Research Article

Received: 11 August 2021 / Accepted: 7 January 2022 / Published: 5 March 2022

Evaluation of E-mail Accounts Used in Public Institutions in Turkey Within the Scope of Personal Data

Mensur Morina

University of Business and Technology, Kosovo;
Hacettape University, Institute of Science, Beytepe, Ankara, Turkey

Endri Papajorgji

Dean, Faculty of Law,
Tirana Business University,
Albania

Muhammet Ali Eren

Hacettepe University, Institute of Science,
Beytepe, Ankara, Turkey

Adrian Alidemaj

University for Business and Technology, Kosovo

DOI: https://doi.org/10.36941/ajis-2022-0041

Abstract

Magna Carta in 1215 and 1789 from the French Revolution in parallel to globalization of human rights all over the world to this day and the state based on the rule of law and forms of government have improved. Therefore, the importance of individual human rights has increased alongside the community rights. The Internet has emerged as a closed circuit in which the computer is connected to withstand up to 1960. The first day, this day of information systems that have manifested themselves in all areas of human existence and has been an integral part of human existence. Knowledge is one of the most important values of modern life. Every day, government agencies and private organizations collect, store, process and transfer significant amounts of data about individuals. This is a natural reflection of the situation has been in government. Protection of personal data is a right of individuals against unauthorized use of their data by other persons or organizations. Especially after 2002 indicate the presence of public institutions in Turkey as well as to offer their digital services to citizens in both. Personal Data related to the establishment of this right The Law on the Protection of the Conservation was passed by the Turkish Grand National Assembly on March 24, 2016. has been enacted. One of the most used services offered by the staff of public institutions and staff to their email. In our study, government extension and content of the person's own e-mail account does not belong to the state providing services it has been examined in the light of the Law on the Protection of Personal Data in Turkey and international regulations in this field.

Keywords: *e-mail, protection of personal data, e-government, encrypted communication*

1. Introduction

Since the first day of humanity, communication between people has been of great importance. For this reason, the communication that started with body movements in the first place, later turned into speech, which is voice communication. In parallel with the development of human relations, coexistence has emerged and communication between communities has shown itself as a type of communication. Communication, on the other hand, refers to the process in which knowledge, thoughts and attitudes are exchanged between individuals and groups through a system of common symbols (Kayıhan, 2001).

From the past to the present, people who are far from each other have been in communication with various means such as smoke, pigeons and messengers. Parallel to the diversification of communication tools, the protection of the confidentiality and security of the content of the communication has come to the fore, and for this reason, encrypted transfer of data between people using cryptological (cryptology, cipher science) methods has emerged. Today, communication in the digital environment is an indispensable part of life, and for this reason, people need to use it at any time of the day and everywhere, both at home and at work. However, it is faced with the problem of whether the data processed through informatics belongs to the institution or organization that provides this service or whether it is in the privacy of the person.

In the light of this information, firstly, definitions of basic concepts such as person and data will be made, and then the legal regulations regarding the protection, processing and transfer of personal data in Turkey will be examined in terms of personal e-mail accounts used in public institutions.

2. Concepts of Person, Data, Personal Data and Email

In order to fully determine the meaning of the concept of personal data, it is necessary to define the word meanings first. According to the Turkish Civil Code (TCC), persons are divided into two as real and legal persons. TCC m. According to 28, “personality begins the moment the child is fully born alive and ends with death.” legal entities are TCCm. In 47, “Communities of persons organized as a stand-alone entity and independent groups of goods dedicated to a certain purpose acquire legal personality pursuant to special provisions concerning themselves.” was stipulated. Accordingly, a person is defined as a "right subject who can have rights and obligations” (Öztan, 2010). The literal meaning of the word personal is “Pertaining to the person, pertaining to the person, belonging to the person” (Turkish language institution dictionary, 2021). Data is “The main element, which is the basis of a research, a discussion, a reasoning. In informatics, a formal and conventional representation of facts, concepts or commands suitable for communication, interpretation and operation. Availability is considered as conformity to communication, interpretation, or processing with persons or machine. In the Regulation on the Processing of Personal Data and Protection of Confidentiality in the Electronic Communications Sector, personal data is defined as "any information relating to an identified or identifiable natural person”.[1] In information processing technologies, information is “the meaning that a person directs to data by making use of the conventional rules used in the form. In the Law No. 5651 on Regulation of Publications Made on the Internet and Combating Crimes Committed through These Publications, it is defined as “the form of data that has gained meaning.”[2] In the Council of Europe Convention No. 108 on the Protection of Individuals Against the Automatic Processing of Personal Data, “Personal data means all information about an identified or identifiable

[1] *Regulation On Processing Personal Data and Protection of Privacy in The Electronic Communications Industry. [Online] Available: https://www.resmigazete.gov.tr/eskiler/2020/12/20201204-13.htm (September 25, 2021).*
[2] *Law On Regulation of Publications Made on The Internet and Fighting Crimes Committed through these Publications.*

natural person, relevant person."[3] In the Council of Europe Convention on Cybercrime, computer data means "any representation of facts, information or concepts suitable for processing in a computer system, including a program that enables the computer system to perform a function." (Council of Europe Convention on Cybercrime, 2001). In line with all this, personal data can be defined as all elements of an identifiable person, important or unimportant, but ready to be processed and have a certain meaning.

Before defining the concept of e-mail, it is necessary to look at the word meanings of these words. First of all, the literal meaning of the word mail is "all of the letters and relics that are sent to or from a place." Electronics is the branch of science that studies the phenomena caused by the action of free electrons" (Turkish language institution dictionary, 2021). In the regulation on the procedures and principles regarding the registered electronic mail system, electronic data is defined as "records produced, transported or stored electronically, optically or similarly or transferred to electronic, optical or similar media."[4] Based on these definitions, the concept of e-mail can be defined as data sent from one place to another in a certain time period by electronic, optical or similar means. As another definition, it can be defined as the written communication of at least identifiable persons via information networks over the internet.

3. Various Regulations on the Protection of Personal Data in Turkish Law

3.1 Constitution of The Republic of Turkey

In the 2nd article of the 1982 Constitution,[5] the concept of a "respect for human rights" state was mentioned, and the protection of human dignity was among the prohibited articles of the constitution. The protection of human dignity is of great importance in the unlawful collection, processing and recording of personal data. The reason for this is the illegal processing of this information on the person's personal information, without his/her free will. Because as a result of processing personal information, human dignity is violated by removing the personality profile consisting of habits, ideological, religious, political and philosophical parameters and making people a simple object by removing them from human values. For this reason, it occurs as a result of the violation of personal rights and even the violation of private life as a result of unlawful processing of all relations of individuals by violating their confidentiality.

The use of e-mail is a tool that covers both the privacy of private life and the freedom of communication. From this point of view, "Everyone has the right to demand the protection of personal data concerning himself/herself, which is brought under the heading "Privacy and Protection of Private Life" in the Rights and Duties of the Person section of the Constitution. This right; which includes many information about their activity, where they accessed, which kind of connection they used, deletions and all their movements that they used for some purposes.Using someone's else information can be only allowed and processed in cases which the other person agree on only in cases where the actions are regulated by law regarding procedures and principles.[6] It also includes being informed about the personal data about the person, accessing these data, requesting their correction or deletion and learning whether they are used for their purposes. Personal data can only be processed in cases stipulated by law or with the explicit consent of the person. The principles

[3] *Draft law on the Protection of Personal data.*
[4] *Regulation On Processing Personal Data and Protection of Privacy in The Electronic Communications Industry. [Online] Available: https://www.resmigazete.gov.tr/eskiler/2020/12/20201204-13.htm (September 25, 2021).*
[5] *Constitution of the Republic of Turkey. [Online] Available: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf (September 25, 2021).*
[6] *Constitution of the Republic of Turkey. [Online] Available: https://www.mevzuat.gov.tr/MevzuatMeti n/1.5.2709.pdf (September 25, 2021).*

and procedures regarding the protection of personal data are regulated by law. According to the regulation, everyone, whether a Turkish citizen or not, has the right to have their data protected, corrected and deleted. This right has not only been granted to Turkish citizens, and everyone will be able to benefit from this right as a constitutional guarantee. Both the privacy of private life and the freedom of communication have been regulated under the same heading, and it has been confirmed that personal data is the confidential area of private life and it has been shown that they are closely related. Because the basis of human rights is human dignity and privacy. One of the most important purposes of the protection of personal data, which is guaranteed by the Constitution, is the right of everyone who leads their life freely within the framework of the democratic social order, to the protection of their personal data. The aforementioned right ensures that the individual can determine his/her rights on his/her data freely in order to protect the individual against the damages caused by the personal data processing activities in democratic and modern societies. Because while people live a certain part of their lives with a limited environment, they do not want anyone to be in a certain area. In the secrecy of private life, the person lives in de facto isolation and distance from society and does not want to be disturbed by anyone. In this section, they want to stay away from public information and intervention. One of the two basic elements of private life is privacy and independence. Confidentiality is the part that should not be interfered with by third parties. Violation of privacy means interference with private life. On the other hand, private life also includes the right to identity. For this reason, the person's unique characteristics such as name, surname, religious belief, age, habits, political opinion cannot be processed, recorded or forced to disclose them without his explicit consent. This situation, which is described as one of the five core rights and cannot be intervened even in cases where a state of emergency is declared, and the constitution art. 15. The limitation or regulation of all these violations is only possible in the case of the limitation reasons listed in the relevant article of the constitution. For example, the article that the Constitution regulates the privacy of private life and the protection of personal data states: “Unless there is a duly given decision from the judge, depending on one threat or more reasons such as security on national bases, strict order that are given to public, pre-prohibition of crime, defending of general health and public morals or protection of the rights and freedoms of others; only in those cases where there is a written order for the authority authorized by law, in those cases delay is inconvenient due to these reasons; No one's clothes, personal papers and belongings can be searched or capture. The decision for the competent authority is submitted to the judge in charge to be approved within twenty-four hours. The judge should announce his decision within forty-eight hours from the capture; if not, the confiscation will be lifted of its own accord.”[7] Depending on the reasons, there are reasons related to private life but limited by law. As can be seen, although the protection of private life is not limited, it is open to intervention by the official authorities of the state in certain situations.

Article 8 of the European Convention on Human Rights states: “Everyone has the right to respect for his private and family life, his home and his correspondence. Any interference by a public authority with the exercise of this right is only necessary in a democratic society and provided that it is prescribed by law, in the interests of national security, public safety, the economic well-being of the country, the protection of peace and order, the prevention of crime, the protection of health or morals, or the rights and freedoms of others. it could be the subject." formatted. Freedom of communication in Article 22 of the 1982 constitution states: “Everyone has the freedom of communication. Confidentiality of communication is essential.” The reasons for limitation are defined as “Unless there is a judge's decision duly given due to one or more of the reasons such as national security, public order, prevention of crime, protection of general health and public morals or protection of the rights and freedoms of others; unless there is a written order of the authority authorized by law in cases where delay is inconvenient due to these reasons; communication cannot

[7] *Constitution of the Republic of Turkey. [Online] Available: https://www.mevzuat.gov.tr/Mev zuatMeti n/1.5.2 709.pdf (September 25, 2021).*

be blocked and its privacy cannot be touched. The decision of the competent authority is submitted to the approval of the judge in charge within twenty-four hours. The judge shall announce his decision within forty-eight hours; otherwise, the decision is automatically lifted. The public institutions and organizations to which the exceptions will be applied are specified in the law. It has been arranged in the form of limitation, showing the reasons for the limitation. Both the privacy of private life and the freedom of communication can only be limited by the limitations listed in the mentioned articles of the constitution.

3.2 Turkish Code of Obligations

The debts of the employer in the Service Contracts section of the Turkish Code of Obligations; wages, work tools and materials, expenses, protection of the worker's personality, punishment condition and release, vacation and leaves, service certificate and finally protection of the worker's personality. In a service contract, which should be understood from this order of the law, the protection of the personality and data of the worker is equally important as the wage is. The use of personal data is in the margin title: "The employer can use the personal data of the worker only to the extent that it is necessary for the employee's work inclination or for the performance of the service contract. Provisions of special laws are reserved" (Turkish law of Obligations, 2011). It is stated that the employee can only use the data that he has to use in the performance of the service contract in a measured manner.

3.3 Turkish Penal Code

Turkish penal code protects "private life" and "secret area of life". The personal information of the person is included in the private life and the secret area of life. In order to punish those who take actions against personal information through the Criminal Law, crimes against personal data have been established in the Turkish Penal Code No. 5237. In the ninth section of the second part of the Law titled "Crimes Against Persons", titled "Crimes Against Private Life and Confidential Area of Life", "recording of personal data" in Article 135, "unlawful giving or seizing data" in Article 136 and 138. In Article 137, the crimes of "not destroying the data" are regulated, and in Article 137, qualified cases that require an increase in punishment are listed.

In the section of Turkish Penal Code,[8] Special Provisions, Offenses Against Persons, Offenses Against Private Life and Confidential Area of Life, in Article 135, the heading of recording personal data is titled, "Anyone who records personal data unlawfully is sentenced to imprisonment from one year to three years. Political, philosophical or religious views of individuals, their racial origins; Any person who unlawfully records information about his moral tendencies, sexual life, health status or union connections as personal data shall be punished in accordance with the provision of the above paragraph." In Article 136, under the heading of illegally giving or seizing the data, it is stated that "A person who illegally gives, disseminates or captures personal data to another person is punished with imprisonment from two years to four years. The confidentiality of the legal value protected by crime, the private life of the person to whom the personal data is related, and with it; Since the right to protect personal data under the Constitution is accepted as a separate right within the privacy of private life, it should also be accepted that the legal value protected by crime is the right to protect personal data (Koca, Üzülmez, 2019). The crimes defined in the above articles; The penalty to be imposed is increased by half, in case it is committed by a public official and by abusing the authority given by his/her duty, by taking advantage of the convenience provided by a certain profession and art.

[8] *Turkish Criminal Law. [Online] Available: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf (September 25, 2021).*

To disseminate personal data is to ensure that personal data is learned by more than one person. (Korkmaz, 2017). However, it should be emphasized here that even in the case of dissemination, it is not necessary for everyone to learn the personal data in question in terms of the occurrence of the crime; Delivery of personal data even to only one person is sufficient for the crime to occur (Dülger, 2016). The act of dissemination can be done by publishing personal data on a website, sending it to groups of messaging applications on smartphones, sharing it as a status update on social media, sending an e-mail to multiple people (Epözdemir, 2019).

In Article 138, under the heading of not destroying the data, it is stated that "Those who are obliged to destroy the data within the system despite the expiry of the time limits set by the laws are sentenced to imprisonment from one year to two years if they do not fulfill their duties. In case the subject of the crime is data that needs to be eliminated or destroyed in accordance with the provisions of the Criminal Procedure Code, the penalty to be imposed is increased by one fold." It is regulated in the form of heavy freedom-binding provisions. In the margin title of violating the confidentiality of communication regulated in Article 132 of the Law, "Anyone who violates the confidentiality of communication between people is punished with imprisonment from one year to three years. If this privacy violation occurs by recording the contents of the communication, the penalty to be imposed is increased by one fold. Anyone who unlawfully discloses the contents of communication between people is punished with imprisonment from two to five years. A person who illegally discloses the contents of communications made with him without the consent of the other party, is punished with imprisonment from one year to three years. If these disclosed data are published through the press and broadcast, the same penalty will be imposed." formatted. It is clear that if these different penal norms are committed with a single act, the perpetrator will be punished with the most severe one, pursuant to the provisions of intellectual discussion in accordance with Article 44 of the Law. However, if the same crime is committed more than once against the same person at different times, the punishment will be increased by applying the provisions of the chain crime in accordance with the provisions of Article 43 of the law. In addition, in case of committing the same crime to more than one person with a single act, the provisions of the chain crime will be applied.

3.4 Criminal Procedure Code

Article 134 of the Criminal Procedure Code No. 5271 states: "In the investigation conducted for a crime, in the presence of strong grounds for suspicion based on concrete evidence and in the absence of the opportunity to obtain evidence in any other way, the request of the public prosecutor. Upon this, the judge decides to search the computer and computer programs and computer logs used by the suspect, to make copies from the computer records, to decipher these records and turn them into text." [9] In cases where there is strong suspicion based only on concrete evidence and there is no possibility of proof in any other way, and only with the decision of a judge, it is ruled that the person's computer, computer records and logs will be interfered and searched or seized. It is obvious that personal privacy is strictly protected. This protection is also valid for computers and computer logs of natural persons as well as computers, computer logs of legal entities, server and storage devices similar to computers.

3.5 Labor Law

It is of great importance to protect personal data, which is defined as all information relating to an identified or identifiable person, and which is a personal right, in business relations as well as in all

[9] *Law of Criminal Procedure. [Online] Available: https://www.mevzuat.gov.tr/mevzuat?Mevzuat No=5271&Mev zuatTu r=1&Mev zua tT ertip=5 (September 25, 2021).*

areas. As a matter of fact, there is a constant interaction throughout the business relationship between the personal data of the employee, who is both legally and economically dependent on the employer, and the employer's right to management, equal treatment obligation, protection and surveillance obligation. Since the unique characteristics of the employment relationship may lead to the unlawful processing of personal data regarding the employee by the employer, the employer must act in accordance with the basic principles of both national and international data protection law, especially the Directive of the Council of the European Union and European Parliament No. 95/46/EC. In this context, the employer cannot violate the employee's rights to access, correct and object to data, and is under the obligation to inform the employee before processing his personal data. Although the employer has the right to freely regulate the employee's use of electronic tools such as computer, internet and e-mail in the workplace, in accordance with the right of management, without harming his personal rights, there are some limits in the employer's supervision of the employee's said use. The principle of proportionality constitutes the basis of the employer's right to control. Therefore, the employer's audit may be carried out because he has legitimate interests in the business and these outweigh the protection of the employee's personal data. In addition, it is obligatory for the employer to inform the employee about the purpose, form and application before the audit, and the audit to be transparent and lawful and carried out in line with a specific purpose. All of these limits also apply to the monitoring and visual surveillance of the worker's communication. In this respect, it can file preventive and protective lawsuits stipulated in Articles 24 and 25 of the Turkish Civil Code, and demand material and moral compensation or the return of unlawful earnings by the employer (Uncular, 2014).

The employer has the authority to examine, in terms of the economic future of the workplace and the employer, the websites visited on the Internet and other electronic communication activities performed by the workers in line with the employment contract at the workplace, in terms of superior benefit. However, in reality, the employer is obliged to respect the private life and freedom of communication of the employee. It is unlawful for the employer to control the private correspondence of its workers and to monitor them at the workplace. However, the above-mentioned employer's economic future and the measures to be taken against possible theft in the workplace make the monitoring in question legal. The worker can only use the powers referred to in Article 25 of the Turkish Civil Code and Article 58/1 of the Code of Obligations against the worker employer, only in cases where there is no legal compliance (Özdemir, 2010).

In the decision of the 9th Civil Chamber of the Court of Cassation dated 19.06.2001 and numbered E. 2001/6100, K. 2001/10524; It is stated that "as the plaintiff claims, the employer's computer records were also used in determining whether there is any overtime receivable"[10] and the employer ruled that the employee could print out and even read the e-mails he wrote about the work. Here, the aim of the employer is to protect the business and to supervise the performance of the employee's business debt and business activities based on the right of management. From here, the employer can control the external link information of the e-mails related to the work done, the date of the e-mail, the time of sending, the volume of the information sent, and the cost of sending the e-mail and the address of the recipient. One of the most used tools for monitoring workers is checking e-mails (Özdemir, 2010).

If the employer considers that the e-mail is business-related, the registration and content control of the e-mail can be done by the employer. In a decision of the Supreme Court; It was determined by the employer that the plaintiff used the computer given to him to do his work at the workplace by accessing shopping and game sites on the Internet during working hours, and that he did not use his time and the computer in line with the act of doing business, and it was pointed out that there was no illegality in the termination of the employee's employment contract. However, in

[10] *Decision of the 9th Civil Chamber of the Supreme Court dated 19.06.2001 and numbered E. 2001/6100, K. 2001/10524. [Online] Available: http://www.kazanci.com.tr (September 25, 2021).*

cases where the employer has a clear instruction to use the computer, internet and e-mail connection at the workplace for business purposes only; All files and e-mails of the worker saved on the computer will be considered as work-related e-mails and communication texts, and in this case, the employer will have the right to see all e-mails and communication texts. However, even in this case, if it is understood from the e-mail address that this e-mail is a private e-mail, the rule that all e-mails are business-related will not apply, and e-mails that are considered private will not be able to be opened or read (Okur, 2006).

3.6 Personal Data Protection Law

The purpose of the law is regulated as the processing of personal data, the protection of the individual's immunity, material and moral existence and fundamental rights and freedoms, and the principles and procedures to be followed by real and legal persons who process personal data. In the justification of the law, it is stated that personal data registry systems are important for two groups.[11] The first of these is those who use personal data registers, and the other group is natural and legal persons for whom personal data is processed. It has been stated that the law was prepared in order to protect and balance the interests of these two groups and to secure personal rights and fundamental rights and freedoms. With this Law, the provisions that were scattered in the legislation were gathered together and put into effect.

In the relevant articles of the Law, "Personal data is processed by real persons within the scope of activities related to themselves or family members living in the same residence, provided that they are not given to third parties and that the obligations regarding data security are complied with. Processing personal data for art, history, literature or scientific purposes or within the scope of freedom of expression, providing that they don't violate national defense, national security, public security, public order, economic security, privacy of private life or personal rights or constitute a crime, also in another part when processing of personal data within the scope of preventive, protective and intelligence activities are carried out by public institutions and organizations authorized by law to ensure national defense, national security, public security, public order or economic security. Processing personal data by judicial authorities or execution authorities in relation to investigation, trial or execution proceedings, also in the cases when situation comes If personal data processing is necessary for the prevention of crime or for criminal investigation, personal data processing is authorized by an authorized public institution based on the authority given by the law. It is necessary for the execution of supervisory or regulatory duties and for disciplinary investigation or prosecution by professional organizations in the nature of public institutions and organizations, Personal data processing is necessary for the protection of the economic and financial interests of the State with regard to budget, tax and financial matters. An exception has been made in the form of regulation, and it has been stipulated that personal data can be processed and transferred due to activities.

It is also regulated in the law that if personal data is processed unlawfully, penal sanctions will be applied in accordance with Articles 135, 136, 137 and 138 of the Turkish Penal Code. the attacked person will be able to seek protection against the attackers. In addition, in the law, the Personal Data Protection Board will decide on the complaints of those whose personal rights are violated due to the processing of personal data by public institutions or organizations or real and private law legal entities, and the right of compensation of the individual whose personal rights are violated is reserved.

---

[11] *Personal Data Protection Law. [Online] Available: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=6698&MevzuatTur=1& Mevzuat Tertip=5 (September 25, 2021).*

3.6.1 Lawful Situations according to The Personal Data Protection Law

It has been regulated that personal data can only be processed with the explicit consent of the person concerned and, except for fulfilling the obligations stipulated in the Laws, the data cannot be processed if the person concerned makes an objection. Also;

- Processing data for the purpose of fulfilling an official duty or public interest due to an obligation stipulated by the law,
- Processing of personal data in order to protect the life or physical integrity of himself or someone else, in case the data subject is unable to express his consent,
- Processing the personal data of the parties to the contract, provided that it is directly related to the establishment and performance of a contract,
- Processing of publicly known personal data due to the fact that it has been disclosed by the relevant persons or there is information available in open registries,

Data processing is mandatory for the data owner's own legitimate interests, as long as it does not harm the fundamental rights and freedoms and legitimate interests of the data owner.

It is accepted that there are reasons for compliance with the law in such cases. In the continuation article, it is stated that personal data related to race, political opinion, philosophical belief, religion, sect or other beliefs, membership of associations, foundations and unions, health and private lives and all kinds of convictions cannot be processed, and that personal data other than those listed in the aforementioned article, private life and in the following cases, provided that adequate measures are taken to ensure the protection of the confidentiality of family life;

a) Obtaining the written consent of the person in cases not prohibited by law,
b) Data processing is obligatory for the maintenance of the life or physical integrity of a person or another person who is unable to express his consent for legal or actual reasons,
c) Data processing is obligatory in order for the data logger owner to use the rights and powers granted by this Law or other laws or to fulfill his obligations, provided that adequate protection is provided to the data subject,
d) Data processing by foundations, associations, trade unions and political parties for their members and members, provided that they are in accordance with their establishment purposes and the legislation they are subject to, and limited to their fields of activity, provided that it is not disclosed to third parties without the consent of the person concerned,
e) It is about the data that has been publicly disclosed by the person concerned,
f) Data processing is mandatory for the establishment, use or protection of a legal right,
g) Personal data for the purpose of performing preventive medicine, medical diagnosis, treatment, care or health services;
    - Health institutions,
    - Insurance companies,
    - Social security institutions,
    - Employers responsible for establishing a workplace health unit,
    - Health-related schools and universities,

It has been stipulated that it may be processed under the supervision of health personnel who are under the obligation to keep secrets in accordance with the relevant laws, legally or according to the professional rules, or another person who is under the obligation of keeping confidentiality at an equivalent level.

Provided that the privacy of private and family life is not touched, and in cases where basic public interests require it, provided that there are adequate protection measures in the relevant legislation, the Personal Data Protection Board may decide to process personal data of a special nature.

Personal data of special nature regarding the investigation of the crime, protection and control

measures and criminal convictions can be processed under the control of the competent authorities, provided that there are adequate protection measures in the relevant laws, but the registry regarding criminal convictions can only be kept under the control of the Ministry of Justice. Data on administrative sanctions and court decisions in the field of private law can also be processed under the control of official authorities.

As can be seen, when processing confidential information and data belonging to individuals, the explicit consent of the person concerned is required. However, in case of an obligation of the person concerned in clause c, personal data may be processed. For example, the person needs to be operated on urgently, but he is unconscious and cannot reach any of his relatives, or even if it is reached, chronic information about the patient cannot be reached. In this case, the patient's personal data may be processed, with the assumption that the patient is unconscious and his consent cannot be obtained. In subparagraph d of the article, foundations and associations, which are indispensable parts of democracy, can only process data without the consent of their members, but without sharing them with third parties, in order to achieve their own purposes.

3.7 Civil Servants Law No. 657

In the duties and responsibilities section of the Civil Servants Law No. 657, the general lines of loyalty, impartiality and loyalty to the state, behavior, cooperation, as well as duties and responsibilities of civil servants are arranged under side headings (Turkish State Officials Law, 1965). In the section of loyalty, civil servants are obliged to start their duty by signing an oath, stating that they will faithfully abide by the Constitution and laws of the Republic of Turkey and will faithfully implement the laws of the Republic of Turkey in the service of the nation. Duties and responsibilities are laws, regulations, regulations, etc. They are held responsible to their superiors for the good and correct execution of their duties by being obliged to comply with the principles specified in the regulatory procedures and to fulfill the duties assigned by their superiors. As it can be seen, civil servants, like everyone else, cannot act against the constitution, law and other regulatory procedures while carrying out their duties. Parallel to this, if the officer deems the order received from his superior to be contrary to the provisions of the Constitution, law, statute and regulation, he does not fulfill it and informs the person who gave that order. If the chief insists on his order and renews it in writing, the officer is obliged to do this order. However, arising from the execution of the order is the responsibility of giving the order. An order, the subject of which constitutes a crime, is not carried out under any circumstances; The person who executes the order cannot escape responsibility and both the officer who carries out the order and the supervisor who gives the order are responsible. Civil servants are obliged to take the necessary measures to fulfill their duties with care and diligence, to protect the State property delivered to them and to keep them ready for service at any time. If the administration has suffered damage as a result of the will, fault, negligence or negligence of the civil servant, this damage must be paid by the relevant official at the current market price. Individuals file a lawsuit against the relevant institution, not against the personnel performing these duties, due to the damages they have incurred in relation to duties subject to public law. The corporation reserves the right of recourse to the responsible person according to general provisions. In addition, 28/4 of the Administrative Procedure Law No. 2577. The article stipulates that a lawsuit for compensation can be filed against a public official who deliberately fails to fulfill the administrative court decision.
Today, state institutions and organizations also provide services to both their own employees and citizens in electronic environment. The most well-known of these applications is turkiye.gov.tr, which is known as the electronic state gate. Public institutions and organizations have gathered the services they offer to the citizens under one roof, and either litigation or military service status certificate can be obtained. However, another service of public institutions is the electronic services they offer to their personnel. Internet and e-mail services are at the forefront of these. Public employees use internet and postal services in order to be faster and more effective in their work and actions.

In accordance with the Law No. 5651 on Regulating Broadcasts Made on the Internet and Combating Crimes Committed Through These Broadcasts[12], collective use provider: as providing the opportunity to use the Internet in a certain place and for a certain period of time; content provider: natural or legal persons who produce, change and provide any information or data presented to users over the Internet; hosting provider: defined as real or legal persons that provide or operate systems hosting services and content, and public institutions, including this definition, record the internal IP distribution logs in their own systems and the value that confirms the accuracy, integrity and confidentiality of this information. and keep these data for at least one and at most two years. Based on the aforementioned definitions, public institutions that provide both internet and e-mail services with the gov.tr extension to their users can be defined as a mass usage provider due to the mass internet service they offer, and as a content and location provider due to the e-mail service they provide. What is meant by internal IP distribution logs is to record the information showing the IP address information distributed in the organization's own internal networks, the start and end date and time of use, and the unique network device number (MAC address) and user names of the computers using these IP addresses. The purpose of this is to fight against crime and criminals, and to determine from which addresses the attack came from both the inside and the outside in the electronic environment after the crime has been committed. In line with these records, what happened at which MAC address, on which day and at what time is obtained retrospectively, and these time-stamped records have the quality of evidence. At this point, another parameter, the privacy of private life and communication, and the protection of personal data come into play.

4. Conclusion

At the last point, it is clear that public personnel working in public institutions are subject to the provisions regulated by Law No. 657 in terms of public law. In this respect, there is no concept of employee and employer as in private law. Depending on the developing technology, there are various information services in public institutions. However, in accordance with the law numbered 5651, it is a legal obligation to record the traffic data of everyone working in the institution and also the logs of the e-mail service provider for certain periods. In private law business relations, the e-mail account given by the employer can be used by the employee in his private works in line with the express and implied consent of the employer, and the mails that are not related to the business should not be examined in terms of content. On the other hand, there is no harm in not examining business-related e-mails. However, the employer may explicitly prohibit the mentioned e-mail account from being used for private works. In this case, it would be more appropriate for the worker to obtain and use another e-mail account that he will use in his private work. This right of the employer, as the owner of the work tools in the workplace, comes from the right to determine whether the tools in the workplace will be used for special purposes or not, based on the right of ownership and management. However, there is no such situation for employees subject to public law. In this respect, the State may impose certain restrictions on its employees through regulatory procedures such as regulations, circulars and directives of the Public Legal Entity or Public Legal Entity. For example, in the 14th article of the Information Security Policies Directive of the Ministry of Interior dated 09/09/2013, under the information systems general usage policy side heading, “Although the Ministry's security systems provide a reasonable level of privacy to individuals, all data created within the Ministry is the property of the Ministry. Users should not use information systems for personal purposes. The institution has the right to periodically audit networks and systems within the framework of this policy.” It explicitly prohibits the use of the e-mail service provided by the institution to its personnel

[12] *Internet Ortaminda Yapilan Yayinlarin Düzenlenmesi Ve Bu Yayinlar Yoluyla Işlenen Suçlarla Mücadele Edilmesi Hakkinda Kanun. [Online] Available: https://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm (Date of access 25/09/2021).*

in their own private business. Parallel to this, in the 5th article of the same directive; "E-mail should not be used for personal purposes. Corporate e-mails can be audited by authorized persons without prior notice were deemed legally necessary."[13] It has been regulated as a legal basis that e-mails can be audited by authorized persons. Here, similar to the private law business relations, it is observed that the use of e-mail in private affairs of the person is clearly prohibited and the content is controlled. In the same way, the same situation exists in the Information Security Policies Directive of the Ministry of Health. According to article 2.19 of the directive; The e-mail account allocated to individuals by the Ministry/Institution is only used for business-related corporate activities. Staff are personally responsible for all e-mails sent using their own account."[14] And according to the 9th paragraph of Article 5; regarding those who do not comply with the Information Security policies and the obligation to keep secrets, it is regulated that action is taken in accordance with the relevant provisions of the Civil Servants Law No. 657 or the employment contract and the relevant provisions of the Law on the Protection of Personal Data No. 6698, and employees are expressly prohibited from using their corporate e-mails in their private business. A similar situation exists in the Ministry of Transport and Infrastructure. according to this; In the 5th and 7th articles of the Information Security Policy Directive dated 06/02/2019 and numbered 10472, Users should not use information systems for personal purposes. Relevant policies should be taken into account in this regard. Email should not be used for personal purposes. Corporate e-mails can be audited by authorized persons without prior notice were deemed legally necessary.[15]

As can be seen, bans have been imposed on the public personnel of the Republic of Turkey regarding the use of e-mail in different ways than in private law business relations, but in the same direction. From this point of view, it would be correct for the prohibited public personnel to have a different e-mail account from the institution e-mail account in their private relations. In this way, he will both use his e-mail account in his own private business and prevent it from being audited as content.

First of all, public personnel's use of the vehicles allocated to them for their own personal needs, other than their intended use, means a loss of production and efficiency for the institution. In the disciplinary part of the Law No. 657, the penalty of reprimand is "To act faulty in the full and timely execution of the given orders and duties, in the fulfillment of the procedures and principles determined by the institutions at the place of duty, in the protection, use and maintenance of official documents, tools and equipment related to the duty." and "Using official tools, equipment and similar items belonging to the state in private affairs." was regulated and punished.

On the one hand, internet traffic data belonging to individuals should be kept within the scope of the fight against crime and criminals, on the other hand, there is information that is tightly connected to individuals and contains the privacy of private life. An absolute balance must be established between these two parameters. For this reason, although public institutions and organizations forbid the e-mail service they offer to their personnel, in case they use it in their private business, in accordance with Article 134 of the Criminal Procedure Law No. 5271; It should not be subject to investigation only within the scope of investigation and prosecution for a crime by a judge's decision and only for the relevant crime. In addition, it will not be possible to violate the personal data of the personnel by searching the belongings of the personnel in the workplace and in

[13] *Ministry of Interior, Information Security Policies Directive. [Online] Available: http://www.canakkalebilgiislem.gov.tr/ortak_icerik/canakkalebilgiislem/kanun-yonetmelik/icisleri-bakanligi-bilgi-guvenligi-politikalari-yonergesi.pdf (September 25, 2021).*

[14] *Information Security Policies Directive of the Ministry of Health. [Online] Available: https://agriism.saglik.gov.tr/Eklenti/123592/0/kilavuz-21-onay-16072019pdf.pdf (September 25, 2021).*

[15] *Ministry of Transport and Infrastructure, Information Security Policies Directive. [Online] Available: https://www.uab.go v.tr/uploads/pages/mevzuat/bilgi-guvenligi-politikalari.pdf (September 25, 2021).*

places such as rooms, drawers and cabinets owned by the public institution by the personnel of another authorized institution.

References

Constitution of the Republic Of Turkey. [Online] Available: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf. (September 25, 2021).

Council of Europe Convention on Cybercrime. [Online] Available: http://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf. (September 25, 2021).

Decision of the 9th Civil Chamber of the Supreme Court dated 19.06.2001 and numbered E. 2001/6100, K. 2001/10524. [Online] Available: http://www.kazanci.com.tr (September 25, 2021).

Draft law on the protection of personal data. [Online] Available: (September 25, 2021). http://www 2.tbm m.gov.tr/d24/ 1/1-0966.pdf. (September 25, 2021).

Dülger, M. V. (2016). Protection of Personal Data with Criminal Norms in the Context of the Law on the Protection of Personal Data and the Turkish Penal Code. *Journal of Istanbul Medipol University Faculty of Law, 3 (2)*.

Epözdemir, R. (2019). Crime of Unlawfully Giving or Capturing Data (Article 136 of the TCK). *Terazi Hukuk Dergisi, Vol: 14, No: 151.*

Information Security Policies Directive of the Ministry of Health. [Online] Available: https://agriism.saglik.gov.tr/ Eklenti/123592/0/kilavuz-21-onay-16072019pdf.pdf (September 25, 2021).

Information Security Policies Directive of the Ministry of Health. [Online] Available: https://dosyamerkez.saglik.gov.tr/Eklenti/15584,bilgi-guvenligi-politikalari-yonergesi20180 502pd f.pdf?0. (September 25, 2021).

Kayıhan, I. (2001). Mass Communication Law, 5. Bası, İstanbul.

Koca, M. Üzülmez, İ. (2019). Crime of Recording Personal Data (TCK art. 135). *D.E.Ü. Journal of the Faculty of Law, Prof. Dr. Gift to Durmuş TEZCAN, C.21.*

Korkmaz, I. (2017). Protection of Personal Data under Criminal Law. Seçkin Publishing, Ankara.

Law on Regulation of Publications maade on the Internet and Fighting Crimes Committed through these Publications. [Online] Available: https://www.resmigazete.gov.tr/es kiler/2007/05/20070523-1.htm. (September 25, 2021).

Ministry of Interior, Information Security Policies Directive. [Online] Available: http://www .mer sin .gov.tr/kurumlar /mersin.gov.tr/KYS/BI M/Bilgi_Guvenligi_Politikasi_Yonergesi.pdf. (September 25, 2021).

Ministry of Transport and Infrastructure, Information Security Policies Directive. [Online] Available: https://www.u ab.go v.tr/ uploads/pages/mevzuat/bilgi-guvenligi-politikalari.pdf (September 25, 2021).

Okur, Z. (2006). New Technology and Labor Law. *Cement Employer Magazine.*

Özdemir, H. (2010). Monitoring of Workers in the Workplace and Protection of Personal Rights of Workers. *Journal of Erzincan University Faculty of Law*, C. XIV, S. 1–2.

Öztan, B. (2010). Basic Concepts of Civil Law, 33 rd edition, Ankara.

Regulation On Procedures and Principles Regarding Registered Electronic Mail System. [Online] Available: https://www.resmigazete.gov.tr/eskiler/2011/08/20110825-7.htm. (September 25, 2021).

Regulation on Processing Personal Data and Protection of Privacy in the Electronic Communications Industry. [Online] Available: https://www.resmigazete.gov.tr/eskiler/2 020/1 2/20 201204-13.htm. (September 25, 2021).

Turkish Criminal Law. [Online] Available: https://www.mevzuat.gov.tr/Mevzu atMetin/1.5.5 237.pdf. (September 25, 2021).

Turkish language institution dictionary. [Online] Available: https://sozluk.gov.tr/ (September 25, 2021).

Turkish Law of Criminal Prodecure. [Online] Available: https://www.mevzuat .gov.tr/mevzuat?MevzuatNo=5271&MevzuatTur=1&MevzuatTertip=5. (September 25, 2021).

Turkish Law Of Obligations. [Online] Available: https://www.mev zuat.gov. tr/MevzuatMetin/1.5.6098.pdf. (September 25, 2021).

Turkish State Officials Law. [Online] Available: https://www.mevzuat.gov.tr/Mev zuatMetin/1.5.657.pdf. (September 25, 2021).

Uncular, S. (2014). Protection of Personal Data of the Worker in the Business Relationship, 1st Edition, Ankara.