INTELLIGENCE SURVEILLANCE OF WIRE COMMUNICATIONS UNDER TURKISH LAW

Yard. Doç. Dr. Saadet Yüksel[*]

"Overall 71.538 wire communications are currently being intercepted and 65% of these communications which means 2/3 of overall wire communications is being intercepted for the purpose of intelligence surveillance now."[1] This is the latest announcement of the President of the Telecommunications Directorate[2] in Turkey. He made this statement, while he was trying to point out that wire communications of the Appeal Court and the Highest Administrative Court have not been intercepted. Even though the numbers are always very speculative, in my opinion, the reason why he was making this announcement shows that interception of wire communications is one of the hot topics in Turkey. This paper will attempt to explain related laws including amendments and analyze the procedure and principles of intelligence surveillance of wire communications and processing the data obtained by such surveillance.

According to the Constitution of 1982, everyone has the right to demand respect for his or her privacy and family life[3] and right to freedom of communication.[4] This communication shall be impeded or its secrecy shall be violated only if there is a judge's order. In cases of an emergency situation which will occur in the event of a delay, an authorized officer's order will be granted on the grounds of "national security, public order, prevention of crime commitment, protection of public health and public morals, or protection of the rights and freedoms of other".[5]

Following the fundamental basis of the Constitution, surveillance of communications is basically regulated under the Turkish Criminal Procedure Code.[6] Before further exploring, I should briefly explain that article of 135 and 250 of the Code along with other related regulations use the term of "telecommunication" in order to explain "communications" which include wire communications. Moreover, the procedure which is regulated by these related

---

[*] İstanbul Üniversitesi Hukuk Fakültesi Anayasa Hukuku Anabilim Dalı.

[1] "Sistem Bulundu Dinleme Cikmadi" (November 16, 2010), http://www.milliyet.com.tr/-sistem-bulundu-dinleme-cikmadi-/guncel/haberdetay/18.11.2010/1315426/default.htm.

[2] http://www.tib.gov.tr/, November 16, 2010, The Turkish Telecommunications Directorate is formed under "the Information and Communication Technologies Authority" in Ankara (November 16, 2010), http://www.tk.gov.tr/eng/english.htm.

[3] Article 20/1 of the 1982 Constitution, Constitution of Republic Turkey, 1982 Consolidated to Law No. 5982 of 2010 (December 17, 2010), http:// heinonline.org.ezp-prod1.hul.harvard.edu/HeinDocs/cowdocs/tr_1982_2010_vc_moj_ smj.pdf.

[4] Article 20/2 of the 1982 Constitution, Constitution of Republic Turkey, 1982 Consolidated to Law No. 5982 of 2010.

[5] Ibid.

[6] The Turkish Criminal Procedure Code, No. 5271, Dec. 4, 2004, Official Gazette numbered 25673, December 17, 2004.

provisions is the interception of communications including wire communications through landlines and cell phones. In this paper, the term of "wire communications" is used instead of using "telecommunication" and it also includes landlines and cell phones.[7] Under Turkish law, interception of oral communications, bugging, by using secret recording devices in a room or physical space is regulated under a different provision which is article 140 of the Turkish Criminal Procedure Code.[8]

I. The Laws of the Intelligence Surveillance of Wire Communications

Under Turkish law, "the Code on Combatting with Criminal Organizations Formed to Obtain Gain/No. 4422"[9] is the first code which provides a legal framework for intelligence surveillance of communications.[10] This code was abolished by the Turkish Criminal Procedure Code which was enacted in 2004. The Turkish Criminal Procedure Code has been regulating surveillance but not intelligence surveillance with prevention purposes. This absence was fulfilled by amending the Code on Duties and Powers of Police, the Code on Gendarmerie and the Code on National Intelligence in 2005.[11] There is a slight distinction between surveillance of wire communications for the purpose of law enforcement investigation to provide evidence for a criminal investigation at trial which is regulated by the article 135 of the Turkish Criminal Procedure Code, [12] and intelligence surveillance of wire communications which is regulated by the Law numbered 5397.[13] While this paper is not meant to be about surveillance for the purpose of law enforcement investigation, I will focus on the principles and regulations of surveillance of communications for the purpose of intelligence gathering in Turkish law. I will also mention the major differences between the above two.

Intelligence surveillance of communications is prohibited by Turkish law only for preventing particular crimes. Unlike surveillance done for law enforcement investigation purposes, [14] there is no specific determination for

---

[7] Nurullah Kunter, Feridun Yenisey, Ayşe Nuhoğlu, **Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku**, 17. ed., İstanbul, Beta, April 2010, p. 44; Mustafa Taşkın, **Adli ve İstihbari Amaçlı İletişimin Denetlenmesi**, Ankara, Seçkin, 2008, p. 75.

[8] The Turkish Criminal Procedure Code, No. 5271, Dec. 4, 2004; for the English version see "the Turkish Penal Procedure Code, trans. Feridun Yenisey, and ed. Jelani Jefferson Exum, Istanbul, 2009".

[9] Art 2 of the Code on Combatting with Criminal Organizations Formed to Obtain Gain/No. 4422, July 30, 1999, Official Gazette numbered 23773, August 1, 1999.

[10] Fatih Selami Mahmutoğlu, "Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, " **Polise Görev, Yetki ve Sorumluluk Veren Mevzuat Uygulamaları Eğitim Projesi (MUYEP) Tebliğleri - 2**, EGM Yayınları Katalog No: 444, Eğitim Dairesi Başkanlığı Yayın No: 43, 2008, Ankara, s. 408 et seq.; Adem Sözüer, "Türkiye'de ve Karşılaştırmalı Hukukta Telefon, Teleks, Faks ve Benzeri Araçlarla Yapılan Özel Haberleşmenin Bir Ceza Yargılaması Önlemi Olarak Denetlenmesi, " **İHFM**, Vol. LV, No:3, 1997, p. 77.

[11] The Code on Duties and Powers of Police, the Code on Gendarmerie and the Code on National Intelligence were amended by the Law numbered 5397 in July 3, 2005, Official Gazette numbered 25884, July 23, 2005.

[12] The Turkish Criminal Procedure Code, No. 5271, December 4, 2004.

[13] The Code on Duties and Powers of Police, the Code on Gendarmerie and the Code on National Intelligence were amended by the Law numbered 5397 in July 3, 2005, Official Gazette numbered 25884, July 23, 2005.

[14] For surveillance of communications for the purpose of law enforcement investigation to provide evidence for a criminal investigation at trial, wire communications of "the

people whose wire communications may be intercepted in intelligence surveillance. However, such an interception shall be done for preventing particular crimes. According to the article 250/1, (a), (b), (c) of the Code, these crimes are (a) producing and trading with narcotic or stimulating substances committed within the activities of a criminal organization, (b) crimes committed by using coercion and threat within an organization formed in order to obtain unjust economic gain, and " (c) crimes committed to endanger national security".[15] However, the interception for the purpose of law enforcement investigation shall only be applicable for crimes such as "sexual abuse of children, bribery, torture, producing and trading with narcotic or stimulating substances, establishing armed criminal organization or supplying weapons to these organizations, crimes against the secrets of the state and spying, and crimes as defined in the Combating Smuggling Act, which carries imprisonment as punishment".[16] Since the Code on Combating Terrorism is not mentioned within this scope, this provision has been subject to a lot of criticism. Furthermore, even though article 135/7 of the Turkish Criminal Procedure Code regulates that communications shall be intercepted only for the crimes stated under this provision, broad interpretation which will help to include some other crimes specified under the Code on Combating Terrorism might be considered.[17]

Like interception for the purpose of law enforcement investigation, interception for the purpose of intelligence gathering shall technically be pursued by the Turkish Telecommunications Directorate.[18] The Directorate which has one chief who is appointed by the Prime Minister and several officers also includes one officer from the National Safety Office, National Intelligence Office and General Command of Gendarmerie. It is pertinent to note the presence of these enforcement agencies' officers because unlike surveillance for the purpose of law enforcement investigation, intelligence surveillance of wire communication is not actually and directly done by this Telecommunications Directorate.[19] According to the regulations, even though the Directorate receives authorizations of interceptions, such an interception is technically pursued by authorized enforcement agencies' officers mentioned above.[20] There are 3 codes that regulate these 3 law enforcement agencies' authority to intercept wire communications and principles that they follow for the interception. These codes are the Code on Duties and Powers of Police, the

---

suspect" or "the accused" may be intercepted under article 135 of the Turkish Criminal Procedure Code, Official Gazette numbered 25673, December 17, 2004, for the English version please see Yenisey and ed. Jefferson Exum, p. 141-145.

15 These crimes are defined by the second book, section 4, chapters 4, 5, 6 and 7 (except for articles 305, 318, 319, 323, 324, 325 and 332) of the Turkish Criminal Procedure Code, also see Art 250/1 of the Turkish Criminal Procedure Code.

16 Article 135 of the Turkish Criminal Procedure Code.

17 Kunter, Yenisey, Nuhoğlu, p. 55, 56.

18 Article 10 of the Regulation on the Principles and Procedure of the Intercepting, Monitoring and Recording Correspondence through Telecommunication", published at the Official Gazette numbered 25989, November 10, 2005, http://www.tib.gov.tr/content/telekom%C3%BCnikasyon-ileti%C5%9Fimba%C5%9Fkanl%C4%B1%C4%9F%C4%B1-g%C3%B6rev-ve-te%C5%9Fkilaty%C3%B6netmeli%C4%9Fi.

19 Kunter, Yenisey, Nuhoğlu, p. 39.

20 Article 10 of the Regulation on the Principles and Procedure of the Intercepting, Monitoring and Recording Correspondence through Telecommunication", published at the Official Gazette numbered 25989, November 10, 2005 (November 19, 2010).

Code on Gendarmerie and the Code on National Intelligence. Before analyzing the principles and procedure that these authorized officers follow, it is important to remark on one of the problematic features of those codes. None of them clearly requires any level of suspicion when they authorize these officers for such an interception. Thus, it might be said that even a simple level of suspicion might be sufficient to issue an interception order.[21] Whereas, for surveillance for the purpose of law enforcement investigation, article 135/1 of the Turkish Criminal Procedure Code requires "reasonable suspicion and failure of trying regular investigative procedures".[22]

1. Authority of the Police to Intercept the Communications

Police is authorized to intercept the communications by the provisional article 7 of the Code on Duties and Powers of Police which was amended in 2005. According to this Code, the police shall intercept wire communications to prevent crimes listed in article 250/1, (a), (b), (c) of the Turkish Criminal Procedure Code. These crimes are (a) producing and trading with narcotic or stimulating substances committed within the activities of a criminal organization, (b) crimes committed by using coercion and threat within an organization formed in order to obtain unjust economic gain, and (c) crimes committed to endanger national security.[23]

The interception order shall be issued by the judge. However, interception without judicial authorization is allowed whenever there is an emergency situation that could exist in cases of delay. In such a situation, the Chief of National Safety Office or the Chief of National Intelligence Office may issue an interception order.[24]

The Code on the Duties and Powers of the Police requires that information gathered by such an interception shall not be used for any purposes other than of those mentioned by the provisional article 7 of the Code. These purposes are listed as "taking protective and preventive measurements on national and territorial integrity of the state, its constitutional order and public security and maintaining safety and public order".

---

[21] Aytekin Geleri, "Türkiye'de İletişimin Denetlenmesi", Stratejik Düşünce Enstitüsü/Institute of Strategic Thinking, July 2010, Ankara, p. 25.

[22] See Cumhur Şahin, **Ceza Muhakemesi Hukuku I**, 2. ed., Ankara, Seçkin, 2011, p. 265; Veli Özer Özbek, M. Nihat Kanbur, Koray Doğan, Pınar Bacaksız, İlker Tepe, **Ceza Muhakemesi Hukuku**, 2. ed., Ankara, Seçkin, 2011, p. 402, 403; Bahri Öztürk, Durmuş Tezcan, Mustafa Ruhan Erdem, Özge Sırma, Yasemin F. Saygılar, Esra Alan, **Nazari ve Uygulamalı Ceza Muhakemesi Hukuku**, Ed. by. Bahri Öztürk, 3. ed., Ankara, Seçkin, 2010, p. 380, 381.

[23] Provisional article 7 of the Code on Duties and Powers of Police, No. 2559, as amended on July 3, 2007 (November 19, 2010), http://www.mevzuat.adalet.gov.tr/html/569.html.

[24] This procedure is mentioned not only by the provisional article 7 of the Code on Duties and Powers of Police but also by the article 5 of the Regulation on the Principles and Procedure of the Intercepting, Monitoring and Recording Correspondence through Telecommunication.

2. Authority of the Gendarmerie to Intercept the Communications

The gendarmerie's authority to intercept communications is regulated by the Code on the Gendarmerie.[25] Like the police, the gendarmerie shall intercept the communications to prevent crimes mentioned at the article 250/1, (a), (b), (c) of the Turkish Criminal Procedure Code. If there is an emergency situation that could exist in cases of delay, the Chief of General Command of Gendarmerie or the Chief of National Intelligence Office may issue an interception order.[26] Up until now, authority of the gendarmerie is similar to the manner in which police intercept the communications. However, the difference exits at the jurisdiction level. Since the crimes that fall within the scope of the police and gendarmerie's authority to intercept are the same, there might be some crimes committed in areas which also fall within the jurisdiction of both the police and gendarmerie.[27] Thus, it is required that the interception orders given under the Code on the Gendarmerie shall include the necessary information and documentation relating to the jurisdiction.[28]

3. Authority of the National Intelligence Office to Intercept the Communications

The National Intelligence Office's authority to intercept the communications is regulated by the Code on the National Intelligence.[29] There are two requirements in order to intercept the communications by the National Intelligence Office: if there is a requirement of fulfilling the duties mentioned by this Code and if there is a serious danger for the democratic state governed by the rule of law. Interception without judicial authorization is allowed whenever there is an emergency situation that exists in cases of delay. In such a situation, the Secretary or the Deputy Secretary of the National Intelligence Office may issue an interception order.[30] It is also important to note that unlike, the police and gendarmerie's jurisdiction restriction, the Office of National Intelligence exercises its duties including the interception over the entire country.[31]

---

[25] Provisional article 5 of the Code on Gendarmerie, No. 2803, as amended on July 3, 2007 (November 19, 2010), http://www.mevzuat.adalet.gov.tr/html/603.html. Please see also article 6 of the Regulation on the Principles and Procedure of the Intercepting, Monitoring and Recording Correspondence through Telecommunication.

[26] Ibid.

[27] Article 10/1 of the Code on Gendarmerie, No. 2803, Official Gazette numbered 17985, March 12, 1983; see also Taşkın, p. 202, 203.

[28] Art 9 of the Regulation on the Principles and Procedure of the Intercepting, Monitoring and Recording Correspondence through Telecommunication.

[29] Article 6 of the Code on the National Intelligence, No. 2937, as amended on July 3, 2007 (November 19, 2010), http://www.mit.gov.tr/kanun.html.

[30] Article 6 of the Code on the National Intelligence; please see also the article 7 of "the Regulation on the Principles and Procedure of the Intercepting, Monitoring and Recording Correspondence through Telecommunication".

[31] Taşkın, p. 202, 203.

II. The Procedure and Principles of Intelligence Surveillance

1. The interception order issued by the judge

An interception order shall be issued by judge.[32] However, as mentioned above, if there is an emergency situation that exists in cases of delay, other authorized enforcement agencies' officers may issue an interception order. However, in the surveillance for the purpose of law enforcement investigation, public prosecutor is authorized to issue an interception order, if there is an emergency situation.[33] Whichever officer issues the order, this order shall be submitted to the judge for his approval within 24 hours and the judge shall make a decision within 24 hours. If this period of time expires or the judge does not approve it, the order shall terminate. In all these situations, the order of authorization or approval must be given by one of the judges of the highest criminal court that has subject matter jurisdiction.

What should an interception order include? There are basically two groups of information that should be included in the order. The first group of information shall be provided in the order only if the relevant authority is able to obtain such information. This typically contains the identity of the person, whose communications are to be intercepted, the nature of the communication facilities, the phone numbers, and the code that makes it possible to identify the communication. The second group of information includes the nature of the interception, to what extent the interception is authorized, the period of time during which such an interception is authorized, the reasons for such interception, and the date and the place where authority to intercept is granted.[34] Moreover, the amendment, in 2007, required that the order which is authorizing the gendarmerie to intercept must also include the jurisdiction which the gendarmerie will exercise while performing its duty[35] in order to avoid jurisdiction conflicts between the police and the gendarmerie. Unlike the first group of information, the second group of information must be specified in the order mentioned above as mandatory information. Therefore, if such information is not present, the communication shall not be intercepted and will be given back to the related enforcement agency to collect this necessary information.[36]

2. Time

The order may permit the interception for a maximum period of three months. Extension of the order may be granted three more times but in any event no longer than three months each. The procedures required to obtain the initial order are to be followed for these extensions as well.[37] Thus, the overall period of the interception shall be twelve months.[38] The extension period differs

---

[32] Provisional article 7 of the Code on Duties and Powers of Police, No. 2559, as amended on July 3, 2007 (November 15, 2010), http://www.mevzuat.adalet.gov.tr/html/569.html.

[33] Article 135 of the Turkish Criminal Procedure Code.

[34] Article 9 of the Regulation on the Principles and Procedure of the Intercepting, Monitoring and Recording Correspondence through Telecommunication.

[35] Ibid.

[36] Article 10/3 of the Regulation on the Principles and Procedure of the Intercepting, Monitoring and Recording Correspondence through Telecommunication.

[37] Article 9 the Regulation on the Principles and Procedure of the Intercepting, Monitoring and Recording Correspondence through Telecommunication.

[38] Mahmutoğlu, p. 416 et seq.

when interception of wire communications is required for the purpose of law enforcement investigation. In such cases, like the intelligence surveillance, the order may permit it for a maximum of three months. However, unlike the intelligence surveillance, this period of time may only be extended once. Therefore, the overall period of the interception shall be six months.[39]

If a situation that involves danger of conspiratorial activities of terrorist organizations and if necessary, like in the interception for the purpose of law enforcement investigation, the judge may extend the period several times. Each extension shall be no longer than three months. If these extensions are interpreted as exceptions, it may be criticized as a broad exception since it does not regulate the number of times the order could be extended. This might not help to accomplish the goal of prevention. It is important to note that in cases of interception for the purpose of law enforcement investigation, these extensions shall be no longer than one month.

It is pertinent to note that unlike the initial orders, extension orders shall be granted only by judges. Since an emergency situation does not exist in the instant case after obtaining the initial order, authorized enforcement agencies' officers cannot issue an extension order.[40]

3. Termination of the Enforcement of the Order

Unlike the decision authorizing the interception, the decision terminating the interception does not need to be given by a judge. There are basically two situations that cause termination of the enforcement of the order of the judge's or law enforcement agencies' officers.

Firstly, in cases where there is an emergency situation that exists in cases of delay, if the judge does not approve the interception order issued by the authorized law enforcement agencies' officers or if these agencies do not submit their order and get the judge's approval within a period of 24 hours, the order shall not be applied. Moreover, if there are no grounds for the interception anymore, the decision shall not be applied.[41] Not only the codes but also the Regulation on the Principles and Procedure of the Intercepting, Monitoring and Recording Correspondence through Telecommunication does not specify the situations that would cause the exhaustion of the grounds of termination. However, for the termination of the enforcement of surveillance for the purpose of law enforcement investigation, these situations are listed more clearly, such as "no grounds for the prosecution of the suspect or no approval from the judge for the order".[42] Even though the judge's decision is not required to terminate the implementation, the enforcement agency or the public prosecutor in the case of surveillance for investigation are required to inform the judge about the termination.

---

[39] Article 135 of the Turkish Criminal Procedure Code.

[40] The extension order authorizing interception for the purpose of law enforcement investigation shall not be granted by the public prosecutor.

[41] Provisional article 7 of the Code on Duties and Powers of Police, article 11 of the Regulation on the Principles and Procedure of the Intercepting, Monitoring and Recording Correspondence through Telecommunication, article 6 of the Code on the National Intelligence, provisional article 5 of the Code on Gendarmerie, and please see also article 1, 2, and 3 of the Code numbered 5397.

[42] Article 137/3 of the Turkish Criminal Procedure Code, for the English version please see Yenisey and ed. Jefferson Exum, pp. 145-147.

There might be two places where the data is saved: authorized law enforcement agencies and the Telecommunications Directorate. The data shall be destroyed within 10 days under the control of the chief of the agency, if it is saved by the enforcement agency. If it is saved by the Directorate, then such information will be destroyed under the control of the Chief of the Directorate, and this termination shall be recorded.[43]

4. The Information Obtained by the Intelligence Surveillance and Confidentiality of the Information and Process

On one hand, the information obtained by the intelligence surveillance of wire communications cannot be used as evidence in an investigation or trial, since it is clearly stated in the codes that the data shall be used only for the purposes mentioned above.[44] On the other hand, the codes which regulate the authority of three law enforcement agencies, with the amendment in 2005, use the term "not legally valid"[45] for information obtained without conforming to the required principles and procedures. Thus, it is not clear what this term is trying to indicate other than saying "not to use this kind of information as evidence". In my opinion, it has intended to point out that it is "not allowed to disclose the information obtained by an illegal interception" since the same amendment makes it a crime for a person to intercept illegally by stating that this person shall be punished under the Turkish Criminal Code.[46]

While it is clear that the information obtained by intelligence surveillance cannot be used as evidence, it is not clear whether or not the information obtained by the surveillance for the purpose of law enforcement can be used as evidence or only instructive data. Although there is a discussion about it, the majority opinion, especially for records of intercepted communications, considers such information as evidence which should be supported by concrete circumstances and arguments.[47]

Principle of confidentiality shall be applied in regard to the process of keeping and saving the records and information obtained by the interception.[48]

---

[43] Article 11/3 of the Regulation on the Principles and Procedure of the Intercepting, Monitoring and Recording Correspondence through Telecommunication.

[44] Provisional article 7 of the Code on Duties and Powers of Police, article 6 of the Code on the National Intelligence, and provisional article 5 of the Code on Gendarmerie.

[45] Provisional article 7/11 of the Code on Duties and Powers of Police, article 6/10 of the Code on the National Intelligence, and provisional article 5/9 of the Code on Gendarmerie.

[46] Ibid.

[47] Özbek, p. 617; Öztürk, p. 353 et seq.; Ersan Şen, **Türk Hukuku'nda Telefon Dinleme, Gizli Soruşturmacı, X Muhbir**, 5. ed., Ankara, Seçkin, 2011, s. 165-171; Kunter, Yenisey, Nuhoğlu, p. 61, 62; İbrahim Şahbaz, İletisimin Denetlenmesi ve Yasak Deliller, Ankara, Yetkin, 2009, p. 182, 183; Mustafa Ruhan Erdem, "Ceza Muhakemesi Kanununda Telekomunikasyon Yoluyla Yapılan İletişimin Denetlenmesi" (November 27, 2010), http://www.ankahukuk.com/index.php?option=com_flexicontent&view=items&cid=154&id=2510&Itemid=126. Constitutional Court, in 1971, stated that although records of intercepted communications are evidence, they are still needed to be evaluated whether they are really belong to the data subject in order to make sure that they are sufficient for accusation, E. 1971/41, K. 1971/67, 17/8/1971 and 19/8/1971, Official Gazette, 15.1.1972/14073 (November 27, 2010), http://www.anayasa.gov.tr/index.php?l=manage_karar&ref=show&action=karar&id=360&content=.

[48] Provisional article 7 of the Code on Duties and Powers of Police, article 6 of the Code on the National Intelligence, and provisional article 5 of the Code on Gendarmerie.

Whichever officer or individual who has been authorized to intercept the communication does not follow the principle of confidentiality shall be immediately subject to the investigation by the public prosecutor.[49] In my opinion, even though this provision is a positive movement, it focuses on the "confidentiality" after the interception has concluded. However, as mentioned for the surveillance for the purpose of the law enforcement investigation[50], it should have been stated that the principle of confidentiality shall also be applicable during and after the application of the order. This might not change the result that interception made without following the principles mentioned above shall be considered illegal and is punishable. However, it might contribute to the emphasis of the prohibition of disclosing the information obtained by an illegal interception.

III. Personal data

In 2010, article 20 of the 1982 Constitution was amended to include that "everyone has the right to ask for the protection of personal data. This right includes being informed of, having access to and requesting the correction and deletion of the data and to be informed whether these are used in furtherance of required purposes. Personal data can be processed only in cases where there is a requirement of the law or consent of the person. The principles and procedures regarding the protection of personal data shall be regulated by law".[51] The reason this paper attempts to include the draft law on the protection of personal data and examines the changes it will make is that, like in European laws, in Turkish law the information obtained by the interception is considered as personal data.[52]

Although the related codes and regulations indicate a statutory remedy for the unlawful interception and disclosure of the information obtained by such an interception, they have not filled the gaps in terms of implementation such as confidentiality of processing the stored data obtained by the interception. Furthermore, Turkey has been criticized for not providing statutory data protections as an OECD country.[53] Eventually, in 2008, a draft code on the protection of personal data which is compatible with Directive 95/46/EC[54] was submitted to the Turkish Parliament. The goal of this draft

---

[49] Provisional article 7/7 of the Code on Duties and Powers of Police, article 6/6 of the Code on the National Intelligence, and provisional article 5/6 of the Code on Gendarmerie.

[50] Article 135/5 of the Turkish Criminal Procedure Code.

[51] Article 20/3 of the 1982 Constitution, Constitution of Republic Turkey, 1982 Consolidated to Law No. 5982 of 2010 (December 17, 2010), http://heinonline.org.ezp-prod1.hul.harvard.edu/HeinDocs/cowdocs/tr_1982_2010_vc_moj_smj.pdf. See also M. Kemal Oğuzman, Özer Seliçi, Saibe Oktay Özdemir, **Kişiler Hukuku (Gerçek ve Tüzel Kişiler)**, İstanbul, Filiz, 2011, p. 160-162; Mustafa Dural, Tufan Öğüz, **Türk Özel Hukuku Cilt II, Kişiler Hukuku**, İstanbul, Filiz, 2011, p. 94-97; Elif Küzeci, **Kişisel Verilerin Korunması**, Ankara, Turhan, 2010, p. 261-266.

[52] Nilgün Başalp, **Kişisel Verilerin Korunması ve Saklanması**, Ankara, Yetkin, 2004, p. 33, 34 and 109, 110.

[53] Colin J. Bennett, Regulating Privacy, **Regulating Privacy: Data Protection and Public Policy in Europe and the United States**, USA, Cornell University, 1992, p. 56, 57.

[54] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 – 0050 (November 25, 2010), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

code which is still being negotiated at the Legislation Commission of the Turkish Parliament is basically to regulate "the rules for processing the personal data".[55] Even though the draft code uses the term "processing", it is important to note that it includes "disclosing" the information. Therefore, while referring to the word of processing in this paper, it will also mean disclosing the information obtained by the surveillance.

The word of "processing" is used in the Draft Code as "activities that would be done on personal data, whether or not by automatic means, such as obtaining, recording, filing, modifying, retrieval, consultation, disclosure by transmission or otherwise making available, placement and blocking"[56]. Before further exploring the Draft Code, I should also briefly elaborate on the data which is protected by the Draft Code as "personal data". According to the article 3/ç, "any information relating to an identified or identifiable person" shall be considered as personal data within the scope of the Draft Code.[57]

1. General Principles for Processing Personal Data

According to the Draft Law, the data shall be obtained for the unambiguous, specific and legitimate purposes and will be processed in compliance with these purposes and in accordance to law. The data shall also provide the identification of the data subject and be kept for no longer than necessary.

2. Personal Data Filing System

One of the important changes made by the Draft is to establish a personal data filing system.[58] This will help to form a publicly open recording system which will include the categories of the data obtained, the purposes of the data processing and identities of the authorized officers that will process the personal data. It is important to note that this system is applicable to obtaining and processing personal data gathered by other kinds of surveillance except intelligence surveillance. As I will mention later, this filing system does not apply to the saving of personal data obtained by intelligence surveillance, instead it will mostly be used for the data that will be processed for historical, statistical, or scientific purposes.

Since transferring of personal data to other countries is permitted under this draft, this file will also include the types of data that might be sent to these countries. In order to be able to send the related data to these countries, the Draft requires that these other countries have at least the same level of protection as well.[59] However, there is also the purpose of prevention crimes[60]

---

[55] The Draft Code on the Protection of Personal Data, No. 1812, April 22, 2008, for the official Turkish version of the draft please see (November 24, 2010), http://www2.tbmm.gov.tr/d23/1/1-0576.pdf.

[56] Article 3/e of the Draft Code on the Protection of Personal Data.

[57] See Anne Cammilleri-Subrenat, Claire Levallois-Barth, **Sensitive Data Protection in the European Union**, Bruxelles, Bruylant, 2007, p. 13-18; Oğuz Şimşek, **Anayasa Hukukunda Kişisel Verilerin Korunması**, İstanbul, Beta, 2008, p. 43.

[58] Article 16-19 of the Draft Code on the Protection of Personal Data.

[59] Article 14 of the Draft Code on the Protection of Personal Data, please see supra note 44.

[60] Article 14/2 of the Draft Code on the Protection of Personal Data, supra note 44. Even though article 14/2 (c) is mentioned the "prevention of crimes", it is not stated which type of crimes would be included in this exception.

exception that permits the transfer of the data even if the other country does not have the same level of the protection.

3. Consent of the Person

Disclosing of the information is allowed, if there is consent of the data subject.[61] However, there are exceptions which allow disclosure without consent such as a requirement of law or any other obligation, a danger of personal injury that requires disclosing the data and already publicly available data.[62] When it comes to disclosing the content of the wire communication intercepted for intelligence purposes, generally in most cases, there is no consent of the person. Thus, on one hand, exception of "law or any other obligatory requirement" mentioned above could be applicable to allow the processing of this kind of personal data. This exception might also be interpreted similarly for the "national security and public order" exception which allows interception of wire communications.

On the other hand, article 22 of the Draft already states that article 6, 11, 16, 17, and 19 are not applicable in cases where there is protection of national security, public order or intelligence surveillance for these purposes. This means that the consent of the data subject (article 6), informing the data subject about the surveillance methods used and the categories of the data (article 11), establishing a personal data filing system which is open to the public (article 16 and 17) and pre assessment before the interception (article 19) do not come within the purview of intelligence surveillance.

It is important to note that even though the government will be able to save the data and process it in compliance with the procedures stated in this code, this still would not permit the use of such data as evidence.

4. The Committee on the Protection of Personal Data

For the first time in Turkish law the Draft Code requires the establishment of a committee on the protection of personal data. This committee is basically responsible for the application of processing the data. According to the article 31 of the Draft Code, it shall review and decide on the applications of people whose rights were violated by processing their personal data, set up the regulatory decisions on processing the data, work in collaboration with international organizations or agencies if necessary, and publish reports annually on its activities.

The Committee will also be responsible for establishing and controlling the personal data filing system mentioned above. It is required that the Committee shall exercise its powers independently. However, in my opinion, the fact that all seven members[63] of the Committee shall be appointed by the Council of Ministers[64] and the Committee's secretariat work shall be done by

---

[61] Article 6/1 and 2 of the Draft Code on the Protection of Personal Data, please see supra note 44.

[62] Article 6/3 of the Draft Code on the Protection of Personal Data, please see supra note 44.

[63] The members of the Committee shall serve 6 years and appointment of the members cannot be renewable. The members including the President of the Committee cannot not be replaced before the regular term expires unless there is criminal sanction about them related to their duties, article 28/3 of the Draft Code on the Protection of Personal Data.

[64] Article 27 of the Draft Code on the Protection of Personal Data.

the Office of Prime Minister[65] might not ensure its independent functioning. The independence of the Committee is crucial because according to the article 26/3 of the Draft Code, the Committee is authorized not only to process the data but also to request information and documents from public authorities.

5. Special Categories of Personal Data

Although the Draft Code establishes special categories of personal data that shall not be processed and the data revealing privacy of the person is considered such a category, the data obtained by surveillance could be processed under this Draft Code by the Committee. However, article 8/3 points out that as a special category, [66] the data related to the investigations, criminal sanctions and application of security measures might be processed by authorized officials, if the laws regulating these measures provide a sufficient level of privacy protection. Therefore, it could be said that the data obtained by intelligence surveillance would be processed by authorized officers rather than this Committee.

IV. Conclusion

While the code does not require any level of suspicion and also does not mention that such an interception is supposed to be the last resort, the provisions should not be unclear. For instance, as it is seen clearly, the categorization of the crimes that require a wire communication to be intercepted for intelligence purposes is quite ambiguous and open to interpretation. Furthermore, the time of the application of this measure is also quite ambiguous since there is no maximum extension period.

In my opinion, one of the most important reasons of having such ambiguous provisions is that an approach to privacy has been ignored for many years in Turkey. Having a constitutional amendment on the protection of personal data just recently and drafting a code compatible with international human rights regulations could be considered as indicators of a positive change in field of privacy. The Draft Code on the Protection of Personal Data requires enacting a regulation for it to be implemented.[67] This Regulation should overcome all ambiguities and make this constitutional amendment feasible in reality and be compatible with the criminal procedure and intelligence surveillance laws.

Bibliography

Başalp, Nilgün: **Kişisel Verilerin Korunması ve Saklanması**, Ankara, Yetkin, 2004.

Bennett, Colin J.: Regulating Privacy, **Regulating Privacy: Data Protection and Public Policy in Europe and the United States**, USA, Cornell University, 1992.

Cammilleri-Subrenat, Anne, Levallois-Barth, Claire: **Sensitive Data Protection in the European Union**, Bruxelles, Bruylant, 2007.

---

[65] Article 30/7 of the Draft Code on the Protection of Personal Data.

[66] Other special categories of data are data dealing with the person's ethnic origin, political opinion, religious or other beliefs, association membership, health and private life, article 7/1 of the Draft Code on the Protection of Personal Data.

[67] Article 39 of the Draft Code on the Protection of Personal Data, please see supra note 44.

Constitution of Republic Turkey, 1982 Consolidated to Law No. 5982 of 2010 (December 17, 2010), http://heinonline.org.ezp-prod1.hul.harvard.edu/HeinDocs/cowdocs/tr_1982_2010_vc_moj_smj.pdf.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 P. 0031 – 0050 (November 25, 2010), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

Dural, Mustafa, Öğüz, Tufan: **Türk Özel Hukuku Cilt II, Kişiler Hukuku**, İstanbul, Filiz, 2011.

Erdem, Mustafa Ruhan: "Ceza Muhakemesi Kanununda Telekomunikasyon Yoluyla Yapılan İletişimin Denetlenmesi" (November 27, 2010), http://www.ankahukuk.com/index.php?option=com_flexicontent&view=items&cid=154&id=2510&Itemid=126.

Geleri, Aytekin: "Türkiye'de İletişimin Denetlenmesi", Stratejik Düşünce Enstitüsü/Institute of Strategic Thinking, July 2010, Ankara.

Kunter, Nurullah, Yenisey, Feridun, Nuhoğlu, Ayşe: **Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku**, 17. ed., İstanbul, Beta, April 2010.

Küzeci, Elif: **Kişisel Verilerin Korunması**, Ankara, Turhan, 2010.

Mahmutoğlu, Fatih Selami: "Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, " **Polise Görev, Yetki ve Sorumluluk Veren Mevzuat Uygulamaları Eğitim Projesi (MUYEP) Tebliğleri - 2**, EGM Yayınları Katalog No: 444, Eğitim Dairesi Başkanlığı Yayın No: 43, 2008, Ankara, s. 405-418.

Oğuzman, M. Kemal, Seliçi, Özer, Oktay Özdemir, Saibe: **Kişiler Hukuku (Gerçek ve Tüzel Kişiler)**, İstanbul, Filiz, 2011.

Özbek, Veli Özer, Kanbur, M. Nihat, Doğan, Koray, Bacaksız, Pınar, Tepe, İlker: **Ceza Muhakemesi Hukuku**, 2. bs., Ankara, Seçkin, 2011.

Öztürk, Bahri, Tezcan, Durmuş, Erdem, Mustafa Ruhan, Sırma, Özge, Saygılar, Yasemin F., Alan, Esra: **Nazari ve Uygulamalı Ceza Muhakemesi Hukuku**, Ed. by. Bahri Öztürk, 3. bs., Ankara, Seçkin, 2011.

Taşkın, Mustafa: **Adli ve İstihbari Amaçlı İletişimin Denetlenmesi**, Ankara, Seçkin, 2008.

Sözüer, Adem: "Türkiye'de ve Karşılaştırmalı Hukukta Telefon, Teleks, Faks ve Benzeri Araçlarla Yapılan Özel Haberleşmenin Bir Ceza Yargılaması Önlemi Olarak Denetlenmesi, " **İHFM**, Vol. LV, No:3, 1997, p. 65-110.

Şahin, Cumhur: **Ceza Muhakemesi Hukuku I**, 2. ed., Ankara, Seçkin, 2011.

Şen, Ersan: **Türk Hukuku'nda Telefon Dinleme, Gizli Soruşturmacı, X Muhbir**, 5. ed., Ankara, Seçkin, 2011.

Şimşek, Oğuz: **Anayasa Hukukunda Kişisel Verilerin Korunması**, İstanbul, Beta, 2008.

The Code on Combatting with Criminal Organizations Formed to Obtain Gain/No. 4422, July 30, 1999, Official Gazette numbered 23773, August 1, 1999.

The Code on Duties and Powers of Police, the Code on Gendarmerie and the Code on National Intelligence were amended by the Law numbered 5397 in July 3, 2005, Official Gazette numbered 25884, July 23, 2005.

The Code on Duties and Powers of Police, No. 2559, as amended on July 3, 2007 (November 19, 2010), http://www.mevzuat.adalet.gov.tr/html/ 569.html.

The Code on Gendarmerie, No. 2803, Official Gazette numbered 17985, March 12, 1983.

The Draft Code on the Protection of Personal Data, No. 1812, April 22, 2008, (November 24, 2010), http://www2.tbmm.gov.tr/d23/1/1-0576.pdf.

The Regulation on the Principles and Procedure of the Intercepting, Monitoring and Recording Correspondence through Telecommunication", published at the Official Gazette numbered 25989, November 10, 2005.

The Turkish Criminal Procedure Code, No. 5271, Dec. 4, 2004, Official Gazette numbered 25673, December 17, 2004.

Yenisey, Feridun (trans.), Jefferson Exum, Jelani (ed.), "The Turkish Penal Procedure Code", Istanbul, 2009.