T.C.
GALATASARAY ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

TÜRK CEZA MUHAKEMESİNDE BİLİŞİM SİSTEMLERİNDE ARAMA, KOPYALAMA VE ELKOYMA

YÜKSEK LİSANS TEZİ

Oğuzhan Emre PARLAK

Tez Danışmanı: Doç. Dr. Emine Eylem AKSOY RETORNAZ

EYLÜL 2019

ÖNSÖZ

Bu çalışmanın konusu bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirleridir. Bu doğrultuda, ilgili tedbirler, Yargıtay kararları, öğretideki görüşler ve karşılaştırmalı hukuk ışığında incelenmiş ve kanunun lafzı ile uygulamada bulunan eksiklikler ve sorunlar tespit edilmeye çalışılmıştır. Son olarak, kanun maddesini savunduğumuz görüşler ışığında yeniden yazılmış ve olanın yanında olması gerekenin ifade edilmesine gayret edilmiştir.

Tez konumun belirlenmesinde bana yol gösteren, desteğini bir an olsun esirgemeyen ve görüşleriyle tezime değer katan danışman hocam Doç. Dr. E. Eylem AKSOY RETORNAZ'a saygı ve teşekkürlerimi sunarım. Bilişim hukuku alanında çalışmama vesile olan ve tez jürimde yer alarak beni onurlandıran Doç. Dr. Pınar MEMİŞ KARTAL'a teşekkürü bir borç bilirim.

Zor zamanımda yardımıma koşan değerli meslektaşlarım A. Yasin UYSAL'a ve Ar. Gör. Bilal Osmanoğlu'na minnetlerimi sunarım.

Bu süreçte her an desteğini hissettiğim, moral ve motivasyon kaynağım biricik eşim Habibe GÜNEŞ PARLAK'a teşekkür ederim ve bu çalışmayı kendisine atfetmek isterim.

Ortaköy-2019

Oğuzhan Emre Parlak

İÇİNDEKİLER

ÖNSÖZ ii
KISALTMALAR v
RESUME vi
ABSTRACT xiii
ÖZET xix
BİRİNCİ BÖLÜM: ELEKTRONİK DELİL VE KARŞILAŞTIRMALI HUKUKTA BİLİŞİM SİSTEMLERİNDE ARAMA, KOPYALAMA VE ELKOYMA TEDBİRLERİ 1
I. TEMEL KAVRAMLAR 1
A. Bilişim 1
B. Bilişim Sistemi 2
C. Bilgisayar Programı 7
D. Bilgisayar Kütüğü 8
E. Veri 9
II. ELEKTRONİK DELİL 11
A. Tanım 11
B. Analog ve Sayısal Delil Ayrımı 12
C. Sayısal Delilin Özellikleri 13
D. Sayısal Delil ile ilgili Kabul Edilen İlkeler 15
1. Avrupa Konseyi Elektronik Delil Rehberi 16
2. ACPO Sayısal Deliller için İyi Uygulama Rehberi 17
3. Sedona İlkeleri 19
III. KARŞILAŞTIRMALI HUKUKTA BİLİŞİM SİSTEMLERİNDE ARAMA, KOPYALAMA VE ELKOYMA TEDBİRLERİ 21
A. FRANSA 21
B. ALMANYA 24
C. BELÇİKA 29
D. AMERİKA BİRLEŞİK DEVLETLERİ 31
İKİNCİ BÖLÜM: BİLİŞİM SİSTEMLERİNDE ARAMA, KOPYALAMA VE ELKOYMA TEDBİRLERİ 37
I. Bilgisayarlarda, Bilgisayar Programları ve Kütüklerinde Arama 40
A. Tedbirinin Hukuki Niteliği 40

B. Tedbirin Kapsamı 42
1. Tedbirin Uygulanacağı Kişiler Bakımından 42
2. Tedbirin Uygulanacağı Cihazlar Bakımından 47
C. Tedbirin Şartları 54
1. Suç Soruşturmasının Varlığı 54
2. Başka Surette Delil Elde Etme İmkanının Bulunmaması 56
3. Somut Delillere Dayanan Kuvvetli Şüphenin Varlığı 59
4. Hâkim ya da Gecikmesinde Sakınca Bulunan Hâllerde Cumhuriyet Savcısı Kararının Bulunması 61
D. Tedbirin Uygulanması 64
1. Yerinde Arama 65
2. Uzaktan Arama 70
II. Bilgisayarlarda, Bilgisayar Programları ve Kütüklerinde Elkoyma 72
A. Tedbirinin Hukuki Niteliği 72
B. Tedbirin Kapsamı 74
C. Tedbirin Şartları 74
1. Arama Tedbirinin Uygulanmış Olması 74
2. Bilişim Sistemlerine, Programlarına ve Kütüklerine Şifrenin Çözülememesinden Dolayı Girilememesi veya Gizlenmiş Verilere Ulaşılamaması ya da İşlemin Çok Uzun Sürecek Olması 75
D. Tedbirin Uygulanması 75
III. Bilgisayarlarda, Bilgisayar Programları ve Kütüklerinde Kopyalama 77
A. Tedbirinin Hukuki Niteliği 77
B. Tedbirin Kapsamı 79
C. Tedbirin Şartları 79
D. Tedbirin Uygulanması 79
1. Adli İmaj Alma 81
2. Özet (Hash) Değeri Alma 83
IV. Bilgisayarlarda, Bilgisayar Programları ve Kütüklerinde Arama, Kopyalama ve Elkoyma Tedbirlerine Karşı Başvuru Yolları ve Kopyalanan Verilerin Yok Edilmesi 84
SONUÇ 88
KAYNAKÇA 91

KISALTMALAR

a.g.e. : Adı Geçen Eser
ACMK : Alman Ceza Muhakemesi Kanunu
ACPO : İngiltere, Galler ve Kuzey İrlanda Emniyet Müdürleri Derneği
AFAM : Almanya Federal Anayasa Mahkemesi
AİHM : Avrupa İnsan Hakları Mahkemesi
AİHS : Avrupa İnsan Hakları Sözleşmesi
AKSSS : Avrupa Konseyi Siber Suç Sözleşmesi – Budapeşte Sözleşmesi
AÖAY : Adli ve Önleme Aramaları Yönetmeliği
BCMK : Belçika Ceza Muhakemesi Kanunu
BKAG : Almanya Federal Adli Polis Teşkilatı Kanunu
C. : Cilt
CMK : Ceza Muhakemesi Kanunu
CMUK : Ceza Muhakemeleri Usulü Kanunu
FCMK : Fransız Ceza Muhakemesi Kanunu
HSK : Hakimler ve Savcılar Kanunu
İÜHFM : İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
KHK : Kanun Hükmünde Kararname
LSE : London School of Economics
NPCC : Ulusal Emniyet Müdürleri Konseyi
OHAL : Olağanüstü Hal
p. : Paragraf
s. : Sayfa
S. : Sayı
TBB : Türkiye Barolar Birliği
TCK : Türk Ceza Kanunu
Y. : Yıl

RESUME

Le sujet de cette thèse est la perquisition, la copie et la saisie des systèmes informatiques dans le droit de procédure pénale turc. Ces mesures de protection figurent dans notre droit sous le titre « perquisition, copie et saisie des ordinateurs, des programmes et des fichiers informatiques » dans le Code de Procédure Pénale et sous le titre « perquisition et saisie des données informatiques stockées » dans la Convention du Conseil de l'Europe sur la cybercriminalité (la Convention de Budapest) que nous avons ratifié par la loi d'approbation datée le 22 Avril 2014. L'objectif de cette étude est d'examiner les mesures pertinentes à la lumière de la pratique, en particulier des décisions de la Cour de Cassation, des opinions de la doctrine et du droit comparé.

Afin de mieux comprendre la perquisition, la copie et la saisie des systèmes informatiques, il est nécessaire de connaître certains concepts utilisés dans le droit, la pratique et la doctrine. Dans cette direction, tout d'abord les concepts d'informatique, de système informatique, de programme informatique, de fichier informatique et de donnée sont définis et expliqués. Etant donné que les systèmes tels que les dispositifs de navigation, les smartphones ne sont pas évalués comme des ordinateurs, et que le concept de système informatique couvre tous les dispositifs qui traitent et transmettent des données, y compris les ordinateurs, le concept de système informatique a été utilisé dans la portée de la thèse. Cependant, la définition du concept de l'ordinateur est donnée sous le titre de système informatique.

Avec le développement des technologies informatiques, les systèmes informatiques, en particulier les ordinateurs et les téléphones portables, font partie de notre vie. Parallèlement à cela, de nouveaux crimes connus sous le nom de cybercrimes ont émergé, et les données obtenues à partir de systèmes informatiques qui n'ont pas de présence concrète ont commencé à être utilisées comme preuve pour la détermination de la vérité matérielle. Ces preuves dites numériques ne sont pas seulement utilisées comme preuves dans les procédures liées aux crimes informatiques. Par exemple, les plans d'action obtenus à partir d'un ordinateur utilisé par un terroriste serviraient de preuve dans la procédure pénale.

Les éléments de preuve à obtenir à la suite des mesures de perquisition, de copie et de saisie des systèmes informatiques sont des éléments de preuve numériques. Par conséquent, dans la deuxième partie du premier chapitre de notre thèse, le concept de preuve numérique est défini, les caractéristiques de la preuve numérique et ses aspects distinctifs sont exprimés. Toutefois, le titre inclut des preuves électroniques. De ces deux concepts interchangeables, la preuve électronique, en fait, est un hyperonyme qui inclut la preuve numérique et la preuve analogique. Par conséquent, dans ce chapitre, d'abord la preuve électronique a été décrite, la preuve analogique et la preuve numérique sont différenciée et puis le concept de preuve numérique a été traité.

Les principes fondamentaux qui sont validés à l'échelle internationale et qui sont considérés comme pertinents pour l'obtention de preuves électroniques ou numériques, sont présentés. Tout d'abord, les principes contenus dans le Guide des Preuves électroniques préparé par le Conseil de l'Europe sont spécifiés, puis les principes fondamentaux dans la Guide des Meilleures Pratiques en matière de Preuves Numériques élaborées par l'ACPO, sont donnés. Enfin, les principes de Sedona sont mentionnés. Les deux autres guides visent principalement à aider la police, les procureurs et les juges pénaux à mettre en œuvre la perquisition, la copie et le saisie pendant les procédures pénales, les principes de Sedona sont établis à utiliser pour les preuves électroniques et la découverte électronique dans les procédures judiciaires. Cependant, ces principes ont une valeur directrice en matière de procédures pénales.

Dans la dernière partie du premier chapitre, la perquisition, la copie et la saisie des systèmes informatiques sont traitées en droit comparé. Dans ce contexte, la législation et les pratiques de l'Allemagne, de la France, de la Belgique et des États-Unis ont été examinées. Ces États, dont les législations sont examinées, sont des parties à la Convention du Conseil de l'Europe sur la cybercriminalité, et la Convention pertinente est approuvée par chacun d'eux et est faite partie de leur législation. Conformément à l'article 19 de la Convention, l'État parti a l'obligation de réglementer les mesures de perquisition, de copie et de saisie des systèmes informatiques ou de leurs données.

Les preuves obtenues à la suite de la mise en œuvre de la perquisition, la copie et la saisie des systèmes informatiques manquent de présences concrètes et ces mesures ont des qualités différentes que des autres preuves, par exemple, ils ne sont obtenus que par certains outils. Les États qui en ont tenu compte ont règlementé ces mesures séparément des mesures générales de perquisition et de saisie en ajoutant des dispositions à leurs codes de procédure pénale.

La France, par exemple, a ajouté des dispositions à la Code de Procédure Pénale relatives à la perquisition et à la saisie, ce qui rend légale la mise en œuvre de ces mesures sur des données numériques. En outre, selon la législation française, il est possible d'effectuer la perquisition à distance aux données accessibles dans les systèmes informatiques où la mesure de perquisition est en œuvre, et aux données dans les systèmes informatiques des suspects par l'emploi des moyens comme le cheval de Troie ou la porte dérobée pour lutter contre les crimes organisés et terroristes.

La Belgique, comme dans la législation turque, a ajouté un article séparé au Code d'Instruction Criminel et a réglé des mesures de perquisition, de copie et de saisie des systèmes informatiques relevant du champ d'application de cet article. En vertu de ces dispositions, les systèmes informatiques peuvent être consultés sur place et il est possible d'effectuer la perquisition à distance aux systèmes informatiques accessibles en ligne à partir de ces systèmes.

En droit allemand, les mesures de perquisition, de copie et de saisie des systèmes informatiques ne sont pas codifiées séparément. Ces mesures continuent d'être appliquées conformément aux dispositions générales relatives à la perquisition et à la saisie. Toutefois, une disposition prévoyant que la mesure de saisie peut être effectuées à autres données électroniques accessibles à partir des systèmes informatiques où la perquisition est en œuvre, est ajoutée au Code de Procédure Pénale. En outre, la police était autorisée à effectuer la perquisition à distance pour des crimes terroristes, comme en droit français, mais la disposition pertinente a été jugée inconstitutionnelle et annulée par la Cour Constitutionnelle.

Enfin, en droit américain, les mesures de perquisition, de copie et de saisie des systèmes informatiques sont examinées. En droit américain, les mesures pertinentes ne sont pas codifiées séparément des perquisitions et saisies générales. Mais le système juridique américain est un système juridique fondé en grande partie sur des décisions de justice. Par conséquent, à la lumière des décisions de justice, les mesures de perquisition, de copie et de saisie des systèmes informatiques, sont mises en œuvre conformément aux dispositions de perquisition, de copie et de saisie en vertu du quatrième amendement à la Constitution des États-Unis et de la loi fédérale sur la procédure pénale.

Dans le deuxième chapitre, les mesures de perquisition, de copie et de saisie des systèmes informatiques en droit turc sont examinées. Ces mesures sont disposées par l'article 134 du Code de Procédure Pénale comme nous l'avons indiqué en haut, ainsi qu'elles sont d'une apparence spéciale des mesures générales de perquisition et de saisie. En outre, l'article 17 du Règlement sur les Perquisitions Judiciaires et Préventives élaboré par le Ministère de la Justice et de l'Intérieur précise les principes et les procédures à suivre lors de la mise en œuvre de ces mesures. En outre, sur les mesures de protection, une réglementation intitulée « Perquisition et saisie de données informatiques stockées » qui font l'objet de notre thèse, se trouve dans la Convention du Conseil de l'Europe sur les Cybercrimes.

La mesure de perquisition est fixée par le législateur comme une *ultima ratio*, c'est-à-dire un dernier recours. En conséquence, la mise en œuvre de cette mesure nécessite l'existence des raisons sérieuses de soupçonner fondées sur des éléments de preuve concrets et l'impossibilité d'obtenir des éléments de preuve de toute autre manière au cours de l'enquête. La mesure est disposée comme une perquisition dans les ordinateurs, les programmes informatiques et les fichiers informatiques, pourtant selon les décisions de la Cour de Cassation, le terme ordinateur serait largement interprété. Ainsi, on considère tout appareil capable de traiter ou de transférer des informations, en particulier les smartphones, comme un ordinateur. En outre, selon le règlement, la mesure de perquisition peut être appliquée sur les appareils qui peuvent être branchés et retirés de l'ordinateur.

La mesure est appliquée à l'ordinateur, aux programmes informatiques et aux fichiers informatiques utilisés par le suspect. Une décision de perquisition rendue par le juge ou, avec la modification du 25 juillet 2018, par le procureur de la République dans les cas où un retard est considéré périlleux, est requise pour que la perquisition soit effectuée. La décision prise par le procureur de la République est soumise à l'approbation du juge, et si le juge n'approuve pas, les copies réalisées et les textes résolus seront détruits.

En règle générale, la mesure de perquisition sera effectuée sur place. Cependant, les outils et les équipements pertinents peuvent être saisis si les mots de passe ne peuvent pas être décryptés, les données confidentielles ne peuvent pas être accédées ou les transactions à effectuer prendrait trop de temps. La loi ne permet pas d'effectuer la mesure de perquisition par l'accès à distance. Cependant, nous sommes obligés de prendre des dispositions juridiques afin qu'on puisse effectuer la perquisition aux données accessibles aux systèmes informatiques où la perquisition est effectuée. En outre, la législation pertinente dispose que la mesure de perquisition peut être effectuée sur des réseaux d'ordinateur et d'autres fichiers informatiques accessibles par l'ordinateur. Par conséquent, il est possible d'effectuer la perquisition sur les fichiers informatiques situés à distance pourvu que l'accès soit réalisé par l'ordinateur faisant l'objet de la perquisition, mais en raison du principe de légalité, cette disposition doit être fixée par la loi non par le règlement.

Si les données obtenues à la suite de la mise en œuvre de la mesure de perquisition ont la qualité de preuve en termes de procédure pénale, les copies exactes de ces données seront prises, résolues et transformées en texte. Afin d'assurer l'intégrité des données, l'une des copies reçues devra être remise au suspect ou à son avocat et il faut extraire la valeur de hachage des copies reçues. En cas de violation de l'intégrité des données, cela compromet l'utilisation de ces données comme preuve dans le cadre d'une procédure pénale, car cela porte atteinte à la fiabilité des données obtenues.

Dans la première version de la loi, la mesure de saisie est disposée comme une mesure qui peut être appliquée en cas d'impossibilité de décrypter des mots de passe, d'accéder aux données confidentielles. Toutefois, dans la pratique, la police saisit des

ordinateur et autres systèmes informatiques sans recourir à la mesure de perquisition. Au lieu de la mise en œuvre conformément à la loi de la mesure de saisie qui porte principalement atteinte aux droits fondamentaux tels que les droits de propriété et de la vie privée, il a eu lieu une modification de la loi en 2018 et avec le changement apporté, la disposition a été ajoutée que si les transactions prennent trop longtemps, il peut être recouru aux mesures de saisie.

En cas de recours à la mesure de saisie, des copies exactes de toutes les données contenues dans les systèmes informatiques seront réalisées, et l'une de ces copies sera remise au suspect ou à son avocat. En outre, les systèmes informatiques saisis seront retournés en cas d'accès à des données confidentielles, de décodage des mots de passe et de réalisation des copies nécessaires. Il n'y a aucune disposition sur ce qu'il faut faire s'il y a des données criminelles telles que la pornographie juvénile ou le virus informatique dans les unités de stockage des ordinateurs à retourner. Toutefois, dans la pratique, les unités de stockage sont confisquées en se référant aux dispositions générales. Dans la doctrine, il est soutenu que les ordinateurs et les systèmes informatiques saisis peuvent être retournées après que les données criminelles soient effacées des unités de stockage ou faites inaccessibles.

La loi dispose les mesures de copie, outre la perquisition et la saisie. Cette mesure est indiquée comme la copie de la totalité ou d'une partie des données contenues dans les ordinateurs ou les fichiers informatiques. Il est nécessaire de comprendre que la copie ici est de prendre l'image des données pertinentes, c'est-à-dire de réaliser une copie exacte.

La mesure de copie peut être effectuées de trois manières différentes. Le premier d'entre eux est la copie des données obtenues à partir de la perquisition. La seconde consiste à copier uniquement les données auxquelles la mesure de perquisition est appliquée, sans saisir les ordinateurs ou autres systèmes informatiques. Dans ce cas, il ne serait pas nécessaire de saisir les ordinateurs et autres systèmes informatiques. Le dernier est la réalisation de copies de données obtenues à la suite de perquisition effectuée aux ordinateurs et les transcriptions informatiques saisis.

Enfin, dans notre thèse, les voies de recours possibles contre ces mesures et l'élimination des données obtenues à la suite de mesures de copie sont abordées.

Dans la partie de conclusion, la critique de l’article de la loi en vigueur et de l'application de cet article est incluse. En outre, conformément à nos critiques, l’article de la loi est récrit.

ABSTRACT

The subject of this thesis is searching, copying and seizing information systems in Turkish criminal procedure law. These measures of protection are regulated in our law in the Criminal Procedure Code under the title of "Searching, copying and seizing computers, computer programs and files" and in the Council of Europe's Convention on Cybercrimes (Budapest Convention - the Council of Europe Convention on Cybercrimes) which we have ratified on 22 April 2014, under the title of "Search and seizure of stored computer data". This study aims to examine the related measures in the light of comparative law, practice, opinions in the doctrine and especially the decisions of the Court of Cassation.

To understand better the searching, copying and seizing measures on information systems, some concepts used in law, practice and doctrine should be known. In this direction, in the first chapter, the concepts of informatics, information system, computer program, computer file, and data have been defined and these concepts have been explained.

Although the concept of computer is used in the law, the fact that the systems like navigation devices and smart mobile phones are not considered computer and that the concept of information systems contains all the devices that process and transmit data including the computer, it is the reason why the concept of information system is used in the thesis. However, the definition of computer concept is given under the title of information system.

With the development of information technologies, information systems, especially computers and mobile phones, have become a part of our lives. With this situation, new crimes known as cybercrimes have emerged, and the data obtained from informatics systems which do not have a concrete existence in the determination of the material truth related to these crimes have begun to be used as evidence. These evidences, which are called as digital evidence, are not used as evidence only in the

proceedings related to informatics crimes. For example, the action plans obtained from the computer used by a terrorist can be used as evidence.

The evidence to be obtained as a result of searching, copying and seizing information systems is digital evidence. Therefore, in the second part of the first chapter of the thesis, the concept of digital evidence is defined, and the features of the digital evidence and its differences from other evidences are expressed. Nevertheless, the title includes the term of electronic evidence. Of these two concepts that can be used interchangeably, electronic evidence is, in fact, a hypernym that includes digital evidence along with analog evidence. Therefore, in this part, first of all, electronic evidence is explained, the distinction between analog and digital evidence is made, and then the concept of digital evidence is discussed.

Fundamental principles, which are considered to be related to the acquisition of electronic or numerical evidence and which have international validity, are included. Firstly, the principles in the Electronic Evidence Manual prepared by the Council of Europe are stated, and then the fundamental principles in the Best Practice Guide on Digital Evidences prepared by ACPO are given. Finally, the Sedona Principles are mentioned.

While the other two guidelines are primarily prepared to assist law enforcement, prosecutors and criminal judges during the exercise of searching, copying and seizing or criminal proceedings, the Sedona Principles are the principles established for electronic evidence and electronic discovery to be used in civil proceedings. These principles, however, have a guiding value in terms of criminal procedure.

In the last part of the first chapter, searching, copying and seizing information systems in comparative law are mentioned. In this context, the legislation and practices of France, Germany, Belgium, and the United States were examined. These states, whose legislation has been examined, are parties to the Council of Europe Convention on Cybercrimes and have been ratified by each of them to become part of their

legislation. Under the article 19 of the Convention, the contracting states have an obligation to regulate searching, copying and seizing information systems or their data.

The evidence obtained as a result of the implementation of searching, copying and seizing information systems has different features from other evidences such as the fact that they do not have any concrete existence and that these measures can only be obtained through certain means. The States which consider this situation have regulated these measures separately from the general search and seizure measures and the provisions they have added to the criminal procedure laws. For example, France has added provisions to the search and seizure clauses of the Code of Criminal Procedure, making it legal to implement these measures on digital data.

In addition, according to the French legislation, it is possible to remotely search the data available in the information systems in the place where the search measure is applied and in the information systems of the suspects using trojan horse or backdoor to combat organized and terrorist crimes. As in the Turkish legislation, Belgium has added a separate article to the Code of Criminal Procedure and has arranged searching, copying and seizing information systems within the scope of this article. According to these provisions, it is possible to make an on-site search in information systems and remote search in information systems that can be accessed online from these systems. In German law, searching, copying and seizing information systems are not regulated separately. These measures continue to be carried out in accordance with the general provisions of search and seizure. However, a provision stipulating that search, seizure measures may be applied to other electronic data accessible from the information systems being searched has been added to the Code of Criminal Procedure. Also, as in French law, law enforcement officials were given the authority to conduct remote searches in the investigation of terror crimes, but the relevant provision was found unconstitutional and was abolished by the Constitutional Court.

Finally, searching, copying and seizing information systems in American law are examined. In American law, the relevant measures are not regulated separately from general search and seizure measures. But the American legal system is a legal system that is based largely on court decisions. Therefore, in the light of court

decisions, searching, copying and seizing information systems are carried out in accordance with the provisions of the Fourth Amendment to the United States Constitution and the search and seizure provisions regulated under the Federal Criminal Procedure Code.

In the second chapter, search searching, copying and seizing information systems in Turkish law are examined. These measures as mentioned above are a special view of the general search and seizure measures regulated under the scope of the article 134 in the Code of Criminal Procedure. Also, Article 17 of the Regulation on Judicial and Preventive Searches, prepared by the Ministry of Justice and the Interior, specifies the principles and procedures to be followed during the implementation of these measures. In addition to these, the Council of Europe Convention on Cybercrimes contains a regulation titled “Search and seizure of stored computer data” which is the subject of our thesis.

The searching is regulated by the legislator as an ultima ratio. Accordingly, the implementation of this measure requires the existence of strong grounds for suspicion based on concrete evidences and no other means of obtaining evidence at the investigation stage. The measure is regulated as searching computers, computer programs, and files, but the term of computer is interpreted broadly by the decisions of the Court of Cassation. Accordingly, any device capable of processing or transmitting information, particularly smartphones, is considered a computer. Also, according to the regulation, the search measure can be applied to devices that can be plugged into and removed from the computer.

The measure will be applied to the computer, computer programs, and files that are in use by the suspect. To search, the search warrant issued by the judge or, with the amendment made on 25 July 2018, by the public prosecutor in the non-delayable case. The decision given by the public prosecutor shall be submitted to the approval of the judge and if the judge does not approve, any copies retained and the texts analyzed shall be destroyed.

As a rule, the search measure will be carried out on site. However, if the passwords cannot be deciphered, confidential data cannot be accessed or the transactions to be carried out will take too long, the relevant tools and equipment may be seized. It is not legally possible to carry out the search measure with remote access. Besides, we have an obligation to make legislation to perform searches on the data accessible in the information systems searched in accordance with the Convention on Cybercrimes. In addition, the relevant regulation stipulates that the search measure can be carried out on computer networks and other computer files accessible via the searched computer. Thus, it is possible to perform a search in remote computer files provided that it is accessible from the searched computer, but this provision should be regulated by law and not by regulation in accordance with the principle of legality.

If the data obtained as a result of the implementation of the search measure is evaluated as evidence in terms of criminal procedure, bit-to-bit copies of these data will be taken and analyzed into text. To ensure data integrity, one of the copies will have to be given to the suspect or his/her representative, and the hashing values of the copies will have to be extracted. If data integrity is compromised, the use of such data as evidence in criminal proceedings will be imperiled, as the reliability of the data obtained is endangered.

The seizure measure was firstly regulated as a measure that could be carried out if the passwords could not be decoded and confidential data cannot be accessed. In practice, however, law enforcement officers seize computers and other information systems without implementing the search measure. Instead of implementing the seizure measure in accordance with the law, which interferes with fundamental rights especially as the right to property and the privacy of private life, the law was amended in 2018, and a provision was added that the seizure measure could be resorted to if the procedures would be too long.

In the event of a seizure measure, one-to-one copies of all data contained in the information systems will be made and one of these copies will be delivered to the suspect or his/her representative. In addition, if the confidential data is accessed, passwords decrypted and necessary copies are taken, then the seized information

systems will be returned. There is no provision on what to do if the storage units of the computers to be returned contain data that may constitute criminal offenses such as child pornography or computer virus. In practice, however, the storage units are confiscated by applying general provisions. Yet, in the doctrine, it is argued that seized computer and information systems can be returned by deleting data from storage units or making them inaccessible.

The law regulates the copying measures beside of the search and seizure measures. This measure is stated as copying all or a part of the data contained in computers or computer files. What should be understood from the copying here is taking the image of the relevant data, id est making a bit-to-bit copy.

The copying measure can be implemented in three different ways. The first one is the copying of the data obtained from the search. The second is copying only the data to which the search measure will be carried out, without the seizure of computers or other information systems. In this case, there will be no need to seize computers and other information systems. The last one is to make copies of the data obtained by searching the seized computers and computer files.

Lastly, in our thesis, the legal remedies against these measures and the destruction of the data obtained as a result of the copying measure are discussed.

In the conclusion part, the article of the law in force and the criticisms about its application are given. In addition, the article of the law has been rewritten in line with our criticisms.

ÖZET

Bu tez çalışmasının konusu, Türk ceza muhakemesi hukukunda bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirleridir. Bu koruma tedbirleri hukukumuzda "bilgisayarlarda, bilgisayar programları ve kütüklerinde arama, kopyalama ve elkoyma" başlığıyla Ceza Muhakemesi Kanununda ve "depolanmış bilgisayar verilerinin aranması ve bunlara elkonulması" başlığıyla 22 Nisan 2014 tarihli uygun bulma kanunu ile iç hukukumuzun bir parçası haline getirdiğimiz Avrupa Konseyi Siber Suç Sözleşmesi'nde (Budapeşte Sözleşmesi – Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi) düzenlenmiştir. Bu çalışmanın amacı başta Yargıtay kararları olmak üzere uygulama, öğretideki görüşler ve karşılaştırmalı hukuk ışığında ilgili tedbirlerin incelenmesidir.

Bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirlerinin daha iyi anlaşılabilmesi için kanunda, uygulamada ve öğretide kullanılan bazı kavramların bilinmesi gerekmektedir. Bu doğrultuda ilk bölümde öncelikle bilişim, bilişim sistemi, bilgisayar programı, bilgisayar kütüğü ve veri kavramlarının tanımı yapılmış ve bu kavramlar açıklanmıştır. Kanunda bilgisayar kavramı kullanmasına rağmen, navigasyon cihazları, akıllı cep telefonları gibi sistemlerin bilgisayar olarak değerlendirilmemesi ve bilişim sistemi kavramının bilgisayar dahil olmak üzere veri işleyen ve aktaran bütün cihazları kapsamasından dolayı, tez kapsamında bilişim sistemi kavramı kullanılmıştır. Bununla birlikte bilgisayar kavramının tanımına bilişim sistemi başlığı altında yer verilmiştir.

Bilişim teknolojilerinin gelişmesi ile birlikte başta bilgisayar ve cep telefonu olmak üzere bilişim sistemleri hayatımızın bir parçası haline gelmiştir. Bu durumla birlikte, bilişim suçları olarak bilinen yeni suçlar ortaya çıkmış ve bu suçlar ile ilgili maddi gerçeğin tespitinde somut bir varlığa sahip olmayan ve bilişim sistemlerinden elde edilen veriler delil olarak kullanılmaya başlanmıştır. Sayısal delil olarak adlandırılan bu deliller yalnızca bilişim suçları ile ilgili yargılamalarda delil olarak

kullanılmamaktadır. Örneğin, bir teröristin kullandığı bilgisayardan elde edilen eylem planları, terör suçlarında delil olarak kullanılabilecektir.

Bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirleri sonucunda elde edilecek deliller sayısal delillerdir. Dolayısıyla, tezimizin ilk bölümünün ikinci kısmında sayısal delil kavramı tanımlanmış, sayısal delilin özellikleri ve diğer delillerden ayrılan yanları ifade edilmiştir. Bununla birlikte, başlıkta elektronik delil ifadesine yer verilmiştir. Birbirinin yerine kullanılabilen bu iki kavramdan aslında elektronik delil, analog delil ile birlikte sayısal delili içerisine alan bir üst kavramdır. Dolayısıyla, bu bölümde öncelikle elektronik delil açıklanmış, analog ile sayısal delillerin ayrımına yapılmış ve daha sonrasında sayısal delil kavramı işlenmiştir.

Bu kısımda son olarak, elektronik veya sayısal delillerin elde edilmesi ile alakalı olarak kabul edilen ve uluslararası geçerliliği bulunan temel ilkeler açıklanmaya çalışılmıştır. Öncelikle, Avrupa Konseyi tarafından hazırlanan Elektronik Delil Rehberinde yer alan ilkeler belirtilmiş, daha sonrasında ise ACPO tarafından hazırlanan Sayısal Deliller ile ilgili En İyi Uygulama Rehberinde yer alan temel ilkelere yer verilmiştir. Son olarak ise Sedona İlkelerine değinilmiştir. Diğer iki rehber, başta kolluk kuvvetleri, savcılar ve ceza hakimlere arama, kopyalama ve elkoyma tedbirleri uygulanırken veya ceza muhakemesi esnasında yardımcı olması için hazırlanırken, Sedona İlkeleri hukuk muhakemelerinde kullanılacak elektronik deliller ve elektronik keşif için belirlenmiş ilkelerdir. Bununla birlikte bu ilkeler ceza muhakemesi açısından yol gösterici bir değere sahiptirler.

Birinci bölümün son kısmında ise, karşılaştırmalı hukukta bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirlerine değinilmiştir. Bu kapsamda, Fransa, Almanya, Belçika ve Amerika Birleşik Devletleri mevzuatları ve uygulamaları incelenmiştir. Mevzuatları incelenen bu devletler, Avrupa Konseyi Siber Suç Sözleşmesi'ne taraf ülkelerdir ve her biri tarafından ilgili sözleşme onaylanarak mevzuatlarının bir parçası haline getirilmiştir. Sözleşmenin 19. maddesine göre, taraf devletlerin bilişim sistemlerinde veya verilerinde arama, kopyalama ve elkoyma tedbirlerini düzenleme yükümlülüğü bulunmaktadır.

Bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirlerinin uygulanması sonucu elde edilen deliller, somut bir varlıklarının olmaması ve bu tedbirlerin ancak belirli araçlar aracılığıyla elde edilebilmeleri gibi diğer delillerden farklı niteliklere sahiptirler. Bunu durumu dikkate alan devletler, bu tedbirleri ceza muhakemesi kanunlarına ekledikleri hükümlerle genel arama ve elkoyma tedbirlerinden ayrı bir şekilde düzenlemişlerdir. Örneğin Fransa, Ceza Muhakemesi Kanununun arama ve elkoyma maddelerine hükümler ekleyerek, bu tedbirlerin sayısal veriler üzerinde gerçekleştirilebilmesini hukuki hale getirmiştir. Ayrıca Fransız mevzuatına göre arama tedbirinin uygulandığı yerde bulunan bilişim sistemlerinde erişilebilen verilerde ve organize suçlar ve terör suçları ile mücadele amacıyla truva atı ya da arkakapı gibi yöntemlerle şüphelilerin bilişim sistemlerindeki verilerde uzaktan arama yapmak mümkündür. Belçika ise, Türk mevzuatında olduğu gibi, Ceza Muhakemesi Kanununa ayrı bir madde ekleyerek, bu madde kapsamında bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirleri düzenlemiştir. Bu hükümlere göre, bilişim sistemlerinde yerinde arama ve bu sistemlerden çevrimiçi ulaşılabilecek bilişim sistemlerinde uzaktan arama yapılabilmektedir.

Alman hukukunda, bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirleri ayrı bir şekilde düzenlenmemiştir. Bu tedbirler, genel arama ve elkoyma hükümlerine göre uygulanmaya devam etmektedir. Bununla birlikte, arama gerçekleştirilen bilişim sistemlerinden erişilebilen diğer elektronik verilerde arama elkoyma tedbirlerinin uygulanabileceğine dair bir hüküm Ceza Muhakemesi Kanununa eklenmiştir. Ayrıca, Fransız hukukunda olduğu gibi terör suçlarıyla ilgili yürütülen soruşturmalarda kolluk kuvvetlerine uzaktan arama yapma yetkisi verilmiş fakat ilgili kanun hükmü anayasaya aykırı bulunmuş ve Anayasa Mahkemesi tarafından iptal edilmiştir.

Son olarak Amerikan hukukunda bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirleri incelenmiştir. Amerikan hukukunda ilgili tedbirler genel arama ve elkoyma tedbirlerinden ayrı olarak düzenlenmemiştir. Fakat Amerikan hukuk sistemi, büyük ölçüde mahkeme kararlarına dayanan bir hukuk sistemidir. Dolayısıyla, mahkeme kararları ışığında bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirleri, Birleşik Devletler Anayasası Dördüncü Değişiklik ve Federal Ceza

Muhakemesi Kanunu kapsamında düzenlenen arama ve elkoyma hükümlerine göre gerçekleştirilmektedir.

İkinci bölümde Türk hukukunda bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirleri incelenmiştir. Bu tedbirler yukarıda belirttiğimiz gibi genel arama ve elkoyma tedbirlerinin özel bir görünümü olarak Ceza Muhakemesi Kanunu m. 134 kapsamında düzenlenmiştir. Ayrıca, Adalet ve İçişleri Bakanlığı tarafından hazırlanan Adli ve Önleme Aramaları Yönetmeliği m.17'de bu tedbirlerin uygulanması sırasında uyulacak esas ve usuller belirtilmiştir. Bunlara ek olarak, Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi'nde tezimizin konusu olan koruma tedbirleri hakkında "depolanmış bilgisayar verilerinin aranması ve bunlara elkonulması" başlığıyla bir düzenleme yer almaktadır.

Arama tedbiri, kanun koyucu tarafından *ultima ratio* yani son çare olarak başvurulacak bir tedbir olarak düzenlenmiştir. Buna göre, bu tedbirin uygulanması için somut delillere dayana kuvvetli şüphe sebeplerinin varlığı ve soruşturma aşamasında başka bir şekilde delil elde etme imkanının bulunmaması gerekmektedir. Tedbir bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama olarak düzenlenmiştir fakat Yargıtay kararlarına göre bilgisayar terimi geniş olarak yorumlanmaktadır. Buna göre, başta akıllı telefonlar olmak üzere bilgi işleyebilen veya aktarabilen her türlü cihaz bilgisayar olarak değerlendirilmektedir. Ayrıca yönetmeliğe göre, arama tedbiri bilgisayara takıp çıkarılabilen aygıtlar hakkında uygulanabilmektedir.

Tedbir şüphelinin kullanımında olan bilgisayarlarda, bilgisayar programları ve kütüklerinde uygulanacaktır. Aramanın gerçekleştirilebilmesi için hâkim ya da 25 Temmuz 2018 tarihinde yapılan değişiklik ile birlikte, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından verilen arama kararı gereklidir. Cumhuriyet savcısı tarafından verilen karar hâkim onayına sunulacak ve hâkimin onay vermemesi durumunda alınan kopyalar ve çözümü yapılan metinler imha edilecektir.

Kural olarak arama tedbiri yerinde gerçekleştirilecektir. Bununla birlikte, şifrelerin çözülememesi, gizli verilere ulaşılamaması ya da yapılacak işlemlerin çok

uzun sürecek olması durumunda ilgili araç ve gereçlere elkonulabilecektir. Arama tedbirini uzaktan erişim ile uygulamak kanunen mümkün değildir. Bununla birlikte, Sanal Ortamda İşlenen Suçlar Sözleşmesi gereğince arama yapılan bilişim sistemlerinde erişilebilen verilerde arama gerçekleştirilebilmesi için kanuni düzenleme yapma yükümlülüğümüz bulunmaktadır. Ayrıca, ilgili yönetmelikte arama tedbirinin bilgisayar ağlarında ve bilgisayar aracılığıyla erişilebilen diğer bilgisayar kütüklerinde gerçekleştirilebileceği düzenlenmektedir. Dolayısıyla, arama yapılan bilgisayardan ulaşmak şartı ile uzakta bulunan bilgisayar kütüklerinde arama yapmak mümkündür fakat bu hüküm kanunilik ilkesi gereğince yönetmelik ile değil kanun ile düzenlenmesi gerekmektedir.

Arama tedbirinin uygulanması sonucunda elde edilen veriler ceza muhakemesi açısından delil niteliği taşıyorsa, bu verilerin birebir kopyaları alınacak ve çözülerek metin haline getirilecektir. Veri bütünlüğünün sağlanabilmesi için, alınan kopyalardan birinin şüpheliye veya vekiline verilmesi ve alınan kopyaların özet değerlerinin çıkartılması gerekecektir. Veri bütünlüğünün bozulması durumunda, elde edilen verilerin güvenilirliğine zarar geldiği için bu verilerin ceza muhakemesinde delil olarak kullanılabilmesi tehlikeye girecektir.

Kanunun ilk halinde elkoyma tedbiri, şifrelerin çözülememesi, gizli verilere ulaşılamaması durumlarında başvurulabilecek bir tedbir olarak düzenlenmiştir. Fakat, uygulamada kolluk kuvvetleri arama tedbirini uygulamadan bilgisayar ve diğer bilişim sistemlerine elkoymaktadır. Başta mülkiyet hakkı ve özel hayatın gizliliği gibi temel haklara müdahale teşkil eden elkoyma tedbirinin kolluk kuvvetleri tarafından kanuna uygun bir şekilde uygulanması yerine, 2018 yılında kanunda değişikliğe gidilmiş ve yapılan değişiklikle yapılacak işlemlerin çok uzun sürecek olması durumunda elkoyma tedbirine başvurulabileceğine dair hüküm eklenmiştir.

Elkoyma tedbirine başvurulması durumunda, bilişim sistemlerinde yer alan bütün verilerin birebir kopyaları çıkartılacak ve bu kopyalardan bir tanesi şüpheliye ya da vekiline teslim edilecektir. Ayrıca, gizli verilere ulaşılması, şifrelerin çözülmesi ve gerekli kopyaların çıkartılması durumunda elkonulan bilişim sistemleri iade edilecektir. İade edilecek bilgisayarların depolama birimlerinde çocuk pornografisi ya

da bilgisayar virüsü gibi suç unsuru teşkil edebilecek verilerin bulunması durumunda ne yapılacağına dair hüküm bulunmamaktadır. Bununla birlikte, uygulamada genel hükümlere başvurularak depolama birimlerinin müsadere edilmektedir. Öğretide ise elkonulan bilgisayar ve bilişim sistemlerinin suç unsuru teşkil eden verilerin depolama birimlerinden silinerek ya da ulaşılamaz hale getirilerek iade edilebileceği savunulmaktadır.

Kanunda arama ve elkoyma tedbirleri haricinde kopyalama tedbiri düzenlenmiştir. Bu tedbir, bilgisayarlarda ya da bilgisayar kütüklerinde yer alan verilerin tamamının ya da bir kısmının kopyalanması olarak ifade edilmiştir. Buradaki kopyalamadan anlaşılması gereken, ilgili verilerin imajının alınması yani birebir kopyasının çıkartılmasıdır.

Kopyalama tedbiri üç farklı şekilde uygulanabilmektedir. Bunlardan ilki arama sonucunda elde edilen verilerin kopyalanmasıdır. İkincisi, bilgisayarlara veya diğer bilişim sistemlerine elkoymaksızın, yalnızca arama tedbirinin uygulanacağı verilerin kopyalanmasıdır. Bu durumda, bilgisayarlara ve diğer bilişim sistemlerine elkonulması gerekmeyecektir. Sonuncusu ise, elkonulan bilgisayarlar ve bilgisayar kütüklerinde arama gerçekleştirilmesi sonucunda elde edilen verilerin kopyalarının çıkartılmasıdır.

Tezimizde son olarak bu tedbirlere karşı başvurulabilecek kanun yollarına ve kopyalama tedbiri sonucunda elde edilen verilerin yok edilmesi konusuna değinilmiştir.

Sonuç kısmında ise, yürürlükte bulunan kanun maddesi ve bu maddenin uygulaması ile ilgili eleştirilere yer verilmiştir. Ayrıca, eleştirilerimiz doğrultusunda kanun maddesi yeniden yazılmıştır.

BİRİNCİ BÖLÜM: ELEKTRONİK DELİL VE KARŞILAŞTIRMALI HUKUKTA BİLİŞİM SİSTEMLERİNDE ARAMA, KOPYALAMA VE ELKOYMA TEDBİRLERİ

I. TEMEL KAVRAMLAR

A. Bilişim

Bilişim, *"verinin saklanması, saklanan verinin elektronik olarak işlenmesi, organize edilmesi, değerlendirilmesi ve iletişim araçları ile aktarılması hususlarını ilgilendiren bir bilim dalı"*[1] olarak tanımlanmaktadır[2]. Dolayısıyla bilişim, hem verilerin işlenmesini, yani veri işlemi hem de verilerin aktarılmasını, yani veri iletişimini ifade eden bir kavramdır[3]. Ayrıca öğretide bilişim sistemlerinin tasarlanması, geliştirilmesi ve üretilmesi ile ilgili konuların da bilişim kapsamına girdiği belirtilmektedir[4].

Fransızca ***"informatique"***[5] sözcüğünün karşılığı olarak 1971 yılında Aydın Köksal tarafından önerilen[6] bilişim sözcüğü, Türkçe'de enformatik olarak da kullanılmaktadır. 765 sayılı Türk Ceza Kanunu'na "Bilişim Alanında Suçlar" babını ekleyen 3756 sayılı kanunda bilişim terimi kullanılmıştır. 5237 sayılı Türk Ceza

---

[1]Olgun Değirmenci, **Ceza Muhakemesinde Sayısal (Dijital) Delil**, Ankara: Seçkin, Mart 2014, s.53.
[2]Benzer tanımlar için Berrin Bozdoğan Akbulut, "Bilişim Suçları", **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, Konya, C. VIII, S. 1-2, 2000, s.546; Caner Yenidünya/Olgun Değirmenci, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul: Legal Yayıncılık, 2003, s.27; Cevat Özel, "Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı", **İstanbul Barosu Dergisi**, İstanbul, C. LXXV, S. 7-8-9, Eylül 2001, s.151; Ceyhun Yurdakul/Ufuk Çağlayan, **Bilgi Teknolojileri Türkiye İçin Nasıl Bir Gelecek Hazırlamakta**, Ankara: Türkiye İş Bankası Kültür Yayınları, 1997, s.1; Murat Volkan Dülger**, Bilişim Suçları ve İnternet İletişim Hukuku**, 4. Baskı, Ankara: Seçkin, 2014, s.67; Recep Yılmaz Yazıcıoğlu, **Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuksal Boyutları İle**, İstanbul: Alfa Kitabevi, 1997, s.131; Yüksel Ersoy, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", **Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi**, Ankara, C.XLIX, S.3-4, 1994, s.151.
[3]Akbulut, **Türk Ceza Hukukunda Bilişim Suçları**, s.13; Bozdoğan Akbulut, **Bilişim Suçları**, s.546.
[4]Emin Doğan Aydın, **Bilişim Suçları ve Hukukuna Giriş,** Ankara: Doruk Yayınları, 1992, s.3; Emin Doğan Aydın, "Bilişim Sistemlerinde Güvenlik, Güvenirlik, Mahremiyet ve Bilişim Suçları", **Marmara İletişim Dergisi**, İstanbul, S.1, Aralık 1992, s.109.
[5]Kavram benzer bir şekilde İngilizce'de "informatics", Almanca'da "informatiks", İtalyanca ve İspanyolca'da "informatica" olarak kullanılmaktadır.
[6]Nişanyan Sözlük, http://www.nisanyansozluk.com/?k=bili%C5%9Fim (Erişim Tarihi: 01.05.2018).

Kanunu'nda da bilişim terimini tercih eden Türk Kanun Koyucu ne kanun kapsamında ne de kanunun gerekçesinde bilişim tanımına yer vermiştir.

Yargıtay Ceza Genel Kurulu, 19 Haziran 2007 tarihli kararında[7] bilişimi *"bilgisayardan da faydalanılmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır hale gelmesine konu olan akademik ve mesleki disipline verilen ad."* olarak tanımlamıştır. Dolayısıyla, uygulamada da bilişim kavramı için öğretidekine benzer bir yaklaşımın benimsendiği ve bilişimin benzer bir şekilde tanımlandığı ifade edilebilecektir.

Son olarak aynı kararda, *"Her ne kadar çoğunlukla "bilişim" ile "bilgisayar" terimleri aynı anlamda kullanılmaktaysa da gerçekte bunlar aynı şey demek değildir. Zira, bilişim sözcüğü bilgisayar kelimesine oranla daha geniş kapsamlıdır."* denilmek suretiyle bilişim ile bilgisayar arasında bir ayrım yapılmıştır. Bu durum, öğretide Dülger tarafından eleştirilmiş ve bir bilim dalı olan bilişim ile bir makine olan bilgisayarın karşılaştırmaya tabi tutulamayacağı ifade edilmiştir[8].

B. Bilişim Sistemi

Bilişim sistemlerinde elektronik delillerin aranması kavramı, birçok hukuk sisteminde bilgisayarlarda arama kavramı ile ifade edilmektedir[9]. Nitekim hukukumuzda da elektronik delillerin elde edilebilmesi için uygulanacak koruma tedbirleri "bilgisayarlarda, bilgisayar programları ve kütüklerinde arama, kopyalama ve elkoyma" başlığıyla CMK m.134'te düzenlenmiştir.

Bilgisayar kavramının hukukumuzda tanımı bulunmamakla birlikte, Adalet Bakanlığı tarafından 2006 yılında hazırlatılan "Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı" kapsamında bilgisayar, "*belleğindeki programa uygun olarak aritmetik ve mantıksal işlemleri yapabilen,*

---

[7]Yargıtay Ceza Genel Kurulu E. 2007/6-136 K. 2007/150 T. 19.6.2007 (kararara ma.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).
[8]Dülger, **a.g.e.**, s.66.
[9]Değirmenci, **a.g.e.**, s.31.

karar verebilen, yürüteceği programı ve işleyeceği verileri ezberinde tutabilen, çevresiyle etkileşimde bulunabilen araçları" ifade etmektedir[10]. Ayrıca, öğretide bilgisayar "*çevre giriş birimleri vasıtasıyla almış olduğu veriyi, depolayan, üzerinde yüklü programlar vasıtasıyla işleyen, sonuçlar çıkartan, veriyi aktaran ve genel olarak tanımlanmış her sorun üzerinde çalışabilen bir aygıt[11]*" olarak tanımlanmaktadır. Bilgisayarın benzer aygıtlardan ayırt edici özellikleri olarak ise, bilişim yeteneğine sahip olması ve belirli bir amaca özgülenmemesi belirtilmektedir[12]. Örneğin, bilgisayarları, akıllı telefonları ve hatta artık beyaz eşyaları bile internete bağlayarak, bu cihazlar arasında internet vasıtasıyla veri aktarımını sağlayan ve dolayısıyla bilişim yeteneğine sahip olan bir modem, sadece cihazları internete bağlama görevine özgülendiği için bilgisayar olarak değerlendirilemeyecektir.

Bilişim yeteneğine sahip her türlü cihazı ifade eden bilişim sistemi kavramı ise, bilgisayarı da kapsayan bir üst kavramdır[13]. Her bilgisayar ya başlı başına bir bilişim sistemidir ya da bir bilişim sisteminin parçasıdır fakat her bilişim sistemi bilgisayar olarak nitelendirilemeyecektir[14]. Örneğin, bilgisayar tanımına uymayan banka ATM cihazları uygulamada Yargıtay tarafından bilişim sistemi olarak kabul edilmektedir[15]. Kanunun "bilgisayar" lafzı dar yorumlandığında, hafızalarında elektronik delil bulundurabilen bu cihazlarda, CMK m.134 kapsamında yer alan koruma tedbirleri uygulanamayacaktır.

Türk Kanun Koyucu 765 sayılı Türk Ceza Kanunu'nda, *"bilgileri otomatik işleme tabi tutan sistem"* ifadesine yer verirken, 5237 sayılı Türk Ceza Kanunu'nda bu ifadeden vazgeçerek, *"bilişim sistemi"* kavramını kullanmaya başlamıştır. Bu kavram değişikliği ile beraber, 5237 sayılı Türk Ceza Kanunu'nun gerekçesinde bir

---

[10]**Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı** (https://www.tbd.org.tr/bilisim-agi-hizmetlerinin-duzenlenmesi-ve-bilisim-suclari-hakkinda-kanun-tasarisi/) (Erişim Tarihi: 31.08.2019).
[11]Değirmenci**, a.g.e.**, s.39-40.
[12]Levent Kurt, **Açıklamalı ve Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunu'ndaki Uygulaması,** Ankara: Seçkin Yayınevi, Eylül 2005, s. 30; Değirmenci**, a.g.e.**, s.35.
[13]Yargıtay Ceza Genel Kurulu, E. 2007/6-136 K. 2007/150 T. 19.6.2007 (kararara ma.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).
[14]Değirmenci, **a.g.e.**, s.54; Dülger**, a.g.e.**, s.57.
[15]Yargıtay 10. Ceza Dairesi E. 2004/14311 K. 2004/10906 T. 2.11.2004 (www.kazanci.com) (Erişim Tarihi: 31.08.2019).

bilişim sistemi tanımına yer verilmiştir. Buna göre "*bilişim sisteminden maksat verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağı veren manyetik sistemlerdir"*[16].

Öğretide bu tanım birçok yazar tarafından eleştirilmiştir. Örneğin, Değirmenci bilişim sistemlerinin elektronik, manyetik, optik, elektrokimyasal ve elektromanyetik olabileceğini belirterek, tanımda yer alan manyetik sistemler ifadesinin tanımı gereksiz yere sınırladığı ifade etmiştir[17]. Ayrıca tanımda, verileri saklama, işleme ve iletme işlevleri olan bilişim sistemlerinin sadece veri-işlem özelliği ifade edilmekte fakat diğer işlevlerine temas edilmemektedir[18].

Uygulamada Yargıtay, bilişim sistemi tanımı olarak 5237 sayılı TCK'nın gerekçesinde yapılan tanımı benimsemektedir ve birçok kararında bu tanıma atıfta bulunmaktadır. Yargıtay'ın bu kararlarına göre, ATM cihazları[19], akıllı cep telefonları[20], tabletler[21], internet sitelerini içerisinde barındıran sunucular[22], elektronik posta adresleri[23] birer bilişim sistemidir. Ayrıca Yargıtay Ceza Genel Kurulunun 19.6.2007 tarihli kararında, Yargıtay Cumhuriyet Başsavcısı tarafından "belleğine bir yazılım yüklenebilme özelliği" ve "komut onaylaması" bilişim sistemlerinin temel özellikleri olarak belirtilmiştir[24].

---

[16]**Türk Ceza Kanunu Madde Gerekçeleri** (http://www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc) (Erişim Tarihi: 31.08.2019).
[17]Değirmenci, **a.g.e.**, s.55.
[18]Ali İhsan Erdağ, "Bilişim Alanında Suçlar (Türk ve Alman Hukukunda)", **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C. XIV, Y. 2010, Sa. 2, s.277.
[19]Yargıtay 10. Ceza Dairesi E. 2004/14311 K. 2004/10906 T. 2.11.2004 (www.kazanci.com) (Erişim Tarihi: 31.08.2019).
[20]Yargıtay 8. Ceza Dairesi E. 2014/30037 K. 2015/14023 T. 18.3.2015 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019); Yargıtay 8. Ceza Dairesi E. 2014/29566 K. 2015/13421 T. 11.3.2015 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).
[21]Yargıtay 8. Ceza Dairesi E. 2014/30037 K. 2015/14023 T. 18.3.2015.
[22]Yargıtay 6. Ceza Dairesi E. 2002/16699 K. 2003/6727 T. 13.10.2003 (www.kazanci.com) (Erişim Tarihi: 31.08.2019).
[23]Yargıtay 12. Ceza Dairesi E. 2015/9555 K. 2016/10731 T. 22.6.2016 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019); Yargıtay 12. Ceza Dairesi E. 2015/15933 K. 2016/277 T. 13.1.2016 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).
[24]Yargıtay Ceza Genel Kurulu E. 2007/6-136 K. 2007/150 T. 19.6.2007.

Avrupa Konseyi Siber Suç Sözleşmesi[25](AKSSS) kapsamında da bir bilişim sistemi tanımına yer verilmiştir. Uygun bulma kanunu ile iç hukukumuzun bir parçası haline getirdiğimiz sözleşmenin resmî gazetede yayınlanan çevirisinde her ne kadar **"bilgisayar sistemi"** ifadesi kullanılsa da sözleşmenin Fransızca nüshası ile İspanyolca, Portekizce ve Rumence dilindeki çevirileri incelendiğinde bu kavramın bilişim sistemini ifade etmek için kullanıldığı görülmektedir[26]. Dolayısıyla sözleşmeye göre bilişim sistemi terimi *"bir veya birden fazlası, bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbiriyle bağlantılı veya ilgili bir grup cihazı"* ifade etmektedir. Bu tanım, bilişim sisteminin yapısını ve veri-işlem işlevini ifade etse de TCK'nın gerekçesinde yer alan tanımda olduğu gibi bilişim sistemlerinin veri-iletim özelliğini ihmal etmektedir.

Ayrıca, "Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı" kapsamında da bir bilişim sistemi tanımı yapılmıştır[27]. Bu tasarıya göre *"bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistem"* bilişim sistemini ifade etmektedir. Bu tanım, bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan ifadesini kullanarak bilişim sisteminin yapısını oluşturan donanım ve yazılıma birlikte yer vermektedir. Ayrıca tanımda bilişimin sistemlerinin temel işlevleri olan veri işleme, veri saklama ve veri iletimi de belirtilmiştir. Dolayısıyla, tasarı kanunlaşmasa da bizce

---

[25]Avrupa Konseyi Siber Suç Sözleşmesi, Türkiye tarafından 10 Kasım 2010 tarihinde imzalanmış ve uygun bulma kanunu ile iç hukukumuzun bir parçası haline getirilmiştir. Öğretide ve Avrupa Konseyi'nin resmî sitesinde yer alan Türkçe çevirisinde "Avrupa Konseyi Siber Suç Sözleşmesi" adıyla anılan sözleşme, 22 Nisan 2014 tarihli uygun bulma kanunu ile onaylanmış ve 2 Mayıs 2014 tarihinde Resmi Gazete'de "Sanal Ortamda İşlenen Suçlar Sözleşmesi" olarak yayımlanmıştır.

[26]Sözleşmenin Fransızca nüshasında **"système informatique"**, İspanyolca ve Portekizce çevirilerinde **"sistema informatico"**, Rumence çevirisinde ise **"sistem informatic"** kavramları kullanılmaktadır. Fransızca nüshası için bakınız https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008156d (Erişim Tarihi:31.08.2019), İspanyolca çevirisi için bakınız https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c (Erişim Tarihi: 31.08.2019), Portekizce çevirisi için bakınız https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa428 (Erişim Tarihi: 31.08.2019), Rumence çevirisi için bakınız https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41f (Erişim Tarihi: 31.08.2019).

[27] **Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı** (https://www.tbd.org.tr/bilisim-agi-hizmetlerinin-duzenlenmesi-ve-bilisim-suclari-hakkinda-kanun-tasarisi/) (Erişim Tarihi: 31.08.2019).

tasarıda yer alan tanım isabetli bir tanımdır[28] ve biz de çalışmamızda bilişim sistemi tanımı olarak bu tanımı benimseyeceğiz.

Bilişim sistemleri temel olarak donanım ve yazılım olarak iki unsurdan oluşmaktadır. Donanım, bilişim sisteminin somut unsurudur. Öğretide donanım merkezi işlem birimi (CPU), hafıza, giriş ve çıkış birimleri olarak dörde ayrılmaktadır[29]. Klavye, dokunmatik ekran ya da USB bellek gibi giriş birimleri bilişim sistemine verinin girişini sağlamaktadır. Bilişim sistemine giren veriler hafıza birimlerinde depolanmakta, depolanan veriler ise merkezi işlem birimi tarafından işlenmektedir. Son olarak çıkış birimleri ise, işlenen veya depolanan verinin kullanıcıya tekrar aktarılmasını sağlayan yazıcı, ekran gibi donanımlardır. USB bellek, DVD ya da bilişim sistemlerinin iletişim altyapılarının bir parçası olan modem gibi cihazlar hem giriş hem de çıkış birimi olabilmektedir. Ayrıca, giriş ve çıkış birimleri çevre birimleri olarak da adlandırılmaktadır[30].

Bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirleri, bilişim sistemlerinin çevre birimleri ile hafıza birimlerinde uygulanabilmektedir. Fakat bu koruma tedbirleri açısından, hafıza birimleri ayrı bir öneme sahiptir. Çünkü, RAM (Rastgele Erişim Belleği) ve Önbellek gibi hafıza birimlerinde veriler sabit disk ya da ROM (Salt Okunur Bellek) gibi hafıza birimlerinin aksine uçucu bir haldedir ve bilişim sistemi kapatıldığı takdirde bu veriler yok olmaktadır. Verilerin uçucu halde bulunduğu hafıza birimlerinde ilgili koruma tedbirleri uygulanırken bu durum dikkate alınmadığı taktirde, elektronik delil niteliğine haiz olabilecek bir kısım veriler geri döndürülemez bir şekilde yok olabilecektir.

Yazılım ise bilişim sistemlerinin soyut unsurudur. Bilişim sisteminden ayrı bir somut bir varlığa sahip olmayan yazılım, programlar ve bu programlar tarafından

---

[28]Nitekim öğretide Tanrıkulu da benzer bir yaklaşımı benimsemektedir. Bkn. Cengiz Tanrıkulu, **Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma**, Ankara: Adalet Yayınevi, 2014, s.13.

[29]Eoghan Casey, **Digital Evidence and Computer Crime: Forensic Science, Computers and The Internet**, Third Edition, Academic Press, April 2011, s.439-440.

[30]J. Stanley Warford, **Computer Systems**, Canada: Jones and Bartlett Publishers, 2010, Fourth Edition Kindle Version, p.1.2.

işlenen verilerden oluşmaktadır. Yazılım, donanımla kullanıcı arasında köprü görevi görmektedir. Dolayısıyla yazılım olmadan, donanım bir mana ifade etmemektedir[31].

C. Bilgisayar Programı

Hukukumuzda bilgisayar programın Ceza Muhakemesi Kanunu kapsamında tanımı yapılmasa da Fikir ve Sanat Eserleri Kanunu'nun 1. maddesinde tanımlandığı görülmektedir. Buna göre, bilgisayar programı "*bir bilgisayar sisteminin özel bir işlem veya görev yapmasını sağlayacak bir şekilde düzene konulmuş bilgisayar emir dizgesini ve bu emir dizgesinin oluşum ve gelişimini sağlayacak hazırlık çalışmaları*" olarak tanımlanmaktadır. Tanımda verilen emir dizgileri, programlama dilleri adı verilen belirli kurallar çerçevesinde yazılmaktadır[32]. Değirmenci, tanımın hazırlık çalışmalarına da yer verecek şekilde geniş ele alınmasını kanunun kapsamına ve koruduğu hukuki değerlere bağlamaktadır[33].

Bilgisayar programları, temel olarak iki temel gruba ayrılmaktadır: İşletim sistemleri ve uygulama programları. İşletim sistemleri bilgisayarın çalışmasını sağlayan temel programlar olup, görevleri işlemci, hafıza ve dosya yönetimidir[34]. Bilgisayarlarımızda Windows, akıllı telefonlarımızda ise Android birer işletim sistemi örnekleridir. Uygulama programları ise, kullanıcıların ihtiyaçları doğrultusunda belirli işleri yapmak için oluşturulmuş programlar olup, hayatın her alanında işlem gerçekleştirmek ve iş yükünü hafifletmek amacıyla sayılamayacak kadar çok türe sahiptir[35]. Örneğin, bilgisayarlarda yazı yazmak için kullandığımız Microsoft Word, ".pdf" uzantılı belgeleri okumak için kullandığımız Adobe Acrobat Reader veya internet sitelerine erişmek için kullandığımız Mozilla Firefox birer uygulama yazılımlarıdır.

---

[31]Osman Gazi Ünal**, Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma**, Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Ceza ve Ceza Usul Hukuku Bilim Dalı, Ankara, 2011, s.8.
[32]Mustafa Balay/Neşe Erses, **Bilgisayar Kullanımı ve İnternet**, Ed: Aysan Şentürk, 2. Baskı, Bursa: Ekin Kitabevi, Kasım 2005, s. 8.
[33]Değirmenci, **a.g.e.**, s.51.
[34]Watford, **a.g.e.**, p.1.1.3.
[35]Değirmenci, **a.g.e.**, s.51.

D. Bilgisayar Kütüğü

Bilgisayar kütüğü, bilgisayarda verilerin ve programların kaynak ve nesne olarak saklandığı mantıksal bir depolama birimidir[36] ve kütükler ilgili programlar kullanılarak kullanıcılar tarafından oluşturulmaktadır[37]. Örneğin, kullanıcı tarafından kelime işlemci programı kullanılarak bilgisayarda bir yazı yazıldığında, bilgisayar tarafından bir kütük (dosya) oluşturulmaktadır. Kullanıcı tarafından yazılan bu yazı yani veriler de oluşturulan bu kütük içerisinde depolanmaktadır.

Bilgisayar kütüğü, bazı yazarlar tarafından İngilizce "log" kelimesinin karşılığı olarak kullanılsa da aslında "computer file" kavramının Türkçe karşılığıdır[38]. Nitekim, TDK Bilgisayar Terimleri Karşılıklar Kılavuzunda "log" kelimesinin karşılığı olarak "günlük" kelimesi, "file" kelimesinin karşılığı olarak ise "kütük" ve "dosya" kelimeleri kullanılmıştır[39]. Değirmenci ise kütükleri insan müdahalesi ile bilgisayar tarafından oluşturulan, günlükleri ise insan müdahalesi olmadan bilgisayar tarafından oluşturulan dosyalar olarak tanımlayarak kütük(file) ve günlük(log) kavramlarının farklı şeyleri ifade ettiğini belirtmiştir[40].

Uygulamada Yargıtay, AKSSS Açıklayıcı Raporunun 187. maddesine[41] atıfta bulunarak, bilgisayar kütüğünü sadece arama yapılan bilgisayarın mantıksal depolama birimleri olarak değerlendirmemekte ve bilgisayar kütüğü kavramı içine internet servis sağlayıcılarının internet erişimi sağladıkları kullanıcılara ait IP numaralarını, diğer erişimleri sağladıkları veri tabanlarını, bir bilgisayar üzerinden ulaşılabilen ortak

---

[36]İbrahim Türkoğlu, **BİL391 İşletim Sistemleri (Ders Notları)**, Elâzığ, 2006, s. 23 http://eng.harran.edu.tr/~nbesli/OS/book1.pdf (Erişim Tarihi: 01.05.2018).
[37]Değirmenci, **a.g.e**., s. 52.
[38]Benzer yaklaşım için, Değirmenci, **a.g.e**., s.52.
[39]Şükrü Haluk Akalın/Erdoğan Bada/Zeynel Cebeci/Levent Acar/Bülent Mıtış/Ali Tan, **Bilgisayar Terimleri Karşılıklar Kılavuzu**, Ankara: Türk Dil Kurumu Yayınları, 2008.
[40]Değirmenci, **a.g.e**., s. 53.
[41]**AKSSS Açıklayıcı Raporu** m.187 *"…bilgisayar sistemlerinin birbirlerine bağlanabilme özelliklerinden dolayı veriler doğrudan aramanın yapıldığı bilgisayarda değil, ama o sistemden kolayca erişilebilecek bir durumda olabilir. Bilgisayarla doğrudan ya da İnternet gibi iletişim sistemleri üzerinden dolaylı olarak bağlantılı bir veri saklama cihazında bulunabilirler. Bu durum, aramayı verilerin gerçekte bulunmakta olduğu yeri içine alacak şekilde genişletmeye (ya da verileri bulundukları yerden aramanın yapılmakta olduğu bilgisayara getirmeye) ya da geleneksel arama yetkilerini her iki noktada daha koordine ve hızlı bir biçimde kullanmaya izin verecek yeni yasaları gerektirebilir ya da gerektirmeyebilir."*. https://rm.coe.int/16800cce5b (Erişim Tarihi: 25.08.2019).

paylaşıma ve kullanıma açık diğer bilgisayarlardaki veri depolama araçlarını da dahil etmektedir[42]. Nitekim bu husus Adli ve Önleme Aramaları Yönetmeliği[43]'nin 17. maddesinin 3. fıkrasında da "*Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır.*" denilerek ifade edilmiştir.

E. Veri

Veri, bilginin bilişim sistemi tarafından işlenebilmesi için belirli bir formata dönüştürülmüş halidir ve bilişim sistemlerinin en temel birimini oluşturur[44]. Bilişim sistemleri, verileri saklayabilir, üzerinde işlem yapabilir, sonuçlar üretebilir, gerektiğinde yeniden okuyabilir ve bu verileri diğer bilişim sistemlerine iletebilir[45]. Veriler sayısal, alfabetik ve işaret özellikli olabilirler, dolayısıyla görünüşte bir değer ifade etseler de anlaşılmaları ancak bilişim sistemleri aracılığıyla olabilmektedir[46]. Veriler, örneğin sistem günlük kayıtları, güvenlik kamerası kayıtları gibi bilişim sistemleri tarafından otomatik olarak oluşturulabileceği gibi, bilişim sistemi kullanıcıları tarafından da oluşturulabilmektedir[47].

Hukukumuzda, veri, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 2. maddesinde "*bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer*" olarak tanımlanmıştır[48]. Ayrıca, AKSSS'de bilgisayar verisi tanımı yer

---

[42]Yargıtay Ceza Genel Kurulu E. 2017/16-956, K. 2017/370, T. 26.9.2017 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).
[43]**Adli ve Önleme Aramaları Yönetmeliği**, Resmî Gazete Tarihi: 01.06.2005 Resmî Gazete Sayısı: 25832.
[44]Zakir Avşar/Gürsel Öngören, **Bilişim Hukuku**, İstanbul: Türkiye Bankalar Birliği, 2010, s.31; Yenidünya/ Değirmenci, **a.g.e**., s.47; benzer tanımlar için Yazıcıoğlu, **a.g.e**., s.29; İlker Tepe, "İnternet (Bilişim) Ceza Hukuku Örneğinde Türk Ceza Hukuku'ndaki Yeni Gelişmeler", **Alman-Türk Karşılaştırmalı Ceza Hukuku**, (Yayına Hazırlayanlar: Prof. Dr. Eric Hilgendorf – Prof. Dr. Yener Ünver), Cilt I, İstanbul, 2010, s.276.
[45]Değirmenci, **a.g.e.,** s.48; Dülger, **a.g.e.,** s.74-76; Ünal, **a.g.e.,** s.10.
[46]Kurt, **a.g.e.**, s. 39
[47]Leyla Keser Berber, **Adli Bilişim: Computer Forensic**, Ankara:Yetkin Yayınları, 2004, s.46.; Yargıtay 16. Ceza Dairesi E. 2015/4672 K. 2016/2330 T.21.04.2016 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).
[48]Aynı tanıma 2006 tarihli Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı'nın 2. maddesinde de yer verilmiştir.

almaktadır. Buna göre, "*bilgisayar sisteminin bir işlevi yerine getirmesini mümkün kılan bir programı da kapsayan, olguların, bilgilerin ve kavramların bir bilgisayar sisteminde işlenmeye uygun haldeki her türlü temsili*" bilgisayar verisidir. Bu tanımdan, 5651 sayılı kanunda yer alan tanımdan farklı olarak, bilgisayar programlarının da veri kapsamında değerlendirilmesi gerektiği anlaşılmaktadır. Nitekim benzer bir şekilde Türk Kanun Koyucu da Türk Ceza Kanunu'nun 243. maddesinin gerekçesinde "*sistem içindeki bütün soyut unsurlar, fıkrada geçen veri teriminin kapsamındadır.*" diyerek sistemin veri haricinde soyut unsurları olan da veri kapsamında değerlendirilmesi gerektiği ifade etmiştir.

Öğretide ise bu tanımlar veriyi sadece bilgisayar verisi olarak özelleştirilmesinden dolayı eleştirilmiştir. Nitekim Ünal, dar bir yorum yapıldığında elektronik yapıdaki delillerin sadece bilgisayardan elde edilebileceği sonucunun çıkartılabileceğini ve dolayısıyla bu bakış açısının CD, DVD ve taşınabilir bellek gibi veri saklama birimlerinin araştırılmasını engelleyebileceğini belirtmiştir[49]. Benzer bir görüşü benimseyen Dülger de bilgisayar verisi kavramı yerine sadece "veri" ya da "sanal veri" kavramlarının kullanılması gerektiğini ifade etmektedir[50].

Veri, bilişim sistemlerimde üç durumda bulunabilmektedir: Durağan haldeki veri (*at rest*), işlem halindeki veri (*in execution*) ve akış halindeki veri (*in motion*). Durağan haldeki veri, bilişim sistemlerinin sabit disklerinde bulunmaktadır ve bu veriler bilgisayar kütüklerinden silinse dahi varlıkları sabit diskler üzerinde devam etmektedir. İşlem halinde veri, bilişim sistemlerinin rastgele erişim belleklerinde ile önbelleklerinde bulunmaktadır ve bu veriler durağan haldeki verileri aksine bilişim sistemi her kapatıldığında silinmektedir. Son olarak akış halindeki veri ise, bir bilişim sisteminden diğer sisteme internet veya yerel ağ gibi bir ağ vasıtasıyla aktarılmakta olan veridir ve bu veriler bilişim sistemlerinde depolanmamaktadır[51]. Verilerin bu şekilde sınıflandırılmasının ceza muhakemesi hukuku açısından önemi ise, durağan haldeki veriler ile işlem halindeki verilerin bilgisayarlarda, bilgisayar programlarında

[49]Ünal**, a.g.e.**, s.12; benzer görüş için Dülger, **a.g.e.**, s.75; Veli Özer Özbek, "Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi", **İÜHFM**, Cilt LIX S.1-2, İstanbul, 2001, s.197.
[50]Dülger, **a.g.e.**, s.75.
[51]Dominik Kirk/Christoph Wegener, "Technical Issues of Forensic Investigations in Cloud Computing Environments", **Workshop on Crytography and Security in Clouds**, Zurich, March 2011, s.2.

ve bilgisayar kütüklerinde arama, kopyalama ve elkoymayı düzenleyen CMK m.134 kapsamında delil niteliğine sahip olabilecekken; akış halindeki verilerin ancak iletişimin tespit, dinlenmesi ve kayda alınmasını düzenleyen CMK m.135 kapsamında delil niteliğine sahip olabilecek olabilmesidir.

Ayrıca adli bilişimde bilgisayar verileri altı farklı düzeyde değerlendirilmektedir. Sıfırıncı düzeyde bilgisayar kütüklerinde yer alan dosyaların isimleri, üstverileri (*metadata*) ve içerikleri bulunmaktadır. Birinci düzeyde, çöp kutusunda yer alan dosyalar, yazıcı kuyruk dosyaları ya da tarayıcı ara bellek dosyaları gibi geçici dosyalar bulunmaktadır. İkinci düzey ise silinmiş dosyalardan oluşmaktadır ve düzeyde dosyalar dosya kütüklerinden silinmiş olmalarına rağmen sabit disk üzerinde varlıklarını sürdürmektedirler. Bu dosyalar dosya kurtarma uygulamaları aracılığıyla kurtarılabilmektedir. Üçüncü düzeyde, kurtarılma faaliyetlerine rağmen bilgisayar kütüklerinde hangi dosyaya ait olduğu tespit edilemeyecek şekilde üzerine veri yazılmış dosyalar yer almaktadır. Dördüncü düzeyde üretici firma tarafından gizlenmiş dosyalar bulunmaktadır. Sürücü kontrolünü yapan ya da bozuk sektörleri yöneten yazılımların bulunduğu bu dosyalara sadece üretici firma ulaşabilmektedir. Son ve beşinci düzeyde ise üzerine yazılma işlemi yapılmış dosyalar bulunmaktadır.[52]

II. ELEKTRONİK DELİL

A. Tanım

Elektronik ve bilişim teknolojilerinde yaşanan gelişmeler, hayatın her alanını olduğu gibi ceza muhakemesi hukukunu da etkilemekte ve değiştirmektedir. Bilgi toplumu olarak adlandırdığımız günümüzde, bu teknolojiler kullanılarak üretilen cihazlar, kanunen suç olarak düzenlenmiş eylemlerde araç veya amaç olarak kullanılabilmekte ya da suçların hazırlık aşamalarında bu cihazlardan faydalanılabilmektedir. Locard'ın Değişim Teorisine[53] göre, fail suçu işlerken yararlandığı bu elektronik cihazlar üzerinde izler bırakmaktadır. İşte bu izler ceza

[52]Bhanu Prakash Battula/B. Kezia Rani/R. Satya Prasad/T.Sudha**,** "Techniques in Computer Forensics: A Recovery Perspective", **Internatinal Journal of Security**, Vol.3, Issue 2., s.29.
[53]"*Locard'ın Değişim Teorisi birbiriyle temasta bulunan iki nesnenin, birbirleri üzerinde ve olay yerinde birtakım izler bırakacağını ifade etmektedir*." Değirmenci, **a.g.e.**, s.25.

muhakemesinde delil olarak kullanılabilmekte ve "*elektronik delil*" olarak adlandırılmaktadır.

Elektronik delil kavramının tanımı ile ilgili öğretide bir görüş birliğinin bulunduğunu söylemek mümkündür. Berber, elektronik delil kavramını "*elektronik bir cihaz üzerinde saklanan veya bu cihazlar aracılığıyla iletilen soruşturma açısından değerli olan bilgi ve veriler*[54]" olarak tanımlamaktadır ve uygulamada Yargıtay tarafından bu tanım benimsenmektedir[55]. Mason ise "*(analog cihazların çıktıları ve dijital formattaki her türlü veri de dahil olmak üzere) herhangi bir aygıt, bilgisayar ya da bilişim sistemi tarafından üretilen, değiştirilen, saklanan veya iletilen ya da iletişim sistemi üzerinde aktarılan ve hüküm süreci ile ilgili olan veriler*[56]" diyerek benzer bir tanıma yer vermiştir. Çalışmamız elektronik delil tanımı olarak, uygulamada olduğu gibi, Berber tarafından yapılan tanım benimsenmiştir.

B. Analog ve Sayısal Delil Ayrımı

Elektronik deliler, kendi içerisinde analog deliller ve sayısal deliller olarak ikiye ayrılmaktadır. Analog sistemler aracılığıyla üretilen ve ispat değerine haiz veriler analog delilleri oluşturmaktadır. Plaklar, fotoğraf filmleri, ses kayıt bantları gibi araçlar üzerinde saklanan analog delillerin ceza muhakemesinde savcı ve hakimler tarafından incelenmesi kolay olsa da bu delillerin üzerinde değişiklik yapmanın mümkün olduğu unutulmamalıdır[57]. Örneğin, 1937 yılında analog bir cihaz ile çekilen bir fotoğrafta Hitler ile dönemin propaganda bakanı Goebbels beraber yer alırlarken, bu fotoğrafın daha sonraki hallerinde Goebbels fotoğrafta bulunmamaktadır[58].

---

[54]Keser Berber, **Adli Bilişim: Computer Forensic**, s.46.
[55]Yargıtay 16. Ceza Dairesi E.2015/4672 K.2016/2330 T. 21.4.2016 (kararara ma.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).
[56]Stephen Mason, "Indroduction", **International Electonic Evidence**, British Institute of International and Comparative Law, 2008, s.xxxv.
[57]Mason**, a.g.e.,** s.xxxv.
[58]Melissa Stanger, **6 People Who Were Literally Erased From History**, http://www.businessinsider.com/people-who-were-erased-from-history-2013-12 (Erişim Tarihi: 01.05.2018)

Sayısal deliller ise sayısal formda saklanan veya iletilen ve ispat değeri bulunan veriler olup[59] bilişim sistemleri, bilgisayar ağları, bilgisayar programları ile CD, DVD, USB bellek, disket, harici ve dahili harddisk, çağrı cihazı, cep bilgisayarları ve cep telefonları gibi diğer elektronik cihazlardan elde edilebilmektedir[60]. Dolayısıyla, CMK m.134 kapsamında bilişim sistemlerinden elde edilecek veriler, ceza muhakemesinde sayısal delil kapsamında değerlendirilecektir. Buna ek olarak, kısaca "veriler hakkındaki veriler" olarak tanımlanan ve bir sayısal delilin geçerliliğini, özelliklerini, ne zaman ve kim tarafından oluşturulduğunu, kimler tarafından kullanılıp değiştirildiğini gösteren üstveriler (metadata) [61] de sayısal delil kapsamındadır[62].

Ayrıca belirtmek gerekir ki, öğretide elektronik delil ve sayısal delil kavramları birbirinin yerine kullanılabilmektedir[63]. Fakat, yukarıda bahsettiğimiz gibi elektronik deliller, sayısal delilin bir üst kavramıdır. Ayrıca, sayısal delilin elektronik delil yerine kullanılması, analog delillerin elektronik deliller kapsamında incelenememesine sebep olacaktır. Bu sebeple, biz sayısal ve elektronik delil kavramlarının birbirinin yerine kullanılmasını doğru bulmuyoruz.

C. Sayısal Delilin Özellikleri

Sayısal deliller, gözle görünmez ve gizli niteliktedir. Bu sebeple sayısal delillerin incelenmesi, klasik delillerden farklı olarak, ancak uygun donanım ve

---

[59]Mark M. Pollitt, "Report on Dijital Evidence", **13th INTERPOL Forensic Science Symposium**, Lyon, France, October 16-19 2001, D. 4, s. 86; sayısal delil kavramı ile ilgili diğer tanımlar için bkn. Eoghan Casey, **a.g.e.**, 2011, s.7; Michael B.Mukasey/Jeffrey L. Sedgwick/David W. Hagy, **Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition**, Washington: National Institute of Justice, Nisan 2008, s.IX http://www.ncjrs.gov/pdffiles1/nij/219941.pdf (Erişim Tarihi: 02.06.2018).

[60]Wayne Jekot, "Computer Forensics, Search Strategies and the Particularity Requirement", **Pittsburgh University Journal of Technology Law and Policy**, V. VII, Spring 2007, s.6.; Yargıtay 16. Ceza Dairesi E. 2015/4672 K.2016/2330 T. 21.4.2016 (kararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

[61]Nadine C. Warner, "Metadata 101: What Lies Beneath", **American Bar Association The Public Lawyer**,Volume 12, No. 2, Summer 2004, s.1 https://www.americanbar.org/content/aba/tools/digitalassetabstract.html/content/dam/aba/migrated/govpub/mo/premium-gd/plom/PLwin04_Warner.pdf (Erişim Tarihi: 01.05.2018); Craig Ball, **Beyond Data about Data: The Ligitator's Guide to Metadata**, 2005, http://www.craigball.com/metadata.pdf (Erişim Tarihi: 01.05.2018).

[62]Değirmenci, **a.g.e.**, s.133

[63]Değirmenci, **a.g.e**., s.128; Ünal, **a.g.e.**, s.16.

yazılımla mümkün olabilecektir[64]. Örneğin, hafıza kartında yer alan bir fotoğraf dosyasını inceleyebilmek için, donanım olarak hafıza kartı okuyucusuna sahip bir bilgisayara; yazılım olarak ise bilgisayarı çalıştıran işletim sistemine ve fotoğraf görüntüleyici bir uygulama programına ihtiyaç duyulacaktır.

Sayısal deliller hassas bir yapıya sahiptir. Nitekim uygulamada Yargıtay da sayısal delillerin gizlenmeye, değiştirilmeye ve bozulmaya elverişli olduğunu ifade etmektedir[65]. Dolayısıyla, sayısal delillerin olay yerinden toplanılması, muhafazası aşamalarında belli yöntem ve kurallar öngörülmüştür. Bu adli bilişim yöntem ve kurallarına uyulmadığı taktirde, deliller tahrip olabilecek ya da delillerin tamamen yok olması riski ile karşı karşıya kalınabilecektir[66]. Örneğin, verilerin uçucu halde bulunduğu Rastgele Erişim Belleği gibi hafıza birimlerinde adli bilişim faaliyetleri yürütülürken, ilgili yöntem ve kurallar dikkate alınmayarak bilişim sistemi kapatıldığı taktirde, Rastgele Erişim Belleğindeki sayısal deliller geri döndürülemez bir şekilde yok olabilecektir.

Sayısal deliller kolaylıkla kopyalanabilmekte ve delil incelemeleri kopya üzerinden yapılabilmektedir[67]. Sayısal delillerin hassas yapısından ötürü, deliller üzerinde birebir kopyalama yöntemi uygulanarak, delillerin imajları oluşturulması ve adli bilişim faaliyetlerinin bu imajlar üzerinden yürütülmesi gerekebilmektedir[68]. Nitekim kanun koyucu da bu durumu dikkate alarak, CMK m.134 kapsamında "*bilgisayarlarda, bilgisayar program ve kütüklerinde kopyalama*" tedbirini düzenlemiştir. Ayrıca, sayısal delillerde orijinal ve kopya arasında kıyaslama yapılarak, delil üzerinde bir değişiklik yapılıp yapılmadığını tespit etmek

---

[64]Değirmenci, **a.g.e.**, s.132; Ünal, **a.g.e.**, s.27; Kubilay Say, "Bilişim Suçlarında Olay Yeri İncelemesinin Hukuki Boyutu", **Ses, Görüntü ve Data İncelemeleri**, Ed: Levent Bayram, Ankara: Adalet Yayınevi, 2008., s. 256; Mukasey/ Sedgwick/ Hagy, **a.g.e.**, s.IX.

[65]Yargıtay 9. Ceza Dairesi E. 2013/9110 K. 2013/12351 T. 9.10.2013 (kararara ma.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).; Yargıtay 16. Ceza Dairesi E. 2015/4672 K.2016/2330 T. 21.4.2016 (kararara ma.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

[66]Keser Berber, **Adli Bilişim: Computer Forensic**, s.8; Ünal, **a.g.e.**, s.16-17, Değirmenci, **a.g.e.**, s.133; Hakan Aydoğan, **Adli Bilişimde Yeni Elektronik Delil Elde Etme Yöntemleri**, Yayımlanmamış Yüksek Lisans Tezi, Polis Akademisi Güvenlik Birimleri Enstitüsü Güvenlik Stratejileri Yönetimi Anabilim Dalı, Ankara, 2009, s.31.

[67]Ünal, **a.g.e**., s.18.

[68]Semih Dokurer, "Adli Bilişim"**, Ses Görüntü ve Data İncelemeleri**, Ed: Levent Bayram, Ankara: Adalet Yayınevi, 2008., s.244.

mümkündür[69]. Bu kıyaslama için kullanılan "*hashing*" gibi yöntemlere çalışmamızın ileriki kısımlarında değinilecektir.

Sayısal delillerin bir başka özelliği ise, silinmelerinin veya yok edilmelerinin zor olmasıdır[70]. Bilişim sistemlerinin hafıza birimlerinde depolanan veriler kullanıcı tarafından silinse ve hatta silinen bu veriler üzerine başka veriler yazılsa dahi adli bilişim yöntemleriyle bu veriler kurtarılabilmektedir.

Türk Ceza Muhakemesi Hukukunda delil serbestisi ilkesi benimsenmiştir ve deliller arası hiyerarşi bulunmamaktadır. Dolayısıyla sayısal veriler, diğer delil türlerinden farklı özellikler göstermesine rağmen delil niteliğine haiz olacak ve hükme esas teşkil edebilecektir[71]. Bununla birlikte, sayısal delillerin hukuka uygun delil olarak kabul edilebilmeleri için aşağıda sayılan niteliklere sahip olması gerekmektedir:

1) Sayısal deliller mahkemede görülmekte olan davada kullanılabilir ve kabul edilebilir olmalıdır.
2) Sayısal deliller, mahkemedeki dava konusu olayla ve faille ilgili olmalı ve aynı zamanda aslına uygun ve güvenilir olmalıdır.
3) Sayısal delillerin elde edilme yolları güvenilir olmalı, deliller hatasız ve doğru olmalıdır.
4) Elde edilebilecek tüm sayısal deliller eksiksiz ve tam olmalıdır.
5) Sayısal deliller ispat değerine haiz ve mahkemeyi ikna edebilir olmalıdır.
6) Sayısal deliller hukuka uygun olmalıdır[72].

D. Sayısal Delil ile ilgili Kabul Edilen İlkeler

Bilişim teknolojilerinin gelişmesi sonucunda ortaya çıkan sayısal delillere hem hukuk muhakemesi hem de ceza muhakemesi açısından hâkim olacak ilkelerin

---

[69]Ünal**, a.g.e**., s.18.
[70]Ünal**, a.g.e**., s.18.
[71]Yargıtay 9. Ceza Dairesi E. 2013/9110 K. 2013/12351 T. 9.10.2013 (kararara ma.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).
[72]Peter Sommer, "Digital Evidence Emerging Problems in Forensic Computing", **LSE**, 2002, s.25; Ali Karagülmez, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, Ankara: Seçkin Yayıncılık, 2014, s.509.

belirlenmesi için ulusal ve uluslararası organizasyonlar tarafından birçok etkinlik, panel düzenlenmiş ve çalışma grupları oluşturulmuştur. Bu çalışmalar neticesinde sayısal delil ile bu delillerin elde edilmesi ve saklanması ile ilgili temel ilkeler tespit edilmeye çalışılmıştır. Türk ceza muhakemesi hukuku açısından bir bağlayıcılığı olmamakla birlikte, bu ilkeler sayısal deliller ile ilgili yol gösterici nitelikler taşımaktadır.

1. Avrupa Konseyi Elektronik Delil Rehberi

Bilişim suçlarıyla mücadelenin güçlendirilmesi amacıyla, Avrupa Birliği ve Avrupa Konseyi işbirliği ve Arnavutluk, Bosna-Hersek, Hırvatistan, Karadağ, Sırbistan, Kuzey Makedonya, Türkiye ve Kosova devletlerinin katılımıyla "Cybercrime@IPA" adıyla bir ortak proje başlatılmıştır. Bu projeye ek olarak 2012 yılında Avrupa Konseyi tarafından Octopus Konferansları düzenlenmiştir. Hem konferanslar hem de proje kapsamında yapılan çalışmalar neticesinde elde edilen sonuçlar bir araya getirilerek, 18 Mart 2013 tarihinde "Avrupa Konseyi Elektronik Delil Rehberi – Kolluk Kuvvetleri, Savcılar ve Hakimler için Temel Rehber" adıyla yayınlanmıştır[73]. Okuyucular tarafından yapılan geri bildirimler sonucunda rehber güncellenerek, 15 Aralık 2014 tarihinde bir kez daha yayınlanmıştır.

Rehber kapsamında elektronik deliller, elektronik delillerin elde edilebileceği kaynaklar, arama ve elkoyma tedbirleri, internet üzerinden elde edilen sayısal deliller, sayısal delilin incelenmesi ve mahkemeye sunulması ile bilgiler verilmiş ve elektronik delillerin elde edilmesi ile ilgili beş temel ilke benimsenmiştir[74].

Bunlardan ilki veri bütünlüğüdür. Mahkemede delil olarak kullanılacak herhangi bir veride, elektronik cihazda ya da medyada herhangi bir değişiklik yapılmamalıdır. Arama ve elkoyma tedbirini uygulayan ve daha sonrasında elde edilen

---

[73]**Counsil of Europe Electronic Evidence Guide – A Basic Guide for Police Officers, Prosecutors and Judges**, Version 2.0, Cybercrime Division - Directorate General of Human Rights and Rule of Law, Strasbourg – France, 15 December 2014, s.8.

[74]**Counsil of Europe Electronic Evidence Guide,** s.14-15.; **Electronic Evidence – A Basic Guide for First Responders, European Union Agency for Network and Information Security**, s.5 https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders (Erişim Tarihi: 07.08.2019).

delilleri muhafaza eden görevliler, ilgili verilerin bütünlüğünü korumakla yükümlüdür. Çalışmakta olan bilişim sistemlerinde arama ve elkoyma tedbirleri işinin ehli kişiler tarafından verilere en az etkide bulunarak gerçekleştirilmelidir.

Denetim izi olarak isimlendirilen ikinci ilkeye göre, elektronik delil elde edilirken yapılan bütün arama, aktarma, depolama, elkoyma gibi işlemler kaydedilmeli ve daha sonrasında denetlenmek üzere muhafaza edilmelidir. Yapılan işlemler üçüncü bir kişi tarafından tekrar edilebilmeli ve bu işlemler sonucunda aynı sonuç elde edilmelidir.

Bilişim sistemlerinde arama ve elkoyma tedbirleri uzmanlık gerektiren koruma tedbirleridir. Dolayısıyla üçüncü ilke, uzman-bilirkişi desteğidir. Bu tedbirler gerçekleştirilirken kolluk kuvvetleri ile birlikte mümkünse bilişim sistemlerinden delil etme konusundan uzmanlaşmış bilirkişiler hazır bulunmalıdır. Bu bilirkişiler, alanında yeterince bilgi sahibi olmalı, tedbirleri uygulayan kolluk kuvvetlerini yönlendirebilmeli, yeterince hukuki bilgiye sahip olmalı, hem kolluk kuvvetleri ile iletişim kurmak hem de ilgili raporların hazırlanması için uygun iletişim ve dil becerilerine sahip olmalı ve bilirkişilik yapabilmek için izin ve belgelere sahip olmalıdır.

Bilişim sistemlerinde arama ve elkoyma tedbirini uygulayacak olan kolluk kuvvetleri, bilirkişi desteği alamıyorlarsa, dördüncü ilkeye göre, elektronik delil elde etme ile ilgili uygun ve gerekli eğitimleri almış olmaları gerekmektedir.

Kabul edilen son ilkeye göre, ilgili görevli ve kurumlar, elektronik delil elde edilirken kanunlara ve ilgili düzenlemelere, adli bilişim ile ceza muhakemesinin temel ilkelerine uygun davranmakla yükümlüdür.

2. ACPO Sayısal Deliller için İyi Uygulama Rehberi

1948 tarihinde Birleşik Krallık kurulan ve yerini 2015 tarihinde NPCC'ye (Ulusal Emniyet Müdürleri Konseyi) bırakan ACPO (İngiltere, Galler ve Kuzey İrlanda Emniyet Müdürleri Derneği), kolluk kuvvetleri ve yargı mensuplarına yol

göstermesi amacıyla "Sayısal Deliller için İyi Uygulama Rehberi"[75] hazırlamıştır. Beşinci sürümü Ekim 2011 tarihinde yayınlanan bu rehberde sayısal deliller için dört temel ilke kabul edilmiştir[76].

Birinci ilke, verilerin bütünlüğü ile ilgilidir ve mahkemede delil olarak kullanılabilecek veriler üzerinde değişikliğe sebep olabilecek her türlü işlemden kolluk kuvvetlerinin ve ilgili diğer görevlilerin kaçınması gerektiğini ifade etmektedir. Buna ek olarak rehberin açıklama kısmında, bilişim sistemi kullanıcılarının farkında olmadan bilişim sistemindeki verileri değiştirebileceği, silebileceği ya da yeni veriler oluşturabileceği belirtilerek, kolluk kuvvetlerinin yapacağı işlemler sonucunda benzer sonuçların doğabileceği ifade edilerek maddeye açıklık getirilmiştir. Ayrıca, veri bütünlüğünün sağlanabilmesi için, bilişim sistemlerinin ya da ilgili verilerin imajlarının çıkartılması gerektiği ifade edilmiştir.

İkinci ilke, sayısal delillere ulaşan ve bu veriler üzerinde ilgili koruma tedbirlerini gerçekleştirecek kişiler ile ilgilidir ve bu kişilerin sayısal deliller konusunda yetkin kişiler olması gerektiğini ifade etmektedir. Ayrıca, bu kişilerin yaptıkları işlemlerin uygunluğu ve sonuçları hakkında bilgi verebilecek düzeyde olmaları gerekmektedir.

Üçüncü ilkeye göre sayısal veriler üzerinde yapılan işlemler kayıt altına alınmalı ve saklanmalıdır. Ayrıca, aynı işlemleri uygulayan üçüncü bir kişi işlemleri ilk gerçekleştiren görevli ile aynı sonucu elde etmelidir. Bu işlemlerin sağlıklı bir şekilde tekrar edilebilmesi için, ilgili verilerin imajları çıkartılmalı ve işlemler imaj üzerinden gerçekleştirilmelidir. Aksi taktirde, ilk işlem sonucunda verilerde değişiklik meydana gelecek ve üçüncü kişi tarafından yapılan denetimde aynı sonuçlar elde edilemeyecektir. Bununla birlikte, uzaktaki bir bilişim sisteminde depolanan verilerde arama yapıldığı durumlarda ilgili verilerin imajını çıkartmak mümkün olmayabilir. Bu

[75]**ACPO Good Practice Guide for Digital Evidence** (https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf) (Erişim Tarihi: 31.08.2019). İlgili rehberin Türkçe tercümesi için bakınız Elif Gökşen, **Türk Ceza Muhakemesinde Dijital Verilerin Delil Değeri**, Yayımlanmamış Yüksek Lisans Tezi, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, Mayıs 2014, s.133-142.

[76]Janet Williams, **ACPO Good Practise Guide for Digital Evidence**, version 5, October 2011, s.6.

durumda, ilgili verilere tekrar ulaşabilecek ve bu verileri mahkemede delil olarak sunabilecek kabiliyetteki kişilerin ilgili işlemleri gerçekleştirmesi gerecektir.

Dördüncü ve son ilke ise soruşturmayı yürüten kişi ile ilgilidir. Buna göre, yapılan işlemlerde ilgili kanunlara, yönetmeliklere ve ilkelere bağlı kalındığının sorumluluğu soruşturmayı yürüten kişiye aittir. Sayısal deliller, belge delilleri ile aynı kanunlara tabidir. Dolayısıyla, sayısal delillerin elde edilmesi sürecinde belge delilleri ile ilgili kanuni düzenlemelere riayet edilmelidir.

3. Sedona İlkeleri

1997 yılında Amerika Birleşik Devletleri'nde bir eğitim enstitüsü olarak kurulan Sedona Konferansı, 2002 yılından itibaren belirli konularda çalışma grupları oluşturmaya başlamış ve ilk çalışma grubunun konusu olarak "Elektronik Belgelerin Hazırlanması ve Muhafazası" seçilmiştir. Elektronik keşif alanında uzmanlaşmış hukukçuları bir araya ilk çalışma grubu sonucunda "Sedona İlkeleri: Elektronik Belge Hazırlamaya ilişkin İyi Uygulama Tavsiyeleri ve İlkeleri" adıyla Mart 2004 tarihinde bir rehber hazırlanmıştır. İlgili rehber, 2006 yılında Amerikan Federal Hukuk Muhakemeleri Kanununda elektronik olarak depolanmış veriler ve elektronik keşif konularında yapılan değişiklere temel teşkil etmiştir[77]. İkinci sürümü 2007, üçüncü sürümü ise 2018 yılında yayınlanan rehberde elektronik olarak depolanmış veriler ve elektronik keşif hakkında belirli ilkeler kabul edilmiştir[78].

Sedona İlkeleri[79], elektronik olarak depolanmış verilerden elde edilecek delillerin hukuk muhakemesinde kullanılacağını dikkate alarak hazırlanmıştır. Dolayısıyla, Avrupa Konseyi Elektronik Delil Rehberi ve AGPO Sayısal Deliller için İyi Uygulama Rehberinden farklı olarak, ceza muhakemesinde hükmün esasına delil teşkil edebilecek sayısal deliller ve bunların elde edilmesi aşamasında doğrudan yol gösterici bir rehber teşkil etmemektedir. Bununla birlikte, bazı ilkelerinin ceza

[77]Julia M. Ong, "Another Step in the Evolution of E-Discovery: Amendments of the Federal Rules of Civil Procedure Yet Again", **Boston University Journal of Science & Technology Law**, V:18, 2012, s.411.
[78]**The Sedona Principles Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production**, 19 Sedona Conference J. 1, 2018, s. 51-53.
[79]Sedona İlkelerinin Türkçe Tercümesi için bakınız Keser Berber, **Adli Bilişim**, s. 168-170.

muhakemesi için yol gösterici olabileceğini dikkate alarak tezimizin bu bölümünde değinmekte fayda görüyoruz.

Örneğin dördüncü ilkeye göre, keşif dilekçesinde elektronik keşif yapılacak bilişim sistemlerinin ve verilerin açık bir şekilde belirtilmesi gerektiği ifade edilmektedir. Benzer bir şekilde soruşturma sırasında savcılık tarafından verilecek arama kararlarında hangi bilişim sistemlerinde ve hangi sayısal verilerde arama tedbirinin uygulanacağının ölçülülük ilkesi gereğince açıkça belirtilmesi gerekmektedir.

Beşinci ilke ve bu ilkeye getirilen yorumlar kapsamında üzerinde elektronik keşif yapılan verilerin muhafaza altına alınması ancak bu konuda mahkemenin ikna edilmesiyle mümkün olmaktadır. Benzer şekilde, bilişim sistemlerinde kopyalama ve elkoyma tedbirleri, arama tedbirinden daha ağır bir şekilde kişi hak ve özgürlüklerine müdahale teşkil ettiği için ancak soruşturma makamı somut gerçeklere dayanarak yetkili mahkeme ya da hâkimi ikna etmesi sonucunda uygulanabilecek tedbirler olması gerekmektedir.

Beşinci ilkeye getirilen yorumlarda muhafaza kavramı verilerin bütünlüğünü bozmadan olduğu gibi korunması olarak ifade edilmektedir. Dolayısıyla, ilgili verilerin bütünlüğünü korumak ancak bu verileri dondurarak yani imajını alarak mümkün olabilmektedir. Ceza muhakemesi kapsamında belirtilen kopyalama tedbirinde benzer bir şekilde bilişim sistemlerinde depolanan verilerin imajlarının alınması yani veri bütünlüğünün korunması gerekmektedir.

Dokuzuncu ilkede, delillerin sadece kullanıcılar tarafından doğrudan ulaşılabilen verilerde değil aynı zamanda silinmiş, parçalanmış ya da gölge verilerde de bulunabileceği belirtilmiştir. Dolayısıyla, ceza muhakemesi kapsamında bu husus dikkate alınarak, arama ve kopyalama tedbirleri silinmiş, geçici belleğe alınmış vb. veriler üzerinde de uygulanması gerekmektedir.

On birinci ilkede keşif için belirli anahtar kelimeler ya da örnekler belirlenmesi ve keşfin bunlar kullanılarak yapılması tavsiye edilmektedir. Ceza muhakemesi

kapsamında usul ekonomisi için benzer yöntemlerin uygulanması gerekmektedir. Aksi taktirde arama tedbirleri uzun zamanlar almakta hatta yerinde tamamlanamayarak ilgili bilişim sistemlerine elkonulması gerekebilmektedir.

III. KARŞILAŞTIRMALI HUKUKTA BİLİŞİM SİSTEMLERİNDE ARAMA, KOPYALAMA VE ELKOYMA TEDBİRLERİ

A. FRANSA

Fransız Hukukunda arama, kopyalama ve elkoyma tedbirleri Fransız Ceza Muhakemesi Kanunu (FCMK) m.56 ve devamında düzenlenmiştir. Avrupa Konseyi Siber Suç Sözleşmesi, 23 Kasım 2001 tarihinde Fransa tarafından imzalanarak yürürlüğe konmuştur. Bunun neticesinde, Fransız Kanun Koyucu sayısal verilerin üzerinde arama yapılabileceğine ve delil niteliği taşıyabilecek sayısal verilere ya da bu verilerin depolandığı araçlara elkonabileceğine dair hükümleri FCMK'ya eklemiştir.

22 Haziran 2004 tarihinde yürürlüğe giren değişikliğe göre, şüpheli ya da suç ile ilgili delillerin elde edilebileceği verileri ellerinde bulunduran kişiler hakkında FCMK m.56 kapsamında arama tedbirine başvurulabilmekte ve bu kişilerin mülkiyetinde bulunan sayısal verilerde arama yapılabilmektedir[80]. Arama tedbiri, Cumhuriyet Savcısının izni ile adli kolluk tarafından gündüz vakti gerçekleştirilmektedir. Arama tedbiri uygulanırken hakkında arama kararı verilen kişi ya da vekili bulunmak zorundadır. Bu kişilerin bulunmaması durumunda, adli kolluk görevi yürütmeyen iki kişinin arama sırasında hazır bulunması gerekmektedir.

Fransız Kanun Koyucu, "bilgisayar" ya da "bilişim sistemleri" gibi ifadeler kullanmak yerine, "sayısal veri" kavramını tercih ederek arama yapılacak araçlar yönünden bir kısıtlamaya gitmemiştir. Dolayısıyla, sayısal verinin bulunabildiği her türlü araçta arama tedbirine başvurmak mümkündür. Teknolojinin hızlı bir şekilde gelişmesi ve sayısal verilerin bulunduğu araçların gün geçtikçe farklılaşması dikkate

[80]https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071154 (Erişim Tarihi: 23.03.2019).

alındığında, arama tedbirinin uygulanacağı araçlar belirtilmeden sayısal veriye odaklanılması tarafımızca doğru bir yaklaşım olarak değerlendirilmektedir.

Arama tedbiri sonucunda delil niteliği taşıyabilecek verilerin bulunması durumunda, yine Cumhuriyet Savcısının kararı ile adli kolluk tarafından ilgili verilerin bulunduğu araçlara elkonulabilecek ya da bu sayısal veriler hakkında kopyalama tedbirine başvurularak ilgili verilerin birebir kopyası çıkartılabilecektir. İlgili kopyanın çıkartılması durumunda, kişinin kullanıma bırakılması tehlikeli ya da kanuna aykırı olan veriler, Cumhuriyet Savcısının onayı ile, yargının eline verilen kopya hariç olmak üzere, silinebilir ve yok edilebilir.

19 Mart 2003 tarihinde yürürlüğe giren FCMK m.57-1'e göre, aramanın yapıldığı yerde bulunan bilişim sistemleri aracılığıyla erişilebilen ve Fransa toprakları içerisinde bulunan sayısal verilerde arama yapılması mümkündür. Bu arama sonucunda delil niteliği taşıyabilecek verilerin elde edilmesi durumunda, bu veriler hafıza birimlerine yazılacak ve bu birimlere adli kolluk tarafından mühürlenerek elkonulabilecektir[81].

Arama, kopyalama ve elkoyma tedbirlerinin tamamlanması sonucunda tutanak düzenlenecek ve tedbirin uygulanması sırasında hazır bulunanların imzası yer alacaktır. Ayrıca, kopyalama ve elkoyma tedbirlerinin uygulandığı veri ve araçların listesi oluşturulacak ve ilgili araçlar mühürlenecektir.

FCMK m.60-3'e göre sayısal verilerin içerisinde bulunduğu araçlara elkoyma tedbirinin uygulanmasından sonra, ilgili incelemelerin yapılabilmesi ve sayısal verilerin bütünlüğünün korunabilmesi amacıyla, adli kolluk amiri ya da Cumhuriyet Savcısının kararı ile FCMK kapsamında bilirkişi görevini yürüten ya da yazılı bir şekilde yemini alınan kişiler tarafından ilgili verilerin yeteri kadar kopyası çıkartılacaktır. İlgili verilerin kopyasının çıkartılması sırasında yapılan her işlem

[81]Olivier Decima, "Les investigations numériques en procédure pénale française: du piratage informatique aux perquisitions et saisies numériques?", **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi**, 2017/1, s.3.

yazıya dökülecek ve işlemin tamamlanması akabinde ilgili hükümlere göre bir rapor oluşturulacaktır.

Fransız Hukukunda yerinde arama tedbirine ek olarak, FCMK kapsamında uzaktan arama tedbiri ile ilgili hükümler de bulunmaktadır. 15 Kasım 2014 tarihinde FCMK m.57-1'e eklenen hükme göre, arama yapılan yerde bulunan bilişim sistemleri aracılığıyla erişilebilen sayısal veriler üzerinde polis ve jandarmanın kullandığı bilişim sistemleri aracılığıyla arama yapılabilmekte ve ceza muhakemesi açısından önem teşkil eden verilere elkonulabilmektedir. Bu hükmün uygulanabilmesi için, öncelikle yerinde arama tedbirine başvurulması gerekmekte, daha sonrasında burada bulunan bilişim sistemi aracılıyla erişilebilen sayısal veriler tespit edilerek, bu veriler üzerinde daha sonrasında polis veya jandarmanın bilişim sistemleri aracılıyla arama ve elkoyma tedbirleri gerçekleştirilmektedir.

Uzaktan arama ile ilgili bir diğer hüküm ise, 3 Haziran 2016 tarihli *"Organize Suçlar, Terörizm ve Bunların Finansmanları ile Mücadeleyi Güçlendiren ve Ceza Muhakemesinin Etkililiğini ve Teminatlarını Arttıran Kanun"* ile FCMK'ya eklenen m. 706-102-1 ve devamında yer almaktadır[82]. Bu hükme göre, organize suçlar ve terör suçları ile ilgili yürütülen soruşturma kapsamında Cumhuriyet Savcısının istemi üzerine Sulh Ceza Hakiminin kararı ile adli kolluk tarafından, ilgili kişilerin rızası olmadan, *"truva atı"* ya da "*arkakapı"* aracılığıyla bu kişilerin sayısal verilerine ulaşılabilmekte, bu veriler bilişim sistemlerinde depolandıkları kaydedilebilmekte, saklanabilmekte ya da aktarılabilmektedir[83].

İlgili hükme göre sulh ceza hâkimi tarafından verilen uzaktan arama kararında, ilgili tedbire başvurma gereği duyulan suç, aramanı gerçekleşeceği yerin konumu, hakkında arama kararı uygulanacak bilişim sisteminin detaylı tarifi ve tedbirin uygulanma süresi belirtilmelidir. Aksi taktirde tedbir sonucu elde edilen veriler soruşturma ve kovuşturma kapsamında kullanılamayacaktır. Tedbirin süresi en fazla 4

[82]İlgili hükmün değişiklik öncesinde hali incelendiğinde, sayısal verilerin yalnızca ilgili bilişim sisteminin ekranında gözüktüğü ya da giriş birimleri aracılığıyla bilişim sistemine girişinin yapıldığı şekilde kaydedilebildiği, saklanabildiği ya da aktarılabildiği, dolayısıyla değişiklik öncesinde yalnızca akış halindeki verilerin hükmün konusunu teşkil ettiği söylenebilecektir.
[83]Decima, **a.g.e.**, s.5.

ay olarak belirlenebilecek ve gerektiği taktirde 4 ay daha uzatılabilecektir. Ayrıca, Sulh Ceza Hâkimi kararıyla herhangi bir zamanda tedbir sona erdirilebilecektir.

Tedbir uygulanırken yapılan her türlü işlem tutanağa geçirilecek ve ilgili tutanakta tedbirin başlangıç ve bitiş tarih ile saatleri belirtilecektir. Elde edilen sayısal veriler mühürlenerek muhafaza altına alınacaktır. Ayrıca, tedbirin uygulanması için gündüz vakti olması gerekmemekte ve bir saat sınırlamaması bulunmamaktadır.

Tedbirin uygulanması sonucunda tesadüfen elde edilen deliller, ceza muhakemesi kapsamında delil niteliği taşımayacak veya tedbiri hukuksuz hale getirmeyecektir. Zamanaşımı süresi içerisinde kamu davasına dönüşmeyen soruşturma dosyaları kapsamında elde edilen sayısal veriler, Cumhuriyet Savcısının ya da Başsavcının talebi üzerine imha edilecek ve bu imha işlemi de tutanağa geçirilecektir.

Yukarıda belirtilen hükümler ışığında Fransız Hukukunda düzenlenen uzaktan arama tedbirinin, tek seferde ve kapalı bir alanda gerçekleştirilmemesi, ilgili kişinin arama tedbirinden haberdar olmaması, tedbirinin gündüz vakti gerçekleştirilmesi zorunluluğunun bulunmaması sebebiyle yerinde arama tedbirinden ayrıştığı ve temel hak ile özgürlüklere daha fazla müdahale teşkil ettiği söylenebilecektir. Nitekim bu durumu dikkate alan Fransız Kanun Koyucu, tedbirin uygulanabilmesi için organize suç ya da terör suçu gibi suçların varlığı ile Sulh Ceza Hakiminin kararını aramakta ve ayrıca tedbirin uygulanacağı bilişim sistemlerinin bilgilerinin arama kararında açıkça belirtilmesi gerektiğini belirtmektedir. Öğretide ise temel hak ve özgürlüklerin daha iyi korunabilmesi için, uzaktan arama tedbirinin arama tedbirinden ayrıştırılarak değerlendirilmesi ve tartışılması gerektiği belirtilmektedir[84].

B. ALMANYA

Bilişim sistemlerinden delil elde etmek amacıyla 90'lı yıllardan beri arama ve elkoyma tedbirleri Almanya'da uygulanıyor olmasına ve Almanya Federal Cumhuriyeti tarafından 21 Kasım 2001 tarihinde imzalanarak, 1 Temmuz 2009

[84]Decima, **a.g.e.**, s.6.

tarihinde AKSSS yürürlüğe konmuş olmasına rağmen Alman Ceza Muhakemesi Kanunu kapsamında bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirleri düzenlenmemiştir. Dolayısıyla, bilişim sistemlerinden sayısal delil elde edilebilmesi için arama ve elkoyma tedbirlerinin genel hükümlerine başvurulmaktadır[85].

Buna ek olarak, kanun uygulayıcıları tarafından ACMK kapsamında yer alan diğer ilgili hükümler geniş yorumlanmakta ve bilişim sistemlerinden delil etme amacıyla bu hükümler kıyasen kullanılabilmektedir. Hem bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirlerinin ACMK'da yer almaması hem de sayısal delillerin elde edilmesi ile alakalı olarak kanun uygulayıcılar tarafından kıyasen diğer hükümlerin uygulanmaya çalışılması Alman öğretisinde eleştirilmektedir[86]. Alman Anayasası m.20'ye göre demokratik bir hukuk devleti olan Almanya'da kendi kişiliğini geliştirme hakkı, özel hayatın gizliliği, haberleşme özgürlüğü vb. gibi temel hak ve özgürlüklere müdahale teşkil eden bir ceza muhakemesi tedbirinin hem AKSSS hükümleri hem de kanunilik ilkesi gereğince kanunda belirtilmesi ve bu tedbirin açıklık ilkesi gereğince sınırlarının kanun maddesi ile çizilmesi gerekmektedir. Nitekim Almanya Federal Anayasa Mahkemesinin temel haklara müdahale teşkil eden hukuki tedbirlere dair esasların kanunda açıkça belirtilmesi gerektiğine dair birçok kararı bulunmaktadır[87]. Örneğin, arama tedbirinin uygulanması sonucunda bulunan bütün bilişim sistemlerine elkonulması kararı, AFAM tarafından kişinin kendi kaderini belirleme hakkına orantısız bir müdahale olarak değerlendirilerek, hukuka aykırı bulunmuştur[88].

ACMK kapsamında delil toplanması, dolayısıyla arama ve elkoyma tedbirleri soruşturma aşamasında uygulanacak tedbirler olarak düzenlenmiştir. Fakat ACMK m.244 kapsamında kovuşturma aşamasında mahkemeye de delil toplama yetkisi verilmiştir. Dolayısıyla, bilişim sistemlerinde arama ve elkoyma tedbirlerine hem

---

[85]Thomas Böckenförde, **Die Ermittlung im Netz: Möglichkeiten und Grenzen neuer Erscheinungsformen strafprozessualer Ermittlungstätigkeit**. Almanya: Mohr Siebeck Verlag. 2003, s.9; aktaran Tanrıkulu, **a.g.e.**, s.218.
[86]Bökckendörfe, **a.g.e.**, s.121-123; aktaran Tanrıkulu, **a.g.e.**, s.220.
[87]Tanrıkulu, **a.g.e.**, s.222.
[88]Almanya Federal Anayasa Mahkemesi 2BvR 279/90 sayı ve 03.09.1991 tarihli kararı; aktaran Tanrıkulu, **a.g.e.**, s.224-225.

soruşturma aşamasında hem de Türk Ceza Muhakemesi Kanununda yer alan düzenlemenin aksine kovuşturma aşamasında başvurulabilecektir.

Almanya Ceza Muhakemesi Hukukunda bilişim sistemlerinde arama yapılabilmesi için, şüpheli hakkında yapılacak aramalar için genel arama tedbirini düzenleyen ACMK m.102'ye başvurulması gerekecektir[89]. Bu hükümlere göre hakkında arama kararı verilecek kişinin bir suç soruşturması kapsamında bir suçun faili, azmettirici ya da suçun işlenmesi öncesinde veya sonrasında yardım ve yataklıkta bulunan, çalıntı malların ticaretini yapan ya da adaletin tecellisine engel olan olarak şüpheli konumunda olması gerekmektedir.

Delil niteliği taşıyabilecek ya da elkonulacak bilişim sistemlerinin üçüncü kişinin mülkiyetinde bulunması durumunda ise, ilgili üçüncü kişiler hakkında arama kararı verilebilecek ve bu kişilerin ilgili bilişim sistemlerinde m.103'e göre arama gerçekleştirilebilecektir. Fakat üçüncü kişiler nezdinde arama tedbirinin gerçekleştirilebilmesi için hakkında arama kararı verilen delil somut ve hakkında şüpheye mahal bırakmayacak şekilde açık olmalı ve arama kararı gerçekleştirilecek bilişim sistemleri ve veriler sınırlandırılmalıdır[90].

ACMK m.98 ve m.105'e göre bilişim sistemlerinde arama ve elkoyma kararları hâkim tarafından verilecek, gecikmesinde sakınca olan hallerde ise savcılık ya da soruşturma görevlileri tarafından verilebilecektir. Soruşturma görevlileri kapsamına giren polis, gecikmesinde sakınca bulunan hallerde arama ve elkoyma kararları vermeye yetkilidir[91]. Yayın kuruluşlarına, matbaalara ya da basına ait yerlerde uygulanacak elkoyma kararlarında mutlaka hâkim kararının bulunması gerekmektedir. Savcılık ya da soruşturma görevlileri tarafından verilen elkoyma kararlarına itiraz halinde ilgili karar üç gün içerisinde hâkim onayına sunulacaktır.

ACMK m.102 ve devam maddelerine göre, bilişim sistemlerinde arama ve elkoyma kararlarında, kararı veren makam ve kişinin bilgileri, hakkında arama tedbiri

---

[89]Tanrıkulu, **a.g.e.**, s.228.
[90]Wolfgang Baer, "LG Frankfurt/M. , 21.10.2003 - 5/8 Qs 26/03 : LG Frankfurt/M.: Durchsuchung bei Internetprovider", **Multimedia und Recht,** 2007, V. 5, s. 339; aktaran Tanrıkulu, **a.g.e.**, s.229-231.
[91]Tanrıkulu, **a.g.e.**, s.238.

uygulanacak kişinin kimliği ve adresi, arama kararına dayanak teşkil eden suç, arama tedbirinin amacı, aramaya konu olan olayın ayrıntılı özeti, arama kararının uygulanacağı bilişim sistemleri ve sayısal veriler, elkonulması beklenen eşyalar, ilgili yasa maddeleri ve arama tedbirinin gerçekleşeceği tarih belirtilmelidir[92]. Ayrıca, arama ve elkoyma kararlarında, bu karalara dayanak teşkil eden vakıalardan, mevcut şüpheden ve arama tedbiri sonucunda elde edilmesi beklenen delillerden ayrıntılı bir şekilde bahsedilmesi gerektiği AFAM kararlarında vurgulanmaktadır[93].

Bilişim sistemlerinde arama tedbiri, kural olarak gündüz vakti[94] gerçekleştirilecek ve m.106'ya göre arama yapılan bilişim sistemlerinin sahibi, arama tedbiri uygulanırken hazır bulunabilecektir. Bu kişinin olmaması durumunda, vekili, erişkin bir yakını, beraber yaşadığı kişiler ya da bir komşusu aramaya katılacaktır. Ayrıca, arama kararının uygulanması sırasında hâkim ya da savcının bulunmaması durumunda, polis ya da soruşturma görevlisi olmamak kaydıyla, bir belediye çalışanı ya da ilçe ahalisinden iki kişi aramada hazır bulunacaklardır.

Üçüncü kişilerin bilişim sistemlerinde arama tedbiri gerçekleştirilmeden önce, aramanın amacı ilgili kişiye ya da bu kişinin yokluğunda hazır bulunana açıklanacaktır. Arama sonucunda, ilgili kişinin istemi üzerine, m.107 kapsamında ilgili kişiye bilişim sistemlerinde arama kararının sebepleri, elkonulan eşyaların listesi ve herhangi bir delil bulunamamışsa bu durumu belirten yazılı bir bildirimde bulunulacaktır.

Arama tedbirinin uygulanması sonucunda delil niteliğine sahip olabilecek verilere, ACMK m.94 kapsamında elkonulacaktır. Alman uygulamasında elkoyma tedbirinin maddi varlığa sahip eşyalar üzerinde uygulanabildiği ve sayısal verilerin maddi varlığa sahip olmadığı kabul edilmektedir[95]. Bununla birlikte, sayısal verilerin

---

[92]Tanrıkulu, **a.g.e.**, s.239.
[93]AFAM 03.09.1991 tarihli ve 2BvR 279/90 sayılı kararı; aktaran Tanrıkulu, **a.g.e.**, s.239.
[94]Gündüz vakti kavramı ACMK m.104/3'te tanımlanmıştır. Buna göre, gündüz vakti 1 Nisan ile 30 Eylül tarihleri arasında sabah dokuz ile akşam dört arası, 1 Eylül ile 31 Mart tarihleri arasında ise sabah dokuz ile akşam altı arasında kalan vakittir.
[95]Joecks Von Wolfgang, **Studienkommentar StPO**, 2. Baskı, Almanya: C.H.Beck Verlag, 2008, s.177; AFAM 2BvR 2099/04 sayılı ve 02.03.2006 tarihli kararı (https://www.bundesverfassungsgericht.de) (Erişim Tarihi: 31.08.2019).

üzerine yazıldığı CD, DVD, disket ve sabit sürücülere maddi bir varlığa sahip olduğu için ACMK kapsamında elkonulabilecektir[96]. Ayrıca, öğretide aramaya konu olan eşyanın maddi bir varlığa sahip olmasının ACMK kapsamında gerekli olmadığını ve dolayısıyla, uygulamanın aksine, genel arama hükümlerine göre doğrudan sayısal verilere elkonulabileceğine dair görüşler bulunmaktadır[97].

Arama tedbirinin uygulanması sırasında üçüncü kişilere ait verilerin ortaya çıkması durumunda, kişinin kendisini geliştirme hakkını ihlal edebilme ihtimali sebebiyle ilgili verilerin bulunduğu veri taşıyıcılarına elkonulmasından kaçınılması gerekmektedir. Nitekim, AFAM kararlarında bu hususa dikkat çekmekte ve ağır kusurla ya da bilinçli olarak bu tür bir ihlale sebep olunması durumunda, ilgili sayısal verilerin ceza muhakemesinde delil olarak değerlendirilemeyeceğini vurgulamaktadır[98].

ACMK'da bilişim sistemlerinde arama, kopyalama ve elkoyma tedbiri bulunmamasına rağmen, m. 110/3'te elektronik depolama araçlarında yapılacak aramaların, bu araçla fiziksel olarak aynı ortamda bulunmayan fakat bu araç vasıtasıyla ile ulaşabilen verileri de kapsayacağı ve bu verilere m.98 gereğince elkonulabileceği belirtilmiştir. AKSSS m.19/2'nin karşılığı olarak düzenlenen bu tedbire göre ilgili verilerde arama yapılabilmesi için, bu verilerin kaybolma tehlikesinin bulunması gerekmektedir.

Son olarak, Alman hukukunda uzaktan arama tedbirine değinmekte yarar vardır. Almanya'da BKAG (Federal Adli Polis Teşkilatı Kanunu) kapsamında yapılan değişiklikle birlikte terör suçları ile ilgili olarak federal kolluk kuvvetlerine uzaktan arama yetkisi verilmiştir. Fakat daha sonrasında bu kanun, anayasaya aykırı bulunarak Alman Anayasa Mahkemesi tarafından iptal edilmiştir[99].

---

[96]AFAM 2 BvR 1027/02 sayılı ve 12.04.2005 tarihli kararı (https://www.bundesverfassungsgericht.de) (Erişim Tarihi: 31.08.2019).
[97]Matthias Jahn/Hans Kudlich, "Die strafprozessuale Zulässigkeit der Online-Durchsuchung", **Juristische Rundschau**, Volume 2007, Issue 2, s.58.
[98]Joecks, **a.g.e.**, s.177; aktaran Tanrıkulu, **a.g.e.**, s.233.
[99]Nurullah Kunter, Feridun Yenisey, Ayşe Nuhoğlu, **Muhakeme Hukuku Dalı Olarak Ceza Muhakamesi Hukuku**, İstanbul: Beta, 2010, s.1110.

C. BELÇİKA

Belçika Hukukunda arama ve elkoyma tedbirleri Belçika Ceza Muhakemesi Kanunu[100] m.35 ve devamında düzenlenmiştir. Bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirleri ise 28 Kasım 2000 tarihinde kabul edilen ve 13 Şubat 2001 tarihinde yürürlüğe giren değişikliklerle beraber kanuna eklenmiştir. Değişiklik öncesinde bilişim sistemlerinde arama ve elkoyma tedbiri genel hükümlere göre gerçekleştirilmiştir. Genel hükümlere göre aranacak ve elkonulacak eşyanın somut bir varlığa sahip olması arandığı için bilişim sistemlerinde yer alan verilerde arama ve elkoyma yapılamamış, bunun yerine somut bir varlığı olan ve verilerin depolandığı CD, DVD ve sabit sürücülere elkonulmuştur[101].

Bilişim sistemlerinde arama tedbiri BCMK m.39bis kapsamında düzenlenmiştir. Bu maddenin 4. fıkrasına göre, bilişim sistemlerinde arama emrinin verilebilmesi için hem arama sonucunda elde edilecek verilerin maddi gerçeğin açığa çıkartılması için gerekli olması hem de uygulanabilecek diğer tedbirlerin ölçüsüz olması ya da delillerin kaybolma tehlikesinin bulunması gerekmektedir.

Arama kararını vermeye yetkili kişi, soruşturma aşamasından sorumlu olan sorgu hakimidir. Arama emri, kural olarak yazılı olarak verilmesi gerekmektedir fakat gecikmesinde sakınca bulunan hallerde emir sözlü olarak verilebilir. Bu durumda, en kısa sürede sözlü emrin gerekçeleriyle birlikte yazılı olarak onaylanması gerekmektedir.

Ayrıca, ilgili maddenin 2. fıkrasına göre adli kolluk amiri elkonulan bilişim sistemlerinde, Kraliyet Savcısı ise kendisi tarafından elkonulabilecek bilişim sistemlerinde arama kararı vermeye yetkilidir. Adli kolluk amirinin ya da Kraliyet Savcısının arama kararı sadece ilgili elkonulan ya da elkonulabilecek olan bilişim

---

[100]**Code d'Instruction Criminelle de Belgique**
https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=1808111730&table_name=loi (Erişim Tarihi: 31.08.2019).

[101]Florence de Villenfagne/Séverine Dusollier, "La Belgique sort enfin ses armes contre la cybercriminalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique", **Auteurs et Média**, 2002, Numéro 1, s.73.

sistemlerinde depolanan verileri kapsamaktadır. Dolayısıyla, böyle bir durumda arama işlemine başlamadan önce bilişim sisteminin diğer bilişim sistemleri ya da dış ağlarla bağlantısı kesilmesi gerekmektedir.

Bununla birlikte, arama sonucunda elde edilecek verilerin maddi gerçeğin açığa çıkartılması için gerekli olması ve uygulanabilecek diğer tedbirlerin ölçüsüz olması ya da delillerin kaybolma tehlikesinin bulunması durumunda, Kraliyet Savcısının yazılı (gecikmesinde sakınca bulunduğu durumlarda sözlü) emriyle arama tedbirinin kapsamına arama tedbirinin uygulandığı bilişim sisteminden erişilebilen ve arama tedbirinin uygulandığı mahalde bilişim sistemleri de dahil edilebilecektir. Fakat bu durumda sadece hakkında arama kararı verilen kişinin ulaşılabildiği verilerde arama gerçekleştirilebilecektir.

Arama tedbirinin uygulanması sırasında, Kraliyet Savcısı ya da Sorgu Hâkimi kararıyla, ilgili bilişim sistemlerinde yer alan güvenlik sistemlerinin geçici olarak devre dışı bırakılması ya da bilişim sistemi tarafından işlenen, aktarılan ya da depolanan şifreli verilerin kırılması amacıyla her türlü teknik tedbire başvurulabilecektir. Bununla birlikte, arama gerçekleştirilen bilişim sistemleri aracılığıyla erişilebilen sistemlerde bu tedbirlerin uygulanabilmesi için Sorgu Hakiminin kararı gerekli olacaktır.

Arama tedbirinin uygulanması neticesinde, arama yapılan ceza yargılamasında maddi gerçeğin açığa çıkarılmasına yardımcı olabilecek yani delil niteliğine haiz olabilecek verilerin bulunması durumunda, bu verilerin depolandığı araçlara elkonulması istenmiyorsa, ilgili veriler ve bu verilerin anlaşılabilir olması için gerekli örneğin bilgisayar programları gibi veriler ile birlikte, arama kararını gerçekleştiren kuruma ait depolama araçlarına kopyalanacaktır. Fakat, gecikmesinde sakınca bulunan hallerde ve teknik yetersizlik durumunda, hakkında arama kararı verilen kişiye ait depolama araçları da kullanılabilecektir. Arama yapılan bilişim sistemleri aracılığıyla erişilebilen bilişim sistemlerinde ise elkoyma tedbiri somut olarak uygulanamayacağı için doğrudan kopyalama tedbirine başvurulacaktır.

Kraliyet Savcısı elkonulan bilişim sistemlerinin ya da kopyalanan verilerin bütünlüğünün ve güvenilirliğinin korunması için her türlü tedbiri alacaktır. Ayrıca, hakkında arama kararı verilen kişinin ilgili veriler ile bu verilerin kopyalarına erişiminin engellenmesi için her türlü teknik yönteme başvurulabilecektir. Şayet suçun konusunu teşkil eden ya da suçun işlenmesi neticesinde oluşan veriler, kamu düzenine ya da genel ahlaka aykırıysa ya da bilişim sistemlerinin bütünlüğü veya bilişim sistemi tarafından işlenen, aktarılan ya da depolanan veriler için tehlike teşkil ediyorsa, Kraliyet Savcısının kararı ile ilgili verilere erişim engellenebilir ya da ilgili verilerin bir kopyası alınarak bu veriler bilişim sisteminden kaldırılabilir. Fakat, arama yapılan bilişim sistemleri aracılığıyla erişilebilen bilişim sistemlerinin Belçika sınırları dışında bulunması durumunda, ilgili veriler hakkında yalnızca kopyalama tedbirine başvurulabilecek ve derhal durum hakkında ilgili devletin yetkili kurumlarına Federal Adalet Bakanlığı aracılığıyla bilgilendirilme yapılacaktır.

Ayrıca, bu tedbirlerin uygulanması sonucunda, bilgileri ve adreslerinin tespit edilmesinin mümkün olmadığı haller dışında, arama kararı uygulanan bilişim sistemlerinin ya da uzantılarının sorumlularına, Sorgu Hâkimi ya da Kraliyet Savcısı tarafından, en kısa sürede bilgilendirme yapılacak ve kopyalanan, erişimi engellenen ya da sistemden kaldırılan bilgiler ile ilgili bir rapor gönderilecektir.

D. AMERİKA BİRLEŞİK DEVLETLERİ

Amerikan Hukukunda bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirleri doğrudan düzenlenmemiş, bunun yerine, bu tedbirler Amerikan Anayasası 4. Değişiklik kapsamında düzenlenen arama ve elkoyma tedbirlerinin kapsamına mahkeme içtihatları ile dahil edilmiştir. Bununla birlikte, fiziki eşyalar ile sayısal verilerin farklı özelliklere sahip olduğu dikkate alınarak bilişim sistemlerinde arama ve elkoyma tedbirlerinin Amerikan Anayasası 4. Değişiklik kapsamında gerçekleştirilmesinin doğru olmayacağını öğretide ifade eden yazarlar bulunmaktadır[102].

[102]Orin S. Kerr, "Search Warrants in an Era of Digital Evidence", **75 Mississippi Law Journal**, V. 85, 2005, s.134.; Kaitlyn R. O'Leary, "What the Founders Did Not See Coming: The Fourth Amendment, Digital Evidence and the Plain View Doctrine", **Suffolk University Law Review**, V.211, s. 211.

Amerikan Anayasası 4. Değişiklik[103], kişileri, konutlarını, eşyalarını ve belgelerini haksız arama ve elkoymalara karşı korumakta ve arama kararı olmaksızın arama ve elkoyma tedbirlerinin uygulanamayacağını ifade etmektedir. Bununla birlikte, aramanın yapılacağı eşya üzerinde ilgili kişinin "makul mahremiyet beklentisi" (*reasonable expectation of privacy*) bulunmuyorsa, yapılan işlem arama tedbiri olarak değerlendirilmeyecek ve arama kararının alınmasına gerek olmayacaktır[104].

Bilişim sistemleri Amerikan Hukukunda tıpkı bir çanta ya da dosya dolabı gibi kapalı bir kutu olarak değerlendirilmektedir[105]. Dolayısıyla, bilişim sistemlerinde yapılacak aramalar için ilgili kişinin makul mahremiyet beklentisinin var olduğu kabul edilmekte ve arama kararı olmadan bilişim sistemlerinde arama tedbirinin uygulamayacağı ifade edilmektedir[106]. Bununla birlikte bilişim sistemlerinde arama kararı verildiği zaman, tedbirin yalnızca ilgili dosyalarda mı gerçekleştirileceği yoksa kolluk kuvvetlerinin bilişim sisteminde yer alan bütün dosyalarda arama yapabileceği konusunda içtihatta görüş ayrılığı bulunmaktadır. Örneğin, Amerikan Yüksek Mahkemesi 5. Daire başka bir suç şüphesiyle bilişim sisteminde arama gerçekleştirildiği zaman çocuk pornografisi ile ilgili belgelerin bulunmasını ve bunlara elkonulmasını hukuka aykırı bulmamış ve ilgili bilişim sisteminde yer alan bütün dosyaları tek bir kapalı kutu olarak kabul etmiştir[107]. Diğer tarafta ise, 10. Daire 2001 tarihli kararında bilişim sistemlerinde yer alan verilerin kişinin özel hayatının birçok farklı konusu ile bilgiler taşıdığını, bu dosyaların tamamında arama tedbirinin uygulanması sonucunda kişinin birçok hakkının ve dolayısıyla bilişim sistemindeki

---

[103] *"Kişilerin, üstlerinin, evlerinin, belgelerinin ve eşyalarının gereksiz aranması ve bunlara el konulmasına karşı bağışıklıkları ihlal edilemeyecek ve bu yetkiyi veren müzekkere mutlaka muhtemel bir nedene dayanacak, yemin ve beyanla desteklenecek ve özellikle aranacak yeri, tutuklanacak kişi ile el konacak eşyaları belirleyecektir."*

[104] Illinois v. Andreas, 463 U.S. 765, 771 (1983) (www.justia.com) (Erişim Tarihi:31.08.2019).

[105] United States v. Ross, 456 U.S. 798, 822-823 (1982) (www.justia.com) (Erişim Tarihi:31.08.2019).

[106] H. Marshall Jarrett/Michael W. Bailie/Ed Hagen/Nathan Judish, **Searching and Seizing Computers and Obtainig Electronic Evidence in Criminal Investigation**, United States of America, Office of Legal Education, s.3; United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Circuit, 2007) (www.justia.com) (Erişim Tarihi:31.08.2019).

[107] United States v. Runyan, 275 F.3d 449, 464-465 (5th Circuit, 2001) (www.justia.com) (Erişim Tarihi:31.08.2019).

her bir dosyanın birbirinden farklı kapalı kutular olarak değerlendirilmesi gerektiğini hükümde ifade etmiştir[108].

Amerikan hukukunda bazı durumlar bilişim sistemlerinde yapılacak aramalarda makul mahremiyet beklentisini ortadan kaldırmaktadır[109]. Amerikan içtihadında bilişim sisteminde depolanan verileri kamuya açık hale getiren[110], ortak sabit sürücülerde depolayan[111], yerel ağda paylaşıma açan[112] ya da internete koyan[113] kişilerin mahremiyet beklentilerinin ortadan kalktığı ifade edilmiştir.

Amerikan hukukunda Türk hukukunun aksine ilgili kişinin aleni ya da zımni rızasını alarak arama kararı olmadan arama tedbirini gerçekleştirmek mümkündür[114]. Bununla birlikte, kolluk kuvvetleri ilgili rızanın varlığını ispatlamakla yükümlüdür[115]. Bilişim sistemlerinde ilgilinin rızası alınarak yapılan arama ve elkoyma tedbirleri uygulanırken, ilgilinin nelere rıza gösterdiğine, rıza gösteren kişinin ilgili bilişim sisteminin sahibi olup olmadığına ve arama tedbirinin uygulanması için verilen rızanın ne zaman ortadan kalktığına dikkat etmek gereklidir[116]. Başka bir yerde inceleme yapmak üzere, ilgili bilişim sistemlerinin depolama birimlerinin kopyalarının çıkartılması ilgilinin rızası ile mümkündür fakat rızanın ortadan kalkması ile ilgili kopyalar iade edilecektir[117]. Ayrıca, Amerikan hukukunda ebeveynlerin on sekiz yaşından küçük çocukları adına, eşler birbirleri adına, aynı bilişim sistemini ortak olarak kullananlar diğer kişiler adına, işverenler işyerinde kullandıkları bilişim sistemleri için işçileri adına rıza gösterebilmektedirler[118].

---

[108]United States v. Walser, 275 F.3d 981, 986 (10th Circuit, 2001) (www.justia.com) (Erişim Tarihi:31.08.2019).
[109]Jarrett/Bailie/Hagen/Judish, **a.g.e.**, s.5
[110]Katz v.United States, 389 U.S. 347, 351 (1967) (www.justia.com) (Erişim Tarihi:31.08.2019).
[111]United States v. Butler, 151 F. Supp. 2d 82, 83-84 (D. Me. 2001) (www.justia.com) (Erişim Tarihi:31.08.2019).
[112]United States v. Stults, 2007 WL 4284721, at *1 (D. Neb. Dec. 3, 2007) (www.justia.com) (Erişim Tarihi:31.08.2019).
[113]United States v. Gines-Perez, 214 F. Supp. 2d 205, 224-26 (D.P.R. 2002) (www.justia.com) (Erişim Tarihi:31.08.2019).
[114]United States v. Milian- Rodriguez, 759 F.2d 1558, 1563-64 (11th Cir. 1985) (www.justia.com) (Erişim Tarihi:31.08.2019).
[115]United States v. Matlock, 415 U.S. 164, 177 (1974) (www.justia.com) (Erişim Tarihi:31.08.2019).
[116]H. Marshall Jarrett/Michael W. Bailie/Ed Hagen/Nathan Judish, **a.g.e.**, s.16
[117]Mason v. Pulliam, 557 F.2d 426, 429 (5th Cir. 1977) (www.justia.com) (Erişim Tarihi:31.08.2019); Vaughn v. Baldwin, 950 F.2d 331, 334 (6th Cir. 1991) (www.justia.com) (Erişim Tarihi:31.08.2019).
[118]Jarrett/Bailie/Hagen/Judish, **a.g.e.**, s.19-27.

Amerikan hukukunda bilişim sistemlerinde arama kararı ile arama tedbiri gerçekleştirilebilmesi için, suç delillerinin, suç unsurlarının ya da suç aletlerinin ilgili bilişim sistemlerinin depolama birimlerinde ya da diğer araçlarında bulunabileceğine dair makul bir şüphenin bulunması gerekmektedir. Ayrıca arama kararında, arama ve elkoyma tedbirlerinin uygulanacağı bilişim sistemleri belirtilmelidir[119]. Arama kararı kapsamında aranılan delillerin hayatın olağan akışı içerisinde bilişim sistemlerinde depolanmış olmasının tespit edilebildiği durumlarda, bilişim sistemi arama kararında belirtilmesine gerek olmadığına dair Amerikan hukukunda kararlar bulunmaktadır[120]. Bununla birlikte hâkim görüşe göre, arama kararı kapsamında bilişim sistemlerine yer verilmiyorsa, arama kararının bilişim sistemleri üzerinde uygulanamayacağını ifade edilmektedir[121].

Bilişim sistemlerinde arama tedbiri için gereken makul şüphenin sağlanabilmesi için birçok farklı yöntem kullanılmaktadır. Bunlarda bir tanesi ilgili kişinin IP adresidir. Suç mağdurları ya da hizmet sağlayıcı aracılığıyla elde edilen IP adresleri, İnternet hizmet sağlayıcıları aracılığıyla sorgulanmakta ve suçun işlendiği saatte ilgili IP adresinin sahibi tespit edilmektedir[122]. Örneğin, Birleşik Devletler/Perez kararında makul şüphenin çocuk pornografisi içeren verilere ulaşan IP adresi ve İnternet hizmet sağlayıcıları aracılığıyla elde edilen ilgili kişinin fiziki adresiyle makul şüphenin oluştuğu belirtilmiştir[123]. Benzer şekilde IP adresi, İnternet hizmet sağlayıcılarında bulunan kayıtlar ve fatura bilgileri ile makul şüphenin oluştuğunu ifade edilmektedir[124].

Kullanılan bir başka yöntem ise, İnternette yer alan kişilere ait hesap bilgilerinin kullanılmasıdır. Bu bilgiler, bir sosyal medya hesabında yer alan profil

---

[119]Jarrett/Bailie/Hagen/Judish, **a.g.e.**, s.63.
[120]United States v. Giberson, 527 F.3d 882, 887 (9th Cir. 2008) (www.justia.com) (Erişim Tarihi:31.08.2019).
[121]United States v. Payton, ___ F.3d ___, 2009 WL 2151348 (9th Cir. July 21, 2009) (www.justia.com) (Erişim Tarihi:31.08.2019).
[122]Jarrett/Bailie/Hagen/Judish, **a.g.e.**, s.65.
[123]United States v. Perez, 484 F.3d 735, 740 (5th Cir. 2007) (www.justia.com) (Erişim Tarihi:31.08.2019).
[124]United States v. Carter, 549 F. Supp. 2d 1257, 1261 (D. Nev. 2008) (www.justia.com) (Erişim Tarihi:31.08.2019).

bilgileri, banka hesap bilgileri ya da diğer iletişim bilgileri olabilmektedir. Örneğin, çocuk pornografisi ile ilgili e-posta göndermek için kullanılan e-posta hesabı sahibinin bu hesapta belirtilen ikametgâh adresinde ve bu adreste yer alan bilişim sistemlerinde arama kararı ile arama gerçekleştirilmiş ve mahkeme ilgili arama kararı ile ilgili makul şüphenin oluştuğuna hükmetmiştir[125].

Amerikan hukukunda bilişim sistemlerinde arama ve elkoyma kararlarında anayasanın ilgili hükmüne göre, arama tedbirinin uygulanacağı yerin ve elkonulacak eşyaların açıkça ifade edilmesi gerekmektedir. Buna, belirlilik ilkesi adı verilmektedir. Belirlilik ilkesine göre, Birleşik Devletler/Upham kararında belirtildiği üzere, arama kararında kolluk kuvvetlerinin arama yapılacak ve elkonulacak eşyaların diğer eşyalardan ayrılabilecek kadar açık bir şekilde ifade edilmesi ve bu elkonulacak eşyaların ilgili karara dayanak teşkil eden makul şüphenin kapsamı içerisinde yer alması gerekmektedir[126].

Belirlilik ilkesi gereğince, elkoyma kararında bilişim sisteminin kendisine mi yoksa bilişim sistemi içerisinde depolanan verilere mi elkonulacağının belirtilmesi gerekmektedir[127]. Bilişim sistemleri kaçaksa ya da bir suç aleti olarak değerlendiriliyorsa bu sistemlerinin kendisine elkonulabilecektir. Örneğin, Birleşik Devletler/Lamb kararında çocuk pornografisi ile ilgili verileri gönderen ve alan bilgisayar suç aleti olarak kabul edilmiş ve ilgili bilgisayarın tamamına elkonulması hukuka uygun bulunmuştur[128]. Bilişim sistemlerinde yer alan veriler yalnızca ceza muhakemesinde delil niteliğine haiz olacaklarsa bilişim sisteminin tamamına elkonulmayacak, sadece ilgili verilere elkonulacaktır[129].

Yukarıda açıkladığımız üzere, bilişim sistemleri Amerikan hukukunda kapalı bir kutu olarak değerlendirilmekte ve her bir kapalı kutu için arama kararı alınması

---

[125]United States v. Terry, 522 F.3d 645, 648 (6th Cir. 2008) (www.justia.com) (Erişim Tarihi:31.08.2019).
[126]United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (www.justia.com) (Erişim Tarihi:31.08.2019).
[127]Jarrett/Bailie/Hagen/Judish, **a.g.e.**, s.70.
[128]United States v. Lamb, 945 F. Supp. 441, 462 (N.D.N.Y. 1996) (www.justia.com) (Erişim Tarihi:31.08.2019).
[129]Jarrett/Bailie/Hagen/Judish, **a.g.e.**, s.72.

gerekmektedir. Ayrıca ilgili kararlarda hangi tür dosyaların hangi bilişim sistemlerinde aranıp elkonulacağının belirtilmesi gerekmektedir[130], aksi takdirde verilen karar genel arama kararına dönüşecek ve belirlilik ilkesini ihlal ederek hukuka uygunluğunu kaybedecektir[131]. Örneğin Birleşik Devletler/Hunter kararında bütün bilgisayarlara, depolama araçlarına ve yazılımlara elkonulması ibaresi[132] ve "Matter of Search Warrant for K-Sports, Inc." kararında arama kararında ise "dahil, ancak bunlarla sınırlı olmamak üzere" ifadesi belirlilik ilkesine aykırı bulunmuştur[133].

Amerikan hukukunda bilişim sistemlerinde arama kararının yerinde uygulanmasının bazı durumlarda uzun sürebileceği dikkate alınarak, ilgili depolama birimlerine elkonulabileceği[134] ya da bu depolama birimleri hakkında kopyalama tedbirine başvurulup ilgili depolama birimlerinin imajının çıkartılabileceği ifade edilmiştir[135]. Buna göre, ya bilişim sistemlerine elkonularak arama tedbiri denetimli bir ortamda uzman tarafından sürdürülecektir ya da bilişim sisteminin depolama birimlerinin imajları çıkartılarak ilgili verilerin bütünlüğü korunacak ve arama tedbirlerine bu imaj üzerinden devam edilecektir.

[130]United States v. Carey, 172 F.3d 1268, 1275(10th Cir. 1999) (www.justia.com) (Erişim Tarihi:31.08.2019).
[131]United States v. Fleet Management Ltd., 521 F. Supp. 2d 436, 443-44 (E.D. Pa. 2007) (www.justia.com) (Erişim Tarihi:31.08.2019).
[132]United States v. Hunter, 13 F. Supp. 2d 574 (D. Vt. 1998) (www.justia.com) (Erişim Tarihi:31.08.2019).
[133]Matter of Search Warrant for K-Sports, Inc., 163 F.R.D. 594 (C.D.Cal. 1995) (www.titleii.com/bardwell/in_re_ksports.txt) (Erişim Tarihi:31.08.2019).
[134]United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) (www.justia.com) (Erişim Tarihi:31.08.2019).
[135]United States v. Hill, 459 F.3d 966, 974-75 (9th Cir. 2006) (www.justia.com) (Erişim Tarihi:31.08.2019).

İKİNCİ BÖLÜM: BİLİŞİM SİSTEMLERİNDE ARAMA, KOPYALAMA VE ELKOYMA TEDBİRLERİ

Türk Hukukunda 1412 sayılı Ceza Muhakemeleri Usulü Kanunu'nun (CMUK) yürürlükte olduğu dönemde, bilişim sistemlerinden delil elde amacıyla düzenlenen bir koruma tedbiri bulunmamaktaydı. Bununla birlikte, 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu[136] m. 4'te *"Bu kanunda öngörülen suçların veya delillerinin ortaya çıkarılması için, suçların işleniş biçimlerine benzer tutum ve davranışlarda bulunan kişilere ilişkin yer, kuruluş, çevre ve kurumundaki, Devletin ulusal güvenliği bakımından gizli kalması zorunlu olanlar hariç her türlü resmi ve özel kayıtlarla bilgisayar verileri incelenebilir."* denilerek, bilgisayar verilerinde arama yapılabileceği düzenlenmekteydi. Dolayısıyla bilişim sistemlerinden delil elde etmek amacıyla uygulanan arama ve elkoyma tedbirleri, CMUK genel arama ve elkoyma hükümlerine göre gerçekleştirilmekteydi[137].

Sayısal delilin ve gün geçtikçe kullanımı yaygınlaşan bilişim sistemlerinin kendine has özelliklerini dikkate alan Türk Kanun Koyucu, özgürlükçü bir yaklaşım[138] sergileyerek yani kişilerin hak ve özgürlüklerini daha iyi bir şekilde korumak adına, bilişim sistemlerinden delil etme amacıyla uygulanacak koruma tedbirlerini 4.12.2004 tarihli 5271 sayılı Ceza Muhakemesi Kanunu'nda düzenlemiştir.

"Bilgisayarda, bilgisayar program ve kütüklerinde arama, kopyalama ve elkoyma" başlığı altında m.134'te düzenlenen koruma tedbirleri, genel arama ve elkoyma tedbirlerinin bilişim sistemlerine ve sayısal verilere uygun olarak uyarlanarak

---

[136]30.7.1999 tarihli ve 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu, 23.3.2005 tarihli ve 5320 sayılı Ceza Muhakemesi Kanununun Yürürlük ve Uygulama Şekli Hakkındaki Kanun m.18 ile mülga edilmiştir.

[137]Tanrıkulu, **a.g.e.**, s.382.

[138]Teknoloji ve hukuku arasındaki ilişki ile ilgili iki farklı bakış bulunmaktadır: Teknolojik gelişmeler karşısında kişilerin temel hak ve özgürlüklerini korumaya devam etmek amacıyla hukuk kurallarının değiştirilmesini öngören özgürlükçü (liberal) yaklaşım ile geleneksel hukuk kuralları takip edilmesini savunan muhafazakâr (conservative) yaklaşım. Özgürlükçü ve muhafazakâr yaklaşım hakkında bkz. Arthur J. Cockfield, "Toward a Law and Technology Theory", **Manitoba Law Review**, Vol. 30, No.3, 2004, s.383-415; Arthur Cockfield/Jason Pridmore, "A Synthetic Theory of Law and Technology", **Minnesota Journal of Law, Science and Technology**, Vol.8, No.2, 2007, s.475-513.

düzenlenmiş halidir[139]. Dolayısıyla, bu koruma tedbirleri kanunun sistematiğine uygun olarak CMK'nın "Koruma Tedbirleri" başlıklı kısmının "Arama ve Elkoyma" başlıklı bölümümde yer almaktadır. Ayrıca, CMK m.134'teki hükmün uygulanmasında uyulacak usul ve esaslar ise Arama ve Önleme Aramaları Yönetmeliği m.17'de belirtilmiştir.

Bunlara ek olarak, 22.04.2014 tarihli ve 6533 sayılı uygun bulma kanunu ile iç hukukumuzun bir parçası haline getirdiğimiz AKSSS m.19'da "Depolanmış Bilgisayar Verilerinin Aranması ve Bunlara El Konulması" başlığı altında, bilgisayar sistemlerinde arama ve elkoyma tedbirleri düzenlenmiştir.

Kanunun lafzında "bilgisayar" ifadesi kullanılsa da öğretide bu durum bazı yazarlar tarafından eleştirilmektedir. Bizim de katıldığımız görüşe göre, bilgisayar kavramı yerine daha kapsayıcı olan bilişim sisteminin kullanılması daha yerinde olacaktır[140]. Aksi taktirde, bilgisayar kavramı dar yorumlandığı zaman, CMK m.134'te düzenlenen koruma tedbirleri bilgisayar tanımına uymayan akıllı telefonlar, GPS cihazları ve araç bilgisayarları gibi bilişim sistemlerinde uygulanamayacaktır.

Bilgisayarda, bilgisayar program ve kütüklerinde arama, kopyalama ve elkoyma tedbirleri, birer koruma tedbiri olduğu için bu tedbirleri incelemeye geçmeden önce koruma tedbiri kavramını açıklamakta fayda vardır. Ceza muhakemesinde muhakeme işlemlerinin sağlıklı olarak yapılabilmesi veya muhakeme sonucunda verilecek kararın tam olarak icra edilebilmesi amacıyla başvurulan, geçici olarak uygulanan, hâkim veya gecikmesinde sakınca bulunan hallerde savcı kararlarına tabi olan ve anayasada düzenlenen temel hak ve özgürlüklere müdahale teşkil eden tedbirlere koruma tedbirleri adı verilir[141].

Anayasa m.13'te anayasada koruma altına alınan temel hak ve özgürlüklerin ancak anayasanın ilgili maddelerinde düzenlenen sebeplere bağlı olarak ve ancak

---

[139]İhsan Baştürk, "Bilgisayar Sistemleri ile Verilerinde Arama, Kopyalama ve Elkoyma", **Fasikül Aylık Hukuk Dergisi**, Y.2, S.9, Ağustos 2010, s.25; Değirmenci, **a.g.e.**, s.313; Yargıtay 16. Ceza Dairesi E. 2015/2056 K. 2017/5023 T. 21.9.2017 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).
[140]İhsan Baştürk, **a.g.e.**, s.25.
[141]Yener Ünver/Hakan Hakeri, **Ceza Muhakemesi Hukuku**, 14. Baskı, Ankara: Adalet, 2018, s.322; Nur Centel/Hamide Zafer, **Ceza Muhakemesi Hukuku**, 15. Bası, Ankara: Beta, 2018, s.354.

kanunla sınırlanabileceği belirtilmiştir. Dolayısıyla, koruma tedbirleri, anayasanın ilgili maddelerinde sebeplere bağlı olarak ancak kanunla düzenlenebilecektir. Benzer şekilde, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirleri açısından bu durum CMK m.134'ün gerekçesinde *"bireye ait kişisel bilgiler üzerinde hak, temel insan haklarından olduğundan hakkın kısıtlanabilmesi için yasal düzenleme gereği açıktır"* denilerek ifade edilmiştir[142].

Koruma tedbirleri, ölçülülük ve belirlilik ilkelerine göre düzenlenmeli ve uygulanmalıdır. Zira, hukuk devleti ilkesinin bir gereği olarak, devlet tarafından temel hak ve özgürlüklere yapılan müdahaleler orantılı, kişiler tarafından öngörülebilir ve hesaplanabilir olması gereklidir. AİHM içtihatlarında belirlilik ilkesi, kanun maddeleri düzenlenirken kanun maddelerinin yeterince açık, belirli ve anlaşılabilir olmasını ifade etmektedir. Ölçülülük ilkesi ise, kamu çıkarı ile kişilerin çıkarları arasında adil bir denge kurulması olarak tanımlanmış ve devletin temel hak ve özgürlüklere yapacağı müdahalelerde devletin takdir yetkisinin denetlenmesi gerektiği belirtilmiştir[143].

Bir başka ifadeyle, ölçülülük ilkesi araçla amacın, uygulanan yöntem ile gayenin dengeli olması anlamına gelmektedir[144]. Bu doğrultuda Ünal, ölçülülük ilkesi gereğince, bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirlerinin kanunla düzenlenmesinin son derece önemli olduğunu ifade etmektedir[145].

Koruma tedbirleri, ceza muhakemesinin sağlıklı yürütülebilmesi ya da muhakeme sonucunda kararın etkili bir şekilde uygulanabilmesi amacıyla uygulandığı için, geçici niteliktedir. Arama, kopyalama ve elkoyma tedbirlerinin geçici olarak bile bilişim sistemlerine uygulanması, müdahalede bulunduğu hak ve özgürlükler

---

[142]**Türk Ceza Kanunu Madde Gerekçeleri** (http://www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc) (Erişim Tarihi: 31.08.2019).
[143]Handyside/Birleşik Krallık, Başvuru Numarası: 5493/72, 7 Aralık 1976 (https://www.rtuk.gov.tr/assets/Icerik/Download/Kararlar/EmsalAIHMKararlari/Handyside-Birle%C5%9Fik%20Krall%C4%B1k%2007.12.1976%20tarih%20ve%205493-72%20Ba%C5%9Fvuru%20Numaral%C4%B1%20Karar.docx?download=true) (Erişim Tarihi: 31.08.2019)
[144]Cumhur Şahin, **Ceza Muhakemesi Hukuku I**, Ankara: Seçkin Yayınevi, 2007, s. 202.
[145]Ünal, **a.g.e.**, s.84.

açısından ağır sonuçlar doğurabilmektedir[146]. Dolayısıyla, bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirleri kanunla düzenlenmesi gerekmektedir.

I. Bilgisayarlarda, Bilgisayar Programları ve Kütüklerinde Arama

A. Tedbirinin Hukuki Niteliği

Genel arama tedbiri, yakalama araması ve delil araması olarak ikiye ayrılmaktadır[147]. Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama tedbirinin amacı, şüpheli tarafından kullanılan bilişim sistemlerinde, işlendiği iddia edilen suça ilişkin sayısal delil, emare ve izlerin araştırılması ve toplanılmasıdır[148]. Dolayısıyla bu tedbiri delil araması kapsamında değerlendirmek gerekmektedir.

Koruma tedbiri, CMK m.130'da düzenlenen avukat bürolarında arama tedbiri gibi genel arama tedbirinin özel bir görünümüdür[149]. Dolayısıyla, m.134 kapsamında düzenlenmeyen konularda, genel arama tedbiri ile ilgili hükümlerine başvurulacaktır[150]. Örneğin, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama tedbirinin uygulama vakti ile ilgili CMK m.134 kapsamında bir düzenleme bulunmamaktadır. Bu sebeple, tedbirin uygulama vaktiyle ilgili genel arama tedbirinin uygulama vaktini düzenleyen CMK m.118 uygulanacak ve tedbir gece vakti gerçekleştirilemeyecektir.

Bilişim sistemlerinde arama tedbiri ile ilgili bir diğer düzenleme ise AKSSS m.19'da yer almaktadır. Bilgisayar verisini arama tedbirinin merkezine koyan bu hükme göre, bir bilgisayar sisteminin tamamı veya bir kısmı ve içerisinde depolanmış bilgisayar verileri ile bilgisayar verilerinin depolanmış olabileceği bir bilgisayar verileri depolama aygıtları aranabilmektedir. AKSSS m.19 ile CMK m.134

---

[146]Ünal, **a.g.e.**, s.84.
[147]Centel/Zafer, **a.g.e.**, s.371;Şemsettin Aksoy, **Avrupa İnsan Hakları Mahkemesi, Uluslararası Yargı ve Yargıtay Kararları Işığında Önleme ve Koruma Tedbiri Olarak Arama**, Ankara: Seçkin Yayıncılık, 2007, s.58.
[148]Değirmenci, **a.g.e.**, s.74-75.
[149]Aslan Ölmez, "Bilgisayarlarda, Bilgisayar Programlarında Kopyalama ve Bunlara Elkoyma", **Terazi Hukuk Dergisi**, S.30, s.46.
[150]Değirmenci, **a.g.e.**, s.74.

karşılaştırıldığında, bilişim sistemlerinin somut unsuru olan donanımın sözleşmede "bir bilgisayar sisteminin tamamı veya bir kısmı", kanunda ise "bilgisayarlar" yazılımın ise sözleşmede "bilgisayar verileri"[151], kanunda ise "bilgisayar programları ve kütükleri" kavramlarıyla ifade edildiği görülmektedir. Fakat, CMK m.134 kapsamında bilgisayar verileri depolama aygıtları hakkında bir düzenleme bulunmamaktadır. Bununla birlikte, AÖAY m.17'de çıkarılabilir donanımlar hakkında da CMK m.134 kapsamında düzenlenen tedbirlerin uygulanacağı belirtilmiştir. Fakat kanunda düzenlenmesi gereken bu hükmün, yönetmelikte düzenlenmesi temel hak ve özgürlüklerin korunması açısından isabetli bulmuyoruz.

Arama tedbiri, başta özel hayatın gizliliği ve konut dokunulmazlığını ihlal eden bir koruma tedbiridir. İhlal ettiği hakların önemine binaen, arama tedbiri ile hükümlere Anayasa m.20 ve m.21 kapsamında yer verilmiştir. Buna göre, milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının haklarının korunması sebebiyle usulüne uygun verilmiş bir hâkim kararıyla ya da gecikmesinde sakınca bulunan hallerde yetkili merciin yazılı emri bulunmadıkça, kimsenin üstü, özel kağıtları ve eşyaları ile konutu aranamayacaktır.

Arama tedbirinin bilişim sistemleri üzerinde uygulanan hali olan, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama tedbiri de anayasada güvence altına alınan özel hayatın gizliliği ve konut dokunulmazlığı haklarına müdahale teşkil etmektedir. Örneğin, bu tedbirin gerçekleştirilmesi için bilişim sistemlerinde sayısal olarak depolanan veriler üzerinde arama yapılmakta ve bunun neticesinde kişilerin şahsi ve aile hayatları ile ilgili belgeleri, görüntüleri ve videoları incelenebilmektedir.

Şirketlere ait bilişim sistemlerinde bu arama tedbiri uygulandığında, şirketlere ait ticari ve mesleki sırlar açığa çıkabilmekte, tedbirin uygulanması sırasında faaliyetlerini bilişim sistemleri olmadan yürütemeyen bankaların, şirketlerin işleyişleri

[151]AKSSS kapsamında bilgisayar verisi, programları da kapsayan bir kavram olarak kullanılmaktadır. **AKSSS Tanımlar – Madde 1/1-b** *""bilgisayar verisi" terimi, bilgisayar sisteminin bir işlevi yerine getirmesini mümkün kılan bir programı da kapsayan, olguların, bilgilerin ve kavramların bir bilgisayar sisteminde işlenmeye uygun haldeki her türlü temsilini ifade eder.".*

durabilmekte ve bu şirketler mali olarak kayıplara uğrayabilmektedir. Dolayısıyla, koruma tedbiri aynı zamana mülkiyet hakkını da ihlal edebilmektedir.

Bunlara ek olarak, tedbirlerin avukatlara ait bilişim sistemlerinde uygulanması durumunda müvekkillere ait gizli bilgilerin açığa çıkabilecek, müvekkil ile avukatı arasındaki ilişki zedelenebilecek ve dolayısıyla müvekkillerin hak arama hürriyetleri tehlike altına girebilecektir.

Bilişim sistemlerinde arama tedbirinin uygulanması sırasında anayasada güvence altına alınan hak ve özgürlükler yukarıda izah edildiği gibi ihlal edilebilmekte ve genel arama tedbiriyle ilgili CMK'nın 116 ile 122. maddeleri arasında düzenlenen hükümler bu hak ve özgürlükleri korumada yetersiz kalabilmektedir. Bu durumu dikkate alan Türk Kanun Koyucu, kanunilik ve ölçülülük ilkesinin gereği olarak bilişim sistemlerinden sayısal delil elde edebilmek için, genel arama tedbirinden ayrı bir koruma tedbirini m.134/1'de düzenleme ihtiyacı duymuştur.

B. Tedbirin Kapsamı

1. Tedbirin Uygulanacağı Kişiler Bakımından

CMK m.134'ün metninde bilgisayarlarda, bilgisayar programları ve kütüklerinde arama tedbirinin soruşturma sırasında şüpheli hakkında uygulanacağı belirtilmektedir. Aynı kanunun tanımlar başlıklı 2. maddesi incelendiğinde, soruşturmanın "*Kanuna göre yetkili mercilerce suç şüphesinin öğrenilmesinden iddianamenin kabulüne kadar geçen evreyi*", şüphelinin ise "*soruşturma evresinde, suç şüphesi altında bulunan kişiyi*" ifade ettiği görülmektedir. Dolayısıyla, kanunun lafzı dikkate alındığında bu tedbirin uygulanabilmesi için öncelikle bir suç şüphesi dolayısıyla yetkili merci olan savcılık tarafından bir soruşturma açılması ve hakkında tedbirin uygulanacağı kişinin ise bu soruşturma kapsamında suç şüphesi altında olması gerekmektedir[152].

[152]Değirmenci, **a.g.e.**, s.318.

Öğretide bazı yazarlar, bu tedbirin soruşturma evresinde olduğu gibi kovuşturma evresinde de uygulanması gerektiğini belirtmektedir. Dolayısıyla bu görüşe göre tedbir şüpheli hakkında uygulandığı gibi, sanık hakkında da uygulanacaktır[153]. Fakat, çalışmamız ilerleyen bölümlerinde ayrıntılı şekilde açıklayacağımız üzere, kovuşturma aşamasının başlayabilmesi için, bir suç işlendiğine dair yeterli şüphe oluşturacak delillerin savcı tarafından toplanılmış olması ve CMK m.134 hükümlerine göre arama tedbirinin uygulanabilmesi için başka surette delil elde etme imkanının bulunmaması gerektiği için biz CMK m.134 kapsamında düzenlenen arama tedbirinin kovuşturma aşamasında sanık hakkında uygulanabileceği görüşüne katılmıyoruz.

Şüpheli dışındaki diğer kişiler hakkında CMK m.134'te düzenlenen arama tedbirinin uygulanması mümkün değildir[154]. Öğretide bu görüş, Değirmenci tarafından üç sebebe dayandırılmaktadır. Birincisi, kanunun lafzında sadece şüpheli kavramına yer verilerek, diğer kişilere yer verilmemesi ve dolayısıyla mefhumu muhalifine göre diğer kişiler hakkında bu koruma tedbirinin uygulanamayacağıdır. İkincisi, genel arama tedbirinin şüpheli veya sanık hakkında uygulanması CMK m.116, diğer kişiler hakkında uygulanması ise CMK m.117 kapsamında düzenlenirken, CMK kapsamında kanunun sistematiğine göre bilgisayarlarda arama tedbirinin diğer kişiler hakkında uygulanmasına yönelik bir hükmün bulunmamasıdır. Üçüncüsü ise, kanunun hazırlık çalışmaları sırasında Kanun Koyucu tarafından diğer kişiler hakkında uygulanacak tedbire bilinçli olarak yer verilmemesidir[155]. Nitekim, Ceza Muhakemesi Kanunu Tasarısında üçüncü kişilerin bilişim sistemlerinde aramaya izin veren bir koruma tedbiri düzenlenmişti. Fakat, CMK m.134 kapsamında düzenlenen koruma tedbirlerinin, kamu kurum ve kuruluşları ile özel hukuk gerçek ve tüzel kişileri hakkında uygulanmasını öngören bu hüküm tasarıdan çıkartılmış ve dolayısıyla kanunlaşmamıştır[156].

---

[153]Değirmenci, **a.g.e.**, s.318.
[154]Ünal, **a.g.e.**, s.91.
[155]Değirmenci**, a.g.e.**, s.319-320.
[156]**Tutanaklarla Ceza Muhakemesi Kanunu**, Ankara: Adalet Bakanlığı Yayın İşleri Dairesi Başkanlığı, 2005, s.580-581.

Bazı suçlarla ilgili yürütülen soruşturmada, örneğin bilişim sistemine girme suçu, failin kullandığı bilişim sistemine ulaşmak ve bu sistem üzerinde arama yaparak delil elde etmek mümkün olamamaktadır. Böyle bir durumda, suç ile ilgili deliller ancak mağdurun bilişim sisteminden elde edilebilmektedir. Nitekim bu durumu dikkate alan Yargıtay 16.04.2007 tarihli kararında "*öncelikle e-posta yolu ile virüs göndererek sistemine zarar verilmiş bir bilgisayarda incelemenin, olayın hemen akabinde yapılması*" gerektiğini ifade ederek, mağdurun ya da şikayetçinin kullanımında olan bilişim sistemlerinde de arama yapılması gerektiğini belirtmiştir[157].

Benzer bir şekilde kolluk kuvvetleri, mağdurun ya da şikayetçinin rızasını almak suretiyle, bu kişilere ait bilişim sistemleri üzerinde arama faaliyetleri gerçekleştirmektedir. Bu arama faaliyetleri sonucunda raporlar oluşturulmakta ve bu raporlar soruşturma dosyasına konulmaktadır[158]. Fakat bizim de katıldığımız öğretideki hâkim görüşe göre CMK m.134 kapsamında mağdurun veya şikayetçinin kullanımında olan bilişim sistemlerinde arama yapmak mümkün değildir[159].

Değirmenci, Yargıtay'ın kararının ve kolluk kuvvetlerinin uygulamalarının yasal bir dayanağı olmadığını belirtmekle birlikte, bu sorunun çözümü için iki çözüm önerisi getirmektedir. Bunlardan ilki mağdurun kullanımında olan bilişim sistemlerini aynı zamanda olay yeri olarak değerlendirerek, bu sistemler üzerinde AÖAY m.9'a göre bilimsel ve teknik yöntemlerle olay yeri inceleme işlemlerinin yapılmasıdır. İkincisi ise, CMK m.134 ve AÖAY m.17 hükümlerinde değişikliğe gidilerek, bu maddelere mağdurun ve şüphelinin açık rızası ile bu kişilere ait bilişim sistemlerinde arama yapılabileceğine dair düzenlemelerin eklenmesidir[160].

Nitekim benzer bir değişiklik CMK m.135 kapsamında düzenlenen "İletişimin Tespiti, Dinlenmesi ve Kayda Alınması" tedbirlerinin uygulanmasında uyulacak usul ve esasların tespit edildiği ve Danıştay tarafından iptal edilen "Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi,

---

[157]Yargıtay 11. Ceza Dairesi E. 2005/6376 K. 2007/2551 T. 16.04.2007 (kararara ma.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).
[158]Değirmenci**, a.g.e.**, s.324.
[159]Baştürk, **a.g.e.**, s.28; Ünal, **a.g.e.**, s.93.
[160]Değirmenci**, a.g.e.**, s.323-324.

Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik"[161] m.10'a "*Bir soruşturma sırasında delil toplama kapsamında, somut olayın özelliğine göre maddî gerçekliğin araştırılması ve adil bir yargılamanın yapılabilmesi için zorunlu olduğu takdirde, açık rızasının bulunması ve iletişim aracının kendisine ait olması şartıyla şikâyetçinin iletişiminin tespiti Cumhuriyet savcısının yazılı kararıyla Başkanlıktan istenir."* fıkrası eklenerek yapılmıştır. Fakat, eklenen bu fıkra Danıştay 10. Dairesi tarafından 24.12.2014 tarihli kararla iptal edilmiştir[162].

Ceza muhakemesinde yargılamanın kurucu unsurlarından biri savunmadır ve Avukatlık Kanunu m.1'e göre, *"avukat, yargının kurucu unsurlarından olan bağımsız savunmayı serbestçe temsil eder"*. Avukatın müvekkili ile olan güven ilişkisinin savunma hakkı açısından önemini ve avukatın mesleki sırlarının korunmasının gerekliliğini dikkate alan Kanun Koyucu, CMK m.130'da *"avukat bürolarında arama"* koruma tedbirini düzenlemiştir. Buna göre, avukat büroları cumhuriyet savcısının denetiminde, mahkeme kararı ile ve kararda belirtilen olayla ilgili aranabilmektedir. Ayrıca, bu arama esnasında baro başkanı veya onu temsil eden bir avukat hazır bulunmak zorundadır.

Bir avukatın suç soruşturması kapsamında şüpheli sıfatına haiz olması durumunda ise avukatın kullanımında bulunan bilişim sistemlerinde arama yapılması gerekebilecektir. Bu durumda hem avukatın özel hayatın gizliliği, mülkiyet hakları ihlal edilecek hem de avukatın meslek sırları açığa çıkarılıp, müvekkilinin savunma hakkına müdahale edilecektir. Bu sebeple öğretide avukatların kullanımında olan bilişim sistemlerinde arama yapılması durumunda, CMK m.130 ve CMK m.134 hükümlerinin beraber olarak uygulanacağı savunulmakta[163] ve uygulamada da

[161]Danıştay Onuncu Dairesi 09/03/2017 tarihli ve 2012/1001 E. 2017/1361 K. sayılı kararı ile Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmeliğin iptaline karar verilmiştir.

[162]Danıştay Onuncu Dairesi 24/12/2014 tarihli ve 2013/3791 E. 2014/8138 K. sayılı kararı ile fıkra iptal edilmiş ve bu karar Danıştay İdari Dava Daireleri Kurulu 24.11.2016 tarihli ve 2015/2131 E. 2016/3097 K. sayılı kararı ile onanmıştır.

[163]Veli Özer Özbek, **CMK İzmir Şerhi, Yeni Ceza Muhakemesi Kanununun Anlamı (Gerekçeli-İçtihatlı)**, Ankara: Seçkin Yayıncılık, 2005, s.503; Ünal, **a.g.e.**, s.94-95; Değirmenci, **a.g.e.**, s.325.

Yargıtay tarafından benzer görüş benimsenmektedir. Nitekim, Yargıtay 16. Ceza Dairesinin 21 Nisan 2016 tarihli kararında sanık sıfatıyla haklarında arama kararı verilen avukatların bürolarında yapılan arama sonucu elkonulan dijital medyaların hükme esas alınmasını, hem CMK m.134 kapsamında bir arama kararı olmaması hem de CMK m.130/2 uyarınca iddiaya konu olan delillerin mühürlenerek hâkim önüne götürülmesi ve hâkimin kararı sonrasında işlem yapılması gerekirken bu hükme aykırı hareket edilmesi dolayısıyla hukuka aykırı bulmuştur[164].

Ayrıca, avukat bürolarında uygulanan bilişim sistemlerinde arama tedbiri savcının gözetiminde ve baro başkanının ya da onu temsil eden bir avukatın denetiminde kolluk kuvvetleri tarafından gerçekleştirilecektir. Nitekim, AİHM Wieser ve Bicos Beteiligungen GmBH/Avusturya kararında, elektronik verilerde arama yapılması sırasında baro temsilcinin etkin denetiminin olmaması sebebiyle, avukatın mesleki sır saklama yükümlülüğünü korumayı amaçlayan muhakeme güvencelerine uygun davranılmadığını tespit etmiş ve AİHS m.8 kapsamında koruma altına alınan özel ve aile hayatına saygı hakkının ihlal edildiğine karar vermiştir[165].

Ceza muhakemesinin iddia makamını temsil eden savcı ve yargılama makamını temsil eden hakimlerin bağımsızlığını korumak adına, Kanun Koyucu, 2802 sayılı Hakimler ve Savcılar Kanunu m.88'de ağır ceza mahkemesinin görevine giren suçlarda suçüstü hali hariç, savcıların ve hakimlerin üstlerinin ve konutlarının aranamayacağını düzenlemiştir. Ayrıca Hakimler ve Savılar Kanunu (HSK) m.82'ye göre hakimler ve savcılar hakkında soruşturma yapılması Adalet Bakanlığı'nın iznine bağlıdır. Dolayısıyla, kanunun lafzında açıkça yer verilmese de öğretide ağır ceza mahkemesinin görevine giren suçlarda suçüstü hali hariç olmak üzere, Adalet Bakanlığı'nın soruşturma izni olmadan hâkim ve savcılar hakkında bilgisayarlarda, bilgisayar programları ve kütüklerinde arama tedbirinin uygulanamayacağı görüşü savunulmaktadır[166].

---

[164]Yargıtay 16. Ceza Dairesi E. 2015/4672 K. 2016/2330 T. 21/04/2016 (kararara ma.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

[165]Wieser ve Bicos Beteiligungen GmBH/Avusturya (Türkçe Çeviri), Başvuru Numarası: 74336/01, 16 Ekim 2007, Çev: Serkan Cengiz https://hudoc.echr.coe.int/tur#{%22fulltext%22:[%22Wieser%20ve%20Bicos%22],%22itemid%22:[%22001-112040%22]} (Erişim Tarihi: 14.05.2018); Wieser ve Bicos Beteiligungen GmBH/Avusturya Davası, Çev: Serkan Cengiz, **TBB Dergisi**, S.82, Mayıs 2009, s.447-466.

[166]Şemsettin Aksoy, **a.g.e.**, s.113.

2. Tedbirin Uygulanacağı Cihazlar Bakımından

Tedbirin düzenlendiği CMK m.134'te, şüphelinin kullandığı bilgisayarlarda, bilgisayar programları ve kütüklerinde arama yapılacağı belirtilmiştir. Dolayısıyla, bir bilişim sisteminde arama yapılabilmesi için, öncelikle bu bilişim sisteminin şüpheli tarafından kullanılmış olması gerekmektedir. Nitekim Yargıtay, arama tedbirinin uygulandığı bilgisayarların şüphelilere kullanımında olup olmadığı tespit edilmeden verilen kararı, eksik araştırma dolayısıyla hukuka aykırı bularak bozmuştur[167].

Bilişim sistemleri, giriş ve çıkış birimleri aracılığıyla, şüpheli tarafından doğrudan kullanılabilmektedir. Örneğin, şüpheli bilgisayarda bir metin yazdığında klavye aracılığıyla bilgisayara veriler girmekte ve bu girdiği verileri ekran aracılığıyla okuyup kontrol edebilmektedir. Bununla beraber, iletişim teknolojilerinin gelişmesi ve bilişim sistemlerini birbirine bağlayan Internet, Extranet ve Intranet gibi iletişim ağlarının ortaya çıkması sonucunda, bilişim sistemlerini uzaktan erişimle kullanmak mümkün hale gelmiştir. Örneğin, bir bilgisayar korsanı (hacker) "*botnet*" adı verilen kötü amaçlı yazılımlar ile başka bilgisayarları ele geçirebilmekte ve bu bilgisayarları kendisi için çalışan "*zombi*" bilgisayarlara dönüştürebilmektedir. Uzaktan kontrol edilebilir hale gelen zombi bilgisayarlar, "*DDos*" adı verilen, toplu olarak hedef bir bilişim sistemine yönlendirilerek yapılan saldırılarda ya da çıkar elde etmek amacıyla kullanılabilmektedir[168].

---

[167]Yargıtay 1. Ceza Dairesi E. 3700 K. 2007/4661 T. 11.06.2007 *"... İddianameye konu olan eylemlerin kanıtı olarak gösterilen ve bir kısım sanıkların yetkilisi ve çalışanı olan Uzanlara ait şirket ve evlerde yapılan aramalar sırasında elde edilen bilgisayar kayıtlarında bulunduğu ileri sürülen elektronik postalar ile yer aldıkları bilgisayarların nerede ve hangi yöntemle elde edildiği, sanıkların kullanımında olup olmadığı, kimler arasında yapıldığı, başkaları tarafından oluşturulma ya da içeriklerine müdahale olanağı bulunup bulunmadığı, İstanbul 1, 2 ve 9. Asliye Ticaret Mahkemelerinin 2000/2180, 2000/2095 ve 2000/2082 Değişik iş sayılı tespit davalarında bilirkişilik yapan sanıklara diğer sanıklar tarafından para ödenip ödenmediği, star digital ya da telefon aboneliği sağlanıp sağlanmadığı ve ücretlerinin kim tarafından ödendiği, düzenlenen bilirkişi raporlarının gerçeklere uygun olup olmadığı hususları araştırılıp, konunun uzmanı bilirkişilerden de mütalaa alındıktan sonra sanıkların hukuki durumlarının tayin ve taktiri yerine eksik araştırmaya dayanılarak yazılı şekilde beraat kararı verilmesi kanuna aykırıdır."*; aktaran Aslan Ölmez, **a.g.e.**, s.50.

[168]Dülger, **a.g.e.**, s.120-121.

Öğretide, bu iki kullanım şekli "fiili" ve "sanal" kullanım olarak adlandırılmış ve şüpheli tarafından fiili olarak kullanılan bilişim sistemlerinde olduğu gibi sanal olarak kullanılan bilişim sistemlerinde de CMK m.134 kapsamında arama yapılabileceği belirtilmiştir[169]. Nitekim, AKSSS m.19/2'de kendi ülke sınırları içerisinde kalmak şartıyla, arama yapılan bilişim sistemlerinden erişim sağlanabilen bilişim sistemlerinde arama yapılabilmesi için gerekli yasama tedbirlerinin alınması gerektiği belirtilmektedir. AÖAY m.17/3'te ise "*bilgisayar ağları ve diğer uzak bilgisayar kütükleri*" ifadesine yer vererek, bilgisayara ağları aracılığıyla sanal olarak kullanılan bilişim sistemlerinde arama yapılabileceğini ifade etmiştir. Fakat bilgisayar ağları ile diğer bilgisayar uzak kütüklerinde aramanın temel hak ve özgürlüklere müdahale teşkil etmesine rağmen yasa ile düzenlenmeyerek yönetmelikte yer verilmesi öğretide eleştirilmektedir[170]. Nitekim, AKSSS m.19/2'ye göre Türk Kanun Kuyucu'nun yerinde arama gerçekleştirilen bilişim sisteminden bilişim ağları aracılığıyla erişilen bilişim sistemlerinin tamamına veya bir kısmında arama yapılması ile ilgili yasal tedbirleri alma yükümlülüğü bulunmaktadır. Anayasamıza göre bu tür tedbirlerin sadece yasa ile düzenlenebileceği göz önüne alındığında, yükümlülüğün bir yönetmelik maddesi ile yerine getirilmesi bizim görüşümüze göre mümkün değildir.

Şüphelinin kullanımında olan bilişim sisteminde arama yapılabilmesi için, bilişim sisteminin şüpheliye ait olması gerekmemektedir. Dolayısıyla, bilişim sistemi üçüncü bir kişiye ait olabileceği gibi, kamu kurum ve kuruluşlarına da ait olabilecektir[171]. Bu görüş, Yargıtay tarafından da benimsenmiş ve şüpheliye ait olmayan fakat şüpheli tarafından kullanıldığı tespit edilen internet kafedeki bilgisayarlarda ve bilgisayar programlarında arama yapılması gerektiği belirtilerek ifade edilmiştir[172].

---

[169]Değirmenci, **a.g.e.**, s.321
[170]Tanrıkulu, **a.g.e.**, s.428.
[171]Ünal, **a.g.e.**, s.92; Değirmenci, **a.g.e.**, s.321.
[172]Yargıtay 5. Ceza Dairesi E. 3891 K. 2005/3230 T.14.11.2005 *"Olay tarihinde sanıkla maktulün internet üzerinde sohbet ettikleri söylenen kafede sanığın 'Kaan' kod adıyla 21 no.lu masada ve maktulün kullandığı belirtilen bilgisayarların ve kullandıkları programın saptanarak bilgisayarlarda ve bilgisayar programının merkezi sisteminde sohbet kaydının mevcut olup olmadığı ve içeriğinde hakaret ve tahrik edici sözler olup olmadığı tespit edilmeden yazılı şekilde hüküm kurulması usule aykırı bulunduğundan hükmün BOZULMASINA, oybirliği ile karar verildi...";* aktaran Ölmez, **a.g.e.**, s.50.

Aranacak veriler ve bu verilerin depolandığı bilişim sistemleri herkese açık alanlarda, örneğin çöp kutularında bulunduğu zaman bu sistemlerden bir suç soruşturması kapsamında delil elde edilebilecektir[173]. Fakat bu bilişim sistemlerinden delil elde etmek için CMK m.134 hükümleri uygulanmayacak ve bu durum için hâkim kararı gerekmeyecektir[174]. Ancak kişilerin mülkiyetinden ya da zilyetliğinden çıkmayan otel odalarındaki ya da evlerinin bahçelerindeki çöplerde bulunan bilişim sistemlerinden delil elde etmek için CMK m.134 hükümleri uygulanmaya devam edecektir[175].

Kanunun lafzına bakıldığında, tedbirin sadece bilgisayarlarda, bilgisayar programları ve kütüklerinde uygulanabileceği anlaşılmaktadır. Fakat giriş bölümünde ifade ettiğimiz gibi, kanunun lafzı dar yorumlandığı durumda bilgisayar tanımına girmeyen fakat veri işleme ve iletme yeteneğine sahip bilişim sistemlerinde bu tedbir uygulanamayacaktır. Bu durumda ise bu cihazlarda depolanan kişisel bilgiler, kanunun gerekçesine uygun olarak korunamayacaktır[176]. Dolayısıyla, Türk Kanun Koyucu tarafından ilgili hükümde değişikliğe gidilmeli ve "bilgisayarlarda, bilgisayar programlarında ve kütüklerinde" ifadesi yerine, daha kapsayıcı bir ifade olarak "bilişim sistemlerinde" ifadesi kullanılmalıdır.

Uygulamada Yargıtay, çalışmamızın giriş bölümünde ifade ettiğimiz gibi, ATM cihazlarını, tabletleri, internet sitelerini içerisinde barındıran sunucuları birer bilişim sistemi olarak kabul etmektedir. Dolayısıyla, Yargıtay'ın kabul ettiği görüşe göre, CMK m.134 kapsamında arama faaliyetleri bilgisayarlarda ve bilhassa Yargıtay tarafından bilişim sistemi olarak kabul edilen cihazlarda yürütülebilecektir. Ayrıca, Yargıtay CD, DVD, flaş bellek, disket, harici ve dahili sabit disk, akıllı telefon ve benzerlerinden sayısal delillerin elde edilebileceğini belirterek, bu cihazlarda arama yapılabilmesi için CMK m.134 hükümlerine dayanan bir arama kararının olması gerektiğini ifade etmektedir[177].

---

[173]Aksoy, **a.g.e.**, s.21.
[174]Tanrıkulu, **a.g.e.**, s.427.
[175]Duygu Çağlar Doğan, "Ceza Muhakemesinde Adli Arama", **TBBD**, S.92, s.167.
[176]*"Madde, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve geçici elkoyma konularını düzenlemektedir. Bireye ait kişisel bilgiler üzerindeki hak, temel insan haklarından olduğundan hakkın kısıtlanabilmesi için yasal düzenleme gerekeceği açıktır."*
[177]Yargıtay 16. Ceza Dairesi E. 2015/2056 K. 2017/5023 T. 21.9.2017 (kararara ma.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

Bilişim sistemlerinde arama koruma tedbirini düzenleyen bir başka hüküm olan AKSSS m.19'da ise bilgisayar kavramı yerine bilgisayar sistemi kavramı tercih edilmiştir. Sözleşme kapsamında "*bir veya birden fazlası, bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbiriyle bağlantılı veya ilgili bir grup cihaz*" olarak tanımlanan bilgisayar sistemi daha kapsayıcı bir kavramdır ve birçok dilde bilişim sisteminin karşılığı olarak kullanılmaktadır.

Hayatımıza haberleşme aracı olarak giren ve teknolojik gelişmeler doğrultusunda bilişim yeteneği kazanan akıllı cep telefonlarında CMK m.134 hükümlerine göre arama tedbiri uygulanmaktadır[178]. Günümüzde akıllı cep telefonları verileri işleyebilmekte, işlediği verileri hafıza birimlerinde saklayabilmekte ve iletişim altyapılarını kullanarak bunları başka bilişim sistemlerine iletilebilmektedir[179]. Yargıtay akıllı cep telefonlarında arama tedbirinin uygulanabileceğini ve bunların depolama birimlerinde inceleme yapılabileceğini[180] ve bu arama tedbirinin uygulanması için CMK m.134 uyarınca akıllı cep telefonlarında arama kararının olması gerektiğini ifade etmektedir[181]. Bununla birlikte, biz kanunun lafzının uygulamada Yargıtay kararları ile genişletilmesini ve akıllı cep telefonlarında CMK m.134 kapsamında arama, kopyalama ve elkoyma tedbirlerinin uygulanmasını isabetli bulmamakta ve yukarıda ifade ettiğimiz gibi kanun lafzının akıllı cep telefonlarını

---

[178]Değirmenci, **a.g.e.**, s.330; Ünal, **a.g.e.**, s.98; Feridun Yenisey, Ayşe Nuhoğlu, **Ceza Muhakemesi Hukuku**, Ankara: Seçkin, 2017, s.431; karşıt görüşler için *"Cep telefonlarından doğrudan doğruya internete girilerek bir bilişim suçu işlendiğinde bu suçun CMK m.134'teki soruşturma yöntemlerine göre soruşturulmasının mümkün olmadığı kanaatindeyiz. Çünkü, CMK 134, bilgisayarların aranmasını düzenlemektedir. Oysa cep telefonu bilgisayar değildir."* Şaban Cankat Taşkın, **Bilişim Suçları**, Bursa: Beta Yayınevi, 2008, s.173)

[179]Değirmenci, **a.g.e.**, s.330.

[180]Yargıtay 8. Ceza Dairesi E. 2014/29566 K. 2015/13421 T. 11.3.2015 "*Şikayetçi ve sanığın bilgisayarlarına veya akıllı cep telefonlarına el konulup hard diskleri incelenerek…"* (kararara ma.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

[181]Yargıtay 17. Ceza Dairesi E. 2015/27517 K. 2017/1716 T. 15.2.2017 *"Cumhuriyet Savcısının talimatıyla yapıldığı belirtilen, telefon inceleme tutanağının düzenlendiği saatten daha önceki bir saatte düzenlenen "fotoğraf teşhis tutanağına" göre şüphe üzerine durdurulan sanığın cep telefonunun Cumhuriyet savcısının emri ya da mahkeme kararı olmadan kolluk görevlileri tarafından incelendiği ve telefonda, müştekiye ait çalıntı motosikletin fotoğrafının telefonda kayıtlı bir kişiye gönderildiğinin tespiti üzerine sanık hakkında mahkumiyet kararı verilmiş ise de; işlevi itibarıyla bilgisayar niteliğinde olan cep telefonu üzerinde inceleme yapılabilmesi için CMK'nın 134. maddesi uyarınca hakim kararı alınması gerektiği bu kararın alınmaması sebebiyle arama ve incelemenin yasaya aykırı olduğu ve bu delilin mahkumiyete esas alınmayacağı gibi bu delil yasal kabul edilse bile sanığın cep telefonunda bulunan motosiklet fotoğrafının müştekiye ait motosiklet olduğu"* (kararara ma.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

kapsayacak bir şekilde bilişim sistemlerinde arama, kopyalama ve elkoyma olarak değiştirilmesi gerektiğini savunmaktayız.

Akıllı cep telefonları aracılığıyla gerçekleştirilen telefon görüşmeleri ve internet aracılığıyla alınıp gönderilen veriler akış halindeki veri statüsünde oldukları için bu veriler "iletişimin tespiti, dinlenmesi ve kayda alınması" başlığıyla CMK m.135'te düzenlenen koruma tedbiri kapsamına girmektedir ve dolayısıyla çalışmamız kapsamında değerlendirilmeyecektir. CMK m.134'te düzenlenen arama tedbiri, sadece bilişim sistemlerinin depolama birimlerinde saklanan durağan verileri incelemeye yönelik olarak düzenlenen bir koruma tedbiridir.

AÖAY m.17'de arama tedbirinin çıkarılabilir donanımlar üzerinde uygulanabileceği belirtilmiştir. Dolayısıyla içerisinde veri saklayabilen disket, CD, DVD, taşınabilir USB bellek, hafıza kartları, harici disk gibi çıkarılabilir depolama cihazlarında arama tedbirleri uygulanabilecektir[182]. Ayrıca, AKSSS kapsamında yapılan bilgisayar sistemi tanımında "birbiriyle bağlantılı ya da ilgili bir grup cihaz" ifadesi yer almaktadır. Buna göre, bilişim sistemleri ile bağlantılı olan çıkarılabilir depolama cihazları AKSSS m.19 hükümlerine göre aranabilmektedir[183]. Fakat, Değirmenci uygulamada çıkarılabilir depolama cihazlarında CMK m.134 kapsamında arama faaliyetlerinin gerçekleştirilmediğini, bunun yerine bu cihazlar için genel arama tedbirlerine başvurulduğunu belirtmektedir[184].

CMK m.134 hükümlerine göre bilgisayar programlarında arama tedbiri uygulanabilmektedir. Bilgisayar programları sayısal delil niteliğine haiz olabilecek verileri kendi içinde barındırabilmektedir. Örneğin, bir kelime işlemci programı olan Microsoft Word, bu program aracılığıyla yazılan son belgelerin kopyalarını ve bu belgelere ait bilgileri içerisinde barındırmaktadır. Bu belgeler ve bu belgelere ait bilgiler ise ceza muhakemesinde delil olabilecektir. Aynı zamanda, kötü amaçlı yazılımlarda olduğu gibi programların bizzat kendileri de delil olabilmektedir[185].

---

[182]Yargıtay Ceza Genel Kurulu E. 2017/956 K. 2017/370 T. 26.09.2017 (kararara ma.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019)
[183]Değirmenci, **a.g.e.**, s.331.
[184]Değirmenci, **a.g.e.**, s.331.
[185]Ünal, **a.g.e.**, s.96; Değirmenci, **a.g.e.**, s.332.

Bilişim sistemlerinde verilerin saklandığı mantıksal depolama birimleri olarak tanımlanan bilgisayar kütükleri, CMK m.134 kapsamında arama yapılabilecek bir diğer yer olarak ifade edilmektedir. Bilişim sistemi tarafından işlenen her türlü veri, sayısal bir şekilde bilgisayar kütüklerinde depolanmaktadır. Örneğin, tez çalışmamız "Bilişim Sistemlerinde Arama, Kopyalama ve Elkoyma.docx" isimli bir kütükte, bu kütük ise bilgisayarımızın "Yerel Disk (C:)" isimli mantıksal bir depolama biriminde saklanmaktadır.

AKSSS, m.19 kapsamında sözleşmeye taraf devletlere ulusal sınırlar içerisindeki diğer uzak bilişim sistemlerindeki verilerin aranmasına ilişkin yasama tedbirlerini düzenleme yükümlülüğü getirmektedir. Türk Kanun Koyucu, günümüze kadar bu yükümlülüğünü yerine getirmek adına kanunla bir yasama tedbiri düzenlememiştir. Bununla birlikte, Adalet ve İçişleri Bakanlıkları, AÖAY m.17'de bilgisayar ağlarında ve diğer uzak bilgisayar kütüklerinde de koruma tedbirinin uygulanacağı belirterek, bilgisayar kütüğü kavramının bir bilişim sisteminin kendi depolama birimleri ile sınırlı kalmayacağını ifade etmiş ve bu kavramı bir bilişim sistemi aracılığıyla ulaşılabilir bütün depolama birimlerine genişletmiştir. Nitekim, uygulamada Yargıtay da benzer bir görüşü benimseyerek, bir bilgisayar üzerinden ulaşılabilen ortak paylaşıma ve kullanıma açık diğer bilgisayarlardaki veri depolama araçlarını ve veritabanlarını bilgisayar kütüğü kavramı içine dahil etmektedir[186].

Bilişim sistemlerinin ya da uzak bilgisayar kütüklerinin belirli kısımlarının kullanıcılara tahsil edilmesi mümkündür. Böyle bir durumda CMK m.134 kapsamında arama sadece şüphelinin kullanımına tahsil edilen kısımda yapılması gerekmektedir[187]. Örneğin, birçok kullanıcı tarafından kullanılan ve her kullanıcı için ayrı bir kullanıcı hesabının bulunduğu şirket bilgisayarlarında arama yapılması durumunda, arama sadece şüphelinin kullanımına açık programlarda ve kütüklerde yapılmalıdır. Benzer bir şekilde, uzak bilgisayar kütüklerinde arama yapılabilmesi için, arama mahallindeki bilişim sisteminden bu kütüklere ulaşılabilmesi, ilgili kütüklerin şüphelinin

[186]Yargıtay Ceza Genel Kurulu E. 2017/16-956, K. 2017/370, T. 26.9.2017 (kararara ma.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).
[187]Değirmenci, **a.g.e.**, s.330.

kullanımında olması ve ulusal sınırlar içerisinde yer alması gerekmektedir. Nitekim bu husus AKSSS m.19/2'de *"bunlara (bilgisayar sistemlerine) erişim sağlanması söz konusu olduğunda ve aranan verilerin kendi ülkesindeki başka bir ve aranan verilerin kendi ülkesindeki başka bir bilgisayar sisteminin tamamında veya bir kısmında depolanmış olduğuna inanmak için gerekçeleri bulunduğunda ve söz konusu veriler yasalara uygun biçimde ilk sistemden erişilebilir veya ilk sistem için kullanılabilir olduğunda, makamlarının arama veya benzer şekilde sisteme erişim işlemlerini süratle diğer sisteme teşmil edebilmelerini sağlamak için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edeceklerdir."* denilerek ifade edilmiştir.

Son olarak, elektronik postalarda CMK m.134 kapsamında arama yapılıp yapılamayacağını değerlendirmek gerekirse, elektronik posta öncelikle bir haberleşme aracıdır. Bu haberleşme aracında postalar elektronik olarak sunucularda tutulmakta ve kişiler arasında bu sunucular vasıtasıyla aktarılmaktadır. Elektronik postalarda veriler akış halindedir ve normal şartlarda bu veriler kişilerin bilişim sistemlerinde depolanmamaktadır. Bu sebeplerden dolayı, elektronik postalarda CMK m.135 kapsamında düzenlenen koruma tedbirleri uygulanmalıdır[188]. Fakat elektronik postalar kişiler tarafından bilişim sistemlerinde depolandığı taktirde, artık veriler akış halinden durağan hale geçmektedir, dolayısıyla böyle bir durumda CMK m.134'te düzenlenen arama tedbirlerine başvurulabilecektir. Öğretide Değirmenci, elektronik postaların göndericinin sunucusundan, alıcının sunucusuna ulaştığı taktirde verilerin durağan hale geçtiğini ve bu sunucular üzerinde CMK m.134 hükümlerinin uygulanabileceğini savunmaktadır[189].

AKSSS kapsamında ise, elektronik posta ile ilgili bir hükme yer verilmemiş ve sözleşmeye ilişkin Açıklayıcı Memorandum[190] m.190'da elektronik postalar ile ilgili düzenlemeler ulusal mevzuatlara ve hukuk sistemlerine bırakmıştır.

---

[188]Ünal, **a.g.e.**, s.99.
[189]Değirmenci, **a.g.e.**, s.333.
[190]**AKSSS Açıklayıcı Memorandum**, Çev: İnternet ve Hukuk Platformu https://www.ozgureralp.av.tr/avrupa-konseyi-siber-suc-sozlesmesi-aciklayici-memorandum-internet-ve-hukuk-platformu-i-v-h-p-cevirisi/ (Erişim Tarihi: 17.05.2018).

C. Tedbirin Şartları

Bilişim sistemlerinde uygulanacak arama tedbirinin, temel hak ve özgürlükleri ne denli ihlal ettiğini dikkate alan Türk Kanun Koyucu, CMK m.134'te bilgisayarlarda ve bilgisayar programları ve kütüklerinde arama tedbirini düzenlemiş ve ayrıca bu tedbire başvurulabilmesi için belli şartlar öngörmüştür. Buna göre, bilişim sistemlerinde arama yapılabilmesi için, öncelikle bir suç soruşturmasının ve somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı gereklidir. Buna ek olarak, başka surette delil elde edilebilme imkanının bulunmaması gerekmektedir. Dolayısıyla, Kanun Koyucu bu tedbiri *ultima ratio* yani son çare olarak başvurulacak bir tedbir olarak düzenlemiştir. Nitekim bu durum, CMK m.134'ün gerekçesinde *"söz konusu işleme başvurulmasının zorunlu olması yani bunun bir "ultima ratio" çare oluşturması gereklidir."* denilerek ifade edilmiştir.

Uygulamada, tedbirlerin özel hayata ve kişisel verilere yönelik olumsuz etkileri ile elektronik delillerin güvenliğinin ve sıhhatinin korunmasının gerekliliğini göz önüne alan Yargıtay, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirlerinin "son çare" olarak başvurulabilecek "özel koşullara tabi" koruma tedbirleri olduğunu kararlarında vurgulamaktadır[191].

Meclise sevk edilen CMK Tasarısında "iletişimin tespiti, dinlenmesi ve kayda alınması" tedbirlerinde olduğu gibi, durağan verilerden delil elde yönelik olarak CMK m.134'te düzenlenen arama tedbiri için de iki yıl ve daha fazla süreli hürriyeti bağlayıcı cezalarda uygulanabileceğine dair bir hüküm bulunmaktaydı. Fakat bu hüküm Adalet Komisyonu görüşmeleri sırasında metinden çıkartılmıştır. Dolayısıyla, kanunlarda suç olarak düzenlenen herhangi bir fiilin soruşturmasında, bu tedbire başvurulabilecektir[192].

1. Suç Soruşturmasının Varlığı

[191]Yargıtay 16. Ceza Dairesi E. 2015/2056 K. 2017/5023 T. 21.9.2017 (kararara ma.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).
[192]Değirmenci, **a.g.e.**, s.337.

CMK m.134'ün birinci fıkrasında Kanun Koyucu, "*bir suç dolayısıyla yapılan soruşturmada*" ifadesine yer vermiştir. Dolayısıyla, bilgisayarlarda ve bilgisayar programları ile bilgisayar kütüklerinde arama tedbirine başvurulabilmesi için, öncelikle CMK kapsamında bir suç soruşturmasının varlığı gereklidir[193]. CMK hükümlerine göre soruşturma evresi bir suç şüphesinin öğrenilmesinden itibaren başlamakta ve iddianamenin kabulüne kadar devam etmektedir.

Suç soruşturması kapsamına girmeyen soruşturmalarda ise, örneğin idari soruşturma ya da disiplin soruşturması, bu tedbire başvurulamayacaktır[194]. Benzer şekilde, 5326 sayılı Kabahatler Kanunu kapsamındaki fiiller bakımından da CMK m.134 hükümlerine başvurulamayacaktır çünkü kabahatler bakımından bir suç soruşturması yürütülmemektedir[195].

Öğretide, kovuşturma aşamasında bilgisayarlarda ve bilgisayar programları ile bilgisayar kütüklerinde arama tedbirine başvurulup başvurulamayacağına dair ise fikir birliği bulunmamaktadır. Bir kısım yazarlar, kovuşturma aşamasında mahkemenin CMK m.225/2'ye göre iddia ve savunmalarla bağlı olmadığını, mahkemenin gerekli gördüğü durumlarda vicdani kanaat getirmek için re'sen delil toplayabileceğini dolayısıyla mahkeme kararıyla bilişim sistemlerinde CMK m.134 hükümlerine göre arama yapılabileceği görüşünü savunmaktadırlar[196]. Uygulamada Yargıtay birçok kararında öğretideki bu görüşü savunan yazarlara atıfta bulunarak, benzer bir yaklaşım benimsediğini vurgulamaktadır[197].

Aksi görüşü savunan yazarlar ise, tedbirin uygulanması için CMK kapsamında bir soruşturmanın varlığı arandığını ve arama tedbirinin sadece şüphelinin kullandığı

---

[193]Tanrıkulu, **a.g.e.**, s.389; Ünal, **a.g.e.**, s.323.
[194]Baştürk, **a.g.e.**, s.25; Ünal, **a.g.e.**, s.100; Değirmenci, **a.g.e.**, s.333; Özen/Baştürk, **Temel Hak ve Özgürlükler Bağlamında Bilişim-İnternet ve Ceza Hukuku**. Ankara: Adalet Yayınevi, 2011, s.144.
[195]Değirmenci, **a.g.e.**, s.337.
[196]Cumhur Şahin, **a.g.e.**, s.251; Değirmenci, **a.g.e.**, s.335; Baştürk, **a.g.e.**, s.25; Ünal, **a.g.e.**, s.100; Tanrıkulu, **a.g.e.**, s.399; Muharrem Özen/Gürkan Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi", **Ankara Barosu Dergisi**, s.2015/1, s.62.
[197]Yargıtay Ceza Genel Kurulu E. 2017/16-956 K. 2017/370 T. 26.9.2017 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019); Yargıtay 16. Ceza Dairesi E. 2017/1443 K. 2017/4758 T. 14.7.2017 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

bilgisayarlarda, bilgisayar programları ve kütüklerinde hakkında uygulanabileceği ve ayrıca kovuşturma aşamasında ilgili tedbirlere başvurmakta hukuki bir yarar bulunmadığını belirterek, bizim de katıldığımız görüşe göre, arama tedbirine sadece soruşturma aşamasında başvurulabileceğini savunmaktadırlar[198]. Nitekim akış halindeki verilerden delil elde edilmesine yönelik düzenlenen CMK m.135'in lafzında *"bir suç dolayısıyla yapılan soruşturma ve kovuşturmada"* ifadesine yer verilirken, CMK m.134'te sadece "*bir suç dolayısıyla yapılan soruşturmada"* ifadesi kullanılmaktadır[199].

Ayrıca, tedbire başvurulabilmesi için başka surette delil elde edebilme imkanının olmaması gerekmektedir. CMK m.170 ve m.175 hükümleri göre, soruşturma evresi sonunda toplanan delillerin, suçun işlendiği hususunda yeterli şüphe oluşturması durumunda savcı tarafından iddianame hazırlanmakta ve bu iddianamenin kabul edilmesi ile birlikte kovuşturma başlamaktadır. Dolayısıyla, savunduğumuz görüşe göre bir suç şüphesinden dolayı açılan soruşturmada yeterli şüphe oluşturacak delil toplanmadan kovuşturma aşamasına geçilemeyecek, kovuşturma aşamasına geçildiğinde ise deliller toplanmış olduğu için CMK m.134 kapsamında düzenlenen arama tedbirine başvurulamayacaktır.

2. Başka Surette Delil Elde Etme İmkanının Bulunmaması

Koruma tedbirleri, yukarıda açıkladığımız gibi ölçülülük ilkesine uygun olarak düzenlenmeli ve uygulanmalıdır. Ölçülülük ilkesi gereğince ise delil elde etmek amacıyla başvurulan koruma tedbirlerinden temel hak ve özgürlüklere en az müdahale teşkil edenlere öncelikle başvurulmalıdır[200]. İkincillik ilkesi olarak adlandırılan bu ilke, Kanun Koyucu tarafından bilgisayarlarda, bilgisayar programları ve kütüklerinde arama tedbirini düzenlenirken dikkate alınmış ve CMK m.134'e *"başka surette delil*

---

[198]Özen/Baştürk, **a.g.e.**, s.144; Ölmez, **a.g.e.**, s.48; Leyla Keser Berber, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma", **Hukuk Merceği, Konferanslar ve Paneller, 25 Nisan 2008 – 24 Temmuz 2008**, Ankara: Ankara Barosu Yayınları, 2010, s.471; Yenisey/Nuhoğlu, **a.g.e.**, s.427; Centel/Zafer, **a.g.e.**, s.459.

[199]Ünver ve Hakeri kovuşturma aşamasında arama, kopyalama ve elkoyma tedbirlerinin uygulanmasının kanunilik ilkesine aykırılık teşkil edeceğini belirterek, böyle bir durum için kanuni düzenlemeye ihtiyaç olduğunu ifade etmektedir. Bkn. Ünver/Hakeri, **a.g.e.**, s.412.

[200]Ünal, **a.g.e.**, s.102; Özen/Baştürk**, a.g.e.**, s.148; Değirmenci, **a.g.e.**, s.343.

elde etme imkanının bulunmaması halinde" ifadesi eklenmiştir. Dolayısıyla, CMK m.134'te düzenlenen arama tedbiri *ultima ratio* bir koruma tedbiridir.

CMK kapsamında, m.134'te düzenlenen "*bilgisayarlarda, bilgisayar programları ve kütüklerinde arama, kopyalama ve elkoyma*", m.135'te düzenlenen "*iletişimin tespiti, dinlenmesi ve kayda alınması*", m.139'da düzenlenen *"gizli soruşturmacı görevlendirilmesi"* ve m.140'da düzenlenen *"teknik araçlarla izleme"* koruma tedbirlerinin uygulanabilmesi için, başka bir surette delil elde etme imkanının bulunmaması gereklidir. CMK'da başka surette delil elde etme imkanının bulunmaması durumu tanımlanmamış ve açıklanmamıştır. Bununla birlikte, iletişimin tespiti ile ilgili Adalet Bakanlığı tarafından çıkarılan ve Danıştay tarafından iptal edilen yönetmelikte bu durum, *"soruşturma veya kovuşturma sırasında diğer tedbirlere başvurulmuş olsa bile sonuç alınamayacağı hususunda bir beklentinin varlığı veya başka yöntemlerden biri veya birkaçının uygulanmasına rağmen delil elde edilememesi ve delillere ancak bu yönetmelikte düzenlenen tedbirlerle ulaşılabilecek olması"* olarak tanımlanmıştı. Bu tanım öğretide Şen tarafından eleştirilmiş, "*diğer tedbirlere başvurulmuş olsa bile sonuç alınamayacağı hususunda bir beklentinin varlığı"* ifadesinin Kanun Koyucunun iradesinin dışına çıktığı belirtilerek, ilgili tanım hukuka aykırı bulunmuştur[201].

İletişimin denetlenmesi koruma tedbiri açısından *"başka surette delil elde etme imkanının bulunmaması"* ifadesini değerlendiren Kaymaz ise, hükmü dar yorumlamakta ve dolayısıyla başka bir surette delil elde imkanının bulunmaması durumu oluşabilmesi için öncelikle diğer soruşturma yöntemlerine başvurulması gerektiğini savunmaktadır[202]. Dolayısıyla, bu görüşe göre iletişimin denetlenmesi tedbirinde olduğu gibi, CMK m.134'te düzenlenen arama tedbirine başvurulabilmesi için ancak diğer soruşturma yöntemlerin uygulanıp, bu yöntemlerle delil elde imkanının olmadığının anlaşılması gerekmektedir. Fakat Değirmenci, diğer yöntemlere başvurulduğu taktirde şüphelinin bilişim sistemlerinde depolanan delilleri

[201]Ersan Şen, **Teknik Araçlarla İzleme**, 23.12.2016 (http://www.haber7.com/yazarlar/prof-dr-ersan-sen/2237114-teknik-araclarla-izleme) (Erişim Tarihi: 31.08.2019).
[202]Seydi Kaymaz, "Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesinin Bir Koşulu Olarak Başka Surette Delil Elde Etme İmkanının Bulunmaması", **Fasikül Aylık Hukuk Dergisi**, Y.2, S.3, Şubat 2010, s.42.

yok edebileceği ihtimalini ortaya koyarak bu görüşü eleştirmektedir[203]. Benzer bir şekilde Karagülmez bilişim suçlarında öncelikle elektronik delillerin toplanması gerektiğini ve diğer delillerin ancak yan delil olabileceğini göz önüne alarak, kanunda sadece bilişim suçları açısından makul şüphenin varlığı durumunda "*ultima ratio"* ilkesine bir istisna getirilmesini gerektiğini savunmuştur[204].

Öğretideki bir görüş, soruşturma aşamasında bazı delillerin elde edilmesi fakat bu delillerin iddia edilen suçun ispatı için yeterli olmaması durumunda, bilgisayarlarda, bilgisayar programları ve kütüklerinde arama tedbirine başvurulması gerektiğini savunmakta ve bu durumda "*ultima ratio*" ilkesinin uygulanmaması gerektiğini belirtmektedir[205]. Maddi gerçeğe hukuka uygun ve kişi hak ve özgürlüklerine saygılı bir şekilde ulaşılması gerektiği ve dolayısıyla her ne pahasına olursa olsun delillerin toplanılmasının hukuka uygun olmadığı göz önüne alındığında bu görüşe katılamamaktayız.

Bir başka görüş iptal edilen Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı Ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelikte yer alan *"başka surette delil elde etme imkanının bulunmaması durumu"* tanımının CMK m.134 bakımından uygulanması gerektiğini ve diğer soruşturma yöntemleri ile delil elde etmenin olanaksız olduğunun kuvvetle öngörülmesi durumunda bilişim sistemlerinde arama tedbirinin uygulanabileceğini savunmaktadır. Buna göre, Cumhuriyet savcısı tarafından *ex ante* bir değerlendirme yapılacak ve bu değerlendirmenin sonunda diğer soruşturma yöntemleriyle delil elde edilemeyeceğine yönelik kuvvetli bir öngörüde bulunulabiliyorsa, CMK m.134'te düzenlenen arama tedbirine başvurulabilecektir. Fakat, böyle bir öngörünün makul sebeplere dayanması gerekecektir, aksi taktirde uygulanan arama tedbiri hukuka aykırı olacaktır[206].

---

[203]Değirmenci, **a.g.e.**, s.343.
[204]Karagülmez, **a.g.e.**, s.267.
[205]İsmail Malkoç/Mert Yüksektepe, **Açıklamalar ve Yorumlarıyla 5271 sayılı Yeni Ceza Muhakemesi Kanunu, C.1**, Ankara: Malkoç Kitabevi, 2008, s.639-640.
[206]Ünal, **a.g.e.**, s.103; Değirmenci, **a.g.e.**, s.343.

Bizim görüşümüze göre ise, CMK m.134 kapsamında arama tedbirinin uygulanabilmesi için, Cumhuriyet savcılarına başka bir soruşturma yöntemiyle delil elde edilip edilmeyeceğine dair ön inceleme yetkisi vermek hem kanunun lafzı ile çelişecek hem de temel hak ve özgürlüklere yapılacak ihlallerin önünü açacaktır. Nitekim, uygulamaya bakıldığında başka bir surette delil elde edebilme olanakları araştırılmadan kanuna aykırı olarak bilişim sistemlerinde arama kararlarının verildiği ve bu suretle Anayasa'da koruma altına alınan temel hak ve özgürlüklerin ihlal edildiği görülmektedir[207]. Dolayısıyla, CMK m.134 kapsamında düzenlenen tedbirlere başvurulması için öncelikle diğer tedbirlerin uygulanmış ve delil elde edilememiş olması gerekmektedir. Ancak, sanal ortamda işlenen suçlarda delillerin genellikle bilişim sistemlerinde bulunması, diğer koruma tedbirleri ile delil elde etmenin neredeyse imkânsız olması ve bilişim sistemlerinde bulunan delillerin kolayca tahrip edilebilir olmaları dikkate alınarak, bu suçlar açısından kanuna bir istisna getirilmesi daha isabetli olacaktır.

3. Somut Delillere Dayanan Kuvvetli Şüphenin Varlığı

5271 sayılı Ceza Muhakemesi Kanunu'nun yürürlüğe giren ilk halinde bilgisayarlarda, bilgisayar programları ve kütüklerinde arama tedbirine başvurmak için gereken şüphe ile ilgili herhangi bir hüküm bulunmamaktaydı. 21.04.2014 tarihinde kabul edilen 6526 sayılı Kanun ile CMK kapsamında düzenlenen koruma tedbirlerinin uygulanabilmesi için aranan şüphe dereceleri ile ilgili değişiklikler yapılmış ve m.134'ün 1. fıkrasına "somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı" ifadesi eklenmiştir. Kanunun genel gerekçesine göre, bu değişikliklerle Avrupa İnsan Hakları Sözleşmesi ve Anayasa'da yer alan temel hak ve özgürlükleri ve bilhassa adil yargılanma hakkının güvence altına alınması ve koruma tedbirlerinden beklenen yarar ile verilmesi muhtemel zararlar arasında ölçülülük ilkesine göre makul bir dengenin kurulması amaçlanmıştır[208].

---

[207]Değirmenci, **a.g.e.**, s.346.

[208]**5271 Sayılı Ceza Muhakemesi Kanununda ve Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun Teklifi ve Adalet Komisyonu Raporu**, s.6 https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss560.pdf (Erişim Tarihi: 28.05.2018)

6526 sayılı Kanun için hazırlanan Adalet Komisyonu Raporunda, somut delillerin ancak suçla ilgili olabileceği dolayısıyla delillere dayanma şartının söz konusu koruma tedbirleriyle bağdaşmadığı ifade edilmiştir. Bu sebeple, rapora göre koruma tedbirlerine bakımından suçun işlendiğine dair kuvvetli şüphe yeterli olacaktır[209].

Öğretide ise somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı, şüphenin hala devam etmekle birlikte neredeyse en güçlü halinde olduğu, gerçeklik ve doğruluk payının en yüksek olduğu, durum olarak ifade edilmektedir. Dolayısıyla, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı, makul şüphe ya da kuvvetli şüphe gibi bir şüphe derecesidir. Bununla birlikte, sonucun gerçek çıkma ihtimali diğer şüphe derecelerine göre daha yüksektir ve bu şüphenin farazi hükümlere değil, somut ve gerçek vakalara dayanması gerekmektedir[210].

Ayrıca, öğretide hem şüphelinin soruşturma konusu suçu işlediğine hem de bilişim sistemleri üzerinde arama tedbiri uygulandığında suça ilişkin delillerin bulunacağına dair somut delillere dayanan kuvvetli şüphenin varlığının bulunması gerektiği ifade edilmektedir[211]. Aksi taktirde, yani sadece şüphelinin suçu işlediğine dair somut delillere dayanan kuvvetli şüphenin varlığının bulunması halinde, bilişim sistemlerinde arama yapılması durumunda bilişim sistemlerinde saklanan ve bahsi geçen suç ile ilişkili olmayan kişisel dosyalarda arama yapılacak ve bunun sonucunda başta özel hayatın gizliliği olmak üzere temel hak ve özgürlükler ihlal edilecektir.

Son olarak, arama tedbire başvurulabilmesi için kanunda belirtilen "başka surette delil elde imkanının bulunmaması" ve "somut delillere dayanan kuvvetli şüphenin varlığı" şartları beraber değerlendirildiğinde, Kanun Kuyucu'nun temel hak ve özgürlüklere müdahale ağır müdahale teşkil eden bu koruma tedbirini, sıkı koşullara bağlayarak ölçülülük ilkesine uygun bir hüküm tesis ettiğini söylemek mümkündür.

---

[209]**5271 Sayılı Ceza Muhakemesi Kanununda ve Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun Teklifi ve Adalet Komisyonu Raporu**, s.29 https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss560.pdf (Erişim Tarihi: 28.05.2018)

[210]İlyas Şahin, "Türk Ceza Yargılaması Hukukunda Koruma Tedbirleri Bakımından Esas Alınan Şüphe Kavramının İncelenmesi", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C.20, S.3, 2014, s.120-121.

[211]Değirmenci**, a.g.e.**, s.352-353.

4. Hâkim ya da Gecikmesinde Sakınca Bulunan Hâllerde Cumhuriyet Savcısı Kararının Bulunması

CMK m.134'e göre bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama tedbirinin uygulanabilmesi için, hâkim ya da gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı kararının bulunması gerekmektedir. Arama kararında, CMK m.134 dayanak gösterilerek bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama tedbirinin gerçekleştirileceği belirtilmelidir. Nitekim Yargıtay, 6 Mayıs 2015 tarihli kararında genel arama kararı ile bilgisayar ve CD'lerde arama yapılmasını hukuka aykırı bulmuş, bu arama sonucu elde edilen delilleri hukuka aykırı delil olarak nitelendirmiş ve bu delillerin hükme esas teşkil edemeyeceğini belirtmiştir[212].

Tedbire sadece soruşturma aşamasında başvurulabileceği göz önüne alındığında, arama kararını vermeye yetkili hâkim sulh ceza hâkimidir. Nitekim, bu husus maddenin gerekçesinde *"karar, soruşturma evresinde sulh ceza hâkimi tarafından gizli olarak verilecektir"* denilerek ifade edilmiştir.

25 Temmuz 2018 tarihinde ise Türk Kanun Koyucu ilgili hükümde değişikliğe giderek arama, kopyalama ve elkoyma kararlarını verme yetkisini gecikmesinde sakınca bulunan hallerde savcıya vermiştir[213]. Bu değişiklik öncesinde gecikmesinde

---

[212]Yargıtay 19. Ceza Dairesi E. 2015/2092 K. 2015/1175 T. 6.5.2015 *"Sanık tarafından işletilen iki ayrı işyerinde arama yapılmasına karar verilmesine karşın, aynı işyerinde bulunan bilgisayarlar üzerinde arama yapılabilmesine olanak tanıyan hükümlere göre verilmiş bir arama kararı bulunmadığı anlaşılmakla, işyerinde bulunan bilgisayarlar üzerinde yapılan arama sonucunda elkonulan ve içerisinde müşteki firmaya ait lisanssız yazılımların olduğu belirtilen harddiskler ve CD'ler hukuka aykırı delil niteliğinde olup hükme esas alınamayacağından, sanık hakkında verilen beraat kararı yasaya uygundur."* (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

[213]Bu değişiklik öncesinde ilgili hükümde 27.07.2016 tarihli ve 668 sayılı KHK ile OHAL süresince geçerli olmak üzere hüküm eklenmiş ve TCK İkinci Kitap Dördüncü Kısım Dördüncü, Beşinci, Altıncı ve Yedinci Bölümde tanımlanan suçlar, Terörle Mücadele Kanunu kapsamına giren suçlar ve toplu işlenen suçlar bakımından bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirlerinin savcılık kararı ile gerçekleştirilebileceği, bu kararın beş gün içerisinde hakimin onayına sunulması gerektiği ve ilgili kararın hakim tarafından tedbirin gerçekleştirilmesinden itibaren on gün içerisinde açıklanacağı belirtilmiştir. Bakınız Bahri Öztürk/Durmuş Tezcan/Mustafa Ruhan Erdem/Özge Sırma Gezer/Yasemin F. Saygılar Kırıt/Esra Alan Akcan/Özdem Özaydın/Efser Erden Tütüncü, **Nazari ve Uygulamalı Ceza Muhakemesi Hukuku**, Güncellenmiş 11. Baskı, Ankara: Seçkin, 2017, s.518-519.

sakınca bulunan hallerde Cumhuriyet savcısının veya savcıya ulaşılamayan hallerde kolluk amirinin yazılı emriyle bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama tedbirinin uygulanması mümkün değildi. Nitekim, Yargıtay 15 Şubat 2017 tarihli kararında Cumhuriyet savcısının talimatıyla şüphelinin cep telefonunda arama yapılmasını hukuka aykırı bulmuş ve CMK m.134 hükümlerine dayanan bir hâkim kararı olmadıkça böyle bir aramanın yapılamayacağını açıkça ifade etmişti[214].

Değişiklik öncesinde, arama tedbirine sadece hâkim tarafından karar verilebilmesi, başka surette delil elde edilme imkanının bulunmaması ve somut delillere dayanan kuvvetli şüphenin varlığı şartları gibi temel hak ve özgürlüklerin korunması açısından bir güvence oluşturduğu öğretide ifade edilmekteydi[215]. Değişiklik ile beraber hükme *"Cumhuriyet savcısı tarafından verilen kararlar yirmi dört saat içinde hâkim onayına sunulur. Hâkim kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde çıkarılan kopyalar ve çözümü yapılan metinler derhâl imha edilir."* ifadesi eklenmiş olsa da bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama tedbiri ile ihlal edilen temel hak ve özgürlükler dikkate alındığında, Cumhuriyet savcısı tarafından verilen karar ile arama tedbirine başvurulmasına olanak sağlayan bu eklemeyi olumsuz bir gelişme olarak değerlendiriyoruz.

CMK m.163'te suçüstü halleri ile gecikmesinde sakınca bulunan hallerde soruşturma işlemlerinin sulh ceza hâkimi tarafından yürütülebileceği belirtilmektedir. CMK m.134 kapsamında arama kararının sulh ceza hâkimi tarafından Cumhuriyet savcısı sıfatıyla talep edilmesi durumunda, aynı sulh ceza hâkimi arama kararına hükmedemeyecektir, bunun yerine arama kararı bir başka sulh ceza hâkimi tarafından verilmesi gerekecektir. Aksi durum, hâkimin tarafsızlığa tarafsızlığına gölge düşürecektir[216].

---

[214]Yargıtay 17. Ceza Dairesi E. 2015/27517 K. 2017/1716 T. 15.2.2017 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).
[215]Ünal, **a.g.e.**, s.105; Değirmenci, **a.g.e.**, s.353.
[216]Ünal, **a.g.e.**, s.106.

Arama kararında hangi hükümlerin bulunacağına dair CMK m.134 kapsamında bir düzenleme bulunmamaktadır. Dolayısıyla, bu konuda genel arama tedbiri için arama kararını düzenleyen CMK m.119/2'ye başvurulacaktır[217]. Bu hükme göre arama kararında, "Aramanın nedenini oluşturan fiil", "aranılacak kişi, aramanın yapılacağı konut veya diğer yerin adresi ya da eşya" ile "karar veya emrin geçerli olacağı zaman süresi" açıkça gösterilmelidir. Bu hüküm bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama tedbiri için uygulandığı taktirde, arama kararında aramanın nedenini oluşturan fiil, aranılacak bilişim sistemi ve kararın geçerli olacağı zaman süresi belirtilmek zorundadır. Öğretide bunlara ek olarak, şüphelinin açık kimliğinin, bilişim sistemlerinde arama yapacak kişilerin kimliklerinin, koruma tedbirinin uygulanması bakımından somut delillere dayanan kuvvetli şüphe sebeplerinin, başka surette delil elde edilememesinin neden mümkün olmadığının ve bilişim sisteminin şüpheliye ait olmadığı durumlar için bilişim sisteminin şüphelinin kullanımında olduğu kanaatini uyandıran sebeplerin arama kararında açıkça belirtilmesi gerektiği ifade edilmektedir[218].

Bilişim sistemlerinde arama kararları ve bu kararların kolluk kuvvetleri tarafından uygulanması ile ilgili en önemli sorunlardan biri, arama kararlarının bütün bilişim sistemlerini kapsayacak şekilde verilmesi ve bunun sonucunda arama faaliyetinin bütün bilişim sistemleri üzerinde uygulanmasıdır. Öğretide bu durum eleştirilmiş ve arama kararında hangi bilişim sistemlerinde arama yapılacağının açıkça belirtilmemesinin hukuka aykırı olacağı ifade edilmiştir[219]. Dolayısıyla bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kararında şüphelinin kullanımında bulunan ve arama yapılacak bilişim sistemleri, çıkarılabilir donanımlar ve uzak bilgisayar kütükleri belirtilmelidir.

Sayısal delil olabilecek veriler, bu verilerin depolandığı bilişim sistemi ve kütükler bilinebiliyorsa arama kararında sadece bu cihazlar ve kütükler sınırlı olarak ifade edilmelidir. Bununla birlikte aranan delil olabilecek verilerin neler olduğu ve

---

[217]Değirmenci, **a.g.e.**, s.353.
[218]Malkoç/Yüksektepe, **a.g.e.**, s. 640; Değirmenci, **a.g.e.**, s.354; Ünal, **a.g.e.**, s.105; Yenisey/Nuhoğlu, **a.g.e.**, s.427.
[219]Değirmenci, **a.g.e.**, s.354.

nerede depolandığı bilinemiyorsa bilişim sistemlerinin, çıkarılabilir donanımların ve uzak bilgisayar kütüklerinin tamamında ya da bir kısmında arama yapılabileceğine dair arama kararı verilebilir[220]. Fakat, soruşturulan suç ile arama yapılacak bilişim sistemi arasında arama kararında illiyet bağının kurulması gerektiği ve sadece söz konusu suç ile ilgili delilleri barındırabilecek bilişim sistemleri, çıkarılabilir donanımlar ve uzak bilgisayar kütüklerinde arama yapılabileceği unutulmamalıdır[221]. İlliyet bağı kurulmadan şüphelinin kullanımında olan bütün bilişim sistemlerinde arama yapılmasına karar verilmesi durumunda ölçülülük ilkesi ihlal edilecek ve bu durum başta özel hayatın gizliliği ve kişisel verilerin korunması olmak üzere temel hak ve özgürlüklere orantısız bir müdahale teşkil edecektir[222]. Nitekim AİHM Petri Sallinen ve Diğerleri/Finlandiya kararında arama gerçekleştirilen yerdeki bütün depolama birimlerinde arama gerçekleştirilmesi ve bunlara elkonulmasını AİHS m.8 kapsamında koruma altına alınan özel hayatın gizliliğini ihlal ettiği yönünde karar vermiştir[223].

D. Tedbirin Uygulanması

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirleri CMK m.134'te terditli olarak düzenlenmiştir. Buna göre, öncelikle şüphelinin kullanımında olan bilişim sistemlerinde arama yapılacak, arama sonucu elde edilen verilerin kopyaları çıkarılacak ve bu veriler metin haline getirilecektir. Şayet bilişim sistemlerinde gizli dosyalara ulaşılamaz ya da bilişim sistemlerine şifrelerin çözülememesi sonucu arama yapılamazsa, bilişim sistemlerine elkonulacak ve elkonulan sistemlerin kopyası çıkarılacaktır.

---

[220]Tanrıkulu, **a.g.e.**, s.395.
[221]Değirmenci, **a.g.e.**, s.354.
[222]Yenisey/Nuhoğlu, **a.g.e.**, s.423.
[223]Petri Sallinen ve diğerleri/Finlandiya, Başvuru Numarası: 50882/99, 27 Eylül 2005 http://hudoc.echr.coe.int/eng?i=001-70283 (Erişim Tarihi: 25.07.2019)

1. Yerinde Arama

CMK m.134 kapsamında düzenlenen arama tedbiri, esas olarak bilişim sistemlerinin bulunduğu yerde başka bir ifadeyle yerinde yapılacak şekilde düzenlenmiştir[224]. Dolayısıyla kolluk kuvvetleri, CMK m.119/4'e göre bilişim sistemlerinin bulunduğu konut ya da işyerinde bilişim sistemlerinde arama tedbirini gerçekleştirecektir. Askeri mahallerde bulunan bilişim sistemlerinde arama tedbiri ise CMK m.119/5'e göre Cumhuriyet savcısının istem ve katılımıyla askerî makamlar tarafından yerine getirilecektir.

Arama tedbirinin uygulanacağı zaman ile ilgili CMK m.134'te bir hüküm bulunmamaktadır. Dolayısıyla, arama zamanı ile ilgili genel arama hükümlerine başvurulacaktır. CMK m.118'de konutta, işyerinde veya diğer kapalı yerlerde gece vaktinde arama yapılamayacağı belirtilmiştir. AÖAY m.31'de ise konutta, işyerinde veya diğer kapalı yerlerde gece vaktinde arama yapılamayacağı tekrar edilmiş, aramanın arama kararında belirtilen süreler içerisinde ve gündüz yapılacağı ifade edilmiştir.

Gece vakti kavramı, TCK m.6'da *"güneşin batmasından bir saat sonra başlayan ve doğmasından bir saat evvele kadar devam eden zaman süresi"* olarak tanımlanmıştır. Bu hükümlere göre bilişim sistemlerinde arama kararı ancak güneş doğmadan bir saat öncesi ile güneş batımından bir saat sonrası arasında uygulanabilecektir. Bununla birlikte gündüz başlayan aramanın gece bitirilmesine bir engel bulunmamaktadır[225].

Aramanın gerçekleştirilmesi sırasında aramada hazır bulunabilecekler konusunda CMK m.134'te bir düzenleme olmadığı için genel hükümlere başvurulacak ve CMK m.120'ye göre, aranılan bilişim sisteminin sahibi veya zilyedi, bunların bulunmaması durumunda ise bu kişinin temsilcisi, hasımlarından biri, beraber oturmakta olduğu bir kişi ya da bir komşusu arama sırasında hazır bulunacaktır. Bu

[224]Özge Sırma, "Güncel Olaylar Çerçevesinde 5271 Sayılı Ceza Muhakemesi Kanununda Arama", **Terazi Hukuk Dergisi**, S.34, 2009, s.37.
[225]Tanrıkulu, **a.g.e,** s.431; Aksoy, **a.g.e.**, s.100.

kişilere aramaya başlamadan önce arama kararı hakkında bilgilendirilme yapılması gerekmektedir. Bilgilendirme yapılmazsa ya da eksik yapılırsa arama hukuka aykırı hale gelecektir[226]. Yine aynı kanun maddesine göre, bilişim sisteminin sahibi ya da zilyedinin avukatı da arama esnasında hazır bulunabilecektir.

Arama kararının uygulanmasında nasıl bir yöntem uygulanacağı ve bu yöntemler kullanılırken hangi cihaz ve programlardan yararlanılacağı ilgili arama kararından elde edilen bilgilerden yararlanılarak önceden tespit edilmelidir[227]. Örneğin, bilgisayarlarda ve akıllı telefonlarda arama yapmak için kullanılan cihazlar ve programlar farklıdır ve bu cihazlarda arama yapılmasında kullanılan yöntemler de farklılaşmaktadır. Dolayısıyla, arama kararında şüphelinin akıllı telefonu ve bilgisayarında arama yapılacağı belirtilmişse, kolluk kuvvetleri bu cihazlara uygun teçhizatı (yazmaya karşı koruma cihazları, yedek depolama donanımları, ağ bağlantı kabloları, bilgisayar vb.) ve programları (adli inceleme, yazmaya karşı koruma, imaj alma yazılımları vb.) yanında getirmeli ve arama kararı uygulanmadan bu cihazlarda uygulanacak yöntemler belirlenmelidir.

Arama tedbiri, adli bilişim uzmanı kolluk kuvvetleri tarafından uygulanmalıdır[228]. Aksi taktirde işin uzmanı olmayan kolluk kuvvetlerin yapacakları hatalar, delil niteliğine sahip olabilecek verilerin tahrip olmasına, silinmesi sebep olabilecek ya da verilerin bütünlüğünü bozulabilecektir. Bu durumda, verilerin delil olma niteliği ortadan kalkabilecek ya hukuka aykırı delil haline gelebilecektir[229].

Bilişim sistemlerinde arama tedbiri uygulanırken, öncelikle delillerin bozulmasını ya da değiştirilmesini önlemek amacıyla, olay yerinin güvenliği sağlanmalıdır. Olay yerine giriş ve çıkışlar kontrol altına alınmalı, giren ve çıkan

---

[226]Sırma, **a.g.e.**, s.36.
[227]Değirmenci, **a.g.e.**, s.361.
[228]Türkay Henkoğlu, **Adli Bilişim**, İstanbul: Pusula, 2014, s.19.
[229]Mustafa İlker Öztürk, **Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesine İlişkin Akış Modelleri**, Yayımlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, Ankara, 2007, s.69.

kişilerin kaydı tutulmalı ve dışarı çıkan kişilerin üzerlerinde herhangi bir bilişim cihazı bulunmadığından emin olunmalıdır[230].

Arama işlemlerine başlamadan önce, bilişim sistemlerinin ve bilişim sisteminin bulunduğu ortamın ayrıntılı fotoğrafları çekilmelidir[231]. Arama yapılacak yerde bulunan ve arama kararında belirtilen bilişim sistemler ve çıkarılabilir donanımlar, örneğin CD, DVD ve taşınabilir bellekler tespit edilmeli ve bunlar kolluk kuvvetlerince muhafaza altına alınmalıdır[232]. Muhafaza altına alınan bütün bilişim sistemleri ve çıkarılabilir donanımlar etiketlenmeli ve etiketlerde yeterli açıklayıcı bilgiler bulunmalıdır. Ayrıca, muhafaza altına alınan cihazların envanter listesi oluşturulmalı ve bütün cihazlar seri numaraları ile birlikte kaydedilmelidir[233].

Arama kararını gerçekleştirecek adli bilişim uzmanları, arama tedbirini uygulamaya geçmeden önce, bilişim sistemlerinde yer alan ve çalıştığında sistemdeki verileri yok edebilen tuzak programları gibi programlara dikkat etmeli ve bilişim sistemlerinin uzaktan kontrol edilmediğinden emin olmalıdırlar. Aksi taktirde, bilişim sistemlerinde depolanan veriler silinebilecek, tahrip edilebilecek veya değişikliğe uğrayabilecektir[234].

Bilişim sistemlerinde depolanan verilerin bütünlüğünü korumak ve değişikliğe uğramalarını engellemek için yazma engelleme donanımları kullanılmalı ya da yazma engelleme yazılımları kurulmalıdır. Bu sayede, arama kararının uygulanması sırasında yapılacak işlemler, sistemlerde depolanan verilerde değişiklik yapamayacaktır[235]. Ayrıca, yazma engelleme sistemleri kurulmadan önce, bilişim sistemlerinde herhangi bir program çalıştırılmamalıdır[236].

---

[230]Henkoğlu, **a.g.e.**, s.19
[231]Henkoğlu, **a.g.e.**, s.20
[232]Öztürk, **a.g.e.**, s.69.
[233]Henkoğlu, **a.g.e.**, s.20.
[234]Değirmenci, **a.g.e.**, s.361.
[235]Değirmenci, **a.g.e.**, s.361.
[236]Cem Günal, "Adli Bilişim ve Delillerin Toplanması", **Özyeğin Üniversitesi Hukuk Fakültesi Bilişim Hukuku Sertifika Programı Sunumu**, 18 Şubat-11 Mart 2012, İstanbul; aktaran Dülger, **a.g.e.**, s.708.

Adli bilişim uzmanları, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama tedbirini basitten karmaşığa doğru farklı teknik ve yöntemler kullanarak gerçekleştireceklerdir. Tedbir uygulanırken, bilgisayar kütüklerinde kelime araması yapılacak, yazılımlar vasıtası ile hafıza birimleri ve çıkarılabilir donanımlar bütünüyle taranacak, silinmiş dosyalar kurtarılacak, gizlenmiş dosyalar ve bilgiler açığa çıkartılacak, içeriği ve uzantısı uyuşmayan dosyalar belirlenecek, sistemlerdeki kötü amaçlı yazılımlara dair bilgiler tespit edilecektir[237]. Arama işlemine çalışır haldeki bilişim sistemlerinde verilerin geçici olarak depolandığı RAM, önbellek ya da yazıcı önbelleği gibi birimlerden başlanmalı ve birimlerin kopyaları çıkartılmalıdır[238]. Arama sonucunda elde edilen verilerin kopyası çıkartılacak ve bu veriler çözülerek metin haline getirilecektir.

Elde edilen verilerin incelenmesi ve analiz edilmesi uzun süreler almakta günlerce hatta aylarca sürebilmektedir ve yerinde bu inceleme ve analizlerin yapılması mümkün değildir[239]. Bu sebeple, öğretide arama tedbirinin amacının soruşturulan suç ile ilgili bütün verilere ulaşmak ve bu verilerin CMK m.134/5 kapsamında birebir kopyasının çıkartılması olduğu ifade edilmektedir[240]. Uygulamada birebir kopya alma işleminin doğru bir şekilde gerçekleştirildiğinden emin olmak işlem özetleme işlemi (hashing) kullanılmaktadır. Verileri bir fonksiyona sokularak sayı ve harflerden oluşan belli sayıda karakterlere indirgendiği özetleme işlemi, tezimiz kapsamında bilgisayarlarda, bilgisayar programlarında ve kütüklerinde kopyalama başlığında açıklanacaktır[241].

Arama kararı, bilişim sistemleri şüphelide kalacak şekilde uygulanmalıdır. Kanun Koyucu, elkoyma tedbirinin ancak bilişim sistemlerinde gizlenmiş bilgilere ulaşılamaması veya bilişim sistemlerinin şifrelerinin çözülememesinden dolayı girilememesi ya da arama işleminin uzun sürmesi durumunda uygulanacağını kanunda öngörmüştür. Arama tedbirinin uygulanması sonucunda elde edilen delil niteliğindeki

---

[237]Değirmenci, **a.g.e.**, s.361.
[238]Henkoğlu, **a.g.e.**, s.24.
[239]Kimberly Nakamaru, "Mining for Manny: Electronic Search and Seizure in the Aftermath of United States v. Comprehensive Drug Testing", **Loyola of Los Angeles Law Review**, V.44, 2011, s.785.
[240]Değirmenci, **a.g.e.**, s.362.
[241]Bakınız s. 82-84.

verilerin kopyası çıkartılması yeterli olacak ve böyle bir durumda bilişim sistemlerine elkonulmayacaktır[242]. 2018 yılında yapılan değişiklik öncesinde arama için yeterli sürenin olmaması ya da teknik ve personel eksikliği sebeplerine dayanılarak uygulamada bilişim sistemlerine elkonulduğu görülmekteydi. Kanuni bir dayanağı olmayan ve öğretide çok eleştirilen bu durum Kanun Koyucu tarafından dikkate alınarak CMK m.134/2'ye "*işlemin uzun sürecek olması*" durumunda da bilişim sistemlerine, programlarına ve kütüklerine elkonulabileceğine dair hüküm eklenerek uygulamada halihazırda var olan duruma kanuni dayanak getirmiştir.

Arama kararının uygulanması sırasında yapılan bütün işlemler yazılı olarak kaydedilmelidir. Ayrıca, kayıtlarda işlemleri gerçekleştiren görevliler de belirtilmelidir. Bu sayede, soruşturma ve kovuşturma aşamasında arama işlemlerine karşı yapılan itirazlarda arama kararının hukuka uygun bir şekilde uygulandığı belgelerle gösterilebilecektir. Aynı zamanda bu yazılı kayıtlar, delillerin incelenmesi aşamasında görevlilere kolaylık sağlayacaktır[243].

Bilişim sistemlerinde arama işlemleri tamamlandıktan sonra CMK m.169/2 hükmüne göre arama tutanağı düzenlenecektir. Tutanağa nelerin yazılacağı ise aynı maddenin dördüncü fıkrasında düzenlenmiştir. Buna göre, tutanakta aramanın yapıldığı yer, tarihi, başlama ve bitiş saatleri, aramayı gerçekleştiren kolluk kuvvetleri isimlerinin, aramaya katılan Cumhuriyet savcısının, savcı katılmadıysa ihtiyar heyetinden veya komşulardan aramaya katılanların, bilişim sistemlerinin sahip ya da zilyetlerinin, onlar yoksa bu kişiler yerine hazır bulunanların isimleri yazılacaktır. Fakat, bu duruma ek fıkra ile istisna getirilmiştir. Buna göre, CMK m.169/7'de sayılı suçlarda ilgili bilişim sistemlerinde arama yapıldığında görevlilerin isimleri yerine sadece sicil numaraları yazılacaktır. Arama tutanağında yer alacak hususlarla ilgili AÖAY m.11 kapsamında da hükümler bulunmaktadır. Bu hükümlere göre, kanundaki belirtilen hususlara ek olarak, arama kararının tarih ve sayısı, aramanın konusu, bilişim sistemlerinin arandığı konut ve işyerleri ve eklentilerinin açık adresi, arama sonucu elde edilen verilerle ilgili bilgiler yer alacaktır.

---

[242]Ünal, **a.g.e.**, s.107.
[243]Henkoğlu, **a.g.e.**, s.20.

Ayrıca, arama tutanağında aramayı gerçekleştiren adli kolluk görevlilerinin, Cumhuriyet savcısının, arama kararını veren sulh ceza hakiminin ve aramada hazır bulunduysa zabıt katibinin imzası bulunmak zorundadır. Şayet arama sırasında şüphelinin avukatı hazır bulunmuşsa, CMK m.169/3'e göre avukatın imzası da bulunacaktır. İmzadan imtina halinde, bu durum sebepleri ile birlikte tutanağa geçirilecektir. Yönetmeliğe göre ise, arama esnasında hazır bulunan herkes tutanağa imza atacak ve tutanağın bir sureti şüpheliye teslim edilecektir.

Tutanağa ek olarak, arama kararı ve işlemleri ile ilgili bir belge verileceği CMK m.121/1'de ifade edilmiştir. Şüphelinin istemi üzerine verilen bu belgede şüpheliye verilecek belgede soruşturması yapılan suç niteliğindeki fiile ve arama işlemlerinin CMK m.116, 117 ve 134. maddelerine uygun olarak yapıldığına dair bilgilere yer verilecektir[244]. Yönetmeliğin 12. maddesinde ise, bu bilgilere ek olarak bilişim sistemlerinde aramanın amacına ve arama sonucunda şüpheyi haklı çıkaracak bir veri elde edilmediyse bu duruma belgede yer verileceği belirtilmiştir. Ayrıca, bu belgede, bilişim sistemlerinde arama yapılmasını gerektiren somut delillere dayanan kuvvetli suç şüphesi varlığının ve neden başka suretle delil elde edilebilmesinin mümkün olmadığının belirtilmesi gerekmektedir[245].

2. Uzaktan Arama

Bilişim sistemlerinde arama işlemleri yerinde yapılabileceği gibi uzaktan kontrol edilerek de yapılabilmektedir. Öğretide uzaktan arama olarak adlandırılan bu tedbir, iki farklı şekilde uygulanabilmektedir. Bunlardan ilki, İnternet başta olmak üzere bilişim ağları üzerinden bilişim sistemlerine bağlanarak arama yapılmasıdır. Bu yöntemle bilişim sistemlerinin hafıza birimleri aranabilmekte, elektronik posta trafiğine müdahale edilebilmekte, anlık mesajlaşmalar ve internet gezinti alışkanlıkları gözlenebilmektedir. İkincisi ise, arama yapılacak bilişim sistemine casus yazılım (Truva atı) yerleştirerek sistem üzerinde arama yapılması ve bilişim sistemlerinde depolanan verilerin kopyalarının kolluk kuvvetlerine gönderilmesidir[246].

---

[244]Sırma, **a.g.e.**, s.38; Tanrıkulu, **a.g.e.**, s.419.
[245]Tanrıkulu, **a.g.e.**, s.419.
[246]Abel Wiebke, "Agents, Trojans and Tags: The Next Generation of Investigators", **International Review of Law, Computers and Technology**, Vol.23, 2009, s.100.

Bilişim sistemlerine casus yazılım yüklenerek uzaktan arama yapılması durumunda, bilişim sisteminde durağan halde ya da akış halinde bulunan veriler üzerinde sürekli bir arama yapılmaktadır. Bununla birlikte, Türk hukukunda arama tedbiri, belli bir tarih ve saatte tek seferde uygulanacak bir tedbir olarak düzenlenmiştir. Bu sebeple, casus yazılım yüklenerek uzaktan arama, Türk hukukuna göre arama olarak nitelendirilemeyecektir. Ayrıca, bilişim sistemlerinde arama tedbiri için şüpheliyi bilgilendirme ve belli kişilerin hazır bulunması yükümlülüğü bulunmaktadır fakat casus yazılım yüklenerek uzaktan aramada, bu durumun aksine, şüphelinin ve aramada hazır bulunması gerekenlerin haberi olmamaktadır. Dolayısıyla, CMK m.134 kapsamında casus programlar yerleştirerek uzaktan aramanın faaliyetlerinin gerçekleştirilmesi mümkün değildir ve yapılan arama hukuka aykırı olacaktır[247].

AÖAY m.17/3'te ve AKSSS m.19/2'de yerinde arama yapılan bilişim sistemlerinden ulaşılabilen ve ulusal sınırlar içerisinde bulunan bilgisayar ağları ile diğer bilgisayar uzak kütüklerinde arama yapılabileceği belirtilmiştir. Fakat bu hükümlere göre de bilişim ağları aracılığıyla uzaktan arama gerçekleştirilemeyecektir çünkü bu maddelerde düzenlenen tedbir, kolluk kuvvetlerinin kullandığı bilişim sistemlerinden erişilerek arama yapılan bilişim sistemleri değil, yerinde arama yapılan sistemden bilişim ağları aracılığıyla erişilebilen diğer sistemlerdir.

Son olarak, Polis Vazife ve Salâhiyetleri Kanunu kapsamında polisin adli görev ve yetkilerini düzenleyen Ek Madde 6'yı incelemekte fayda görüyoruz. 2/1/2017 tarihli ve 680 sayılı KHK ile ilgili maddeye bir fıkra eklenmiş ve polise, sanal ortamda işlenen suçlarda, sanal ortamda araştırma yapma yetkisi verilmiştir. Burada düzenlenen yetkinin amacı ilgili kişinin kimlik tespitinin yapılmasıdır ve ilgili araştırma ancak sanal ortamda yürütülebilecektir. Dolayısıyla, bu hükme dayanarak bilişim sistemlerinde uzaktan arama gerçekleştirmek mümkün değildir. Aksi taktirde, kanunilik ve ölçülülük ilkesine aykırı olarak, herhangi bir hâkim veya gecikmesinde

[247]Değirmenci, **a.g.e.**, s.364.

sakınca bulunan hallerde savcı kararı olmadan, kişilerin bilişim sistemlerinde uzaktan arama gerçekleştirilecektir.

II. Bilgisayarlarda, Bilgisayar Programları ve Kütüklerinde Elkoyma

A. Tedbirinin Hukuki Niteliği

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde elkoyma tedbiri, hukukumuzda *"Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde ya da işlemin uzun sürecek olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir."* denilmek suretiyle CMK m.134/2'de düzenlenmiştir.

Koruma tedbirinin düzenleniş amacı, şifre ile koruma altına alınmış bilişim sistemlerine girilerek arama tedbirinin gerçekleştirilmesi ya da arama tedbiri sırasında ulaşılamayan gizlenmiş verilerin çözülerek kopyalanmasıdır. Bilişim sistemlerine kolluk kuvvetlerince elkonulacak, elkonulan bilişim sistemlerinin hafıza birimlerinin kopyaları çıkartılacak ve bu kopyalar üzerinden şifreli veya gizlenmiş dosyalar çözülerek arama işlemleri tamamlanacaktır. Fakat uygulamada elkoyma tedbirinin istisna bir tedbir olduğu dikkate alınmamakta ve elkoyma tedbirinin uygulanması için gereken şartlar dikkate alınmadan kolluk kuvvetleri tarafından bilişim sistemlerine elkonulmaktadır[248].

Bilgisayarlarda, bilgisayar programları ve kütüklerinde elkoyma tedbiri, genel elkoyma tedbirinin özel bir düzenlemesidir. Dolayısıyla, CMK m.134 kapsamında düzenlenmeyen konularda, genel elkoyma tedbiri ile ilgili CMK hükümlerine başvurulacaktır[249]. Örneğin, askeri mahallerde yapılacak elkoyma ile ilgili CMK m.134'te bir hüküm bulunmamaktadır. Dolayısıyla askeri mahallerde bilişim sistemlerine elkoyma kararının kimin tarafından uygulanacağı ile ilgili CMK m.127/6'ya başvurulacaktır.

---

[248]Yener/Hakeri, **a.g.e.**, s.409.
[249]Değirmenci, **a.g.e.**, s.74.

AKSSS kapsamında ise bilişim sistemlerine elkoyma tedbiri m.19/3'te ifade edilmiştir. Buna göre, sözleşmeyi imzalayan tarafların bilişim sistemlerinin tamamına ya da bir kısmına elkoyma, elkonulan bilişim sistemlerindeki verilerin bir kopyasını çıkartarak bunları muhafaza etmeye ve ilgili verilerin bütünlüğünü korumaya yönelik yasama tedbirleri çıkarma yükümlülükleri bulunmaktadır. CMK m.134 kapsamında düzenlenen elkoyma tedbiri incelendiğinde Türk Kanun Koyucunun yukarıda belirtilen sözleşmeden doğan yükümlülüklerini yerine getirdiği söylenebilecektir. Bununla birlikte, AKSSS m.19/3'e göre, tarafların *"erişim sağlanan bilgisayar sistemlerindeki bilgisayar verilerini erişilemez hale getirmeye veya kaldırmaya"* yönelik bir yasama düzenlemesi yapma zorunluluğu bulunmaktadır. Kanunlarımızda arama yapılan bilişim sistemlerinden erişilebilen bilişim sistemlerinde arama yapılmasına yönelik bir düzenleme olmadığı gibi, bu erişim sağlanan bilişim sistemlerindeki verileri erişilemez kılmaya ya da kaldırmaya yönelik bir hüküm de bulunmamaktadır.

Elkoyma tedbiri, başta özel hayatın gizliliğini, konut dokunulmazlığını ve mülkiyet hakkını ihlal eden bir koruma tedbiridir. İhlal ettiği hakların önemine binaen, elkoyma tedbiri ile hükümlere Anayasa m.20 ve m.21 kapsamında yer verilmiştir. Buna göre, milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının haklarının korunması sebebiyle usulüne uygun verilmiş bir hâkim kararıyla ya da gecikmesinde sakınca bulunan hallerde yetkili merciin yazılı emri bulunmadıkça, kimsenin özel kağıtları, eşyaları ile konutunda yer alan eşyalarına elkonulamayacaktır.

Bilişim sistemlerine elkonulması halinde yukarıda izah edildiği üzere anayasada güvence altına alınan hak ve özgürlükler ihlal edilecektir. Bu durumu dikkate alan Türk Kanun Koyucu hem kanunilik hem de ölçülülük ilkelerin gereği olarak CMK 123 ve 127. maddeleri arasında düzenlenen genel elkoyma tedbirinden farklı bir koruma tedbiri düzenleme ihtiyacı duymuş ve bu doğrultuda CMK

m.134/2'de bilişim sistemlerinde uygulanmak üzere özel bir elkoyma tedbiri düzenlemiştir[250].

B. Tedbirin Kapsamı

CMK m.134'te elkoyma tedbirinin uygulanacağı kişiler ya da cihazlar bakımından arama tedbirinden ayrı bir düzenleme yer almamaktadır. Dolayısıyla tedbirinin uygulanacağı kişiler ve cihazlar bakımından tezimizin bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kısmına bakılması gerekmektedir[251].

C. Tedbirin Şartları

1. Arama Tedbirinin Uygulanmış Olması

Bilişim sistemlerinde elkoyma tedbirinin uygulanabilmesi için, arama tedbiri bir önkoşuldur. Bu sebeple, arama tedbirinin uygulanması için gereken suç soruşturmasının varlığı, başka surette delil etme olanağının bulunmaması, somut delillere dayanan kuvvetli şüphenin varlığı ve cumhuriyet savcısının isteği üzerine hâkim kararının bulunması koşulları elkoyma tedbiri için de gerekecektir.

Hâkim kararı ile ilgili öğretide, genel arama ve elkoyma tedbirlerinde olduğu gibi bilgisayarlarda, bilgisayar programları ve kütüklerinde arama kararının elkoyma kararını da kapsaması gerektiği ileri sürülmüştür[252]. Bununla birlikte, bizim de katıldığımız hâkim görüş arama, kopyalama ve elkoyma tedbirlerinin farklı tedbirler olduğu ve dolayısıyla hâkim tarafından verilen kararda bu tedbirlerin ayrı ayrı belirtilmesi gerektiği yönündedir[253].

---

[250]Ünal, **a.g.e**., s.84.
[251]Bakınız s.42-53.
[252]Ünal, **a.g.e.**, s.106.
[253]Vahit Bıçak, **Suç Muhakemesi Hukuku**, Ankara, Seçkin Yayınevi, 2010, s. 584; Değirmenci, **a.g.e.**, s.355.

2. Bilişim Sistemlerine, Programlarına ve Kütüklerine Şifrenin Çözülememesinden Dolayı Girilememesi veya Gizlenmiş Verilere Ulaşılamaması ya da İşlemin Çok Uzun Sürecek Olması

Arama tedbirinin uygulanması sırasında bilişim sistemlerine, programlarına ve kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş verilere ulaşılamaması durumunda CMK m.134'te düzenlenen bilgisayarlarda, bilgisayar programlarında ve kütüklerinde elkoyma tedbirine başvurulabilecektir[254]. 7145 sayılı ve 25 Temmuz 2018 tarihli kanun ile hükme *"ya da işlemin uzun sürecek olması"* ifadesi eklenmiştir. Aslında uygulamada var olan ve kolluk kuvvetleri tarafından elkoyma tedbirine başvurmak için bir sebep olarak öne sürülen bu durum, Temmuz 2018'de yapılan değişiklik ile kanuna eklenmiş ve meşru hale getirilmiştir.

D. Tedbirin Uygulanması

Elkoyma tedbirinin amacı arama tedbirinin bilişim sistemleri üzerinde kanunun emrettiği şekilde uygulanmasıdır. Fakat elkoyma durumunda arama tedbiri kanunun birinci fıkrasında düzenlendiği gibi yerinde değil, bilişim sistemlerinin kolluk kuvvetlerince götürüldüğü yerde tamamlanacaktır.

Bilişim sistemlerine elkonulması durumunda, CMK m.134/3'e göre sistemdeki bütün verilerin yedeklemesi yapılacaktır. Aynı maddenin 4. fıkrasına göre ise verilerin bir kopyası şüpheliye ya da vekiline verilecektir. CMK m.134'te yapılan değişiklik öncesinde bir kopyanın şüpheliye veya vekiline verilmesi isteğe bağlı olarak düzenlenmişken, değişiklik sonrası kopya verilmesi kanuni bir zorunluluk haline getirilmiştir. Bizce, yapılan bu değişiklik delillerin sıhhatinin korunması açısından önemli bir değişikliktir. Bu sayede, bilişim sistemlerinden alınan ve mahkemeye sunulan veriler ile şüphelinin elinde bulunan veriler arasında karşılaştırma yapılabilecek ve hassas özelliğe sahip sayısal delillerin değiştirilmediğinden emin olunabilecektir.

---

[254]Değirmenci, **a.g.e.**, s.355.

Uygulamada Yargıtay 16. Ceza Dairesi, 21.9.2017 tarihli kararında *"aramayı gerçekleştiren kişilerce elkoyma işlemine geçildiği sırada sistemdeki verilerin yedeklemesi (imaj-adli kopya) yapılmadan ve yedekten bir kopya alınıp şüpheli veya vekiline verilmeden, ya da yukarda yazılı nedenlerden dolayı mahalde yedekleme ve yedekten kopya verme olanağının bulunmadığının objektif olarak kabulünde zorunluluk bulunan hallerde, aramayı yapan kolluk birimince dijital delillere müdahaleyi önleyecek şekilde, seri numaraları tutanağa yazılmak suretiyle usulüne uygun olarak zapt edilip mühürlenmeden, şüpheli veya müdafinin istemesi halinde nezaret etme ve denetleme imkanı sağlanarak inceleme mahalline kadar eşlik etmesi sağlanmadan ve bu yerde şüpheli veya müdafinin hazır bulunmasına imkan verildikten sonra mümkün olan en kısa süre içinde mühür açılıp, dijital medyanın derhal imajının alınarak ilgilisine de imajlardan bir kopya ve orijinal medya teslim edilmeden, yine sanık veya müdafinin mühür açma işlemi sırasında hazır bulunmasının mümkün olmadığı hallerde, mühür açma işleminin arama ve el koyma kararını veren hakimin huzurunda açılarak imaj alma işleminin bu sırada yapılması yoluna gidilmeden inceleme yapılması halinde arama ve elkoyma işleminin kanuna ve hukuka uygunluğundan bahsetmek mümkün olmadığı gibi bu yolla elde edilen delillerin de hukuka uygunluğu tartışılır hale gelecek ve yargılama makamınca hükme esas alınması mümkün olamayacaktır"* diyerek, elkoyma tedbirinin uygulanması durumunda bilişim sistemindeki verilerin yedeğinin alınarak bir kopyasının şüpheliye ya da vekiline verilmesi gerektiğinin altını çizmiş ve kanuna aykırı olarak yedeklemesi yapılmayan bilişim sistemlerinden elde edilen delilleri hükme esas teşkil eden ilk derece mahkemesinin kararını bozmuştur[255].

Bilgisayarlar, bilgisayar programlarında ve kütüklerinde elkoyma tedbiri uygulandıktan ve ilgili yedekler şüpheliye veya vekiline verildikten sonra, arama tedbirinde olduğu gibi CMK m.169 kapsamında bir elkoyma tutanağı düzenlenecektir. Tutanakta elkoymanın yapıldığı yer, tarihi, başlama ve bitiş saatleri, elkoymayı gerçekleştiren kolluk kuvvetleri isimlerinin, elkoyma işlemine katılan Cumhuriyet savcısının, savcı katılmadıysa ihtiyar heyetinden veya komşulardan elkoyma işlemine katılanların, bilişim sistemlerinin sahip ya da zilyetlerinin, onlar yoksa bu kişiler

[255]Yargıtay 16. Ceza Dairesi E. 2015/2056 K. 2017/5023 T. 21.9.2017 (kararara ma.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

yerine hazır bulunanların isimleri yazılacaktır. Ayrıca, elkoyma tutanağında elkoyma tedbirini gerçekleştiren adli kolluk görevlilerinin, Cumhuriyet savcısının, elkoyma kararını veren sulh ceza hakiminin ve aramada hazır bulunduysa zabıt katibinin imzası bulunmak zorundadır. Şayet elkoyma esnasında şüphelinin avukatı hazır bulunmuşsa, CMK m.169/3'e göre avukatın imzası da bulunacaktır. İmzadan imtina halinde, bu durum sebepleri ile birlikte tutanağa geçirilecektir.

CMK m.121/3'te elkonulan eşyaların defterinin tutulacağı ve bunların resmi mühürle mühürleneceği veya işaret konulacağı belirtilmiştir. Ayrıca, aynı maddenin 1. fıkrasında elkoyma tutanağına ek olarak, hakkında elkoyma tedbiri uygulanan kişinin istemi üzerine, elkonulan bilişim sistemlerinin listesini içeren bir defterin verileceği ve 2. fıkrada elkonulan bilişim sistemlerine ilişkin görüş ve iddialara yer verileceği de belirtilmiştir.

Elkonulan bilişim sistemleri üzerinde arama tedbirlerinin gerçekleştirilmesi ya da depolama birimlerinin imajlarının alınması sonucunda, mülkiyet hakkının daha fazla ihlal edilmemesi için elkonulan bilişim sistemleri şüpheliye derhal iade edilecektir[256]. Türk hukukunda bilişim sistemlerinin en geç ne zaman iade edilmesine dair bir hüküm bulunmamasına karşılık, Amerikan hukukunda otuz günlük bir süre belirlenmiş ve buna uyulmadığı taktirde elde edilen delillerin ceza muhakemesinde kullanılamayacağı belirtilmiştir[257]. Uygulamada, incelemelerinin uzun sürdüğü belirtilerek, elkonulan bilişim sistemleri aylar hatta yıllar sonra iade edilebilmektedir. Bu durumun önüne geçilebilmesi için, görüşümüze göre, CMK m.134'ün lafzına Amerikan hukukunda olduğu gibi bir en geç iade süresi eklenmesi gerekmektedir.

III. Bilgisayarlarda, Bilgisayar Programları ve Kütüklerinde Kopyalama

A. Tedbirinin Hukuki Niteliği

[256]Yenisey/Nuhoğlu, **a.g.e.**, s.434.
[257]United States v. Brunette, 76 F. Supp. 2d 30, D. Me. (1999) (www.justia.com) (Erişim Tarihi:31.08.2019).

Sayısal deliller, tezimizin ilk kısmında açıkladığımız üzere fiziksel delillerden farklı özellikler göstermektedir. Örneğin, sayısal deliller ancak belirli donanım ve yazılımlar aracılığı ile incelenebilmekte ve bu delillerin sayısal ortamda birebir kopyaları oluşturulabilmektedir. Bu durumu dikkate alan Kanun Koyucu *"Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkanının bulunmaması halinde, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına…karar verilir."* denilerek CMK m.134/1'de ve *"Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir."* denilerek CMK m.134/5'te bilgisayarlarda, bilgisayar programlarında ve kütüklerinde kopyalama tedbirini düzenlenmiştir.

Amerikan Hukukunda, kopyalama tedbiri ile kişinin mülkiyet hakkına yasal bir müdahale yapıldığı için elkoyma tedbirinin içerisinde değerlendirilmektedir[258]. Bununla birlikte Türk Kanun Koyucu, kopyalama tedbirini, sayısal delillerin fiziksel delillerden farklılıklarını göz önüne alarak CMK kapsamında ayrı bir tedbir olarak düzenlemiştir. Dolayısıyla bu tedbiri kendine özgü bir tedbir olarak değerlendirmek daha doğru olacaktır[259].

Kanun Koyucu, ayrıca teknik yetersizlikler dolayısıyla sayısal delillerin incelenmesinde yaşanabilecek sorunların önüne geçilebilmesi ve ilgili delillerin üstverileri ile birlikte değerlendirilebilmesi için CMK m.134/1'e *"bu kayıtların çözülerek metin hâline getirilmesine ... karar verilir"* hükmünü eklemiştir. Dolayısıyla sayısal deliller adli bilişim uzmanları tarafından incelenecek, çözümlenecek ve mahkemenin anlayıp ceza muhakemesinde değerlendirebileceği bir şekilde metin haline getirilecektir. Nitekim benzer bir görüşü savunan Tanrıkulu da sayısal delillerin bilirkişiler tarafından mahkeme ya da soruşturma makamlarının anlayacağı şekilde metne dönüştürülmesi gerektiğini savunmaktadır[260].

---

[258]Orin S. Kerr, "Search and Seizure in a Digital World", **Harvard Law Review**, V. 119, 2005, s.565.
[259]Değirmenci, **a.g.e.**, s.373.
[260]Tanrıkulu, **a.g.e.**, s.362-363.

B. Tedbirin Kapsamı

Bilişim sistemlerinde kopyalama tedbirinin uygulanabilmesi için öncelikle bu sistemlerde arama tedbirinin uygulanması gerekmektedir. Arama tedbiri sonucu delillerin elde edilmesi durumunda kopyalama tedbirine başvurularak ilgili bilişim sisteminin tamamının ya da bir kısmının kopyası çıkarılacaktır. Arama tedbiri sırasında şifreli bilişim sistemlerine ya da gizlenmiş verilere ulaşılamazsa, yukarıda ifade edildiği şekilde öncelikle elkoyma tedbirine başvurulacak ve daha sonrasında elde edilen deliller kopyalanacaktır. CMK m.134'te kopyalama tedbirinin uygulanacağı kişiler ya da cihazlar bakımından arama tedbirinden ayrı bir düzenleme yer almamaktadır. Dolayısıyla tedbirinin uygulanacağı kişiler ve cihazlar bakımından tezimizin bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kısmına bakılması gerekmektedir.

C. Tedbirin Şartları

Bilişim sistemlerinde kopyalama tedbirinin uygulanabilmesi için elkoyma tedbirinin uygulanıp uygulanmadığına bakılmaksızın arama tedbirinin uygulanması gerekmektedir. Bu sebeple, arama tedbirinin uygulanması için gereken suç soruşturmasının varlığı, başka surette delil etme olanağının bulunmaması, somut delillere dayanan kuvvetli şüphenin varlığı ve cumhuriyet savcısının isteği üzerine hâkim kararının bulunması koşulları kopyalama tedbiri için de gerekecektir.

D. Tedbirin Uygulanması

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde kopyalama tedbiri, CMK m. 134 kapsamında üç farklı şekilde uygulanabilmektedir. Bunlardan ilki, maddenin 1. fıkrası gereğince arama tedbiri uygulandıktan ve sayısal delil teşkil edebilecek veriler toplandıktan sonra kopyalama tedbirine başvurulmasıdır. Buradaki amaç, arama tedbiri sonucunda elde edilen verilerin bütünlüğünü ve özgünlüğünü muhafaza ederek, bu verilerin birebir kopyalarının çıkartılarak bunların yine aynı maddenin 1. fıkra kapsamında çözülerek metin haline getirilebilmesi ve dolayısıyla mahkemeye sunulabilmesini sağlamaktır.

Yukarıda açıkladığımız üzere, maddenin 2. fıkrasında arama tedbirinin uygulanması sonucunda şifreler çözülemezse, gizli bilgilere ulaşılamazsa ya da işlem uzun sürecekse elkoyma tedbirine başvurulabilecektir. Kanun koyucu 5. fıkrada ise, elkoyma tedbirine başvurulmaksızın bilişim sistemlerindeki verilerin tamamının ya da bir kısmının kopyasının alınabileceğini düzenlemiştir. Dolayısıyla, tedbirin ikinci uygulanma şekli, kanunda elkoyma tedbirine başvurulabilmesi için gereken şartlar var olmasına rağmen bunlara elkoymaksızın kopyalama tedbirine başvurulmasıdır. Böylelikle hem adli bilişim uzmanları tarafından arama tedbirinin gereğince uygulanabilmesi ve kopyalanan verilerin bütünlüğünün ve özgünlüğünün korunması sağlanacak hem de bilişim sistemi ve kütüklerine elkonulmayarak başka mülkiyet hakkı olmak üzere kişi hak ve özgürlüklerine daha az müdahale edilmiş olacaktır. Nitekim Yargıtay kararlarında da bu durum, sayısal delillere olası müdahalelerin engellenmesi, güvenli bir şekilde elkonulup arama tedbirinin uygulanması için mahallinde adli imajın alınıp, bilişim sistemlerinin şüpheliye bırakılması gerektiği vurgulanmaktadır[261]. Ayrıca, tedbir uygulanırken orantılılık ilkesi gereğince öncelikle bilişim sisteminde yer alan verilerin ilgili kısımlarının birebir kopyası alınması, bu durumun mümkün olmaması halinde ise verilerin tamamının kopyası çıkarılması gerekecektir[262].

Öğretide, suç unsuru ya da suç aleti olarak değerlendirilebilecek zararlı yazılım ya da çocuk pornografisi gibi verilerin kopyasının çıkartıldıktan sonra, bilişim sistemlerinde erişilmez kılınması ya da silinmesi gerektiği belirtilmekte ve Siber Suç Sözleşmesi'nde yer alan fakat ilgili kanunda yer verilmeyen bu durum eksiklik olarak değerlendirilmektedir[263].

İlk iki uygulama şeklinde kopyalama tedbirine arama kararının çıkarıldığı dolayısıyla bilişim sistemlerinin bulunduğu yerde başvurulacaktır. İlk şekilde kopyalama tedbiri gerçekleştirildiği zaman, kanunda özel bir düzenleme olmadığı için genel arama hükümlerine göre arama tedbirinin ve devamında kopyalama tedbirinin

[261]Yargıtay 16. Ceza Dairesi E. 2015/2056 K. 2017/5023 T. 21.9.2017 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).
[262]Tanrıkulu, **a.g.e.**, s.371.
[263]Yenisey/Nuhoğlu, **a.g.e.**, s.433.

uygulandığına dair tutanak düzenlenirken, ikinci şekilde bu tutanağa ek olarak ilgili maddenin 5. fıkrasına göre, kopyası alınan veriler kâğıda yazdırılacak ve bir tutanak düzenlenerek ilgililer tarafından imzalanacaktır. Uygulamada Yargıtay, hakkında kopyalama tedbirine başvurulan sayısal verilerin kâğıda yazdırılmamasını ve yazdırılan bu verilerin tutanağa geçirilmemesini usule ve kanuna aykırı olduğunu kararlarında ifade etmekte ve bu sayısal verileri hukuka uygun olarak değerlendirerek hükme esas teşkil eden kararları bozmaktadır[264].

Tedbirin üçüncü uygulama şekli ise ilgili maddenin 2. fıkrasına göre öncelikle bilişim sistemlerine elkonulması ve daha sonrasında kopyalama tedbirine başvurulmasıdır. Bu yöntemde ilk iki uygulama şeklinin aksine kopyalama tedbiri olay yerinde değil, adli bilişim uzmanı tarafından ilgili bilişim sisteminin elkonulduktan sonra incelendiği yerde gerçekleştirilmektedir.

1. Adli İmaj Alma

Kopyalama tedbirinin amacı, ilgili sayısal delillerin ya da bu delillerin yer aldığı hafıza birimleri veya kütüklerin birebir kopyasının alınması ve bu şekilde veri bütünlüğünün korunması ve bu verilerin değişmesi ya da değiştirilmesinin önüne geçilmesidir[265]. Nitekim uygulamada Yargıtay adil yargılamanın sağlanması ve elde edilen verilerin delil niteliğine haiz olabilmesi için, sayısal verilerin belirli teknikler kullanılarak toplanması ve bu verilerin eksiksiz ve bozulmamış bir şekilde yargılama makamlarına sunulması gerektiğinin altını çizmektedir[266]. Adli imaj alma olarak da adlandırılan birebir kopyalamada, hafıza birimlerinde ya da bilgisayar kütüklerinde işleme başlanıldığı tarihten itibaren her türlü işlemin ve değişikliğin görülebilmesi amacıyla ilgili birimin *"bit to bit"* kopyası alınmaktadır[267]. Sıradan kopyalama, yedekleme ya da ayna imaj almadan farklı olan bu yöntemde, hafıza birimlerinde silinen verilerin arta kalan verileri ve boş alanların da kopyası alınarak yeni imaja

[264]Yargıtay 16. Ceza Dairesi E. 2015/4672 K. 2016/2330 T.21.4.2016 (kararara ma.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).
[265]Değirmenci, **a.g.e.**, s.374.
[266]Yargıtay 16. Ceza Dairesi E. 2015/2056 K. 2017/5023 T. 21.9.2017 (kararara ma.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).
[267]Berber, **Adli Bilişim: Computer Forensic**, s. 47.

taşınır. Adli imaj alma sayesinde, bilişim sistemlerinin hafıza birimlerinden silinen fakat ceza yargılamasında delil değerine haiz olup yargılamanın gidişatını değiştirebilecek veriler elde edilebilmektedir[268].

Öğretide ve uygulamada, ilgili maddenin 3. fıkrasında yer alan "yedekleme" ifadesinden "adli imaj alma" işleminin anlaşılması gerektiği belirtilmekte ve delillerin sıhhatinin korunması amacıyla, alınan imajın özet değerinin çıkarılması, bu durumun tutanağa geçirilmesi ve her türlü imaj alma faaliyetinin şüpheli veya vekili huzurunda gerçekleştirilmesi gerektiği vurgulanmaktadır[269].

Birinci bölümde açıkladığımız üzere, sayısal deliller yapılarından ötürü kolayca değişikliğe uğrayabilmekte ya da tahrip edilebilmektedir. Dolayısıyla, kopyalama tedbiri sonucunda elde edilen verilerin özgünlüğünü korumak ve bu verilerden elde edilebilecek sayısal verilerin güvenirliğini korumak amacıyla belli tedbirler alınması gerekmektedir. Öncelikle, kopyalama tedbiri sonucunda elde edilen adli imajın yazılacağı hafıza birimlerinin temiz olması gerekmektedir. Aksi halde, hafıza birimlerinde halihazırda var olan veriler, kopyalama tedbiri sonucunda elde edilen veriler ile beraber aynı hafıza biriminde yer almaya devam edecek ve bu durum elde edilecek sayısal delillerin özgünlüğüne ve güvenilirliğine zarar verecektir[270]. Dolayısıyla kopyalama tedbiri sonucunda elde edilen adli imajlar için ya daha önce kullanılmamış hafıza birimlerinin kullanılması ya da daha önce kullanılmış hafıza birimlerinin kullanım öncesinde temizlenmesi ve bu durumun bir tutanak ile belirtilmesi gerekecektir[271]. Ayrıca, delillerin bilişim korsanları ya da başka kişiler tarafından İnternet gibi dış ağlar aracılığıyla ele geçirilememesi ya da değişikliğe uğratılamaması için, bu hafıza birimleri, dış ağlara açık olmayan ve yalnızca adli bilişim uzmanı tarafından erişilebilen bilişim sistemlerinde saklanmalıdır[272].

---

[268]Tanrıkulu, **a.g.e.**, s.364.
[269]Özen/Özocak, **a.g.e.**, s.73; Yargıtay 16. Ceza Dairesi E.2015/4672 K.2016/2330 T. 21.04.2016 (kararara ma.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).
[270]Tanrıkulu, **a.g.e**., s.365.
[271]Casey, **a.g.e.**, s.483.
[272]Casey, **a.g.e.,** s.484.

2. Özet (Hash) Değeri Alma

Sayısal delillerin özgünlüğünün ve güvenirliğinin korunması için gereken bir diğer tedbir ise bu delillerin ya da kopyalama tedbiri sonucunda elde edilen adli imajların özet değerlerinin alınmasıdır[273]. Henkoğlu tarafından sayısal verilerin parmak izi ya da DNA'sı[274] olarak değerlendirilen özet değeri, Bilgi Teknolojileri ve İletişim Kurumunun 24/08/2011 tarihli ve 2011/DK-14/461 sayılı Kararı ile tespit edilen "Güvenli İnternet Hizmetine İlişkin Usul ve Esaslar" kapsamında "dosya bütünlük değeri" olarak ifade edilmiş ve "*Bir bilgisayar dosyasının içindeki verilerin matematiksel bir işlemden geçirilmesi sonucu elde edilen ve dosyanın içerisindeki verilerde bir değişiklik yapılıp yapılmadığını kontrol için kullanılan dosyanın özünü belirten değer*" olarak tanımlanmıştır. Dolayısıyla, elde edilen sayısal veriler ya da adli imaj bir algoritmaya tabi tutulacak ve bunun sonucunda bir değer elde edilecektir. Bu özet değerinde bir değişiklik olması durumunda ise, sayısal verilerde de bir değişiklik meydana gelmiş olduğu anlaşılacaktır. Özet değerini bir mühre benzeten Tanrıkulu, bozulan mührün eski haline getirilememesi gibi, değişikliğe uğrayan bir dosyanın da eski özet değerine tekrar ulaşılamayacağını belirtmektedir[275].

Adli bilişim uzmanların özet değeri alırken değişik algoritmalardan faydalanabilmektedir. Birbirinden farklı yazılım mühendisleri tarafından hazırlanan bu algoritmalar kendi içerisinde farklı özellikler barındırabilmektedir. Bunlardan ilki özet değerinin uzunluğudur. Örneğin, 1992 yılında B. Kaliski tarafından tasarlanan MD2 algoritması 128 bitlik bir özet değeri üretirken[276], Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standarts and Technology) tarafından 1995 yılında ilan edilen SDH-1 algoritması 160 bitlik bir özet değeri vermektedir[277].

Özet değeri algoritmalarının bir diğer farklılığı ise verimliliği yani çalışma hızıdır. Adli bilişim uzmanları tarafından verimliliği yüksek bir algoritmanın

---

[273]Öğretide bazı yazarlar özet değeri alınmayan sayısal verilerin de delil olarak değerlendirilebileceğini ve hükme esas teşkil edebileceğini savunsa da biz tezimizde bu görüşe katılmıyoruz.
[274]Henkoğlu, **a.g.e.**, s.54.
[275]Tanrıkulu, **a.g.e.**, s.372.
[276]Burton S. Kaliski Jr., **The MD2 Message-Digest Algorithm**, April 1992, s.1, https://tools.ietf.org/html/rfc1319 (Erişim Tarihi: 22 Ocak 2019).
[277]National Institute of Standards and Technology, "Secure Hash Standard (SHS)", **Federal Information Processing Standarts Publication**, 180-4, March 2012, s.3.

kullanılması, özet değeri alma süresini kısaltarak kopyalama tedbirinin uygulanma süresini azaltacaktır.

Ceza muhakemesi açısından kullanılan algoritmaları en önemli özelliği ise güvenilirliğidir. Örneğin, 1990 yılında geliştirilen MD4 algoritmasının hataları 1995 yılında Hans Dobbertin tarafından tespit edilmiş[278] ve bu algoritma yerini MD5'e bırakmıştır. 2008 yılında ise benzer bir şekilde MD5 algoritmasının hatalarının olduğu ve aynı belgenin özet değerlerinin farklı çıkabildiği tespit edilmiştir[279]. Dolayısıyla, sayısal verilerin özgünlüğünün ve dolayısıyla ceza muhakemesinde delil olabilme vasfının korunabilmesi için, adli bilişim uzmanları tarafından güncel ve güvenirliği yüksek bir algoritma kullanılmalıdır.

Son olarak belirtmek gerekir ki, sayısal verilerin özet değerlerinin alınması ve bu değerlerin ceza muhakemesi boyunca değişikliğe uğramaması ilgili verilerin delil sıfatına haiz olmasını sağlamayacak, sadece bu verilerin özgünlüğünü koruduğunu belirtecektir[280]. Nitekim, ilgili sayısal veriler özet değeri alınmadan önce değişikliğe uğramış ya da bilişim sistemini kullanan ve arama kararı çıkarılan kişiye zorla ürettirilmiş olabilir[281].

IV. Bilgisayarlarda, Bilgisayar Programları ve Kütüklerinde Arama, Kopyalama ve Elkoyma Tedbirlerine Karşı Başvuru Yolları ve Kopyalanan Verilerin Yok Edilmesi

Bilgisayarlarda, bilgisayar programları ve kütüklerinde arama, kopyalama ve elkoyma tedbirlerine başvurulabilmesi için, hâkim kararı ya da cumhuriyet savcısının kararı üzerine hâkim onayı gerekmektedir. Dolayısıyla ilgili tedbirlere karşı CMK m. 267'de düzenlenen itiraz yoluna başvurulabilecektir[282].

---

[278]Hans Dobbertin, "Cryptanalysis of MD4", **Journal of Cryptology**, Volume 11, Issue 4, pp 253–271, s.254.
[279]Carnegie University - Software Engineering Institute - CERT Coordination Center, **MD5 Vulnerable to Collision Attacks**, https://www.kb.cert.org/vuls/id/836068/ (Erişim Tarihi: 22.01.2019).
[280]Cumhur Şahin/Neslihan Göktürk, **Ceza Muhakemesi Hukuku II**, Ankara: Seçkin, 2014, s.45.
[281]Alexander Geschonneck, **Computer Forensic, Computerstraftaten Erkennen, Ermitteln, Aufklären**, 4. Aktualisierte Auflage, Deutchland: Dpunkt Verlag, 2010, s.74; aktaran Tanrıkulu, **a.g.e.**, s. 370.
[282]Ünal, **a.g.e.**, s.128; Değirmenci**, a.g.e.**, s.381.

İtiraz CMK m.268'de belirtilen 7 günlük süre içerisinde, tedbir kararını veren Sulh Ceza Hakimliğine karşı yapılacaktır. İlgili Sulh Ceza Hakimliği itirazı haklı bulduğu takdirde tedbir kararını düzeltecek ya da kaldıracak, itirazı haklı bulmadığı durumda ise aynı maddenin 3. fıkrasına göre belirlenecek itirazı incelemeye yetkili Sulh Ceza Hakimliğine gönderecektir.

Bilişim sistemlerine karşı elkoyma başvurulmuşsa, CMK m.267'de belirtilen itiraz yoluna ek olarak, kovuşturma aşaması sona erene kadar m. 127/4'te belirtilen hukuki yoluna başvurarak soruşturma aşamasında Sulh Ceza Hakimliğinden kovuşturma aşmasında ise kovuşturmayı yürüten mahkemeden elkoyma tedbirinin gerekliliğinin değerlendirilmesini talep edebilir[283]. Her ne kadar ilgili karşı başvuru yolu sadece elkoyma tedbiri için düzenlenmiş olsa dahi, görüşümüze göre, sayısal verilere sanal olarak elkonulan kopyalama tedbirine karşı kıyasen ilgili hukuki yola başvurulabilecektir.

Bilişim sistemlerinde arama işlemleri tamamlanarak, ilgili verilerin kopyasının çıkarılması ve bunların metin haline getirilmesi durumunda ya da yukarıda belirtilen karşı başvuru yollarıyla elkoyma kararının kaldırılması durumunda, artık bilişim sistemlerine elkonulmasına ve muhafaza edilmesine gerek olmayacaktır. Bu durunda, CMK m131/1'e göre, elkonulan bilişim sistemi re'sen ya da talep üzerine, soruşturma aşamasında Cumhuriyet Savcısı veya Sulh Ceza Hakimliği, kovuşturma aşamasında ise ilgili mahkeme kararıyla sahibine iade edilecektir. İade kararı kesin karar olup bu karara karşı başvuru yolu bulunmamaktadır. İade kararının reddedilmesi halinde ise yukarıda belirtiğimiz gibi m.267 kapsamında karara itiraz edilebilir[284].

Kanun Koyucu, CMK m.141 kapsamında soruşturma ve kovuşturma aşamasında şüpheli ya da sanık hakkında uygulanan koruma tedbirleri sonucunda uğranılan maddi ve manevi zararlara karşı tazminat talebinde bulunulabileceğini düzenlemiştir. Dolayısıyla, arama tedbirinin özel bir görünümü olan bilgisayarlarda,

[283]Ünal, **a.g.e.**, s.128; Değirmenci**, a.g.e.**, s.381.
[284]Ünal, **a.g.e.**, s.129; Değirmenci**, a.g.e.**, s.381.

bilgisayar programlarında ve kütüklerinde arama tedbirinin hakkında ölçüsüz bir şekilde uygulanması sonucunda zarara uğrayan kişi, ilgili maddenin 1. fıkrasının (i) bendine göre maddi ve manevi tazminat talebinde bulunabilecektir[285]. Nitekim, arama ve elkoyma tedbirleri için ölçülülük kavramına AİHM kararlarında vurgu yapılmaktadır. Mahkeme, arama kararının ve tedbirin uygulanmasının kanun uygun olup olmadığını, meşru bir amaca sahip olup olmadığını ve demokratik bir toplumda gerekli olup olmadığını denetleyerek, Funke/Fransa[286] ile Niemietz/Almanya[287] davalarında başvuranlar lehine tazminata hükmetmiştir.

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde elkoyma ve kopyalama tedbirleri için, bilişim sistemine yukarıda açıkladığımız koşullar oluşmamasına rağmen elkonulması veya kopyalanması, elkonulan bilişim sistemlerinin korunması için gerekli tedbirlerin alınmaması ya da amaç dışı kullanılması ile elkonulan bilişim sisteminin zamanında geri verilmemesi durumunda, zarara uğrayan kişi CMK m.141 1. fıkra (j) bendine göre maddi ve manevi tazminat talebinde bulunabilecektir[288]. Nitekim AİHM, başvuranın bilgisayarında arama tedbiri uygulanarak ilgili deliller elde edilmiş olmasına rağmen 6 yıldan uzun bir süredir ilgili bilgisayarın adli birimler tarafından alıkonulmasını, bilişim sistemlerinde elkoyma tedbirlerinin ölçülü bir şekilde uygulanmaması olarak değerlendirmiş ve Rusya tarafından Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinin ihlal edildiğini tespit ederek Smirnov/Rusya[289] kararında başvuran lehine tazminata hükmetmiştir.

Hakkında cumhuriyet savcısının kararı sonucunda kopyalama tedbiri uygulanan sayısal veriler, kanunda belirtilen yirmi dört saatlik sürenin dolması ya da hâkim tarafından aksi şekilde karar verilmesi durumunda çıkarılan kopyaların ve

---

[285]Özbek/Doğan/Bancaksız/Tepe, **Ceza Muhakemesi Hukuku**, s.363; Ünal, **a.g.e.**, s.130; Değirmenci**, a.g.e.**, s.381.

[286]Funke/Fransa, Başvuru Numarası: 10828/84, 25 Şubat 1993 https://hudoc.echr.coe.int/tur#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-57809%22]} (Erişim Tarihi: 3.03.2019)

[287]Niemietz/Almanya, Başvuru Numarası: 13710/88, 16 Aralık 1992 https://hudoc.echr.coe.int/tur#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-57887%22]} (Erişim Tarihi: 3.03.2019)

[288]Özbek, **CMK İzmir Şerhi**, s.505; Ünal, **a.g.e.**, s.130; Değirmenci**, a.g.e.**, s.381.

[289]Smirnov/Almanya, Başvuru Numarası: 71362/01, 7 Haziran 2007 https://hudoc.echr.coe.int/tur#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-57887%22]} (Erişim Tarihi: 3.03.2019)

çözümü yapılan metinlerin derhal imha edileceği CMK m.134/1'de düzenlenmiştir. Bununla birlikte, hakkında kopyalama tedbiri uygulanan kişi hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da kovuşturma sonucunda beraat kararının verilmesi durumunda kopyalanan verilere ne yapılacağına dair CMK m.134 kapsamında bir hüküm bulunmamaktadır. Başta kişisel veriler olmak üzere temel hak ve özgürlüklere müdahale teşkil eden kopyalama tedbiri kapsamında böyle bir düzenlemenin yer almaması, öğretide bir eksiklik olarak değerlendirilip eleştirilmektedir[290].

Öğretide Ünal, iletişimin tespiti, dinlenmesi ve kayda alınmasına atıfta bulunarak, hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da kovuşturma sonucunda beraat kararının verilmesi durumunda, kopyalanan verilerin CMK m. 137/3 hükmü gereğince kıyasen on gün içerisinde imha edilmesi ve bu durumun tutanakla tespit edilmesi gerektiğini ifade etmektedir[291]. Kanaatimizce, kanun maddesinde değişiklik yapılarak, benzer bir hükmün CMK m.134 kapsamına eklenmesi ve böyle bir değişiklik yapılana kadar kıyasen m.137/3'ün uygulanması gerekmektedir.

[290]Centel/Zafer, **a.g.e.**, s.461.; Değirmenci, **a.g.e.**, s.380.
[291]Ünal**, a.g.e.**, s.127.; benzer görüş için Değirmenci, **a.g.e.**, s.320.

SONUÇ

Hukukumuzda bilişim sistemlerinden delil elde etmek amacıyla, Ceza Muhakemesi Kanunu kapsamında "bilgisayarlarda, bilgisayara programlarında ve kütüklerinde arama, kopyalama ve elkoyma" tedbirleri düzenlenmiştir. Fakat, görüşümüze göre, uygulamada ve kanunun lafzında bazı sorun ve eksiklikler bulunmaktadır.

CMK m.134'te düzenlenen koruma tedbirlerinde bilgisayarlarda, bilgisayar programı ve bilgisayar kütüğü terimleri kullanılmaktadır. Uygulamada Yargıtay bilgisayar ifadesini geniş yorumlamakta ve bilgisayar tanımına uymayan fakat bilişim yeteneğine sahip bulunan akıllı cep telefonu, GPS cihazları gibi sistemler hakkında CMK m.134 kapsamında düzenlenen koruma tedbirlerinin uygulanabileceğini savunmaktadır. Fakat, kanunun lafzı dar yorumlandığında bu tedbirler bilgisayar dışındaki bilişim sistemlerinde uygulanamayacaktır. Ayrıca, ilgili tedbirler tek bir maddede düzenlenmiştir. Bu durumun önüne geçmek için kanunda değişiklik yapılmalı ve her bir koruma tedbiri "bilişim sistemlerinde arama, kopyalama ve elkoyma" başlığı altında ayrı maddelerde düzenlenmelidir.

Tezimizin konusu olan koruma tedbirleri, başta mülkiyet hakkı, kişisel verilerin korunması ve özel hayatın gizliliği gibi temel hak ve özgürlüklere müdahale teşkil etmesi sebebiyle kanun koyucu tarafından son çare olarak başvurulacak tedbir olarak düzenlenmiştir. Ayrıca, ölçülülük ilkesi gereğince ilgili tedbirlerin uygulanabilmesi için hâkim kararı gerekmektedir ve yalnızca belli şartların gerçekleşmesi durumunda elkoyma tedbiri uygulanabilmektedir. Fakat 2018 yılında kanunda yapılan değişiklik ile birlikte savcı kararı ile tedbirler uygulanabilir hal gelmiş ve işlemlerin uzun sürecek olması, elkoyma tedbirinin uygulanabilmesi için kanuni dayanak haline getirilmiştir. Kanunda yapılan değişiklikleri isabetli bulmuyoruz ve özellikle işlemlerin uzun sürecek olması sebebiyle elkoyma tedbirinin uygulanabilmesi düzenlemesini, halihazırda kolluk kuvvetleri tarafından uygulanan arama tedbiri uygulanmaksızın bütün bilişim sistemlerine elkoyma durumunun meşrulaştırılması olarak değerlendiriyoruz. Dolayısıyla, görüşümüze göre ilgili hükümler kanundan çıkartılmalıdır.

AKSSS, başka bilişim sistemlerinde depolanan fakat arama kararı verilen bilişim sistemleri aracılığıyla erişilebilen veriler ile çıkarılabilir depolama birimlerinde arama, kopyalama ve elkoyma işlemlerinin gerçekleştirilebilmesi için taraf devletlere gereken tedbirleri alma sorumluluğu yüklemektedir. Bu doğrultuda, arama, kopyalama ve elkoyma tedbirleri Adli ve Önleme Aramaları Yönetmeliği'nde çıkarılabilir donanımlarda, bilgisayar ağlarında ve diğer uzak bilgisayar kütüklerinde uygulanabilecek şekilde düzenlenmiştir. Bununla birlikte, kanunda benzer bir düzenleme yer almamaktadır. Temel hak ve özgürlüklere müdahale teşkil eden koruma tedbirlerinin kapsamının yönetmelik ile genişletilmesini isabetli bulmuyoruz. Dolayısıyla, görüşümüze göre, başka bilişim sistemlerinde depolanan veriler ile çıkarılabilir depolama birimleri ile ilgili kanuna ekleme yapılmalıdır.

Elkoyma tedbiri, başta mülkiyet hakkı olmak üzere temel hak ve özgürlüklere müdahale teşkil etmektedir. Ölçülülük ilkesi gereğince, elkoyma tedbirinin en kısa sürede sona erdirilmesi gerekmektedir. Nitekim, Amerikan hukukunda elkonulan bilişim sistemlerinin en geç otuz gün içerisinde iade edileceğine dair bir hüküm bulunmakta ve bu sürenin geçirilmesi durumunda elde edilen deliller ceza muhakemesinde delil olarak kullanılamamaktadır. Uygulamada, elkonulan bilişim sistemlerinin aylar sonra iade edildiği dikkate alındığında, Amerikan hukukunda yer alan düzenlemeye benzer bir hükme CMK m.134 kapsamında yer verilmesi gerekmektedir.

Bu doğrultuda, Türk hukukunda bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirlerini düzenleyen CMK m.134 şu şekilde düzenlenmelidir:

CMK m.134/A Bilişim Sistemlerinde Arama

(1) Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, hâkim tarafından şüphelinin kullandığı bilişim sistemlerinde arama yapılmasına karar verilir.

(2) Arama, çıkarılabilir donanımlar ile diğer bilişim sistemlerinde depolanan ve arama yapılan bilişim sisteminden erişilebilen verilerde de yapılabilir.

CMK m.134/B Bilişim Sistemlerinde Elkoyma

(1) Bilişim sistemlerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde gerekli kopyaların alınabilmesi için bu araç ve gereçlere hakim kararı ile elkonulabilir.
(2) Şifrenin çözülmesi ve gerekli kopyaların alınması işlemleri otuz gün içinde gerçekleştirilir.
(3) Bilişim sistemlerinde depolanan ve suç konusu olan veriler erişilemez hale getirilir, çıkarılabilir donanımlar ise müsadere edilir.
(4) İşlemlerin tamamlanması durumunda, elkonulan cihazlar ise gecikme olmaksızın iade edilir.

CMK m.134/C Bilişim Sistemlerinde Kopyalama

(1) Arama sonucunda elde edilen veya elkonulan bilişim sisteminde yer alan bütün verilerin hâkim kararı ile kopyaları çıkartılır. Bilişim sistemlerine elkoymaksızın sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir.
(2) Veri bütünlüğünün sağlanabilmesi amacıyla çıkartılan kopyalar üzerinde özetleme işlemi uygulanır.
(3) Çıkartılan kopyalardan bir tanesi şüpheliye ya da vekiline verilir ve bu husus tutanağa bu husus tutanağa geçirilerek imza altına alınır.
(4) Kopyalanan verileri inceleme yetkisi, Cumhuriyet savcısına ve hâkime aittir.
(5) Kopyalama işleminin uygulanması sonrasında şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da kovuşturma sonucunda sanığın berat etmesi halinde, çıkartılan kopyalar Cumhuriyet savcısının denetimi altında en geç on gün içinde yok edilerek, durum bir tutanakla tespit edilir.

KAYNAKÇA

I. KİTAPLAR VE MAKALELER

Akalın Şükrü Haluk/Bada Erdoğan/Cebeci Zeynel/Acar Levent/Mıtış Bülent/Tan Ali, **Bilgisayar Terimleri Karşılıklar Kılavuzu**, Ankara: Türk Dil Kurumu Yayınları, 2008.

Aksoy Şemsettin, **Avrupa İnsan Hakları Mahkemesi, Uluslararası Yargı ve Yargıtay Kararları Işığında Önleme ve Koruma Tedbiri Olarak Arama**, Ankara: Seçkin Yayıncılık, 2007.

Avşar Zakir/Öngören Gürsel, **Bilişim Hukuku**, İstanbul: Türkiye Bankalar Birliği, 2010.

Aydın Emin Doğan, "Bilişim Sistemlerinde Güvenlik, Güvenirlik, Mahremiyet ve Bilişim Suçları", **Marmara İletişim Dergisi**, İstanbul, S.1, Aralık 1992.

Aydın Emin Doğan, **Bilişim Suçları ve Hukukuna Giriş,** Ankara: Doruk Yayınları, 1992.

Aydoğan Hakan, **Adli Bilişimde Yeni Elektronik Delil Elde Etme Yöntemleri**, Yayımlanmamış Yüksek Lisans Tezi, Polis Akademisi Güvenlik Birimleri Enstitüsü Güvenlik Stratejileri Yönetimi Anabilim Dalı, Ankara, 2009.

Baer Wolfgang, "LG Frankfurt/M. , 21.10.2003 - 5/8 Qs 26/03 : LG Frankfurt/M.: Durchsuchung bei Internetprovider", **Multimedia und Recht,** 2007, V. 5.

Balay Mustafa/Erses Neşe, **Bilgisayar Kullanımı ve İnternet**, Ed: Aysan Şentürk, 2. Baskı, Bursa: Ekin Kitabevi, Kasım 2005.

Baştürk İhsan, "Bilgisayar Sistemleri ile Verilerinde Arama, Kopyalama ve Elkoyma", **Fasikül Aylık Hukuk Dergisi**, Y.2, S.9, Ağustos 2010.

Battula Bhanu Prakash/Rani B. Kezia/Prasad R. Satya/Sudha T.**,** "Techniques in Computer Forensics: A Recovery Perspective", **Internatinal Journal of Security**, Vol.3, Issue 2.

Bıçak Vahit, **Suç Muhakemesi Hukuku**, Ankara, Seçkin Yayınevi, 2010.

Bozdoğan Akbulut Berrin, "Bilişim Suçları", **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, Konya, C. VIII, S. 1-2, 2000.

Böckenförde Thomas, **Die Ermittlung im Netz: Möglichkeiten und Grenzen neuer Erscheinungsformen strafprozessualer Ermittlungstätigkeit**. Almanya: Mohr Siebeck Verlag. 2003.

Carnegie University - Software Engineering Institute - CERT Coordination Center, "MD5 Vulnerable to Collision Attacks", (https://www.kb.cert.org/vuls/id/836068/).

Casey Eoghan, **Digital Evidence and Computer Crime: Forensic Science, Computers and The Internet**, Third Edition, Academic Press, April 2011.

Centel Nur/Zafer Hamide, **Ceza Muhakemesi Hukuku**, 15. Bası, Ankara: Beta, 2018.

Cockfield Arthur J., "Toward a Law and Technology Theory", **Manitoba Law Review**, Vol. 30, No.3, 2004.

Cockfield Arthur/Pridmore Jason, "A Synthetic Theory of Law and Technology", **Minnesota Journal of Law, Science and Technology**, Vol.8, No.2, 2007.

Counsil of Europe**, Electronic Evidence Guide – A Basic Guide for Police Ofiicers, Prosecutors and Judges**, Version 2.0, Cybercrime Division - Directorate General of Human Rights and Rule of Law, Strasbourg – France, 15 December 2014.

Çağlar Doğan Duygu, "Ceza Muhakemesinde Adli Arama", **TBBD**, S.92, s.167

Decima Olivier, "Les Investigations Numériques en Procédure Pénale Française: Du Piratage Informatique aux Perquisitions et Saisies Numériques?", **Galatasaray Üniversitesi Hukuk Fakültesi Dergisi**, 2017/1.

Değirmenci Olgun, **Ceza Muhakemesinde Sayısal (Dijital) Delil**, Ankara: Seçkin, Mart 2014.

De Vllenfague Florence/Dusollier Séverine, "La Belgique sort enfin ses armes contre la cybercriminalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique", **Auteurs et Média**, 2002, Numéro 1.

Dobbertin Hans, "Cryptanalysis of MD4", **Journal of Cryptology**, Volume 11, Issue 4.

Dokurer Semih, "Adli Bilişim"**, Ses Görüntü ve Data İncelemeleri**, Ed: Levent Bayram, Ankara: Adalet Yayınevi, 2008

Dülger Murat Volkan**, Bilişim Suçları ve İnternet İletişim Hukuku**, 4. Baskı, Ankara: Seçkin, 2014.

Ersoy Yüksel, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", **Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi**, Ankara, C.XLIX, S.3-4, 1994.

European Union Agency for Network and Information Security, **Electronic Evidence – A Basic Guide for First Responders**. (https://www.enisa.europa.eu/publications/electronic-evidence-a-basic-guide-for-first-responders).

Günal Cem, "Adli Bilişim ve Delillerin Toplanması", **Özyeğin Üniversitesi Hukuk Fakültesi Bilişim Hukuku Sertifika Programı Sunumu**, 18 Şubat-11 Mart 2012.

Henkoğlu Türkay, **Adli Bilişim**, İstanbul: Pusula, 2014.

Jahn Matthias/Kudlich Hans, "Die strafprozessuale Zulässigkeit der Online-Durchsuchung", **Juristische Rundschau**, Volume 2007, Issue 2.

Jarrett H. Marshall/Bailie Michael W. /Hagen Ed/Judish Nathan, **Searching and Seizing Computers and Obtainig Electronic Evidence in Criminal Investigation**, United States of America, Office of Legal Education

Jekot Wayne, "Computer Forensics, Search Strategies and the Particularity Requirement", **Pittsburgh University Journal of Technology Law and Policy**, V. VII, Spring 2007.

Kaliski Jr. Burton S., **The MD2 Message-Digest Algorithm**, April 1992.

Karagülmez Ali, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, Ankara: Seçkin Yayıncılık, 2014.

Kaymaz Seydi, "Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesinin Bir Koşulu Olarak Başka Surette Delil Elde Etme İmkanının Bulunmaması", **Fasikül Aylık Hukuk Dergisi**, Y.2, S.3, Şubat 2010.

Kerr Orin S., "Search and Seizure in a Digital World", **Harvard Law Review**, V. 119, 2005.

Kerr Orin S., "Search Warrants in an Era of Digital Evidence", **75 Mississippi Law Journal**, V. 85, 2005.

Keser Berber Leyla, **Adli Bilişim: Computer Forensic**, Ankara:Yetkin Yayınları, 2004.

Keser Berber Leyla, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma", **Hukuk Merceği, Konferanslar ve Paneller, 25 Nisan 2008 – 24 Temmuz 2008**, Ankara: Ankara Barosu Yayınları, 2010.

Kirk Dominik/Wegener Christoph, "Technical Issues of Forensic Investigations in Cloud Computing Environments", **Workshop on Crytography and Security in Clouds**, Zurich, March 2011.

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

Kurt Levent, **Açıklamalı ve Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunu'ndaki Uygulaması,** Ankara: Seçkin Yayınevi, Eylül 2005.

Malkoç İsmail/Yüksektepe Mert, **Açıklamalar ve Yorumlarıyla 5271 sayılı Yeni Ceza Muhakemesi Kanunu, C.1**, Ankara: Malkoç Kitabevi, 2008.

Mason Stephen, "Indroduction", **International Electonic Evidence**, British Institute of International and Comparative Law, 2008.

Mukasey Michael B./Sedgwick Jeffrey L./Hagy David W., **Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition**, Washington: National Institute of Justice, April 2008.

Nakamaru Kimberly, "Mining for Manny: Electronic Search and Seizure in the Aftermath of United States v. Comprehensive Drug Testing", **Loyola of Los Angeles Law Review**, V.44, 2001.

National Institute of Standards and Technology, "Secure Hash Standard (SHS)", **Federal Information Processing Standarts Publication**, 180-4, March 2012.

O'Leary Kaitlyn R., "What the Founders Did Not See Coming: The Fourth Amendment, Digital Evidence and the Plain View Doctrine", **Suffolk University Law Review**, V.211.

Ong Julia M., "Another Step in the Evolution of E-Discovery: Amendments of the Federal Rules of Civil Procedure Yet Again", **Boston University Journal of Science & Technology Law**, V:18, 2012.

Ölmez Aslan, "Bilgisayarlarda, Bilgisayar Programlarında Kopyalama ve Bunlara Elkoyma", **Terazi Hukuk Dergisi**, S.30, Şubat 2009.

Özbek Veli Özer, **CMK İzmir Şerhi, Yeni Ceza Muhakemesi Kanununun Anlamı (Gerekçeli-İçtihatlı)**, Ankara: Seçkin Yayıncılık, 2005

Özbek Veli Özer, "Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi", **İÜHFM**, Cilt LIX S.1-2, İstanbul, 2001.

Özbek Veli Özer/Doğan Koray/Bacaksız Pınar/Tepe İlker, **Ceza Muhakemesi Hukuku**, Gözden Geçirilmiş 10. Baskı, Ankara: Seçkin Yayıncılık, 2017.

Özel Cevat, "Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı", **İstanbul Barosu Dergisi**, İstanbul, C. LXXV, S. 7-8-9, Eylül 2001.

Özen Muharrem/Baştürk İhsan, **Temel Hak ve Özgürlükler Bağlamında Bilişim-İnternet ve Ceza Hukuku**. Ankara: Adalet Yayınevi, 2011.

Özen Muharrem/Özocak Gürkan, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi", **Ankara Barosu Dergisi**, s.2015/1.

Öztürk Bahri/Tezcan Durmuş /Erdem Mustafa Ruhan/Gezer Özge Sırma /Saygılar Kırıt Yasemin F./Alan Akcan Esra/Özaydın Özdem/Tütüncü Efser Erden, **Nazari ve**

Uygulamalı Ceza Muhakemesi Hukuku, Güncellenmiş 11. Baskı, Ankara: Seçkin, 2017.

Öztürk Mustafa İlker, **Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesine İlişkin Akış Modelleri**, Yayımlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, Ankara, 2007.

Pollitt Mark M., "Report on Dijital Evidence", **13th INTERPOL Forensic Science Symposium**, Lyon, France, October 16-19 2001, D. 4.

Say Kubilay, "Bilişim Suçlarında Olay Yeri İncelemesinin Hukuki Boyutu", **Ses, Görüntü ve Data İncelemeleri**, Ed: Levent Bayram, Ankara: Adalet Yayınevi, 2008.

Sırma Özge, "Güncel Olaylar Çerçevesinde 5271 Sayılı Ceza Muhakemesi Kanununda Arama", **Terazi Hukuk Dergisi**, S.34, 2009

Sommer Peter, "Digital Evidence Emerging Problems in Forensic Computing", **LSE**, 2002.

Şahin Cumhur, **Ceza Muhakemesi Hukuku I**, Ankara: Seçkin, 2007.

Şahin Cumhur/Göktürk Neslihan, **Ceza Muhakemesi Hukuku II**, Ankara: Seçkin, 2014.

Şahin İlyas, "Türk Ceza Yargılaması Hukukunda Koruma Tedbirleri Bakımından Esas Alınan Şüphe Kavramının İncelenmesi", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C.20, S.3, 2014.

Tanrıkulu Cengiz, **Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma**, Ankara: Adalet Yayınevi, 2014.

Taşkın Şaban Cankat, **Bilişim Suçları**, Bursa: Beta Yayınevi, 2008.

The Sedona Conference, **The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production**, 19 Sedona Conference J. 1, 2018

Tepe İlker, "İnternet (Bilişim) Ceza Hukuku Örneğinde Türk Ceza Hukuku'ndaki Yeni Gelişmeler", **Alman-Türk Karşılaştırmalı Ceza Hukuku**, (Yayına Hazırlayanlar: Prof. Dr. Eric Hilgendorf – Prof. Dr. Yener Ünver), Cilt I, İstanbul, 2010.

Tutanaklarla Ceza Muhakemesi Kanunu, Ankara: Adalet Bakanlığı Yayın İşleri Dairesi Başkanlığı, 2005.

Türkoğlu İbrahim, **BİL391 İşletim Sistemleri (Ders Notları)**, Elâzığ, 2006, s. 23

Ünal Osman Gazi**, Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma**, Yayımlanmamış Yüksek Lisans Tezi, Gazi

Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Ceza ve Ceza Usul Hukuku Bilim Dalı, Ankara, 2011.

Ünver Yener/Hakeri Hakan, **Ceza Muhakemesi Hukuku**, 14. Baskı, Ankara: Adalet, 2018.

Von Wolfgang Joecks, **Studienkommentar StPO**, 2. Baskı, Almanya: C.H.Beck Verlag, 2008.

Warford J. Stanley, **Computer Systems**, Canada: Jones and Bartlett Publishers, 2010, Fourth Edition Kindle Version

Warner Nadine C., "Metadata 101: What Lies Beneath", **American Bar Association The Public Lawyer**, Volume 12, No. 2, Summer 2004.

Wiebke Abel, "Agents, Trojans and Tags: The Next Generation of Investigators", **International Review of Law, Computers and Technology**, Vol.23, 2009.

Wieser ve Bicos Beteiligungen GmBH/Avusturya Davası, Çev: Serkan Cengiz, TBB Dergisi, S.82, Mayıs 2009.

Williams Janet, **ACPO Good Practise Guide for Digital Evidence**, version 5, October 2011.

Yazıcıoğlu Recep Yılmaz, **Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuksal Boyutları ile**, İstanbul: Alfa Kitabevi, 1997.

Yenidünya Caner/Değirmenci Olgun, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul: Legal Yayıncılık, 2003.

Yenisey Feridun/Nuhoğlu Ayşe, **Ceza Muhakemesi Hukuku**, Ankara: Seçkin, 2017.

Yurdakul Ceyhun/Çağlayan Ufuk, **Bilgi Teknolojileri Türkiye İçin Nasıl Bir Gelecek Hazırlamakta**, Ankara: Türkiye İş Bankası Kültür Yayınları, 1997.

II. MAHKEME KARARLARI

Almanya Federal Anayasa Mahkemesi 2 BvR 279/90 sayı ve 03.09.1991 tarihli kararı. (Cengiz Tanrıkulu, **Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma**, Ankara: Adalet Yayınevi, 2014)

Almanya Federal Anayasa Mahkemesi 2 BvR 2099/04 sayılı ve 02.03.2006 tarihli kararı (www.bundesverfassungsgericht.de) (Erişim Tarihi: 31.08.2019).

Almanya Federal Anayasa Mahkemesi 2 BvR 1027/02 sayılı ve 12.04.2005 tarihli kararı (www.bundesverfassungsgericht.de) (Erişim Tarihi: 31.08.2019).

Funke/Fransa, Başvuru Numarası: 10828/84, 25 Şubat 1993 (hudoc.echr.coe.int) (Erişim Tarihi: 25.07.2019).

Handyside/Birleşik Krallık, Başvuru Numarası: 5493/72, 7 Aralık 1976 (www.rtuk.gov.tr) (Erişim Tarihi: 31.08.2019).

Illinois v. Andreas, 463 U.S. 765, 771 (1983) (www.justia.com) (Erişim Tarihi:31.08.2019).

Katz v.United States, 389 U.S. 347, 351 (1967) (www.justia.com) (Erişim Tarihi:31.08.2019).

Mason v. Pulliam, 557 F.2d 426, 429 (5th Cir. 1977) (www.justia.com) (Erişim Tarihi:31.08.2019).

Matter of Search Warrant for K-Sports, Inc., 163 F.R.D. 594 (C.D.Cal. 1995) (www.titleii.com/bardwell/in_re_ksports.txt) (Erişim Tarihi:31.08.2019).

Niemietz/Almanya, Başvuru Numarası: 13710/88, 16 Aralık 1992 (hudoc.echr.coe.int) (Erişim Tarihi: 25.07.2019).

Petri Sallinen ve diğerleri/Finlandiya, Başvuru Numarası: 50882/99, 27 Eylül 2005 (hudoc.echr.coe.int) (Erişim Tarihi: 25.07.2019).

Smirnov/Almanya, Başvuru Numarası: 71362/01, 7 Haziran 2007 (hudoc.echr.coe.int) (Erişim Tarihi: 25.07.2019).

United States v. Butler, 151 F. Supp. 2d 82, 83-84 (D. Me. 2001) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Brunette, 76 F. Supp. 2d 30, D. Me. (1999) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Carey, 172 F.3d 1268, 1275(10th Cir. 1999) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Carter, 549 F. Supp. 2d 1257, 1261 (D. Nev. 2008) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Giberson, 527 F.3d 882, 887 (9th Cir. 2008) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Gines-Perez, 214 F. Supp. 2d 205, 224-26 (D.P.R. 2002) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Fleet Management Ltd., 521 F. Supp. 2d 436, 443-44 (E.D. Pa. 2007) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Circuit, 2007) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Hill, 459 F.3d 966, 974-75 (9th Cir. 2006) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Hunter, 13 F. Supp. 2d 574 (D. Vt. 1998) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Lamb, 945 F. Supp. 441, 462 (N.D.N.Y. 1996) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Matlock, 415 U.S. 164, 177 (1974) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Milian- Rodriguez, 759 F.2d 1558, 1563-64 (11th Cir. 1985) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Payton, ___ F.3d ___, 2009 WL 2151348 (9th Cir. July 21, 2009) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Perez, 484 F.3d 735, 740 (5th Cir. 2007) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Ross, 456 U.S. 798, 822-823 (1982) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Runyan, 275 F.3d 449, 464-465 (5th Circuit, 2001) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Stults, 2007 WL 4284721, at *1 (D. Neb. Dec. 3, 2007) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Terry, 522 F.3d 645, 648 (6th Cir. 2008) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (www.justia.com) (Erişim Tarihi:31.08.2019).

United States v. Walser, 275 F.3d 981, 986 (10th Circuit, 2001) (www.justia.com) (Erişim Tarihi:31.08.2019).

Vaughn v. Baldwin, 950 F.2d 331, 334 (6th Cir. 1991) (www.justia.com) (Erişim Tarihi:31.08.2019).

Yargıtay 1. Ceza Dairesi E. 3700 K. 2007/4661 T. 11.06.2007 (Aslan Ölmez, "Bilgisayarlarda, Bilgisayar Programlarında Kopyalama ve Bunlara Elkoyma", **Terazi Hukuk Dergisi**, S.30, Şubat 2009).

Yargıtay 5. Ceza Dairesi E. 3891 K. 2005/3230 T.14.11.2005 (Aslan Ölmez, "Bilgisayarlarda, Bilgisayar Programlarında Kopyalama ve Bunlara Elkoyma", **Terazi Hukuk Dergisi**, S.30, Şubat 2009).

Yargıtay 6. Ceza Dairesi E. 2002/16699 K. 2003/6727 T. 13.10.2003 (www.kazanci.com) (Erişim Tarihi: 31.08.2019)

Yargıtay 8. Ceza Dairesi E. 2014/30037 K. 2015/14023 T. 18.3.2015 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

Yargıtay 8. Ceza Dairesi E. 2014/29566 K. 2015/13421 T. 11.3.2015 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

Yargıtay 9. Ceza Dairesi E. 2013/9110 K. 2013/12351 T. 9.10.2013 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

Yargıtay 10. Ceza Dairesi E. 2004/14311 K. 2004/10906 T. 2.11.2004 (www.kazanci.com) (Erişim Tarihi: 31.08.2019).

Yargıtay 11. Ceza Dairesi E. 2005/6376 K. 2007/2551 T. 16.04.2007 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

Yargıtay 12. Ceza Dairesi E. 2015/9555 K. 2016/10731 T. 22.6.2016 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

Yargıtay 12. Ceza Dairesi E. 2015/15933 K. 2016/277 T. 13.1.2016 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

Yargıtay 16. Ceza Dairesi E. 2015/2056 K. 2017/5023 T. 21.9.2017 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

Yargıtay 16. Ceza Dairesi E. 2015/4672 K. 2016/2330 T.21.04.2016 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

Yargıtay 16. Ceza Dairesi E. 2017/1443 K. 2017/4758 T. 14.7.2017 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

Yargıtay 17. Ceza Dairesi E. 2015/27517 K. 2017/1716 T. 15.2.2017 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

Yargıtay 19. Ceza Dairesi E. 2015/2092 K. 2015/1175 T. 6.5.2015 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

Yargıtay Ceza Genel Kurulu E. 2007/6-136 K. 2007/150 T. 19.6.2007 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

Yargıtay Ceza Genel Kurulu E. 2017/16-956, K. 2017/370, T. 26.9.2017 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019).

Yargıtay Ceza Genel Kurulu E. 2017/956 K. 2017/370 T. 26.09.2017 (karararama.yargitay.gov.tr) (Erişim Tarihi: 31.08.2019)

Wieser ve Bicos Beteiligungen GmBH/Avusturya, Başvuru Numarası: 74336/01, 16 Ekim 2007 (hudoc.echr.coe.int) (Erişim Tarihi: 31.08.2019).

III. İNTERNET KAYNAKLARI

https://www.adalet.gov.tr

https://www.americanbar.org

https://www.bundesverfassungsgericht.de

https://www.businessinsider.com/people-who-were-erased-from-history-2013-12

https://www.coe.int/cybercrime

https://www.craigball.com/metadata.pdf

https://www.enisa.europa.eu

https://www.haber7.com/yazarlar/prof-dr-ersan-sen/2237114-teknik-araclarla-izleme

https://hudoc.echr.coe.int

http://www.justia.com

https://www.kazanci.com

https://www.legifrance.gouv.fr

https://www.ncjrs.gov

https://www.nisanyansozluk.com

https://www.ozgureralp.av.tr

https://www.rtuk.gov.tr

https://www.tbd.org.tr

https://www.tbmm.gov.tr

https://www.thesedonaconference.org

https://www.titleii.com/bardwell/in_re_ksports.txt

https://karararama.yargitay.gov.tr

TEZ ONAY SAYFASI

Üniversite	: T.C. GALATASARAY ÜNİVERSİTESİ
Enstitü	: SOSYAL BİLİMLER ENSTİTÜSÜ
Hazırlayanın Adı Soyadı	: Oğuzhan Emre PARLAK
Tez Başlığı	: Türk Ceza Muhakemesinde Bilişim Sistemlerinde Arama, Kopyalama ve Elkoyma
Savunma Tarihi	: 16 / 09 / 2019
Danışmanı	: Doç. Dr. E. Eylem AKSOY RETORNAZ

JÜRİ ÜYELERİ

Unvanı, Adı Soyadı	İmza
Doç. Dr. E. Eylem AKSOY RETORNAZ	
Doç. Dr. Pınar MEMİŞ KARTAL	
Doç. Dr. Güçlü AKYÜREK	

Enstitü Müdürü
Prof. Dr. M. Yaman ÖZTEK