UiO : Faculty of Law
University of Oslo

DEPARTMENT OF PRIVATE LAW

ELECTRONIC EVIDENCE

PRIVACY CONCERNS RELATING TO THE COLLECTION OF ELECTRONIC EVIDENCE: UNDER TURKISH LEGAL SYSTEM AND CYBERCRIME CONVENTION

Master Thesis

GÜZ GÜLTAN

Acknowledgements

I would like to express my sincere appreciation to those who have provided me assistance and support during the research process. My project supervisor, Inger Marie Sunde, for offering her valuable expertise and enthusiastic support; all the members of Norwegian Research Centre for Computers and Law (NRCCL) for their precious encouragement, and lastly, my family who have made this valuable experience possible for me and provided endless support at every step of the Master's Degree Programme.

GÜZ GÜLTAN

Table of Contents

1 INTRODUCTION

1.1 Statement of the Problem

We are living in a technology intensive world where internet is the most significant source of information, a substantial part of communication is carried out electronically and storage of data is digitalized. This great shift towards the digital world also means that information, having conclusive force and used to be necessarily in physical presence, do not have to be physically present anymore. For instance, a letter had to be written on a paper in order to be send, but with the state of the art it is possible to send the same letter without the need to form it physically.

In the modern age, crimes also have digital dimension. Either they are committed using digital equipment or the information relating to crimes are found in electronic format. The crimes committed using the means of information and communication technologies; such as computers, networks, mobile phones and other electronic mediums, as either tools or targets are called cybercrimes. The information relating to any crime, which are either stored or transmitted in digital form, on the other hand, are called electronic evidence. Thereby, in a law suit or criminal prosecution, evidence are frequently found and collected in digital form from the digital communication services and/or the digital storage media. Evidence in electronic form serve to same aims with traditional evidence, but they bring along some concerns and treats, especially in the course of their collection, such as potential privacy violations.

With the widespread utilization of electronic information resources and services, it became highly important and requisite for the legislatures together with the inter-governmental and the international organizations to regulate the issues concerning electronic evidence. Some domestic laws provided for specific procedures for the collection of electronic evidence, such as Turkish law which will be presented in the following chapters of this research,

while the others adapted the existing rules on traditional- mostly physical or paper-based-evidence and developed corresponding interpretations, such as the US law.

As to the regulatory efforts at the international level, a general, internationally accepted approach may be developed on electronic evidence as a concept; however setting specific rules on the procedures relating to the collection of electronic evidence and expecting them to be internationally accepted and adopted by all the national laws would not be that simple. This is because criminal procedural laws "tend to be very specific to each jurisdiction"[1] and are applicable territorially. States pursue different aims and adopt different methods in the course of their activities relating to the area of criminal law. The Council of Europe Convention on Cybercrime (Cybercrime Convention)[2], though, is rather one of the most successful and comprehensive example of the international regulatory efforts.

However, both the domestic regulations and the international instruments have one common problem: procedures relating to the collection of electronic evidence, especially the electronic search and seizure and the interception of communication, pose threat against individuals' privacy. The problem does not arise only due to the nature of the electronic evidence, but it grows in relation to the way that the procedures are regulated. The problem will be analyzed based on the relevant regulations under Turkish law and Cybercrime Convention.

Thereby, in order to develop a practice that minimizes the privacy violation risks related to the application of criminal procedures, it is particularly important to answer the following questions:

- What are the procedures relating to the collection of electronic evidence under Turkish law and Cybercrime Convention?
- What is the relation between privacy and procedural rules relating to the collection of electronic evidence in general?

[1] Walden, I. *Computer Crimes and Digital Investigations* (2007), p.353
[2] Further information will be provided in the following chapters.

- What are the privacy concerns that come along with the regulations on search and seizure of computers in the Turkish legal system?
- What are the privacy concerns that come along with the regulations on interception of communication in the Turkish legal system?
- What are the privacy criticisms brought against the Cybercrime Convention?
- What are the recommendations proposed to enhance the protection of privacy?

This research aims to provide some guidance for answering the above questions with a brief review on what is electronic evidence, the differences between traditional and electronic evidence, the types of electronic evidence.

1.2 Subject and Structure of the Thesis

This paper will provide general information on electronic evidence, but the main focus is the privacy concerns that arise in relation to the procedures on the collection of electronic evidence, especially electronic search and seizure and interception of communication.
Structure of the paper is as follows:
Chapter 2 covers what electronic evidence is, differences between traditional evidence and electronic evidence, types of electronic evidence and procedures relating to the collection of electronic evidence under Turkish law and Cybercrime Convention.
Chapter 3 will present the following issues: general principles on and limitations to the right to privacy regulated in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and the Constitution of the Republic of Turkey (TC), privacy concerns in relation to the regulations on electronic search and seizure and interception of communication procedures under various Turkish legislation and lastly, the criticisms brought against the Cybercrime Convention concerning privacy matters and the proposed recommendations.
And at last Chapter 4 will sum up all the information provided and the arguments developed throughout the paper.

1.3 Methodology

This thesis has two primary focus, first one is how the electronic evidence are regulated in the Turkish legal system and the Cybercrime Convention and the second one is what are the threats against privacy in relation to the criminal procedures regulated under Turkish legislation and the Cybercrime Convention.

The main reason behind the selection of Turkish law and Cybercrime Convention is: the Convention has to be put into force in Turkey[3] which means a parallel regulation to the Convention has to be provided in the Turkish legal system. Nevertheless, the existing state of the regulations differ, therefore each subject covered in this paper are presented within the context and sole of the relevant legislation. Yet, it is important to keep in mind that this is not a comparative study of Turkish law and Cybercrime Convention.

This research is, in general, a conceptual framework. Regarding the regulations on electronic evidence, though, two elements stand out: descriptive method and exploratory method. Various concepts, within the context, are described, and in order to gain familiarity with the phenomenon and acquire new insight, explanations on the regulations under Turkish legal system and Cybercrime Convention are provided.

As regards to the abovementioned second subject, whereas, analysis has been made about the regulations on the right to privacy, the electronic search and seizure and the interception of communication, relevant approaches on these subjects are identified, and associated critiques about the regulations in the Turkish law and Cybercrime Convention are asserted.

Additionally, relevant examples from case-law are presented in order to shed light on the problems arising from the implementation and the application of electronic search and seizure and interception of communication. Also, steady interpretations concerning the applications of those procedures and the privacy violations can be established in the light of those suitable precedents. Regrettably, Turkish case-law lacks relevant precedents on the subject; therefore, it has been referred to cases from other legal systems. Great majority of

[3] Turkey has signed the Cybercrime Convention on November 10, 2010 but it has not been ratified yet- please see http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

the cases are from the US case-law, due to the fact that it is very well-developed concerning the electronic evidence, and also the Fourth Amendment is concerned with the protection of privacy in a similar fashion as Article 8 of the EHRC and Article 13 of the TC[4].

The provisions of the TC and the TCPC, referred throughout the study, are from the official translations of the texts. However, other referred legislation do not have official translations, therefore no citation has been made from the provisions of those instruments.

[4] Further explanation will be provided under Chapter 3.

2 ELECTRONIC EVIDENCE

2.1 What is Electronic Evidence?

Electronic evidence is any probative information stored or transmitted in digital form[5]. Such information can be stored in computer hard drive, optical disks, floppy disks, remote internet storage, handheld devices, memory cards, network servers, emails etc.[6].

Formal rules relating to the admissibility of evidence vary among different jurisdictions, though, Turkish courts consider six issues during their assessment: electronic evidence, like any other evidence, must be:

- admissible,
- authentic,
- accurate,
- complete,
- convincing to courts,
- in compliance with provisions on 'evidence obtained by illegal or unfair means' (especially provisions related to search, copy and seizure)[7]

Digitally stored or transmitted information with a probative value, which is also admissible, authentic, accurate, complete, convincing to courts and in compliance with the procedural rules, can be used at trial[8] as electronic evidence. Nevertheless, before the trial, specifically during the investigation, ensuring that the collected information meet the above requirements is of primary importance.

---

[5] Pollitt, M. M., *Report on Digital Evidence* (2001), p. D4-89
[6] Lange, M.C.S. and Nimsger, K.M., *Electronic Evidence and Discovery: What Every Lawyer Should Know Now* (2009), p. 72
[7] Article 38(6) of the TC and article 134 of the TCPC, Karagülmez, A. *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri* (2011), p. 395&395
[8] Casey, E. *Digital Evidence and Computer Crime* (2000), p. 48&49

2.2 Differences between Traditional Evidence and Electronic Evidence

Peter Sommer outlined the following differences between traditional and electronic evidence in his article titled "Digital Evidence: Emerging Problems in Forensic Computing":

- In principle, it is hard to change the structure of traditional/physical evidence; whereas electronic data may change within a computer and/or a transmission line at any moment.
- When physical evidence is altered it would most probably leave traces or at least the alteration would be perceptible; however electronic evidence can be easily altered without leaving any trace.
- It may be much easier to change or distort the electronic evidence than the physical evidence during the collection process.
- Traditional evidence can be perceived at first sight; whereas most of the immediate electronic evidence cannot be read by humans, "many exhibits are print-out derived from primary electronic material".
- Electronic data can be obtained to the amount electronic devices record them.
- The velocity of technology has a profound effect on the quality of electronic evidence and the possibility of obtaining them[9].

In the article it is also stated that electronic evidence increase some of the treats which already exist regarding the traditional evidence; such as more commercial transactions are recorded, it is much easier to trace a person's history and activities or it becomes possible to carry out computer-assisted investigation methods[10] which leads to perform legal assessments, such as this paper.

---

[9] This comparison has been adopted in the Turkish doctrine as well. e.g. Karagülmez, A. *Bilişim Suçları ve Soruşturma- Kovuşturma Evreleri* (2011), p. 394

[10] For the differences of physical and electronic evidence also see. Casey, E. *Digital Evidence and Computer Crime* (2000), p. 4&5

2.3 Types of Electronic Evidence

An electronic document or information consists of various data, sometimes comprising more than one quality; for instance, electronic mails consist: data that conveys the meaning or substance of a communication and data indicating the communication's origin, destination, route, time, date and size. Due to this reason, each piece of legislation adopts or creates a corresponding classification for electronic evidence with respect to its type[11]. In order to apprehend the procedures relating to the collection of electronic evidence explained in the following chapters, it is useful to take a look at the varying categorizations adopted in the Turkish legal system and the Cybercrime Convention.

2.3.1 In Turkish Legal System

There have been various classifications of evidence made in the Turkish doctrine. Within the scope of this research, two of those are relevant: with regards to evidential value and with regards to the content of evidence.

With regards to evidential value, evidence can be classified as: primary evidence, which do not require corroboration and are direct, and secondary evidence that need to be corroborated and are indirect[12]. Ersan Şen, who is a criminal law professor and a lawyer, makes a further subdivision among the secondary evidence as physical evidence and artificial evidence. Physical evidence are traces occurred during the crime or by the tools used in the crime, such as knife wound or forged money. These can also belong to the concerned person, for instance finger print, blood and strand of the suspect or victim. Whereas, artificial evidence are traces that do not reveal naturally but formed by people, like the special clothing worn or accessories used during the crime or records attained through interception of

[11] For example; Article 2 of the Directive 2002/58/EC, Article 1 of the Cybercrime Convention
[12] Dinler, V., *Ceza Muhakemesinde Delillerin Toplanması* (2009), p.8&9

communication[13]. With regards to the evidential value, the electronic evidence may classify as secondary and artificial evidence.

With regards to the content of the evidence, there are testimonial evidence, documentary evidence and real evidence/indications[14]. Testimonial evidence are submissions of the suspect or the accused or victim(s) and witness statements. Documentary evidence are written records, sound and imagery recordings. And all the rest are considered as real evidence or indications which require corroboration[15]. Electronic evidence may fall under documentary evidence or real evidence, but not testimonial evidence due to the fact that the testimony has to be given in front of the court or law enforcement officers in order it to qualify as testimonial evidence.

Nevertheless, none of the Turkish legislation specifically mentions electronic evidence and makes a distinction based on the types of the electronic evidence, such as content data, traffic data or communications data. It is only possible to infer electronic evidence based on the mean used to obtain it.

2.3.2 In Cybercrime Convention

The Convention refers to the term 'computer data' which basically stands for 'electronic evidence'. 'Computer data' means data in electronic form or data that can be directly processed by computer system[16], including content, traffic and subscriber data[17]. Three different types of electronic evidence, in particular, referred in the Convention are 'content data', 'traffic data' and 'subscriber data'.

---

[13] Şen, E., *Ceza Yargılaması Süreci* (2011), p.286
[14] Dennis, I. H., *The Law of Evidence* (1999), p. 369 et seq. and also Kunter, N. and Yenisey, F., *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku* (2002), p. 564 et seq.
[15] Dinler, V., *Ceza Muhakemesinde Delillerin Toplanması* (2009), p.9
[16] The Explanatory Report, ¶25
[17] *supra note*, ¶28 and 136

Content Data

The Convention does not provide for definition of 'content data', but in paragraph 209 of the Explanatory Report it is stated that 'content data' "refers to the communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data)"[18].

Traffic Data

According to Article 1(d) of the Cybercrime Convention, 'traffic data' means:

> *"... any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service"*

Subscriber Data/ Information

According to Article 18(3) of the Cybercrime Convention, 'subscriber information' means:

> *"...any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:*

---

[18] An example definition of content data can be found in the 'Model Policy Guidelines & Legislative Texts'[18] prepared under the HIPCAR project, which is: *"content data means any data whether in digital, optical, or other form, including metadata, that conveys essence, substance, information, meaning, purpose, intent, or intelligence, either singularly or when in a combined form, in either its unprocessed or processed form. Content data includes any data that conveys the meaning or substance of a communication as well as data processed, stored, or transmitted by computer programs".* Available at: http://hipcar.gov.kn/sites/hipcar.gov.kn/files/HIPCAR_1-2-B_Model_Policy_Guidelines_and_Legislative_Texts_Electronic_Evidence.pdf

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Different from 'content' and 'traffic' data, the subscriber data includes forms of data other than computer data, meaning that it does not, exclusively, have to be in electronic form.

2.4 Procedures Relating to the Collection of Electronic Evidence

2.4.1 Turkish Law

This subchapter will be presenting general information on Criminal Procedure Law in Turkey, followed by related provisions on the collection of electronic evidence.

The main aim of a criminal proceeding is to ensure fact-finding and secure a fair trial in the sense of Article 6 of the ECHR[19]. Criminal proceedings have two phases: investigation and prosecution. Investigation is "the phase that comprises transactions, starting with gaining knowledge of suspicion of a committed crime by competent authorities…, and continuing until the indictment has been approved"[20]. And prosecution is "the phase beginning with the decision on the admissibility of the indictment and ending with the final judgment"[21].

[19] Article 160(2) of the TCPC
[20] Article 2(e) of the TCPC
[21] Article 2(f) of the TCPC

In order to ensure fact-finding and secure a fair trial, collection of evidence takes place during the investigation[22]. Public prosecutor is obliged, through the law enforcement officers, who are under his command, to collect and secure evidence[23]. "In cases where, at the end of the investigation phase, collected evidence constitute sufficient suspicion that a crime has been committed, then the public prosecutor"[24] prepares an indictment. Apparently, collection of evidence is a transaction related to the investigation which, as a rule, shall be kept secret[25] and entered the case records[26]. "The execution of the interactions related to the investigation shall be achieved according to the orders and directions of the public prosecutor"[27]; however, some of the interactions related to the investigation, such as 'interception of correspondence through telecommunication'[28] or 'search of computers, computer programs and transcripts, copying and provisional seizure'[29], require a judge approval or decision. This is, mostly, because such interactions are considered to be coercive measures[30] which serve to the investigation of the factual truth and conclusion of a fair judgment and trial, but yet bring limitations on Constitutional rights and freedoms of people of interest[31]. Under the Turkish Code of Criminal Procedure (TCPC), procedures of electronic evidence collection are regulated as coercive measures.

Although TCPC does not provide for a definition of electronic evidence, procedures related to the collection of electronic evidence are as follows:

---

[22] Article 160(2) of the TCPC
[23] Article 160(2) of the TCPC
[24] Article 170(2) of the TCPC
[25] Article 157(1) of the TCPC is contrary to the rule on the main hearing which is open to the public (Article 182(1) of the TCPC). An example of the secrecy of the investigation is the Article 135(5) of the TPCP which states that interception of communication "decisions rendered and interactions conducted according to the provisions of this article shall be kept confidential while the measure is pending".
[26] Article 169(2) of the TCPC
[27] Article 164(2) of the TCPC
[28] Article 135 of the TCPC
[29] Article 134 of the TCPC
[30] See. The title of the TCPC, First Book, Part Four, in the original text, is 'coercive measures'.
[31] Aydıner, Ö.F., *Avrupa İnsan Hakları Sözleşmesi ve İç Hukukumuzda Koruma Tedbirleri Olarak Tutuklama* (2007), p.21 et seq.

- Search of computers, computer programs and transcripts, copying and provisional seizure (Article 134)

Computers, computer programs and records used by the suspect can be searched, copied and analyzed only if there is a judge decision. This measure can be taken only if it is not possible to obtain evidence by any other mean, in other words, it is applicable as a last resort. Second paragraph of the provision allows for provisional seizure of the computer and equipment, if it is deemed to be necessary for the retrieval and copying of information which are inaccessible- as the passwords are undecipherable- or unreachable- as they are hidden. In case of seizure, a back-up of all the data in the system shall be made. It is also permissible, without seizing the computer or computer records, to copy the data entirely or partially. Copied data shall be printed on paper and this situation shall be recorded and signed by those who are concerned.

- Locating, listening and recording of correspondence (Article 135)

Listening and recording of correspondence and assessment of information related to signals are exclusively applicable to crimes listed under paragraph 6 of the article which are deemed serious[32]. If, during the investigation of a crime that falls within the catalogue, there exist strong grounds of suspicion indicating that the crime has been committed and there is no other possibility to obtain evidence, suspect's correspondence can be located, listened or recorded and information related to signals can be assessed with a decision given by judge or, in case delay is prejudicial, by public prosecutor. However, suspect's correspondence with people who enjoy the privilege of refraining from testimony as a witness[33] shall not be recorded. In such cases, in which this situation has appeared after the recording was conducted, the recordings shall be destroyed immediately. The decision of locating, listening and recording of correspond-

[32] These are mostly crimes against human rights, national security or territorial integrity.
[33] See. Article 45 of the TCPC

ence and assessment of information related to signals "shall include the nature of the charged crime, the identity of the individual, upon whom the measure is going to be applied, the nature of the tool of communication, the number of the telephone, or the code that makes it possible to identify the connection of the communication, the nature of the measure, its extent and duration"[34]. Duration of the measure shall be maximum 3 months, but may be extended once in individual crimes and numerous times in organized crimes[35]. Decisions rendered and interactions conducted according to the provision shall be kept confidential while the measure is pending[36].

- Enforcement of decisions, destroying the contents of the communication (Article 137)

Article 135 of the TCPC sets the principles for interception of communications, whereas Article 137 regulates the application of the interception. The decision rendered according to Article 135 shall be immediately enforced, including the implantation of the relevant devices, by the service provider officers, in cases where it is requested in writing (this would be the 'production order' in the sense of Cybercrime Convention) by the public prosecutor or by the law enforcement officers who has been empowered by the public prosecutor[37]. "The recordings that are produced according to Article 135 shall be decoded and transcribed into written form by individuals who are appointed by the public prosecutor"[38]. In cases where it is decided that there is 'no ground for prosecution'[39] or where judge does not approve the interception decision given by the public prosecutor[40] during the execution of the measure provided under Article 135, the execution of the measure shall be terminated immediately and recordings related to the locat-

[34] Article 135(3) of the TCPC
[35] Article 135(3) of the TCPC
[36] Article 135(5) of the TCPC
[37] Article 137(1) of the TCPC
[38] Article 137(2) of the TCPC
[39] Article 172(1) of the TCPC
[40] Article 135(1) of the TCPC

ing and listening of correspondence shall be destroyed within 10 days[41]. After the recordings are destroyed, the person of interest shall be informed in writing about the reasons, context, duration and outcomes of the measure[42].

- Coincidental evidence (Article 138)

Coincidental evidence is the evidence which is not connected to an ongoing investigation or prosecution but happens to be revealed in the course of a search or seizure or interception of communication carried out in connection to that particular investigation or prosecution. First paragraph of the provision enables the use of coincidental evidence obtained during a search or seizure in another criminal procedure. If such evidence generates reasonable grounds of suspicion that another criminal offense has been committed, it is shall be immediately secured and the public prosecutor shall be informed thereof. Whereas, the second paragraph prohibits the use of coincidental evidence obtained during the performance of interception of communication in the investigation or prosecution of a crime which does not fall under Article 135(6) of the TCPC. In other words, the evidence must raise suspicion of a crime that is listed in Article 135(6) has been committed, so that it may be secured and the public prosecutor may be informed thereof.

- Surveillance with technical means (Article 140)

Business premises of a suspect, as well as his activities conducted in public areas, may be subject to surveillance with technical means, including voice and imagery recordings, provided that, there is no other possibility of obtaining evidence, there exist strong grounds of suspicion indicating that the crime has been committed and the crime being investigated falls under the list provided in the same provision. The decision on surveil-

[41] Article 137(3) of the TCPC
[42] Article 137(4) of the TCPC

lance shall be given by judge or, in case delay is prejudicial, by public prosecutor[43], for up to 4 weeks which may be extended once, if necessary[44]. Surveillance of residence is prohibited[45]. Also the evidence obtained according to this provision cannot be used in the investigation and prosecution of a crime other than those listed in the article[46].

In addition to the regulations under TCPC, there are some other laws and regulations concerning the applications of aforementioned measures providing definitions for the terms used and details about the principles to be followed during their applications which will be covered when relevant.

2.4.2 Cybercrime Convention

The Convention intents to provide a legal basis for the harmonization of domestic criminal substantive law in the area of cybercrime and the domestic criminal procedural law for more effective criminal investigations and proceedings[47]. Chapter II of the Convention regulates "measures to be taken at the national level" and Section 1 provides provisions concerning substantive criminal law. Section 2 on procedural law issues, whereas, is subject to analysis.

According to Article 14(1), each party shall adopt legislative and other measures necessary to establish the powers and procedures for the purpose of specific criminal investigations or proceedings which are applicable to "the collection of evidence in electronic form of a criminal offence"[48]. Establishment, implementation and application of the powers and procedures "which shall incorporate the principle of proportionality"[49] are subject to condi-

[43] Article 140(2) of the TCPC
[44] Article 140(3) of the TCPC
[45] Article 140(5) of the TCPC
[46] Article 140(4) of the TCPC
[47] The Explanatory Report, ¶16
[48] Article 14(1)(c) of the Cybercrime Convention
[49] Article 15(1) of the Cybercrime Convention

tions and safeguards provided for the protection of human rights and liberties[50]. Apart from these common provisions, the Convention provides the following provisions regarding the electronic evidence and related collection procedures:

- Expedited preservation of stored computer data (Article 16)

'Data preservation' means keeping data, which is already stored, secure and safe. In other words, protecting the already stored data "from anything that would cause its current quality or condition to change or deteriorate"[51]. This provision aims to secure the data from being lost and/or intentionally manipulated or deleted by ensuring that the Parties adopt necessary provisional measures to oblige the custodian or other person who is to preserve the computer data, such as businesses or service providers, to maintain the data integrity by means of preservation order for data and/or communications, including the traffic data. Howsoever the data cannot be preserved for a period longer than 90 days, unless a subsequent renewal of the order is provided[52]. In addition to the time limit set out in paragraph 2, Parties are required to introduce confidentiality measures in order to "protect the privacy of the data subject or other persons who may be mentioned or identified in that data"[53].

- Expedited preservation and partial disclosure of traffic data (Article 17)

"Obtaining stored 'traffic data' that is associated with past communications may be critical in determining the source or destination of a past communication, which is crucial to identifying"[54] the perpetrator(s). Even though the provision does not specify the means to preserve traffic data expeditiously, separate preservation order on each service provider can be issued or a single order that would apply to all identified service pro-

[50] Article 15 of the Cybercrime Convention is relatively important as for the provision of adequate level of protection of right to privacy, regulated under Article 8 of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, which will be analyzed in Chapter 3.
[51] The Explanatory Report, ¶151
[52] *supra note*, ¶155 and 156
[53] *supra note*, ¶163
[54] *supra note*, ¶166

viders involved in a specific communication transmission can be served sequentially[55]. Clearly specifying the type of traffic data in the order is crucial in order to obtain a sufficient amount of traffic data that would serve to trace the origin and destination of the communication and to identify the perpetrator[56].

- Production order (Article 18)

Production order is a less coercive measure compared to, for instance, search and seizure of computer data, in which a person or service provider is compelled to provide or submit stored or existing computer data or subscriber information in that person's or service provider's possession or control. By means of production order, telephone number or e-mail address associated with a particular subscriber name or subscriber's name or address associated with a particular telephone number or e-mail address can be requested[57]. Although the provision does not specifically refer to confidentiality, confidentiality is essential as "production order can sometimes be employed as a preliminary measure in the investigation, preceding further measures such as search and seizure or real-time interception of other data"[58].

- Search and seizure of stored computer data (Article 19)

Search of electronic evidence is similar to the search of traditional evidence in two ways: "gathering of the data occurs during the period of the search and in respect of data that exists at that time"[59] and "the precondition for obtaining legal authority to undertake a search is the existence of grounds to believe,… that such data exists in a particular location and will afford evidence of a specific criminal offence"[60]. However, as the computer data is in intangible form and can only be read by certain equipment, the data itself cannot be seized like the traditional evidence. Instead the physical medium, where the data is stored, can be seized. Or a tangible copy of the data, such as print-out, or

[55] *supra note*, ¶168
[56] *supra note*, ¶169
[57] *supra note*, ¶182
[58] *supra note*, ¶175
[59] *supra note*, ¶186
[60] *supra note*, ¶185

copy of the data on a physical medium, such as USB, can be made and then the tangible or physical copy can be seized. A further difficulty in search and seizure of computer data is that the data may not be stored in the particular computer that is searched rather the data can be accessible through an associated data storage device or communication system, like the Internet[61]. Therefore paragraph 2 provides for extension of search and similar access to another computer system or part of it where there is ground to believe that the data required is stored in that other computer system, but only if the other system or part is in the territory of the authority carrying out the search[62]. The provision of information must be reasonable according to paragraph 4 which "may include disclosing a password or other security measure to the investigating authorities"[63]. Nevertheless if disclosure of a password or other security measure threatens the privacy of third parties or other data, then only the necessary information shall be disclosed[64]. By the way, the provision does not touch upon the issue of notification of interested parties[65].

- Real-time collection of traffic data (Article 20)

Real-time collection of traffic data "can correlate the time, date and source and destination of the suspect's communications with the time of the intrusions into the systems of victims, identify other victims or show links with associates"[66]. Traffic data can be collected only if associated communications are specified[67]. It is also important to carry out the collection without the knowledge of the investigated party[68]. Intrusiveness of collection of 'traffic data' in comparison to collection of 'content data' is controversial[69], but it is considered that the 'traffic data' is necessary "to trace the source of a

[61] *supra note*, ¶187
[62] *supra note*, ¶193
[63] *supra note*, ¶202
[64] *supra note*, ¶202
[65] *supra note*, ¶204. As a result there may be disparities among domestic laws.
[66] *supra note*, ¶218
[67] *supra note*, ¶219
[68] *supra note*, ¶225
[69] *supra note*, ¶143

communication as a starting point for collecting further evidence or as part of the evidence of the offence"[70].

- Interception of content data[71] (Article 21)

"Traditionally, the collection of content data in respect of telecommunications (e.g., telephone conversations) has been a useful investigative tool to determine that the communication is of an illegal nature"[72]. The real-time interception of telecommunications is relatively important, as well as the past telecommunications, in order to reveal completed crimes and to prevent the occurrence of crimes that are in the process[73]. This article is an exact parallel of Article 20, so the above explanations apply equally to the interception of content data[74], in fact "the conditions and safeguards applicable to real-time interception of content data may be more stringent than those applicable to the real-time collection of traffic data"[75]. "As interception of content data is a very intrusive measure on private life"[76].

[70] *supra note*, ¶29
[71] For the definition of content data please see ¶229 of the Explanatory Report
[72] The Explanatory Report, ¶228
[73] *supra note*, ¶228
[74] *supra note*, ¶230
[75] *supra note*, ¶231
[76] *supra note*, ¶215

3 PRIVACY CONCERNS RELATING TO THE COLLECTION OF ELECTRONIC EVIDENCE

Human rights and fundamental freedoms may become controversial when it comes to evidence retrieval. As a matter of fact, coercive measures, which are used as means of gathering evidence, are closely related to human rights and fundamental freedoms[77]. This is because coercive measures, such as arrest, custody, search and seizure, bring restrictions on the fundamental rights and freedoms of the suspects and even, in some cases, of the third parties. It is accepted that human rights and fundamental freedoms can be restricted in certain circumstances[78] provided that; for instances, it is necessary in a democratic society in the interests of national security, public safety or for the prevention of disorder or crime. According to Article 13 of the TC;

> "Fundamental rights and freedoms may be restricted only by law and in conformity with the reasons mentioned in the relevant articles of the Constitution without infringing upon their essence. These restrictions shall not be in conflict with the letter and spirit of the Constitution and the requirements of the democratic order of the society and the secular Republic and the principle of proportionality".

Primarily, the right in question shall be determined in order to set the limitations on the use of restriction of rights. Thereby, in terms of procedures for the collection of electronic evidence, especially for search and seizure of computer data and interception of communications, the right to respect for private and family life, in particular, is the one being endangered to a greater extent.

The regulations on right to privacy in the ECHR and TC are parallel. According to Article 8(1) of the ECHR and Article 20(1) of the TC, everyone has the right to respect for his pri-

[77] Human rights and fundamental freedoms referred herein are those granted in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).
[78] Article 18 of the ECHR

vate and family life. However, the respect for correspondence falls under the right to privacy in the ECHR; whereas, it is granted in Article 22 of the TC, under the title of "Freedom of Communication". That is to say, the Article 20 of TC is regulated in a way that it is related to the search and seizure and the Article 22 of TC is rather related to the interception of communication[79].

According to the second paragraph of Article 8 of the ECHR, "…in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others", there can be interference with the exercise of right to privacy. As it is mentioned previously[80], signatories of the Cybercrime Convention have to ensure conditions and safeguards which provide for adequate protection of human rights, in this context such as the right to privacy. Apparently, the main reasoning behind the imposition of the procedures regulated under Chapter II of the Cybercrime Convention is that the applications of the procedures are necessary for the prevention of crime. However, as it will be supported by some court decisions presented in the following chapters, the application of the procedures shall also comply with the necessities of a democratic society and the protection of the rights and freedoms of other individuals.

Moreover, the sole purpose of prevention of crime should not be considered sufficient to interfere with individuals' right to privacy as it may cause an erroneous assumption like as long as the aim of the application of a coercive measure is to prevent crimes, the human rights and fundamental freedoms can be put at stake. In some cases, this erroneous assumption results in exercise of excessive force or discretion by the law enforcement officers. In order to strike a balance between the interest in effective law enforcement and intrusion on the right to privacy, applications of the procedures shall pursue the interests of a democratic

[79] Restriction purposes regulated under Articles 20 and 22 of the TC will be explained separately under Chapters 3.1.1 and 3.1.2.
[80] Please see. Chapter 2.4.2.

society and principle of proportionality. In other words, the coercive measure must be necessary in and proportionate with the concrete case.

Within this context, the analysis on the privacy violations either of the suspect's or the third parties' is a delicate subject which shall be analyzed separately in relation to the regulations on search and seizure of computers and interception of communication under Turkish law. First part of this chapter, will present the issue in relation to Turkish legislation, and the explanations will be supported by the legislations of other states and examples from various states' case-law, especially due to the fact that Turkish case law on the subject is relatively poor. And in the second part, privacy concerns related to the regulations in the Cybercrime Convention will be presented covering both the electronic search and seizure and the interception of communications.

3.1 In Turkish Legal System

3.1.1 Search and Seizure of Computers

"Generally, a warrant is required to search and seize evidence… To obtain warrant, investigators must demonstrate probable cause and detail the place to be searched and the persons or things to be seized. More specifically, investigators have to convince a judge [in the civil-law] or magistrate [in the common-law] that, in all probability: a crime has been committed, evidence of crime is in existence, and the evidence is likely to exist at the place to be searched"[81].

[81] Casey, E. *Digital Evidence and Computer Crime* (2011), p.57

There have been several cases brought before the US Courts on the grounds of unreasonable and/or unlawful search and seizure[82]. Katz v. United States[83] Case is one of the most widely known decision which provides explanations on the interpretations of the unreasonable search and seizure and discussions on the nature of the right to privacy and the legal definition of a search. Although, the Katz decision is on traditional search and seizure, provisions and interpretations relating to the traditional search and seizure are also applicable to the electronic searches. However, in the Turkish legislation there are different provisions for traditional and electronic search and seizure.

When the Turkish case-law is considered, one can see that electronic search has never been challenged on the grounds of violation of right to privacy, instead two issues were addressed: what are the proper conditions for collecting evidence and what techniques shall be used[84]. However the legal problems (not technical) are the main focus of the paper and this section. There are two groups of legal problem relating to the search and seizure of computers associated with privacy: problems arising from legislation and problems that occur during the application.

i) Problems arising from legislation

Article 20(2) of the TC is related to search and seizure; however search and seizure of the computers is not explicitly mentioned in the provision:

> "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 commitment, protection of public health and public morals, or protection of the rights and freedoms of

[82] For instance; People v. Triggs. 8 Cal.3d 884 (1973), United States v. Turner. 98-1258 (1999), Wisconsin v. Schroeder. 99-1292-CR (1999)

[83] 389 U.S. 347 (1967)

[84] 11CD, 16.04.2007, E. 2005/6376, K. 2007/2551

> others, or unless there exists a written order of an agency authorized by law in cases where delay is prejudicial, again on the above-mentioned grounds, neither the person nor the private papers, nor belongings, of an individual shall be searched nor shall they be seized…"

Absence of an explicit reference to computers seems like an omission which raises the question whether computers can be considered as 'belongings' or 'private papers'. However, this absence should not imply that the search and seizure of computers are excluded from the application of this provision; because if the provision is interpreted as it does not include computers, then it would not be possible to claim violation of right to privacy with respect to computer search and seizure.

Computer, which is to be searched or seized, may not be a 'belonging' in the sense of article 20(2); for instance, it may belong to a third party but may be in the physical possession of the suspect. Similarly, the copies made at a computer search, which comprise large amounts of (personal) data, may not be interpreted as 'private papers' in the traditional sense. Therefore either the provision shall be amended in a way that allows computers to fall under the scope of the article or a steady interpretation in line with the above explanations shall be developed by the judiciary.

Furthermore, Article 20(2) of the TC shall be equally applicable, as if the private papers or belongings were being searched or seized, to the cases where it is claimed that during the exercise of a search or seizure of computer the right to privacy is violated. By equal application, it is meant that for the computer search and seizure there shall also be a decision given on the grounds of national security and public order, for prevention of crime, protection of public health and public morals, or protection of the rights and freedoms of others. However, it is important to emphasize that the latest amendments to the Constitution were in 2004, whereas computer search and seizure found its legal basis in 2005 under the TCPC, meaning that after the provision of computer search and seizure, legislatures have not amended the Constitution concordantly; therefore, until such amendment is made inter-

pretation of the Article 20(2) of TC shall allow for taking the developments in the society into account.

Even though the Article 20(2) of TC does not explicitly refer to computers, there are procedural rules relating to the search and seizure of computers under different legislations. The main regulation on computer search and seizure is the Article 134 of TCPC, which is as follows:

> "(1) Upon the motion of the public prosecutor during an investigation with respect to a crime, the judge shall issue a decision on the search of computers and computer programs and records[85] used by the suspect, the copying, analyzing, and textualization of those records, if it is not possible to obtain the evidence by other means.
> (2) If computers, computer programs and computer records are inaccessible, as the passwords are not known, or if the hidden information is unreachable, then the computer and equipment that are deemed necessary may be provisionally seized in order to retrieve and to make the necessary copies. Seized devices shall be returned without delay in cases where the password has been solved and the necessary copies are produced.
> (3) While enforcing the seizure of computers or computer records, all data included in the system shall be copied.
> (4) In cases where the suspect or his representative makes a request, a copy of this copied data shall be produced and given to him or to his representative and this exchange shall be recorded and signed.

[85] Instead of the 'computer records', the word 'log' is more accurate. Pls see. Özbek, V. Ö. *Ceza Muhakemesi Hukuku* (2006), p.363. and Dolar, Y. *CMK'da Bilgisayarlarda, Bilgisayar Programlarında, Bilgisayar Kütüklerinde Arama Ve Elkoyma Müessesesi* (2009)

(5) It is also permissible to produce a copy of the entire data or some of the data included in the system, without seizing the computer or the computer records. Copied data shall be printed on paper and this situation shall be recorded and signed by the related persons".

The provision does not make any reference to probable cause; whereas the general provision on search and seizure specifically states that a physical search on the suspect or search on his belongings, residence, business or other premises can be conducted only if there is probable cause that the evidence may be obtained by such conduct[86]. Imposing a probable cause requirement for the physical search but not for the electronic search seems to be inappropriate.

Besides, both the traditional and the electronic search are regulated under Part II of the Regulation on Judicial and Preventive Search[87] with the title of 'Judicial Search'. Articles 5-16 all refer to judicial search; whereas Article 17 regulates specifically electronic search, oddly, without making any reference to previous provisions on the judicial search.

Additionally, Article 5 provides the definition of judicial search which does not mention computers or other electronic devices at all, same as Article 20(2) of the TC. This definition is particularly important due to the fact that, according to Article 5 of the Regulation probable cause[88] is a precondition only for judicial search, but neither for electronic nor for preventive search there is such precondition.

These two ambiguities raise the question of whether electronic search should be interpreted as a special type of judicial search or as an entirely distinct procedure. If it is regarded as a special type, then the general provisions on judicial search, including the provision on probable cause, will be applicable to the electronic search as well. But if it is interpreted as

[86] Article 116 of the TCPC
[87] Articles between 5 and 17 of the Regulation No. 25832
[88] Article 6 of the Regulation No. 25832

a distinct procedure, such interpretation will constitute a major differentiation, with respect to the preconditions, among different search procedures. Briefly, if the existence of probable cause is not required for electronic search, it will be easier for the law enforcement officers to apply this procedure. In other words, law enforcement officers may resort to electronic search more often even when it is quite obvious that no evidence may be collected from the electronic devices. Thereby, conducting unnecessary electronic search would lead to an increase in the possibility of privacy violations.

Similar criticisms were presented on the subject, such as the regulations on electronic search do not provide for a degree of belief, which may be interpreted as if the existence of a simple suspicion that a crime is committed is sufficient to conduct an electronic search[89]. Furthermore, it is argued that the electronic search and the interception of communications constitute equivalent threat against the privacy; where strong grounds of suspicion is required for the application of interception of communications and simple suspicion of crime is regarded sufficient for the electronic search. Thereby, the respective alteration on the degree of suspicion is inconvenient as for the applications of two equally intrusive measures[90].

Article 19 of the Cybercrime Convention on search and seizure of stored computer data does not explicitly refer to probable cause either, though in paragraph 186 of the Explanatory Report it is stated that;

> "With respect to the search for evidence, in particular computer data, in the new technological environment, many of the characteristics of a traditional search remain…. The preconditions for obtaining legal authority to undertake a search remain the same. The degree of belief required for obtaining legal authorization to

[89] Ozbek, O. *Hukuk Devletinde Bireysel Guvenlik Ekseninde Bilisim Teknolojileri* (2009), p.8
[90] ibid

> search is not any different whether the data is in tangible form or in electronic form."

Similarly, the Fourth Amendment of the U.S. Constitution, which applies to electronic search as well as traditional search, states that;

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".

That is to say, same degree of belief is required for traditional search and electronic search both in the Fourth Amendment and in the Cybercrime Convention. In theory, the possibility of facing privacy violations, by virtue of the degree of belief, are equal in both types of search. Thereby, it seems that the implementations in the Fourth Amendment and in the Cybercrime Convention are more adequate in comparison with the Turkish legislation on this particular subject.

Another inconsistency, arising from the regulatory divergence and increasing the possibility of privacy violations, is that Article 134(1) of the TCPC allows for search on computers, computer programs and logs; whereas Article 17(2) of the Regulation on Judicial and Preventive Search extends the application of search to computer networks, logs on remote computers and other removable electronic devices; such as USB or external hard drive. In the hierarchy of laws, statutes are superior to regulations, meaning that a norm in a regulation cannot be contrary to the norm in a statute which forms the legal basis for that very norm in the regulation[91]. Also the provision in the regulation cannot broaden the scope of

[91] Gözübüyük, Ş. And Tan T., *İdare Hukuku Genel Esaslar* (2001), p.126

the provision[92] in the statute which is exactly the case with article 134 of the TCPC and article 17 of the Regulation on Judicial and Preventive Search. For instance, assuming that upon a decision complying with the requirements in Article 134 of the TCPC and Article 17(2) of the Regulation on Judicial and Preventive Search, a search is conducted on a suspect's computer networks, logs on remote computers or other removable electronic devices[93]. The suspect or his attorney can claim that such search is illicit and the legal basis of the search is in contrast with the general principles of law on the grounds that Article 17 of the Regulation broadens the scope of Article 134 of the TCPC. In this context, the search will be considered illegal; thereby, it is also a violation of suspect's right to privacy.

Lastly, none of the provisions on electronic search provide for an obligation to delete or to destroy the electronic data that have been copied during the search. Obligation to delete or to destroy the collected data is prominent in three situations: a) the data may proved to be irrelevant to the criminal charge, b) at the end of the investigation it may be concluded that there is no evidence with sufficient gravity to justify the suspicion which is required to open a public claim, or there is no legal possibility of prosecution[94] c) the judgment may be an acquittal[95]. The necessity to impose an obligation to delete was stressed in the Turkish doctrine[96], by stating that the absence of such safeguard, especially in terms of the deletion of data relevant to an individual whose innocence has been proved, do not accord with the principle of protection of fundamental rights and freedoms[97].

ii) Problems that occur during the application

1) Extension of the Scope of Search: Applying the rationale used for analyzing privacy concerns in relation to traditional search to the electronic search might be a useful

[92] Yavuzcan, E., *Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma (cmk 134)* (2010)
[93] Provisions are identical, except the variation on devices to be searched.
[94] Article 172(1) of the TCPC- "Decision on no ground for prosecution"
[95] Article 223(1)&(2) of the TCPC
[96] Centel, N. and Zafer, H., *Ceza Muhakemesi Hukuku* (2005), p. 312
[97] Özbek, O. *Hukuk Devletinde Bireysel Güvenlik Ekseninde Bilişim Teknolojileri* (2009), p. 12

way to apprehend and evaluate the problems that occur during the application of electronic search. For these reasons, let's suppose that there has been a murder. In accordance with forensics report and witness statements, the victim was shot with a gun and the suspect had escaped from the crime scene with a red pickup truck, but the murder weapon was not discovered from the crime scene. After the identification of the suspect, police wanted to conduct search on suspect's house and car. Purpose of the search would be discovering the gun used in the crime and other evidence relating to the crime; for instance, plans, photographs or writings indicating that the crime is premeditated. In such scenario, the police have to get a search warrant in accordance with the Article 119 of the TCPC[98] and Article 7 of the Regulation on Judicial and Preventive Search[99].

In order to conduct a legal search it is crucial that there is probable cause that the evidence may be obtained from the place where the search will be conducted[100]. Additionally, the following points must be specified in the search warrant:

- The act which is the ground for the search,

---

[98] "(1) The members of the security forces shall conduct searches upon the order of the judge, or if there is peril in delay, upon a written order of the public prosecutor, if the public prosecutor is not reachable, upon a written order of the superior of the security force. However, searches in private dwellings, business places, as well as other property closed to the public, shall be conducted upon the order of the judge; or in cases where there is peril in delay, upon the written order of the public prosecutor. The outcome of the search conducted upon the written order of the superior of the security forces shall be notified to the office of the public prosecution immediately.
(2) The search warrant or order shall clearly include; a) The conduct that constitutes the ground for the search, b) The person with respect to whom the search shall be conducted, the address of the dwelling or the place to be searched, or the material that is to be searched, c) The time limitation of the validity of the warrant or order.
(3) The open identities of those who have conducted the search shall be included in the document produced after the search.
(4) If private dwellings, business premises or properties that are not open to the public are to be searched without the public prosecutor being present, then two members of the community council in that district or two neighbors shall be called to be present, in order to be entitled to conduct the search.
(5) The search in places assigned for military services shall be conducted by the competent military authorities upon the motion and with the participation of the public prosecutor."
[99] Substantially same with Article 119 of the TCPC, the only difference between provisions is the wording.
[100] Article 116 of the TCPC

- The person with respect to whom the search shall be conducted, the address of the residence or other premises to be searched, or the material that is to be searched,
- The time period in which the warrant is valid[101].

In the given example the act of murder is the ground for the search, there is an identified suspect and the suspect's house and car are the places where the search will be exercised. Concordantly, if the validity period of the search, together with the above mentioned information, is written in the warrant, the search will be formally legal.

So what would it be like if the same rationale is applied to an electronic search? Let's take child pornography as an example. A person is suspected of possessing child pornography material and in line with the previous explanations[102] assuming that there is probable cause to conduct an electronic search, some questions come to mind: what should be the scope of the search and how should it be determined?

In the murder example, murder weapon is the main evidence that is searched by the police, suspect's house and car are the places to search, meaning that the scope of that search is pretty much precise. On the other hand, it is not that simple to be precise when it comes to electronic search.

Suspect's computer is naturally the main source of evidence, but they can be found anywhere within the computer system and even in the networks, logs on remote computers and other removable electronic devices; therefore investigators come across with a great amount of electronic data.

[101] Article 119 of the TCPC
[102] See Chapter 3.1.1.

Geographical scope of a search (warrant) and volume of the data subject to search are the problems faced by the law enforcement[103]. For the very reason, investigators always have to keep in mind what is being searched for which is in the given example the child pornography material. Any data irrelevant to child pornography, such as files relating to suspect's work, should not be searched that, otherwise, may constitute a violation of privacy.

"Different cybercrimes [all kinds of crimes] result in different types of digital evidence. For example, cyberstalkers often use e-mail to harass their victims, computer crackers sometimes inadvertently leave evidence of their activities in log files, and child pornographers have digitized images stored on their computers. Additionally, operating systems and computer programs store digital evidence in a variety of places. Therefore, the ability to recognize digital evidence depends on an investigator's familiarity with the type of crime that was committed and the operating system(s) and computer program(s) that are involved"[104]. Thereby, in order not to interfere with the right to privacy, investigators carrying out the search shall be familiar with the types of electronic evidence, such as .doc (text), .jpg (image) and .wmv (video) files, and the operating system(s) and computer program(s).

Issues related to the scope of electronic search were discussed in the Bradley v. State of Delaware Case (2012). Briefly, in the case, based on several patient complaints of sexual misconduct against former pediatrician Bradley and the information provided from different sources, the police applied a search in Bradley's business premises to obtain electronic evidence indicating the alleged sexual misconduct. Various electronic devices and files were discovered, not just related to the sexual misconduct allegations but to child pornography as well. At the appeal, Bradley claimed that "the warrant itself was defective because the affidavit in sup-

[103] Walden, I. *Computer Crimes and Digital Investigations* (2007), p.277&278
[104] Casey, E. *Digital Evidence and Computer Crime* (2000), p.48

port of the search warrant application did not allege facts establishing probable cause that the patients' medical files would be found in a white outbuilding on the BayBees Pediatrics property, would be contained in digital format, or would relate to the crimes described in the search warrant application. Bradley also contends that the police exceeded the scope of the search warrant by proceeding with a general search to locate and seize evidence without probable cause". However, the Court concluded that Bradley's claims lack merit on the grounds that "the affidavit of probable cause alleged sufficient facts to support the search warrant …, the actions of the police officers in executing the search warrant were reasonable and within the bounds of the warrant issued".

Arguments and explanations asserted in the Court decision are very much useful to comprehend and determine boundaries of a legal electronic search that will have direct impact on cases in which the right to privacy is claimed to be infringed on the grounds of unreasonable or illegal search.

Another consequence of not setting precise boundaries to the scope of a search may be the privacy violation claims from third parties; for instance, during a search on a suspect's private computer, work related documents may be found by the investigators or a search can be conducted on suspect's office computer, which is supposed to be used for work only, but that is not often the real situation. In such cases, it is not just the suspect's right to privacy what is endangered, it is the employers', other employees', clients'… etc. rights to privacy that are also put at stake with the application of the search. Similarly, a computer may be used by multiple users, therefore when a search is carried out on that common computer, other users' may claim privacy violations, if the scope of the search is not carefully and precisely set[105].

[105] For further explanation on drafting, obtaining, and executing search warrants with respect to electronic evidence; please see Ferraro, M. M., and Casey, E., *Investigating Child Exploitation and Pornography: The Internet, Law and Forensic Science* (2004).

2) Coincidental Evidence Collected at Electronic Search: "Digital investigators are generally authorized to collect and examine only what is directly pertinent to the investigation"[106], in other words the main focus of the search shall be the crime under investigation and evidence relating to that crime. However, according to Article 138(1) of the TCPC; "If a search or seizure reveals an evidence that is not connected to the current investigation or prosecution, but there are reasonable grounds of suspicion that another criminal offense was committed, those items shall be immediately secured and the public prosecutor shall be informed thereof". This possibility provided by Article 138(1) may be used to conduct general, exploratory search[107] which may result in breach of right to privacy.

As noted above in the Turkish legislation, in terms of electronic search, there is not a requirement, like having grounds to believe that evidence may be obtained by the conduct of an electronic search. Absence of such ground may constitute a threat against right to privacy with respect to coincidental evidence, together with the reasons presented in the above chapters. Since, without the obligation to fulfill such requirement, the investigators may search the unnecessary and/or irrelevant parts of a computer system, just to gather coincidental evidence indicating or revealing other crimes. In that case, the main purpose of the search is not collecting electronic evidence relating to the crime that is being investigated, but instead gathering as much evidence as possible against the suspect indicating that he committed other crimes.

In the Turkish doctrine, it is suggested that due to the ease in gathering coincidental evidence and the risk of facing with the 'fruit of the poisonous tree' doctrine, the electronic search and seizure shall be limited to certain serious crimes, similar with

[106] Casey, E., *Digital Evidence and Computer Crime* (2011), p.235
[107] For further explanations on general search see; Galloway, Jr. R. W., *The Uninvited Ear: The Fourth Amendment Ban On Electronic General Searches* (1982)

the regulations on interception of communication, which may be a better safeguard for the right to privacy[108].

In the US legal system coincidental evidence does not exist as a concept. The cases, in which evidence indicating other crimes is to be found in course of a search, are dealt according to a doctrine, developed in the Coolidge v. New Hampshire Case (1971), called the 'plain view'.

"An example of the applicability of the 'plain view' doctrine is the situation in which the police have a warrant to search a given area for specified objects, and in the course of the search come across some other article of incriminating character"[109]. In other words, "...under certain circumstances the police may seize evidence in plain view without a warrant"[110]. However; "the plain view doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges"[111]. "The extension of the original justification is legitimate only where it is immediately apparent to the police that they have evidence before them"[112]. In the United States v. Carey (1998) and the United States v. Comprehensive Drug Testing, Inc. (2009) cases, the plain view doctrine is discussed in detail with respect to electronic searches.

In the United States v. Carey (1998)[113], "…the investigator found child pornography on a machine while searching for evidence of drug-related activity but the images were inadmissible because they were outside of the scope of the warrant"[114]. Based on the characteristics of the case, the Court decided that the investigator had

[108] Özbek, O., *Hukuk Devletinde Bireysel Güvenlik Ekseninde Bilişim Teknolojileri* (2009), p.8
[109] United States v. Comprehensive Drug Testing, Inc. (2009)
[110] ibid
[111] United States v. Carey. (1998)
[112] United States v. Comprehensive Drug Testing, Inc. (2009)
[113] United States v. Carey. (1998)
[114] Casey, E., *Digital Evidence and Computer Crime* (2011), p.59

exceeded the scope of the warrant, stating that "seizure of the evidence upon, which the charge of conviction was based, was a consequence of an unconstitutional general search, and the district court erred by refusing to suppress it"[115]. However, it is also stated that the "results are predicated only upon the particular facts of this case, and a search of computer files based on different facts might produce a different result"[116].

Whereas, in the United States v. Comprehensive Drug Testing, Inc. (2009), which raised many questions about procedures to be followed in electronic search, "…the court set out guidelines for electronic searches and seizures so that the 'plain view' doctrine did not allow electronic fishing expeditions. The guidelines followed an approach that is routinely used for electronic surveillance. However, on rehearing the case following objections from government prosecutors, the court's new opinion removed the guidelines though it still concluded that the search at issue was impermissible"[117]. Judge Bea, who had partially agreed and partially disagreed with the decision, stated that: "A valid 'plain view' seizure of items that are truly 'immediately apparent' would have required the agent to display only the testing results for the ballplayers for whom he had a warrant, and seize only evidence of additional illegality if such evidence is 'immediately apparent' as part of the segregated results for those ballplayers"[118]. This case is of great importance; because the "…Court recommended stricter controls for forensic analysis of digital evidence, challenging the concept of plain view in the digital dimension and suggesting approaches to reduce the risk of associated privacy violations"[119].

---

[115] United States v. Carey. (1998)
[116] ibid
[117] http://epic.org/2010/09/ninth-circuit-strips-search-gu.html
[118] United States v. Comprehensive Drug Testing, Inc. (2009)
[119] Casey, E., *Digital Evidence and Computer Crime* (2011), p.59

3) Seizure of electronic evidence: In accordance with the Article 134 of TCPC, law enforcement officers can seize the copies of computer records, computers and equipment in course of an electronic search. Copies of the computer records can be seized if it is permitted in the decision given by the judge[120]. In the second paragraph of the same provision, it is stated that computers and equipment can be seized if it is deemed to be necessary for the retrieval and copying of information which are inaccessible- as the passwords are undecipherable- or unreachable- as they are hidden. However, operating systems, user names and passwords are not necessary for analyzing computers as a part of digital forensics. Therefore, in reality, seizure applies not because the passwords are undecipherable, but because the search and analysis of the evidence takes a long time. The provision shall be amended corresponding to the characteristics of digital forensics.

4) Amount of the seized electronic data: "Electronic surveillance presents additional problems. It is a sweeping form of investigatory power. It extends beyond a search, for it records behavior, social interaction, and everything that a person says and does. Rather than a targeted query for information, surveillance is often akin to casting a giant net, which can ensnare a significant amount of data beyond that which was originally sought"[121].

The amount of information collected as evidence and seized in the course of an electronic search was in fact at issue in a recent case[122] in Norway. In the case brought before the Norwegian High Court, there were two suspects and the police conducted a search on one of the suspects' computer. The hard disk and the other 'physical storage media' were seized by the police and a mirror image of the docu-

[120] Article 134(1) of the TCPC
[121] Solove, D.J., *Reconstructing Electronic Surveillance Law* (2004), p. 1279
[122] HR-2011-1744-A

ments was made, and then the devices were returned to the suspect. However 16 million computer files, in total, were obtained, so that an automatic search by using key words, file extensions and location had to be run on all the files and only the relevant files are included in the case documents/records.

According to Section 264 of the Norwegian Criminal Procedure Act, "…the prosecuting authority shall send a copy of the indictment and the summary of the evidence to defense counsel together with the documents relating to the case". In the case, both of the defendants requested the copies of the all 16 million documents obtained from the search due to the principles of equality of arms and the right to contradiction, as provided for by the right to get a copy of the case documents in Section 264.

However their requests were denied. The reasons of denial were different for each defendant. For the defendant whose computer was searched the reason of the denial was that his computer had been returned thereby he already had the source of data and there was no need to copy 16 million documents. Whereas for the other defendant, the Court said that he can be provided with the copies of the documents which had been picked out by the automatic search, but his request had to be denied for the rest of the documents on the grounds that the grant of access to the irrelevant documents may amount to the violation of the privacy of third parties who had interaction with the defendant, whose computer was searched, through his computer. But the case also shows that the obtainment of a large quantity of data does not necessarily mean that the police have a great quantity of information. If the police had looked through all the data, then all the files had to be copied and included as part of the case documents.

The huge storage capacity of the electronic devices bring along the difficulty of dealing with a great amount of information which have to be carefully evaluated in the course of an electronic search and seizure. Clearly, relevance is a significant is-

sue that sets the boundaries for the protection of the right to privacy of the suspects and the third parties.

3.1.2 Interception of Communications

According to Article 22(1) of the TC, "everyone has the right to freedom of communication". Although, "secrecy of communication is fundamental"[123], 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 others"[124], the right to freedom of communication can be restricted with a duly given judge decision. Otherwise, communication shall not be impeded and its secrecy shall not be violated[125].

Communication can be intercepted if one or more of the aforementioned reasons exist. The interception can be judicial or pre-emptive. If the communication is intercepted in the course of criminal investigation for the collection of evidence, then it is called judicial interception which finds its legal basis in the TCPC. Whereas; when the interception takes place for intelligence purposes or to prevent certain serious crimes that have the potential to endanger the constitutional order and public security, it is called interception for intelligence purposes, pre-emptive interception or administrative interception[126]. The European Commission emphasizes the importance of establishing sound legal framework on the interception of telecommunications, by stating that "a clear distinction between judicial interception and interception for intelligence purposes needs to be made, in line with European best practices. Appropriate control mechanisms need to be put in place to ensure that these tools are not misused"[127].

---

[123] Article 22(1) of the TC
[124] Article 22(2) of the TC
[125] Article 22(2) of the TC
[126] Yenisey, F., *Çıkar Amaçlı Örgüt Suçlarındaki Araştırmalar* (2000), p.118; Şen, E., *İletişimin Denetlenmesi Tedbiri* (2007), p.101.
[127] European Commission, *Commission Staff Working Document* (2012), p.34

Although pre-emptive interception is not a mere criminal procedure and this study focuses on criminal investigation procedures, the application of pre-emptive interception, in accordance with the existing regulation, constitutes a great threat against the right to freedom of communication and the right to privacy, therefore it is noteworthy to, briefly, take a look at it.

The pre-emptive interception of communication was put into effect with the Law No.5397 amending Law No. 2559 on 'Police Duty and Authority', Law No. 2803 on 'Military Police Organization, Duty and Authority' and Law No. 2937 on 'Government Intelligence Services and National Intelligence Organization'. With the Law No.5397, the police, military police and National Intelligence Organization are authorized to intercept communication[128]. Within the scope of the interception, these organizations are allowed to locate, listen and/or record communications and/or evaluate the information on signals, but they are not allowed to locate mobile phones as the aim in the pre-emptive interception is not catching a suspect(s). The measure is applicable for all types and means of communication; however there is not a limitation on to whom it may be applicable, in other words it can be applicable to anyone who is likely to commit a crime. Additionally, the regulation on pre-emptive interception does not provide for any degree of suspicion. The pre-emptive interception is applicable any time and does not have to be applied as a last resort, meaning that even if it is possible to prevent the occurrence of a crime by other means, this measure may be taken[129]. Furthermore, there is no safeguard providing that the person, whose communication was intercepted, shall be informed at any point either during the exercise of the measure or afterwards[130].

---

[128] The police and military police are authorized to intercept communications for the prevention of the crimes listed under article 250(a), (b) and (c) of the TCPC, except spying, and the National Intelligence Organization is authorized to intercept communications if there is a serious threat against the principles stated under article 2 of the TC in order to ensure national security, reveal the acts of espionage, determine the disclosure of state secrets and prevent terrorism. Pls. see additional article 7 of the Law No. 2559, additional article 5 of the Law No. 2803 and amended article 6 of the Law No. 2937

[129] Taşkın, M., *Türk Hukukunda Adli ve Önleme Amaçlı İletişimin Denetlenmesi: Sorular ve Çözüm Önerileri* (2010), p.496

[130] ibid, p.497

Going back to the judicial interception, the main principles for this type of interception are regulated under Article 135 of the TCPC[131]. Enforcement of the decisions rendered in accordance with Article 135 and destroying of the contents of the communication are regulated in Article 137 of the same Code. Besides, in 2005, 'Regulation on the Principles and Procedures Relating to the Locating, Listening and Recording of Correspondence through

[131] "(1) The judge or, in cases of peril in delay, the public prosecutor, may decide to locate, listen to or record the correspondence through telecommunication or to evaluate the information about the signals of the suspect or the accused, if during an investigation or prosecution 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 judge for his approval and the judge shall make a decision within 24 hours. In cases where the duration expires or the judge decides the opposite way, the measure shall be lifted by the public prosecutor immediately.
(2) The correspondence of the suspect or the accused with individuals who enjoy the privilege of refraining from testimony as a witness shall not be recorded. In cases where this circumstance has been revealed after the recording has been conducted, the conducted recordings shall be destroyed immediately.
(3) The decision that shall be rendered according to the provisions of subparagraph 1 shall include the nature of the charged crime, the identity of the individual, upon whom the measure is going to be applied, the nature of the tool of communication, the number of the telephone, or the code that makes it possible to identify the connection of the communication, the nature of the measure, its extent and its duration. The decision of the measure may be given for maximum duration of 3 months; this duration may be extended one more time. However, for crimes committed within the activities of a crime organization, the judge may decide to extend the duration several times, each time for no longer than one month, if deemed necessary.
(4) The location of the mobile phone may be established upon the decision of the judge, 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 decision related to this matter shall include the number of the mobile phone and the duration of the interaction of locating (the establishment). The interaction of locating shall be conducted for maximum of three months; this duration may be extended one more time.
(5) Decisions rendered and interactions conducted according to the provisions of this article shall be kept confidential while the measure is pending.
(6) The provisions contained in this article related to listening, recording and evaluating the information about the signals shall only be applicable for the crimes as listed below:
a) The following crimes in the Turkish Criminal Code; 1. Smuggling with migrants and human trafficking (Arts. 79, 80), 2. Killing with intent (Arts. 81, 82, 83), 3. Torture (Arts. 94, 95), 4. Sexual assault (Art. 102, except for subsection 1), 5. Sexual abuse of children (Art. 103), 6. Producing and trading with narcotic or stimulating substances (Art. 188), 7. Forgery in money (Art. 197), 8. Forming an organization in order to commit crimes (Art. 220, except for subsections 2, 7 and 8), 9. Prostitution (Art. 227, subparagraph 3), 10. Cheating in bidding (Art. 235), 11. Bribery (Art. 252), 12. Laundering of assets emanating from crime (Art. 282), 13. Armed criminal organization (Art. 314) or supplying such organizations with weapons (Art. 315), 14. Crimes against the secrets of the state and spying (Arts. 328, 329, 330, 331, 333, 334, 335, 336, 337).
b) Smuggling with guns, as defined in Act on Guns and Knives and other Tools (Art. 12),
c) The crime of embezzlement as defined in Act on Banks, Art. 22, subparagraphs (3) and (4),
d) Crimes as defined in Combating Smuggling Act, which carry imprisonment as punishment,
e) Crimes as defined in Act on Protection of Cultural and Natural Substances, Arts. 68 and 74.
(7) No one may listen and record the communication through telecommunication of another person except under the principles and procedures as determined in this Article."

Telecommunications and Evaluation of Information on Signals and the Establishment, Duties and Authority of the Telecommunications Directorate' (Regulation No. 25989) and in 2007, 'Regulation on the Application of Interception of Correspondence Through Telecommunications, Undercover Investigator and Surveillance with Technical Means Provided in the Code of Criminal Procedure' (Regulation No. 26434) were put into force.

Aim of the Regulation No. 25989 is to provide more detailed regulation on the procedures and principles related to- both judicial and pre-emptive- interception of communication[132]; however, apart from the provision on definitions[133] and the regulation related to the establishment, duties and authorities of the Telecommunication Directorate[134], it is hardly possible to say that the Regulation introduces further regulation on interception. Whereas, Article 1 of the Regulation No. 26434 states the aim of the Regulation as; to set principles and procedures that are applicable to the requests and decisions related to and applications of the following measures: interception of communications, undercover investigator and surveillance with technical means, and as a matter of fact, it does bring detailed provisions. Nevertheless, there are some inconveniences emerging from the legislation on judicial interception of communication, but it shall be born in mind that all the explanations below relate to Article 135 of the TCPC, as it sets the framework, unless another provision is specifically mentioned.

In the course of interception the following activities may be carried out: locating[135], listening and recording of the communications[136], evaluating the information about the signals[137]

---

[132] Article 1(a) of the Regulation 25989
[133] Article 3 of the Regulation No. 25989
[134] Article 16 et seq. of the Regulation No. 25989

[135] Article 3(i) of the Regulation No. 25989 and article 4(f) of the Regulation No. 26434- 'Location of communication': Activities directed to locate data relating to outgoing calls, incoming/received calls, geographical location, and identity, without interfering with the content of the communication.

[136] Article 3(h) of the Regulation No. 25989 and article 4(e) of the Regulation No. 26434- 'Listening and recording of the communication': Activities directed to the listening and recording of the conversations or all other sorts of communication carried through telecommunications by appropriate technical means.

and locating mobile phones. Article 135 of the TCPC provides two important safeguards for the protection of the right to privacy and the freedom of communication. Firstly, different from the provision on electronic search and seizure, the judicial interception is applicable only if there are strong grounds of suspicion indicating that the crime has been committed. And secondly, recording of the correspondence between the suspect or the accused and the individuals who enjoy the privilege of refraining from testimony as a witness[138] is prohibited. This prohibition could constitute a remarkable safeguard for the protection of the right to privacy as the people listed under Article 45 of the TCPC are immediate family, but if the prohibition had included the locating and the listening of the communications[139], together with the recording of communications. In this sense, existing wording of the provision is open to exploitations[140].

The interception of communication is applicable only if there is no other possibility to obtain evidence which is interpreted as 'last resort' in the Turkish doctrine; in practice, however, it may cause abusive applications.

According to Article 4(c) of the Regulation No. 26434, just the expectation of not being able to obtain evidence by other means is sufficient for fulfilling the requirement of not having any other possibility to obtain evidence. That is to say, if it is expected that the investigation will not be successful by the exercise of so called 'classical measures', such as arrest, interview or seizure, or the effort made to get successful results from the classical measures is burdensome, then it is considered that there is no other possibility of gathering evidence[141]. In such case, the investigators do not have to, firstly, apply other measures and

---

[137] Article 3(p) of the Regulation No. 25989 and article 4(h) of the Regulation No. 26434- 'Information on signals': All kinds of data processed for the transmission of communication within a network and for billing purposes. and article 4(ı) of the Regulation No. 26434- 'Evaluation of the information on signals': Activities carried out, within the scope of the decision given by the authorities, to trace and give meaning to the signals left in communication networks without interfering with the communication.
[138] Article 45 of the TCPC
[139] Yavuz, H.A., *Ceza Yargılamasında Bir Koruma Tedbiri Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi* (2005), p.249
[140] ibid
[141] Kunter, N. and Yenisey, F., *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku* (2002), p. 640.

then prove that they could not get any result by such conduct. It is possible to directly apply interception of communication[142], not as a 'last resort'. Thereby, the application of this requirement is rather subjective and subject to arbitrariness and exploitation which, in this way, could not serve as an objective and adequate safeguard for the protection of the right to privacy.

Although the interception of communication is a measure that is applicable for the collection of evidence, which is essentially an investigative activity, it is possible to apply this measure also during the prosecution. Prosecution is "the phase beginning with the decision on the admissibility of the indictment and ending with the final judgment"[143]. According to Article 170 (2) of the TCPC, "in cases where, at the end of the investigation phase, collected evidence constitute sufficient suspicion that a crime has been committed, then the public prosecutor shall prepare an indictment" which shall contain, along with some other points[144], the "evidence of the offense"[145]. If the prosecution has begun, this would mean that the collected evidence is sufficient to give a judgment[146]. In that case, applying or conducting new measures should not be a necessity anymore, but if it is still necessary to apply coercive measures to reveal the facts then it should not be proceeded to the prosecution[147]. In this respect, it is correct to say that the interception applied during the prosecution does not merely pursue the aim of fact-finding. In other words, the aim of the prosecution is to decide, based on the existing evidence, whether the accused committed the alleged crime(s), whereas the aim of the coercive measures is fact-finding which is specific to the investigation phase. Therefore, the application of such an intrusive measure during the prosecution is not proportionate with the targeted aim of the measure itself. According to Article 13 of the TC, the restriction shall not be contrary to the principle of proportionality

---

[142] Yavuz, H.A., *Ceza Yargılamasında Bir Koruma Tedbiri Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi* (2005), p.247
[143] Article 2(f) of the TCPC
[144] See. Article 170(3) of the TCPC
[145] Article 170(3)(j) of the TCPC
[146] Taşkın, M., *Türk Hukukunda Adli ve Önleme Amaçlı İletişimin Denetlenmesi: Sorular ve Çözüm Önerileri* (2010), p.490
[147] Taşkın, M., *Adlî ve İstihbarî Amaçlı İletişimin Denetlenmesi* (2008), p.98

which, otherwise, would constitute a violation of the right in question. Disproportionate application of interception would amount to violation of right to privacy and freedom of communication.

Another inconvenience, resulting from the way that Article 135 of the TCPC has been regulated, is related to the extension of the duration of the interception decision. If the interception decision is given in order to collect evidence relating to the crimes committed within the activities of a criminal organization, the duration of the interception decision may be extended several times, if deemed necessary[148]. However neither of the regulations state when or under what conditions extension is deemed to be necessary, and also there is not a limitation on how many times the decision of interception can be extended. So in such case one may consider that extension is necessary until some evidence is obtained. But is it convenient to extend the decision and continue to apply interception forever? The answer shall be no to that question, because such an application would be excessive and arbitrary, and it would possibly result in violations of right to privacy and freedom of communication[149].

In Klass and Others v. Germany Case (1978), the European Court of Human Rights (ECtHR) established significant principles that shall be followed both during the enactment and the application of surveillance measures, namely interception of communications. In its judgment, the Court accepted that surveillance provided for under the national legislations "…amount to an interference [by the public authorities] with the exercise of the right set forth in Article 8 para.1" of the ECHR. Thereby, "the cardinal issue arising under Article 8"[150] was addressed as "whether the interference so found is justified by the terms of paragraph 2 of the Article"[151]. Since the second paragraph of the article provides an exception to the right to privacy, the Court laid emphasis on the narrow interpretation of the excep-

[148] Article 135(3) of the TCPC
[149] Yiğit, N., *Arama, Elkoyma ve Gizli Koruma Tedbirleri* (2005), p.26&27
[150] Klass and Others v. Germany Case (1978)
[151] ibid

tion by stating that the "powers of secret surveillance of citizens … are tolerable under the Convention [ECHR] only in so far as strictly necessary for safeguarding the democratic institutions"[152]. "In order for the 'interference' … not to infringe Article 8 (art. 8), it must, according to paragraph 2 (art. 8-2), first of all have been 'in accordance with the law'"[153]; however it still remains to be determined whether the other requisites laid down in paragraph 2 of Article 8 (art. 8-2) are also satisfied. That is to say, in each case it shall be determined whether the application of interception of communication is necessary in a democratic society for one of the purposes enumerated in the paragraph. Although the Court leaves to the domestic legislature a certain degree of discretion on determining the surveillance systems and policies, it also stresses that "whatever system of surveillance is adopted, there [has to] exist adequate and effective guarantees against abuse"[154]. The assessment of whether there exists adequate and effective guaranties shall be done on a case-by-case basis "as [to] the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law"[155].

Furthermore, in Malone v. the United Kingdom Case (1984), the ECtHR reinforced its approach about the interception of communications and developed the following interpretation on the phrase 'in accordance with the law':

> "The Court would reiterate its opinion that the phrase 'in accordance with the law' does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention [ECHR] … The phrase thus implies - and this follows from the object and purpose of Article 8 (art. 8) - that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph 1 (art. 8-1)…"

[152] ibid
[153] ibid
[154] ibid
[155] ibid

These approaches have been pursued by the ECtHR in the later cases[156], in which, it is inferred that "…tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated"[157].

3.2 Under Cybercrime Convention

3.2.1 Criticisms against the Convention

The Convention, especially during its drafting process, faced much criticism from privacy groups and civil liberties organizations, most of which are established in the US. In 2005, Marc Rotenberg- at the time the EPIC[158] President- and Cédric Laurant- at the time the EPIC Director, International Privacy Project, Policy Counsel- released the 'EPIC Statement on COE Cybercrime Convention, Treaty 108-11' and put forth the following criticisms against the Convention;

- *The Convention Lacks Adequate Safeguards for Privacy*: "The treaty would create invasive investigative techniques while failing to provide meaningful privacy and civil liberties safeguards, and specifically lacking judicial review and probable cause determinations required under the Fourth Amendment. A significant number of provisions grant sweeping investigative powers of computer search and seizure and government surveillance of voice, e-mail, and data communications in the interests of law enforcement agencies, but are not counterbalanced by accompanying protections of individual rights or limit on governments' use of these powers".

[156] See. Halford v. the United Kingdom Case (1997) and P.G. and J.H. v. the United Kingdom Case (2001)
[157] Kopp v. Switzerland Case (1998)
[158] The Electronic Privacy Information Center

- *Vague and Weak Privacy Protections*: "This provision [Article 15 of the Cybercrime Convention] is quite vague, and is not reiterated with specific and detailed protections within any of the specific provisions. For example, provisions on expedited preservation of stored computer data and expedited preservation and partial disclosure of traffic data make no mention of limitations on the use of these techniques with an eye to protection of privacy and human rights. Furthermore, the vagueness of this provision (and others) introduces the risk of enhancement of the flaws and benefits of the Cybercrime Convention overall, as the Convention is transposed into the laws of ratifying countries which may have drastically different pre-existing privacy and human rights protections".
- *Insufficient Recognition of International Human Rights Obligations:* "Examination of the Preamble is extremely illuminating on this point, with eight clauses related to the interests of law enforcement, crime-prevention, and national security, and only two oriented toward protection of privacy and human rights. Coupled with the lack of consideration of, and compliance with, important international conventions on human rights, it becomes clear that the Cybercrime Convention is much more like a law enforcement 'wish list' than an international instrument truly respectful of human rights".

The abovementioned criticisms are justifiable for the states which are party to the Cybercrime Convention but not to the ECHR, such as Canada, Japan, South Africa and USA; because although Article 15 of the Cybercrime Convention requires the parties to respect human rights and freedoms, the rights and safeguards afforded by the states, which are not party to the ECHR, may not be adequate to the rights and protection measures afforded by the parties to the ECHR. In other words, Article 15 does not provide for a harmonized protection system equally applicable in all the signatory states[159].

[159] The list of signatory states to the ECHR is available at:
http://conventions.coe.int/treaty/Commun/ChercheSig.asp?NT=005&CM=&DF=&CL=ENG
And the list of signatory states to the Cybercrime Convention is available at:
http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

Most of the criticisms against the Convention center upon the new powers acknowledged to law enforcement to conduct investigations and surveillance. It is strongly argued that the procedural rules undermine individual privacy rights and expand surveillance powers too far[160]. Moreover, it is also stated that the Convention does not place explicit limits on the powers and does not create mechanisms to ensure that the powers are not being misused[161]. David Banisar, who is a lawyer and consultant in the Washington, DC area, and Gus Hosein, who is a visiting fellow at the London School of Economics, name this model created by the Convention as the '*High-Investigative-Powers/ Low-Rights-Protections'*[162].

3.2.2 Proposed Recommendations

David Banisar and Gus Hosein recommend that the model of '*High-Investigative-Powers/ Low-Rights-Protections'* shall be reversed to a model "where *High-Investigative-Powers* can be sought because *High-Rights-Protections* are already assured"[163]. If this cannot be achieved, then at least "a model that grants a base-case, basic necessities in cybercrime legislation, and then lets signatory states, at their own discretion without international pressure through the ambiguous formulation of the requirements of this convention, manage and interpret what is required for their national interests"[164] shall be adopted. They call it '*Adequate-Investigative-Powers/ Adequate-Rights-Protections'* model. By virtue of such model, individuals' rights are expected to uphold the highest form of protection[165].

As it is suggested by the authors, an example of adequate protection may be, "when the CoE [Cybercrime Convention] mentions 'empowering' competent authorities for investigation…, [it] must [be] ensure[d] at the early stages that the clause is included: 'with signifi-

---

[160] Archick, K. *Cybercrime: The Council of Europe Convention* (2004), p.3
[161] Banisar, D. and Hosein, G., *A Draft Commentary on the Council of Europe Cybercrime Convention* (2000)
[162] ibid
[163] ibid
[164] ibid
[165] ibid

cant controls, i.e. judicial warrants, and under probable cause based on evidence acquired elsewhere.' This is a philosophical point, but must be mentioned early on, and not as some add-on. Otherwise this convention is all about granting powers to law enforcement agencies, and dismisses the CoE's [Cybercrime Convention's] own claim to be respectful of human rights. In creating a legislative infrastructure for searching, surveillance, and seizure, to not discuss the constraints on such a system denies all that we have learned about political systems. To leave it up to national discretion basically mandates increasing powers, while not raising the levels of protection of individuals"[166].

Similarly, the Global Internet Liberty Campaign (GILC) has also proposed some recommendations in the 'Member Letter' that they had published in 2000, even before the Convention was opened for signature. In spite of the fact that the Convention underwent tremendous amendments, some issues raised back then still keeps their actuality and validity. The recommendations which may as well stand today are as follows:

- the use of invasive powers must be applied only to serious crimes,
- the concept of 'proportionality' must be defined at the international level, and agreed uniformly and unilaterally,
- a consistent regime of civil liberties protections must be added,
- clear limits shall be set to the powers involving situations where civil liberties are compromised,
- a clear definition of 'content data' shall be provided with and it shall be clearly differentiated from the 'traffic data',
- the powers of interception and data gathering devices shall be limited so as to absolutely limit the invasiveness- "…if technical means are used, these means must separate out the traffic of the specific user under investigation, gather only the legally

[166] ibid

permitted amount of data, disallow tampering, and respect the shifting division between content and traffic data…"[167],

- the difference between retention and preservation of data requires explicit protections.

The GILC also stated that the traffic data collection is as invasive as the interception of content data; therefore, it urges sufficient uniform constraints prior to the collection. With respect to investigative powers, it is argued that "…the Convention must also establish a maximum threshold of investigative techniques that are acceptable; unjudicious access and data warehousing are gross invasions of civil liberties"[168].

[167] GILC, *Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime Version 24.2* (2000)
[168] ibid

4 CONCLUSION

Electronic evidence is any probative information stored or transmitted in digital form and is different from traditional evidence in following aspects: may change within a computer and/or transmission line at any moment, may be easily altered without leaving any trace, is easily changeable/distortable during its collection, may not be perceived at first sight, needs to be transformed to a humanly readable form, may be obtained to the amount it is recorded and much effected by the velocity of technology.

Turkish law neither mentions electronic evidence nor provides a categorization based on the types of electronic evidence as in the Cybercrime Convention. Despite the deficiencies, such as the absence of definition of 'content data', structure in the Convention is clearer and more appropriate, thereby adoption of a similar categorization system in the Turkish law is suggestible.

Another difference between the Turkish law and the Cybercrime Convention relates to the procedures on collection of electronic evidence. Turkish law provides for 'search of computers, computer programs and transcripts, copying and provisional seizure', 'locating, listening and recording of correspondence' and 'surveillance with technical means'. Whereas, the Convention provides for 'expedited preservation of stored computer data', 'expedited preservation and partial disclosure of traffic data', 'production order', 'search and seizure of stored computer data', 'real-time collection of traffic data' and 'interception of content data'.

Nevertheless, there is one mutual problem of these two instruments: privacy concerns relating to the collection of electronic evidence. Article 8 of the ECHR and Articles 20 and 22 of the TC regulate the 'right to privacy and respect for correspondence', and Article 15 of the Cybercrime Convention requires respect for human rights and fundamental freedoms. However, Article 8(2) of the ECHR and Articles 13, 20(2) and 22(2) of the TC allow for restriction of the right to privacy and respect for correspondence. If it is necessary in a democratic society and for the prevention of disorder or crime, in compliance with the principle of proportionality, the right to privacy may be restricted; however, due to the existing regulation on the procedures relating to the collection of electronic evidence, there are certain treats against privacy.

Article 20(2) of the TC does not refer to computers. Thereby, it is ambiguous whether computers may be interpreted as included in the provision and whether the provision is applicable to electronic search. If it is in affirmative, it will be possible to resort to Article 20(2) in cases where there is violation of right to privacy in the course of an electronic search. However acceptance of the contrary will block the opportunity of affording Constitutional protection to the individuals' right to privacy in cases where privacy violations occur during the application of electronic search.

Neither Article 134 of the TCPC nor Article 17 of the Regulation on Judicial and Preventive Search set 'probable cause' as a precondition of electronic search, meaning that the simple suspicion that a crime has been committed is sufficient for the application of such an intrusive measure. Therefore, unnecessary electronic search may be conducted by the law enforcement which could increase the risk of violating individuals' privacy. The regulation under the Turkish law has to be amended, harmonizing the grounds of traditional and electronic search as in the Fourth Amendment of the U.S. Constitution and the Cybercrime Convention.

Another issue that has to be amended in Article 134 of the TCPC is that communication networks, logs on remote computers and other remote electronic devices have to be included in the provision or these have to be excluded from the scope of Article 17 of the Regulation on Judicial and Preventive Search in order to create compliance with the general principles of law.

In none of the legislation, there is an obligation to delete the electronic data that have been copied during an electronic search; however, provision of such obligation is extremely important in terms of according with the principle of protection of human rights and fundamental freedoms.

In addition to the legislative problems, the first difficulty in the application of electronic search is that the geographical scope of an electronic search is not easy to determine. However in order to avoid such problem the law enforcement officers may be familiarized with the different types of electronic evidence left behind in a computer system and the parts of computer systems in which the relevant evidence may be obtained. This would help to set

the scope of an electronic search precisely and not to exceed the scope which, otherwise, may constitute infringement of the right to privacy.

Second problem about the application of electronic search is that due to the weak grounds set for electronic search, in particular, the absence of 'probable cause' precondition, the measure may be performed to obtain coincidental evidence which would amount to a general search. In order to avoid such electronic fishing expeditions and exploratory search giving rise to privacy violations, the discussions and approaches developed in the U.S. case-law on the 'plain view doctrine' shall be taken into consideration.

According to Article 134 of the TCPC, it is possible to seize copies of computer records, computers and equipment, if the data is inaccessible or unreachable; however, the grounds of seizure do not correspond with the characteristics of digital forensics, thereby requires amendment.

In the course of electronic search a great amount of data may be seized and some of the data may comprise information related to third parties. By running automatic search with keywords, file extension etc. potential privacy violations may be avoided as the law enforcement officers would not be looking through all the data gathered. And also it is necessary to include only the data relevant to the case to the case documents.

As to the interception of communication, there are two types of interception: judicial and pre-emptive. The pre-emptive interception is applicable to anyone, at any time, without any notification necessary. Due to such broad and lose scope of application, the potential of privacy infringements is quite high.

On the other hand, application of judicial interception is limited only to certain serious crimes, and only if there are strong grounds of suspicion. However, these are not enough to say that the regulation on judicial interception provides sufficient safeguards for the protection of fundemental freedoms. First of all, correspondence of the suspect with individuals' who may refrain from testimony cannot be recorded; however it may be listened or located. In this sense, it still contains treat against privacy.

Interception of communication is supposed to be a last resort; however, according to the understanding in the Turkish doctrine, the law enforcement officers do not have to make an

actual effort to obtain evidence by other means, so the application on the measure remains rather subjective and subject to arbitrariness and exploitation.
Furthermore, the legislation allows for the application of interception during the prosecution which causes the measure to go beyond its purpose and be disproportionate with its original aim. This has to be corrected in order not to contradict with Article 13 of the TC and carry out a procedure infringing the right to privacy.
The regulation on the interception decision given upon the activities of a criminal organization does not set a maximum limit for the extension of the decisions and the situations where the extension is deemed necessary. Thereby, it is likely that the measure may be used excessively and arbitrarily.
During the enactment and the application of the surveillance measures, the principles determined by the ECtHR in its case-law on the Article 8 of the ECHR shall be taken into consideration.

However, the Cybercrime Convention does not also seem to be solving the problems relating to privacy, due the fact that it introduces invasive investigation techniques which are not counterbalanced with adequate safeguards for privacy or, in other words, the privacy protections afforded in the Convention are vague and weak. Moreover, in the Convention the recognition of international human rights obligations are insufficient. Based on the privacy criticisms brought against the Convention several recommendations have been proposed. Among all recommendations the most purposive ones are: setting clear limits to the powers involving situations where civil liberties are compromised, applying the use of invasive powers only to serious crimes, defining the concept of 'proportionality' at the international level, agreed uniformly and unilaterally.

Consequently, the regulations in Turkish law and Cybercrime Convention concerning electronic evidence and procedures on collection of electronic evidence and their applications endanger the right to privacy. For the elimination of privacy concerns both legislation have to be improved by ensuring better safeguards and stronger conditions for the protection of human rights and fundemental freedoms.

REFERENCES

List of Judgments/ Decisions

Bradley v. State of Delaware Case. (2012). Supreme Court Of The Sate Of Delware. Case Number 476, 2011. Available at

http://courts.delaware.gov/opinions/download.aspx?ID=178080

Coolidge v. New Hampshire Case. (1971). U.S. Supreme Court. Case Number 403 U.S. 443. Available at

http://supreme.justia.com/cases/federal/us/403/443/case.html

Halford v. the United Kingdom Case (1997). ECtHR. Application Number 20605/92. Available at

http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58039

Katz v. United States. (1967). Court of Appeals, 9th Circuit. Case Number 389 U.S. Available at

http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=389&invol=347

Klass and Others v. Germany Case. (1978). ECtHR. Application Number 5029/71. Available at

http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57510

Kopp v. Switzerland Case. (1998). ECtHR. 13/1997/797/1000. Available at

http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-58144

Malone v. the United Kingdom Case. (1984). ECtHR. Application Number 8691/79. Available at

http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57533

P.G. and J.H. v. the United Kingdom Case. (2001). ECtHR. Application Number 44787/98 Available at

http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-59665

People v. Triggs. (1973). Supreme Court of California. Case Number 8 Cal.3d 884. Available at

http://scocal.stanford.edu/opinion/people-v-triggs-22922

United States v. Carey. (1998). Appeals Court, 10th Circuit. Case Number 98-3077. Available at

http://caselaw.findlaw.com/us-10th-circuit/1317424.html

United States v. Comprehensive Drug Testing, Inc. (2009). Court of Appeals, 9th Circuit. Available from

http://www.wired.com/images_blogs/threatlevel/2009/08/seizure.pdf

United States v. Turner. (1999). Court of Appeals, 1st Circuit. Case Number 98-1258. Available from

http://caselaw.findlaw.com/us-1st-circuit/1020499.html

The Supreme Court of Norway (2011) HR-2011-1744-A, Case Number 2011/866.

Wisconsin v. Schroeder (1999). Court of Appeals, Wisconsin. Case Number 99-1292-CR. Available from

http://www.courts.state.wi.us/html/ca/99/99-2264.HTM

Yargitay 11. Ceza Dairesi, 16.04.2007, E. 2005/6376, K. 2007/2551

Legislation

ECHR - The 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms

Constitution of the Republic of Turkey (TC) - 7.11.1982 tarihli ve 2709 sayılı Türkiye Cumhuriyeti Anayasası (Official translation is available at: http://www.anayasa.gov.tr/images/loaded/pdf_dosyalari/THE_CONSTITUTION_OF_THE_REPUBLIC_OF_TURKEY.pdf)

Cybercrime Convention – Convention on Cybercrime CETS No.: 185

Explanatory Report - The Explanatory Report to the Convention on Cybercrime CETS No.: 185

Fourth Amendment of the U.S. Constitution - United States Constitution, Bill of Rights, Amendment IV

Law No.5397 – 3.7.2005 tarihli ve 5397 sayılı Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun

Norwegian Criminal Procedure Act - Lov om rettergangsmåten i straffesaker (Straffeprosessloven), LOV-1981-05-22-25

Regulation No. 25989 - Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi Ve Kayda Alınmasına Dair Usul Ve Esaslar İle Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev Ve Yetkileri Hakkında Yönetmelik, R.G. tarih 10.11.2005, sayı 25989

Regulation No. 26434 - Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı Ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik, R.G. tarih 14.02.2007, sayı 26434

Regulation on Judicial and Preventive Search (Regulation No. 25832) - 01.06.2005 tarihli ve 25832 sayılı Adlî Ve Önleme Aramaları Yönetmeliği

Turkish Code of Criminal Procedure (TCPC) - 04.12.2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanunu (Official translation is available at: http://www.justice.gov.tr/basiclaws/cmk.pdf)

Literature

Archick, K., *Cybercrime: The Council of Europe Convention*, CRS Report for Congress, July 22, 2004. Available at

http://fpc.state.gov/documents/organization/36076.pdf

Aydıner, Ö.F., *Avrupa İnsan Hakları Sözleşmesi ve İç Hukukumuzda Koruma Tedbirleri Olarak Tutuklama*, S.Ü. Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı Yüksek Lisans Tezi, Konya, 2007. Available at

http://www.belgeler.com/blg/16hw/avrupa-insan-haklari-szlemesi-ve-i-hukukumuzda-korum-tedbiri-olarak-tutuklama-the-european-convention-on-human-rights-and-arrest-as-a-measure-of-protection-in-our-domestic-law

Banisar, D. and Hosein, G., *A Draft Commentary on the Council of Europe Cybercrime Convention*, October 2000. Available at

http://privacy.openflows.org/pdf/coe_analysis.pdf

Casey, E. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3rd ed., Academic Press, 2011.

Casey, E. *Digital Evidence and Computer Crime*, 2nd ed., Academic Press, 2000.

Centel, N. and Zafer, H., *Ceza Muhakemesi Hukuku*, 3. Bası, Beta Basım Yayım Dağıtım, İstanbul, 2005.

European Commission, *Commission Staff Working Document (accompanying the document Commission Communication on a Feasibility Study for a Stabilisation and Association Agreement between the European Union and Kosovo {COM(2012) 602 final})*, Brussels, 23.10.2012. Available at

http://ec.europa.eu/enlargement/pdf/key_documents/2012/package/ks_analytical_2012_en.pdf

Dennis, I. H., *The Law of Evidence*, 1st ed., Sweet & Maxwell, 1999

Dinler, V., *Ceza Muhakemesinde Delillerin Toplanması*, T.C.Polis Akademisi Güvenlik Bilimleri Enstitüsü Suç Araştırmaları Anabilim Dalı Yüksek Lisans Tezi, Ankara, 2009. Available at

http://hitit.academia.edu/VeyselDinler/Books/665839/Ceza_Muhakemesinde_Delillerin_Toplanmasi

Dolar, Y. *CMK'da Bilgisayarlarda, Bilgisayar Programlarında, Bilgisayar Kütüklerinde Arama Ve Elkoyma Müessesesi*, Çağın Polisi Dergisi, Yıl.8, Sayı.94, Ekim 2009. Available at

http://www.caginpolisi.com.tr/94/index.htm

Ferraro, M. M., and Casey, E., *Investigating Child Exploitation and Pornography: The Internet*, Law and Forensic Science, Academic Press, 2004.

Galloway, Jr. R. W., *The Uninvited Ear: The Fourth Amendment Ban On Electronic General Searches*, Santa Clara Law Review, Vol.22, No.4, 1982. Available at

http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2014&context=lawreview&sei-redir=1&referer=http%3A%2F%2Fwww.google.no%2Furl%3Fsa%3Dt%26rct%3Dj%26q%3Dgeneral%2520exploratory%2520search%2520us%2520cases%2520fourth%2520amendment%26source%3Dweb%26cd%3D5%26sqi%3D2%26ved%3D0CDkQFjAE%26url%3Dhttp%253A%252F%252Fdigitalcommons.law.scu.edu%252Fcgi%252Fviewcontent.cgi%253Farticle%253D2014%2526context%253Dlawreview%26ei%3D5MaSUOyVE-

Wg4gTD24HIDw%26usg%3DAFQjCNG72mjG1m31qvxki3zf9wOh980nxg#search=%22general%20exploratory%20search%20us%20cases%20fourth%20amendment%22

GILC, *Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime Version 24.2*, December 12, 2000. Available at http://gilc.org/privacy/coe-letter-1200.html

Gözübüyük, Ş. and Tan T., *İdare Hukuku Genel Esaslar*, 1.Cilt, Turhan Yayınevi, Ankara, 2001.

Karagülmez, A., *Bilişim Suçları ve Soruşturma- Kovuşturma Evreleri,* Seçkin Yayınevi, Ankara, 2011.

Kunter, N. and Yenisey, F., *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku*, 12.Bası, Beta Yayınları, İstanbul, 2002.

Lange, M.C.S. and Nimsger, K.M., *Electronic Evidence and Discovery: What Every Lawyer Should Know Now*, 2nd ed., ABA Publishing, 2009.

Özbek, O., *Hukuk Devletinde Bireysel Güvenlik Ekseninde Bilişim Teknolojileri*, I. Hukukun Gençleri Sempozyumu, Ankara, 20-21 Mart 2009. Available at http://www.umut.org.tr/HukukunGencleri/TamMetinlerSunular/OnurOzbek.pdf

Özbek, V. Ö. *Ceza Muhakemesi Hukuku*, Seçkin Yayınevi, Ankara, 2006.

Pollitt, M. M., *Report on Digital Evidence*, 13th INTERPOL Forensic Science Symposium, Lyon, France, October 16-19 2001. Available at https://secure.interpol.int/Public/Forensic/IFSS/meeting13/Reviews/Digital.pdf

Rotenberg, M. and Laurant, C., *EPIC Statement on COE Cybercrime Convention, Treaty 108-11'*, July 26, 2005. Available at http://epic.org/privacy/intl/senateletter-072605.pdf

Solove, D.J., *Reconstructing Electronic Surveillance Law*, George Washington Law Review, Vol. 72, No. 6, August 2004. Available at http://heinonline.org/HOL/Page?handle=hein.journals/gwlr72&div=56&g_sent=1&collection=journals

Sommer, P., *Digital Evidence: Emerging Problems in Forensic Computing*, London School of Economics & Political Science, 2002. Available at
http://www.cl.cam.ac.uk/research/security/seminars/2002/2002-05-21.pdf

Şen, E., *Ceza Yargılaması Süreci (The Process of Criminal Justice)*, Türkiye Barolar Birliği Dergisi, Sayı.97, Kasım- Aralık 2011. Available at
http://portal.ubap.org.tr/App_Themes/Dergi/2011-97-1113.pdf

Şen, E., *İletişimin Denetlenmesi Tedbiri*, Ceza Hukuku Dergisi, Yıl 2, Sayı 4, Ağustos 2007.

Taşkın, M., *Adlî ve İstihbarî Amaçlı İletişimin Denetlenmesi*, 2. Baskı, Seçkin Yayınevi, Ankara, 2008.

Taşkın, M., *Türk Hukukunda Adli ve Önleme Amaçlı İletişimin Denetlenmesi: Sorular ve Çözüm Önerileri*, Türkiye Adalet Akademisi Dergisi (TAAD), Yıl.1, Sayı.2, Temmuz 2010. Available at
http://www.humanlawjustice.gov.tr/Upload/Dergiler/taad2/165.pdf

Walden, I., *Computer Crimes and Digital Investigations*, Oxford Press, 2007.

Yavuz, H.A., *Ceza Yargılamasında Bir Koruma Tedbiri Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi*, Türkiye Barolar Birliği Dergisi (TBB), Sayı.60, 2005. Available at

Yavuzcan, E., *Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma (cmk 134)*, 2010. Available at
http://www.hukuki.net/entry.php?4-Bilgisayarlarda-bilgisayar-programlarinda-ve-kutuklerinde-arama-kopyalama-ve-elkoyma-(cmk-134)&bt=8

Yenisey, F., *Çıkar Amaçlı Örgüt Suçlarındaki Araştırmalar*, Hukuk Kurultayı 2000, Cilt 2, Ankara.

Yiğit, N., *Arama, Elkoyma ve Gizli Koruma Tedbirleri*, Adalet Bakanlığı Seminer Notları, Ankara, 2005. Available at
http://www.sucveceza.org/Hukuki-makaleler/Arama-elkoyma-ve-gizli-koruma-tedbirleri.pdf