection is not compatible with international legal and *de facto* standards such as ECHR, the Convention no.108 and the GDPR. Turkish legislation does not effectively protect human rights in this aspect.

The author evaluates the Turkish jurisprudence in the light of case law of the European Court of Human Rights regarding the right to privacy. Some judicial decisions (especially decisions of the Turkish Constitutional Court) with regards to consent are not compatible with the ECtHR approach. Moreover, the Turkish Data Protection Board which has been established by the Data Protection Legal Act (Law no. 6698) based on the Convention no. 108 has some important cases regarding this issue which is not so effective in terms of protection.

The objective of the present study is to evaluate the compatibility of Turkish data protection law concerning the personal data protection of employees with international legal and *de facto* standards such as ECHR, the Convention no.108 and the GDPR.

The hypothesis of this thesis is that the Turkish data protection law by legislation and case law is not efficiently protecting employees' personal data. There are some deficiencies in terms of data protection such as the lack of capability of consent, absence of some basic principles such as accountability and so on. Turkish data protection law should be adjusted in order to be compatible with the GDPR.

Additionally, there is a need for new legislation which should cover the area of protection of employees' data by regulating some topics such as special circumstances of video surveillance at workplaces, monitoring correspondence and usage of technical devices, facial recognition and fingerprint systems and so on and so forth.

Furthermore, even if case law is not comprehensive to compare, when some decisions of Turkish courts especially the Turkish Constitutional Court in terms of monitoring correspondence there are some incompatibilities with the criteria set forth by case law of the ECtHR. The decisions regarding other common areas such as monitoring by facial recognition systems, fingerprint systems and video surveillance are mostly in accord with each other.

In order to substantiate the hypothesis set forth above, this work implements analytical and comparative methods within the scope of human rights law. It specifically aims to evaluate

the system implementing because of the absence of effective protection system in Turkey is getting less an effective from day to day in the presence of the new technologies.

The need for a more efficient protection system for personal data of employees is being expressed by international and regional organizations and Turkey is still debating whether there is a need for change data protection law in general let alone thinks to improve this specific area. The paper analyses firstly international and regional protection of the right to privacy and data protection rights of employees, subsequently compares them with Turkish legislation and underlines the discrepancies of the Turkish legislation in terms of data protection in general and specific protection of employees' personal data.

Moreover, it analyses the most common infringement types with the case law of the ECtHR and compares them with the case law of Turkish courts, especially the Turkish Constitutional Court, the Council of State and The Turkish Data Protection Board.

Former researches in this area are formed mainly within the scope of labour law which is one of the branches of private law. On the contrary, this work approaches the subject in the field of human rights law and evaluates the issue from the perspective of the right to privacy, personal rights and so on and so forth. Additionally, this work as a new narrative underlines the importance of independent legislation when it comes to protection of personal data of employees.

This work consists of three chapters. The first chapter will try to evaluate the effectiveness of the international and regional regulations with regards to the protection of personal data of employees having regard to the undeniable link between the right to privacy and data protection law.

In the second chapter, Turkish data protection law will be analyzed and some deficiencies will be underlined such as the necessity of a general act in order to protect personal data of employees and the incompatibility of Turkish data protection law with the GDPR.

The third chapter will be comprised of three common problematic types of data protection law in employment context which can be listed as video surveillance at workplace, monitoring of correspondence and facial recognition and fingerprints systems.

These issues are not strictly linked with the field of employment but can be considered as some of the most problematic areas in data protection law in general. For the sake of the limit of this work, these common types will be evaluated with the case law of the ECtHR and Turkish courts especially the Constitutional Court and the Council of State whether they are in accordance with each other and Turkish case law, in general, is comprehensive when it comes to protection of employees' personal data.

Keywords: the right to privacy, data protection, employee, workplace

1. DATA PROTECTION LAW IN EMPLOYMENT CONTEXT

1.1. Evaluation of the International Protection of Employees' Personal Data

When it comes to international regulations concerning data protection, firstly provisions with regards to the right to privacy should be set forth because of the undeniable link between the right to privacy and data protection. Afterwards, more specific data protection regulations should be examined.

The right to privacy, because of its important link to data protection law, is one of the basic concepts. Although data protection is an independent branch from the right to privacy protection nowadays, it is a fact that it stemmed from the right to privacy. Even though it is being said that "Data protection and privacy are related but nevertheless distinct concepts"[21], the issue concerning the distinction between data protection rights and the right to privacy is not accepted consensually.

For example, in the Directive (95/46/EC) had been regulated the area of data protection within the EU, personal data has been protected as if should be protected under the right to privacy. However, after the acceptance of the provision regarding the protection of personal data in the CFREU[22], the GDPR also is established to protect the personal data on the grounds of the independent data protection rights from the right to privacy. In the meantime, the ECtHR is still using the right to privacy in ECHR on account of the protection of personal data in its case law. It did not accept it as an independent branch yet.

Whether data protection will henceforth be acknowledged as a distinct branch from the right to privacy or not, it is the fact that between data protection and the right to privacy there is "a strong linkage"[23] and the importance of the right to privacy when it comes to the protection of personal data is obvious.

[21] Dove, E.S. EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. - The Journal of Law Medicine & Ethics, 46, 2018, Page 1014.
Accesible at:
https://www.researchgate.net/publication/330316678_The_EU_General_Data_Protection_Regulation_Implications_for_International_Scientific_Research_in_the_Digital_Era/link/5c581528a6fdccd6b5e1620a/download
[22] Charter of Fundamental Rights of the European Union("CFREU"), Strasbourg, 26.10.2012. Article 8.
[23] Lloyd, I.J. Information Technology Law. Oxford University Press. 8th Edition, 2017, Page 34.

The right to privacy has been one of the most important and controversial human rights in history. It maybe has always been existed with humankind. However, as a legal concept in terms of the human rights sphere, it is said to be advocated in the famous article called "Right to Privacy" by Samuel Warren and Louis Brandeis and in this article, it is seen that it is also mentioned as a "right to be let alone."[24]

Right to privacy is such a right hard to define and has not been defined well notwithstanding the fact that it is considered "at the heart of much civil libertarian thought".[25] The meaning of privacy has been changing from time to time[26] and has been evaluated and determined again and again.[27] The ECtHR also avoided and stated in its one of the trademark cases[28] with regards to the right to privacy that defining and limiting the notion of private life is not "possible or necessary to attempt."[29]

However, the definition and limitation of the right to privacy maybe have never been controversial like this day. Additionally, the right to privacy itself "appears more important and relevant today than ever."[30] The reason is mainly because the transformation that has been generated by the digital age. Due to the digital age, the transformation of human relations, collection and processing of huge amount of data and intense usage of the internet, privacy has become vulnerable day by day.

The other important thing concerning the right to privacy apart from the struggle when trying to define is that it is constantly clashing with other fundamentally accepted rights such as freedom of expression[31], freedom of the press, freedom of obtainment of information and so on and so forth. Due to these clashes, the subject becomes more and more important and fragile. Therefore, it should be focused carefully to not harm others when this right is tried to

[24] Warren, D.S., Brandeis, L.D. The Right to Privacy - Harvard Law Review, Vol. 4, No. 5, 1890, p. 195. Accessible at: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf
[25] Robertson, D. A Dictionary of Human Rights. Europa Publications. 2nd Edition, 2004, Page 179.
[26] DeVries, W. Protecting privacy in the digital age. - Annual Review of Law and Technology, Berkeley Technology Law, Vol. 18, No. 1, 2003, Page 283-311.
[27] Warren, D.S., Brandeis, L.D. The Right to Privacy, op.cit., Page 193.
[28] Niemietz v. Germany, judgment, App. No. 13710/88, ECtHR, 16.12.1992. Accessible at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22\%22CASE%20OF%20NIEMIETZ%20v.%20GERMANY\%22%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-57887%22]}
[29] Mowbray, A. Cases and Materials on the European Convention on Human Rights. Second Edition. Oxford University Press, .2007, Page 485.
[30] Penney, J. The Right to Privacy. The end of Privacy Fatalism. Human Rights, Digital Society and the Law A Research Companion(Ed.Mart Susi). Routledge. 2019, Page 44.
[31] Lloyd, I.J. Information Technology Law. op.cit, Page 32.

be protected.[32] For example, when the issue is to collecting and processing data, it should be done balanced with the right to seek information.[33]

If classical human rights instruments would be examined in terms of the right to privacy, it can be seen that there is a consensus regarding it. For example, in the ICCPR art. 17 asserts that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."[34] whereas the ECHR art. 8 "Everyone has the right to respect for his private and family life, his home and his correspondence."[35]

One additional example of the above ones can be given from the CFREU art. 7 which declares that "Everyone has the right to respect for his or her private and family life, home and communications."[36] It should also not be forgotten that the right to privacy can be limited under specific circumstances such as other non-absolute rights. Also, it must be admitted that these provisions are "broad and vague"[37] in terms of definition and limitation.

Ultimately, it can be said that the right to privacy is such a right hard to determine the scope and it has been and still is changing constantly. However, maybe one of the most affecting eras is the digital age in terms of the transformation of the right to privacy. This is the main reason that the data protection law as an independent branch has emerged. Nonetheless, the right to privacy, especially because it is conflicting perpetually with other fundamental rights, is one of the most controversial human rights.

Within the scope of this work, it also should be said that the protection of the personal data of employees is considered as both the right to privacy and/or a data protection issue nationally and internationally. Employees' data protection has emerged as an important problem primarily because of two developments. One of them is the new technological developments which has made much easier for the intrusion of the employees' private life by employers and

[32] Jeffery, A. J. Free speech and press: An absolute right? - Human Rights Quarterly, 8(2), 1986, Page 225.
[33] Land, M. Toward an International Law of the Internet. - Harvard International Law Journal. Vol 54 No. 2, 2013, Page 430. Accessible at: https://harvardilj.org/wp-content/uploads/sites/15/2013/10/HILJ_54-2_Land.pdf
[34] International Covenant on Civil and Political Rights("ICCPR"). New York 16.12.1966, e.i.f. 23.03.1976. Accessible at: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx
[35] Convention for the Protection of Human Rights and Fundamental Freedoms("ECHR"). Rome, 04.11.1950, e.i.f. 03.09.1953. Accessible at: https://www.echr.coe.int/documents/convention_eng.pdf
[36] CFREU, op.cit. Article7.
[37] Milanovic, M. Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age. - Harvard International Law Journal, Vol. 56, No.1, 2015, Page 83. Accessible at: https://harvardilj.org/wp-content/uploads/sites/15/561Milanovic.pdf

the other one is the enlargement of the notion of the right to privacy which started to comprise places other than home, correspondence etc. [38]

Since the right to privacy is one of the classical human rights and one of the oldest ones, it has been always established in classical human rights instrument. Some of them have lost effectiveness; others still are affecting largely the area of human rights. Additionally, because of the fact that the right to privacy is one of the most controversial human rights due to constant conflict with other fundamental human rights especially with the freedom of expression[39], it has been always one of the popular topics in human rights law sphere.

When it comes to the protection of human rights at the international level, the first document should be mentioned is the Universal Declaration of Human Rights("UDHR").[40] Indeed, the UDHR has been "the first, and possibly the singularly most important step taken by the United Nations"[41] on the purpose of the protection of human rights.

Regarding the right to privacy, the UDHR art.12 declares 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." As it is seen from the provision, while the first sentence shows the classical negative side of the right, the second sentence gives states an obligation for the protection of the right.[42] Thus, it can be said that this article compasses both negative and positive obligations for protection.

Even if the article 12 of the UDHR has been one of the most important, powerful and guiding provisions regarding the right to privacy, it should be said that it is not legally binding. However, as it is known, the same provision has been accepted by the member states of the United Nations in the ICCPR art. 17 in this way it has been a legally binding regulation as well.

---

[38] Bronstein, A. International and Comparative Labour Law. op.cit., Page 181.
[39] Smith, R.K.M. Textbook on International Human Rights. Oxford University Press, 7th edition, 2016, Page 182.
[40] Universal Declaration of Human Rights ("UDHR"). Paris, 10.12.1948.
Accessible at: https://www.un.org/en/universal-declaration-human-rights/
[41] Smith, R.K.M. op.cit., Page 38.
[42] Zlemele, I. Privacy, Right to, International Protection. Max Planck Encyclopedia of Public International Law. Oxford Public International Law, 2009.
Accessible at: https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e863

Besides these classical norms regarding the right to privacy, since 2018 United Nations declared the importance of the protection of the right to privacy in the digital age and started to work on this issue particularly. The General Assembly and the Human Rights Council have made nine resolutions to guide states, companies and individuals with regards to the danger of the violation of the right to privacy by using the new technologies because new technologies are getting more and more complex and improved hence can and are used to infringe the right to privacy through multiple ways.

The United Nations and most specifically Human Rights Office of the High Commissioner has been working on this issue. The importance and danger have been underlined by Michelle Bachelet, the UN High Commissioner for Human Rights, as "At its best, the digital revolution will empower, connect, inform and save lives. At its worst, it will disempower, disconnect, misinform and cost lives."[43]

It is the fact that these resolutions are not legally binding, however, as international guidance for the right to privacy in recent times and with recent dangers, resolutions have already affected the issue and in the future, they will affect much more. Also, they may open the way to establish legally binding international instruments in forthcoming times. More importantly, they show the will of the member states. Because it is inevitable that there will be a need for further assessment on the international level.

These resolutions generally underline the importance and danger of this issue and compass several aspects such as online and offline rights, effective remedy, transparency, the importance of the term consent with regards to data protection, cyber-bullying and cyber-stalking, crimes against vulnerable groups and monitoring of the right within the member states through the reporting system.[44]

Additionally and may be one of the most important aspects in terms of mass surveillance and data collecting that even if it is being done abroad may be considered within the scope of the human rights protection.[45] In the ninth resolution made by the General Assembly dated

[43] Michelle Bachelet, Human rights in the digital age - Can they make a difference?. Japan Society, New York, 17 October 2019. Key Speech.
[44] Resolutions No. 75/176, 42/15, 73/179, 37/2, 34/7, 71/199, 28/16, 69/166 and 68/167 of the General Assembly and Human Rights Council.
Accessible at: https://www.ohchr.org/EN/Issues/DigitalAge/Pages/InternationalStandardsDigitalPrivacy.aspx
[45] Milanovic, M. op.cit., Page 85.

16.12.2020[46], it has been accepted that this issue will be on the table for the next sessions as well. Hence, it can be said that despite the numerous resolutions, the United Nations is still taking this problem into consideration as the uttermost importance.

Apart from the sources of the UN, there are also some documents that should be mentioned with regards to the right to privacy and data protection. Even if they are not legally binding, they are still important sources that are guiding governments, companies and individuals.

As it is known, ILO is the most related special agency of the United Nations in terms of the protection of the employees' rights and one of the most known international organizations because of the unique structure. It includes not just states but also employees and employers to its works thus harmonize these three parts. The ILO has some standards which are "basic principles and rights at work."[47] The fundamental purpose of the ILO is to implement those standards and monitoring them.[48]

ILO has multiple complaint procedures in order to protect the standards that are established by a couple of conventions.[49] These conventions are legally binding, however, it also should be said that the ILO has not a good so-called reputation regarding the forcing the member states to go in accordance with its standards. This is mainly because some kind of judiciary system could not be established such as the ECtHR or the CFEU. Hence, it can be said that the ILO is sometimes considered a "toothless tiger".[50]

Nevertheless, the ILO is still the most effective international organization when it comes to the protection of employees' rights and Turkey which is the country that this paper will work on is a member of the ILO. Additionally, improvement and promotion of its "standards is of

[46] Resolution 75/176. op.cit.
[47] International Labour Organization. Rules of the Game An introduction to the standards-related work of the International Labour Organization. Centennary Edition 2019, Geneva. Page 18 Accessible at: https://www.ilo.org/global/standards/information-resources-and-publications/publications/WCMS_672549/lang--en/index.htm
[48] Haworth, N. Hughes, S., Wilkinson, R. The international labour standards regime: a case study in global regulation. - Environment and Planning A 2005, volume 37, 2005, Page 1942. Accessible at: https://www.academia.edu/31688189/The_international_labour_standards_regime_a_case_study_in_global_regulation
[49] OECD. Trade, Employment and Labour Standards A Study of Core Workers' Rights and International Trade. 1996. Page 154-156. Accessible at: https://www.oecd-ilibrary.org/docserver/9789264104884-en.pdf?expires=1586420650&id=id&accname=guest&checksum=31FB6003C9AE6D2CF3885AF299F00C13
[50] Lyutov, N. The ILO System of International Labour Standards and Monitoring Procedures: Too Complicated to be Effective?. - Zbornik PFZ, 64, (2), 2014, Page 256. Accessible at: https://www.researchgate.net/publication/297699071_The_ilo_system_of_international_labour_standards_and_monitoring_procedures_Too_complicated_to_be_effective

fundamental importance to the ILO."[51] Thus, the ILO standards and other documents which are not legally binding should be examined regarding the protection of employees' personal data.

The ILO standards are mainly focusing on some categories which are the freedom of association, right to collective bargaining, abolition of forced labour, rights regarding wage, child labour and discrimination. These topics are being held by the fundamental conventions. Other than these subjects, there are some other issues that ILO has conventions and recommendations.

Unfortunately, the ILO has no specific convention regarding the protection of the employees' personal data. Instead, there is a non-binding document called the ILO Code of Practice of the Protection of Workers' Personal Data. It is a relatively old document published in 1997.

If the improvement of technology is considered, it can be said that the Code of Practice is highly inefficient anymore. However, it is still one of the most important guiding documents. It includes significant subjects from the collection, security and storage of personal data of employees' to individual rights to collective rights. Despite its small volume, the content that it possesses is remarkable and highlights most of the principles in that area thus will be referred to frequently.

As per other non-binding documents, the Guidelines for the regulation of computerized personal data files[52] of the United Nations and the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[53] of the OECD can be listed with underlining the fact that they do not include specific provisions regarding employee rights but mostly set forth principles of data protection.

All in all, it should be said that, despite the nature of this issue and the necessity of the fact that it should be dealt with internationally, there are no binding international instruments yet.

[51] International Labour Conference. ILO Centenary Declaration for the Future of Work adopted by the Conference at Its One Hundred And Eighth Session, Geneva. Page 6. Accessible at: https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---relconf/documents/meetingdocument/wcms_711674.pdf

[52] Guidelines for the Regulation of Computerized Personal Data Files. The General Assembly, 14.12.1990 Accessible at:https://www.refworld.org/pdfid/3ddcafaac.pdf

[53] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD, 23.12.1980. Accessible at: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Because it is also a reality that is hard to establish a binding international instrument especially for controversial subjects such as data protection. Furthermore, it is affecting states, companies and individuals to a large extent in terms of politics, democracy, human rights to finance, development and many more aspects.

It seems that for now, the subject is mostly being handled by national legislations due to the fact that "employment law is still strongly localised, even though a growing number of people work online and travel across borders in their employment."[54] However, the conditions regarding this issue are changing and in a sense are forcing the international community to establish international instruments.

Notwithstanding the lack of legally binding international instrument, some of the regional regulations and implementations have a particular impact. Additionally, they are more tend to be legally binding instruments compared to international ones hence needs to be looked at carefully.

1.2. Evaluation of the Regional Protection of Employees' Personal Data

The main actors that should be mentioned regarding data protection on a regional level are the European Union ("EU") and the Council of Europe. Because the EU has established one of the most important and guiding regulations with regards to data protection called the GDPR and the Council of Europe has constituted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data("Convention no.108")[55] and Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows ("Additional Protocol no.181").[56]

These three instruments have importance on a general level however it should be also said that they are important for the case of Turkey maybe even more. This is mainly because

[54] Blackmer, W.S.(2019). Data Protection in the Private Sector: convergence or localisation of rights and expectations?. Human Rights, Digital Society and the Law A Research Companion (Ed.Mart Susi). Routledge. Page 295.

[55] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention no.108"). Strasbourg, 28.01.1981, e.i.f. 01.10.1985. Accessible at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

[56] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows.("Additional Protocol no. 181"). Strasbourg, 08.11.1981. Accessible at: https://rm.coe.int/1680080626

Turkey is a member of the Council of Europe and bound with these instruments legally. Even if it is not a member of the EU, Turkey when established its own regulation regarding data protection imitated the regulations of the EU because of the fact that it is still trying to get a membership. Additionally, it is true that the GDPR is the most logical regulation to be imitated because it is novel and trying to overcome the deficiencies in this area.

The Convention no.108 and the Additional Protocol no. 181 both are instruments regarding automatic processing. The Convention no. 108 has established and opened for signature in 1981. It was a significant step because it was the first legally binding instrument with regards to data protection. Following that, the Additional Protocol no.181 has established in 2001. The Convention no. 108 is one of the main reasons that also as a member state, Turkey has its own regulations with regards to data protection because it makes the member states have their own legal documents to regulate this area with terms that outlined in the Convention no. 108.

The Additional Protocol is also particularly important because it makes the member states have their own supervisory authorities which are entitled to have a right to investigate, intervene, engage in legal proceedings etc. They also should be independent. The Protocol was the main reason that now Turkey has a supervisory authority called Personal Data Protection Authority which has powers set forth in the Additional Protocol no. 181 and it has been playing a significant role to establish a data protection system in Turkey.

Because of the fact that the Convention no. 108 is a relatively outdated instrument, it has been modernised by protocol in 2018[57]. This is mainly because the area that the Convention is regulating is such an area that is changing constantly through technological improvements. The Modernised Convention has particular changes with regards to the protection of human rights.[58]

Should the modernized convention is examined; the first thing that would be seen is the importance of the right to privacy. In art. 1 which is regulating the object and purpose of this convention underlines the higher value of the right to privacy than other human rights.[59]

[57] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data. Elsinore, 18.05.2018. Accessible at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf
[58] The whole comparison can be seen at https://rm.coe.int/cahdata-convention-108-table-e-april2018/16808ac958
[59] Convention no. 108, op.cit., Article 1.

Hence, it can be understood that the convention particularly seeks to protect the right to privacy.

The Convention no. 108 highlights the importance of the legitimacy and transparency while processing data.[60] When data quality is concerned, Convention gives responsibility to member states to make necessary legislation, monitor the data processing activities and take any measurements to implement the principles set forth by the Convention. These principles are of particular importance and lay down by other instruments such as the GDPR as well and also have great value in the employment context because the data belongs to employees is processed by employers mainly to keep on the right side of the law.

Legislations often give employers responsibilities for many reasons to process data of their employees which are the main grounds of legitimacy. Hence, if employers process data of their employees without any legal or logical grounds or if the proportionality exceeds, it means that it is unlawful as per the Convention and needs to be dealt with by member states.

The Convention also juxtaposed the special categories of data that need to be handled carefully because of their nature. They are some categories that can be considered sensitive because when it comes to data from these groups, the right to privacy may be in particular danger.

The issue to define which types of data should be considered as sensitive "has long been a contentious issue"[61] but according to the Convention no. 108 art. 6. they are genetic data, personal data regarding criminal procedures, biometric data and data which is revealing the relation of racial origin, political opinion, trade union membership, sexual life etc.[62]

These kinds of data should only be processed in accordance with the law with some measurements have to be taken in advance. It can be said that for employment context, data processed by employers are often can be considered as special or sensitive data which have more protection such as criminal records, the birthplace, biometric data such as photo, video, fingerprint etc and trade-union membership.

[60] Convention no. 108, op.cit., Article 5.
[61] Lloyd, I.J. Information Technology Law. op.cit., Page 58.
[62] Convention no. 108, op.cit., Article 6.

Thus, as per the Convention, it can be said that the protection of personal data of employees is of much more importance compared to a regular data protection system. This work asserts that whether data in question falls within the scope of special categories or sensitive data definitions or not, it should be considered as sensitive data and should be protected by national legislations more carefully.

The Convention has art. 8 and art. 9 which includes the rights of the data subject.[63] They do not have to be detailed however it should be said that these rights are in accordance with the ones set forth by the GDPR and Turkish legislation such as the right to erasure, right to have a remedy, right to consent and others. The deficiencies of the Turkish legislation compared to the Convention no.108 and the GDPR will be taken into consideration in the following chapters.

The Convention no. 108 and the Additional Protocol no. 181 have been maybe the most important instruments which are legally binding for member states including Turkey. As mentioned above, the main reasons for having comprehensive legislation with regards to data protection and supervisory body which has significant impact are these instruments. Turkey has signed the convention in 1981 however it was the year 2016 that is ratified and entered into force right after the establishment of the national legislation.

It should be also mentioned that Turkey has two declarations regarding the ratification of the Convention. One is that it declared its ratification does not mean the acceptance of the Republic of Cyprus as a party of the Convention. Another one is that Turkey does not apply the Convention to some specific groups of data processing which are " a) The automatic processing of personal data realized by natural persons exclusively for their personal use or household purposes, b) Public registers specifically regulated by Law in Turkey, c) Data which are available to the general public information in accordance with Law, d) Personal data which are processed by public institutions for the purposes of national security, defence and to the investigation and prevention of criminal offences."[64]

[63] Convention no. 108, op.cit, Article 8-9.
[64] Declarations can be accessed at:
https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/declarations?p_auth=eEdZ5vdJ&_coeconventions_WAR_coeconventionsportlet_enVigueur=false&_coeconventions_WAR_coeconventionsportlet_codeNature=10&_coeconventions_WAR_coeconventionsportlet_searchBy=state&_coeconventions_WAR_coeconventionsportlet_codePays=TUR

The second declaration mentioned above can be harmful when trying to protect human rights in terms of data processing. Because it mainly allows state bodies to not go in accordance with the Convention and it should be underlined the fact that the number of people which are working as an employee of the state is significant. Thus, state bodies are also considered as employers hence they also should be under the supervision of the Convention as employers and they only should process data of their employees without the supervision of the Convention if it falls within the scope of the purpose of national security, defence and criminal procedures.

All in all, the Convention no. 108, Additional Protocol no. 181, national legislation came into force and the supervisory body has been established in 2016, hence it can be said that Turkey is comparatively new in building the data protection system and so it has deficiencies by means of legislation and implementation will be mentioned in following chapters.

Before getting into the GDPR, some recommendations of the CoE should be also mentioned. Because, although they do not have binding power, they have value concerning data protection in terms of the employment context. There are recommendations regarding data protection and the right to privacy in general such as Recommendation concerning data used for insurance purposes or profiling, the right to privacy on the internet, protection of medical data and so on and so forth.[65]

However, the related one is the Recommendation on "protection of personal data used for employment purposes" ("Recommendation No. R (89)2") which is highly important despite the fact that it is outmoded.[66] It is later revised with the new recommendation called Recommendation No. R (2015)5. According to the latter recommendation, the reason for revision is "in order to continue to provide an adequate level of protection for individuals in the context of employment".[67]

In this formerly mentioned recommendation, the importance of the Convention no. 108 has been underlined, the fact that automatic data processing used by employers has been used much more often thus should be careful to avoid any infringement in terms of protection of employees' data. It also mentioned that it is crucial to understand the different relationship

[65] Recommendations Accessible at: https://www.coe.int/en/web/cdcj/recommendations-resolutions-guidelines
[66] Recommendation No. R (89) 2. op.cit.
[67] Recommendation No. R (2015)5. CoE. 01.04.2015. Accessible at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a

between employees and employers because of its also the nature of collectivity and underlined the fact that member states may have different traditions as per employee-employer relations. It emphasized the rights that employees' have in general terms and stress the importance of the right to privacy of employees in the workplace. Notwithstanding the fact that it is an outdated recommendation and legally binding instruments have been accepted after it, it is still in employment context one of the leading documents.

However, it should be also said that this recommendation is established in "a time when the Internet was only at its beginning."[68] Hence new recommendation is needed to be given. R (2015) 5 is a much more comprehensive and detailed document compared to its predecessor. It includes some aspects that have never been touched before.

For example as per the latter recommendation, "The processing must comply with certain principles and restrictions, such as the principle of transparency and consulting employees' representatives before placing monitoring systems in the workplace. The recommendation also states that employers should apply preventative measures, such as filters, instead of monitoring employees' internet usage."[69]

Even if it is not a legally binding document, it may and should be an inspiration for future legally binding national and/or international legislations. Because, as it was needed to have a new recommendation in this area in the employment context, it is now needed to have legally binding regulations. As it will be examined below, Turkish regulations are not efficient for data protection in general let alone provide enough protection in the employment context.

The GDPR should be also mentioned before getting into national legislation of Turkey with regards to data protection. Because, even if it is not legally binding for Turkey, the GDPR has been and still is affecting countries and their national legislations all around the world. It can be seen that the GDPR "is another example of the EU trying to create international standards and taking a somewhat aggressive approach in ensuring this through the expansion of the

[68] https://www.coe.int/en/web/human-rights-rule-of-law/2015-news/-/asset_publisher/8X0wvBBc60he/content/council-of-europe-committee-of-ministers-has-adopted-a-recommendation-on-the-processing-of-personal-data-in-the-context-of-employment
[69] CoE. Handbook on European data protection law 2018 edition. 2018, Page 331-332.

territorial scope of the GDPR beyond Europe's borders". [70] That is to say, the GDPR is not just a regulation for the EU but its effect is sprawling throughout the world.

Additionally, Turkey is still trying to get a membership of the EU thus is trying to make its legislations in accordance with the regulations set forth by the EU. Also, "since the territorial scope of the GDPR applies where the personal data processing activities are related to the offering of goods or services to data subjects that are in the Union by a controller or processor not established in the Union, data controllers located in Turkey might be required to comply with the GDPR".[71]

That is to say, the GDPR is "massive (99 articles over 88 pages and 55,000 words), complex, omnibus data protection law that provides a comprehensive legal framework for the protection of Europeans' personal data" [72] and because of the aforementioned reasons is affecting Turkey eloquently.

The GDPR is touching almost all of aspects of data protection such as consent, rights of the data subject, duties and responsibilities of the controller and processor, establishment of the independent supervisory authorities and so on and so forth. Before the GDPR there are directives especially 95/46/EC[73] mainly regulating this area for the fact that it is a "rights-based field of EU policy"[74].

Even if it is said that within the EU legal instruments "there is no formal hierarchy" [75], regulations are such instruments that are directly applicable while directives are mostly considered as guiding documents for member states. That is to say that, regulations are general instrument and directly applicable such as national legislation, directives on the other hand can aim at specific members and guide them to make their own legislation, in plain words directives give the ground rules and aims while let member states to choose their own methods. The Directive thus can be defined as not directly applicable like regulations.

---

[70] Pajuste, T. The Protection of personal data in a digital society. The role of the GDPR. Human Rights, Digital Society and the Law A Research Companion (Ed.Mart Susi), Routledge, 2019, Page.314.
[71] Kınıkoğlu, B., Zengin, S., Akdere, K.C. Turkey. The Privacy, Data Protection and Cybersecurity Law Review.(Ed.A.C.Raul). 6th Edition.The Law Reviews, 2019, Page 360.
[72] Dove, E.S. EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. The Journal of Law Medicine & Ethics, 46, 2018). Page 1013.
[73] Directive 95/46/EC. EU. 24.10.1995. e.i.f. 23.11.1995. Accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046
[74] Craig, P. Burca, G.D.(2011). EU Law Text, Cases, and Materials. Fifth Edition. Oxford University Press. Page 392.
[75] Ibid. Page 104.

On the basis of this information, the data protection area became much more important with the establishment of the GDPR. Firstly, it is directly applicable and binding for all member states and also it started to unify the implementation within member states. Additionally, non-member states including Turkey have been affecting by the GDPR to a large extent. It is considered to be the main legal document when it comes to data protection and it touches almost all of the aspects mentioned above. Additionally, it also shows parallelism with the Convention no.108.

As per data protection in the employment context, it has some specific provisions and recitals. The most important one is art. 88/1 and it states that "Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context..."[76]

It is clear from the provision that the GDPR underlines the specific importance of the protection of personal data of employees because of the contradictory nature of the relationship between employee and employer. However, instead of making such specific provisions, it guides to member states to take this subject into consideration with their national legislations.[77] Before the GDPR, directives have been criticized by trade unions given the fact that they do not include specific provisions regarding the protection of employees' personal data.[78] However, it seems that the issue in terms of these critics has not been changed to a large extent.

Art. 88/2 declares that "Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place."[79] It shows us some particular points in this regard such as transfers of employees' data, surveillance at workplace and transparency.

[76] GDPR, op.cit., Article 88/1.
[77] Ogriseg, C. GDPR and Personal Data Protection in the Employment Context. - LLI, Vol. 3, No. 2, 2017, Page 4.
[78] Rustad, M., Paulsson, S.R. Monitoring Employee E-Mail And Internet Usage: Avoiding The Omniscient Electronic Sweatshops: Insights From Europe. - University of Pennsylvania Journal of Labor and Employment Law, 2005, Page 70.
[79] GDPR, op.cit., Article 88/2.

It also highlights the importance of the fundamental rights of employees hence can be said that this provision has a high value for this topic. However, at the same time, it is seen that the subjects referred to in this provision are highly vague. The only thing this provision is doing is underline the importance but not giving some specific protection. It is understandable that the GDPR is a regional regulation and hard to has specific provisions rather than establishing the ground rules of the subject. However, as it will be examined in the next chapter, national legislations should have specific regulations for data protection in employment context as it is said in this article.

Concerning this topic, art. 9 of the GDPR is also one of the important provisions that should be highlighted. As in the Convention no.108, GDPR also determines some special categories of personal data for more protection. It asserts that "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."[80]

However in the following provision it makes an exception when "processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject".[81]

This is mainly because of the fact that employers have a right or obligation stem from some reasons such as health at work, right to property, duty to protect the rights of other or other rights and obligations set forth by national legislation to collect and process data of employees and data mostly falls within the scope of the definition given by the GDPR art. 9 as above. Hence, the exception is legitimate but only to some extent that the rights of the data subject which in this case employee are being protected by national legislation. Hence, it can be said that processing this kind of special data of employees are allowed to some extent according to the GDPR.

[80] GDPR, op.cit., Article 9.
[81] GDPR, op.cit., Article 9.

In consequence, the GDPR has underlined the importance of the protection of employees' personal data and guided the member states or employers and trade unions to determine the conditions of this particular issue.

Apart from these powerful instruments mentioned above, CFREU should be also referred to when it comes to data protection even if the fact that Turkey is not a member of the EU thus is not legally bound by CFREU. This is important to say that CFREU is the first human rights instruments that regulate data protection as an independent human right from the right to privacy.

According to CFREU art. 8 "Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority."[82]

This article is of high importance because of the fact that it does not just include the provision that is giving subjects to this particular right, it also gives the ground rules of this right such as consent, specification, right of access, right to rectification, independent authority and so on. Hence, it can be said that this article in human rights instruments comprises most of the aspects given in the GDPR and the Convention no. 108. It is also important from the fact that it provides the make the CJEU case law stronger.

Besides CFREU, the EU has other important provision with regards to data protection which enshrines data protection rights of individuals within the member states of the EU. This provision appears in the Treaty on the Functioning of the European Union ("TFEU") as article 16(1) and 16(2) which state "Everyone has the right to the protection of personal data concerning them. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within

[82] CFREU, op.cit., Article 8.

the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities."[83]

Because of these regulations laid down in TFEU which is one of the main treaties and has the same legal power with CFREU thus together they "set the constitutional framework for the life of the EU"[84], it is clear that data protection as per the EU has been one of the most valuable areas to work on.

Consequently, it can be said that regional instruments are much more detailed, binding and essential documents compared to international regulations naturally. However, as it is seen especially from the GDPR that the major role for data protection in general and in the employment context is national legislations.

Before getting into national legislations of Turkey regarding this issue, it is valuable to remind that Turkey is legally bound by the instruments of the UN, the CoE and has to take into consideration not legally binding documents thereof. Additionally, even if it is not a member of the EU, Turkey has been highly affected by the policy and regulations of the EU and in terms of the data protection the EU is the first place that Turkey is looking for thus the EU regulations especially GDPR is one of the most important instrument when making comparison with Turkish legislation in order to analyze the possible deficiencies or differences that should be evaluated.

[83] Treaty on the Functioning of the European Union ("TFEU"). 26.10.2012.
Accesible at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012E/TXT&from=EN
[84] Borchardt, K. The ABC of EU Law. European Union, 2017, Page 90.

2. ASSESSMENT OF REGULATIONS IN TURKEY

2.1. Necessity of Legal Act for Employees' Data Protection

In order to determine whether there is a need for an independent legal act for the protection of employees' personal data formally and substantially, the first thing that should be done is to evaluate the present regulations in Turkish law in this context.

Turkey is the 13th member state of the Council of Europe in 1950[85], ECHR had been accepted into Turkish Law in 1954 and individuals have been given the right to petition to ECtHR in 1987 which can be defined as the year that is especially important for human rights developments in Turkey.[86] Hence, both the Convention and the decisions of the Court has been legally binding for Turkey approximately for more than thirty years.

Afterwards, more recently Turkey incorporated both the Convention no.108 and the Additional Protocol no. 181 into its law in 2016 at the almost same time as the establishment of the Law no. 6698 which is the main legislation concerning data protection. Thus, apart from its own legislation, Turkey is legally bound by the international instruments mentioned above and decisions of the ECtHR as they are like its own national legislation.

Additionally, because Turkey has been one of the members of ILO, regardless of the fact that it does not have a legally binding instrument, Turkey still has to take ILO's instruments and recommendations and other means of regulations into account advertently.

For the sake of the hierarchy of norms, the first regulation that should be mentioned is the Constitution of Turkey[87] which inspired by both the UDHR and the ICCPR as most of the other constitutions[88]. The Constitution gives specific importance to the right to privacy because of the fact that contrary to others, for the right to privacy there are three articles that are established. The first one art. 20 says that "Everyone has the right to demand respect for

[85] https://www.coe.int/en/web/portal/turkey
[86] Buckley, C. The European Convention on Human Rights and the Right to Life in Turkey. - Human Rights Law Review. Vol 1, No 1, 2001, Page 35.
[87] Constitution of the Republic of Turkey. 18.10.1982, e.i.f. 9.11.1982. English version accessible at: https://www.anayasa.gov.tr/en/legislation/turkish-constiution/
[88] Elkins, Z., Ginsburg, T., Simmons, B. Getting to Rights: Treaty Ratification, Constitutional Convergence, and Human Rights Practice. - Harvard International Law Journal . Vol. 54 No. 1, 2013, Page 63 Accessible at: https://harvardilj.org/wp-content/uploads/sites/15/2013/06/HLI102.pdf

his/her private and family life. Privacy of private or family life shall not be violated."[89] This article is almost the same version of the one in the other international instruments.

The interesting and more progressive thing is that with the amending of the Constitution in 2010, one paragraph has been added to this article which declares that "Everyone has the right to request the protection of his/her personal data. This right includes being 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. 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."[90]

This provision is highly important for Turkish Law because of the fact that it shows that even if it is established within the provision of the right to privacy it needs much more attendance independently. This provision includes multiple cornerstones of data protection areas such as explicit rights like the right to be informed, access etc., the principle of lawfulness and the concept of explicit consent. Hence, it should be said that even it is on the principal level, this provision affects the legislation and the decision of courts and administrative bodies. Also, it should be mentioned that this provision is almost similar to one in the CFREU.

The other two articles are about the inviolability of the domicile and the freedom of communication which are also related to the employees' personal data because of the fact that one of the most common ways to breach the employees' rights regarding personal data is monitoring their communications via multiple tools. The most given example is the monitoring of the emails of employees. Hence, even though they are established as principles, these articles are also of high importance. Art. 21 declares that "The domicile of an individual shall not be violated."[91] and art. 22 says that "Everyone has the freedom of communication. Privacy of communication is fundamental."[92]

Apart from these articles, it should be also mentioned that employees right to organize unions and rights of collective labour agreement as per art. 51 and 53 which are related with also this

[89] Constitution of the Republic of Turkey, op.cit, Article 20
[90] Ibid, Article 20
[91] Ibid, Article 21
[92] Ibid, Article 22

topic because collective labour agreement is one of the most important tools for employees to entitle such rights including data protection rights.[93]

For example, in the GDPR as mentioned before declares in art. 88 that "Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context..."[94] and it also with art. 9 define the union membership information as sensitive data.[95] Thus, in the employment context, the right to organize unions and the right of collective labour agreements are playing crucial roles in terms of data protection.

Additionally and lastly, the Constitution gives duty to state in respect of the protection of employees by saying in the art. 49 that "The State shall take the necessary measures to raise the standard of living of workers, and to protect workers and the unemployed in order to improve the general conditions of labour, to promote labour, to create suitable economic conditions for prevention of unemployment and to secure labour peace."[96]

The second important legislation regarding the right to privacy and data protection is the "Regulation of Publications on The Internet and Combating Crimes committed by means of Such Publication"("Law no.5651")[97] which has been famed for its misuse for restriction of social media and censorship. It has been used to restrict to reach the famous websites such as Youtube, Wikipedia and others.[98] It is commonly criticized by having provisions regulating that administration is able to take access blocking decisions without any decision of the court.[99]

[93] Constitution of the Republic of Turkey, op.cit., Article 51-53.
[94] GDPR, op.cit., 88.
[9595] GDPR, op.cit., 9
[96] Constitution of the Republic of Turkey, op.cit., Article 49.
[97] Regulation of Publications on The Internet and Combating Crimes committed by means of Such Publication"("Law no.5651"). 04.05.2007, e.i.f. 23.05.2007. Accessible at: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf
[98] Akdeniz, Y. Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship, 2010, Page 3.
Accessible at: https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/pdf/speak_up/osce_freedom_of_the_media_on_turkey_and_internet_censorship.pdf
[99] Clayton ,R., Kjerulf-Thorgeırsdottır, H., Dıjk, P. Benedek, W., Turk, K. (European commission for Democracy Through Law(Venice Commission)).(2016). Opinion on Law No. 5651 on Regulation of Publicatıons On the Internet and Combating Crimes commıtted by means of such Publicatıon("The Internet Law"). Page 16. Accessible at: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)011-e

One of the most controversial articles of the Law no. 5651 and also related with the right to privacy is the article 9/A. The topic of this article can be translated as "blocking the access to content because of the right to privacy".[100] It is principally established to restrict to access some web sites which can include the breach of the right to privacy.

This procedure is under normal conditions initiated by an individual who claims that infringement regarding his/her right to privacy has occurred via a specific website. However, it also can be started by the decision of administration in some circumstances. Administration can restrict access to these websites without the decisions of court. Subsequently, it must be evaluated within 24 hours by court whether the right to privacy is infringed or not.

As mentioned before, the conflict between the right to privacy and other fundamental rights especially freedom of expression is of dangerous level when it comes to this legislation. Via the power that is given to administration and state, it has been misused to restrict the other fundamental rights especially the freedom of expression.[101] At first sight, it may be seen as the protective legal act for the right to privacy; however, it has been probably mostly used for political reasons than to protect the right to privacy of individuals.

Additionally, these restriction decisions can be made without a time limit or any other limits. For example, in 2017 the famous website Wikipedia has been restricted and could not be reached until 2020 with the decision made on the basis of the Law no. 5651. It has been started to be reached with the decision of the Turkish Constitutional Court saying that this blockage is causing the breach of the freedom of expression. [102]

Regarding the right to privacy and data protection, there are also criminal law provisions in the Turkish Penal Code ("Law no. 5237") between art. 134 and 140. [103] According to art. 134 "Any person who violates the privacy of another person's personal life shall be sentenced to a penalty of imprisonment for a term of one month to three years. Where the violation of privacy occurs as a result of recording images or sound, the penalty to be imposed shall be increased by one fold. Any person who unlawfully discloses the images or sounds of

[100] Law no.5651, op.cit., Article 9/A.
[101] Akgül, M., Kırlıdoğ, M. Internet Censorship in Turkey. - Internet Policy Review Journal on Internet Regulation. Vol 4, Issue 2, 2015, Page 10. Accessible at: https://policyreview.info/articles/analysis/internet-censorship-turkey
[102] The Decision of the Turkish Constitutional Court(Wikimedia Foundation Inc. and Others no. 2017/22355). Accessible at: https://kararlarbilgibankasi.anayasa.gov.tr/BB/2017/22355
[103] Turkish Penal Code ("Law no. 5237"). 26.09.2004. e.i.f. 12.10.2004. Accessible at:
Accessible at: https://www.legislationline.org/download/id/6453/file/Turkey_CC_2004_am2016_en.pdf

another person's private life shall be sentenced to a penalty of imprisonment for a term of two to five years. Where the offence is committed through the press or broadcasting, the penalty shall be the same."[104]

It is seen from the article that legislator divided the situations whether infringement occurs with lawful means or unlawful means. Also, it can be said that depending on the way of infringement, the penalty may be increased.

Data protection apart from the right to privacy in the area of criminal law is regulated by art. 135, 136 and 137.[105] As per these provisions, illegally recording, obtaining or giving data are prohibited and if data is sensitive including trade union relation penalty shall be increased. Besides these protection provisions, as per art. 138, if data that should be destroyed legally is failed to be destroyed, responsible individuals shall be imprisoned for one to two years.

Lastly, according to art. 139, these crimes excluding illegally record, obtain or give data or failure to destroy data are subject to complaint. That is to say that the breach of the right to privacy is subject to complaint and without complaint by victim authorities shall not take action. It is seen from this provision is that the protective provisions regarding data protection are not subject to complaint thus as per the Turkish Penal Code they are of high importance and should be investigated by the authorities ex officio. This shows the significance and value of the protection of individuals' data. [106]

Apart from these provisions, there are also some articles related to the confidentiality of communication. Because of the fact that it may be one of the most seen issues regarding the right to privacy between employees and employers which are called the monitoring correspondence of employees, these provisions should be also underlined. According to those provisions, if a violation of confidentiality of communication occurs by means of listening, recording, disclosing, eavesdropping etc. it should be penalized on the basis of art. 132 and art.133.

The first law regarding employees in terms of data protection is Turkish Labour Law ("Law no. 4857"). Despite the fact that this legal code is the main code with regards to employee and

[104] Law no. 5237, op.cit., Article 134.
[105] Law no. 5237, op.cit., Article 135-137.
[106] Law no. 5237, op.cit., Article 139.

employer relations, there are no detailed provisions for data protection. There is only one article that is highly inefficient and behind the times. Law no. 4857 art. 75 states that "The employer shall arrange a personnel file for each employee working in his establishment. In addition to the information about the employee's identity, the employer is obliged to keep all the documents and records which he has to arrange in accordance with this Act and other legislation and to show them to authorized persons and authorities when requested. The employer is under the obligation to use the information he has obtained about the employee in congruence with the principles of honesty and law and not to disclose the information for which the employee has a justifiable interest in keeping as a secret."[107]

This provision is mostly about the personal file of employees however it is important in terms of data protection because it gives to employers a duty to use the data of employees in accordance with the law and principle of honesty and not disclosing the information to the detriment of employees.

Apart from the Law no. 4857, there are more specific provisions in Turkish Code of Obligations ("Law. no. 6098") despite the fact that it is Lex Generalis compared to Law. no. 4857. This is because Law no. 6098 has been established later than Law no. 4857 hence it has much more specific regulations within the scope of labour law.

According to art. 417 of the Law no. 6098, an employer has a responsibility to protect employees' personality and as per art. 419 employers should use personal data of employees' proportionately with employees' inclination and performance. With these provisions, the legislator underlined the importance of the proportionality principle of data protection law in the employment context.[108]

Turkish Social Security Law ("Law no. 5510") should be also mentioned because it has specific provisions of data protection in the employment context.[109] According to Law no. 5510 art. 78/2 "... Confidentiality of health information of the universal health insurance

[107] Turkish Labour Law ("Law no. 4857"). 22.05.2003. e.i.f. 10.06.2003. Accessible at: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.4857.pdf
[108] Turkish Code of Obligations ("Law. no. 6098"). 11.01.2011. e.i.f. 04.02.2011. Accessible at: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.6098-20120704.pdf
[109] Social Insurance and Universal Health Insurance Law ("Law no. 5510"). 31.05.2006, e.i.f. 16.06.2006. Accessible at: https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/74711/133294/F-379338786/TUR74711 Eng.pdf

holders and their dependants is fundamental...."[110] This provision inclines to protect health information which is the specific group of data or can be called sensitive data in terms of data protection law.

Additionally, in Social Security Institution Act ("Law. no. 5502"). art. 35 states that the personal data of universal health insurance holders and their dependents cannot be sold or shared.[111] With this way, legislator tried to protect the health information.[112]

Among Turkish regulations, there are provisions regarding data protection in general and some rare provisions in the employment context given above. However, it is clear to see that there is a need for an independent legal act to regulate data protection rules in the employment context. Because provisions related are dispersed and hard to explore.

Moreover, these regulations related with employment are outdated and they are not including novel difficulties arising from the new technologies. It must be underlined the fact that the most related provision given above is the provision regarding physical personal files.

Independent legal act regarding data protection in employment context should comprise criteria of video surveillance, monitoring correspondence and usage of internet/technological devises, monitoring of working time etc. These criteria can be taken from the case law of the ECtHR and turned into regulation. Moreover, in this legal act, it must be underlined that the consent as a reason of lawful data processing should be exceptional and when used it should be clear, precise and actual. For instance, it can be taken at certain intervals.

Additionally, details of the employees' rights in terms of data protection and the right to privacy in general should be determined and principles of how the balance should be struck between the rights of employees and employers must be constituted. Lastly, the positions and authorities of unions in terms of data protection law should be concretized. Because, in terms of the employee-employer relationship, unions are one of the crucial actors.

[110] Law no. 5510, op.cit, Article 78/2.
[111] Law. no. 5502, op.cit., Article 35.
[112] Dursun, Y. The Protection of Labour According To 6698 Numbered Protection of Personal Datas Law. Master's Thesis, Dokuz Eylül University, 2019, Page 14.

Overall, because of the reasons such as disorder of the relative provisions, outdatedness and incompatibility with the sui generis conditions of the employment context, there is a clear need for an independent legal act or at least a separate subpart in the Law no. 6698.

2.2. Incompatibility of the Law no. 6698 with the GDPR

The most important legislation in Turkey with regards to data protection besides the articles of the Constitution is the Law no. 6698. It is prepared in 2016 and came into force in 2018 such as the GDPR. However, when preparing this legal act, 95/46/EC was the instrument that was predicated on. It can be said that the Law no. 6698 "may be regarded as a translation of the"[113] 95/46/EC. At the same time, the GDPR came into force. That is to say that the present and main regulation with regards to data protection in Turkey is the one that is a translation of the former directive and it has some deficiencies. Because this is the fact that the reason to establish the GDPR was that the directive has some deficiencies.

It firstly laid down the principles in the Law no. 6698 should be in accordance with which are "lawfulness and fairness", "being accurate and kept up to date where necessary", " being processed for specified, explicit and legitimate purposes", "being relevant, limited and proportionate to the purposes for which they are processed", "being stored for the period laid down by relevant legislation or the period required for the purpose for which the personal data are processed".[114]

These principles are showing parallelism with ones regulating in the 95/46/EC and they also coincide with ones that set forth in the GDPR to a large extent. However, two of the most important changes that the GDPR has brought are the two main principles called transparency and accountability.[115] These principles unfortunately are not found in the Law no. 6698 because of the fact that they were also not in the 95/46/EC.

[113] Geden, A.M., Bengshir, T.K. Reflections from GDPR to Turkish Data Protection Act in the Context of Privacy Principles. - IMISC 2018 Conference Proceedings, 2018, Page 118. Accessible at: https://www.researchgate.net/publication/330307696_Reflections_from_GDPR_to_Turkish_Data_Protection_Act_in_the_Context_of_Privacy_Principles
[114] GDPR, op.cit.
[115] Ibid.Page. 118.

Especially for the prim implementation of data protection law, accountability is a crucial principle and several other principles are feeding on it[116]. Otherwise, other principles cannot be implemented in a healthy way. That is to say that the Law no. 6698 is even not in accordance with the GDPR in principles hence needs to be changed. This issue is not for the protection of employees' personal data but for the whole data protection law.

The other incompatibility is with regards to definitions and responsibilities of controller and processor that both the Law no. 6698 and the GDPR have provisions regarding data controllers and data processors. According to the Law no. 6698 art.3, the data processor is "the natural or legal person who processes personal data on behalf of the data controller upon its authorization" and the data controller is "the natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data filing system."[117] The GDPR has similar definitions. However, when it comes to responsibilities, there are huge differences arising from the fact that the Law no. 6698 is the equivalent of the former directive.

As per both the former directive and the Law no. 6698, data controller is the main responsible subject whereas the data processor has limited responsibility. One of the biggest changes that came with the GDPR is that it loaded responsibilities to data processors with regards to data security precautions, recording of processing activities, additional notification obligations, for public authorities to designate a data protection officer and some other responsibilities concerning transferring of personal data internationally. Also, it makes it compulsory for a comprehensive contract between controller and processor regarding details of processing.[118]

The Law no. 6698 has limited provisions regarding the controller and processor. The line between them is not always clearly seen in terms of determining who the processor is and who the controller is. Additionally, the responsibilities thereof are ambiguous.

The main responsible understood from the Law no. 6698 is the data controller which is not compatible with the provisions of the GDPR. Day by day, the complexity of the relationship between controller and processor is increasing hence there is a clear need for more detailed

[116] Kaya, M.B. The New Paradigm of Data Protection Law: The Principle of Accountability. - İstanbul Hukuk Mecmuası, 78 (4), 2021, Page 1865.
[117] Law no. 6698, op.cit., Article 3.
[118] Bakırel, N.B. Allocation of Responsibility Among Data Controller and Data Processor within the Scope of General Data Protection Regulation and Turkish Law on the Protection of Personal Data. Master's Thesis. Hacettepe University, 2020, Page73-80.

regulations in terms of determining the controller and processor and responsibilities thereof in Turkish data protection law. The ambiguity is explicit when looked at the guideline made by the Turkish Data Protection Board.[119] There are a couple of criteria that are also not specific in order to determine who is the controller and who is the processor.

In the employment context, data controllers are mostly employers whether is a natural person or legal person but also processors are in this relationship as companies that are giving accounting services, cloud services, security services or any other services to employers and processing the data of the employees. Thus, it is also highly important in employment context that the Law no. 6698 should be compatible with the GDPR in terms of definitions and responsibilities of controller and processor. This is crucial to determine who can be held accountable when there is any infringement of employees' personal data.

When it comes to data protection in the employment context, the art. 88 of the GDPR should be also mentioned and should be compared with the Law no. 6698. The art. 88 as mentioned above has a value of recommendation to member states. It is directing member states to establish some other provisions for data protection in employment context by legislation or collective labour agreements.

Also, it underlines that when establishing those regulations, they need to be a safeguard for fundamental rights and human dignity when it comes to transparency, transferring the data and surveillance at workplace. Even it is more of a guiding article; it has the utmost value for the protection of personal data of employees. In the Law no. 6698 however, there is not one simple provision with regards to the employment context. This kind of article should be embedded to the Law no. 6698 in order to guide both the state and employers in terms of data protection in the employment context.

One other incompatibility is regarded to the term of consent. In order to process data, it needs to be lawful. As per the GDPR and the Law no. 6698 there are a couple of conditions which make data processing as lawful. The first one is the consent. The concept of the consent which can be categorized as one of the cornerstone concepts in data protection law is regulated by the GDPR and the Law no. 6698 differently.

[119] Guide Accessible at: https://kvkk.gov.tr/SharedFolderServer/CMSFiles/f63e88cd-e060-4424-b4b5-f6413c602060.pdf

It can be seen when compared that the Law no. 6698 uses the term "explicit consent" where the GDPR uses the term "consent". At first sight, it may be presumed that the Law no. 6698 gives much more protection in terms of consent by looking at that it even specifies the consent should be explicit. However, when looking at the definitions of those terms, it is seen that the case is the opposite of what it would be presumed. The Law no. 6698 defines "explicit consent" as "freely given, specific and informed consent"[120] while the GDPR defines "consent" as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".[121]

It is clear to see that the consent of the GDPR has a much structured and detailed definition thus has wider protection than the explicit consent of the Law no. 6698. Even the Law no. 6698 fell behind the 95/46/EC let alone it would be compatible with the GDPR. The 95/46/EC defines consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."[122]

Apart from the significance of consent in general terms and incompatibility and deficiency of Turkish data protection law, it should be added that consent is also an explicitly important concept when it comes to employer-employee relations because of the fact that consent may not be considered as the main term to understand that two parties have an agreement due to the unbalanced nature of this relationship.

That is to say that, the real issue here is "the economic imbalance between the employer asking for consent and the employee giving consent will often raise doubts about whether or not consent was given freely."[123] All in all, when it comes to the employee-employer relationship, the privacy rights of employees are "particularly precarious because it is pitted against strong economic interests of employers."[124]

In labour law, consent may not have the same meaning because in constant occasions, consents of employees for multiple reasons have been taken but the real intents of employees are different. The only reason for employees to give their consents requested by employers is

[120] Law no. 6698, op.cit., Article 3.
[121] GDPR, op.cit, Article 4.
[122] Directive 95/46/EC, op.cit.
[123] CoE. Handbook on European data protection law. op.cit, Page332
[124] Witzleb, N. Employee Monitoring and Surveillance under Australian Law: The Need for Workplace Privacy Legislation. Perspectives on Privacy (Eds.Dieter Dörr, Russel L. Weaver), 2014, Page 126.

to continue to work. Hence, it can be said that for employee-employer relations, data protection law cannot be based on only the concept of consent. Law should protect the rights of employees even if consent has been given. Additional regulations for this situation should be established such as more detailed consent should be taken from employees for processing their data or even some of the types of data may be restricted despite the fact that employees give consent. The special nature of this relationship forces legislator to regulate this area in much more detail.

This situation is also laid down by EDPB[125] that due to imbalance of power between employees and employers, rather than depending on consent as a reason for lawful data processing, employers should prefer other reasons of lawfulness set forth in the art. 6 of the GDPR. As per the EDPB, relying on consent should be exceptional. The other reasons of legitimacy are also regulated in the Law no. 6698 such as performance of a contract, compliance with a legal obligation etc.

However, as will be given below chapters, consent can be accepted as Turkish Courts as a reason for lawful processing and the concept of consent in the Law no. 6698 has a weak definition, it is necessary to make changes even if the fact that it is generally accepted as exceptional by the EDPB. Especially in terms of video surveillance, monitoring correspondence and working time with new technologies including fingerprints or facial recognition systems, employers deem to just take a general consent of their employees and do have to feel obliged to search for other lawfulness reasons.

Overall, even if in employment context it is accepted as exceptional way, due to the fact that it is still being used largely by employers in Turkey and for the sake of data protection in general, the concept of consent should be changed and established in a more detail way such in the GDPR.

There are a lot of other incompatibilities between the GDPR and the Law no. 6698. For example the Law no. 6698 does not have a concept of the data protection officer which can be useful in the employment context. Even if they do not strictly relate to employment, from processing of data of children to data protection impact assessment, from right to be forgotten to right to data portability, there are numerous and highly important changes that came with the GDPR unfortunately take no part in Turkish data protection law which ultimately affect

[125] European Data Protection Board.(2020). Guidelines 05/2020 on consent under Regulation 2016/679. p. 8.

the protection of personal data of employees as well. Hence, the Law no. 6698 should be changed in order to be compatible with the GDPR in the shortest time to prevent further infringements.

3. ANALYSIS OF COMMON TYPES OF INFRINGEMENTS WITH JUDICIAL DECISIONS

When it comes to processing personal data of employees, there are numerous forms and reasons. While some of them are deriving from the intents of employers to protect their own premises and/or rights, others can be simply originating from responsibilities laid down to employers by several regulations. All in all, it is clear that the list involving these types cannot be considered as exhaustive hence common types should be narrowed down by looking to some of their features.

These common types of infringements when processing personal data of employees are selected; video surveillance at workplace, monitoring correspondence and monitoring working time via facial recognition and fingerprints systems. Because, firstly these can be considered as data processing includes potential infringements. Furthermore, monitoring correspondence is the most common type and others are specifically important because they are processing biometric data hence needs to be dealt with carefully. Additionally, Turkish case law is not comprehensive enough yet for other types of processing of employees' data ergo cannot be compared with the case law of the ECtHR properly. All in all, it can be said that these types have been selected because of their sensitivity and generality and also the fact that the Turkish case law does not include multiple decisions regarding other types of infringements.

These types are frequently being happened not just in Turkey but all around the world simply because of the fact that the relationship between employers and employees are mainly established on the basis of similar principles set aside minor traditional differences. Thus, these types should be examined in terms of the human rights aspect as well.

To understand the case law in Turkey with regard to data protection, some decisions of the ECtHR and Turkish Courts should be examined. Even if the fact that Turkey is not a member of the EU, some decisions of the CFREU regarding this issue can be considered a guide for data protection law as well. However, for the sake of the limit of this work, case law of the ECtHR will be compared with the Turkish case law.

According to the ECtHR, it is the states' responsibility "to take reasonable and appropriate measures to secure"[126] the right to privacy.[127] Hence, the ECtHR has created a wide case law regarding the right to privacy which also comprises data protection.

Regarding the protection of employees' personal data, the first topic that should be examined is surveillance at workplace. This topic is widely defined and comprises surveillance by video or other means, monitoring the use of devices especially computers, data regarding employees' entering to or exiting from workplace so on and so forth.

When it comes to the case law of surveillance at workplace, the main court should be looked is the ECtHR. Like it has been mentioned previously, the ECtHR renders decisions regarding surveillance at work place in terms of the Article 8 of ECHR. Article 8 is mainly established in order to protect four areas as following; private life, family life, home and correspondence. These are by nature vague terms and in order to avoid conflicts regarding their limits and meanings, the ECtHR has given such important verdicts.

The definition and the limits of concepts of family life and home have been established with the several ECtHR cases.[128] However, in terms of this work's subject, concepts of private life and correspondence have much more importance. Because, ECtHR has been and is working on these cases regarding surveillance at workplace according to these terms.

There are several touchstone cases which have built the case law of ECtHR with respect to surveillance at workplace. It should be said that, apart from those cases will be mentioned below, there are multiple cases regarding data protection in general thus these are the ones that fit the subject perfectly.

As it has been said earlier, there can be different types of surveillance such as video surveillance, monitoring the correspondences (email, telephone etc.) or personal files and

[126] Lloyd, I.J. Information Technology Law. op.cit., Page 25.
[127] Hatton and Others v. United Kingdom, judgment, App. no.36022/97, ECtHR, 08.07.2003.
Accessible at: https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-788265-805159%22]}
[128] Marckx v. Belgium. judgment, App. no. 6833/74, ECtHR, 13.06.1979, 17. Olsson v. Sweden (no.1). judgment, App. No. 10465/83, ECtHR, 24.03.1988, 18. Paradiso and Campanelli v. Italy. judgment, App. no. 25358/12, ECtHR, 24.01.2017., Chiragov and Others v. Armenia. judgment, App. no. 13216/05, ECtHR, 16.06.2015., 19. Winterstein and Others v. France. judgment, App. no. 27013/07, ECtHR, 17.10.2013 and others.
Decisions Accessible at:
https://hudoc.echr.coe.int/eng#{%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22]}

belongings. That is to say, it can be defined as a broad concept. It can be classified as physical and digital surveillance.[129] The cases of the ECtHR concerning this issue can be varied in terms of forms of surveillance. Court did not limit itself with the formality of surveillance but mostly evaluated cases whether the concepts of private life and correspondence comprise the situation in this respect.

3.1. Video Surveillance at Workplace

One of the most popular cases of the ECtHR in terms of video surveillance at the workplace is López Ribalda v. Spain.[130] To summation, the case has been made for employees had been working in a supermarket. In order to investigate the reason for economic losses, the employer decided to set up surveillance cameras that some of which were visible while others were hidden. After the footage showed that applicants were stealing from the employer, they had been dismissed.

Chamber ruled that the employees' rights to respect for their private life laid down in the art. 8 of the ECHR simply because of the fact that video surveillance had been prolonged and deployed not compatible with legislation. Also, it is alleged that the domestic courts failed to make a balance between the right to privacy of employees and interests of employer coming from the right to property.

However, Grand Chamber reversed the judgment and decided there is no violation in terms of art. 8. The Court in this decision underlined the importance of the criteria laid down in Bărbulescu v. Romania case even if it was not regarding video surveillance but monitoring correspondence and usage of the internet simply because those criteria can be reevaluated with new technologies and can be implemented mutatis mutandis.

Hence, the Grand Chamber accentuated that the following conditions should be investigated before making conclusions whether surveillance is not proportionate and may infringe the right to privacy of employees; whether employees had been notified beforehand in a clear way regarding video surveillance, the level of the privacy in the place which is monitored (in this case, for example, the monitoring places are simply checkout place and the entrance of

[129] Abdurrahimli, F. Big Boss is Watching You! The Right to Privacy of Employees in the Context of Workplace surveillance. op.cit., Page 10.
[130] López Ribalda v. Spain. judgment, App. no. 1874/13 and 8567/13, ECtHR, 17.10.2019. Accessible at: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-12630%22]}

the supermarket which can be concluded by the Grand Chamber as low-level privacy places), whether employer justified the monitoring(in this case, it was an investigation of the reason of economic losses which is considered as a legitimate reason by the Court), whether there is a compatibility between the legitimate aim and consequences of the monitoring and lastly whether employees had been informed with regards to their safeguards such as the right to complaint, inform the representatives of employees etc.

By looking at these criteria, the Grand Chamber ruled that the video surveillance, in this case, is proportionate hence the national court's decision is correct and national authorities had not failed to protect the right of these employees. Because employees had been informed, there was a legitimate reason for monitoring, the areas for monitoring were not high-level privacy areas and proportionate in terms of the reason and so on thus these criteria had been met for video surveillance. Additionally, the Court underlined the fact that it was not just one employee who was threatening the employer's interest but several employees were in the same position hence this kind of surveillance had become compulsory in order to protect the right to property of the employer.

The other important case of the ECtHR is Köpke v. Germany[131] regarding video surveillance at the workplace and even if it is decided before López Ribalda v. Spain, it should be mentioned due to the fact that it is one of the cornerstone decisions of the ECtHR in this context. Set aside the background of the case which is similar to the López Ribalda v. Spain, some aspects of the Court should be put into words. Firstly, the Court underlined the importance of the balance between the right to privacy of employees and the right to property and the interests of employers once again. The primary duty of the state is to strike a balance between those rights. Moreover, it accentuated that video surveillance must be proportionate and should have a legitimate reason.

It is highly important as mentioned before that balance between rights should be struck. Due to the controversial nature of the relationship between employees and employers, numerous rights belong to both parties constantly encounter. In terms of video surveillance and data protection in general, mostly employers' right to property and employees' right to privacy are being clashed like in the former case. Both rights are highly valuable and need to be protected

[131] Köpke v. Germany. judgment, App. no. 420/07, ECtHR, 05.10.2010.
Accessible at: https://hudoc.echr.coe.int/eng#{%22appno%22:[%22420/07%22],%22itemid%22:[%22001-101536%22]}

delicately. Hence, the main reason of these criteria lay down above made by the ECtHR directed to harmonize these two rights and evaluate each case separately to determine which right outweighs.

When it comes to Turkish Courts regarding video surveillance, some decisions should be evaluated whether they are compatible with the above decisions of ECtHR and case law in general thereof. However, there is no noteworthy decision of the Turkish Constitutional Court and Court of Cassation with regards to video surveillance of workplaces, hence some of the Council of State's and Turkish Data Protection Board decisions can be evaluated and compared with the ECtHR case law.

One of the Council of State's case opened by a union of public employees with regards to video surveillance in a public university.[132] In this case, the Council of State, by referring to the abovementioned cases of ECtHR and also importantly Antović and Mirković v. Montenegro case[133] which has a similar background, ruled that video surveillance must be proportionate and has to have a legitimate reason and must be the last resort to implement. It also underlined the interpretation of ECtHR in Antović and Mirković v. Montenegro case how the right to privacy laid down in art. 8 comprehend "private social life" which is the "possibility for the individual to develop his or her social identity."[134]

The Turkish Data Protection Board is despite it is not a court, has a related decision.[135] In this case, the employee has opened a case before the court to protect her rights. The employer submitted the video surveillance records to the court and the employee applied to the Board alleging that her personal data without her explicit consent unlawfully be submitted to the court. The Board made a decision that the employer is a cargo company and there are different regulations regarding security measures for cargo companies hence video surveillance is legitimate regardless of whether there is a consent or not.

---

[132] Council of State case no. 2015/2995, Decision no. 2018/1736, 14.05.2018. Accessible in Turkish at: https://www.turkegitimsen.org.tr/userfiles/files/danistay_10daire_karar_2018_1736.pdf

[133] Antović and Mirkovic v. Montenegro. judgment, App. no. 70838/13, ECtHR, 28.11.2017. Accessible at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjMm9aI7OHvAhXLHXcKHeASB_cQFjABegQIBBAD&url=https%3A%2F%2Fhudoc.echr.coe.int%2Fapp%2Fconversion%2Fdocx%2Fpdf%3Flibrary%3DECHR%26id%3D001-178904%26filename%3DCASE%2520OF%2520ANTOVI%25u0106%2520AND%2520MIRKOVI%25u0106%2520v.%2520MONTENEGRO.pdf&usg=AOvVaw1U0wfqkPg8HReQ0qbTNhKG

[134] Antović and Mirković v. Montenegro. op.cit, p.8

[135] The Turkish Data Protection Board case no. 2020/494 Accessible at: https://kvkk.gov.tr/Icerik/6925/2020-494

Council of State's case mentioned above is compatible with the case law of the ECtHR because of the fact that it is referring multiple of decisions of the ECtHR and implementing the same criteria which is established by the ECtHR. However, it is seen that for the Turkish Data Protection Board, it cannot be said that its decision is accordance with the case law of the ECtHR. It is true that there are other legitimacy reasons for data processing besides consent and for employment context it is clear that mostly other legitimacy reasons are being used.

Furthermore, it is underlined by the ECtHR and the EDPB that the processing of employees' personal data is a delicate issue because of the imbalance of power and needs to be evaluated in more detail and there is an additional need for protection. Hence, when it comes to data protection of employees', legitimacy reasons should be interpreted in a strict sense, otherwise, with simple administrative regulations or even administrative actions, protection of employees' personal data can be prevented.

3.2. Monitoring Correspondence

As per the ECtHR case law, telephone calls[136] or emails[137] and internet usage from/in business premises are considered to be defined within the scope of private life and correspondence hence should be protected prima facie.[138] It has been clearly declared that without any warning, individuals may have legitimate expectations for privacy hence infringement may be emerged in such cases.[139]

In addition to that, it also decided that surveillance of usage of computer can be understood within the boundaries of the protection of employers' rights.[140] Thus, it should be evaluated

[136] Case of Halford v. The United Kingdom. judgment, App. no. 20605/92, ECtHR, 18.04.1996. Accessible at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjKzuzE2azvAhVOpIsKHbk7CKAQFjAEegQIGBAE&url=http%3A%2F%2Fhudoc.echr.coe.int%2Fapp%2Fconversion%2Fdocx%2Fpdf%3Flibrary%3DECHR%26id%3D001-45813%26filename%3DHALFORD%2520v.%2520THE%2520UNITED%2520KINGDOM.pdf%26logEvent%3DFalse&usg=AOvVaw00sSF_hFIGxcjJRO1b0GTT

[137] Case of Copland v. The United Kingdom. judgment, App. no. 62617/00, ECtHR, 03.04.2007. Accessible at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22copland%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-79996%22]}

[138] Barbulescu v. Romania. App. no. 61496/08, ECtHR, 05.09.2017. Accessible at: https://hudoc.echr.coe.int/spa#{%22itemid%22:[%22001-177082%22]}

[139] Bronstein, A. International and Comparative Labour Law. Current Challenges. op.cit., Page192.

[140] Libert v. France. judgment, App. no. 588/13, ECtHR, 02.07.2018. Accessible at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjYlNDPtJ_wAhVCl4sKHWFVA9sQFjABegQIAhAD&url=https%3A%2F%2Fhudoc.echr.coe.int%2Fapp%2Fconversion%2Fpdf%2F%3Flibrary%3DECHR%26id%3D003-6014614-

whether the protection of the personal data of employees is infringed by monitoring correspondence or computer usage in terms of each case. However, like it is said before, prima facie it is deemed to be infringed by the Court and then it is investigated whether it can be legitimized by the circumstances set forth in Article 8/2 or by general disciplines of law. The principle of proportionality with this case and all the other cases related has been and still is one of the most important criteria in order to evaluate whether the line is crossed or not.[141]

Some of the cornerstone decisions of the ECtHR with regards to monitoring correspondence are Halford v the United Kingdom and Barbulescu v. Romania. Even if the Halford v the United Kingdom case was considered as "the first case"[142] with regards to monitoring of correspondence of employees, Barbulescu v. Romania case is the one giving comprehensive aspect to this issue. Hence, Barbulescu v. Romania will be analyzed and will be compared with two important and actual decisions of the Turkish Constitutional Court. With this way, it will be analyzed whether case law of Turkish Constitutional Court is compatible with the ECtHR decisions.

Barbulescu v. Romania case was regarding an employee who had been using the computer and internet in the workplace for personal correspondence even it is restricted by the employer with an internal regulation which also had been confirmed by the employee. The Employer has recorded the personal correspondence of the employee and subsequently, employee had been asked to explain why he did not follow the rules in this regard. However, the employee was not informed about the monitoring of correspondence. After some negotiations, the employment contract was terminated by the employer.

Overall, this case is important because of the fact that in this decision criteria had been formulized with regards to monitoring correspondence. As it is mentioned while examining the López Ribalda v. Spain case for video surveillance, it established the main structure of legitimacy of the monitoring of correspondence. Briefly, the employee must be notified, the employer has to have legitimate reasons for monitoring, monitoring of correspondence must be last resort meaning that if any other system would be less intrusive then that way should be

---

7713110%26filename%3DJudgment%2520Libert%2520v.%2520France%2520-%2520employer%2527s%2520consultation%2520of%2520work%2520computer%2520files.pdf&usg=AOvVaw2MUxnu5O-X-Bv5pQb3Gea-

[141] Dimitriv, G. Ilieva, D. Makshutova, R. What data protection rights do employees have in 2018, 2019, Page 27.

[142] Abdurrahimli, F. Big Boss is Watching You! The Right to Privacy of Employees in the Context of Workplace Surveillance. op.cit., Page 48.

implemented, results must be compatible with aims, the employee must be provided with safeguards such as the possibility to complain and the state should provide access to remedy in this regard.

Before getting into case law of the Turkish Constitutional Court, it should be better to mention the structure and authority of it. When it comes to case law with regards to employees' personal data protection, the Turkish Constitutional Court is the main court that should be looked at. It has two main jurisdiction areas as the constitutional review of norms and the individual applications. For the purpose of protection of fundamental rights and freedom, individual application process is coming forward as a primary proceeding.

Individual applications have been started to be accepted in the Turkish Constitutional Court with the amendments of the Constitution in 2010 in order to be compatible with the ECHR and the ECtHR. All individuals who allege that their fundamental rights enshrined in the ECHR and the Turkish Constitution can take their cases to the Turkish Constitutional Court. It is alleged that the establishment of the individual applications to the Constitutional Court improved the fundamental rights and freedoms.[143]

Applying to the Constitutional Court is a prerequisite for appealing to the ECtHR thus both Constitutional Court and case law thereof is highly important for the protection of fundamental rights and freedoms in Turkey including the right to privacy and data protection. Briefly should be said the jurisdiction of the Constitutional Court in terms of individual applications is that jurisdiction ratione materiae involves fundamental rights and freedoms set forth in ECHR and the Constitution, jurisdiction ratione personae includes real persons and private legal person in exceptional circumstances. In order to apply to this proceeding, it must be firstly said that legal remedies should be exhausted and the application must be made within thirty days after the final decision.[144]

All in all, before getting into some specific cases regarding this work's topic, because of the fact that the Turkish Constitutional Court is in the highest place of the legal system in Turkey

[143] Aslan, V. The Role of Turkish Constitutional Court in the Democratization Process of Turkey:From 2002 to Present. Constitutionalism in a Plural World(Ed. Botello, C.S., Terrinha, L.H., Coutinho, 2017, page 141. Accessible at: https://www.researchgate.net/publication/326692889_The_Role_of_Turkish_Constitutional_Court_in_the_Democratization_Process_of_Turkey_From_2002_to_Present/link/5b5f4a470f7e9bc79a6f49ec/download

[144] Constitutional Court of Turkey. Introductory Booklet. Accessible at: https://ayam.anayasa.gov.tr/media/2745/introductorybooklet.pdf

and it is a final court to be applied in terms of protection of fundamental rights and freedom domestically, all its decisions arising from individual applications are binding and it is a compulsory stage for applying to the ECtHR, the importance of it should be underlined.

The Constitutional Court has particular case law with regards to the right to privacy and data protection such as decisions which have declared that information of "name, surname, birth date, birthplace as well as telephone number, motor vehicle license plate, social security number, passport number, resume, picture, image and sound records etc."[145] falls within the scope of personal data hence needs to be protected by the data protection law and the important thing is to remember when determining whether data is personal or not is that whether data is related or not[146] or such case that the Court interpreted the Constitution broadly and ruled that legal persons are also under the protection of Constitution with regards to data protection in some circumstances.[147] However, for the limitation of the topic, the decisions of the Court regarding the protection of employees' personal data should be observed.

One case is novel and involves one of the most important aspects when it comes to data protection in the employment context, the term of "consent". The case dated 12.01.2021 is regarding whether the monitoring of one of the employees' work emails by the employer is justifiable or not. The applicant was an employee of a private bank and had been working since 2007. He accepted with employment contract that he is responsible for using the work email just for work purposes, he could be inspected without pre-notice and he could not have a right to oppose this inspection. It is subsequently understood thanks to one inspection that the applicant had been using the work email for another purpose and henceforth his employment contract had been terminated.

After the exhaustion of legal remedies, The Court had been applied for allegations of infringement of the right to privacy and freedom of communication. The Court ruled that the state has negative and positive obligations in terms of the protection of fundamental rights and freedoms, positive obligations involve establishing an effective legal system, fair trial and constitutional supervision. It set forth that it is compulsory to redress the balance between

[145] The Turkish Constitutonal Court case 2014/74 Accessible at: https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2014/74?KararNo=2014%2F74
[146] The Turkish Constitutonal Court case 2014/74, op.cit.
[147] The Turkish Constitutonal Court case 2014/74 Accessible at: https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2014/183?KararNo=2014%2F183

employers' interest and fundamental rights and freedom of employees. In order to make it happen, it is crucial as per the Court to evaluate that whether the inspection could be justified by the employer, it has been realized in accordance with the principle of transparency and proportionality, it is inevitable and no other light-weighted interference could be used.

The Court, as a result, declared that the interference of the employer is justified and in accordance with the purpose thus applicant's right to privacy and freedom of communication have not been infringed. The main basis for the Court is that the employee has been informed of the employment contract, it is not necessary to take specific consent for this inspection, it is clear that the applicant had used his work email to the detriment of the interest of the employer and his employment contract.[148]

It should be said that there is another parallel decision made by the Constitutional Court in this regard.[149] That is to say that this is the general approach of the Court when it comes to monitoring the correspondence that is there is general consent in the employment contract, the Court's opinion is that there is no violation. However, in other situation meaning that there is not any consent and pre-notice, the Court decides that there is an infringement of the right to privacy.[150]

Regarding the main case detailed given above, with the acceptance of the fact that the Court repeated the fundamental principles of data protection law, data protection in the employment context as it has been evaluated above chapters has its own unique conditions especially concerning the concept of "consent". This case is a good example to notice the difference in terms of data protection between other groups of people and employees. Because the meaning of consent as a legitimate interest could be differentiated between those groups of people. That is to say for example for customers it can be reasonable to take consent for the processing of their data whereas it can simply mean nothing when it comes to employee-employer relations.

[148] The Turkish Constitutonal Court case Application no. 2018/31036
Accessible at: https://www.resmigazete.gov.tr/eskiler/2021/02/20210205-15.pdf
[149] The Turkish Constitutonal Court case Application no. 2013/4825
Accessile at: https://kararlarbilgibankasi.anayasa.gov.tr/BB/2013/4825
[150] The Turkish Constitutonal Court case Application no. 2016/13011
Accessile at:
https://kararlarbilgibankasi.anayasa.gov.tr/BB/2016/13011?KelimeAra%5B%5D=ki%C5%9Fisel+veri&KelimeAra%5B%5D=i%C5%9F%C3%A7i

This concern can be also seen from the Opinion 2/2017 of the Article 29 Data Protection Working Party which has been replaced by the European Data Protection Board ("EDPB") that "Employees are almost never in a position to freely give, refuse or revoke consent, given the dependency that results from the employer-employee relationship. Given the imbalance of power, employees can only give free consent in exceptional circumstances, when no consequences at all are connected to acceptance or rejection of an offer."[151]

The Court in this case interpreted the issue as if it does not have special circumstances with the fact that it has occurred between employee and employer. Even though there are no special regulations in Turkish legislation with regards to the term of consent for employment relations, it is still the responsibility of the state to protect the fundamental rights and freedoms of individuals and consider the different situations. Employment contracts are different from general contracts by means of their duration, power imbalance and so on and so forth.

Given the reasons above that taking consent while signing the employment contract should not be enough to process data, monitor correspondence and breach the right to privacy. It can be hard to implement always taking distinct consents for any types of data processing or monitoring but it can be taken for example at regular intervals and keep informing employees at the same time. It is important to balance between the interest of employees and employers but with this way, because of the fact that it is already an imbalanced relationship, general data protection system is hard enough to protect employees' personal data in terms of consent as it is seen in the example case of the Constitutional Court.

These decisions also must be compared with the criteria set forth in Barbulescu v. Romania case. Monitoring of correspondence in these cases had been justified with one provision in employment contracts. It can be seen easily that condition regarding notification of employees is met. However, it should be accepted that these notifications are weak and outdated. The extent of the monitoring is vague, employers could not provide legitimate reasons for monitoring, because of the fact that there is no certain aim, results are not compatible with aims and lastly employees had not been provided for adequate safeguards. It is easily seen

[151] Opinion 2/2017 of the Article 29 Data Protection Working Party Accessible at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169

that the criteria of the ECtHR with regards to monitoring of correspondence had not been implemented in Turkish Constitutional Court decisions.

3.3. Facial Recognition and Fingerprint Systems

Facial recognition and fingerprint systems are being established in order to follow the employees' entrance to and exit from workplaces thus also record working times. According to the GDPR art. 4/14 " 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."[152] The Law no. 6698 has a similar provision. This type of data should only be processed under special circumstances. Hence, it can be easily said that data processed by Facial recognition and fingerprint systems are biometric data[153] and definitely fall within the scope of sensitive data.

Sensitive data can only be processed with the explicit consent for specific purposes. According to the GDPR art. 9/2, sensitive data can be processed if "processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject."[154] It is important to understand that as it is written in this provision, sensitive data in the field of employment can be processed without the explicit consent but in one condition, the fundamental rights and the interests of employees' should be safeguarded.

It can be said that there is no specific case law of the ECtHR on this issue, however, there are a couple of decisions declaring that collected data with new technologies such as electronic surveillance, facial recognition systems or fingerprints should be interpreted within the scope of the right to privacy and balance should be struck between data subject's rights and legitimate purposes of the processing. Otherwise, it can lead to a violation of the right to

[152] GDPR, op.cit., Article 4/14.
[153] Woodward, J.C., Horn, C., Gatune, J., Thomas, A. Biometrics.A Look at Facial Recognition. - RAND, 2003, Page 3-4. Accessible at: https://apps.dtic.mil/sti/pdfs/ADA414520.pdf
[154] GDPR, op.cit., art. 9/2.

privacy.[155] Also, the delicacy of the facial recognition technologies is recently underlined by the Council of Europe Secretary-General by saying that "At is best, facial recognition can be convenient, helping us to navigate obstacles in our everyday lives. At its worst, it threatens our essential human rights, including privacy, equal treatment and non-discrimination, empowering state authorities and others to monitor and control important aspects of our lives – often without our knowledge or consent".[156]

In order to evaluate Turkish case law regarding this issue, case law of the ECtHR with regards to video surveillance and monitoring correspondence especially criteria set forth in Barbulescu v. Romania decision can be utilized with the core principles of data protection law.

When it comes to monitoring of working time in decisions of Turkish courts, it can be said that some specific decisions of the Council of State can be given. The decision was made by the Council of State[157], which can be defined as the appeal court when it comes to administrative legal acts meaning that to decisions made by the administrative court can be brought before the Council of State in order to be reversed.

In this case, a union on behalf of its members suits a file against one of the public institution which public employees have been working for. The case is regarding that in order to record the working time of employees, the employer constituted the facial recognition system and by creating this system it started to record the employees in and out times from and to the workplace. The Union alleged that the data has been collected by this system are recorded into a database thus this procedure should be defined as data processing and must be abandoned due to the fact that it is against constitutional principles, human rights law and data protection law.

The Administrative Court ruled against the allegations of the Union by stating that this procedure is not realized in every other units and for this unit, it is inevitable to be used in order to follow the working time healthily because for this unit there were some problems

[155] ECtHR. New Technologies Factsheet, 2021.
Accessible at: https://www.echr.coe.int/Documents/FS_New_technologies_ENG.pdf
[156] Accessible at: https://www.coe.int/en/web/portal/-/facial-recognition-strict-regulation-is-needed-to-prevent-human-rights-violations-
[157] Kaya, M.B., Taştan, F.G. Personal Data Protection Law. Second Press. Onikilevha Press, 2019, Page 627-630. Accessible at: https://www.mbkaya.com/hukuk/veri-koruma-hukuku.pdf
Council of State case no. 2017/816

occurred in terms of working times of employees, also these data collecting by the facial recognition system are being turned into numerical codes and it does not mean it is recording data hence it cannot be interpreted as there is a violation.

The Council of State delivered its judgment by referring to the provisions laid down by the Constitutions and the ECHR art. 8 with regards to the right to privacy and stated that this procedure should be considered as processing of personal data, even it has emerged in the public area it is still in the context of the right to privacy and there is no guarantee that this data collected will not be used for something else in the future hence this procedure gives rise to a violation of the right to privacy of employees and should be cancelled.

Council of State is persistent regarding facial recognition systems in workplaces. There is another decision which is similar to the abovementioned case and it is given by one of the highest chamber in the Council of State.[158] Thus, it can be said that in terms of facial recognition systems in workplaces there is concrete stare decisis.

Another case of the Council of State is regarding the monitoring working time of employees by using a fingerprint system.[159] The case is brought before the administrative court by a union on behalf of its members who are working one of the state hospitals. The Administrative Court ruled that the card system has been already tried and it was not effective as it should be, there is no real harm of this fingerprint system for employees hence the administrative implementation is justifiable. However, the Council of State in its final decision gave its decision in accordance with its other decision regarding facial recognition systems mentioned above and found the union right for its legal action. The Court referred the related constitutional provisions and the ECHR art. 8 and found that this procedure is causing the infringement of employees rights thus needs to be abandoned.

These cases are highly important because of numerous reasons. Firstly, it is clear to understand that these cases have been brought up by a union on behalf of its members. Additionally, these employees are public employees and the workplaces are public institutions hence it is one of the many reasons to believe that data protection in the employment context

[158]Council of State case no. 2015/2958
Accessible at: http://www.kesk.org.tr/wp-content/uploads/2018/07/Y%C3%BCz-Tan%C4%B1ma-Sistemi-%C4%B0le-Mesai-Takibi-Hukuka-Ayk%C4%B1r%C4%B1d%C4%B1r-Dan%C4%B1%C5%9Ftay-Tokat-Karar%C4%B1.pdf
[159] Kaya, M.B., Taştan, F.G. Personal Data Protection Law. op.cit., Council of State case no. 2014/2242

comprises both private and public employees. They are also important because of the fact that they created case law with regards to monitoring working times by facial recognition systems and fingerprint systems. These situations are affecting both private and public employees to a large extent.

Apart from the court decisions, the issue has been also interpreted by the Turkish Data Protection Board. In one of its cases regarding the monitoring of employees' entrance to and exit from workplace by processing biometric data, as compatible with the decision of the Council of State abovementioned, the Board concluded that these types of data processing cannot be considered as proportionate, relevant and limited to purposes hence actions of this personnel which are responsible for this infringement should be investigated in terms of discipline proceeding and data which has been processed until this decision should be erased.[160]

It can be seen from the decisions abovementioned, Turkish case law is compatible with the case law of the ECtHR in that regard. By looking at example decisions, it is clear that Turkish courts are making their decisions by referencing the important decisions of the ECtHR and principles of the data protection law.

[160] The Board Decision no. 2020/915 date 01.12.2020 Accessible at: https://kvkk.gov.tr/Icerik/6872/2020-915

CONCLUSION

The right to privacy has been one of the most vulnerable human rights throughout history. Likewise, it has been maybe the most controversial human rights too because of the fact that it is constantly clashing with other rights, especially freedom of expression, freedom of the press and so on and so forth. Additionally, the difficulty of defining and limiting the right has been creating further problems.

All in all, the discussions with regards to the right to privacy have been continuing in terms of its definition, limitation and necessity to strike a balance with other fundamental rights. However, the astonishing improvement of technology in the recent period has changed the mentioned issues remarkably and caused to creation of novel legal areas. One of the most popular and related to the right to privacy areas is called data protection law. In company with the stunning development of technology especially the invention of the internet, the right to privacy has reached a phase that now it is in the most endangered situation. Internet and other technologies that make surveillance in general much easier are threatening the right to privacy to a large extent.

Throughout the world, states started to establish regulations in order to control this new and mostly unknown universe. However, because of its rich content and unstoppable progression makes it quite formidable. From cyber wars to e-commerce or from data protection rights to intellectual property rights of the art pieces created by artificial intelligence software programs, states have hard times regulating those controversial areas in accordance with the development of technology. Indeed, even states conclude to regulate, technology goes to a new phase that more complicated legal problems have emerged.

Nevertheless, states and international/regional organizations are working on these issues to understand the pros and cons hence prevent some possible infringements and problems. Because now from almost all fundamental rights but especially the right to privacy to national securities and from democracy and rule of law to equality, all cornerstone principles and rights of international law and human rights are at utmost stake.

More specifically and in terms of human rights, it can be said that the most affected human right is the right to privacy. Data protection, in general, is still mostly considered as the area is

within the scope of the right to privacy hence international standards of the right to privacy should be implemented for data protection issues smoothly. However, some instruments such as the CFREU acknowledge data protection law as a separate topic than the right to privacy. On the other hand, for example, the ECtHR is still considering the data protection issues as the subtopic of the right to privacy thus looking at related cases in terms of the article which is regarding the right to privacy. Nevertheless, it is undeniable fact that the right to privacy and data protection law are strictly related.

In recent times, it can be seen that these problems caused by the rapid development of technology have not been talked about issues just with respect to human rights law, most if not all law areas have been affected substantially such as criminal law, finance law and so on and so forth. However, when it comes to the right to privacy and lack of an effective system of data protection, one of the most affected groups of people are employees hence labour law has been affected dramatically.

Because of the very nature of the imbalanced relationship between employees and employers, in labour law issues have been getting much more complicated hence they should not be looked at as if issues emerged between other groups of people. The same rules cannot be implemented to employee and employer relations in a similar way. This is mainly because of the fact that employees are much powerless compared to employers. This fact can be seen from for example the existence of the unions which have been established just from the very fact that employees have one by one almost zero power before employers.

With the rapid development of technology, the protection of employees' personal rights has become much more difficult. Some new tools gave employers more opportunity to monitor their employees and workplaces. Some implementations have even become ordinary applications such as surveillance of workplace and premises by video and audio recording tools, monitoring the employees working times with facial recognition and fingerprint systems. Additionally, personal correspondence of employees is being tried to be prevented or controlled.

These are the common fragile implementations that can be harmful to employees' personal data rights. However, it should be also underlined that infringements can be occurred in many different forms other than these mentioned such as leakage of personal data of employees', exposing the sensitive data of employees and so on and so forth.

The hypothesis of this thesis, the Turkish data protection law by legislation and case law is not effectively protecting employees' personal data, has been verified by the thesis. To prove the hypothesis, the first research question of this work was whether Turkish regulations are efficient for protecting the rights of employees' personal data and they are in compliance with international legal and de facto standards.

The Law no. 6698 is the principal legal act of Turkey with regards to data protection in general. There are related provisions set forth in several legal acts however it can be said that they are far from regulating this specific area. Firstly, it should be mentioned that Turkey has taken the former directive of the EU regarding data protection to excerpt it and established its own data protection legislation which is the Law no. 6698. Thus, it is clear that the problems of the former directive and the reasons of why the GDPR has been established are taken to the Law no. 6698 almost identically. The comprehensive protection system of the GDPR could not be simulated in Turkey.

The new and effective tools such as processing of data of children, data protection impact assessment, right to be forgotten, right to data portability and so on and so forth are still not in Turkish regulations hence legislation should be changed in order to be in compliance with the GDPR. This is not just for the protection of employees' personal data but a necessity to constitute an effective system for everyone. Additionally, conformity between the GDPR and Turkey's regulations makes better international protection for personal data as well because of the very international nature of data protection.

When it comes to the specific area of protection of employees' personal data, it can be said that even the GDPR has deficiencies despite the fact that in the article 88 it highlighted the importance of this topic and directed the member states to make their legislations more protective in terms of employees' rights. This can be caused because of the fact that the GDPR, even though it is a legally binding regulation, is general character and mostly trying to direct member states to have similar legislations for further protection. This feature of it having general and vague provisions has been criticized. For the protection of employees' personal data, it would have more detailed provisions with regards to consent, conditions of workplace and correspondence surveillance and so on and so forth. However, it also can be said that this is not a national legislation; it is enough for the GDPR to direct member states to have such legislations to cover these specific areas.

The Law no. 6698 has deficiencies in terms of some aspects mentioned above. These discrepancies are mostly related with data protection in general but they are also affecting the protection of employees' personal data to a large extent. However, one of the other recommendations of this work is the necessity of the comprehensive legal act which includes exceptional circumstances of the protection of employees' personal data.

When the Turkish regulations are investigated, it can be seen that there are related provisions among several legal acts but most of them are general provisions regarding data protection. Additionally, there are some regulations for the right to privacy such as the Constitution, the Criminal Code, the Labour Law so on and so forth. Among them, it can be said that may be the only strictly related one is the one in the Labour Law which is simply regularizing the physical personal file involving employees' personal data. It can be easily said by just looking at this provision that Turkish Law is outmoded and far from having a comprehensive protection system thus needs to be altered progressively.

The first and foremost step for realizing an efficient system in Turkey is to establish an independent legal act or at least a considerably large chapter in the Law no. 6698 or the Labour Law. This legal act should include the same principles set forth by the GDPR but also the recommendations and guidelines of the ILO and the CoE. With this way, more related but not binding international instruments can be evolved into a binding legal act. Furthermore, it should be underlined that this legal act is the first place to look at in pursuant of lex specialis.

The legal act should establish provisions that include criteria for common infringements such as surveillance at workplace and correspondence of employees via video recording, facial recognition and fingerprint systems and all other potential technologies. These criteria should be in accordance with the criteria set forth by the ECtHR in several cases. With this approach, the criteria of the ECtHR which can be considered as the most protective system in terms of surveillance and monitoring can be transformed to binding provisions rather than being legal precedent. Because, as it will be mentioned below, Turkish courts with some cases show the unwillingness to implement the ECtHR decisions strictly and made some decisions were not in accordance with the case law of the ECtHR. Hence, there is an absolute need for these criteria to be converted to binding provisions.

The GDPR art. 88 underscored the importance of the collective labour agreements as well. Thus, as a suggestion, in this legal act, there can be some provisions for data protection

provisions can be written to collective labour agreements for further protection and details of some sort of monitoring system is being handled by unions can be determined.

The second research question of the work is whether Turkish case law in accordance with the case law of the ECtHR in terms of common infringement cases such as video surveillance at workplace, monitoring correspondence and monitoring of working time via facial recognition and fingerprint systems. It should be accepted that there various maybe limitless types of infringements because of the very complex nature of the relationship between employees and employers, however, these types are both evaluated by the ECtHR and especially higher courts of Turkey. Additionally, it must be accentuated that Turkish case law, in general, is not comprehensive and wealthy in terms of data protection in general and more specifically in terms of the protection of employees' personal data.

When it comes to the case law of the ECtHR it can be said that the most famous case is Barbulescu v. Romania. The Court in this case laid down the main criteria for monitoring the employees' correspondence. These criteria can be juxtaposed as following; employers should clearly notify employees in terms of surveillance, privacy level in the workplace should allow for surveillance, legitimate aim and results should be compatible and employees should be informed that they have some safeguards.

Also in López Ribalda v. Spain, the Court declared that these criteria can be used for video surveillance as well. Hence, it can be said that these criteria can be considered as the main source for monitoring the employees in general. For example, for monitoring of working time via facial recognition and fingerprint systems, there are no specific cases of the ECtHR, however with simple logic it can be easily said that they can and should be implemented for these types of cases as well.

Turkish Constitutional Court, despite the case law of the ECtHR, declared in several cases that consent taken with the labour agreements in terms of monitoring of correspondence of employees is enough for legitimacy. This is the exact opposite of the case law of ECtHR. ECtHR states that monitoring should be exceptional and it can be said there is legitimacy only if these criteria mentioned are realized.

The employer, in this case, does not notify employees, there is no interpretation of privacy level in the workplace, there is no apparent legitimate or even any particular aim thus there is

no conformity between aim and results and because employees do not know anything about the monitoring it is clear that there are no safeguards known by employees. The approach of the Constitutional Court makes it almost impossible to compare its decisions with the criteria set forth by the ECtHR.

Additionally, it should be also underlined the fact that the term of consent, despite the value in data protection law, is and should not be the main legitimacy reason in the employment context. Because of the imbalanced nature of the relationship between employees and employers, consent cannot be taken as a legitimacy reason. This point has been declared by the former Article 29 Data Protection Working Party as well. It declared that consent can be a reason for legitimacy only in some exceptional circumstances. Hence, the decisions of the Constitutional Court are not just contradictory to the case law of the ECtHR but also are against the special circumstances of the data protection in the employment context.

For the facial recognition systems and fingerprint systems, even if there is no specific cases of the ECtHR, it can be said that the higher courts of Turkey render their decisions in accordance with the general case law of the ECtHR with regards to data protection and the right to privacy. In their decisions, case law of the ECtHR is mostly referred. This comment is also valid for video surveillance at workplace.

Consequently, it can be said that the main problem for the case law of Turkish courts is the approach of the Turkish Constitutional Court with regards to monitoring of correspondence and general illogical thinking of usage of consent as legitimacy reason in employment relations. However, for the other areas, it can be said that the Turkish case law is not still comprehensive. This can be caused because of the fact that data protection law, in general, can be considered still as one of the newest legal areas in Turkey and let alone employees, people, in general, are not fully aware of their rights and obligations.

As time progresses, it is inevitable for the Turkish courts will have to deal with these cases to a large extent. This is why the need for a general legal act to regulate this problematic area before getting into a phase that there is no detailed legislation and also no comprehensive jurisprudence is being recommended.

All in all, these recommendations have to be realized together in order to establish an effective data protection system for employees' personal data. Data protection regulation the

Law no. 6698 should be interpreted again and become legislation compatible with the GDPR which is one of the most important data protection regulations throughout the world and considered as it includes de facto standards with regards to data protection.

Additionally, a separate legal act for employees personal data protection should be established which will cover the specific circumstances of the issue such as consent, surveillance at workplace, monitoring the correspondence, authority and obligations of union and role of collective labour agreements and so on and so forth.

Lastly, with the necessary changes in legislation, Turkish courts case law should be in accordance with the case law of the ECtHR with regards to data protection in general and specifically employees' personal data. It is observed that especially as per monitoring correspondence, the approach of the Turkish Constitutional Court is not compatible with the case law of the ECtHR thus needs to be altered.

BIBLIOGRAPHY

Literature

1. Ackoff, R. L. From Data to Wisdom. - Journal of Applies Systems Analysis, Vol 16, 1989.
2. Akdeniz, Y. Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship, 2010.
3. Akgül, M., Kırlıdoğ, M. Internet Censorship in Turkey. - Internet Policy Review Journal on Internet Regulation. Vol 4, Issue 2, 2015.
4. Aslan, V. The Role of Turkish Constitutional Court in the Democratization Process of Turkey:From 2002 to Present. Constitutionalism in a Plural World(Ed. Botello, C.S., Terrinha, L.H., Coutinho, P.), 2017.
5. Baskarada, S., Koronios, A. Data, Information, Knowledge, Wisdom (DIKW): A Semiotic Theoretical and Empirical Exploration of the Hierarchy and its Quality Dimension. - Australasian Journal of Information Systems. 18(1), 2013.
6. Bernstein, J.H. The Data-Information-Knowledge-Wisdom Hierarchy and its Antithesis. City University of New York (CUNY) Academic Works Publications and Research, 2009.
7. Blackmer, W.S. Data Protection in the Private Sector: convergence or localisation of rights and expectations?. Human Rights, Digital Society and the Law A Research Companion (Ed.Mart Susi). Routledge, 2019.
8. Borchardt, K. The ABC of EU Law. European Union, 2017.
9. Bronstein, A. International and Comparative Labour Law. Current Challenges. ILO, 2009.
10. Buckley, C. The European Convention on Human Rights and the Right to Life in Turkey. - Human Rights Law Review. Vol 1, No 1, 2001.
11. Clayton ,R., Kjerulf-Thorgeırsdottır, H., Dıjk, P. Benedek, W., Turk, K. (European commission for Democracy Through Law(Venice Commission)). Opinion on Law No. 5651 on Regulation of Publicatıons On the Internet and Combating Crimes commıtted by means of such Publicatıon(“The Internet Law”), 2016.
12. Craig, P. Burca, G.D. EU Law Text, Cases, and Materials. Fifth Edition. Oxford University Press, 2011.
13. DeVries, W. Protecting privacy in the digital age. Berkeley Technology Law, 2003.

14. Dimitriv, G. Ilieva, D. Makshutova, R. What data protection rights do employees have in 2018, 2019.
15. Dove, E.S. EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. - The Journal of Law Medicine & Ethics. 46, 2018.
16. Elkins, Z., Ginsburg, T., Simmons, B. Getting to Rights: Treaty Ratification, Constitutional Convergence, and Human Rights Practice. - Harvard International Law Journal . Vol. 54 No. 1, 2013.
17. Geden, A.M., Bengshir, T.K. Reflections from GDPR to Turkish Data Protection Act in the Context of Privacy Principles. - IMISC 2018 Conference Proceedings, 2018.
18. Haworth, N. Hughes, S., Wilkinson, R. The international labour standards regime: a case study in global regulation. - Environment and Planning A 2005, volume 37, 2005.
19. Jeffery, A. J. Free speech and press: An absolute right. - Human Rights Quarterly, 8(2), 1986.
20. Kaya, M.B. The New Paradigm of Data Protection Law: The Principle of Accountability. - İstanbul Hukuk Mecmuası, 78 (4), 2021.
21. Kaya, M.B., Taştan, F.G. Personal Data Protection Law. Second Press. Onikilevha Press, 2019.
22. Kınıkoğlu, B., Zengin, S., Akdere, K.C. Turkey. The Privacy, Data Protection and Cybersecurity Law Review. (Ed.A.C.Raul). 6th Edition. The Law Reviews, 2019.
23. Land, M. Toward an International Law of the Internet. - Harvard International Law Journal. Vol 54 No. 2, 2013.
24. Liew, A. Understanding Data, Information, Knowledge And Their Inter-Relationships. - Journal of Knowledge Management Practice, Vol. 7, No. 2, 2007.
25. Lloyd, I.J. Information Technology Law. Oxford University Press. 8th Edition, 2017.
26. Lyutov, N. The ILO System of International Labour Standards and Monitoring Procedures: Too Complicated to be Effective?. - Zbornik PFZ, 64, (2), 2014.
27. Michelle Bachelet, Human rights in the digital age - Can they make a difference?. Japan Society, New York, 17 October 2019. Key Speech.
28. Milanovic, M. Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age. - Harvard International Law Journal. Vol. 56 No.1, 2015.
29. Mowbray, A. Cases and Materials on the European Convention on Human Rights. Second Edition. Oxford University Press, 2007.
30. Ogriseg, C. GDPR and Personal Data Protection in the Employment Context. - LLI, Vol. 3, No. 2, 2017.

31. Pajuste, T. The Protection of personal data in a digital society. The role of the GDPR. Human Rights, Digital Society and the Law A Research Companion (Ed.Mart Susi). Routledge, 2019.
32. Penney, J. The Right to Privacy. The en of Privacy Fatalism. Human Rights, Digital Society and the Law A Research Companion (Ed. Mart Susi). Routledge, 2019.
33. Purtova, N. The law of everything. Broad concept of personal data and future of EU data protection law. - Law, Innovation and Technology, 10:1, 2018.
34. Robertson, D. A Dictionary of Human Rights. Europa Publications. 2nd Edition, 2004.
35. Rustad, M., Paulsson, S.R. Monitoring Employee E-Mail And Internet Usage: Avoiding The Omniscient Electronic Sweatshops: Insights From Europe. - University of Pennsylvania Journal of Labor and Employment Law, 2005.
36. Sander, J.D. Terms: Data, Information and Knowledge. SAI Computing Conference. London, UK, 2016.
37. Smith, R.K.M. Textbook on International Human Rights. Oxford University Press; 7th edition, 2016.
38. Wang, Y. Formal Cognitive Models of Data, Information, Knowledge, and Intelligence. WSEAS Transactions on Computers, 2015.
39. Warren, D.S., Brandeis, L.D. Harvard Law Review, Vol. 4, No. 5, 1890.
40. Wilkinson, L. The Grammar of Graphics.(Statistics and Computing). Second Edition. Springer, 2005.
41. Witzleb, N. Employee Monitoring and Surveillance under Australian Law: The Need for Workplace Privacy Legislation. Perspectives on Privacy (Eds.Dieter Dörr, Russel L. Weaver), 2014.
42. Woodward, J.C., Horn, C., Gatune, J., Thomas, A. Biometrics. A Look at Facial Recognition. - RAND, 2003.
43. Zlemele, I. Privacy, Right to, International Protection. Max Planck Encyclopedia of Public International Law. Oxford Public International Law, 2009.

Master Theses

1. Abdurrahimli, F. Big Boss is Watching You! The Right to Privacy of Employees in the Context of Workplace Surveillance. Master's Thesis. Lund University, 2020.
2. Bakırel, N.B. Allocation of Responsibility among Data Controller and Data Processor within the Scope of General Data Protection Regulation and Turkish Law on the Protection of Personal Data. Master's Thesis. Hacettepe University, 2020 .

3. Dursun, Y. The Protection of Labour According to 6698 Numbered Protection of Personal Datas Law. Master's Thesis. Dokuz Eylül University, 2019.

International, Regional and National Instruments

1. Article 29 Data Protection Working Party. Opinion 2/2017 on Data Processing at Work, 2017.
2. Convention for the Protection of Human Rights and Fundamental Freedoms("ECHR"). Rome, 04.11.1950, e.i.f. 03.09.1953.
3. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention no.108"). Strasbourg, 28.01.1981, e.i.f. 01.10.1985.
4. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows.("Additional Protocol no. 181"). Strasbourg, 08.11.1981.
5. Recommendation No. R (2015)5, CoE. 2015.
6. Recommendation No. R (89) 2, CoE, 1989.
7. Handbook on European data protection law 2018 edition, CoE, 2018.
8. Constitutional Court of Turkey. Introductory Booklet.
9. New Technologies Factsheet, ECtHR, 2021.
10. Guidelines on consent under Regulation 2016/679, EDPB, 2020.
11. Charter of Fundamental Rights of the European Union("CFREU"), Strasbourg, 26.10.2012.
12. General Data Protection Regulation. Strasbourg, 27.04.2016, e.i.f.25.05.2018.
13. Code of Practice of Protection of workers' personal data, ILO. 2003.
14. Centenary Declaration for the Future of Work adopted by the Conference at Its One Hundred and Eighth Session, ILO, 2019.
15. Rules of the Game An introduction to the standards-related work of the International Labour Organization. Centennary Edition, ILO, 2019.
16. Trade, Employment and Labour Standards A Study of Core Workers' Rights and International Trade, OECD, 1996.
17. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD, 2013.
18. Treaty on the Functioning of the European Union ("TFEU"). 26.10.2012.
19. Constitution of the Republic of Turkey. 18.10.1982, e.i.f. 9.11.1982.

20. Guideline of Controller and Processor, Turkish Data Protection Board.
21. Turkish Penal Code ("Law no. 5237"). 26.09.2004. e.i.f. 12.10.2004.
22. Social Insurance and Universal Health Insurance Law ("Law no. 5510"). 31.05.2006, e.i.f. 16.06.2006
23. Universal Declaration of Human Rights ("UDHR"). Paris, 10.12.1948.
24. International Covenant on Civil and Political Rights("ICCPR"). New York 16.12.1966, e.i.f. 23.03.1976.
25. Guidelines for the Regulation of Computerized Personal Data Files. The General Assembly, 14.12.1990.

Jurisprudence

1. The Joined Cases C-465/00, C-138/01 and C-139/01, CJEU, 20.05.2003.
2. Council of State case no. 2014/2242
3. Council of State case no. 2015/2958
4. Council of State case no. 2015/2995
5. Council of State case no. 2017/816
6. Niemietz v. Germany, judgment, App. No. 13710/88, ECtHR, 16.12.1992.
7. Antović and Mirkovic v. Montenegro. judgment, App. no. 70838/13, ECtHR, 28.11.2017.
8. Barbulescu v. Romania. judgment, App. no. 61496/08, ECtHR, 05.09.2017.
9. Chiragov and Others v. Armenia. judgment, App. no. 13216/05, ECtHR, 16.06.2015.
10. Copland v. The United Kingdom. judgment, App. no. 62617/00, ECtHR, 03.04.2007.
11. Halford v. The United Kingdom. judgment, App. no. 20605/92, ECtHR, 18.04.1996.
12. Hatton and Others v. United Kingdom, judgment, App. no.36022/97, ECtHR, 08.07.2003.
13. Köpke v. Germany. judgment, App. no. 420/07, ECtHR, 05.10.2010.
14. Libert v. France. judgment, App. no. 588/13, ECtHR, 02.07.2018.
15. López Ribalda v. Spain. judgment, App. no. 1874/13 and 8567/13, ECtHR, 17.10.2019.
16. Marckx v. Belgium. judgment, App. no. 6833/74, ECtHR, 13.06.1979.
17. Olsson v. Sweden (no.1). judgment, App. No. 10465/83, ECtHR, 24.03.1988.
18. Paradiso and Campanelli v. Italy. judgment, App. no. 25358/12, ECtHR, 24.01.2017.

19. Winterstein and Others v. France. judgment, App. no. 27013/07, ECtHR, 17.10.2013.
20. The Turkish Constitutional Court case no. 2017/22355
21. The Turkish Constitutional Court case no. 2013/4825
22. The Turkish Constitutional Court case no. 2014/74
23. The Turkish Constitutional Court case no. 2016/13011
24. The Turkish Constitutional Court case no. 2018/31036
25. The Turkish Data Protection Board case no. 2020/494
26. The Turkish Data Protection Board case no. 2020/915

Non-exclusive licence to reproduce thesis and make thesis public

I, Aykut Özgürsoy,

1.herewith grant the University of Tartu a free permit (non-exclusive licence) to reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

Compatibility of Employees' Personal Data Protection in Turkey with International Legal And De Facto Standards,

supervised by Aleksei Kelli,

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Aykut Özgürsoy

28.04.2021