DOI: 10.20472/IAC.2015.016.024

MEHMET ONURSAL CIN
Selcuk University, Faculty of Law, Turkey

WIRETAPPING AS A SECRET INVESTIGATION MEASURE IN TURKISH CRIMINAL JURISDICTION LAW

Abstract:

Organized Crimes are increasing all over the world. Besides, communication technologies evolving rapidly. And criminal organizations benefit from this case. Local Investigation authorities who have to struggle with organized crime are also required to take advantage of this technological development. During a criminal investigation, wiretapping is a very important method of obtaining evidence. This measure is the most effective one in the other secret investigation measures and it also violates freedom of communication and private life, which are under guarantee of Turkish Constitution. Because of that the legal formulation and implementation should be performed very carefully.

The aim of this article is to discuss the legal and social dimensions of wiretapping system in Turkish Criminal Procedure. Although it is similar to the German System, due to political, social and demographic conditions, some major changes have been made.

According to Turkish Constitution Art.22 which entitled Freedom of communication; everyone has freedom of communication. This freedom and its confidentiality can only be limited because of national security, public order, prevention of crime, protection of the general public health and ethic rules or the protection of the rights and freedoms of others. In order to limit these freedoms, an authorized judge should make a decision that depends counted reasons by Art.22. Also The European Convention on human rights (ECHR) Art.8 regulates that all people have right to be respected their private and family life, for his home and correspondence. As a Law State no one have permit to violate the Constitution and ECHR. It is a serious crime to wiretap or to use a machine to capture the communications of others without court approval, unless one of the parties has given his prior consent.

In recent years, due to the implementation of the unlawful wiretapping in Turkey, we can say that Turkish Criminal Jurisdiction System experienced many sensational cases and scandals. Many official institutions have authority to wiretap in our law system. (Police, Army, Intelligence Agency) But the real problem is illegal eavesdropping. The government must struggle to these malicious people who eavesdrop to citizens by wiretapping devices that can be easily purchased over the Internet. Because this type of listening, has been put majority of our people into “someone’s eavesdropping me" paranoia.

In this context, the study aims to investigate the way of using wiretapping and its shortcomings in the process of criminal investigation of Turkish criminal system.

Keywords:

wiretapping, eavesdropping, criminal jurisdiction law

JEL Classification: K14

Introduction

Communication, which can be defined as the sharing of feelings, thoughts, and information through all possible means or the individual establishing relationships with other individuals or with society or the process of learning or spreading news, thoughts, and opinions, is the most fundamental element of the freedom of communication which is protected by international conventions and constitutions. Along with that, it may from time to time become necessary to restrict these rights in order to ensure security of both the individual and society. As result, surveillance of communications has been introduced to law, as carried out in the form of wiretapping, recording of the individuals' phone calls, and location through assessment of signal data between devices.

It is undisputable fact that mankind has achieved major improvements in fundamental rights and freedoms throughout the 20th century. Whereas the 21st century was expected to bring along further improvement of freedoms through the impact of technologic developments, quite the contrary happened in consequence of the terrorist attacks that occurred in the USA on September 11, 2001. In the years thereafter, the issue of restricting the human rights entwined in the paradox of freedom versus security has always evolved contrary to individual liberties, which is attributable mainly to concerns such as terrorism, internal security, espionage, organized crime etc. all threatening the sovereignty of the state.

Surveillance of communications, which imposes restriction on the most important ones of these liberties, is a very effective method of obtaining evidence. Even though it is described as a measure of secret investigation in terms of procedural law, it is a classical measure of protection with regard to the purposes and properties it has. It is necessary that both its legal formulation and implementation is actualized studiously, because it has the characteristic to violate crucial concepts including communication freedom and protection of private life which is guaranteed by the Constitutions of many countries.

The European Court of Human Rights does give states the chance to use this method in their fight against terrorism and organized crime. On grounds of past experience, the Court is in the opinion that wiretapping through diverse communication techniques is an effective solution in the public authorities' fight against modern forms of crime.

In light of these developments, surveillance of communication between persons was introduced to the Turkish Code of Criminal Procedure by way of a new enactment in 2005. Although in this respect, Article 135 of the Turkish Code of Criminal Procedure (CMK) does have the title "detection, wiretapping and recording of communication", the section where said article is inserted has the title "surveillance of communication made through telecommunication". Hence, the term of surveillance is considered to be inclusive of detection, wiretapping, and recording of communication made through telecommunication as well as signal data assessment and mobile phone location, although the latter two are not included in the heading of the relevant article. In this article, we have planned to scrutinize some problematic aspects based on legal regulations in Turkey.

1. The term “Surveillance of Communications”

1.1 Definition

New opportunities, brought along by fast development in both science and technology, have caused far-reaching changes in every sphere of life. New concepts, new results, new criminal emerging as result of these changes have made it mandatory to make certain regulations in criminal law and criminal procedure law. As part of secret investigation measures, surveillance of communication is a regulation which has been introduced for that purpose, and is applied with the aim to reveal the truth. But because this measure does by its own nature violate certain fundamental rights and liberties, it must be implemented according to rules which are defined with strict lines and preclude any intervention or interpretation of arbitrary nature. Moreover, because the measure is implemented secretly as a requirement of it and the suspect or accused is informed late about the situation or not informed at all, legal supervision is not possible and this situation may lead to violation of rights (Yavuz, 2005, p.2).

Nowadays, all states have legal regulations in the criminal procedure law which gives the investigation and prosecution bodies the chance to surveil communication made through telecommunication. In Turkish law, there was no such legal regulation until 10 years ago, although it was well-known that this measure intervened with fundamental rights and liberties and therefore must have well-grounded legal basis, even back in those days (Zafer, 1999, p.283). In Turkish law, the measure in question obtained legal regulation the first time with the enactment of the “Prevention of Benefit-Oriented Criminal Organizations Law” in 1999. In said law, surveillance of communication was formulated as “wiretapping and detection of communication”. Besides in doctrine, the terms “secret wiretapping of phone calls as protective measure”, “wiretapping of communication means”, “surveillance of communication”, “surveillance of communication made through telecommunication”, “eavesdropping”, and “wiretapping” had also been in use for long (Özbek, 2006, p.419).

The Code of Criminal Procedure (CMK), enacted on 01 June 2005, introduced new regulations about this issue and replaced the Prevention of Benefit-Oriented Criminal Organizations Law. Along with that, certain regulations were also introduced for the prevention of crime. The legal regulations use the term “surveillance of communication made through telecommunication” for such type of measures.

1.2 Legal Character

There is the need for certain measures in order to prevent crime in society or to obtain evidence and reveal the perpetrators whenever a crime is committed. Some of these measures are preventive measures which serve for the purpose of preventing crime or threat. Others are protective measures which serve for the purpose of investigating the suspected motives and obtaining of evidence after a crime is committed (Gümüşay, 2009, p.10). These measures can come into agenda in the framework of both the prevention authority of police prior to crime and judicial authority after crime. The general characteristic of these measures that they are measures of the last resort which

are temporary, proportional, and written in law (Döner, 2012, p.3). Legal remedies, which facility the acts and actions of criminal justice, give the chance to prevent alterations that would prevent the reveal of truth during prosecution, and require intervention to constitutional rights and liberties in order to make sure that judgments delivered at the end of prosecution do not remain inconclusive and litigation costs are paid, are called protective measures in Turkish law (Şahin, 2004, p.25).

Surveillance of communication made through telecommunication is a protective measure that is taken both to prevent commitment of crime and fight against already committed crimes. This measure is applied in two different ways, namely prevention of crime and obtaining evidence about the suspect of a crime. Surveillance of communication for evidence gathering purposes is carried out according to the norms laid down in the Code of Criminal Procedure (CMK), whereas surveillance of communication for the purpose of preventing crime is principally carried out according to the Law on Police Assignment and Authority Code (PVSK). In Turkish Law, surveillance of communication made through telecommunication is also used within the scope of intelligence activities carried out to protect national security, along with the purposes described in this article.

1.3. Legal Regulations

1.3.1. Turkish Constitution

General principles applicable to the restriction of rights and liberties are laid down in Article 13 of the Constitution of 1982. Accordingly, general reasons of restriction accepted for all rights and liberties are removed and replaced by restrictions intended only for a specific right or liberty, while acknowledging the rule that fundamental rights and liberties can be restricted by law only. The principle adopted is that when restricting any right or liberty, the essence of that right or liberty must remain untouched, ruling out any restrictions which would make impossible the exercise of fundamental rights and liberties. Finally, the “principle of proportionality” is introduced to the issue of restriction. In this framework, the proportionality principle means referral to favorable, required and proportional tools to reach the pursued purpose in the intervention of fundamental rights and freedoms(Taşkın, 2003, p.336). Second section of the Turkish Constitution includes regulations about the right and protection of privacy. Article 20 regulates the “right and protection of privacy”, Article 21 regulates the “immunity of domicile”, and Article 22 regulates the “freedom of communication”. In all of these articles, it is emphasized that, above all, the freedom of communication is basic principle, followed by conditions of restricting this freedom. Lastly, it is regulated that different authority can be given to certain public institutions and agencies with regard to restricting the freedom of communication, and that this power must be identified by law.

Article 22 of the Turkish Constitution provides that everyone has the freedom of communication, that privacy of communication is fundamental, and that unless there exists a decision duly given by a judge on one or several of the grounds of national security, public order, prevention of crime, protection of public health and public morals, or protection of the rights and freedoms of others, or unless there exists a written order

of an public prosecutor in cases where delay is prejudicial, again on the above-mentioned grounds, communication shall not be impeded nor its privacy be violated. The decision of the public prosecutor shall be submitted for the approval of the judge having jurisdiction within twenty-four hours. The judge shall announce his verdict within forty-eight hours from the time of seizure; otherwise, seizure shall be automatically lifted. In contrast, the former Turkish Constitution of 1961 did not give any such authorithy to the public prosecutor, and the freedom of communication could be restricted only by a decision duly given by a judge.

1.3.2. Prevention of Benefit-Oriented Criminal Organizations Law

As is written hereinabove, the first explicit regulation with regard to surveillance of communication was made for the first time in the Prevention of Benefit-Oriented Criminal Organizations Law (ÇASÖMK). Before that, the Turkish system lacked any law which would give authority for the direct and explicit wiretapping of communications for preventive purposes (Ünver-Hakeri, 2006, p.188). Provisions about search and seizure until the enactment of the Prevention of Benefit-Oriented Criminal Organizations Law used to be implemented through comparison in order to surveil communication made through telecommunication (Kunter-Yenisey-Nuhoglu, 2008, p.697). It can be said that the regulations laid down in the Prevention of Benefit-Oriented Criminal Organizations Law were close to the principles emphasized under Article 8 of the European Convention on Human Rights (Altıparmak, 2014, p.41).

Article 2 of the Prevention of Benefit-Oriented Criminal Organizations Law regulated that communications of people suspected of commission of or participation in the crimes under that Law or aiding and abetting authors of such crimes after commission of the crime can be tapped. The aim was to obtain evidence about such people. However, it did not take long until the aim of obtaining evidence on ground of that Law was expanded to include also wiretapping of communications to prevent the commitment of crimes. But the decision to do wiretapping for preventive purposes on grounds of these provisions meant a very broad interpretation of law, and as result, this practice was abandoned soon. According to provisions of the Prevention of Benefit-Oriented Criminal Organizations Law, surveillance of communication could be applied only to those people who were suspected of a certain number of crimes. In addition, this measure could also be taken against people suspected of commission of or participation in the crimes under that Law or aiding and abetting authors of such crimes after commission of the crime (Şahin Cumhur, 2006, p.86-87).

1.4. Relationship between Surveillance of Communication and Fundamental Rights and Liberties

1.4.1. The Right of Privacy

In Turkish Law, right of privacy can be analyzed under four interrelated titles. In this respect, the four titles can be defined as follows: “territorial privacy” which includes issues such as the immunity of an individual’s apparels, private papers, and belongings as well as the immunity of domicile, “privacy of communication” which includes the individual’s letters, phone calls, e-mails, and other means of communication, “privacy of physical integrity” which includes interventions to physical integrity such as genetic tests, drug tests etc., and “data privacy” which includes the gathering, use, and general processing of data (Ketzimen, 2008, p.192).

According to the European Court of Human Rights, private life is a very broad concept which cannot be defined with all of its aspects. The concept is clearly wider than the right to privacy, however, and it concerns a sphere within which everyone can freely pursue the development and fulfilment of his personality (Kilkelly, 2012, p.8). The private sphere of life is a distinctive sphere which includes the elements of confidentiality and independency, and in which the individual has the right to be left calm and alone (Gümüşay, 2009, p.20). As an element necessitated by private life, independency can be described as the right to choose one’s own style and type of life, behaviours, personal actions, and relationships in the broadest sense possible. Confidentiality is an environment of existence which is kept outside the curiosity sphere of third parties, and can be defined as privacy against external interventions to the personal, relational, and familial spheres of life of each and every individual (Kaboglu, 2002, p.292).

Regulations for the protection of private life are enacted in both national and international texts. In these regulations, everybody has the fundamental right to create a small world in which the individual can freely do whatever the individual wants, without interference by other people.

1.4.2. Freedom and Confidentiality of Communication

We already mentioned that in the “Rights and Duties of the Individual” Chapter of the Turkish Constitution, the principles of respect for private and family life, inviolability of the domicile, freedom and privacy of communication are regulated and protected. Freedom and privacy of communication is considered within the scope of the right to privacy on one hand, and as an independent fundamental right on the other (Şen, 1999, p.724). The concept of “freedom of communication”, as can be seen in Article 22 of the Turkish Constitution, does actually mean “privacy of communication” and “inviolability of mails”. Liberties regarding mass communications made through newspapers, televisions, radios etc. have no direct relation to liberties which are associated with private communication such as letters, telegraph, telephone, and alike. Since the term “communication” is used in the Turkish Constitution, all sorts of non-public personal communication made through diverse means such as letters, telephone, facsimile, telegraph, pagers, e-mail, and computer are taken under protection (Şen, 2007, p.4).

Freedom of communication, as one of the rights falling within the scope of right to privacy, can be defined as the people being able to communicate their thoughts and feelings through means of communication (telephone, radio, fax, letter, internet etc.) without having to concern about their communications be found out or recorded by third parties (Tüysüz, 2010, p.83). In Turkish Law, it is accepted that communication established through aforementioned means of communication is confidential, while the freedom of communication and right to privacy acknowledged as a fundamental right protect the individual against attacks by both the state or private individuals (Sözüer, 2009, p.71). Privacy of communication must be understood as both the fact that communication is established between individuals and a sharing of information or data takes places, and that the contents thereof are confidential (Kaymaz, 2013, p.87).

The right to respect for one's communication is a right to uninterrupted and uncensored communications with others (Kilkelly, 2012, p.19). One of the most serious and widespread intervention to the right to respect for one's correspondence is the surveillance of communication. Wiretapping term as a prevention precaution in the administrative law framework and also as a protection precaution in the framework of law of criminal procedure is a frequently encountered situation in national laws (İnceoglu, 2013, p.231).

Article 8 of the European Convention on Human Rights does secure the right to respect for one's correspondence. Means of communication such as mail, phone, fax, and personal internet are means where the right to respect for one's correspondence is exercised. Phone calls made from private or business premises are considered as communication in the sense of Article 8(1) of the Convention. According to the Court, Article 8 of the Convention does acknowledge everybody's right to respect for one's correspondence, and protect the confidentiality of private communications, regardless of whatever the content and form thereof might be. This means that what is protected by Article 8 of the Convention is the confidentiality of all words which individuals might use when they communicate (Dogru-Nalbant, 2013, p.10).

2. Surveillance of Communication in the framework of Code of Criminal Procedure (CMK)

2.1. Legal regulation

Within the scope of the Criminal Law Reform made in Turkey approximately ten years ago, significant alterations were made also to the Code of Criminal Procedure, with several new procedural law institutions being added into the law. For sure, surveillance of communication made through telecommunication has been one of the most important innovations. Articles 135 to 138 of the Code include detailed regulations about the issue. Accordingly: "The court or, in cases of peril in delay, the public prosecutor, may decide to locate, wiretap or record the communication through telecommunication or to evaluate the information about the signals of the suspect or the accused, if during an investigation or jurisdiction conducted in relation to a crime there are strong grounds of suspicion indicating that the crime has been committed and there is no other possibility to obtain evidence." The public prosecutor shall submit his decision immediately to the

court for his approval and the court shall make a decision within 24 hours. In case of expiration or if the court decides on the contrary, the measure is revoked by the Republic Prosecutor immediately. Measures to be taken pursuant to this article are decided unanimously by the high criminal court. Unanimity must also be sought when deciding on this measure upon objection.

When filing a request, a certificate or report showing the owner and user (if known) of the line or means of communication, against which the measure is going to be placed, shall be enclosed too. Communication of suspect or accused with persons whose witnessing is abstained cannot be recorded. In cases where this circumstance has been revealed after the recording has been conducted, the conducted recordings shall be destroyed immediately. The decision of the measure may be given for maximum duration of two months; this duration may be extended by one month. However, for crimes committed within the activities of a crime organization, the court may decide to extend the duration several times, each time for no longer than one month and not more than three months in aggregate, if deemed necessary.

The location of the mobile phone can be determined upon the decision of the court, or in cases of peril in delay, by the decision of the public prosecutor, in order to be able to apprehend the suspect or the accused. The interaction of locating shall be conducted for maximum of two months; this duration may be extended by one month.

The communications of the suspect or accused person made through telecommunication can be surveil by decision of the court during investigation and jurisdiction. The decision shall include the type of the charged crime, the identity of the individual, upon whom the measure is going to be applied, the type of the tool of communication, the number of the telephone, or the code that makes it possible to identify the connection of the communication, as well as the duration of the measure. Decisions rendered and interactions conducted according to the provisions of this article shall be kept confidential while the measure is pending.

The provisions contained in this article related to wiretapping, recording and evaluating the information about the signals shall only be applicable for the crimes as listed below:

Those which are included in Turkish Criminal Code;

Migrant smuggling and human trafficking, Deliberate Murder, Torture, Sexual assault, Sexual abuse of children, Qualified theft and plundering, manufacture and trade of narcotics or stimulants, forgery of money, Prostitution, Cheating in bidding, Bribery, Laundering of asset values originating from crime, Disrupt the unity and territorial integrity of the state, Crimes against the constitutional order and the well functioning of this order, Crimes against the secrets of the state and espionage, Smuggling with guns, as defined in Act on Firearms and Knives and other Tools, The crime of embezzlement as defined in Act on Banks, Crimes as defined in Anti Smuggling Act, which carry imprisonment as punishment, Crimes as defined in Act on Protection of Cultural and Natural Substances.

No one can wiretap and record the communication through telecommunication of another person except under the principles and procedures as determined in this Article.

2.2. Purpose and Scope

Offenders benefit from means of telecommunication offered by technology to be able to commit crime and erase the tracks of the crime committed. The purpose of criminal proceedings is to reveal the material fact, in which frame surveillance of telecommunications should be regarded as normal (Yavuz, 2004, p.239). Utilizing the surveillance of communication as a measure in criminal proceedings which constitutes a heavy intervention to fundamental rights and freedoms, and increasing effectiveness of the measure and reduce its adverse effects all require certain conditions and a strict decision-making process, and an efficient surveillance system against abuses (Erdem, 2001, p.301).

Surveillance of telecommunications as a measure is referred to both in scope of the administrative inspection before the crime and during investigation and prosecution stages due to the commission of an offense. Whereas, the subject of our review is limited to the scope of the surveillance under a criminal investigation and prosecution initiated in case of a crime or a criminal suspicion. Pursuant to the legal arrangement in the Criminal Code, the surveillance of communication as a measure aims at obtaining evidence of a crime already committed or currently being committed (Ozturk, 2006, p.592).

2.3. Types of Surveillance of Communication

Pursuant to the Article 135 of the Code of Criminal Procedure, detection, wiretapping and recording of conversations made by telecommunication, evaluation of signal data and detection of the location of a mobile phone can be considered as types of surveillance and obtaining evidence. In this sense, the contents of the terms specified in the relevant law must be defined.

2.3.1. Wiretapping

Wiretapping means live monitoring and listening of conversations made via telecommunications in the communication media and environment (Kunter - Yenisey - Nuhoglu, 2006, p.705). Surveillance of telecommunications can be also defined as eavesdropping of all kinds of communication by covert means, and recording and evaluation of the data obtained therefrom. Means of communication refers to a wide range of equipment offered by modern technology, including telephone, fax, computer and all wired or wireless devices (Çoksezen, 2006, p.3).

According to another definition, surveillance of the communication refers that conversations by means of telecommunication are listened to by an authorized third party who thus gains information about the communication performed. Eavesdropping is the listening of telephone conversations, communication made by fax and computer and other written and oral communication by security officers (Yenisey,1999, p.48). However, it is not the listening-in and recording of conversations but the technical surveillance procedure stipulated in article 140 of the Code of Criminal Procedure to

listen to and to record conversation on phones, computers or any other device by using them as a receiver or transmitter except for the suspect's or the accused person's communication with others (Meran, 2006, p.36).

2.3.2. Recording of Communication

Recording of communication must be understood as recording of communication being made by means of telecommunication and any other type of communication by other technical tools (Kunter-Yenisey-Nuhoglu, 2006, p.705) According to another definition, it refers to the recording of conversations made through telecommunication by an authorized third party by means of a recording device (Özbek,2006, p.421). In other words, it means surveillance by copying communication data and recording it on suitable means (Kaymaz, 2012, p.112).

It is not sufficient to only listening to communication in struggle with organized crime. This is because it is usually known that members of criminal organizations are aware of the fact that their phone conversations are wiretapped and therefore they avoid disclosing beneficial information for police officers in their phone conversations, encrypt their conversations or give false information to misguide police officers. Surveillance of communication is allowed by having regard to circumstances in which monitoring of phone conversations for only once may not always be adequate for obtaining evidence. In this way, it will be possible to obtain better results by checking the records again and again (Yenisey, 1999, p.118).

2.3.3. Determination of the Communication

Determination of the communication refers to procedures involving detection of information about calls made and received, location and identity data regarding the communication between means of communication without intervening in the content of communication. Determination of communication within the frame of the Code of Criminal Procedure means identifying with whom the suspect or the accused communicates through telecommunication, which involves only the suspect or the accused (Özbek, 2006, p.422). Accordingly, determination of communication does not have the purpose of finding out the content of communication but identifying with whom, when, where and how long the suspect or the accused communicated. Although the subject is not fully clarified in the definition made in the regulation which explains these terms in the related article of the law, identification of unsuccessful attempts to have a phone conversation, such as when the mobile phone is off, does not respond or is not available, is also acceptable in scope of determination of communication. Moreover, there are a number of authors suggesting that, in case a phone number to be contacted is forwarded to another number, the identification of forwarding and forwarded numbers must also be considered within the same scope (Kaymaz, 2012, p.113).

Even though some authors have accepted the concept of determination of communication in line with the definition in the regulation (Özbek, 2006, p.421), the term 'determination of communication' has not been used only in this sense and it is claimed that information called as "external connection data" regarding between whom and at what time the communication was made are not included in this scope (Öztürk-Erdem,

2006, p.593). Another opinion suggests that determination within the frame of CMK indicates identification of the location of the phone or the user (Kunter-Yenisey-Nuhoglu, 2006, p.715).

Turkish Supreme Court defined communication in a decision as the determination of detailed information about the communication made by the suspect by the telephone he/she uses in the inquiry phase, in other words, determination of the connections with whom and when is made[1].

According to another definition, determination of communication refers to the identification of who were called via a certain phone number, how long the conversation took and who were contacted via e-mail (Çolak-Taşkın,2007, p.622). Determination of communication should not be considered as a concept only related to communication via phone. Identification of traffic data, which are generated by the computer systems in the chain of communication to send a message from the starting point to the destination without any intervention to the content of communication, and which indicate the initial point of communication, the path followed, date, time, dimensions, time and the type of service used in this communication, is also regarded as the determination of communication. Accordingly, identification of the Internet address of a sender or receiver of an electronic mail, time and duration of connection, the system used and paths followed for connection will be considered as included in scope of determination (Kaymaz, 2013, p.116).

The concept of determination of communication is called as HTS (Historical Traffic Search) in the court practices and, on the contrary to the wiretapping procedure, contains historical phone record data. (Taşkın, 2008, p.77). Determination of communication is available as a measure for all crimes regardless of whether or not they are included in above mentioned types of crime (Meran, 2006, p.36)

2.3.4. Evaluation of Signal Data

Signal data means any kind of data processed for communication or invoicing of communication on a network. Evaluation of signal data involves transfer of invoice, software and mechanical information from the data to a virtual pool, where they are subject to a secondary process and then evaluated and processed for any other purpose. There is no intervention to the content of communication at this point. It is noted in the definition that such information is already stored by companies for invoicing processes (Şahin, 2006, p.381). The regulation setting out the provisions about the subject defines the evaluation of signal data not as an intervention to the content of communication, but as the process of identifying traces of signal data on communication systems in frame of a decision by an authorized body, and to draw meaningful conclusions from such data (Taşkın, 2008, p.86).

The processes of evaluating signal data and determining communication are very similar to each other, which causes interference and confusion in practice. This

[1] Decree dated 03.10.2005 with File no 2005/14969 E, Decree no 20489 K, by the Criminal Dept. No. 5 of the Court of Appeals (YKD June 2006, V.32, I.6, p.992)

confusion might lead to application of the evaluation of signal data also in terms of ordinary crimes under the title of determination of communication, and may cause serious human rights violations.

2.3.5. Determination of Mobil Phone Location

There is no significant problem in the definition and implementation of this concept. A decision on the identification of location can be implemented with assistance of the GSM operator offering the related service for the capture of the suspect or the accused. The suspect or the accused can be captured upon an investigation by police officers after the mobile phone used by the suspect or the accused and the nearby base stations to which the mobile phone is connected are detected. Determination of location can be applied not only to mobile phones used by the suspect or the accused but also to mobile phones which can be beneficial for capturing suspect or the accused or mobile phones of persons other than the suspect or the accused (Nuhoglu,2006, p.12). Mobile phones exchange signals with the base station of the GSM operator within the coverage area where they are located and communication is established when the signal sent by the phone is responded by the base station. The location and number of the phone sending the signal can be detected by using the signal data which is sent by the phone (Kaymaz, 2009, p.53).

There are different opinions about the mobile telephone location determination in the doctrine. According to an opinion, it is claimed that the term determination of communication is not legitimate on the grounds that this term also comprises identification of the location of a mobile phone (Özbek et al., 2008, p.266). Another opinion suggests that identification of the location of a mobile phone differs from other types of surveillance and should be set out as a separate protection measure on the grounds that it aims at arresting the suspect or the accused and is individually specified in the law (Yokuş, 2007, p.112). Whereas, a different opinion defines surveillance of a mobile phone for the identification of its location not as a separate type of surveillance of communication but as a special type of determining communication and evaluating signal data (Şahin, 2006, p.265).

2.4. Objective Conditions for the Surveillance of Communication

There are some conditions which are objectively expected to be realized in any circumstances so that the evidences obtained upon surveillance of communication can be used at the public prosecutor's investigation or in criminal jurisdiction. Any failure in fulfilling the requirements of any of these conditions will cause the obtained evidence to be considered as "illegal evidence" and will not be suitable for use in criminal procedure.

2.4.1. Existence of a Suspect or an Accused

1- The Article 135 of the Turkish Code of Criminal Procedure stipulates that surveillance of the correspondence through telecommunication is allowed if during an investigation or prosecution is being conducted in relation to a crime. This Code describes persons

subject to prosecution as the suspect or the accused, and defines these terms in another article. In this frame, the suspect means the person who is under the suspicion of crime during the public prosecutor's investigation. And, the accused is defined as the person who is under the suspicion of crime from the beginning of trial until the finalization of the sentence.

However in German law, surveillance of communication of persons who are not under suspicion is possible under certain conditions. In Turkish law, in situations where the suspect is not certain yet, measure of surveillance of the communication cannot be resorted and reaching decision for the determination of a communication in general sense will be violation of the law as well.

2.4.2. Lack of Opportunity to Obtain Evidence by another Method

Surveillance of communication as a measure requires that there must be no opportunity to obtain evidence by other means during the investigation or the prosecution carried out, and there must be a strong suspicion based on concrete evidence that the suspect or the accused has committed the crime. Surveillance of communication cannot be referred to as a measure if there is an opportunity to obtain evidence about the suspect by other means. For instance, if it is possible to obtain necessary evidence through surveillance of the accused person's daily life by the police, surveillance of communication cannot be referred to as a measure (Soyaslan, 2007, p.267). The regulation defines the term of "lack of opportunity to obtain evidence in an other method " as the existence of an expectancy that no result will be obtained even if other measures are referred to during the investigation or jurisdiction, or a failure in obtaining evidence despite the exercise of one or several of any other methods, and the capability of obtaining the evidence only by means of such measure. However, this definition is not taken into consideration in practices of public prosecutors and courts; a decision on the surveillance of communication can be easily taken in the event of a suspicion that one of the types of crime specified in CMK may have been committed. Even the Ministry of Justice declared to the citizens that important constitution and human rights violations were made on this matter recently.

It is neither possible not appropriate to draw an analogy between the state of "lack of opportunity to obtain evidence by an other method" and "the existence of an expectancy that no result will be obtained" and to reach to the conclusion of "the existence of an expectancy that no result will be obtained" in frame of the definition in article 135/1 of CMK. If evidence can be obtained by applying other means of investigation in a concrete case, then such means should be applied. The character of investigation measures is their enforcement according to the principle of proportionality. If it is possible to achieve the objective by such means that are less restrictive on freedom, it will be disproportionate to apply such means that are more restrictive on freedom.

2.4.3. Existence of Concrete Evidence Creating Strong Suspicion

The Code requires that facts pointing out to the existence of a strong suspicion of crime, or in other words, "reasons for strong suspicion" must be available; this requirement of the Law expressly indicates that the law seeks proportionality between the weight of possibility of risk and the costs, which refers to the restrictions that will result from the protection measure.

According to Turkish Criminal proceedings system, suspicion is divided into two as basic suspicion and intense suspicion (Taşkın, 2008, p.102). Intense suspicion may also be classified as adequate suspicion and strong suspicion. Some authors divide suspicion into two groups as adequate suspicion and strong suspicion. Adequate suspicion is the state in which the possibility for an accused person to be convicted is stronger than the possibility for him/ her to be acquitted as a result of the trial to be performed according to the available evidence (Şen, 2011, p.69). Whereas, strong suspicion is the state in which the possibility for the accused to be convicted is strongly possible as a result of the trial to be performed according to the available evidence (Öztürk-Erdem, 2007, p.494). According to another criminal law expert, what is meant by the presence of strong suspicion reason is not the criminal suspicion about the commitment of a crime, but it must be understood as the presence of strong crime suspicion about the commitment of a crime by the suspect or accused (Sen, 2009, p.68).

According to an opinion in the doctrine, what is meant by “strong suspicion reasons about the commitment of a crime” included in the article provision is; the presence of concrete, tangible (strong) indications based on events. It is asserted that the suspicion sought in the application of the article provision consists of “simple and reasonable suspicion depending on strong indications”. According to this opinion, wiretapping would turn out to be unnecessary if the existence of such a strong suspicion was sought as all the evidences would have already been obtained. Therefore, the term "reasons for strong suspicion" should be understood as a degree of suspicion which is more intense than a simple initial suspicion but does not necessarily have to reach to the degree of an adequate or strong suspicion. (Kunter, Yenisey and Nuhoğlu, 2005, p. 724; Özbek, 2005, p.567). There are a number of authors who criticize the requirement for strong suspicion of crime on basis of their claim that it would make it harder to implement this measure (Taşkın, 2006, p.398). However, it can be argued that the arrangement is appropriate when it is taken into consideration that the measure constitutes a heavy and profound intervention to private life of individuals as well as their freedom of information (Yurtcan, 2005, p.359), , that the aim is to exercise this measure as the last resort to obtain evidence and that it is an exceptional measure.

Although the condition that there must be strong suspicion in the law made the provision inapplicable, it is not able to be concluded from the article text that simple suspicion is sufficient (Turhan, 2006, p.267). Simple suspicion is the lightest degree of suspicion. This refers to the state when the act alleged to have been committed is a crime and may be subject to investigation. Evidences which are at least in form of indications are needed to confirm existence of a simple suspicion. Therefore, suspicion based on estimation cannot be qualified as a simple suspicion.

3. Characteristics of the Obtained Evidences and Their Usage in Judgment

3.1. In Terms of Illegally Obtained Evidence

It is the result of human nature that persons who are under the suspicion of crime are likely to protect themselves from the crime and to hide or even destroy evidences. On the other hand, the purpose of Investigation by the Public Prosecutor is, to detect offenders by legal methods and to obtain evidence related to them (Kahraman, 2007, p.382).

As it is accepted in the modern criminal jurisdiction that unlimited search for the facts will damage numerous personal and social values, an approach focusing on "finding the truth no matter what" is unacceptable. This is because there is an anonymous saying in Criminal Justice, "A poisonous tree will certainly have poisonous fruits." It must be noted that criminal procedure is a type of procedure in which not only the offenders but also the innocents are included. Therefore, there have been efforts to protect personal freedoms and social values through a number of restrictions which are called as evidence prohibitions in the Turkish Law (Öztürk,1995, p.7).

The Article 38/7 titled "Principles of Crimes and Punishments" in the Turkish Constitution stipulates that findings which are illegally obtained cannot be accepted as evidences. The Article 217/2 of the Turkish Code of Criminal Procedure (CMK) contains the provision that "The charged crime may be proven by using all kinds of legally obtained evidence". Pursuant to the mentioned provisions of the constitution and the relevant law, evidences obtained from wiretapping which is not subject to a duly passed court decree cannot be used in criminal procedure.

Another controversial issue about evidence prohibitions is the question of whether it is possible to consider other concrete findings as evidence by taking illegally obtained evidences as basis (Yıldız, 2002, p.193). If evidence prohibitions are violated, such evidence will not be taken as basis for the final sentence. This is considered as an absolute prohibition on evaluation of evidences. Meanwhile, pursuant to the distal effect of evidence prohibitions, other evidences regarding other crimes, obtained upon implementation of the measure, will become inappropriate to be taken as basis of the judgment. This is due to the fact that, as we said before, a poisonous tree will certainly have poisonous fruits.

3.2. In Terms of Incidentally Obtained Evidences

If, during the wiretapping of a suspect's phone upon court order, evidences which are not related to the pending investigation by the public prosecutor but which demonstrate that another crime has been committed, such crimes can be kept by the public prosecutor and used in a new investigation. However, the only requirement is, the new crime that is thought to be committed must be included in the catalogue of crimes in the article 135 of CMK. Otherwise, it will not be possible to use such incidentally obtained

evidences, which will then be immediately destroyed.

Conclusion

Throughout the last decade in which the Law on Criminal Procedure has set out the terms of surveillance of communication made through telecommunication between individuals for purpose of capturing criminals and obtaining evidences, in addition to the illumination of very crucial cases in our country owing to this, unfortunately enormous human rights violations and scandals have been experienced. Although the law regulates the surveillance conditions clearly, it was revealed years later that some inquiry officers abused their power and wiretapped conversations of people who are not crime suspects. Due to the close relationship of the law system and politics in our country and occasional attempts of politicians to dominate the law, we all have witnessed some illegal wiretapping cases. We are deeply sorry to note that unfair arrests and imprisonments have taken place as a result of illegal wiretapping practices which involved surveillance of the conversations of certain individuals or groups in order to punishing them politically, and false allegations that they were criminal organizations. Although many people who are alleged to have established an enterprise to overthrow the constitutional order and the government and are imprisoned for a long time and released after it is understood years later that these evidences are obtained illegally. This situation damages the trust in law and investigation authorities in the country. Although there are supreme court decrees expressing that the information obtained by the recording of telephone conversations don't have the proof ability on their own and these shall be supported by other evidences, and the people shall not be convicted in the framework of the words uttered over the phone, unfortunately we saw hundreds of sentenced people just wiretapped and no other evidences against them. These samples are absolutely unacceptable for the fair trial principle. Besides, the right against self-incrimination, as an important component of this principle, has been violated several times when the records were share with the press although supposed to be confidential. And people were shown guilty although their guilt was not proven yet. The disclosure to press of call texts, which have nothing to do with the alleged crime but are in all respects part of the person's private and even secret life, is something that is definitely unacceptable in a state of law. However, CMK consists of significant regulations about keeping these recordings confidential. If the sanctions on this matter were aggravated in Turkish Penal Code, tarnishing of people in the society would not be this easy

Even though it is necessary to accept that the measure is abused at times due to the problems indicated above, the principal problem is pirate wiretapping that made out of CMK. Many official institutions have authority to wiretap in our law system. (Police, Army, Intelligence Agency) But the real problem is illegal eavesdropping. The government must struggle to these malicious people who eavesdrop to citizens by wiretapping devices that can be easily purchased over the Internet. Because this type of listening, has been put majority of our people into "someone eavesdropping me" paranoia. We should not forget that, it seems impossible for a society who doesn't feel

safe legally to live peacefully either.

References

ALTIPARMAK K. (2014) *Büyük Biraderin Gözetiminden Çıkış: Telefonların İzlenmesinde Devletin Sorumluluğu.* Ankara: TBBD.

ÇOKSEZEN, A. (2006) *5271 Sayılı Ceza Muhakemesi Kanunu ve Avrupa İnsan Hakları Sözleşmesi Çerçevesinde Ceza Muhakemesi Tedbiri Olarak İletişimin Dinlenmesi*. İstanbul.

ÇOLAK H., and TAŞKIN M. (2007) *Ceza Muhakemesi Kanunu Şerhi*. Ankara: Seçkin Yay.

DOĞRU, O. and NALBANT A. (2013) *İnsan Hakları Avrupa Sözleşmesi Açıklama ve Önemli Kararlar*. Ankara: Pozitif Mat.

DÖNER, İ. (2012) Arama-elkoyma, dijital verilere elkoyma, *AİHM Kararları Işığında Koruma Tedbirleri ve İfade Özgürlüğü Sempozyumu*. Ankara: Mart 2012.

ERDEM, M. R. (2001) *Organize Suçlulukla Mücadelede Gizli Soruşturma Tedbirleri.* Ankara: Seçkin Yay.

GÜMÜŞAY, M. (2009) *Türk Hukukunda Adli ve Önleme Amaçlı Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi*, Ph.D. Thesis İstanbul: Marmara University, Institute of Social Sciences.

İNCEOĞLU, S. (2013) *İnsan Hakları Avrupa Sözleşmesi Ve Anaya*sa. Ankara: Şen Mat.

KABOĞLU, İ. (2002) *Özgürlükler Hukuku*. Ankara: İmge Kitabevi

KAHRAMAN, M. (2007) Koruma tedbiri olarak adli arama. *Yargıtay Dergisi*. 33(3).

KAYMAZ S. (2013) *Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi*. Ankara: Seçkin Yay.

KETİZMEN, M. (2008) *Türk Ceza Hukukunda Bilişim Suçları*. Ankara: Adalet Yay.

KILKELLY, U. (2012) *Özel Hayata Ve Aile Hayatına Saygı Gösterilmesi Hakkı, Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesinin Uygulanmasına İlişkin Kılavuz*, İnsan Hakları El Kitapları, No.1 Ankara: Şen Matbaa

KUNTER N., YENİSEY, F. and NUHOĞLU, A. (2008) *Ceza Muhakemesi Hukuku*. İstanbul: Beta Yayınevi

KUNTER, N., YENİSEY, F. and NUHOĞLU, A. (2006) *Muhakeme Hukuk Dalı Olarak Ceza Muhakemesi Hukuku*, İstanbul: Beta Yayınevi.

MERAN, N. (2006) *Adli ve Önleme Amaçlı İletişimin Denetlenmesi.* Ankara: Adalet Yay.

NUHOĞLU, A. (2006) Adli amaçlı telekomünikasyon yoluyla yapılan iletişimin denetlenmesi ile teknik araçlarla izleme tedbirine konu olan suçlar. *Yargı Dünyası*. August 128. 9

ÖZBEK, V. Ö. (2005) *CMK İzmir Şerhi - Yeni Ceza Muhakemesi Kanunu'nun Anlamı: 1.Bası*. Ankara: Seçkin Yay.

ÖZBEK, V. Ö. (2006) *Ceza Muhakemesi Hukuku*. Ankara: Seçkin Yay.

ÖZBEK, V. Ö. et al. (2008) *Ceza Muhakemesi Hukuku*. Ankara: Seçkin Yay.

ÖZTÜRK, B. (1995) *Yeni Yargıtay Kararları Işığında Delil Yasakları*. Ankara: AÜSBF İnsan Hakları Merkezi Yayınları.

ÖZTÜRK, B. and ERDEM, M. R. (2006) *Uygulamalı Ceza Muhakemesi Hukuku, Yeni Ceza Muhakemesi Kanununa Göre Yenilenmiş 9. Baskı*. Ankara: Turhan Kitabevi.

ÖZTÜRK, B. and ERDEM, M. R. (2007) *Uygulamalı Ceza Muhakemesi Hukuku. 11. Baskı.* Ankara: Seçkin Yayınevi

ŞAHİN, C. (2006) *Ceza Muhakemesi Şerhi*. Ankara: Seçkin Yay.

ŞAHİN, İ. (2004) *Türk Ceza Yargılaması Hukukunda Yakalama ve Gözaltına Alma*. Ankara: Seçkin Yayınevi

ŞEN, E. (1999) Türk hukukunda telefonların gizlice dinlenmesi sebebiyle gündeme gelen hukuka aykırılık sorunu ve kişi haklarına keyfi müdahaleler. *Pof. Dr. Sahir ERMAN Armağanı.* İstanbulÇ Vakıf.

ŞEN, E. (2007) İletişimin denetlenmesi tedbiri. *Ceza Hukuku Dergisi*. August, 5.

ŞEN, E. (2011) *Telefon Dinleme*. Ankara: Seçkin Yayınevi.

SOYASLAN, D. (2007) *Ceza Muhakemesi Hukuku* 3.Baskı. Ankara: Yetkin.

SÖZÜER, A. (2009) Türkiye'de ve karşılaştırmalı hukukta telefon, teleks, faks ve benzer araçlarla yapılan özel haberleşmenin bir ceza yargılaması önlemi olarak denetlenmesi. *İÜHFM*. 55(3). 65-110.

TAŞKIN, M. (2003) Türkiye'de çıkar amaçlı suç örgütleriyle mücadele, mücadelede kullanılabilecek yeni yöntemler. *Adalet Dergisi*. 15.

TURHAN, F. (2006) *Ceza Muhakemesi Hukuku: 1. Bası*. Ankara: Asil Yay.

TÜYSÜZ, H. (2010) *Suçla Mücadelede İletişimin Denetlenmesi*. Master Thesis. Ankara: Police Academy, Institute of Security Sciences

ÜNVER Y. and HAKERİ, H. (2006) *Sorularla Ceza Muhakemesi Hukuku*. Ankara: TBBD.

Yargıtay Kararları Dergisi (YKD) Haziran 2006, 32(6), 992

YAVUZ, A. H. (2005) Ceza yargılaması hukukunda telekomünikasyon yoluyla yapılan iletişimin denetlenmesi kavramı, *TBB Dergisi*. 60.

YAVUZ, H. (2004) Ceza yargılamasında bir koruma tedbiri olarak telekomünikasyon yoluyla yapılan iletişimin denetlenmesi. *TBB Dergisi*. 60. 235-262.

YENİSEY, F. (1999) *Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu*. Ankara: Seminer

YILDIZ, A. K. (2002) *Ceza Muhakemesinde İspat ve Delillerin Değerlendirilmesi*. Ph. D. Thesis. İstanbul: Istanbul University, Institute of Social Sciences.

YOKUŞ, S. H. (2007) Postada el koyma ve telekomünikasyon yoluyla yapılan iletişimin denetlenmesi. *TBB Dergisi*. 69. 97-124.

YURTCAN, E. (2005) *Ceza Yargılaması Hukuku: 11'inci Bası*. İstanbul: Vedat Kitapçılık.

ZAFER, H. (1999) *Ceza Hukukunda Terörizm*. İstanbul: Beta Yay.