

T.C.
DOKUZ EYLÜL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
KAMU HUKUKU PROGRAMI
YÜKSEK LİSANS TEZİ

BİLGİSAYARLARDA, BİLGİSAYAR
PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA,
KOPYALAMA VE ELKOYMA (CMK MD. 134)

Çağatay YÜKSEL

Danışman
Dr. Öğretim Üyesi Pınar BACAKSIZ

İZMİR – 2022

TEZ ONAY SAYFASI



YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum “Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma (CMK md. 134)” adlı çalışmanın, tarafımdan, akademik kurallara ve etik değerlere uygun olarak yazıldığını ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve bunu onurumla doğrularım.

14/11/2022

Çağatay YÜKSEL

ÖZET
Yüksek Lisans Tezi
Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama,
Kopyalama ve Elkoyma (CMK md. 134)
Çağatay YÜKSEL

Dokuz Eylül Üniversitesi
Sosyal Bilimler Enstitüsü
Kamu Hukuku Anabilim Dalı
Kamu Hukuku Programı

Bilişim sistemleri, teknolojinin hızlı gelişimi ile günümüzde her alanda yerini almış, hayatımızla iç içe geçmiştir. Geline nokta, bilişim sistemlerinin olmadığı bir hayat düşünülemez. Öte yandan; bilişim sistemlerinin, hayatımızın bu denli içinde yer alması, suç işlenmesi sırasında en çok kullanılan araçlardan birisi olmasına ve suça ilişkin delillerinin en çok saklandığı ortam haline gelmesine neden olmuştur.

İnsanlar kendilerine ilişkin en hassas ve en özel verilerini bilişim sistemlerinde saklamaktadırlar. Bu anlamda; suçla mücadelede klasik tedbirler yetersiz kalmış, bilişim sistemlerine özgü hareket tarzları geliştirmek şart olmuştur. Bilişim sistemlerine yapılacak müdahale ile elde edilmek istenen hukuki yarar ile temel hak ve özgürlere müdahale arasında makul bir denge gözetilmesi gerekmektedir. Yine, bilişim sistemlerinde yer alan verilerin hassas yapısı, değiştirilmeye ve tahrif edilmeye uygunluğu verilere müdahale konusunda özenli davranmayı gerektirmiştir. Karşılaştırmalı hukukta, bilişim sistemlerine özgü koruma tedbirleri düzenlenen ülkeler bulunmakla birlikte, genel arama ve elkoyma usullerini sürdüren ülkeler de bulunmaktadır. Hukuk düzenimizde genel arama ve elkoyma tedbirlerinden ayrı düzenleme yapılarak, bilişim sistemlerine özgü koruma tedbiri geliştirilmiş olması son derece yerinde bir uygulamadır.

Çalışmamızda, 5271 sayılı Ceza Muhakemesi Kanununda özel bir arama ve elkoyma tedbiri olarak düzenlenen bilgisayarlarda, bilgisayar programlarında

ve kütüklerinde arama, kopyalama ve elkoyma tedbiri ele alınmıştır. Öncelikle, koruma tedbirleri ve dijital deliller açıklanmıştır. Çalışmamızın devamında söz konusu koruma tedbiri, Yargıtay ve AİHM kararları ile öğretideki tartışmalar ışığında açıklanmaya çalışılmış, tedbire ilişkin tartışmalı güncel hususlar incelenmiş ve konuya dair katkı sunulmaya çalışılmıştır.

Anahtar Kelimeler: Dijital Delil, Bilgisayar, Bilişim Sistemi, Arama, Kopyalama, Elkoyma

ABSTRACT

Master's Thesis

**Search, Copy and Seizure In Computers, Computer Programs and Their Files
(CPC art. 134)**

Çağatay YÜKSEL

Dokuz Eylül University

Graduate School of Social Sciences

Department of Public Law

Public Law Program

Information systems, with the rapid development of technology, have taken their place in every field and are intertwined with our lives. At this point, a life without information systems is unimaginable. On the other hand, information systems being so much in our lives has caused it to be one of the most used tools for commissioning a crime and to become the environment where the evidence of the crime is stored the most.

People store their most sensitive and private data in information systems. In this sense, classical measures against crime have been insufficient, and it has become necessary to come up with actions specific to information systems. A reasonable balance should be observed between the legal benefit sought to be obtained intervening in information systems and the interference with fundamental rights and freedoms. Also, the sensitive nature of the data in information systems and its susceptibility for alteration and falsification necessitated a careful attention to data intervention. In comparative law, along with the countries that have specific protection measures for information systems, there are also countries that maintain general search and seizure procedures. In our legal system, it is absolutely an appropriate practice that a protection measure specific to information systems has been developed by setting a separate regulation from general search and seizure measures.

In this study, searching, copying and seizure measures in computers, computer programs and their files, which are regulated as specific search and

seizure measure in Criminal Procedure Code No. 5271, are discussed. At the outset, protection measures and digital evidence are explained. In the continuation of this study, the mentioned protection measure has been tried to be explained in the light of decisions of Supreme Court and ECHR and the debates in the doctrine and, the controversial current issues regarding the measure have been examined and a contribution has been tried to be made on the subject.

Keywords: Digital Evidence, Computer, Information System, Search, Copy, Seizure

**BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE
KÜTÜKLERİNDE ARAMA, KOPYALAMA VE ELKOYMA (CMK MD. 134)**

İÇİNDEKİLER

TEZ ONAY SAYFASI	ii
YEMİN METNİ	iii
ÖZET	iv
ABSTRACT	vi
İÇİNDEKİLER	viii
KISALTMALAR	xiii
GİRİŞ	1

BİRİNCİ BÖLÜM

**GENEL OLARAK KORUMA TEDBİRLERİ VE BİLGİSAYARLARDA,
BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA,
KOPYALAMA VE ELKOYMA**

1.1. CEZA MUHALEMESİ HUKUKUNDA KORUMA TEDBİRLERİ	4
1.1.1. Koruma Tedbirleri Kavramı	4
1.1.2. Koruma Tedbirlerinin Ortak Özellikleri	5
1.1.2.1. Yasal Dayanağın Bulunması	5
1.1.2.2. Hüküm Verilmeden Önce Anayasal Bir Özgürlüğün Sınırlandırılması	6
1.1.2.3. Araç Mahiyetinde Olması	7
1.1.2.4. Suç Şüphelerinin Belli Bir Yoğunlukta Bulunması	8
1.1.2.4.1. Şüphe Kavramı	8
1.1.2.4.2. Basit Şüphe	9

1.1.2.4.3. Makul Şüphe	10
1.1.2.4.4. Yeterli Şüphe	10
1.1.2.4.5. Kuvvetli Şüphe	11
1.1.2.5. Geçici Nitelikte Olması	11
1.1.2.6. Görünüşte Hakklılık	12
1.1.2.7. Gecikmesinde Tehlike (Sakınca) Bulunması	13
1.1.2.8. Orantılılık (Ölçülülük İlkesi) Bulunması	14
1.1.2.9. Yetkili Mercii Kararına Dayanma	15
1.2. DİJİTAL DELİL	16
1.2.1. Tanımı	16
1.2.2. Analog Delil ile Dijital Delil Ayrımı	17
1.2.3. Dijital Delillerin Özellikleri	19
1.2.4. Dijital Delilin Ceza Muhakemesinde Yeri	22
1.2.5. Dijital Delil Elde Etmede Başlıca Standartlar ve İlkeler	23
1.2.5.1. AK Elektronik Delil Elde Etme Rehberi	23
1.2.5.2. ABD Gizli Servis Dijital Delile El Koyma Rehberi	25
1.2.5.3. ACPO Sayısal Delillere İlişkin İyi Uygulama Rehberi	25
1.3. BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA, KOPYALAMA VE ELKOYMA	26
1.3.1. Tedbirin Amacı	27
1.3.2. Tedbirin Kapsam ve Konusu	28
1.3.2.1. Kişi Yönünden	29
1.3.2.1.1. Şüpheli ve Sanık	29
1.3.2.1.2. Diğer Kişiler	32
1.3.2.1.3. Avukatlar	33
1.3.2.1.4. Milletvekilleri	36

1.3.2.1.5. Hakimler ve Savcılar	36
1.3.2.2. Düzenlemede Doğrudan Yer Alan Bilişim Sistem Cihazları	38
1.3.2.2.1. Bilgisayar	38
1.3.2.2.2. Bilgisayar Programı	44
1.3.2.2.3. Bilgisayar Kütüğü	46
1.3.2.3. Düzenlemede Doğrudan Yer Almayan Bilişim Sistem Cihazları	49
1.3.2.3.1. Cep Telefonları	49
1.3.2.3.2. Taşınabilir Veri Depolama Ortamı (TVDO)	52
1.3.2.3.3. Bulut Bilişim Sistemleri	54
1.3.2.3.4. Elektronik Postalar	56
1.3.2.4. Düzenlemede Bilgisayar Teriminin Tercih Edilmesi	58
1.3.3. Tedbirin Hukuki Niteliği	60
1.3.3.1. Genel Olarak	60
1.3.3.2. Benzer Koruma Tedbirleri ile İlişkisi	61
1.3.3.2.1. Arama Tedbiri	61
1.3.3.2.2. Elkoyma Tedbiri	63
1.3.3.2.3. Postada Elkoyma Tedbiri	65
1.3.3.2.4. İletişimin Tespiti, Dinlenmesi ve Kayda Alınması Tedbiri	66
1.3.4. Tedbirin Temel Hak ve Özgürlüklerle İlişkisi	68
1.3.5. CMK md. 134'e İlişkin Yasa Değişiklikleri	71
1.3.5.1. 6526 Sayılı Yasa	71
1.3.5.2. 7145 Sayılı Yasa	72

İKİNCİ BÖLÜM
BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA ARAMA,
KOPYALAMA VE ELKOYMA KORUMA TEDBİRİNİN ŞARTLARI VE
UYGULANMASI

2.1. BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA KOPYALAMA VE ELKOYMA TEDBİRİNİN ŞARTLARI	75
2.1.1. Arama ve Kopyalama Yönünden	75
2.1.1.1. Suç Dolayısıyla Yürütülen Bir Soruşturmanın Varlığı	76
2.1.1.2. Somut Delillere Dayanan Kuvvetli Şüphe Bulunması	79
2.1.1.3. Başka Bir Şekilde Delil Elde Etme Olanağının Bulunmaması	81
2.1.1.4. Hâkim Kararının Bulunması	83
2.1.2. Elkoyma Yönünden	87
2.1.2.1. Arama, Kopyalama Tedbirine Karar Verilmiş Olması	89
2.1.2.2. Şifrenin Çözülememesinden Dolayı Bilgisayara Girilememesi veya Gizlenmiş Bilgilere Ulaşılamamış Olması	90
2.1.2.3. İşlemin Uzun Sürecek Olması	91
2.2. TEDBİRİN UYGULANMASI	92
2.2.1. Bilgisayarlarda, Bilgisayar Programları ve Kütüklerinde Arama ve Kopyalama	94
2.2.1.1. Genel Olarak	94
2.2.1.2. İmaj Alma ve Kopya Üzerinden İnceleme	95
2.2.1.3. Özet Değer (Hash) Hesaplama	98
2.2.2. CMK md. 134 Kapsamında Elkoyma Tedbirinin Uygulanması	100
2.2.2.1. Verilerin Yedeklemesinin Yapılması	100
2.2.2.2. Kopyalama ve Metin Haline Dönüştürme	103
2.2.2.3. Elkonulan Eşyanın İadesi	104

2.2.2.4. Suç Unsuru Barındıran Veri Kopyasının Durumu	105
2.3. TEDBİR SONRASI ELDE EDİLEN VERİLERİN YOK EDİLMESİ	106
2.4. TESADÜFEN ELDE EDİLEN DELİLLER	108
2.5. TEDBİRE KARŞI KANUN YOLU	110
2.6. HUKUKA AYKIRI KORUMA TEDBİRLERİ NEDENİYLE TAZMİNAT	111
2.7. TEDBİRİN HUKUKA AYKIRI UYGULANMASI NEDENİYLE CEZA HUKUKU SORUMLULUĞU GEREKTİREN HALLER	112
SONUÇ	115
KAYNAKÇA	118

KISALTMALAR

ACPO	Association of Chief Police Officers
AİHM	Avrupa İnsan Hakları Mahkemesi
AİHS	Avrupa İnsan Hakları Sözleşmesi
AK	Avrupa Konseyi
AK-SSS	Avrupa Konseyi Siber Suç Sözleşmesi
AÖAY	Adli ve Önleme Aramaları Yönetmeliği
AyM	Anayasa Mahkemesi
BIOS	Basic Input Output System
bkz.	Bakınız
C.	Cilt
CD.	Ceza Dairesi
CD	Compact Disk
CGK	Ceza Genel Kurulu
CHD	Ceza Hukuku Dergisi
CMK	Ceza Muhakemesi Kanunu
CMUK	Ceza Muhakemeleri Usulü Kanunu
CPU	Central Processing Unit
çev.	Çeviren
DVD	Digital Versatile Disc
E.	Esas Numarası
E.T.	Erişim Tarihi
ENIAC	Electronic Numerical Integrator And Computer
FSEK	Fikir ve Sanat Eserleri Kanunu
HASH	Veri Bütünlüğünü Kontrol Eden Tek Yönlü Şifreleme Algoritmasıdır.
Gb	Gigabyte
GPS	Global Positioning System
K.	Karar Numarası
Kanun	5271 sayılı Ceza Muhakemesi Kanunu
KYOK	Kovuşturmaya Yer Olmadığına Dair Karar

md.	Madde
NPCC	National Police Chiefs' Council
UNIVAC	Universal Automatic Computer
USB	Universal Serial Bus
PC	Personel Computer
RAM	Random Access Memory
Rehber	AK Elektronik Delil Elde Etme Rehberi
ROM	Read-Only Memory
S.	Sayı
s.	Sayfa
TCK	5237 sayılı Türk Ceza Kanunu
TDK	Türk Dil Kurumu
TVDO	Taşınabilir Veri Depolama Ortamı
Yönetmelik	Adli ve Önleme Aramaları Yönetmeliği

GİRİŞ

Geçmişten günümüze ortaya konan pek çok yenilik, doğrudan ya da dolaylı olarak bilgisayar dünyasına katkı sağlamıştır. Günümüzde bilgisayar; eğlence, iletişim, sosyal medya, tıbbi alanlar, bankacılık ve muhasebe işlemleri gibi çok çeşitli amaçlarla kullanılabilmektedir. Vatandaşlar, devletle olan pek çok idari iş ve işlemlerini e-devlet veya e-devlet tabanlı portal sistemleri üzerinden gerçekleştirilebilmektedir. Öte yandan, iş dünyası da dijital çağa ayak uydurmuştur. Pek çok sistem; bilişim veri tabanları üzerinde yer edinmiş, çalışanlar işyerine dahi gitmeden evden çalışma sistemine geçmişlerdir. Birçok ticari işletme, işinin çok önemli kısmını bilgisayarlar aracılığıyla yürütmektedir. Bilgisayarların bir an için olmaması durumunda şirketlerin faaliyetleri durma noktasına gelecektir.

Tüm bu gelişmeler ile dijital bir dönüşüm meydana gelmiştir. Söz konusu dönüşümün, pek çok olumlu etkisi olduğu gibi, olumsuz etkiler de ortaya çıkarmıştır. Bilgisayar kullanımı, suç işleme metodolojisini başka bir noktaya getirmiştir. Bilişim sistemleri, pek çok suça araç olabildiği gibi, işlenen suçlarda araç olmasa dahi suç delillerini barındırabilmektedir. Bu anlamda; bilgisayar, dijital delillerin bulunabildiği başlıca ortamlardan biridir. Dijitalleşen dünyada, suçla mücadele konusunda da etkin metotlar belirlemek zaruret haline gelmiştir. Klasik koruma tedbirleri, artık bilişim sistemlerinin kullanıldığı suçlarla mücadelede ya yetersiz kalmakta ya da temel hak ve özgürlükleri ihlal etmektedir.

CMUK döneminde, bilgisayarlara yönelik arama ve elkoyma tedbiri bulunmamaktaydı. Genel arama ve elkoyma tedbiri aynı zamanda bilgisayarlara da uygulanmaktaydı. Ancak, bilişim sistemlerinde yer alan verilere özgü arama usulünün olmaması büyük bir eksiklikti.

Bilişim sistemlerine yönelik arama ve elkoyma tedbiri, temel hak ve özgürlüklere yoğun müdahale niteliği taşımaktadır. Ayrıca, bilişim sistemlerinde yer alan veriler, yok edilebilir, çalınabilir, uzaktan dahi kolayca değiştirilebilir nitelikte hassas yapıdadır. Bu anlamda, bilişim sistemlerine yönelik arama ve elkoyma, genel arama ve elkoyma tedbirinden ayrı bir düzenleme gerektirmektedir.

Kanun koyucu, CMK md. 134 ile bilişim sistemlerine özgü arama ve elkoyma tedbirini düzenlemiş ve gerekçesinde “*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.” ifadesine yer vermiştir. Böylece, hukuk düzenimizde temel hak ve özgürlüklere yoğun müdahalede bulunan bilişim sistemlerinde arama ve elkoyma tedbiri ilk kez özgü nitelikte düzenlenmiştir. CMK md. 134’te yer alan koruma tedbiri tek bir tedbir gibi görünse de esasen madde içeriğinde üç ayrı tedbir barındırmaktadır. Bunlar; arama, kopyalama ve elkoyma tedbirleridir. İlgili bölümlerde bu tedbirler detaylı şekilde incelenecektir.

Çalışmamızın ilk bölümünde, koruma tedbirleri, dijital deliller ile CMK md. 134 kapsamında bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kopyalama ve elkoyma koruma tedbiri genel olarak ele alınmıştır. Öncelikle; koruma tedbirleri kavramsal olarak tanımlanmış, devamında koruma tedbirlerinin özelliklerine yer verilmiştir. Elektronik deliller açıklanmış, birbirinin yerine kullanılan ve karıştırılan elektronik delil, analog delil ve dijital delil kavramlarının arasındaki farklar açıklanmıştır. Analog deliller gelişen teknoloji ile birlikte yok olmaya yüz tutmuştur. Buna karşılık, dijital delillerin uygulama alanı giderek genişlemektedir. Bu minvalde, ceza usul hukukunun amacı olan maddi gerçeğin ortaya çıkarılması sürecinde dijital delillerin yeri incelenmiştir.

Çalışmamızın devamında, tezimizin özünü oluşturan bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbirinin incelenmesine geçilmiştir. Öncelikle, bu özgü koruma tedbiri ilişkili olduğu diğer koruma tedbirleriyle karşılaştırılmış ardından tedbirin amacı açıklanmış ve tedbirin kapsamı ile kişi yönünden ve cihaz yönünden konusu değerlendirilmiştir. Tedbir ile doğrudan düzenleme alanı bulan bilgisayar, bilgisayar programı ve bilgisayar kütüğü ile tedbirde doğrudan yer almayan ve fakat tedbirin uygulama alanı bulunduğu cep telefonları, taşınabilir veri depolama ortamları, bulut bilişim sistemleri ile elektronik postalar incelenmiştir.

Bilişim sistemlerine özgü arama, kopyalama ve elkoyma tedbiri; temel hak ve özgürlüklere yoğun müdahalede bulunması nedeniyle yasa koyucu tedbirin uygulanması oldukça sıkı şartlara bağlanmıştır. Çalışmamızın ikinci bölümünde, yasa koyucunun düzenlediği bu şartlar incelenmiş, öğretilerde yer alan tartışmalara ve yargı

kararlarına yer verilmiş ve tedbirin uygulama şartlarına ilişkin çeşitli öneriler getirilerek literatüre katkı sunulmaya çalışılmıştır.

Çalışmamızın son kısmında ise; tedbirin uygulanması süreci ele alınmış, tedbirin uygulanma safhasında tesadüfen elde edilen delillerin akıbeti incelenmiş ve tedbire karşı uygulanacak kanun yolu değerlendirilmiştir. CMK md. 141 kapsamında, koruma tedbirleri nedeniyle tazminat kurumunun uygulanabilirliği kıymetlendirilerek, tedbirin uygulanma sürecinde ceza hukuku sorumluluğu gerektiren durumlar incelenmiştir.



BİRİNCİ BÖLÜM

GENEL OLARAK KORUMA TEDBİRLERİ VE BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA, KOPYALAMA VE ELKOYMA

1.1. CEZA MUHAKEMESİ HUKUKUNDA KORUMA TEDBİRLERİ

1.1.1. Koruma Tedbirleri Kavramı

Koruma tedbirleri, ceza muhakemesinin gereği gibi yürütülebilmesi veya hükmün sonucunda infazının mümkün kılınması ve yerine getirilmesi maksadıyla verilen ve bazı temel hak ve özgürlüklere müdahaleyi gerektiren hukuki işlemlerdir¹. Koruma tedbirleri, henüz hüküm verilmeden temel hak ve hürriyetleri ve insan haklarının belli oranlarda kısıtlamaktadır². Koruma tedbirleri, bir yandan da doğrudan ya da dolaylı olarak delil elde etme metodudur³.

Öğretide; koruma tedbirleri 1412 sayılı CMUK döneminde Kanun'un kavram birliğine sahip olmaması nedeniyle farklı terimlerle anılmaktaydı. 5237 sayılı Ceza Muhakemesi Kanunu dönemiyle birlikte, söz konusu tedbirler sistematik şekilde, koruma tedbirleri başlığında toplanarak terim sorunu ortadan kaldırılmıştır⁴.

Koruma tedbirleri, esasen hukukun her alanında yer almaktadır. Söz konusu kurum; idari yargılamada “*yürütmenin durdurulması tedbiri*” olarak karşımıza çıkarken, medeni yargılamada ise “*ihtiyati tedbir*” ve “*delil tespit işlemleri*” olarak görünür. Ceza yargılamasında ise, “*tehlike tedbirinin*” bir çeşidi olarak koruma tedbirleri yerini almıştır⁵.

Koruma tedbirlerinin amacı, muhakemeyi mümkün kılmak, yargılama sonucu verilecek hükmün infazının uygulanır olmasını sağlamaktır. Öte yandan, koruma

¹ Veli Özer Özbek ve diğerleri, **Ceza Muhakemesi Hukuku**, 13. baskı, Seçkin Yayıncılık, Ankara, 2020, s. 250; Feridun Yenisey ve Ayşe Nuhoglu, **Ceza Muhakemesi Hukuku**, 8. baskı, Seçkin Yayıncılık, Ankara, 2020, s. 314; Bahri Öztürk ve diğerleri, **Ceza Muhakemesi Hukuku**, 8. baskı, Seçkin Yayıncılık, Ankara, 2021, (CMK), s. 441; Cumhur Şahin ve Neslihan Göktürk, **Ceza Muhakemesi Hukuku-1**, 11. baskı, Seçkin Yayıncılık, Ankara, 2021, (CMK-1), s. 283.

² Bahri Öztürk ve diğerleri, **Ceza Muhakemesi Hukukunda Koruma Tedbirleri**, 4. baskı, Seçkin Yayıncılık, Ankara, 2021, (Koruma Tedbirleri), s. 29.

³ Şahin ve Göktürk, CMK-1, s. 263.

⁴ Öztürk ve diğerleri, Koruma Tedbirleri, s. 27.

⁵ Yenisey ve Nuhoglu, s.313.

tedbirleri delillerin toplanmasını olanaklı kılarken delil karartma ihtimalinin de önüne geçmektedir⁶.

CMK'da pek çok koruma tedbiri yer almaktadır. Örnek olarak; yakalama, gözaltına alma, zorla getirme, tutuklama, arama, elkoyma, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kopyalama ve elkoyma, vücudun muayenesi, iletişimin denetlenmesi, teknik araçlarla izlemedir. Öğretide, koruma tedbirlerini geleneksel koruma tedbirleri ve modern koruma tedbirleri olarak ikiye ayırarak inceleyen yazarlar⁷ da bulunmaktadır.

1.1.2. Koruma Tedbirlerinin Ortak Özellikleri

Ceza muhakemesinde yer alan koruma tedbirlerinin, belli başlı ortak özellikleri bulunmaktadır. Öğretide, yazarlar bahse konu özellikleri çeşitli başlıklar⁸ altında ele almıştır. Bu özellikleri genel olarak şu şekilde sıralayabiliriz; koruma tedbirinin yasa ile düzenlenmiş olması, henüz hüküm verilmeden temel bir hakkı sınırlanması, bir araç mahiyetinde olması, şüphelerin belli bir yoğunlukta olması, geçici olması, görünüşte haklılık bulunması, gecikmede sakınca bulunması, oranlılık (ölçülülük) ilkesine uygun olması ve yetkili bir merciin kararının bulunmasıdır⁹.

1.1.2.1. Yasal Dayanağın Bulunması

1982 Anayasasında; temel hak ve özgürlüklerin kısıtlanmasına yönelik olağan ve olağanüstü dönemde olmak üzere iki farklı rejim yer almaktadır. Olağan dönemde temel hak ve özgürlüklerin kısıtlanmasını öngören 13. madde şu şekilde düzenlenmiştir; *“temel hak ve hürriyetler, özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir. Bu sınırlamalar, Anayasanın sözüne ve ruhuna, demokratik toplum düzeninin ve lâik Cumhuriyetin gereklerine ve ölçülülük ilkesine aykırı olamaz.”* Buna

⁶ Şahin ve Göktürk, CMK-1, s. 263.

⁷ Öztürk ve diğerleri, Koruma Tedbirleri, s.223.

⁸ Özbek ve diğerleri, s. 359; Yenisey ve Nuhoglu, s. 315; Öztürk ve diğerleri, Koruma Tedbirleri, s. 29; Şahin ve Göktürk, CMK-1, s. 287; Ahmet Gökçen ve diğerleri, **Ceza Muhakemesi Hukuku**, 5. baskı, Adalet Yayınevi, Ankara, 2021, s. 379.

⁹ Öztürk ve diğerleri, Koruma Tedbirleri, s. 28.

göre, Anayasamızda temel hak ve özgürlüklerin kısıtlanması için olağan dönemde yasal düzenleme yapılması gerekliliği açıkça düzenlenmiştir¹⁰.

Anayasamızın 90/son maddesi gereğince, usulüne uygun yürürlüğe girmiş uluslararası sözleşmeler, Kanun hükmündedir. Dolayısıyla, koruma tedbirlerine ilişkin uluslararası düzenlemeler de iç hukukumuzda Kanun hükmüne kavuşmuştur¹¹. Bu düzenlemelerden en önemlisi AİHS'dir. AİHS'de, Sözleşmede bulunan temel hak ve özgürlükler yönünden hangi durumlarda kısıtlamaya gidilebileceği her bir madde yönünden düzenlenmiştir¹². AİHM, Sözleşmede yer alan temel hak ve özgürlüklere ilişkin ayrı ayrı karar vermekte ve içtihat geliştirmektedir. Ancak, şunu belirtmek gerekir ki, AİHM değerlendirmede bulunurken “*yasayla öngörülmüş olma*” kavramını sıklıkla kullanmakta ve ulusal uygulamalarda kanunilik ilkesini titizlikle aramaktadır.

Koruma tedbirleri, temel hak ve özgürlükler ile insan haklarını henüz bir mahkeme hükmü olmaksızın kısıtlama anlamına gelir¹³. Bu bağlamda, anayasa ve uluslararası sözleşmeler ile korunan temel hak ve özgürlüklere karşı¹⁴; koruma tedbirlerine başvurabilmek için yasal dayanak bulunması zorunludur¹⁵. Kanuni düzenlemesi bulunmayan koruma tedbiri uygulanamaz. Yine, benzer şekilde yasal zemini bulunan bir koruma tedbirinin kanun ile düzenlenen şartları kıyas yoluyla genişletilemez¹⁶. Ancak yasal düzenlemesi bulunan koruma tedbirlerine ilişkin “*ikincil konuların*”, yeni bir koruma tedbiri getirmeyecek mahiyette diğer düzenleyici işlemler ile yapılabilmesi mümkündür¹⁷.

1.1.2.2. Hüküm Verilmeden Önce Anayasal Bir Özgürlüğün Sınırlandırılması

Bireyin temel hak ve özgürlükleri mahkeme hükmü ile kısıtlanabilmektedir. Koruma tedbirleri ise henüz yargılamanın sona ermediği durumlarda kişilerin temel

¹⁰ Öztürk ve diğerleri, Koruma Tedbirleri, s. 29.

¹¹ Öztürk ve diğerleri, Koruma Tedbirleri, s. 29.

¹² Özen Kaya Göçmen, **Yakalama ve Gözaltı Koruma Tedbirleri**, Seçkin Yayıncılık, Ankara, 2021, s. 31.

¹³ Öztürk ve diğerleri, Koruma Tedbirleri, s. 29.

¹⁴ Göçmen, s. 26.

¹⁵ Mustafa Ruhan Erdem ve diğerleri, **Dijital Ceza Muhakemesi Hukuku**, Seçkin Yayıncılık, Ankara, 2022, s. 464.

¹⁶ Şahin ve Göktürk, CMK-1, s. 267.

¹⁷ Göçmen, s. 32.

hak ve özgürlüklerini kısıtlamaktadır. Kişinin suçu işleyip işlemediği henüz kesinleşmiş mahkeme kararıyla ortaya konmamıştır.

Koruma tedbirlerinin bir kısmı, bireyin sadece tek bir temel hak ve hürriyetine müdahale ederken, diğer kısmı birden çok temel hak ve hürriyeti tek seferde kısıtlayabilmektedir¹⁸. Örneğin, çalışmamızın konusu olan bilgisayarlarda, bilgisayar programları ve kütüklerinde arama, kopyalama ve elkoyma tedbiri özel hayatın gizliliği, mülkiyet hakkı gibi birden çok temel hak ve hürriyeti tek seferde kısıtlamaktadır.

1.1.2.3. Araç Mahiyetinde Olması

Koruma tedbiri yalnızca kendi başına bir anlam ifade etmeyen, muhakeme süresince eski durumu muhafaza etmek ve verilecek kararın uygulanabilirliğini sağlamak adına kullanılan bir araçtır¹⁹. Muhakemenin bütünü göz önüne alındığında bu vasıta oluş doğrudan ya da dolaylı olabilir²⁰. Örneğin; yakalama, gözaltına alma tedbirinin, gözaltına alma ise tutuklama tedbirinin birer vasıtasıdır.

Muhakeme bütününde amaç, maddi gerçeğe ulaşmak ve bu doğrultuda hükmü kurarak hükmün infazını sağlamaktır. Koruma tedbirleri ise, bu neticeye ulaşmak adına kullanılan ve kamu düzeninin de sağlanmasına yarayan birer vasıta²¹. Eş deyişle; koruma tedbirleri, başka bir işlemin gerçekleşmesine yarayan araç niteliğindedir. Anayasa, AİHS ve CMK ayrı ayrı incelendiğinde koruma tedbirlerinin araç olma niteliği açıkça düzenlenmiş olmasa da koruma tedbirlerin varlık amacı göz önüne alındığında araç niteliğinde olduğu görülmektedir²².

¹⁸ Göçmen, s. 26.

¹⁹ Yenisey ve Nuhoglu, s. 323.

²⁰ Yenisey ve Nuhoglu, s. 324.

²¹ Şahin ve Göktürk, CMK-1, s. 268; Muzaffer Korkmaz, **Koruma Tedbirleri Nedeniyle Tazminat Davaları**, Seçkin Yayıncılık, Ankara, 2019, s. 27.

²² Göçmen, s. 46.

1.1.2.4. Suç Şüphelerinin Belli Bir Yoğunlukta Bulunması

1.1.2.4.1. Şüphe Kavramı

Şüphe ile eş anlamlı sözcük olan kuşku²³, Türk Dil Kurumu Sözlüğünde, “*Bir olguyla ilgili gerçeğin ne olduğunu kestirememekten doğan kararsızlık, kuruntu, işkil, şüphe, acaba, şek*” olarak tanımlanmıştır. Ceza Muhakemesi hukukunda ise “*gerçekliği hususunda bazı maddi vakıalar bulunmakla birlikte doğruluğu araştırılıp delillerle ispat edilmeye muhtaç bir durum*” olarak tanımlanmaktadır²⁴.

Ceza muhakemesi hukukunda şüphe soruşturmanın başında delillere dayanan bir tahmin iken²⁵; soruşturma ilerledikçe ve usul hukukunun diğer evrelerine geçtikçe daha da yoğunlaşır.

Ceza muhakemesinde koruma tedbirlerine karar verebilmek için öncelikle olaya dair şüphenin var olması gerekir²⁶. Ancak, her bir ceza muhakemesi aşamasında şüphenin farklı türleri aranmakta ve bir sonraki aşamaya geçilmesinin ön koşulunu oluşturmaktadır²⁷. Ceza muhakemesinde amaç; muhakeme başlamadan önce var olan şüpheyi yok etmektir²⁸. Bu anlamda, Cumhuriyet savcısı suç şüphesini aydınlatarak, delilleri toplamak, koruma altına almak ve yeterli delile ulaştığında kamu davası açmakla görevlidir²⁹.

Öğretide, şüphe kavramı ağırlıkla basit şüphe, makul şüphe, yeterli şüphe ve kuvvetli şüphe olarak ayrıma tabi tutulmuştur.

Soruşturmaya başlarken ilk olarak basit şüphe aranırken, koruma tedbirlerine başvurmak için makul şüphe, yeterli şüphe, kuvvetli şüphe gibi daha yoğun şüpheler aranmaktadır. Hüküm verebilmek için ise, somut olay hakkında kanaatin şüpheden arınmış ve kesinlik kazanmış olması gereklidir.

²³ “Türk Dil Kurumu Sözlüğü”, <https://sozluk.gov.tr/>, (20.02.2022)

²⁴ Eryılmaz, Mesut Bedri, Türk ve İngiliz Hukukunda ve Uygulamasında Durdurma ve Arama , Ankara, 2003, s. 47.’den aktaran; Mehmet Yayla, **Ceza Muhakemesi Hukukunda İspat ve Şüphe**, Seçkin Yayıncılık, Ankara, 2016, s. 115.

²⁵ Öztürk ve diğerleri, CMK, s. 269.

²⁶ Öztürk ve diğerleri, Koruma Tedbirleri, s. 30.

²⁷ Ayça Akpek, **Tutuklamada Kuvvetli Suç Şüphesi**, Seçkin Yayıncılık, Ankara, 2020, s. 50.

²⁸ Mesut Bedri Eryılmaz, **Ceza Muhakemesi Hukuku Dersleri**, Seçkin Yayınevi, Ankara, 2012, s. 42.

²⁹ Metin Yıldırım, **Genel ve Özel Ceza Soruşturması**, 2. baskı, Adalet Yayınevi, Ankara, 2020, s. 106.

Ceza muhakemesinde delil olmaksızın şüpheden söz edilemez. Benzer şekilde, şüphe olmaksızın da muhakeme evresine geçilemez. Nitekim, ceza muhakemesinin başlangıç noktası suç şüphesidir³⁰. Öte yandan; yasa koyucu koruma tedbirleri yönünden tek bir şüpheden bahsetmemiş, her bir koruma tedbiri için, ilgili koruma tedbirinin temel hak ve özgürlüklere müdahale yoğunluğuna göre farklı şüphe çeşitlerini aramıştır³¹.

Çalışmamıza konu koruma tedbiri olan bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kopyalama ve elkoyma yönünden, söz konusu tedbire başvurabilmek adına Kanun koyucu kuvvetli şüphenin varlığını aramıştır.

1.1.2.4.2. Basit Şüphe

Basit şüphe; ceza muhakemesinde yoğunluğu en hafif olan³², *başlangıç şüphesi* olarak da bilinen şüphedir. Bu şüphe çeşidinin dayandığı deliller basit, yetersiz ve/veya sayıca azdır. Soruşturmaya başlanabilmesi için en azından belli yaşanmış olayların, *belirti* şeklinde bulunan delillerin suçun işlendiği yönünde izlenim vermesi gerekir³³. Belirti şeklinde bulunmayan ve belli olaylara dayanmayan şüphe, soruşturma başlatmaya yeterli olmamaktadır³⁴.

Başlangıç şüphesinden bahsetmek için, suç işlendiği izlenimi veren somut vakıalara dayanan halin, *“kriminalistik bilimin ortaya koyduğu tecrübe kurallarına göre kovuşturulabilir nitelikte olan bir suç fiilinin mevcut bulunduğu ihtimalinin”* ortaya konması gerekir³⁵.

CMK md. 160’a göre³⁶; Cumhuriyet savcısının soruşturma başlatabilmesi için *bir suçun işlendiği izlenimi veren bir halin* olması gerektiğini düzenlemiştir. Yasa, soruşturmanın başlatılması için ortaya konan bu durum öğretide şüphe olarak karşılık

³⁰ Öztürk ve diğerleri, CMK, s. 442.

³¹ Öztürk ve diğerleri, Koruma Tedbirleri, s.30.

³² Yayla, s. 118.

³³ Yener Ünver ve Hakan Hakeri, **Ceza Muhakemesi Hukuku**, 15. Baskı, Seçkin Yayıncılık, Ankara, 2019, s. 443.

³⁴ Öztürk ve diğerleri, Koruma Tedbirleri, s. 32.

³⁵ Yenisey ve Nuhoglu, s. 328.

³⁶ CMK md. 160 *“Cumhuriyet savcısı, ihbar veya başka bir suretle bir suçun işlendiği izlenimini veren bir hâli öğrenir öğrenmez kamu davasını açmaya yer olup olmadığına karar vermek üzere hemen işin gerçeğini araştırmaya başlar.”*

bulmuş ve basit şüphe olarak derecelendirilmiştir³⁷. Basit şüphenin tahmine değil olaylara dayanması gerekir. Olaylara dayanmayan şüphe üzerinde soruşturmaya başlanması keyfiyet içerir³⁸.

1.1.2.4.3. Makul Şüphe

Ceza muhakemesi hukukunda bir diğer şüphe türü ise *makul şüphedir*. Kanun koyucu, *makul şüphe* kavramını Kanun ile tanımlamamıştır. Ancak, söz konusu kavramın tanımına Adli ve Önleme Aramaları Yönetmeliği md. 6'da yer verilmiştir. Yönetmeliğe göre *makul şüphe*,

hayatın akışına göre somut olaylar karşısında genellikle duyulan şüphedir. Makul şüphe, aramanın yapılacağı zaman, yer ve ilgili kişinin veya onunla birlikte olanların davranış tutum ve biçimleri, kolluk memurunun taşındığından şüphe ettiği eşyanın niteliği gibi sebepler göz önünde tutularak belirlenir. Makul şüphede, ihbar veya şikâyeti destekleyen emarelerin var olması gerekir. Belirtilen konularda şüphenin somut olgulara dayanması şarttır. Arama sonunda belirli bir şeyin bulunacağını veya belirli bir kişinin yakalanacağını öngörmeyi gerektiren somut olgular mevcut bulunmalıdır.

şeklinde ifade edilmiştir.

Belli koruma tedbirleri yönünden yasa koyucu makul şüphenin varlığını aramıştır. Örneğin, CMK md. 116 ile düzenlenen arama tedbirinde³⁹; kanun koyucu şüpheli veya sanık hakkında arama kararı verilebilmesi için makul şüpheyi şart koşturmuştur.

1.1.2.4.4. Yeterli Şüphe

Soruşturma evresinde toplanan delillerin, suçun işlendiği yönünde yeterli derecede şüphe oluşturmaları durumu ise, CMK md. 170/2'ye göre⁴⁰, Cumhuriyet

³⁷ Centel-Zafer, Ceza Muhakemesi Hukuku, s.80'den aktaran; Değirmenci, **Ceza Muhakemesinde Sayısal (Dijital) Delil**, Seçkin Yayınevi, Ankara, (Sayısal), s. 348.

³⁸ Yenisey ve Nuhoglu, s. 328.

³⁹ CMK md.116; “Yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe varsa; şüphelinin veya sanığın üstü, eşyası, konutu, işyeri veya ona ait diğer yerler aranabilir.”

⁴⁰ CMK md. 170/2; “Soruşturma evresi sonunda toplanan deliller, suçun işlendiği hususunda yeterli şüphe oluştuyorsa; Cumhuriyet savcısı, bir iddianame düzenler.”

savcısı iddianame düzenler. İddianame düzenlenmesi için gerekli olan orta yoğunluktaki⁴¹ bu şüphe derecesi ise, öğretide *yeterli şüphe* olarak adlandırılmaktadır⁴². Cumhuriyet savcısı suçun işlendiğine ilişkin *yeterli şüphesi* bulunmuyorsa, iddianame düzenlemez ve kovuşturmayaya yer olmadığına dair karar verir.

1.1.2.4.5. Kuvvetli Şüphe

Kuvvetli şüphe ise, suçun işlendiğine ilişkin kuvvetli his oluşturacak, delil veya olguların bulunduğu durumu ifade eder. Eldeki bulgulara göre, yargılamada şüpheli/sanığın mahkûm olacağı durumunun kuvvetle muhtemel olması⁴³ anlamına gelir⁴⁴. Eş deyişle; kuvvetli şüphe, somut olgular ya da delillerle desteklenmiş, şüpheli/sanığın suçu işlediği yönündeki mahkûmiyet kararı verilmesi kuvvetle muhtemel olduğu şüphe çeşididir⁴⁵.

Ceza Muhakemesi Kanunu'nda yer alan koruma tedbirlerinin bir kısmında kuvvetli şüphe aranmıştır. Yine, temel hak ve hürriyetleri önemli ölçüde kısıtlamaya sebebiyet veren CMK md. 134'te yer alan koruma tedbirine ilişkin kuvvetli şüphenin aranması yerinde olmuştur.

1.1.2.5. Geçici Nitelikte Olması

Koruma tedbirleri, maddi gerçeğin ortaya çıkarılma sürecinde araç olması itibariyle geçici mahiyettedir. Koruma tedbirlerine başvurulması sonrası maddi gerçeğe ulaşılması halinde ilgili tedbirin derhal sonlandırılması gerekir⁴⁶.

Koruma tedbirlerinin geçici niteliği, bir kısım tedbirler yönünden tedbirin uygulanacağı süre yönüyle değerlendirilmektedir. Örneğin, Kanun gereği yakalama tedbiri en yakın mahkemeye götürülmesi için gereken süre hariç kırk sekiz saatten

⁴¹ Yenisey ve Nuhoğlu, s. 328.

⁴² Öztürk ve diğerleri, CMK, s. 443; Öztürk ve diğerleri, Koruma Tedbirleri, s. 33; Yenisey ve Nuhoğlu, s. 328; Yayla, s. 124.

⁴³ Öztürk ve diğerleri, CMK, s. 443.

⁴⁴ Yayla, s. 126.

⁴⁵ Öztürk ve diğerleri, CMK, s. 271; Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, 8. baskı, Seçkin Yayınevi, Ankara, 2020, s. 583.

⁴⁶ Öztürk ve diğerleri, CMK, s. 444.

veya dört günden fazla süremez⁴⁷. Bu yönüyle, söz konusu tedbirler bakımından belli süreler düzenlenmiş ve geçicilik bu şekilde sağlanmıştır.

Diğer bir kısım tedbirler bakımından ise açıkça düzenlenmiş süre bulunmamakla beraber, söz konusu tedbir başka koruma tedbirine karar verilene kadar yahut hüküm kurulana kadar uygulama alanı bulur. Örneğin, somut olaya ilişkin tutuklama kararı verilince yakalama tedbiri sonlanırken, muhakeme sonucu hüküm kurulduğunda tutuklama tedbiri sona erer⁴⁸.

Bazı tedbirler yönünden ise, tedbiri haklı gösteren sebeplerin yoğunluğunun değişmesi halinde, mevcut tedbir yerini daha ağır ya da daha hafif tedbirlere bırakır⁴⁹. Örneğin; delil karartma şüphesi nedeniyle tutuklama tedbiri uygulanan somut olayda, delil karartma şüphesinin ortadan kalkması ile tutuklama tedbirinin sonlandırılması gerekir.

1.1.2.6. Görünüşte Haklılık

Koruma tedbirlerine, hukuk dünyasında bir hakkın tehlikede olması durumunda başvurulur. Bahse konu hakkın var olup olmadığı uzunca bir araştırma sonucu ortaya çıkabileceğinden, hakkın var olduğuna ilişkin haklı görünüşle yetinilir. Bu durum “*görünüşte haklılık*” ya da “*ihtimal sebepleri*” olarak anılır.

Ceza muhakemesinde ihtimal sebepleri, suçluluk şüphesi sebepleri olarak anılır ve maddi gerçeğe ulaşmak adına isnadın esasına ilişkin araştırmayı gerektirir⁵⁰. Görünüşte haklılık, koruma tedbirinin uygulanması safhasında Kanun’da yer alan şartları taşıdığı hususunda kanaatin oluşmasıdır⁵¹. Muhakeme bir tereddüt ve şüphe safhası olmasının yanında koruma tedbirine başvurmak için mahkûmiyet ihtimalinin yüzde yüz olması gerekmemektedir. Korunmak istenen durumun ileri gerçekleşmesinin muhtemel olması yeterlidir⁵². Mühim olan, koruma tedbirine karar verilmesi ve uygulama anının o an için muhtemel şekilde haklı görünmesi olup mutlak

⁴⁷ Yenisey ve Nuhoglu, s. 324.

⁴⁸ Yenisey ve Nuhoglu, s. 324.

⁴⁹ Yenisey ve Nuhoglu, s. 324.

⁵⁰ Yenisey ve Nuhoglu, s. 324.

⁵¹ Göçmen, s. 43.

⁵² Yenisey ve Nuhoglu, s. 325.

haklılık seviyesine gelmemesidir⁵³. Zira, mutlak haklılık seviyesine muhakeme sonunda varılacaktır⁵⁴. Yine, koruma tedbirine sadece başvururken değil, uygulama süresince de “*görünüşte haklılık*” hususu aranmaktadır. Zira koruma tedbirlerinin uygulanması anında “*görünüşte haklılık*” unsuru ortadan kalkmış ise ilgili tedbir sonlandırılmalıdır.

1.1.2.7. Gecikmesinde Tehlike (Sakınca) Bulunması

Koruma tedbirine başvurulmaması yahut geç başvurulması halinde, muhakemenin hiç veya gerektiği şeklinde yapılamaması ya da hükmün infazının gerçekleşemez duruma gelmesi halinde, gecikmede tehlike bulunduğu kabul edilir⁵⁵. Gecikmesinde tehlike bulunup bulunmaması, her koruma tedbiri ve somut olaya göre ayrı ayrı değerlendirilir. Somut olay değerlendirildiğinde, gecikmesinde tehlike bulunmuyorsa bu tedbirlere başvurulmasına gerek yoktur⁵⁶.

Mevzuatımızda “*gecikmesinde sakınca bulunan hal*” hususu kavramsal olarak Yakalama, Gözaltına Alma ve İfade Alma Yönetmeliğinin tanımlar üst başlıklı 4. maddesinde “*Gecikmesinde sakınca bulunan hâl; derhâl işlem yapılmadığı takdirde suçun iz, eser, emare ve delillerinin kaybolması veya şüphelinin kaçması veya kimliğinin saptanamaması ihtimalinin ortaya çıkması hâlini ifade eder.*” şeklinde tanımlanmıştır.

Hükmün kurulmasından önce, koruma tedbirlerinin temel hak ve özgürlüklere müdahale etmesinden ötürü, ancak zorunlu hallerde koruma tedbirlerine başvurulması mümkündür. Gecikmesi durumunda ortaya çıkacak tehlikenin mümkün olması yetmez, tehlikenin muhtemel olması gerekir⁵⁷. Zira, basit muhtemel bir tehlike yeterli değildir, derhal müdahale edilmediği vakit beklenen zararın ortaya çıkması ihtimalinin varlığını gösteren somut ve fiili hususlarla ortaya konan tehlike söz konusu olmalıdır⁵⁸.

⁵³ Göçmen, s. 43.

⁵⁴ Şahin ve Göktürk, CMK-1, s. 269.

⁵⁵ Şahin ve Göktürk, CMK-1, s. 268.

⁵⁶ Öztürk ve diğerleri, Koruma Tedbirleri, s. 35.

⁵⁷ Yenisey ve Nuhoglu, s. 325.

⁵⁸ Yenisey ve Nuhoglu, s. 325.

1.1.2.8. Orantılılık (Ölçülülük İlkesi) Bulunması

Hukukun pek çok alanında olduğu gibi, koruma tedbirlerine karar verilirken de ölçülülük ilkesi gözetilmelidir. Ölçülülük ilkesi, koruma tedbirine karar verilme sürecinde elde edileceği değerlendirilen yarar ile koruma tedbiri neticesinde ortaya çıkan zarar arasında makul bir denge bulunması gerekliliğidir⁵⁹.

Ölçülülük prensibi, Anayasamızın 13. maddesi ile düzenlenmiştir. Bu vesile ile temel hak ve özgürlüklerin kısıtlanmasında ölçülülük prensibine uyulması bir zorunluluk haline getirilmiştir. Ölçülülük, araçla sağlanmak istenen amacın, yöntemle ile varılmak istenen hedefin arasında denge olmasıdır⁶⁰. Aracın, amaçtan daha değerli olmaması ve aynı amaca daha az değerli araçla ulaşılabiliriyorsa onun tercih edilmesi gerekir.

AİHM, pek çok kararında ulusal uygulamaların ölçülülük ilkesine uygunluğunu denetlemiştir. Kararlarında, *“başvurulan yöntemler ile gözetilen amaç arasında makul bir ölçülülük”* ilişkisini aramış ve bu ölçülülük ilişkisinin aşılması durumunda AİHS ile teminat altına alınmış hakkın ihlal edildiğine hükmetmiştir⁶¹.

Ceza Muhakemesi Hukukunda yer alan koruma tedbirlerinin amacı muhtemel yakın tehlikenin sebep olabileceği zarardan muhakemeyi korumaktır⁶². Bazı durumlarda Kanun koyucu öngördüğü ölçüyü açıkça ortaya koyabilir. Örnek olarak, CMK md. 100/4 gereği, *“sadece adli para cezasını gerektiren suçlarda veya vücut dokunulmazlığına karşı kasten işlenenler hariç olmak üzere hapis cezasının üst sınırı iki yıldan fazla olmayan suçlarda”* tutuklama kararı verilemez. Buna göre, Kanun koyucunun belli cezaları gerektiren suç tiplerinde tutuklama koruma tedbirinin ölçülü olmadığını kıymetlendirmiş ve hâkim ya da Mahkemenin bu tedbire başvurmasını engellemiştir. Yine, vücut dokunulmazlığına karşı işlenen kasten suçları madde kapsamı dışında tutmuştur. Ölçülülük ilkesine ilişkin bir başka açık düzenlemeyi 5395 sayılı Çocuk Koruma Kanun’unda görmekteyiz. Kanun 21. maddeye göre; *“on beş yaşını doldurmamış çocuklar hakkında üst sınırı beş yılı aşmayan hapis cezasını gerektiren fiillerinden dolayı tutuklama kararı verilemez.”* Burada da belli miktarda

⁵⁹ Öztürk ve diğerleri, CMK, s. 445; Öztürk ve diğerleri, Koruma Tedbirleri, s. 37.

⁶⁰ Şahin ve Göktürk, CMK-1, s. 269.

⁶¹ Göçmen, s. 39.

⁶² Yenisey ve Nuhoglu, s. 327.

cezanın altını gerektiren suç tiplerine ilişkin tutuklama kararı verilmesinin ölçülülük prensibine uygun düşmediği değerlendirilmiştir.

Kanun hükmünde açık düzenleme olmasa da her somut olayda ölçülülük ilkesine dikkat edilmesi gerekir⁶³. Ölçülülük değerlendirmesi sadece koruma tedbirine karar verilme anından ibaret değildir. Tedbire karar verilmesinden sonra muhtemel zararın ağırlığı şüpheli/sanık lehine değişirse koruma tedbirinin geri alınması yahut daha hafif derecedeki tedbire karar verilmesi gerekecektir⁶⁴.

1.1.2.9. Yetkili Mercii Kararına Dayanma

Koruma tedbirleri, temel hak ve özgürlükleri kısıtlaması sebebiyle mutlaka belli merciler tarafından verilen karar neticesinde uygulanabilir⁶⁵. Koruma tedbirlerine kural olarak hâkim; bazı istisnai hallerde ise Cumhuriyet savcısı, kolluk amiri karar verir⁶⁶.

Bir kısım koruma tedbirlerine sadece hâkim karar verebilir. Örneğin; tutuklama (md.101/1), taşınmaz hak ve alacaklara elkoyma (md.128/9), adli kontrol (md.110/1), şirket yönetimi için kayyım tayini (md.133/1), avukat bürolarında arama elkoyma ve postada elkoyma (md.130/1), gizli soruşturmacı görevlendirmesi (md.139/1) gibi tedbirlere sadece hâkim kararı gerekir⁶⁷. Hâkimden kasıt; soruşturma aşamasında sulh ceza hâkimi, kovuşturma aşamasında ise Mahkemedir.

Bir diğer kısım koruma tedbirlerinde ise karar verme yetkisi kural olarak hâkimde olmakta ve fakat gecikmesinde sakınca bulunan hallede Cumhuriyet savcısı da karar verebilmektedir. Örneğin; bilgisayarlarda, bilgisayar programları ve kütüklerinde arama, kopyalama ve elkoyma (md.134/1), postada elkoyma (md.129/1), teknik araçlarla izleme (md.140/2), telekomünikasyon yoluyla yapılan iletişimin denetlenmesi (md.135) tedbirlerinde Cumhuriyet savcısı da yetkilidir.

Diğer koruma tedbirlerinde ise hâkim ve Cumhuriyet savcısının yanında Cumhuriyet savcısına ulaşamayan hallerde kolluk amiri de yetkilidir. Arama

⁶³ Öztürk ve diğerleri, Koruma Tedbirleri, s. 37.

⁶⁴ Yenisey ve Nuhoglu, s. 327.

⁶⁵ Öztürk ve diğerleri, Koruma Tedbirleri, s.37.

⁶⁶ Öztürk ve diğerleri, CMK, s. 445.

⁶⁷ Öztürk ve diğerleri, Koruma Tedbirleri, s. 37. ; Şahin ve Göktürk, CMK-1, s. 270.

(md.119/1) ve elkoyma (md.127/1) tedbiri bu kapsamda yer alan tedbirlerdendir. Gözaltı (md.91/1, 4) kararı verme yetkisi ise Cumhuriyet savcısı ve kolluğa aittir.

Koruma tedbirlerine yetkili makamlarca karar verilmiş olması ilk bakışta kanuna uygunluk noktasında karine teşkil etse de asıl dikkate alınması gereken husus tedbir kararın genel ve özel tüm şartlara uygunluk taşımasıdır⁶⁸. Ayrıca gecikmesinde sakınca bulunan hallerde istisnai olarak Cumhuriyet savcısı ve kolluk amirine yetki tanınmış olsa da her somut olay yönünden gecikmesinde ne gibi sakınca bulunduğu ilgili makam tarafından gerekçelendirilmelidir.

1.2. DİJİTAL DELİL

1.2.1. Tanımı

Gelişen teknoloji ile birlikte suç metodolojisi değişmiş ve delillerin elde edildiği ortamlar farklılaşmıştır. Nitekim, yakın gelecekte günlük işlemlerin neredeyse tamamının elektronik ortama aktarılacağını söylemek mümkündür⁶⁹. Kişinin imzasının da dijital ortama aktarılması ve dijital imzanın şartlarının oluşması halinde kâğıda atılan imza ile aynı hükümde olması bu teoriyi doğrulamaktadır.

Geleneksel koruma tedbirleri, yerini modern koruma tedbirlerine bırakmış, buna bağlı olarak delil elde etme yöntemleri de farklılaşmıştır. Geline nokta bilişim sistemleri hayatımızın önemli bir parçası haline gelmiş ve dijital veri ile dijital delil kavramları sıkça kullanılır olmuştur. Zira, günümüzde kimi olaylar dijital delillere başvurulmadan aydınlatılamaz hale gelmiştir⁷⁰.

Dijital veri ile dijital delil sıklıkla birbirinin yerine kullanılsa da farklı anlamlar barındıran kavramlardır. Mevzuatımızda veri kavramı, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un tanımlar üst başlıklı 2. maddesinde “*bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri ifade eder*” şeklinde tanımlanmıştır. Ancak biz bu tanıma yetersiz buluyoruz. Günümüzde, bilgisayar ile

⁶⁸ Korkmaz, s. 28.

⁶⁹ Gülfer Akın, “Belgede Sahtecilik Suçlarının Konusu Olarak Elektronik/Dijital Belge”, **Bilişim Hukuku Dergisi**, Cilt: 3, Sayı: 1, 2021, s. 87.

⁷⁰ Begüm Gürel ve İpek Mengilli, “Dijital Delil Kavramı ve Yargılamadaki Yeri”, **Leges Hukuk Dergisi**, Cilt: 139, 2021, s. 82.

aynı işleve sahip pek çok donanım bulunmaktadır. Örneğin; akıllı telefon, tablet gibi donanımlar oldukça nitelikli cihazlar olarak bilgisayarın tüm kabiliyetlerine sahiptirler. Dolayısıyla, veri kavramını bilişim sistemlerinin tamamını kapsayacak şekilde tanımlanması yerinde olurdu. Burada yer alan veri kavramını esasen dijital veri olarak anlamamız daha doğru olacaktır.

Dijital delil ise dijital veriden daha farklı anlamdadır. Dijital delil, adli bilişime konu bir çalışma esnasında bilgisayar, telefon, tablet gibi bilişim sistemi ve veri barındıran depolama birimleri üzerinden elde edilen adli delillerdir⁷¹. Bir başka deyişle “*iddia edilen bir fiilin ispatında kullanılmak istenen veya kullanılan; elektronik ortamda oluşan/ oluşturulan, değiştirilen, iletilen veya saklanan veri, kayıt ve belgelerdir*”⁷². Dijital delil dijital verinin delil değerine sahip olanıdır. Dijital deliller çeşitli tiplerde bulunmaktadır. Veri dosyaları, silinmiş ancak üçüncü parti yazılımla kurtarılmış dosyalar, CD, DVD, USB bellek gibi TVDO ortamları, akıllı telefon, bilgi sistem LOG kayıtları, bulut bilişim sistemlerinde yer alan veriler, sosyal medya verileri gibi pek çok veriler dijital delile konu olabilir.

1.2.2. Analog Delil ile Dijital Delil Ayrımı

Analog delil, dijital delil ve elektronik delil kavramlarına giriş yapmadan önce elektronik, analog ve dijital kavramını açıklama yerinde olacaktır. Elektronik, *serbest elektronların etkisiyle oluşan olayları inceleyen bilim dalı* olarak tanımlanmaktadır⁷³. Etrafımızda yer alan buzdolabı, televizyon, bilgisayar, cep telefonu gibi pek çok cihazın temelini oluşturur.

Elektronik bilim dalı, *analog ve dijital* olmak üzere iki alt dala ayrılır. Analog ve dijital kavramları esasen iki farklı mantıkta çalışan sinyaldir. Fransızca *analogue* kelimesinden türetilmiş *analog* kavramı, giriş sinyallerinin başkaca sinyaller ile toplama, çarpma gibi işlemlere tabi tutulması sonucu değişiklik gösteren ve başka bir çıkış sinyaline dönüşmesi sonucu elde edilen sinyallerdir⁷⁴. *Dijital* kavramı ise,

⁷¹ Türkay Henkoğlu, **Adli Bilişim**, 2. baskı, Pusula 20 Teknoloji ve Yayıncılık, İstanbul, 2014, s. 5.

⁷² Çetin Arslan, “Dijital Delil ve İletişimin Denetlenmesi”, **Ceza Hukuku ve Kriminoloji Dergisi**, Cilt: 3, Sayı: 2, 2015, s. 255.

⁷³ “Türk Dil Kurumu Sözlüğü”, (07.05.2022).

⁷⁴ Uğur Kaynakçıoğlu, “**Ceza Muhakemesinde Dijital Deliller**”, (Yayınlanmamış Yüksek Lisans Tezi), Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2015, s. 25.

temelde “0” ve “1” değerlerinden oluşan ikili kod sistemi kullanılması neticesinde elde edilir. Temelde “1” değeri, akımın geçme anı olarak ifade edilirken; “0” değeri akımın olmadığı durumdur. İşte bu “0” ve “1” değerlerinin belli bir mantık dizilimiyle arka arkaya sıralanması ile *dijital* sinyal ortaya çıkar. Bu noktada *analog* sinyal ile *dijital* sinyal arasında en temel fark sürekliliktir. Analog sistemler sürekli üretilen *sinüzoidal* sinyal mantığıyla çalışırken *dijital* sistemler kesik kesik sinyal sıralaması ile çalışır. Günümüzde *modülasyon* adı verilen teknik ile her iki sinyalin birbirine dönüştürülmesi de mümkündür.

Analog delil, dijital delil ve elektronik delil sıklıkla birbirinin yerine kullanılan ve karıştırılan kavramlardır. Ancak; elektronik delil, analog ve dijital delil kavramlarını kapsayan daha genel nitelikli üst bir kavramdır. Elektronik delil⁷⁵, *elektronik bir cihaz üzerinde saklanabilen veya bu cihazlar aracılığıyla iletilebilen muhakeme bakımından değeri olan bilgi ve verilerdir*. Analog delil, fotoğraf filmleri, ses kayıt bantları gibi analog sistemlerin ürünü olan delillerdir⁷⁶. Dijital deliller ise, yukarıda açıklanan dijital formda üretilip saklanan verileri içeren delillerdir. Günümüzde çok yaygın şekilde dijital delil bulunmaktadır. Bilgisayar, cep telefonu, tablet, gibi pek çok veri taşıyan cihazlarda dijital delil bulunmaktadır. Ayrıca hukuk düzenimizde maddi gerçeğin ortaya çıkarılması adına sıklıkla dijital delile başvurulmaktadır. Günümüzde, analog delil hayatın pek çok alanından yok olmaya yüz tutmuş olmakla beraber dijital delil varlığını güçlendirerek korumaktadır⁷⁷.

Mevzuatımızda yer alan düzenlemelerde hem *elektronik* hem de *dijital* terimine yer verildiği görülmektedir.

Elektronik terimine yer verilen birtakım düzenlemeler;

- TCK md.6’da “*elektronik kitle iletişim aracı*”, md.105 ve md.297 de “*elektronik haberleşme aracı*” ifadelerine,
- CMK md.38/A “*elektronik işlemler*” üst başlığı tercih edilmiş, madde metninde “*elektronik ortam*”, “*elektronik imza*” terimlerine yer verilmiş,

⁷⁵ Berber, Adli Bilişim, s. 46.den aktaran; Osman Gazi Ünal, “**Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma**”, (Yayınlanmamış Yüksek Lisans Tezi), Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2011, s. 16.

⁷⁶ Oğuzhan Emre Parlak, “**Türk Ceza Muhakemesinde Bilişim Sistemlerinde Arama, Kopyalama ve Elkoyma**”, (Yayınlanmamış Yüksek Lisans Tezi), Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2019, s. 12.

⁷⁷ Değirmenci, Sayısal, s. 130.

- Yine CMK çeşitli maddelerinde *elektronik posta* kavramı kullanılmış,
- 5809 sayılı Elektronik Haberleşme Kanunu, 5070 sayılı Elektronik İmza Kanunu, 6563 sayılı Elektronik Ticaretin Düzenlenmesi Hakkında Kanun gibi pek çok kanunda başlıkta yahut madde metninde elektronik kavramına yer verilmiştir.

Dijital terimine yer verilen düzenlemeler;

- 7194 sayılı Dijital Hizmet Vergisi ile Bazı Kanunlarda ve 375 Sayılı Kanun Hükmünde Kararnamede Değişiklik Yapılması Hakkında Kanun,
- 7252 sayılı Dijital Mecralar Komisyonu Kurulması ile Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanunlarda başlık olarak *dijital* kavramı kullanılmış,
- 7332 sayılı Hayvanları Koruma Kanunu ile Türk Ceza Kanunu'nda Değişiklik Yapılmasına Dair Kanun'da *dijital kimliklendirme* yöntemi düzenlenmiştir.

Dikkat edildiğinde, yakın tarihli düzenlemelerde *dijital* teriminin nispeten yaygınlaştığı görülmektedir. TCK ve CMK'da dijital terimine yer verilmemiştir.

1.2.3. Dijital Delillerin Özellikleri

Sayısal delillerin muhakemede kullanılabilmesi için kendine has birtakım özellikleri bulunması gerekir. Öğretide⁷⁸; akla uygunluk, kabul edilebilirlik, gerçeklik, eksiksiz olma, güvenilirlik, inanılabilirlik, tekrar edilebilirlik bu özellikler arasında sayılmıştır. Ancak esasen bu özelliklerin dijital delilde bulunması için en temelde delil bütünlüğünün sağlanmış olması, eş deyişle delilin orijinalliğinin korunmuş olması gerekir.

En temelde klasik deliller, elle tutulur gözle görülür özelliğe sahipken dijital deliller maddi varlığa sahip değildir. Bu nedenle, klasik delillerde uygulanan; elkoyma, muhafaza altına alma usulleri dijital delillerde farklılık gösterecektir.

Dijital delilleri barındıran veri depolama ortamları fiziksel olarak görünür durumda iken, cihaz üzerindeki veriler soyut durumdadırlar. Dijital deliller yalnızca kendini bünyesinde barındıran veri depolama ortamıyla anlamlı hale gelirler⁷⁹. Bu

⁷⁸ Gürel ve Mengilli, s. 83; Cemal Araalan, “Digital Evidence in Turkish Law Türk Hukukunda Dijital Deliller”, **GSI Articletter**, Cilt: 203, 2015, s. 204.

⁷⁹ Ünal, s. 17; Değirmenci, Sayısal, s. 132; Resul Göksoy, **Ceza Muhakemesinde Dijital Delillerin Elde Edilmesi ve Güvenilirliğinin Sağlanması**, Seçkin Yayıncılık, Ankara, 2019.

nedenle, söz konusu delillerin toplanması saklanması ve değerlendirilmesi sürecinde kendine has yapısı dikkate alınmalı ve titizlikle davranılmalıdır.

Sayısal delillerin klasik delillere nazaran hem avantajlarının hem de dezavantajlarının olduğunu söylemek mümkündür.

Sayısal deliller klasik delillere göre; tahrif edilme ve değiştirilme olanağı çok daha yüksektir⁸⁰. Geline nokta, bilişim sistemleri yerel alan ağı ve geniş alan ağı ile birbirine her an bağlantılı hale gelmiştir. Pek çok bilişim sistemi ve buna bağlı olarak dijital veri uzaktan erişime açık hale gelmiş ve sistemler arası senkronizasyon sağlanmıştır. Sayısal verilerin çok önemli kısmı bulut bilişim sistemlerinde saklanmaktadır. Bu husus, beraberinde suç delillerine üçüncü kişilerce her an müdahale edilmesinin önünü açmış, dijital delile ilişkin güvenilirlik problemini ortaya çıkarmıştır.

Sayısal deliller bulunduğu ortamda diğer verilere göre çok fazla olmakla⁸¹ beraber suça konu veri ile ilgili ilgisiz pek çok veri ile bulunmaktadır. Bu nedenle, suça konu verinin ayrıştırılması güç hale gelebilmektedir. Yine, suça konu verinin aranması sürecinde bilişim cihazlarında kişisel veriye nüfuz edilebilmektedir. Bu bağlamda, suça konu verinin diğer verilerin arasında aranması sürecinin titizlikle yürütülmesi ve konu dışı verilere müdahalede bulunulmaması gerekir.

Dijital deliller klasik delillere nazaran dış etkilerden kalıcı olarak etkilenmesi daha olanaklıdır. Dijital veri barındıran cihazın, düşürülmesi yanlış voltajda elektrik verilmesi elektromanyetik dalga, aşırı ısınma gibi dış ortam etkilerinden kolaylıkla etkilenerek kalıcı zarar görebilir⁸².

Kötü niyetli kişilerce dışarıdan yapılan müdahaleler klasik delillerde tespit edilmeye daha müsaitken dijital delillerde bu husus oldukça zordur⁸³.

Dijital delillerin kendine has bir kısım avantajları da bulunmaktadır. Fiziksel delillerin inceleme yapılarak tükenebilmesine⁸⁴ karşın, sayısal deliller, yedek alınabilen ve yedeği üzerinde inceleme yapılabilen delillerdir⁸⁵. Alınan bu yedekler

⁸⁰ Değirmenci, Sayısal, s. 133.

⁸¹ Burak Çekiç, "Bilgisayar Verilerinde Arama, Kopyalama, Elkoyma Tedbirinin Hukuki Niteliği ve Benzer Kavramlar", **Tekirdağ Namık Kemal Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 2021, Sayı: 1, 2021, s. 157.

⁸² Gürel ve Mengilli, s. 88.

⁸³ Gürel ve Mengilli, s. 89.

⁸⁴ Değirmenci, Sayısal, s. 314.

⁸⁵ Haydar Yener Arıcı, **Adli Bilişim**, Seçkin Yayıncılık, Ankara, 2018, s. 51.

uygun muhafaza koşullarında süresiz saklanabilir. Böylece, muhakeme sonuna kadar delillerin muhafaza altına alınması sağlanmaktadır.

Dijital delillerin bir diğer özelliği, delilin kasten ya da sehven silinmesi durumunda dahi delile ulaşılmasının mümkün olmasıdır⁸⁶. Gerçekten de uygun yazılımlarla silinen verilerin dahi geri getirilmesi mümkündür. Hatta, donanımsal arızalarda, verinin bulunduğu disk alanına zarar gelmemesi halinde verinin geri getirilmesi sağlanmaktadır.

Sayısal delillerde diğer delillerde bulunmayan birtakım üst veriler (meta data) bulunur. Bu üst verilerde verinin adı, verinin boyutu oluşturulma tarihi, oluşturanın adı gibi bilgiler yer alır⁸⁷. Bu üst veriler soruşturmada değerlendirilecek ve sayısal delilin bir parçası olarak kıymetlendirilecektir⁸⁸.

Avrupa Konseyi Elektronik Delil Elde Etme Rehberinde de dijital delillerin özelliklerine ilişkin çeşitli tespitlerde bulunulmuştur. Buna göre, dijital deliller klasik delillerin pek çok özelliğini taşımakla beraber ayrıca kendine has birtakım özellikler de barındırmaktadır. Bu özellikleri şu şekilde ele alabiliriz⁸⁹.

Öncelikle, dijital deliller alanında uzmanlaşmış kimseler haricinde görünmezdir. Eş deyişle, uzman olmayan kimse nereye bakacağını bilmezken konunun eğitimini almış profesyonel kimseler uygun yaklaşımla dijital delili elde edebilecektir.

Klasik delillere nazaran dijital deliller yok olmaya oldukça elverişlidir. Örneğin, bilgi sistemlerinde RAM adı verilen bellekte yer alan veriler bilgi sisteminin her açılışında kendiliğinden yok olmakta ve sistem açık kaldığı sürece oluşturulan yeni veriler eski verilerin üzerine yazılmaktadır.

Dijital deliller normal kullanım esnasında da kendiliğinden değiştirilebilir ya da yok edilebilir. Örneğin, bilgisayar çalışma esnasında veriler otomatik ya da kullanıcı eliyle geçici bellekten kalıcı belleğe geçiş yapabilir.

⁸⁶ Arıcı, s.51.

⁸⁷ Çekiç, 156.

⁸⁸ Şenel Sarsıkoğlu, “Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı”, **Türkiye Adalet Akademisi Dergisi**, Cilt: 0, Sayı: 22, 2015, s. 520.

⁸⁹ EUROPEAN UNION, “Electronic Evidence Guide a Basic Guide for Police Officers, Prosecutors and Judges”, Cybercrime Division - Directorate General of Human Rights and Rule of Law, 2014, https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf, (22.03.2022), ss. 10, 11.

Dijital delilleri, tahrif etmeden yedeklemek mümkündür. Dijital deliller orijinali ile aynı şekilde süresiz olarak birden fazla yedeklenebilir, her bir yedek üzerinde bağımsız şekilde çalışma gerçekleştirilebilir.

1.2.4. Dijital Delilin Ceza Muhakemesinde Yeri

Ceza muhakemesinde amaç, *maddi gerçeğin* ortaya çıkarılmasıdır. Bu bağlamda, maddi gerçeğin ortaya çıkarılması için mahkeme belli delillere bağlı kalmadan, her türlü delilin değerlendirebileceği *delil serbestliği* ilkesi benimsenmiştir⁹⁰. Ceza muhakemesinde delil serbestliği ilkesi, CMK md.217/2 “*Hâkim, kararını ancak duruşmaya getirilmiş ve huzurunda tartışılmış delillere dayandırabilir. Bu deliller hâkimin vicdanî kanaatiyle serbestçe takdir edilir*” şeklinde düzenlenerek mevzuatta yerini almıştır.

Yargıtay bir kararında⁹¹, elde edilen bulguların delil olarak nitelendirilmesi adına belli bir çerçeveye çizmiştir. “*Gerçek; akla uygun ve realist, olayın bütünü veya bir parçasını temsil eden kanıtlardan veya kanıtların bir bütün olarak değerlendirilmesinden ortaya çıkarılmalıdır. Yoksa birtakım varsayımlara dayanılarak sonuca ulaşılması ceza yargılamasının amacına kesinlikle aykırıdır.*” Buna göre; delil, maddi vakıa ile ilişkili olmalı ve delilin doğruluğu gerçekliği hususunda şüphe duyulmamalıdır⁹².

Söz konusu ilke, dijital deliller yönünden de geçerlidir. Dijital delillerin çok fazla olması karşısında tüm delillerin birlikte değerlendirilmesi gerekir. Ayrıca, dijital delilin hükme esas alınabilmesi için; öncelikle Anayasa md. 38/6, CMK md. 206/2, 217 gereği hukuka uygun yollarla elde edilmiş olması gerekir.

Ceza muhakemesinde bazı vakıalar dijital delile başvurmaksızın çözüme kavuşmamaktadır. Bazı vakılarda ise; hâkim, savcı ve kolluğun suçu aydınlatmasında kolaylaştırıcı etkisi bulunmaktadır. Bu anlamda dijital deliller klasik delillere göre daha çok tercih edilir konuma gelmiştir⁹³.

⁹⁰ Özbek ve diğerleri, s. 77; Erdem ve diğerleri, s. 365.

⁹¹ Yargıtay CGK, 22.11.2018 tarih, 2017/723 E., 2018/562 K. Sayılı Kararı.

⁹² Dülger, s. 605.

⁹³ Gürel ve Mengilli, s. 82.

Elektronik delil, genel delil sistemi içinde yer alan bir tür delil formudur. Delil çeşitlerini belge, beyan, belirti delili olarak ayırma tabi tuttuğumuz varsayımında; elektronik delil somut olaya göre belge ya da belirti delili olarak nitelendirilebilir⁹⁴.

Bilişim sistemlerinden elde edilen delillere ilişkin adli tahkikat yürütülürken iki husus üzerinde durulması önemlidir. Bunlar; davayla ilgili toplanan elektronik delillerin güvenilir olup olmadığı hususu ile kolluk kuvvetinin elektronik delillerin toplanıp getirilmesi sırasında uygulanan işlemlerin güvenilir olup olmadığı hususudur⁹⁵. Bu anlamda dijital delilin söz konusu özelliklerinin var olmasının en temelinde delil bütünlüğünün korunması gelir. Nitekim dijital deliller siber saldırılara açıktır. Bu husus, dijital delillere ilişkin bilinen en zayıf yanıdır. Geçmişten günümüze siber saldırılar incelendiğinde, ülkelerin güçlü bir şekilde korudukları kritik altyapı sistemlerine bile oldukça önemli siber saldırılar yapılmış ve bunların bir kısmı başarılı olmuştur. Bu anlamda, dijital delillerin siber saldırıya açık olduğu ve dijital delil bütünlüğünün değerlendirmesinde söz konusu hususun göz önünde bulundurulması gerektiği unutulmamalıdır.⁹⁶

1.2.5. Dijital Delil Elde Etmede Başlıca Standartlar ve İlkeler

Dijital delillerin klasik delillere nazaran kendine has yapısı bulunmakla beraber bu delillerin elde edilmesi süreci de farklıdır. Dijital delillerin elde edilme sürecine ilişkin ulusal ve uluslararası düzeyde çeşitli çalışmalar yapılmış belli ilkeler ortaya konarak uygulayıcılara rehber oluşturulmaya çalışılmıştır.

1.2.5.1. AK Elektronik Delil Elde Etme Rehberi

Avrupa Konseyi tarafından kolluk, savcı ve hakimler için temel elektronik delil elde etme rehberi, Mart 2013'te tamamlanmış; Aralık 2014 ise, ikinci basımı

⁹⁴ Değirmenci, Sayısal, s. 130.

⁹⁵ Ali Karagülmez, **Bilişim Suçları ve Soruşturma Kovuşturma Evreleri**, 5. baskı, Seçkin Yayıncılık, Ankara, 2014, s. 607.

⁹⁶ Örneğin, 2000 yılında Avusturya'da eski bir çalışan bir kısım atık istasyonunun komutasına izinsiz şekilde girerek yaklaşık bir milyon litrelik atığı nehre yönlendirmiş, yine 2010 yılında İran nükleer enerji altyapısı *stuxnet* isimli kötücül yazılımla saldırıya uğramıştır. Muhammet Karaca ve Ensar Gül, "Kritik Altyapılara Yönelik Bilişim Suçları, Türkiye ve AB Uygulamaları", **Bilişim Hukuku Dergisi**, Cilt: 3, Sayı: 1, 2021, ss. 6, 7.

gerçekleşmiştir. Rehberin amacı, elektronik delil elde etme sürecinde adım adım uygulanacak liste oluşturmaktan ziyade genel ilkeler ortaya koymaktadır⁹⁷.

AK Elektronik Delil Elde Etme Rehberinde dijital delilin elde edilme sürecinde dijital delile ilişkin bir takım temel ilkeler belirlenmiştir. Günümüz ihtiyaçlarına göre söz konusu ilkelerin belirlendiği ve fakat gelişen teknoloji ile birlikte bu ilkelerin dönüşüme uğrayabileceği belirtilmiştir.

Rehberde yer alan ilk ilke veri bütünlüğüdür. İlkeye göre, mahkemede yargılamaya konu olacak herhangi bir dijital veri ya da cihaza verileri değiştirecek herhangi bir yazılımsal ya da donanımsal müdahalede bulunulmamalıdır. İlkeye göre, dijital delilin bütünlüğünden olay yerinde görev yapan kolluk sorumludur.

İkinci ilkeye ise denetim izi adı verilmiştir. Bu ilkede amaç kolluk kuvvetinin dijital delile ilişkin işlemlerinin denetlenebilir kılınmasıdır. Dijital delile ilk temastan işlem sona erene kadar yapılan her işlem kayıt altına alınmalıdır. Bu vesile ile sonradan üçüncü kişilerin aynı deliller üzerinde aynı işlemleri gerçekleştirerek aynı hukuki sonuca ulaşabilmeleri teyit edilir.

Bir diğer ilke ise uzman desteğinin sağlanmasıdır. Koruma tedbirinin gerçekleştirilmesi esnasında dijital delile müdahale edileceği öngörülüyor ise olay yerine bilişim sistemlerine müdahale konusunda uzman bir kolluk görevlisi götürülmelidir. Bu uzman kişinin alanında tecrübeli, kanunun tatbik edilmesine hâkim, iletişim konusunda bilgili olması beklenir.

Yeterli eğitim olarak adlandırılan ilkeye göre ise, olay yerine alanında uzman kişilerin götürülememesi durumunda, ilk müdahalede bulunacak kolluğun dijital delilleri arayıp uygun usullerle müdahalede bulunacak yetkinliğe ulaşacak eğitime tabi tutulması gerekir.

Rehberde yer alan son ilkeye göre ise, dava sürecinde görevli tüm kişi ve kurumlar, delil güvenliğine genel adli bilişim kurallarına ve kanun hükümlerine uygun davranmalıdır.

⁹⁷ EUROPEAN UNION, “Electronic Evidence Guide a Basic Guide for Police Officers, Prosecutors and Judges”, Cybercrime Division - Directorate General of Human Rights and Rule of Law, 2014, https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf, (22.03.2022), s.8.

1.2.5.2. ABD Gizli Servis Dijital Delile El Koyma Rehberi

Söz konusu rehber ABD gizli servisi ve ABD'nin çeşitli eyaletlerinde yer alan kolluk kuvvetlerinin ortak çalışmasıyla hazırlanmıştır. Rehber, kolluk kuvvetlerinin dijital delillere yaklaşımının uygun usullerle sağlanmasını amaçlamıştır. Dijital delillere yaklaşım ilkeleri olarak nitelendirilebilecek altın kurallar belirlenmiştir.

Söz konusu altın kurallar, mümkün olduğunca dijital delillere uzman personel tarafından müdahale edilmesi, bilişim sistemlerine uygulanacak koruma tedbirlerine ilişkin yasal dayanak olması, bilişim sistemi kapalı ve açık olmasına yönelik özel müdahalede bulunulması, bilişim sisteminin otomatik şekilde delil imha etmeye programlandığına ilişkin şüphe bulunması durumunda derhal güç kablusunun çekilmesi suretiyle bilişim sisteminin kapatılması gerektiği, olay yerinde bulunan koruma tedbirine konu bilişim sisteminin konumu, ekranını alacak şekilde ayrıntılı şekilde fotoğraf çekilmesi şeklinde sıralanmıştır⁹⁸.

1.2.5.3. ACPO Sayısal Delillere İlişkin İyi Uygulama Rehberi

ACPO 1948 yılında İngiltere, Galler ve Kuzey İrlanda ülkeleri nezdinde kurulmuş olan, kolluk uygulamalarını geliştirmeyi amaçlamış, kamu yararına çalışan kuruluştur. 2015 yılında yerini NPCC'e bırakan kuruluş, dijital delillere uygun yaklaşımı geliştirmek amacıyla 1998 yılında bir rehber hazırlamış ve 2011 yılında son sürümü yayımlamıştır⁹⁹.

Söz konusu rehberde dijital delillere müdahalelere ilişkin dört temel ilkeye yer verilmiştir. Rehberde yer alan ilkeler; dijital delillere erişim, müdahale ve elkoyma ile ilgili uyulması tavsiye edilen temel kuralları içermektedir.

Rehberde yer alan ilk ilke verilerin güvenliğine ilişkindir. Bu ilkede yargılamaya konu olacak dijital delile ilişkin verilerin kolluk kuvveti tarafından

⁹⁸ U.S. Secret Service, "Best practices for seizing electronic evidence v.4.2", 2007, <https://www.cwagweb.org/wpcontent/uploads/2018/05/BestPracticesforSeizingElectronicEvidence.pdf>, (15.11.2021), s. 2.

⁹⁹ Janet Williams, "ACPO Good Practice Guide for Digital Evidence", ACPO, Association of Chief Police Officers, 2011, https://www.npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence_Vers%205_Oct%202011_Website.pdf, (03.10.2022).

kesinlikle değiştirilmemesi gerektiği ifade edilmektedir. Rehber bu ilke ile veri bütünlüğünün sağlanmasını amaçlamaktadır.

İkinci ilke de ise, dijital delilin orijinaline temas edecek kişinin yetkin olması gerektiği ifade edilmiştir. İlkede aynı zamanda dijital delile temas edecek kişinin bu delile temas etmenin gerekliliğini ve delile erişimin sonuçlarını açıklayabilir olması gerektiği yer almaktadır. Kanaatimizce, ilkede olay mahallinde yapılacak her türlü işlemin ayrıntılı şekilde tutanak altına alınmasının gerekliliği değerlendirilmiştir.

Üçüncü ilke de, dijital delile yapılan tüm müdahalelerin kayıt altına alınması gerekliliği düzenlenmiştir. Dijital delile yapılacak müdahalelerin kayıt altına alınması, söz konusu işlemlere ilişkin şüphe olması durumunda, tüm işlemlerin baştan tekrar edilmesi sağlanacaktır.

Son ilke de ise dijital delile müdahale eden kolluk görevlilerinin sorumluluğu düzenlenmiştir. İlgili kolluk görevlisi ve uzman personel delillere müdahale ederken tüm sorumluluğu üstlenmesi ve söz konusu ilkelere bağlı kalması gerekir.

Horsman¹⁰⁰, ACPO ilkelerin günümüz ihtiyaçlarını karşılayıp karşılamadığına ilişkin bir inceleme makalesi kaleme almıştır. Yazar, ACPO ilkelerin 2010 yılında ortaya konduğunu, o tarihten bu yana herhangi bir güncellemede bulunulmadığını ve fakat teknolojinin anılan yıldan bu yana hızlı bir gelişim sergilediğini bu anlamda ilkelerin içinde bulunduğumuz çağın gerisinde kaldığını değerlendirmiştir.

1.3. BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA, KOPYALAMA VE ELKOYMA

CMK md. 134 kapsamında yer alan bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyala ve elkoyma koruma tedbiri, esasen üç ayrı koruma tedbirini barındırmaktadır. Bu üç koruma tedbirinin uygulamasını ayrıntılı şekilde düzenleyen yasa maddesi bulunmamaktadır. Öğretide, aşağıda yer alan şekilde tasniflemeye yer verilmiştir¹⁰¹.

- *Arama tedbiri yönünden yapılabilecek işlemler: verilere erişme, verilerde arama, şifre bulma, silinen verileri geri getirme, kriptolu verileri*

¹⁰⁰ Graeme Horsman, “ACPO principles for digital evidence: Time for an update?”, **Forensic Science International: Reports**, Cilt: 2, Sayı: 100076, 2020, s. 2.

¹⁰¹ Çekiç, s. 161.

deşifre etme, veri kurtarma, veri çıkarma (Extracting), verilerin ilişkilerini, aidiyetini belirleme, analiz etme, yorumlama, raporlama ve sunum.

- *Kopyalama tedbiri kapsamında icra edilebilecek işlemler: adli kopya (imaj) alma, verilerin bütünlüğünü, doğruluğunu, güvenilirliğini koruma, veri bütünlüğü değeri hesaplama (HASH değerleri alma), verilere el koyma, alınan adli kopyadan bir suretini şüpheli veya müdaftine verme.*

- *El koyma tedbiri kapsamında icra edilebilecek işlemler: donanımlara elkoyma, delil toplama, koruma, delil zinciri oluşturma, delilleri uygun şekilde paketleme, nakletme ve saklama.*

Bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirini uygularken her bir koruma tedbiri kapsamında icra edilebilecek işlemleri belirlemek gereklidir. Söz konusu işlemlerin de karşılaştırmalı hukukta yer alan terimlerle ilişkilendirilerek terim birliğinin ortaya konması gereklidir. Nitekim, bilişim sistemlerine ilişkin uygulanan tedbirlerin uluslararası niteliği bulunmaktadır.

1.3.1. Tedbirin Amacı

Ceza Muhakemesi Hukukunun amacı, maddi gerçeğin araştırılması ve failin cezalandırılmasıdır¹⁰². Koruma tedbirleri, genel olarak delil elde etme sürecinde araç olarak kullanılır¹⁰³. CMK md. 134 ile düzenlenen çalışmamıza konu tedbirin amacı ise, klasik arama ve elkoyma tedbirlerinde olduğu gibi suça ilişkin delil elde etmektir. Esasen, bilgisayarlarda arama, kopyalama ve elkoyma; klasik arama ve elkoyma tedbirinin özel bir şeklidir¹⁰⁴. Bu anlamda, CMK md. 134 kapsamında yer alan koruma tedbirinin amacı, bilişim sistemlerinde yer alan delillerin elde edilmesidir¹⁰⁵.

Bilişim sistemleri, insan yaşamının hemen hemen her alanına girmiştir. Bilgisayarda yer alan verilere erişimin engellenmesi, bu verilerin kolaylıkla değiştirilebilmesi ve ortadan kaldırılması oldukça kolaydır¹⁰⁶. Bu nedenle, bilişim sistemlerinde yer alan delillere ilişkin özel bir koruma tedbiri düzenlenmesine ihtiyaç

¹⁰² Özbek ve diğerleri, s. 41.

¹⁰³ Cumhuriyet Şahin, “Ceza Muhakemesinde Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma”, **Yaşar Hukuk Dergisi**, Cilt: 1, Sayı: 2, 2019, s. 271.

¹⁰⁴ Özbek ve diğerleri, s. 387.

¹⁰⁵ Muharrem Özen ve Gürkan Özocak, “Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)”, **Ankara Barosu Dergisi**, Cilt: 73, Sayı: 1, 2015, s. 62.

¹⁰⁶ Özbek ve diğerleri, s. 391.

duyulmuştur. Bilişim sistemlerine özgü koruma tedbirinin yasal zeminin oluşturulması, gelişen teknoloji ile suçla mücadele etme konusunda daha sistematik araçlar kullanımını sağlayacak, aynı zamanda suçun tarafı olabilecek kişilerin temel hak ve özgürlüklerinin korunmasında önemli kazanım elde edilecektir.

Ceza Muhakemeleri Usulü Kanunu (CMUK) döneminde, bilişim sistemlerine özgü koruma tedbiri bulunmamaktaydı. Bu sebeple, bilişim sistemlerinde arama ve elkoyma usulleri genel hükümlere göre yapılmaktaydı¹⁰⁷. Ancak, bilgisayar verileri, maddi dünyada elle tutulur gözle görülür olmadığından, kendine has muhakeme usulüne ihtiyaç duyulmuştur. Bu vesile ile, yeni Ceza Muhakemesi Kanununda bilişim sistemlerine yönelik özel bir koruma tedbiri düzenlenerek, kanaatimizce bir eksiklik giderilmiş, elektronik ortamda saklanıp korunan verilerin muhakemede delil olarak kullanılması kolaylaştırılmış ve sistematik hale getirilmiştir¹⁰⁸.

1.3.2. Tedbirin Kapsam ve Konusu

Ceza Muhakemesi Kanununda yer alan arama; konutta, işyerinde, araçlarda yapılabileceği gibi üst araması şeklinde de gerçekleştirilebilir. Elkoyma ise, bu arama neticesinde elde edilen suçta kullanılmış ya da suçu aydınlatabilecek eşyaların mülkiyetinin sonlandırılmasıdır. CMK md. 134'te yer alan koruma tedbiri; genel arama ve elkoyma tedbirine göre, kişi ve konu yönünden daha sınırlı ve daha özgü bir koruma tedbiridir.

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbiri, genel arama ve elkoyma tedbirinden ayrıldığı başlıca husus; koruma tedbirinin konusudur¹⁰⁹. Söz konusu tedbirin konusu “*bilgisayarlar*”, “*bilgisayar programları*” ve “*bilgisayar kütükleri*”dir.

“*Bilgisayar*”, “*bilgisayar programları*” ve “*bilgisayar kütükleri*” Kanunda açıkça tanımlanmamıştır. Adli ve Önleme Aramaları Yönetmeliğinde, CMK md.134'e ek olarak; “*bilgisayar ağları*”, “*uzak bilgisayar kütükleri*” ve “*çıkarılabilir donanımların*” elkoyma tedbirine konu olabileceği düzenlenmiş ve fakat bu kavramların tanımına da Yönetmelikte yer verilmemiştir.

¹⁰⁷ Değirmenci, Sayısal, s. 314.

¹⁰⁸ Yenisey ve Nuhoğlu, s. 428.

¹⁰⁹ Özbek ve diğerleri, s. 390.

Günümüzde, bilgisayarlar ile aynı işlevi gören, pek çok donanım bulunmaktadır. Kanun koyucu, madde metninde, koruma tedbirinin konusunu oluşturan birtakım unsurları doğrudan sıralamıştır. Bunlar; “*bilgisayar*”, “*bilgisayar programları*” ve “*bilgisayar kütükleri*”dir. Ancak, geline nokta Kanunda doğrudan yer verilmese de bilgisayar ile aynı özelliği taşıyan bilgisayar mahiyetinde bulunan pek çok cihaz bulunmaktadır. Bu anlamda uygulamada, akıllı telefonlar, GPS cihazları, verileri dijital işleyip saklama özelliğinde olan tüm donanımlar CMK md.134 kapsamında değerlendirilmektedir. Öte yandan, iç ağlar, veri tabanları, sunucular, bulut bilişim sunucuları, ağ anahtarlama cihazları, uç anahtarlama cihazları da madde kapsamında değerlendirilmektedir¹¹⁰.

Çalışmamızda ayrıntılı şekilde inceleneceği üzere, dijital veri üreten cihazların bir kısmı CMK md. 134 kapsamında değerlendirilmekteyken, diğer kısmı bu madde kapsamında yer almamaktadır.

Kanunda yer alan madde metnine göre; bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbiri, soruşturma evresinde şüpheli yönünden başvurulabilecek koruma tedbiridir. Ancak, uygulamada kovuşturma evresinde sanık yönünden de uygulanmakla beraber öğretide görüş birliği bulunmamaktadır.

1.3.2.1. Kişi Yönünden

1.3.2.1.1. Şüpheli ve Sanık

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirine başvurulması için öncelikle ortada suç soruşturması ve buna bağlı olarak şüpheli sıfatı taşıyan kişi/kişiler bulunması gerekir. Söz konusu tedbir, madde metninde açıkça şüpheliye yönelik düzenlenmiştir.

Öğretide, koruma tedbirinin yalnızca soruşturma evresinde şüpheli hakkında uygulanabileceğini savunan yazarlar çoğunlukta olmakla beraber, kovuşturma evresinde sanık yönünden de uygulanabileceği savunan yazarlar da bulunmaktadır.

¹¹⁰ Cengiz Tanrıkulu, **Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma**, (Yayınlanmamış Doktora Tezi),Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2014, s. 358.

Ünver ve Hakeri'ye göre¹¹¹; CMK md. 134'te yer alan düzenleme gereği, kovuşturma evresinde sanığın mülkiyetinde olan ya da kullandığı bilgisayara ilişkin arama ve elkoyma tedbirine başvurulamaz.

Şen/Eryıldız'a göre¹¹²; CMK md. 134'te sadece “*soruşturma aşaması*” ve “*şüphelinin*” kullandığı cihazlardan bahsedilmektedir. Bu anlamda, söz konusu tedbir kanunilik ve belirlilik ilkesi gereği, sadece soruşturma aşamasında şüpheli hakkında uygulanabilir¹¹³.

Nitekim, Kanun koyucunun açık düzenlemesi karşısında öğretide aksi kanaatte olan yazarlar da bulunmaktadır. Şahin/Göktürk'e göre¹¹⁴; yargılama esnasında delil toplamaya engel olacak hüküm olmaması nedeniyle bahse konu tedbire kovuşturma evresinde sanık yönünden de kıyasen başvurulabilir. Değirmenci'ye göre¹¹⁵, ceza muhakemesinin kendisine yüklenen işlevi doğrultusunda söz konusu tedbire kovuşturma evresinde sanık yönünden de başvurulabilir.

Genel arama tedbirinin düzenlendiği CMK md. 116'ya göre; arama tedbirine “*şüpheli veya sanık*” yönünden başvurulabileceği açıkça yer verilmiştir. Yine, taşınmazlara, hak ve alacaklara elkoyma tedbirini düzenleyen CMK md. 128'in de “*şüpheli veya sanık*” hakkında uygulanabileceği açıktır.

Benzer nitelikte koruma tedbirlerini düzenleyen bu maddelerin şüpheli veya sanık hakkında uygulanabileceği açık şekilde yer almaktayken; bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kopyalama ve elkoyma tedbirinin kovuşturma evresinde sanık hakkında uygulanabileceği açıkça düzenlenmemiştir. Kanaatimizce, kanunilik ilkesi gereği, söz konusu tedbir kovuşturma aşamasında sanık hakkında uygulanamaz. Ancak bu durum kovuşturma evresinde bir eksiklik meydana getirecektir. Nitekim, mahkeme iddianameyi kabul ettikten sonra, kovuşturma evresinde delil toplanması gerekebilir. Bu durumda, CMK'ya göre klasik arama ve elkoyma tedbirine başvurmak hukuka uygun ve fakat bilgisayarlarda bilgisayar programlarında ve kütüklerinde arama tedbirine başvurmak hukuka aykırı olacaktır. Bu durum, bilişim sistemlerine özgü koruma tedbirinin varlık amacına ters

¹¹¹ Ünver ve Hakeri, s. 937.

¹¹² Ersan Şen ve H. Sefa Eryıldız, **Elkoyma**, Seçkin Yayıncılık, Ankara, 2017, s. 204.

¹¹³ Benzer görüş için bkz. Hüsnü Aldemir, **Adli Önleme Arama ve Elkoyma**, 2.baskı, Seçkin Yayınevi, Ankara, 2018, s.179; Öztürk ve diğerleri, CMK, s.213.

¹¹⁴ Şahin ve Göktürk, CMK-1, s. 355.

¹¹⁵ Değirmenci, Sayısal, s. 318.

düşmektedir. Bu anlamda söz konusu boşluğu dolduracak yasal düzenleme yapılması elzemdir.

Tedbire konu, bilişim sistem cihazı her durumda şüphelinin mülkiyetinde olmayabilir. Şüpheli, üçüncü kişinin mülkiyetinde olan bir cihazı kiralamış ya da ödünç almış ve buna bağlı kullanmış da olabilir. Yine, şüpheli kamu kurum ve kuruluşunda görev yapıyorsa, buradaki kamu malı olan bilgisayarı da kullanmış olabilir. Bu durumda, şüphelinin kullandığı üçüncü kişinin ya da devletin mülkiyetinde olan bilişim sistem cihazı hakkında CMK md. 134'te yer alan koruma tedbirine başvurulabilir. Tedbire başvurulmasında nihai amaç, arama ve elkoyma işlemi neticesinde delil elde edilmesidir. Tedbire konu bilişim sistem cihazının şüpheliye ya da üçüncü kişiye ait olmasında fark bulunmamaktadır¹¹⁶. Bu noktada; önemli olan husus, arama ve elkoyma işlemine konu bilgisayarın şüpheli tarafından kullanılmış olmasıdır. Eğer, şüpheli üçüncü kişiye ait bilgisayarı kullanmamışsa, bu durumda CMK md. 134 hükümleri uygulanamaz¹¹⁷. Yargıtay; konuya ilişkin değerlendirmede bulunduğu bir kararında¹¹⁸; şüpheli/sanığın kullanması koşuluyla üçüncü kişinin mülkiyetinde olan bilişim sistemi hakkında arama kararı verilebileceğine hükmetmiştir. Kanaatimizce Yargıtay'ın hükmü yerindedir.

CMK md.134 metninde, “*şüphelinin kullandığı*” bilişim sistemlerini kapsam altına almıştır. Şüphelinin bilgisayarı kullanması, fiziken olabileceği gibi uzak masaüstü bağlantısı gibi sanal kullanım şeklinde de gerçekleşebilir. Bu noktada, maddenin uygulanmasına ilişkin herhangi bir tereddüt bulunmamaktadır. Ancak, bulut bilişim gibi çoklu kullanıcı sunucu bilgisayarlarında tek bir şüpheli yönünden tüm sunucuda yer alan tüm veriler hakkında koruma tedbiri uygulanması tedbirin maksadını aşacaktır. Bu durumda, sadece şüphelinin hesabında (*account*) yer alan, şüphelinin verileri hakkında arama/elkoyma gerçekleştirilerek, diğer kullanıcıların hesaplarındaki verilerin arama kapsamı dışında tutulması gerekir¹¹⁹.

¹¹⁶ Aldemir, s. 75.

¹¹⁷ Ünver ve Hakeri, s. 939.

¹¹⁸ “...*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...” Karar için bkz; Aslan Ölmez, “Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Kopyalama ve Bunlara Elkoyma”, **Terazi Hukuk Dergisi**, Cilt: 4, Sayı: 30, 2009, s. 50.

¹¹⁹ Aynı yönde görüş için bkz; Değirmenci, Sayısal, s. 321.

1.3.2.1.2. Diğer Kişiler

Şüphelinin kullanımına girmemiş ve üçüncü kişinin mülkiyetinde olan ya da mağdur/suçtan zarar gören kişilerin bilişim sistemleri yönünden inceleme yapma ihtiyacı doğarsa, mezkûr koruma tedbirine başvurulamaz. Nitekim, Kanun'un lafzi yorumuna bakıldığında özel bir arama ve elkoyma tedbiri niteliğinde olan CMK md. 134, diğer kişiler bakımından tedbire karar verilmesine müsaade edilmediği görülecektir¹²⁰.

Teknolojinin gelişmesiyle geline nokta, mağdur/suçtan zarar görenin ya da başkaca üçüncü kişinin bilgisayarı kendilerinin rızası olmaksızın kullanılarak suç işlenebilmektedir. Örneğin, bu üçüncü kişilerin bilgisayarına virüs, trojan gibi zararlı yazılımlar yüklenebilmekte ve bu yazılımlar vesilesiyle başka sistemlere yönelik suç işlenebilmektedir. Bu durumlarda bu bilgisayarlar suçun aydınlatılmasında çok önemli rol oynamakta ve hatta bazı durumlarda bu bilgisayarların incelemesi yapılmadan suç aydınlatılamamaktadır.

Söz konusu duruma ilişkin öğretide çeşitli görüşler bulunmaktadır. Şahin'e göre¹²¹ CMK md.117 kapsamında kullanılan bilişim sistemi şüpheliye ait olmasa da arama yapılması mümkündür. Ancak maddede açık düzenleme olmamasına karşın, söz konusu arama mağdura karşı işlenen suçlarla sınırlı olmalıdır. Değirmenci¹²², sorunun çözümüne dair iki çözüm ortaya koymuştur. Bunlardan ilki, bilişim sistemlerine karşı işlenen suçlarda bilişim sisteminin olay yeri niteliğinde olmasından bahisle, CMK md. 160/2¹²³ ve Yönetmelik md. 9¹²⁴ uyarınca, Cumhuriyet savcısının delil toplama yetkisine dayanarak bilişim sistemlerinin incelenebileceğidir. İkinci çözüm ise, İletişimin Denetlenmesi Yönetmeliği md. 10/4¹²⁵'e benzer bir düzenlemenin Adli ve

¹²⁰ Değirmenci, Sayısal, s. 319.

¹²¹ Şahin, s. 277.

¹²² Değirmenci, Sayısal, ss. 323, 324.

¹²³ CMK md. 160/2; "Cumhuriyet savcısı, maddî gerçeğin araştırılması ve adil bir yargılamanın yapılabilmesi için, emrindeki adli kolluk görevlileri marifetiyle, şüphelinin lehine ve aleyhine olan delilleri toplayarak muhafaza altına almakla ve şüphelinin haklarını korumakla yükümlüdür."

¹²⁴ Adli ve Önleme Aramaları Yönetmeliği md.9; "Suç işlenen yerlerde, sebep ve sonuç ilişkisini ortaya koyacak delillerin aranması, bulunması ve el koyulması için geliştirilmiş bilimsel ve teknik araştırma işlemlerinin, herkesin girip çıkabileceği kamuya açık alanlarda yapılması için bir emir veya karar gerekmez."

¹²⁵ Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik md10/4; "Bir soruşturma sırasında delil toplama kapsamında, somut olayın özelliğine göre maddî gerçekliğin araştırılması ve adil bir yargılamanın yapılabilmesi için zorunlu olduğu takdirde,

Önleme Araması Yönetmeliği md. 17'ye eklenerek şikayetçi ve mağdurun rızası bulunması durumunda, kendisine ait bilişim sisteminde Cumhuriyet savcısının dijital delil araştırmasına imkân sağlanabileceğidir.

Kanaatimizce, ilk çözümden ziyade diğer çözüm daha uygulanabilir niteliktedir. Kanun koyucu, CMK md. 134'ü ayrık düzenlemesinde başlıca amacı, gerekçesinde de yer verdiği üzere mezkûr tedbire başvurulması halinde temel hak ve özgürlüklere yoğun müdahalede bulunulmasıdır. Bilişim sistemlerinin, mağdur bakımından olay yeri mahiyetinde değerlendirilerek, CMK md. 160/2'ye tabi tutulması; bunun karşısında şüpheli bakımından da CMK md. 134 uygulanması durumunda, Kanun koyucunun şüpheliyi mağdura göre çok daha fazla koruması gündeme gelecektir. Nitekim; yasa koyucu CMK md.134'ü koruma tedbiri olarak düzenlemiş ve sıkı şartlara bağlamıştır. Diğer çözümün daha uygulanabilir olduğunu değerlendirmekle beraber, anılan düzenlemenin yönetmelikten ziyade Kanun'da yer verilmesi gerektiğine inanıyoruz. Öte yandan, anılan düzenlemenin gerçekleşene kadar mağdur/suçtan zarar gören yönünden şahsın rızası var ise, hukuka uygunluk nedenlerinden “ilgilinin rızası” devreye girebilecektir¹²⁶.

1.3.2.1.3. Avukatlar

Avukatlara yönelik ceza muhakemesine ilişkin özel usuller öngörülmüştür. 1136 sayılı Avukatlık Kanunu md. 58'e göre avukatların görevleri sırasında işledikleri suçlara ilişkin yürütülecek soruşturma, Adalet Bakanı iznine tabidir. Adalet Bakanı'nın izin vermesi üzerine, avukat büroları ve konutlarında arama yapılabilmesi için mahkeme kararı gerekir. Mahkeme kararı sonucunda, arama faaliyeti ancak baro temsilcisinin katılımı ve Cumhuriyet savcısının denetiminde gerçekleştirilir. Öte yandan, avukat hakkında üst araması yapılamaz. Bu kuralın tek istisnası ise, ağır ceza mahkemesinin görev alanına giren suçüstü hali durumudur.

Avukat bürolarına ilişkin aramalara yönelik, CMK md. 130 ile özel düzenleme yapılmıştır. Buna göre, “Avukat büroları ancak mahkeme kararı ile ve kararda belirtilen olayla ilgili olarak Cumhuriyet savcısının denetiminde aranabilir. Baro

açık rızasının bulunması ve iletişim aracının kendisine ait olması şartıyla şikâyetçinin iletişiminin tespiti Cumhuriyet savcısının yazılı kararıyla Başkanlıktan istenir.”

¹²⁶ Şen ve Eryıldız, s. 189.

başkanı veya onu temsil eden bir avukat aramada hazır bulundurulur.” Avukatlık Kanunu’nda avukatların görevine yönelik suçlara ilişkin özel usul kuralları düzenlenmişken, CMK’da ise avukatların bürolarında gerçekleştirilecek aramalara yönelik özel bir düzenleme getirilmiştir.

Avukat faaliyetlerini yürüteceği tek bir büro açma yetkisine sahiptir. Söz konusu büroyu, bağlı olduğu Baro Başkanlığına bildirmek durumundadır. CMK md. 130 ile istisnai arama usulü öngörülen bürodan bahsedilen, avukatın Baro Başkanlığına bildirdiği bürodur.¹²⁷ Avukat, Baro Başkanlığına bildirdiği büro dışındaki konutunu ya da diğer işyerlerini avukatlık bürosu olarak kullandığını ileri sürerek, CMK md.130 kapsamında değerlendirilmesi gerektiği talep edemez.

Ceza muhakemesinin kurucu üç unsurundan birisi olan savunma makamı için Kanun koyucu tarafından düzenlenen istisnalar, esasen avukata mesleki olarak daha güvenli bir ortam sağlamak amaçlıdır¹²⁸. Zira, madde metni incelendiğinde bu husus açıkça görülecektir.

Avukatlık Kanunu md. 58 ile CMK md. 130 birlikte değerlendirildiğinde şu sonuçlara varılabilir. Avukatların *görevlerinden doğan veya görev sırasında işledikleri suçlardan dolayı haklarında yapılacak soruşturma* kapsamında Avukatlık Kanunu md. 58 hükmü gereği yapılacak aramalar, hâkim kararı doğrultusunda baro temsilcisi ile Cumhuriyet savcısı gözetiminde icra edilmelidir. Avukat bürosunda yapılacak arama ise, CMK md. 130 gereği mahkeme kararı ile gerçekleştirilmelidir. Yine, bu aramada da baro temsilcisi ile Cumhuriyet savcısı gözetimi şartı bulunmaktadır¹²⁹. Avukatın, *şahsi suçlarından dolayı konutunda veya aracında* yapılacak arama, genel hükümlere tabidir. Somut olayda; gecikmesinde sakınca bulunan halin şartlarının bulunması durumunda, Cumhuriyet savcısı da arama emri verebilir. Avukatın şahsi suçlarından dolayı yapılacak aramalarda, Cumhuriyet savcısı ve baro temsilcisi bulundurma zorunluluğu da bulunmamaktadır. Ancak, avukatın *şahsi suçundan dolayı olsa da bürosunda* yapılacak aramalarda mahkeme kararı gerekmektedir. Dolayısıyla, avukatın bürosunda yapılacak aramalarda, soruşturmaya konu suçun görev suçu ya da şahsi suç olmasına ilişkin bir ayrım bulunmamaktadır.

¹²⁷ Aldemir, s. 233.

¹²⁸ Özbek ve diğerleri, s. 301.

¹²⁹ Aldemir, ss. 231, 232.

CMK md. 130'un ilk fıkrasında avukat bürolarında yapılacak aramanın mahkeme kararı ile gerçekleştirilebileceği düzenlenmiştir. Bu noktada, bir an için avukat bürolarında aramanın kovuşturma aşaması ile sınırlı olduğu düşünülebilir. Ancak, maddenin ikinci fıkrası¹³⁰ ile yorumlandığı vakit; avukat bürolarında arama tedbirine hem soruşturma aşamasında hem de kovuşturma aşamasında başvurulabileceği söylenebilir. Bu noktada, çalışmamızın ilgili bölümünde yer verdiğimiz CMK md.134'te yer alan koruma tedbirine kovuşturma evresinde başvurulup başvurulamayacağına ilişkin tartışma, avukat bürolarında yapılacak aramalar için de geçerlidir.

Avukatlara ilişkin bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kopyalama ve elkoyma tedbiri CMK md.130 ile CMK md. 134'ün birlikte uygulama alanı bulacaktır. Her iki maddede de tedbire başvurulması için, Kanun koyucu hâkim kararının varlığını aramıştır. Bu nedenle, avukat bürolarında yer alan bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirine başvurulması için hâkim kararı gerekmektedir¹³¹. Öte yandan, CMK md. 130 ile avukat bürolarında yapılacak aramaya ilişkin Cumhuriyet savcısının denetimini ve baro başkanı veya onu temsil eden avukat huzurunda yapılması şart koşulmuştur. Buna göre, CMK md.134 kapsamında verilen arama kararı da Cumhuriyet savcısının denetiminde ve baro başkanı veya onu temsil eden avukat nezaretinde gerçekleştirilmelidir. Aksi halde, yapılacak arama hukuka aykırı kabul edilecektir.

Günümüzde pek çok avukat, kendi evini büro (home office) olarak kullanmaktadır. Bu anlamda, avukat konutunu büro olarak kullanıyorsa, söz konusu konut da CMK'da öngörülen avukatın bürosu niteliğini almaktadır. Bu nedenle, avukatın konutu hakkında da muhakeme hükümleri yönünden CMK md.130 uygulama alanı bulacak¹³², kanaatimizce yukarıda değindiğimiz üzere avukatın konutunda yer alan bilişim sistemlerine ilişkin CMK md 130 ve md.134 birlikte uygulama alanı bulacaktır.

¹³⁰ CMK md.130/2 nin ilgili bölümüm şu şekildedir; "...bu konuda gerekli kararı vermesi, **soruşturma evresinde sulh ceza hâkiminden, kovuşturma evresinde hâkim veya mahkemeden istenir...** "

¹³¹ Değirmenci, Sayısal, s. 325.

¹³² Ersan Şen, "Avukat , Hakim ve Savcıların Aranması", **Ankara Barosu Dergisi**, Cilt: 0, Sayı: 2, 2013, s. 341.

1.3.2.1.4. Milletvekilleri

Milletvekilleri, Anayasa md. 83 doğrultusunda yasama dokunulmazlığına sahiptir. Yasama dokunulmazlığı; milletvekillerinin suç işlemesinden dolayı Meclisin kararı olmaksızın, adli tahkikata maruz bırakılmamasıdır. Yasama dokunulmazlığının amacı, milletvekillerinin asılsız ve keyfi ithamlara maruz kalmasının ve buna bağlı olarak meclis çalışmalarından ayrı kalmamasını sağlamaktır¹³³.

Muhakeme engeli olarak yasama dokunulmazlığının neleri kapsayacağı Anayasa md.83/2’de sıralanmıştır. Buna göre, seçimden önce veya sonra bir suç işlediği ileri sürülen bir milletvekili, ağır cezayı gerektiren suçüstü hali ve seçimden önce soruşturmasına başlanılmış durumlar hariç olmak üzere, Meclisin kararı olmadıkça tutulamaz, sorguya çekilemez, tutuklanamaz ve yargılanamaz.

Söz konusu hüküm milletvekilleri hakkında soruşturma yapılamaması anlamına gelmemektedir. Milletvekilleri hakkında şikâyet ya da ihbar olması durumunda, soruşturma yapılarak fezleke düzenlenir. Bahse konu fezleke TBMM Başkanlığı’na gönderilir¹³⁴. Soruşturma esnasında Anayasa’da dokunulmazlık kapsamında yer alan tedbirler dışında muhakeme işlemlerine milletvekilleri yönünden de başvurulabilir. Örneğin, milletvekillerinin usulüne uygun olarak telefonları dinlenebilir, evi ve üstü aranabilir¹³⁵. Yine, CMK md. 134 kapsamında bilişim sistemlerinde arama, kopyalama ve elkoyma koruma tedbirine başvurmak mümkündür.

1.3.2.1.5. Hakimler ve Savcılar

Hâkim ve savcılar hakkında soruşturma ve kovuşturma usulleri 2802 sayılı Hâkim ve Savcılar Kanunu’nda düzenlenmiştir. Kanun md. 82’ye göre; “*Hâkim ve savcıların görevden doğan veya görev sırasında işlenen suçları, sıfat ve görevleri gereğine uymayan tutum ve davranışları nedeniyle, haklarında inceleme ve soruşturma yapılması Adalet Bakanlığının iznine bağlıdır.*”

¹³³ Kemal Gözler, **Türk Anayasa Hukuku Dersleri**, 15. baskı, Ekin Yayınevi, Bursa 2015, s. 204.

¹³⁴ Aldemir, s. 229.

¹³⁵ Metin Feyzioğlu, “Yasama Dokunulmazlığı”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 42, Sayı: 1, 1991, s. 31.

Kanun koyucu, hâkim ve savcılara ilişkin soruşturma usulleri yönünden ilgili suçun ağır ceza mahkemesinin görev alanına girip girmemesi bakımında, ikili bir ayrıma tabi tutmuştur. Hâkim veya savcının üzerine atılı suç, ağır ceza mahkemesinin görev alanına giren suçüstü halinde ise, hazırlık soruşturması genel hükümlere göre yapılır. Buna göre, CMK md. 134'te yer alan koruma tedbiri genel hükümlere göre işletilecektir¹³⁶.

Ağır ceza mahkemesinin görev alanına giren suçüstü halleri dışında, hâkim ve savcılar işlediği iddia olunan suçlar sebebiyle, yakalanamaz, üzerleri ve konutları aranamaz, sorguya çekilemez¹³⁷. Bu kapsamda, CMK md.134 yönünden ayrık bir düzenleme bulunmaması karşısında, bilişim sistemlerinde arama tedbirinin genele arama tedbirine ilişkin özgü bir düzenleme olması özelliği karşısında hâkim ve savcılar bakımından uygulanamayacağı söylenebilir¹³⁸.

2802 sayılı Kanun'a göre, hâkim ve savcıların görevlerine yönelik suç işleyip işlemediklerine ilişkin inceleme ve soruşturma işlemleri adalet müfettişlerince yapılır. Bu kapsamda, müfettişlerce lüzum görülmesi üzerine yeminle dinleme, istinabe yoluna başvurma ve zorunlu hallerde arama yapılabilir¹³⁹. Ancak, CMK md. 134 kapsamında yer alan bilişim sistemlerinde arama kopyalama ve elkoyma tedbiri, niteliği itibariyle genel arama tedbirinden ayrık düzenlenmiş olması nedeniyle adalet müfettişlerince başvurulacak tedbir niteliğinde değildir¹⁴⁰.

¹³⁶ Değirmenci, Sayısal, s. 327.

¹³⁷ 2802 sayılı Hâkim ve Savcılar Kanunu md. 88; "Ağır ceza mahkemesinin görevine giren suçüstü halleri dışında suç işlediği ileri sürülen hâkim ve savcılar yakalanamaz, üzerleri ve konutları aranamaz, sorguya çekilemez. Ancak, durum Adalet Bakanlığına derhal bildirilir."

¹³⁸ Değirmenci, Sayısal, s. 327.

¹³⁹ 2802 sayılı Hakimler ve Savcılar Kanunu md. 101; "Adalet müfettişleri lüzum gördükleri kimseleri yeminle dinler gerektiğinde istinabe yoluna başvurabilir ve soruşturmanın zorunlu kıldığı hallerde arama yaparlar. Sübut delillerini, gereken bilgileri bütün daire ve kuruluşlardan doğrudan doğruya toplarlar. Adalet müfettişlerince yapılacak denetim, inceleme ve soruşturmalarda ilgili kuruluş ve kişiler istenecek her türlü bilgi ve belgeyi vermek zorundadırlar."

¹⁴⁰ Değirmenci, Sayısal, s. 337.

1.3.2.2. Düzenlemede Doğrudan Yer Alan Bilişim Sistem Cihazları

1.3.2.2.1. Bilgisayar

1.3.2.2.1.1. Bilgisayar Kavramı

“Bilgisayar” Türk Dil Kurumu Sözlüğünde¹⁴¹; “çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin” şeklinde tanımlanmıştır. Bilgisayar, bireylerin yapacağı işleri, hesaplamaları çok daha hızlı ve çok daha doğru şekilde gerçekleştirmektedir.

“Bilgisayar” kavramı, TDK’nın Bilim ve Sanat Terimleri Sözlüğünde¹⁴² ise; “Çok sayıda aritmetiksel ya da mantıksal işlemlerden oluşan bir işi, çalışması sırasında bir işletmenin işe karışması gerekmeksizin, önceden verilmiş bir izlenceye göre, özdevimli olarak yürüten bir veri işleyici. Bir bilgisayar dizgesi elektronik ve mekanik birimlerden oluşan donanım ile bu donanım birimlerini ya da kaynakları istenen işlere yöneltip verimli bir çalışma düzeni içerisinde kullanabilmek için gerekli tüm izlencelerden ve veri yapılarından oluşan yazılım öğelerini kapsar. Minibilgisayar, mikrobilgisayar tanımlarının dışındaki geleneksel bilgisayarlar ana işlem birimlerinin hız ve yapısına, ana belleklerinin sığasına, dış belleklerin numeric multiplication ve giriş-çıkış birimlerinin türünlüğüne, sayısına ve hızına göre büyük, orta boy ya da küçük dizgeler olarak sınıflandırılır.” şeklinde açıklanmıştır.

Bilgisayarın tarihi yaklaşık 2000 yıldır kullanılan abaküse dayanmaktadır. 1617 yılında Charles Napier tarafından, *Napierin Kemikleri* (Napier’s Bones) adı verilen hesaplama aracı ortaya konmuştur. *Napierin Kemikleri*, İskoçya’da ürünlerin miktarını hesaplama amacıyla üretilen, ahşap ya da fildişi çubuklarından oluşan abaküse benzer çarpma işleminin de uygulanabildiği araçtır¹⁴³. *Blaise Pascal*, 1662 yılında vergi memuru olan babasına yardım amaçlı ilk dijital hesap makinesini icat etmiştir. 1800’lü yılların başında *Charles Babbage* tarafından ilk mekanik bilgisayarın temelleri atılmış, 1930’lu yıllarda da *Clifford Berry* tarafından elektronik bilgisayar

¹⁴¹ “Türk Dil Kurumu Sözlüğü”, (13.01.2022).

¹⁴² “Türk Dil Kurumu Sözlüğü”, (13.01.2022).

¹⁴³ Mueller Scott, **Upgrading and Repairing PCs**, 15. baskı, Que, Indiana, 2004, s. 10.

üretilmiştir. Özellikle İkinci Dünya Savaşında ortaya çıkan askeri ihtiyaçlar sebebiyle bilgisayar hızla gelişmiş ENIAC olarak bilinen yaklaşık 167 metre kare alan kaplayan devasa bilgisayar üretilmiştir¹⁴⁴. 1947 yılında ise günümüz modern programlanabilir bilgisayarı olan UNIVAC ticari amaçla üretilmiştir. 1975 yılında ise IBM tarafından ilk kişisel bilgisayar (PC) üretilerek satışı gerçekleştirilmiştir. O günden bu yana, bilgisayar teknolojisi hızla ilerlemiş ve hayatımızın her alanına girmiştir.

Yukarıda izah ettiğimiz doğrultuda, bilgisayarın tarihte gelişimiyle paralel şekilde ilk ortaya çıkmasından bu yana “sayısal makine”, “matematiksel makine”, “otomatik makine”, “otomatik sayısal makine”, “elektronik sayısal integratör ve hesap makinesi”, “hassas değerli otomatik hesap makinesi”, “otomatik olarak kontrol edilen sıralı hesap makinesi”, “bilimsel hesap makinesi” “hesap otomati” gibi terimlerle anılmıştır. Amerikalılar tarafından ise, hesaplamak anlamına gelen *to compute* sözcüğünden türetilmiş *computer* kelimesi, bilgisayara verilen genel isim olmuştur¹⁴⁵.

Bilgisayarlar karmaşık sistemlerden oluşarak, bilişim özelliğine sahip olması ile diğer programlanabilir cihazlardan ayrılır¹⁴⁶. Bilgisayar yeterli şekilde kavramsallaştırılmış ve iyi tanımlanmış problemler üzerinde çalışabilen aygıttır¹⁴⁷. “Girdi”, “süreç” ve “çıkı” işlemlerini gerçekleştiren, ikili kod ve hesaplama şekline dayalı kodlama metodu içerir¹⁴⁸.

Bilgisayar kavramının teknik tanımlamaları ve özelliklerinin yanında, hukuki tanımlamaları da karşımıza çıkmaktadır. 765 sayılı TCK’da, bilişim suçlarına ilişkin düzenlemede bulunan 3765 sayılı Kanun’da, bilgisayar için “*bilgileri otomatik işleme tabi tutan sistem*” kavramı tercih edilmişse de daha sonraki kanun tasarıları ve 5237 sayılı Kanun’da bu kavrama yer verilmemiştir¹⁴⁹.

Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı md. 2’ye göre; “*bilgisayar; belleğindeki programa uygun olarak aritmetik ve*

¹⁴⁴ Scott, s. 15.

¹⁴⁵ Dülger, s. 56; Karagülmez, s. 48.

¹⁴⁶ Sivarama P. Dandamudi, **Fundamentals of Computer Organization and Design**, Springer, New York, 2013, s. 6.

¹⁴⁷ Yılmaz Yazıcıoğlu, **Bilgisayar Suçları**, Alfa Basım Yayın Dağıtım, Bursa, 1997, s. 27.

¹⁴⁸ Karagülmez, s. 47.

¹⁴⁹ Değirmenci, Sayısal, s. 36.

mantıksal işlemleri yapabilen, karar verebilen, yürüteceği programı ve işleyeceği verileri ezberinde tutabilen, çevresiyle etkileşimde bulunabilen araçları” ifade eder.

Sanal Ortamlarda İşlenen Suçlar Sözleşmesinde¹⁵⁰ “bilgisayar” kavramından ziyade “bilgisayar sistemi” kavramı tercih edilmiş ve bu şekilde bir tanımlamaya yer verilmiştir. Bilgisayar sistemi sözleşmede tanımlar başlıklı md.1 ile “bilgisayar sistemi terimi bir veya birden fazlası, bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbirleriyle bağlantılı veya ilgili bir grup cihazı ifade eder” şeklinde tanımlanmıştır.

Dülger, öğretide yer alan tanımları “bilgisayarın yaptığı işler ve fonksiyona göre” ve “bilgisayarın fiziksel özellikleri ile yaptığı işler ve fonksiyonlarına göre” olmak üzere iki başlık¹⁵¹ altında ele alarak incelemiştir. Bilgisayar kavramını ilk başlık kapsamında, “yeterince kavramsallaştırılmış ve iyi tanımlanabilmiş her türlü problem üzerinde çalışabilen aygıt” olarak; diğer başlık altında ise “insanlar tarafından hazırlanıp yüklenen programlar yardımıyla bilgileri bir düzende saklamak, işleyerek yeni sonuçlar üretmek, üretilen bilgileri başka yerlere iletmek, başka yerlerdeki bilgilere ulaşmak gibi amaçlarla kullanılan makineler” olarak tanımlamıştır.

Yukarıda yer verilen tanımlarda bilgisayarın tanımlamalarının ortak özelliği, önceden belirlenen kurallar çerçevesinde verilerin otomatik işleme tabi tutularak ortaya bir veri ürünü çıkarılmasıdır. Yukarıda yer alan bu tanımlamalara katılmakla beraber, teknolojinin bizi getirdiği yeri göz önünde bulundurduğumuzda eksik olduğu kanaatindeyiz. Nitekim; bu tanımlara ilave olarak, günümüzde bilgisayar teknolojisi önceden belirlenen kuralların da ötesine geçerek, yapay zekâ çerçevesinde kendi kendine öğrenme fonksiyonu da gerçekleştirmektedir. Dolayısıyla önceden belirlenen belli fonksiyonel işlemlere ilave olarak öğrenme yeteneği olan yapay zekâ sistemlerinin de tanımlamalara dahil edilmesi gerekir.

Yargıtay güncel tarihli bir kararında¹⁵², bilgisayar kavramı ve madde kapsamında olması gereken uygulama alanıyla ilgili tespitte bulunmuştur. Yargıtay kararında;

¹⁵⁰ 23.11.2001 tarihli, Sanal Ortamda İşlenen Suçlar Sözleşmesi.

¹⁵¹ Dülger, ss. 58, 59.

¹⁵² Yargıtay CGK 25.02.2020 tarih, E.2016/544, K.2020/127 sayılı kararı, Yargıtay CGK 04.02.2020 tarih, E.2019/286, K.2020/52 sayılı kararı.

CMK'nın 134. maddesinde geçen bilgisayar teriminden ne anlaşılması gerektiği konusu CMK'da açık bir şekilde belirtilmemiştir. Bilgisayar; belleğindeki programa uygun olarak aritmetik ve mantıksal işlemleri yapabilen, karar verebilen, yürüteceği programı ve işleyeceği verileri ezberinde tutabilen, çevresiyle etkileşimde bulunabilen araçları ifade etmektedir. Genel olarak 134. maddesinin uygulamada; bilgisayar, akıllı telefonlar, GPS cihazları, donanım ve yan donanımlar, verileri dijital olarak kaydetme ve işleme yeteneğinde olan her türlü dijital cihazları kapsadığı kabul edilmektedir. Aynı şekilde madde kapsamına; iç ağlar, veritabanları, sistem odaları, sunucular, yedek üniteler, arşivler, veri iletim hatları, yönlendiriciler vs. dâhilinde bulunan tüm dijital alanlar, veriler ve veri taşıyıcıları da girmektedir. Zira bunlar belleğindeki programa uygun olarak aritmetik ve mantıksal işlemleri yapabilen, karar verebilen, yürüteceği programı ve işleyeceği verileri ezberinde tutabilen, çevresiyle etkileşimde bulunabilen araçlar olan bilgisayarların bileşenleri olarak fonksiyon icra etmektedir.

ibaresine yer vermiştir. Yargıtay kararında bilgisayar kavramını geniş yorumlamıştır. Kanaatimizce, Yargıtay'ın bu şekilde geniş yorumu yerindedir. Nitekim, aksinin kabulü halinde CMK md. 134'ün uygulaması oldukça daralacak madde ile varılması hedeflenen amaçtan uzaklaşılacaktır.

Her ne kadar söz konusu koruma tedbirinin tüm bilişim sistemlerini içerir şekilde kaleme alınması gerektiğini düşünsek de halen bilgisayar, kişilerin en mahrem en özel verilerinin bulunduğu cihazların başında gelir¹⁵³. Nitekim, pek çok hukuk düzeninde dijital delilin araştırılması süreci bilgisayarda arama kavramı ile ifade edilir¹⁵⁴. Ceza Muhakemesi Kanunu'nda da bilişim cihazlarında yer alan dijital delilin elde edilme süreci yönünden, bilgisayar terimi tercih edilmiştir.

1.3.2.2.1.2. Bilgisayar Bileşenleri

Bilgisayarlar günümüzde kullanım amaçlarına göre çeşitli gruplara ayrılırlar. Bunlar; büyük işletmeler, internet servis sağlayıcı gibi geniş tabanlı ağ yönetimine yarayan sunucu bilgisayarları, kişisel kullanıma özgülünmüş kişisel bilgisayarlar (PC),

¹⁵³ Osman Yaşar ve Cengiz Otacı, **Ceza Muhakemesi Kanunu**, 10. baskı, Seçkin Yayınevi, Ankara, 2022, s. 1105.

¹⁵⁴ Değirmenci, Sayısal, s. 31.

bir ağ yapısı içerisinde çalışacak şekilde tasarlanmış terminal (iş istasyonu) bilgisayarları, taşınabilir özellikteki diz üstü bilgisayarları ve günümüzde pek kullanım yeri kalmayan cep bilgisayarı¹⁵⁵ ile avuç içi bilgisayarlardır¹⁵⁶. Bunlara ilave olarak, günümüzde tablet bilgisayarlar ve giyilebilir bilgisayarlar da eklenmiştir.

Bilgisayar, en temelde yazılım ve donanımdan oluşur. Donanım, bilgisayarın maddi dünyada varlık gösteren aygıtlarına verilen genel addır. Yazılım ise, elle tutulur ve gözle görülür olmayan donanımsal araçları, kullanmak ve yönetmek için kullanılan uygulamalar olarak anılır¹⁵⁷.

Donanım; yazılım komutlarını yerine getiren, bilgisayarın fiziki bileşenlerini ifade eder. Bunlardan bir kısmı bilgisayar kasasının içinde yer alırken; diğer bir kısmı bilgisayar kasasının dışında bulunur. Bilgisayar kasasının dışında bulunan aygıtlar ancak bilgisayarla ilişkilendirilerek donanımsal bütünlük kazandırıldığı takdirde bilgisayar dünyasında anlam kazanır.

Bilgisayar kasasının içinde genel olarak; anakart, işlemci, RAM (random access memory), sabit disk, ekran kartı, ses kartı gibi donanımlar yer alırken; kasa dışında klavye, fare, harici mikrofon/kamera, hoparlör ve harici bellekler bulunur. Bunlardan her bir donanımın kendine özgü işlevi bulunmaktadır¹⁵⁸.

Anakart, bilgisayarın tüm donanımlarının takıldığı ve bu donanımların iletişiminin sağlandığı elektronik devrelerden oluşan bilgisayarın kalbi olarak nitelendirilebilecek parçadır¹⁵⁹. Anakartlar, genellikle üzerinde yonga seti, işlemci soketi, ROM BIOS, işlemci gerilim düzenleyicisi ve pil barındırır. Bazı anakartlar, üzerinde gömülü şekilde bulunan ekran kartı, ses kartı, ethernet kartı da barındırabilir¹⁶⁰. Anakartın en önemli parçası yonga setidir¹⁶¹. Yonga seti, anakartın beynini oluşturan; işlemci, önbellek sistem veri yolları gibi bilgisayarın içindeki veri akışını denetleyen birimdir¹⁶².

¹⁵⁵ Levent Emmungil, **Bilgisayar Donanımı**, Ankara, 2010, s. 56.

¹⁵⁶ Mehmet Özgüler, **Bilgisayar Donanımı**, 3. baskı, Akademi Yayınevi, Rize, 2007, ss. 1–4.

¹⁵⁷ Şeyhmus Aydoğdu ve diğerleri, **Bilgisayara Giriş**, Pegem Akademi Yayıncılık, Ankara, 2017, s. 11.

¹⁵⁸ Yazıcıoğlu, s. 31.

¹⁵⁹ Hans-Peter Messmer, **The Indispensable PC Hardware Book**, 4. baskı, Pearson Education, Great Britain, 2002, s. 7; Ali Döngel, **Bilgisayar Donanımı ve Elektronik**, 2. baskı, Tuna Matbaacılık, Ankara, 2012, s. 36; Scott, s. 227.

¹⁶⁰ Scott, s. 227.

¹⁶¹ Döngel, s. 36.

¹⁶² Orhan Özçatalbaş ve diğerleri, **Bilgisayar**, Ekin Yayınevi, Ankara, 2008, s. 45.

BIOS¹⁶³, terim olarak temel girdi çıktı sistemi olarak anılır. BIOS, en temel yazılım olan işletim sistemi ile donanımın konuşmasını sağlayan ara yüz kodudur¹⁶⁴. Bahse konu arayüz kodu kullanıcının düzenleme yapamadığı sadece sistem tarafından veri okumasının yapılmasına imkân tanınmış, ROM¹⁶⁵ isimli bellekte bulunur. Bilgisayar, güç düğmesine basılarak ilk açıldığında, tüm donanımın sürücü bilgilerini içeren BIOS, sistemin uyumlu şekilde açılmasına yarar.

İşlemci, sistem tarafından sağlanan tüm işlemleri kontrol eden¹⁶⁶ ve sistemin merkezindeki tüm veri akışını sağlayan birimdir¹⁶⁷. Mikroişlemciler elektrik sinyallerinin aktığı milyonlarca transistordan oluşurlar. Bilgisayarın toplama çıkarma çarpma bölme gibi yaptığı tüm işlemler bu sinyaller aracılığıyla gerçekleşir¹⁶⁸. Aslında, söz konusu sinyal bilgisayarın en temel mantığı olan 0 ve 1 temeline dayanır.

Bellek, bilgisayar sistemi içinde yer alan işlemcinin çalışma alanıdır¹⁶⁹. RAM¹⁷⁰, işletim sistemi, uygulama yazılımları ve verilerin geçici depolandığı ve işlemcinin hızlı şekilde erişim sağladığı fiziksel olarak küçük boyutlu bir depolama birimidir. RAM, kısa dönemli bellek özelliği taşır. Bilgisayarın her yeni açılışında bu bellekte yer alan tüm veriler silinir. Bellek genel olarak okuma ve yazma olmak üzere iki temel işlemi gerçekleştirir¹⁷¹. RAM, sadece bilgisayar çalıştığı sırada üzerinde veri bulundurabilmesi ve kullanıcı tarafından üzerine veri yazılabilmesi ile ROM'dan ayrılır.

Harddisk, tıpkı RAM gibi bir bellek türüdür. Harddisk üzerinde yer alan veriler bilgisayarda enerji bulunmadığı durumda dahi saklanmaya devam edilir. RAM'in üzerine geçici olarak veri yazılabilirken, Harddisk üzerine ileride yeniden kullanılabilmek amacıyla kalıcı veri yazılabilir. Harddisk'in üzerinde genel olarak işletim sistemi, uygulama yazılımları ve sistem verileri ile kullanıcı verileri bulunur. Harddisk, CMK md. 134 kapsamında bilgisayarlarda, bilgisayar programlarında ve

¹⁶³ BIOS: Basic Input Output System

¹⁶⁴ Scott, s. 365.

¹⁶⁵ ROM *Read Only Memory* anlamına gelir. BIOS sistemi bilgisayara üç temel ROM kaynağından ulaşabilir. Bunlar, Anakartta yer alan ROM, sürücülerin yüklü olduğu ROM, diğer parçalarda yer alan ROM; Scott, s. 369.

¹⁶⁶ Dandamudi, s. 16.

¹⁶⁷ Messmer, s. 8.

¹⁶⁸ Döngel, s. 60.

¹⁶⁹ Scott, s. 422.

¹⁷⁰ RAM (*Random Access Memory*), rasgele erişilebilir bellek anlamına gelir.

¹⁷¹ Dandamudi, s. 23.

kütüklerinde arama, kopyalama, elkoyma koruma tedbiri açısından, bilgisayar içerisinde yer alan en önemli donanımdır. Adli bilişim uzmanları söz konusu koruma tedbiri kapsamında arama, kopyalama işlemini genel olarak harddisk üzerinde yapar. Ancak bilişim sistemlerinde yer alan veriler harddiskle sınırlı olmadığından RAM ya da diğer donanımlar üzerinde de arama yapılmaktadır.

1.3.2.2.2. Bilgisayar Programı

Çalışmamıza konu koruma tedbirinde açıkça düzenlenmiş bir diğer husus, bilgisayar programlarıdır. Bilgisayar programları, bilgisayarın belli bir işlemi yerine getirilmesi maksadıyla tasarlanmış komutlar zinciridir¹⁷². Bilgisayar dili, insanların günlük hayatta anladığı dilden çok farklıdır. Bilgisayar programlama ile eldeki sorun bilgisayarın anlayacağı dile çevrilerek çözüme kavuşturulmaktadır¹⁷³.

Bilgisayar programının tanımına mevzuatımızda, 5846 sayılı Fikir ve Sanat Eserleri Kanununda yer verildiği görülmektedir. Buna göre, bilgisayar programı¹⁷⁴; *“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 çalışmalarını”* ifade eder. Kanun koyucu, tanımda hazırlık çalışmalarına da yer vererek bilgisayar programlarını geniş biçimde tanımlamıştır. Burada bilgisayar programının hazırlık aşamasını da fikri mülkiyet hakları çerçevesinde korumaya almaktır¹⁷⁵. Nitekim, ana yazılım pek çok alt yazılımların bir araya gelmesinden oluşur. Her bir yazılım parçası başkaca işlere de özgülenebileceğinden ayrı ayrı eser niteliğindedir. Bu anlamda, kanaatimizce tanımın geniş koruma sağlayacak şekilde yapılmış olması yerindedir.

Yargıtay güncel tarihli bir kararında¹⁷⁶ bilgisayar programı hakkında tespitte bulunmuştur. Yargıtay kararında; *“Bilgisayar programı, bir bilgisayar vasıtasıyla belirli bazı görevleri gerçekleştirmek için oluşturulan yazılı talimatlar dizisi olarak*

¹⁷² Batuhan Aktaş, “Bilgisayarlarda, Bilgisayar Programlarında Ve Kütüklerinde Arama, Kopyalama ve Elkoyma Tedbiri Üzerine Bir İnceleme”, *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*, Cilt: 14, Sayı: 2, 2017, s. 219.

¹⁷³ Dandamudi, s. 5.

¹⁷⁴ 5846 sayılı Fikir ve Sanat Eserleri Kanunu md.1/B (g) de tanımlanmıştır.

¹⁷⁵ Değirmenci, Sayısal, s. 51.

¹⁷⁶ Yargıtay CGK 25.02.2020 tarih, E.2016/544, K.2020/127 sayılı kararı, Yargıtay CGK 04.02.2020 tarih, E.2019/286, K.2020/52 sayılı kararı.

tarif edilmektedir. Esasen bilgisayar programları bilgisayarların çalışmasını sağlayan düz metin komutlarıdır. Genelde bilgisayarlar, program olmaksızın fonksiyon icra edemezler.” ibarelerine yer vermiştir.

Bilgisayar bir konuya ilişkin verileri içine alan, bu verileri önceden belirlenmiş komutlarla bir işleme koyan ve bu işlemleri bir çıktı (output) olarak ortaya koyan sistemler bütünüdür¹⁷⁷. Bilgisayarın, herhangi bir işlemi yerine getirebilmesi için yazılım dilinde belirli bir mantıkta dizilmiş komut kodlara ihtiyaç vardır. Bu anlamlı kodlar bütünü, bilgisayar programını oluşturmaktadır. Yazılım olmadan donanıma herhangi bir işlem yaptırılamamaktadır.

Yazılım, öğretilde ağırlıklı iki ana başlık altında incelenmiştir¹⁷⁸. Bunlar, işletim sistemi (yazılımı) ve uygulama yazılımıdır. İşletim sistemi, diğer programların çalışması ve bilgisayarın temel işlevini yerine getirmesine yarayan en alt katmanda çalışan programlardır¹⁷⁹. İşletim sistemi, bilgisayarın başlamasından donanım öğelerinin birbiriyle uyumlu çalışmasına ve sistemsel olay ve sorunların kaydedilmesine kadar tüm temel bilgisayar işlemlerinin yürütüldüğü yazılımdır. Günümüzde kullanılan en popüler işletim sistemleri Windows, Mac OS, Pardus, Linux’dür. Uygulama programları ise, kullanıcı isteklerini karşılamaya yönelik ortaya çıkan hayatın pek çok alanını kolaylaştırıcı özelliği olan, işletim sistemi üzerinde çalışan programlardır¹⁸⁰. Stok yönetim programları, muhasebe programları, doküman yönetim sistemi, kelime işlemci yazılımı gibi pek çok örnek verilebilir.

İşletim sistemi ile uygulama yazılımı arasındaki temel fark, yazılımın özgülendikleri konulardır. İşletim sistemi genel olarak bilgisayarın çalışmasını sağlamaya odaklanırken, “uygulama yazılımı” kullanıcının belli bir ihtiyacının karşılanması ve kendisine yönelik yararlı sonuçların ortaya çıkarılmasını sağlar¹⁸¹. Yine, öğretilde üçüncü sınıf olarak programlama dilleri de değerlendirilmektedir. Programlama dilleri hem işletim sistemlerinin hem de uygulama yazılımlarının

¹⁷⁷ Aytekin İşman, “Bilgisayarlar ve Eğitim”, **Sakarya Üniversitesi Eğitim Fakültesi Dergisi**, Cilt: 0, Sayı: 2, 2001, s. 6.

¹⁷⁸ Dülger, ss. 62, 63; Değirmenci, Sayısal, s. 46.

¹⁷⁹ Davut Özkul, “Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi”, **Sayıştay Dergisi**, Cilt: 13, Sayı: 44, 2002, s. 15.

¹⁸⁰ Olgun Değirmenci, “Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbirinde (CMK m. 134), 7145 Sayılı Kanunla Yapılan Değişikliklerin Değerlendirilmesi”, **Terazi Hukuk Dergisi**, Cilt: 13, Sayı: 147, 2018, (7145), s. 52.

¹⁸¹ Dülger, s. 63.

kodifiye edildiği yazılımlardır. Günümüzde; c, c++, c#, python, sql, oracle, html ve css en yaygın kullanılan programlama dillerindendir.

Bilişim sistemi kullanılarak işlenen suçlarda, fail suç işlenirken sistem üzerinde belli izler bırakmaktadır¹⁸². Bırakılan bu izler uzmanlar tarafından çözümlenebilmektedir. Hatta sistem üzerindeki veriler silinse dahi üçüncü parti yazılımlar ile geri getirilebilmektedir. Bu anlamda sayısal delil bakımından programlar da içinde veri bulundurmakta ve önem taşımaktadır¹⁸³.

1.3.2.2.3. Bilgisayar Kütüğü

CMK md. 134 kapsamında, açıkça düzenlenmiş diğer bir husus ise, bilgisayar kütükleridir. Bilgisayar kütüğü kavramı kanunda açıkça tanımlanmamıştır. Bu nedenle, bilgisayar kütüğünden ne anlaşılması gerektiğine ilişkin görüş birliği bulunmamaktadır.

Öğretide, kütük kavramının karşılığının ne olduğuna ilişkin açıklamalar getirilmeye çalışılmıştır. Bazı yazarlarca¹⁸⁴; bilgisayar kütüğü kelimesi İngilizcede kullanılan “log” kelimesinin karşılığı olarak kullanılmaktadır.

Dülger’e göre¹⁸⁵; bilgisayar kütüğü, “*sabit taşınabilir ya da bulut formunda her türlü veri taşımaya ve depolamayı yarayan araçlar ya da sistemlerdir*”.

Aktaş’a göre¹⁸⁶; bilgisayar kütükleri sanal ortamdaki verilerin disk üzerinde saklanması için oluşturulan belirli büyüklükteki veri yapısı olarak tanımlanmaktadır.

Keskin ise¹⁸⁷, “*bilgisayar ve bilgisayar kütüklerinin tanımlarının beraber düşünüldüğünde, kaydetme özelliği olan tüm cihazların bilgisayar kütüğü*” olarak değerlendirilebileceği görüşündedir.

¹⁸² Yavuz Erdoğan, **Türk Ceza Kanununda Bilişim Suçları**, Legal Yayınevi, İstanbul, 2012, s. 398.

¹⁸³ Değirmenci, Sayısal, s. 51.

¹⁸⁴ Ölmez, s. 46; Özbek ve diğerleri, s. 391; Değirmenci, Sayısal, s. 25; Özge Apiş, “Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Koruma Tedbiri”, **Yasama Dergisi**, Cilt: 13, Sayı: 37, 2018, s. 75.

¹⁸⁵ Dülger, s. 585.

¹⁸⁶ Aktaş, s. 220.

¹⁸⁷ Salih Keskin, “Bilişim Suçlarında Ceza Muhakemesi Kanununun 134. Maddesindeki Hükümlerin Uygulanmasında Yaşanan Aksaklıklar”, **Kırıkkale Üniversitesi Sosyal Bilimler Dergisi**, Cilt: 11, Sayı: 2, 2021, s. 651.

Değirmenciye göre¹⁸⁸, “log” kelimesinin sözlük anlamı, *kütük* kelimesine karşılık gelmesine karşın bilişim dünyasında tam olarak bu anlamda kullanılmamaktadır. “Log” kelimesi daha çok “günlük” anlamında kullanılmaktadır.

Kanaatimizce, Değirmencinin tespiti yerindedir. Nitekim, bilgisayar “log” kayıtları, daha ziyade bir sistemde yer alan olaylara ilişkin erişim saati, kullanıcı bilgisi, MAC adresi¹⁸⁹ gibi kayıtlardan oluşarak, bunların sistem tarafından otomatik tutulmasıyla ortaya çıkar. Kanun koyucu, yasa maddesinde, söz konusu koruma tedbirini bununla sınırlamadığı düşüncesindeyiz.

Kütük, “*oluşturucusu tarafından belirlenmiş ilişkili bilgiler topluluğudur*.”¹⁹⁰ Daha açık ifadeyle işletim sisteminin, kullanıcı için sanal olan görev ve bellek yönetimi ile veri depolarını aynı mantıksal görünümde olacak şekilde sakladığı mantıksal depolama birimine kütük denir¹⁹¹. Kütük teriminin terminolojide karşılığı daha çok İngilizce “*file*” kelimesidir¹⁹². Kütük terimi, insan eliyle oluşturulan verileri depolamakta kullanılan mantıksal depolama birimleri ve dosya dizinleridir¹⁹³.

Özetle, insan müdahalesi olmaksızın bilgisayar sistemi tarafından otomatik işlenen kayıtlar “log”ları; insan müdahalesi ile oluşturulmuş bilgisayar sistemi tarafından saklanan kayıtlar ise *kütükleri* oluşturmaktadır¹⁹⁴. Örneğin, internete erişim sağlandığında ağdan indirilen herhangi bir görsel “*kütük*” olarak saklanırken internet erişim sağlayıcı ya da BTK tarafından hangi adrese ne zaman erişildi gibi yukarıda belirtilen otomatik alınan ve saklanan kayıtlar “log” olarak anılmaktadır. Kanun koyucunun kütüklerde arama yapılmasından kastının bilişim sistemlerinde veri saklanması yarayan araçların tamamında yer alan dosyayı “*file*” kastettiğini değerlendirmekteyiz.

¹⁸⁸ Değirmenci, Sayısal, s. 52.

¹⁸⁹ MAC adresi, bilgisayarın ethernet kartına üretici tarafından kodlanan bir bilgidir. Her donanım için özel bir adresi vardır. Aynı MAC adresine sahip birden fazla ağ cihazı yoktur.

¹⁹⁰ İbrahim Türkoğlu, “BİL391 İşletim Sistemleri (Ders Notları)”, 2006, <http://eng.harran.edu.tr/~nbesli/OS/book1.pdf>, (03.10.2022), s. 23.

¹⁹¹ İbrahim Türkoğlu, “BİL391 İşletim Sistemleri (Ders Notları)”, 2006, <http://eng.harran.edu.tr/~nbesli/OS/book1.pdf>, (03.10.2022), s. 23.

¹⁹² Değirmenci, Sayısal, s. 51.

¹⁹³ Değirmenci, Sayısal, s. 332.

¹⁹⁴ Değirmenci, Sayısal, s. 53.

Nitekim, Yargıtay bir kararında¹⁹⁵ dosya kapsamında alınan bilimsel mütalaaaya yer vermiş, “*bilgisayar kütükleri*” ifadesinin masaüstü ve dizüstü bilgisayarla sınırlı olmadığı, tüm TVDO, mobil cihazlar ve bellekler de dahil olmak üzere üzerinde dijital veri işlenen veri araçlarında yer alan tüm dijital dosyaları kapsadığı değerlendirilmiştir. Yine, Adli ve Önleme Aramaları Yönetmeliğinin 17. Maddesinde el koyma sırasında zorunlu kılınan yedekleme işleminin Kanun kapsamı genişletilerek “*bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımlar hakkında da*” uygulama alanı bulmasının yasal dayanağı aynı çıkarıma dayanmaktadır. Öte yandan, Yargıtay, bilgisayar kütüklerinin sadece kullanıcının kendi bilgisayarında bulunan bilgisayar programı marifetiyle kullanılabilen, verilerin saklandığı veri depolama araçlarıyla sınırlı olmadığını, bunun yanında bir bilgisayar aracılığıyla ulaşılabilen ağda saklanan ya da kullanıma açık diğer bilgisayarlarda bulunan veri araçlarını da kapsadığını değerlendirmektedir.

Yargıtay’ın güncel tarihli başka bir kararında¹⁹⁶ ise, bilgisayar kütüklerinin Türkçeye her ne kadar “log” olarak çevrilse de aslında kastedilenin İngilizce’de “*database*” (veritabanı) kelimesine karşılık geldiğini bu bağlamda veri saklayan her türlü cihazın bilgisayar kütüğü olarak değerlendirileceğini belirtmiştir.

Yargıtay’ın yukarıda yer verilen her iki kararında yer alan bilgisayar kütüklerine ilişkin tespitin birlikte değerlendirdiğimizde yerinde buluyoruz. Nitekim, bilgisayar kütükleri, bilgi sistemlerinde yer alan veri depolama araçlarındaki tüm dijital verileri ihtiva eder. Bu veriler, bilgisayarın sabit diskinde bulunan verilerden ibaret değildir. Aynı zamanda; TVDO’da yer alan veriler, bilgisayar ağları, uzak masaüstü ağları ve bulut bilişim sunucularında yer alan veriler de bilgisayar kütükleri kapsamında değerlendirilmelidir.

¹⁹⁵ Prof.Dr. Bülent SANKUR, Boğaziçi Üniversitesi, Elektrik/Elektronik Mühendisliği Bölümü, Prof. Dr. Ahmet Celal Cem Say, Boğaziçi Üniversitesi, Bilgisayar Mühendisliği Bölümü, 21.11.2015 tarihli Bilimsel mütalaa; Yargıtay 16. CD. 24.04.2017 tarih, E.2015/3, K.2017/3 sayılı kararı.

¹⁹⁶ Yargıtay CGK 25.02.2020 tarih, E.2016/544 K.2020/127 sayılı kararı, Yargıtay CGK 04.02.2020 tarih, E.2019/286, K.2020/52 sayılı kararı.

1.3.2.3. Düzenlemede Doğrudan Yer Almayan Bilişim Sistem Cihazları

Adli ve Önleme Araması Yönetmeliği md. 17 ile Ceza Muhakemesi Kanunu md. 134'te yer alan koruma tedbiri detaylandırılmıştır. Yönetmelik ile Kanun'da düzenlenen koruma tedbirinin kapsamı genişletmeye çalışılmıştır.

Yönetmelik md.17/4 ile bilgisayar veya bilgisayar kütüklerine ilişkin verilerin yedeklemesi işleminin bilgisayar ağları ve diğer uzak bilgisayar kütükleri çıkarılabilir donanımlar hakkında da uygulanabileceği düzenlenmiştir. Böylece, Kanun'da yer alan eksiklik giderilmeye çalışılmıştır.

Madde metninde yer aldığı gibi bilgisayar kavramının dar yorumlanması, CMK md. 134'ün kapsamını daraltacak ve temel hak ve özgürlüklerin kişi aleyhine daraltılmasına sebep olacaktır. Öğretide ve uygulamada tıpkı bilgisayar gibi CMK md. 134 kapsamında değerlendirilen ancak maddede doğrudan yer almayan cihazlar da bulunmaktadır. Bunlardan bir kısmı, cep telefonları, taşınabilir veri depolama ortamları, bulut bilişim sistemleri, elektronik posta sunucu ve istemcileridir. Ancak kanaatimizce dijital veri içeren tüm cihazlar ve veri taşıma ortamları CMK md. 134 kapsamında değerlendirilmelidir.

1.3.2.3.1. Cep Telefonları

Cep telefonu, en temelde kişiler arası iletişimi sağlamak amacıyla ortaya çıkmıştır. Ancak, günümüzde cep telefonlarının kullanım amacı, kişiler arası iletişimin çok ötesine geçmiştir. Cep telefonu kişiler arası ve kitleler arası iletişimi sağlamanın yanında, bir bilgisayarın yapabileceği hemen hemen tüm işlevleri yerine getirebilmektedir.

Cep telefonlarının ana işlevi bilişim faaliyetleri olmasa bile¹⁹⁷, bilgisayarlarda olduğu gibi ekran, işlemci, bellek bulundurarak aynı yapısal özelliği taşımaktadır. Öte yandan, akıllı telefonlar bilgisayarlarla aynı işlevsel özellikleri de barındırmaktadır. Akıllı telefonlar da işletim sistemi ve uygulama yazılımları barındırmakta ve bu telefonlar üzerinde pek çok veri işlenebilmekte, saklanabilmekte, geniş alan ağı, yerel alan ağına dahil olabilmekte, uzaktan bilgisayar gibi kontrol edilebilmektedir. Yine, e-

¹⁹⁷ Şen ve Eryıldız, s. 200.

posta ile haberleşme sağlanmakta, kelime işlemci programları kullanılabilir¹⁹⁸. Bu bağlamda, CMK md. 134 kapsamına akıllı telefonların dahil olduğu söylenebilir¹⁹⁸.

Uygulamada, cep telefonlarına el konulmasına ilişkin zaman zaman hatalı usuller takip edilebilmektedir. Yukarıda, kısaca bahsettiğimiz gibi, günümüzde cep telefonlarının gelişen teknoloji ile bilgisayarlardan pek farkı kalmamıştır. CMK md. 134'te yer alan koruma tedbirinin madde metninde bilgisayar kavramına yer vermesinden ötürü, cep telefonlarına kolluk kuvveti doğrudan elkoyma işlemi gerçekleştirebilmektedir¹⁹⁹. Ancak, bu uygulama hukuka aykırıdır. Cep telefonları hakkında hukuka aykırı elkoyma kişisel verilerin ve özel hayatın gizliliğine müdahale anlamına gelecektir.

Öğretide, cep telefonlarına ilişkin uygulanacak koruma tedbirinin ne olması gerektiği tartışılmıştır. Bir görüşe²⁰⁰ göre, cep telefonlarına ilişkin elkoyma tedbiri yönünden ikili ayırım benimsenmiştir. Buna göre; koruma tedbirinin konusu, cep telefonlarının sesli iletişim, kısa mesaj gibi telefon fonksiyonuna yönelik ise, CMK 116 vd. yer alan basit elkoyma tedbiri uygulanacaktır. Ancak, cep telefonlarının bilgisayar özelliğine ilişkin delil elde edilmek isteniyorsa, CMK md.134'te yer alan bilgisayarlarda, bilgisayar programlarında ve kütüklerinde elkoyma tedbiri uygulanacaktır. Bir diğer görüşe göre²⁰¹ ise cep telefonları ile kişiler arası iletişimin, telefon mesajı vasıtasıyla gerçekleştirmekle e-posta ile gerçekleştirilmesi arasında tek farkın birisinin internet üzerinden diğerinin ise operatör üzerinden gönderilmesi olduğu, yine telefon mesajının da aynı zamanda bilgisayarda görünebilme imkanının da olması göz önünde bulundurulduğunda böyle bir uygulama farkının tercih edilmesinin ikna edici olmadığı değerlendirilmiştir. Yine benzer bir başka görüşe göre²⁰² ise, cep telefonlarına ilişkin ikili bir ayırım yapmanın hukuki temeli bulunmamaktadır. Zira, yazar kanunda yer almayan ayırımın daha sonradan sübjektif kriterler geliştirilerek ortaya konmasının uygulamada karmaşa yaratacağı ve hukuki belirlilik ve güvenilirlik ilkesine aykırılık teşkil edeceği düşüncesindedir.

¹⁹⁸ Değirmenci, Sayısal, s. 330.

¹⁹⁹ Özen ve Özocak, s. 69.

²⁰⁰ Özen ve Özocak, s. 67; Öztürk ve diğerleri, Koruma Tedbirleri, s. 211.

²⁰¹ Dilek Özge Uğraş, "Bilgisayarlarda, Bilgisayar Programlarında ve Bilgisayar Kütüklerinde Arama, Kopyalama ve Elkoyma", **Türkiye Barolar Birliği Dergisi**, Cilt: 34, Sayı: 154, 2021, s. 104.

²⁰² Seda Yağmur Sümer, "Ceza Muhakemesinde Mobil Telefona/Akıllı Telefona Elkoyma ve Müdahale İmkanları", **İzmir Barosu Dergisi**, Cilt: 87, Sayı: 1, 2022, s. 92.

Günümüzde, bazı telefonlarda kullanıcının tercih etmesi halinde kısa mesajın (sms) internet aracılığıyla gönderilebildiği söylenebilir. Hatta, senkronizasyon özellikleri aktif edildiğinde; kullanıcının cep telefonu, akıllı saat, bilgisayar ve tabletlerinin hepsinde aynı arama ve mesaj kayıtları eşleşmektedir. Bu durumda, tüm sistemlerde aynı anda aynı veri oluşmaktadır. Aynı verinin, bilgisayardan alındığında CMK md.134 kapsamında değerlendirilirken cep telefonundan alınması halinde CMK md.116 kapsamında değerlendirilmesi, kanunilik ilkesine aykırı olacaktır.

Bu açıklamalar ışığında cep telefonlarına ilişkin aramalarda CMK md. 116 ve CMK md. 134 arasında daha farklı bir ayrım yapmanın teoride uygun olacağını değerlendirmekteyiz. Cep telefonlarının sadece kişi araması özelliğine ilişkin arama yapılacaksa CMK md. 116 geri kalan tüm işlevlerine ilişkin aramalarda ise CMK md. 134 uygulanması doğru olacaktır. Ancak şunu önemle belirtmek gerekir ki pratikte, hem arama kararının bu şekilde ayrıntılı verilmesi hem de uygulama esnasında kolluk kuvvetlerinin böylesi hassasiyeti sağlaması da oldukça güç olacaktır. Nitekim, tedbirin uygulama safhasında ilgili bilişim sisteminin adli kopyası alınmakta, hash değeri çıkarılarak inceleme yapılmaktadır. Bu noktada, yedekleme sürecinde genellikle adli kopya almaya yarayan donanım, kendisine bağlanan belleğin tamamının kopyasını almaktadır. Bu anlamda, esasen arama kayıtları da yedekleme işlemine konu olacak ayrım yapılamayacaktır.

Yargıtay bir kararında²⁰³, işlevi itibarıyla bilgisayar niteliğinde olan cep telefonu üzerinde inceleme yapılabilmesi için CMK md. 134 uyarınca karar alınması gerektiği ve bu kararın alınmamış olmasının yasaya aykırılık teşkil etmesinden ötürü, elde edilecek delillerin de mahkumiyete esas teşkil edemeyeceğine hükmetmiştir. Yargıtay'ın kararı yerindedir. Nitekim, yukarıda açıklandığı üzere günümüz

²⁰³ Yargıtay 17. CD 15.02.2017 tarih, E.2015/27517, K.2017/1716 sayılı Kararı; "Cumhuriyet Savcısının talimatıyla yapıldığı belirtilen, telefon inceleme tutanağının 20.04.2014 saat 14.10'da düzenlendiği, bu saatten daha önceki bir saatte saat 12.57'de 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 K ismiyle 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 ve sanık tarafından çalındığına dair sanığın mahkumiyetine yeterli, kesin ve inandırıcı delil bulunmaması sebebiyle sanığın atılı suçtan beraatine karar verilmesi gerekirken, yetersiz gerekçeyle yazılı şekilde mahkumiyetine karar verilmesi," "Hukuk Türk", <https://www.hukukturk.com/>, (20.02.2022)

teknolojisi itibariyle cep telefonları nitelik olarak bilgisayar mahiyetindedir. Çok önemli bir kısmı, dijital veri oluşturup saklayabilmekte, bilgisayarlarla eş güdümlü çalışabilmekte, bilgisayar ağlarına bağlanarak bulut bilişim sunucularına erişmektedir. Bu bağlamda, cep telefonlarında oluşturulan verilerin bilgisayar, bilgisayar kütüğü olarak değerlendirilmesi ve CMK md. 134'ün uygulama alanına alınması doğru olacaktır.

1.3.2.3.2. Taşınabilir Veri Depolama Ortamı (TVDO)

1980'li yıllardan sonra bilgisayarın içinde yer alan belleklerin dışında, veri yedekleme, veri taşıma, geçici ve kalıcı veri depolama amacıyla²⁰⁴ taşınabilir veri depolama ortamları (TVDO) geliştirilmiştir. Yine, zamanla işletim sistemi ve uygulamaların gelişmesiyle beraber saklama kapasitesi artmış ve daha büyük boyutlu donanımlara ihtiyaç duyulmuştur. TVDO'lara; floppy disk, CD, DVD, Usb bellek, yüksek kapasiteli bellek örnek olarak verilebilir.

Veri depolama yönünden; TVDO ile bilgisayar dahilinde bulunan belleklerin donanımsal açıdan farklı teknolojiler barındırmasına rağmen, işlevsellik yönünden farkı bulunmamaktadır. Nihayetinde, hepsinin ortak amacı üzerinde sanal olarak veri barındırmaktır. TVDO'ların, farkı bilgisayarla bütünleşik olmaksızın kullanıcı nezdinde taşınabilir olmasıdır.

Öğretide, bizim de katıldığımız görüşe göre²⁰⁵, TVDO ortamlarının veri barındırması ve yapılacak aramanın TVDO'nun cismani varlığından ziyade içerisinde yer alan dijital verilere yönelik olmasından bahisle, TVDO'lara yönelik olarak da tıpkı bilgisayarlar gibi, CMK md. 134'ün işletilmesi gerekir. Öte yandan, TVDO'nun veri özelliğinden ziyade cismani varlığı ile ilgili bir delil değerlendirmesi yapılacaksa (parmak izi vs.) genel arama hükümlerine tabi olacaktır.

Yine, Siber Suçlar Sözleşmesinde "*bilgisayar sistemi*" veri işleyebilen herhangi bir cihaz veya birbiriyle bağlantılı veya ilgili bir grup cihaz olarak tanımlanmıştır²⁰⁶. TVDO'lar da ana bilgisayara bağlanabilen ve bu vesileyle veri işlenebilen aygıtlardır. Bu anlamda, TVDO'lar da bilgisayarın bir parçası olarak

²⁰⁴ Scott, s. 664.

²⁰⁵ Değirmenci, Sayısal, s. 331.

²⁰⁶ Avrupa Konseyi Siber Suçlarla Mücadele Sözleşmesi.

kullanılırlar. Buna göre ülke olarak katıldığımız Siber Suçlar Sözleşmesi'ne göre TVDO'ların da bilgisayar olarak değerlendirilmesi gerekmektedir.

Yargıtay bir kararında²⁰⁷ CD'lere uygulanması gereken koruma tedbirinin CMK md. 134 olmasına ilişkin zorunluluk bulunmadığına ilişkin karara hükmetmiştir. Yargıtay kararının gerekçesinde

Mahkeme kararına istinaden yapılan aramada sanığa ait cd'ler ve bilgisayar kasasının muhafaza altına alındığının belirtildiği, aynı gün Sulh Ceza Mahkemesi'nden el koymanın onaylanmasına dair CMK'nın 127/1 maddesi uyarınca karar alındığı ancak, arama sonrası bilgisayarların yedeklemesinin yapılıp şüpheliye verildiğine dair bir ibareye tutanakta yer verilmediği gibi, bilgisayar kütüklerinde arama yapılmasından önce mahkemeden bu hususta karar alınmadığının anlaşıldığı, bu suretle CMK'nın 134. maddesi hükümlerine riayet edilmeyerek bilgisayar kütüklerinde bilirkişi incelemesi yaptırıldığı, bilgisayar kasasında hukuka aykırı yapılan bu arama ve el koyma sonucu elde edilen delillerin de hukuka aykırı yöntemle elde edilmiş delil niteliğinde bulunduğu anlaşılmaması karşısında, yalnızca cd'lerin delil olarak kullanılabileceği;

ibaresine yer vermiştir. Yargıtay bu kararında CD'ler hakkında genel arama ve elkoyma tedbirinin uygulanacağına hükmetmiştir.

Yargıtay'ın başka bir kararında²⁰⁸ ise,
CD, DVD, flash bellek, disket, harici ve dahili harddisk, bilgisayar özelliği içeren noktaları bakımından akıllı telefon ve benzerlerinden elde edilen ve tamamı "dijital delil" olarak adlandırılan, suistimale müsait olan verilerin; sıhhatini ve güvenliğini sağlamak amacıyla ve bireyin özel hayatına, kişisel verilerine yönelik olumsuz tesirleri göz önünde tutularak "son çare" olarak başvurulabilecek "özel koşullara bağlı" bir koruma tedbiri olması nedeniyle, genel adli aramadan ayıksı ve istisnai olarak, ayrıntılı düzenlenmiş olup, bu hallerde arama kararının yalnızca hakim tarafından verilebileceği öngörülmüştür.

ibaresine yer vererek CD'ler hakkında da CMK md. 134'ün işletilmesi gerektiğine hükmetmiştir.

²⁰⁷ Yargıtay 18.CD 28.03.2016 tarih, E.2015/23959, K.2016/6096 sayılı kararı.

²⁰⁸ Yargıtay 16.CD 21.04.2016 tarih, E.2015/4672, K.2016/2330 sayılı kararı, Yargıtay CGK 04.02.2020 tarih, E.2019/286, K.2020/52 sayılı kararı.

Yine, Yargıtay’ın güncel tarihli ve bizim de katıldığımız başka bir kararında²⁰⁹

genel olarak 134. maddesinin uygulamada; bilgisayar, akıllı telefonlar, GPS cihazları, donanım ve yan donanımlar, verileri dijital olarak kaydetme ve işleme yeteneğinde olan her türlü dijital cihazları kapsadığı kabul edilmektedir. Aynı şekilde madde kapsamına; iç ağlar, veri tabanları, sistem odaları, sunucular, yedek üniteler, arşivler, veri iletim hatları, yönlendiriciler vs. dâhilinde bulunan tüm dijital alanlar, veriler ve veri taşıyıcıları da girmektedir.

ibaresine yer vererek esasen dijital veri taşıyıcılardan birisi olan CD’nin de CMK md. 134 kapsamında yer aldığını değerlendirmiştir.

Konuya ilişkin Yargıtay’ın ilk kararı ile diğer iki kararı çelişkilidir. Kanaatimizce, Yargıtay’ın CD’ler hakkında genel arama ve elkoyma tedbirinin uygulanabileceğine ilişkin değerlendirmesi hatalıdır. Yargıtay, bu kararında CD ile diğer bilişim sistemlerinde yer alan veri depolama ortamlarını ayrı tutmuştur. Ancak, önemli olan ilgili donanımın dijital veri barındırmasıdır. Nihayetinde, maddenin düzenlenme amacı, temel hak ve özgürlüklere müdahale yoğunluğunun yüksek olmasından ötürü koruma tedbirinin genel arama ve elkoyma tedbirine göre sıkı şartlara bağlanmasıdır. Dijital ortamda bulunan kişisel verinin bilgisayar hardiskinde olması ile CD üzerinde olması arasında herhangi fark bulunmamaktadır. Nitekim, pek çok CD’ye veri ekleme hususu olanaklı olduğu gibi, dijital delilin tahrif edilmesi de diğer dijital delillerle aynı derecede mümkündür. Özetle, dijital veri taşıyan tüm cihaz ve ortamlar hakkında CMK md.134 hükümleri uygulama alanı bulmalıdır.

1.3.2.3.3. Bulut Bilişim Sistemleri

Bulut bilişim, geçmiş 2000’li yıllara dayanan, “*bilişim aygıtları arasında bilgi paylaşımına imkân tanıyan hizmetlere verilen genel ad*” olarak tanımlanabilir²¹⁰. Yine bir başka ifadeyle, “*bir veri merkezinde çok sayıda sunucuyu birlikte kullanarak*

²⁰⁹ Yargıtay CGK 25.02.2020 tarih, E.2016/544, K.2020/127 sayılı kararı.

²¹⁰ Lillard, Terrence V./Garrison, Clint P/Schiller, Craig A./Steele, James, Digital Forensics For Network, Internet and Cloud Computing, Burlington 2010, s. 6’dan aktaran; Özde Dereboylular, “Bulut Bilişim Bakımından Arama ve Elkoymaya İlişkin Hükümlerin Uygulanabilirliği”, **Ceza Hukuku Dergisi**, Cilt: 14, Sayı: 39, 2019, s. 164.

bunlar üzerinde sanallaştırılmış bir platform üzerinden yazılım ve donanım servislerinin kullanılması” şeklinde²¹¹ ifade edilebilir.

Bulut bilişim, çok geniş yelpazede uygulanmış, cep telefonları, giyilebilir bilgi sistemleri gibi tüm bilişim sistemlerini içeren tüm teknolojinin omurgası haline gelmiştir²¹². Bulut bilişim ile hedef yeryüzündeki tüm cihazların birbiriyle bağlantılı ve uyumlu çalışmasını sağlamak ve veri iletişimini gerçekleştirerek ilişkilendirilmiş toplum yaratmaktır²¹³.

Bulut bilişimin toplum hayatına çok geniş yelpazede katkı sağladığı kuşkusuzdur. Ancak, suç dünyasında da bulut bilişim önemli ölçüde kullanılmaktadır. Bu bağlamda, bulut bilişim üzerinde saklanan verilere ilişkin arama usullerinin ortaya konması gerekmektedir.

Şüpheli tarafından suç işleme kastıyla bulut bilişim sistemlerinin kullanılması durumunda da CMK md. 134’ün uygulanması gerektiği söylenebilir. Bulut bilişimde kişilerin kullandığı alanlar sanal olarak sınırlandırılmaktadır. Fiziken, tek bir sunucu üzerinde birbirinden habersiz pek çok kullanıcı bulunmaktadır. Bu bağlamda; şüpheli genellikle bulut bilişim sisteminin tamamını değil, sadece kendisine sanal olarak sınırlandırılmış alanı kullanır. Bulut bilişim alanı üzerinde CMK md. 134 kapsamında arama yapılması durumunda, şüpheliye tahsis edilmiş alanla sınırlı kalmak gerekir. Aksi halde, hakkında koruma tedbiri verilen şüphelinin ötesinde çok sayıda kişinin verileri aranmış olunur ki bu da yasa koyucunun amacının aşılması anlamına gelir.

Bulut bilişim sistemlerinde arama yapmak hazırda bulunan bilişim sistemlerine nazaran daha zor olabilir. Bulut bilişim, hizmet sağlayıcı ülke sınırları içinde olabileceği gibi, ülke sınırları dışında da olabilir. Bulut bilişim, hizmet sağlayıcıda yer alan kullanıcı hesabının parola ve şifresi bilinmesi durumunda, doğrudan arama yapılabilir. Ancak, şüphelinin parola/şifresi bilinmiyorsa; söz konusu bulut bilişim hizmet sağlayıcı ülke sınırları dışında ise uluslararası adli yardımlaşma kapsamında

²¹¹ Hooper, Christopher/Ben, Martini/Choo, Kim Kwang Raymond, “Cloud Computing and Its Implications for Cybercrime Investigations in Australia”, Computer Law and Security Report 29/2, (2013), 152-163; Selvi/Küçükşille, Bulut Ortamında Adli Bilişim, s. 268.’den aktaran; Dereboylular, s. 164.

²¹² Nick Antonopoulos ve Lee Gillam, **Cloud Computing**, 2. baskı, Springer, Swindon UK, 2011, s. 3.

²¹³ İlişkilendirilmiş toplum olarak çevirdiğimiz terim öğretilde “NoE, network of everything” ve “networked society” olarak dile getirilmiştir; Antonopoulos ve Gillam, s.3.

arama yapılabilir. Ülke sınırları içinde olması durumunda ise şüphelinin hesabıyla sınırlı olmak üzere arama yapılabilir²¹⁴.

Bulut bilişim sistemlerine el koyma işlemi çoğu zaman fiilen mümkün değildir. Zira bulut bilişim sistemi ekseriyetle dağıtık mimariyi kullanmaktadır. Tek bir doya dahi genellikle tek bir sunucu belleğinde barınmamaktadır. Dosyalar aynı sunucu içerisinde birden fazla bellekte bulunabileceği gibi fiziksel olarak farklı bölgelerde de bulunuyor olabilir²¹⁵.

Bulut bilişim sistemlerinde arama işlemi çoğu zaman uzaktan arama şeklinde gerçekleştirilmektedir. Bu noktada, bazı sorunlar ortaya çıkabilmektedir. Şüphelinin genellikle, uzaktan arama yöntemiyle delil toplandığından haberi olmamaktadır. Bu sebeple, şüphelinin usul hükümlerine uyulduğunu takip etme hakkını engellediği gibi kolluk ya da üçüncü kişilerin hukuka aykırı müdahalelerinin önünü açmaktadır. Ayrıca, uzaktan arama yapılırken sıklıkla kullanılan RFS yazılımı nedeniyle verinin hash değeri alınamamakta, bu nedenle delil bütünlüğü hususunda şüpheli yaklaşımına sebep olmaktadır²¹⁶. Bu bağlamda, bulut bilişim hakkında koruma tedbirlerine özgü düzenleme yapılması uygun olacaktır.

1.3.2.3.4. Elektronik Postalar

Elektronik posta, kullanıcıların çevrimiçi bir hizmete bağlı olarak dünyanın neredeyse her yerinden bilgi iletmesine ve almasına olanak sağlayan, devrim niteliğinde bir iletişim aracıdır²¹⁷.

Bilgisayar sistemi, herhangi bir ağa bağlı olabileceği gibi bağımsız da kullanılabilir. Elektronik delil, bir elektronik araç üzerinde barındırılan veya bu araçlar vesilesiyle iletilen, soruşturma yönünden değeri olan verilerdir. Suçlular arasında yapılmış haberleşme maksatlı e-postaları ve suç örgütlenmesini gösteren veri tabanı dosyalarını elektronik deliller arasında saymak mümkündür²¹⁸.

²¹⁴ Değirmenci, Sayısal, s. 330.

²¹⁵ Dereboylular, s. 172.

²¹⁶ Özen ve Özocak, ss. 50, 51.

²¹⁷ Liz Thach, "Using Electronic Mail to Conduct Survey Research", **Educational Technology**, Cilt: 35, Sayı: 2, 1995, s. 27.

²¹⁸ Leyla Keser Berber, Adli Bilişim, Yetkin, 2004, s. 46, 50; Yargıtay CGK 26.09.2017 tarihli, E.2017/956 K.2017/370 sayılı kararı.

Elektronik postalar, dijitalleşen çağımızda klasik postanın yerini almış haberleşmenin önemli çeşitlerinden birisidir. Esasen, klasik postadan tek farkı aynı işleyişin elektronik ortamda gerçekleşmesidir. E-postada da bir alıcı bir verici bir de mesaj bulunmaktadır. Ancak burada mesaj, klasik postada olduğu gibi kâğıt formunda, insan eliyle değil, elektronik veri formunda istemci ve sunucular marifetiyle iletilmektedir.

Günümüzde e-posta çok yaygın şekilde kullanılmaktadır. Yapılan bir araştırmaya konu verilere göre, her gün yaklaşık 294 milyar e-posta gönderilmektedir²¹⁹. Günden güne bu sayı ciddi bir şekilde artmaya devam edecektir. Bu kadar e-posta, içinde mutlaka suç unsuru barındırmaktadır. Bu anlamda, e-postaya yönelik uygulanması gereken usul hükümlerinin ele alınmasında fayda bulunmaktadır.

E-posta ile iletişim, esasen Anayasa md. 22 ile korunan haberleşme hürriyetinin konusudur. Ancak, e-posta bilgisayara kaydedildiği vakit artık iletişimden ziyade özel hayatın gizliliği kapsamındadır. Öğretide; e-postanın denetlenmesi ikili ayrıma tabi tutulmuştur²²⁰. Buna göre; göre e-postanın içeriği sunucuda bulunduğu süreçte, CMK md.135-138 arasında yer alan koruma tedbirine tabidir. Bu süreçte, ortada bir iletişim hali söz konusu olup, korunmaya değer hak haberleşme hürriyeti kapsamındadır. Ancak e-posta sunucudan bilgisayara kaydedilirse artık iletişim süreci sona ermiş olup; korunmaya değer hak, özel hayatın gizliliği olacaktır. Bu bağlamda, uygulanması gereken koruma tedbiri CMK md.134 olacaktır.

Bilgisayar sistemi, herhangi bir ağa bağlı olabileceği gibi bağımsız da bulunabilir. Elektronik delil, bir elektronik araç üzerinde barındırılan veya bu araçlar vesilesiyle iletilen, soruşturma yönünden değeri olan verilerdir. Suçlular arasında yapılmış haberleşme maksatlı e-postaları ve suç örgütlenmesini gösteren veri tabanı dosyalarını elektronik deliller arasında saymak mümkündür²²¹.

²¹⁹ Ufuk Taşçı ve Ali Can, “Türkiye’de Polisin Siber Suçlarla Mücadele Politikası:1997-2014”, **Fırat Üniversitesi Sosyal Bilimler Dergisi**, Cilt: 25, Sayı: 2, 2015, s. 230.

²²⁰ Şen ve Eryıldız, s. 200; Gökhan Yaşar Duran, “Ceza Muhakemesi Kanunu’nda (CMK) Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma (CMK m.134)”, **Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 14, Sayı: 173, 2019, s. 189.

²²¹ Leyla Keser Berber, Adli Bilişim, Yetkin, 2004, s. 46, 50; Yargıtay CGK 26.09.2017 tarihli, E.2017/956 K.2017/370 sayılı kararı.

1.3.2.4. Düzenlemede Bilgisayar Teriminin Tercih Edilmesi

Mülga 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu madde 4 “*Bu Kanunda öngörülen suçların veya delillerin ortaya çıkarılması için, suçların işleniş biçimlerine benzer tutum ve davranışlarda bulunan kişilere ilişkin yer, kuruluş, çevre ve kurumdaki, Devletin ulusal güvenliği bakımından gizli kalması zorunlu olanlar hariç her türlü resmi ve özel kayıtlarla bilgisayar verileri incelenabilir.*” şeklinde düzenlenmiştir. Mülga Kanun’da bilgisayarlara ilişkin tedbir kapsamında, “*bilgisayar verileri*” terimi kullanılmıştır. CMK md. 134 ile mezkûr düzenleme tam olarak aynı değildir. Mülga Kanun’da yer alan düzenleme sadece Kanun kapsamında yer alan suçlara yönelik uygulanabileceği gibi uygulama şartları da farklıdır²²². Yine de öğretide *bilgisayar verisi* kavramının kullanılmasının daha uygun olacağını savunanlar bulunmaktadır²²³.

CMK md. 134’te yer alan koruma tedbiri; bilgisayarlar, bilgisayar programları ve kütükleri yönünden düzenlenmiştir. Söz konusu koruma tedbiri yönünden terim sorunu olduğu açıktır. Günümüzde bilgisayar artık daha özgü bir kavramdır. Oysaki, tedbir daha çok bilişim dünyasındaki tüm bilgi sistemlerini içermektedir. Adli Önleme Aramaları Yönetmeliği md. 17 ile koruma tedbirinin kapsamı genişletilmeye çalışılmış “*bilgisayar ağları*”, “*uzak bilgisayar kütükleri*” ve “*çıkarılabilir donanımların*” da söz konusu koruma tedbirine konu olabileceği düzenlenmiştir.

TCK’da ise 243-246 maddeleri arasında *bilişim alanında suçlar* üst başlığı ile bilgisayar dünyasına ilişkin suç tipleri düzenlenmiştir. Söz konusu düzenlemelerde *bilişim* teriminin tercih edilmesi, günümüz teknolojisinin geldiği nokta göz önüne alındığında uygun bir seçim olmuştur. Yine; Türk Ceza Kanunu ve Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun Teklifinde, *ısrarlı takip*²²⁴ üst başlığıyla yeni bir suç tipi öngörülmüş ve yasalaşmıştır. Madde metninde seçimlik fiiller düzenlenirken *bilişim sistemlerini* kullanarak temas kurmaya çalışmak eylemi seçimlik hareket olarak yer almış ve cezalandırılması hedeflenmiştir.

²²² Değirmenci, Sayısal, s. 317.

²²³ Çekiç, s. 159.

²²⁴ Kanun metni şu şekilde düzenlenmiştir. “*İsrarlı bir şekilde fiziken takip etmek ya da haberleşme ve iletişim araçlarını, bilişim sistemlerini veya üçüncü kişileri kullanarak temas kurmaya çalışmak suretiyle bir kimse üzerinde ciddi bir huzursuzluk oluşmasına ya da kendisinin veya yakınlarından birinin güvenliğinden endişe duymasına neden olan faile 6 aydan 2 yıla kadar hapis cezası verilir.*”

CMK md. 134'te ise mezkûr koruma tedbiri, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kopyalama ve elkoyma olarak düzenlenmiştir. Tedbirde yer alan bilgisayar kavramı, uygulamada geniş yorumlanarak diğer bilişim sistemleri yönünden de tatbik edilmektedir. Öğretide, bizim de katıldığımız hâkim görüşe göre²²⁵; söz konusu koruma tedbiri, bilgisayar ağları, diğer uzak bilgisayar kütükleri, çıkarılabilir donanımları, cep telefonları ve diğer elektronik veri barındırıcıları da içerir ayrıntılı bir düzenleme yapılması gereklidir. Öte yandan, Anayasa md. 38/6 gereği ceza muhakemesinde kullanılan delillerin kanuna uygun elde edilmiş olması gerekir. Kanun'da yer alan ifadenin neyi kapsayıp neyi kapsamadığı hususunda tereddüt bulunmaması gerekir. Ayrıca, CMK md. 1²²⁶ ile belirlenen Kanun kapsamı doğrultusunda her iki Kanun'da yer alan terimlerin birbiriyle ve günümüzle uyumlu olması uygun olacaktır. Bu şekilde Kanunların etkinliğini artacak ve uygulayıcılara ışık tutacaktır. Bu yönüyle; CMK'nın, TCK'da yer aldığı gibi *bilişim sistemi* terimini tercih etmesi ve *bilişim sistemlerinde arama* olarak düzenlenmesinin daha doğru olacağı kanaatindeyiz.

Çalışmamıza konu koruma tedbirinin konusu; *bilgisayarlar*, *bilgisayar programları* ve *bilgisayar kütükleri* olarak üç farklı hususu kapsayacak şekilde düzenlenmiştir. Esasen, bilgisayarlarda yapılan arama ile bilgisayar kütüklerinde yapılan arama ve bilgisayar programlarında yapılan arama arasında anlamlı bir fark bulunmamaktadır. Bilgisayarlarda yapılan arama, bilgisayar belleğinde olan suçla ilişkilendirilebilir veriyle sınırlıdır. Kanun koyucu sadece bilgisayarlarda arama olarak düzenleme yapmış olsaydı, arama yapılacak cihazın kapsamı değişmeyecekti. Bu bağlamda, madde metninde bilgisayar kütükleri ve bilgisayar programları olarak yapılmış ayrı düzenlemenin, uygulamaya herhangi bir katkısı olmadığı kanaatindeyiz. Öte yandan, bilgisayarlarda haricen kullanılan bellekler bilgisayar kavramı kapsamına girmediği düşünülürse, bilgisayar kütüğü kapsamına da girmeyecektir. Bu nedenle kanaatimizce işin hukuki niteliğinin yanında, teknik yönden de bilgisayarlar ile bilgisayar kütüklerinin ayrı ayrı düzenlenmesi yerine *bilişim sistemlerinde arama* şeklinde düzenlenmesinin uygun olacağı kanaatindeyiz. Ayrıca belirtmek gerekir ki, arama konusu bilgisayar verisi olmadığı durumda, söz gelimi bilgisayar kasasının

²²⁵ Yenisey ve Nuhoğlu, s. 435; Şen ve Eryıldız, s. 199.

²²⁶ CMK md. 1 “Bu Kanun, ceza muhakemesinin nasıl yapılacağı hususundaki kurallar ile bu sürece katılan kişilerin hak, yetki ve yükümlülüklerini düzenler.”

içinde saklanan uyuşturucu maddeye ilişkin arama yapılacaksa, CMK md. 134 kapsamında değil; md. 116 vd. kapsamında gerçekleştirilecektir.

1.3.3. Tedbirin Hukuki Niteliği

1.3.3.1. Genel Olarak

CMK md. 134'te yer alan bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kopyalama ve elkoyma tedbirinin; koruma tedbirlerinin özelliklerine sahip olması ve henüz hüküm verilmeden temel bir hakkı sınırlandırması²²⁷ ile maddi gerçeğin ortaya çıkarılması amaçları göz önünde bulundurulduğunda hukuki niteliğinin *koruma tedbiri* olduğu görülmektedir. Yine, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kopyalama ve el koyma tedbirinin uygulanmasına geç kalınması durumunda tedbirin konusunun imkânsız hale gelmesi mümkündür. Bu anlamda; önleme tedbirinden ziyade koruma tedbiri bulunduğu söylemek mümkündür²²⁸.

Bilişim sistemlerinde bulunan verilere ilişkin özel düzenleme niteliğindeki arama ve elkoyma tedbiri hiç olmasaydı dahi, genel arama ve elkoyma tedbirinin bilgi sistemlerine uygulanabileceği değerlendirilmektedir²²⁹. Fakat, bilişim sistemlerinde yer alan sayısal delillere özgü özelliklere istinaden böyle bir özel düzenlemenin bulunması delil niteliği yönünden yerinde olmuştur.

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kopyalama ve el koyma tedbirinin yakın tehlike durumunda ve hatta ortaya çıkmış ve failin suç işlediğine ilişkin şüphe bulunması durumunda alınır²³⁰. Mezkûr koruma tedbiri özel hayatla doğrudan ilgilidir²³¹. Bu nedenle, özel bir düzenleme gerektirmiştir. Bilgisayarda yer alan verilere el koyma, teknolojik gelişmelerle geline nokta zorunluluk haline gelmiştir. Bu bağlamda, arama ve elkoyma işleminin tıpkı genel

²²⁷ Öztürk ve diğerleri, Koruma Tedbirleri, s. 211.

²²⁸ Özbek ve diğerleri, s. 359.

²²⁹ Değirmenci, Sayısal, s. 313.

²³⁰ Özbek ve diğerleri, s. 359.

²³¹ Öztürk ve diğerleri, Koruma Tedbirleri, s. 211.

arama ve elkoyma tedbirinde olduğu gibi kanuna dayandırılması gerekmektedir²³². Aksi halde yapılacak arama, kopyalama ve elkoyma tedbiri hukuka aykırı olacaktır.

1.3.3.2. Benzer Koruma Tedbirleri ile İlişkisi

Bilişim sistemlerine özgü arama ve elkoyma tedbiri, hukuk düzenimizde CMK'da yer almaktadır. Öte yandan, diğer koruma tedbirlerinden genel arama ve elkoyma tedbiri, postada elkoyma tedbiri ile iletişimin tespiti dinlenmesi ve kayda alınması tedbirine belli oranda benzerlikler göstermekle beraber ayrıldıkları hususlar bulunmaktadır. Bu anlamda, çalışmamıza konu koruma tedbirini bu çerçevede diğer koruma tedbirleri ile karşılaştırarak değerlendirmenin yararlı olacağını düşünüyoruz.

1.3.3.2.1. Arama Tedbiri

Arama, gizlenen bir kişi ya da eşyanın bulunup ortaya çıkarılması amacıyla yapılan bir faaliyettir²³³. Arama, önleme araması ve adli arama olmak üzere ikiye ayrılır. Her iki arama da konut, işyeri, araç, kapalı alanlarda yapılabileceği gibi kişinin durdurulup üstünün aranması şekliyle de icra edilebilir.

Adli arama²³⁴, işlenmiş bir suçun aydınlatılması maksadıyla icra edilen şüpheli ya da sanığın, delil olacağı değerlendirilen gizlenen şeyin ortaya çıkarılması amacıyla yapılan konut, işyeri, araç, kapalı alanlarda gerçekleştirilen arama faaliyetidir²³⁵. Adli arama işlemi esnasında hakkında karar verilenin, özel hayatı ve aile bütünlüğü CMK ile diğer Kanunlara göre araştırılma işlemi yapılırken sınırlandırılır. Adli arama kararı, suç işlendikten sonra ya da suçun işlendiğine dair şüphenin ortaya çıkmasından sonra verilir.

²³² Dülger, s. 580.

²³³ Aldemir, s. 9.

²³⁴ Adli ve Önleme Aramaları Yönetmeliği madde 5'te adli arama tanımı şu şekilde yapılmıştır; “Adli arama, bir suç işlemek veya buna iştirak veyahut yataklık etmek makul şüphesi altında bulunan kimsenin, saklananın, şüphelinin, sanığın veya hükümlünün yakalanması ve suçun iz, eser, emare veya delillerinin elde edilmesi için bir kimsenin özel hayatının ve aile hayatının gizliliğinin sınırlandırılarak konutunda, işyerinde, kendisine ait diğer yerlerde, üzerinde, özel kâğıtlarında, eşyasında, aracında 5271 sayılı Ceza Muhakemesi Kanunu ile diğer kanunlara göre yapılan araştırma işlemidir.”

²³⁵ Gökçen ve diğerleri, s. 448.

Önleme araması²³⁶ ise, idari nitelik taşıyan, millî güvenlik ve kamu düzeninin, genel sağlık ve genel ahlâkın veya başkalarının temel hak ve hürriyetlerinin korunması, suç işlenmesinin önlenmesi, taşınması veya bulundurulması yasak olan her türlü silâh, patlayıcı madde veya eşyanın tespiti, amacıyla, hâkim kararı veya gecikmesinde sakınca bulunan hâllerde mülkî âmirin yazılı emriyle yapılan arama işlemidir.

Adli arama tedbiri, CMK md.116²³⁷ ve devamında düzenlenmiştir. İki koruma tedbiri, esasen benzer tedbirlerdir. Ancak, söz konusu tedbirler arasında tedbirin konusu, tedbire karar verme yönünden yetki ve tedbire karar verilmesi için gerekli şüphe derecesi yönünden farklılıklar bulunmaktadır.

Arama tedbiri ile bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama tedbiri arasındaki en temel fark, arama tedbirinin konusudur²³⁸. CMK md. 116'da yer alan arama tedbiri, her türlü eşyaya yönelik uygulanabilecekken; CMK md. 134'te yer alan arama tedbirinin konusunu *bilgisayar, bilgisayar programı ve kütüğü* oluşturur. Bu yönüyle; CMK md. 134, genel arama tedbirinin özel bir görünüşüdür.

CMK md.116 ile düzenlenen arama tedbirine, *sanık ve şüpheli* yönünden başvurulabileceği açıkça düzenlenmiştir. Buna göre, adli arama tedbirine, *şüpheli* ya da *sanık* sıfatı almış kişiler yönünden başvurulabilecektir²³⁹. Ancak, CMK md.134'te yer alan koruma tedbirine *sanık* yönünden başvurulabileceğine ilişkin açık düzenleme söz konusu değildir²⁴⁰. Madde metninde, bir suç dolayısıyla yapılan soruşturmadan bahsedilerek *şüpheli* yönünden koruma tedbirine karar verilebileceği düzenlenmiştir. Kovuşturma evresinde *sanık* yönünden söz konusu CMK md. 134'te yer alan tedbire başvurulup başvurulamayacağı ise öğretilerde tartışma konusu olmuştur. Çalışmamızın ilgili yerinde bu husus etraflıca ele alınmıştır.

CMK md. 116'da yer alan arama tedbiri ile CMK md. 134 ile düzenlenmiş bilişim sistemlerinde arama tedbiri arasında, ilgili koruma tedbirini kararı vermeye

²³⁶ Adli ve Önleme Aramaları Yönetmeliği madde 19 ile düzenlenmiştir.

²³⁷ CMK md.116 “*Yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe varsa; şüphelinin veya sanığın üstü, eşyası, konutu, işyeri veya ona ait diğer yerler aranabilir.*” şeklinde düzenlenmiştir.

²³⁸ Özbek ve diğerleri, s. 358.

²³⁹ Aldemir, s. 16.

²⁴⁰ Konuya ilişkin ayrıntılı açıklamalara ilgili bölümde yer verilmiştir.

yetkili kiři yönünden de ayrıık düzenleme mevcuttur. CMK md.119'a²⁴¹ göre; arama kararı vermeye yetkili kiři *hâkim*, gecikmesinde sakınca bulunan hallerde *Cumhuriyet savcısı*dır. Konut, işyeri ve kamuya açık olmayan kapalı alanlar hariç olmak üzere; Cumhuriyet savcısına ulaşılammaması durumunda ise *kolluk amirinin* yazılı emri ile kolluk görevlileri arama tedbirini gerçekleştirebilir. Kanun koyucu, madde metninde genel arama kararını verme yetkisine sahip kimseleri kademeli olarak belirlemiştir. CMK md. 134'te yer alan bilişim sistemlerinde arama tedbirinde ise, koruma tedbiri kararı verme yetkisi *hâkim* ve gecikmesinde sakınca bulunan hallerde *Cumhuriyet savcısındadır*. *Cumhuriyet savcısı* tarafından verilen kararlar ise yirmi dört saat içinde *hâkim* onayına sunulur. Hâkim konuya ilişkin kararını en geç yirmi dört saat içinde verir. *Kolluk amirine* CMK md. 134'te yer alan bilişim sistemlerinde arama tedbiri yönünden yetki verilmemiştir.

Yine, CMK md. 116'da yer alan genel arama tedbiri ile CMK md. 134 ile düzenlenen bilişim sistemlerinde arama tedbiri arasında, tedbire karar vermek için gerekli *şüphe* derecesi yönünden fark bulunmaktadır. Arama tedbirine karar vermek için kanun koyucu *makul şüphe* olmasını yeterli görmüştür. Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama tedbirinde ise kanun koyucu *somut delillere dayanan kuvvetli şüphe sebeplerinin* varlığını aramıştır. *Makul şüphe*, hayatın olağan akışına göre genellikle olaylar karşısında duyulan şüphe iken, *kuvvetli şüphe* kişinin suçu işlediğine ilişkin kuvvetle muhtemel nitelikteki şüphedir. Bu anlamda Kanun Koyucu CMK md. 134'ü çok daha sıkı şartlara bağlamıştır.

1.3.3.2.2. Elkoyma Tedbiri

Anayasamızda ve Ceza Muhakemesi Kanununda, elkoyma tedbirinin tanımı yapılmamıştır. Elkoyma tedbirinin tanımına, Adli ve Önleme Aramaları Yönetmeliği 4. Maddesinde yer verilmiştir. Buna göre elkoyma; "*Suçun veya tehlikelerin önlenmesi amacıyla veya suçun delili olabileceği veya müsadereye tâbi olduğu için,*

²⁴¹ CMK md. 119 "*Hâkim kararı üzerine veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının, Cumhuriyet savcısına ulaşamadığı hallerde ise kolluk amirinin yazılı emri ile kolluk görevlileri arama yapabilirler. Ancak, konutta, işyerinde ve kamuya açık olmayan kapalı alanlarda arama, hâkim kararı veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının yazılı emri ile yapılabilir. Kolluk amirinin yazılı emri ile yapılan arama sonuçları Cumhuriyet Başsavcılığına derhal bildirilir.*" Şeklinde düzenlenmiştir.

bir eşya üzerinde, rızası olmamasına rağmen, zilyedin tasarruf yetkisinin kaldırılması işlemini” ifade etmektedir.

Elkoyma tedbiri, CMK md. 123’te; “İspat aracı olarak yararlı görülen ya da eşya veya kazanç müsadereyesinin konusunu oluşturan malvarlığı değerleri, muhafaza altına alınır. Yanında bulunduran kişinin rızasıyla teslim etmediği bu tür eşyaya elkonulabilir.” şeklinde düzenlenmiştir.

Öğretide, elkoyma tedbiri adli elkoyma ve önleme amaçlı elkoyma şeklinde iki başlık altında incelenmektedir²⁴². Önleme amaçlı elkoyma, suç işlenmesinin önlenmesi, mili güvenliği ve kamu düzeninin genel sağlık ve ahlakın korunması amacına hizmet eden idari bir işlem iken, adli arama suç işlenmesinden sonra başvurulmuş, suç delili sayılabilecek ya da eşya ve kazanç müsadereyesine tabi eşyanın koruma altına alındığı adli bir işlemdir²⁴³.

Adli elkoyma ise; öğretide basit elkoyma ve özel elkoyma olarak ikiye ayrılmaktadır. CMK md. 123 kapsamına giren elkoyma basit elkoyma olarak nitelendirilir. İspat aracı kapsamında yararlı olduğu değerlendirilen ve müsadere konusunu oluşturan malvarlığı değerleri basit elkoyma kapsamında değerlendirilir²⁴⁴. Postada elkoyma, taşınmaz hak ve alacaklara elkoyma, bilgisayarlar, bilgisayar programlarına ve kütüklerine elkoyma ise CMK’da özel olarak düzenlenmiştir. Bu kapsamda, elkoyma tedbiri bilgisayarlar, bilgisayar programlarında ve kütüklerinde gerçekleştirilmesi durumunda bilişim sistemlerine özgü bir koruma tedbiri olacaktır.

CMK md. 134 ile düzenlenen bilişim sistemlerine elkoyma tedbirine başvurabilmek için Cumhuriyet savcısının konuya ilişkin istemi bulunması gerekir. Ancak Cumhuriyet savcısı istemde bulunduktan sonra hâkim tedbir kararını alabilir. Basit elkoyma tedbirinde, hâkim kararının yanında gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı elkoyma kararı verebilir. Bununla birlikte; bilgisayarlar, bilgisayar programlarına ve kütüklerine elkoyma tedbirinde Cumhuriyet savcısının gecikmesinde sakınca bulunan hallerde dahi²⁴⁵ elkoyma kararı verme yetkisi bulunmamaktadır²⁴⁶.

²⁴² Şen ve Eryıldız, s. 20.

²⁴³ Şen ve Eryıldız, s. 20; Aldemir, s. 13.

²⁴⁴ Şen ve Eryıldız, s. 20.

²⁴⁵ Kanunda arama kararı yönünden savcı yetkisi tanımlanmış olmasına rağmen elkoyma yönünden bu yetki tanımlanmamıştır.

²⁴⁶ Öztürk ve diğerleri, Koruma Tedbirleri, s. 212.

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde elkoyma; bilgisayarda yer alan verilere inceleme amacıyla geçici elkoyma mahiyetindedir. CMK md. 134'e göre asıl olan ilgili bilişim sistemine değil bilişim sisteminde yer alan verilere hatta bunların bir kopyasına elkoymadır. Tedbirinin hukuki hedefi, bilişim sistemlerinde yer alan dijital verilerdir. Tedbir, bilgisayarın maddi varlığıyla doğrudan ilişkili olmayıp, tedbire konu eşyanın mülkiyetini sonlandırmayı hedeflememektedir. Oysa klasik elkoyma, tedbire konu eşyanın maddi varlığına ilişkindir. Klasik elkoyma tedbirine karar verildiğinde eşyanın mülkiyeti sonlandırılmaktadır.

1.3.3.2.3. Postada Elkoyma Tedbiri

İnsanoğlu, geçmişten günümüze çağın ortaya koyduğu teknoloji doğrultusunda iletişimde kalmıştır. Nitekim, bu iletişim suç işlemek adına da kullanılmaktadır. Postada elkoyma, elkoyma tedbirinin özel bir şeklidir. Postada elkoyma terimi ile eşya mahiyetindeki mektup, koli, kutu, paket gibi maddi varlık hakkında gerçekleştirilebileceği gibi; telgraf, teleks gibi haberleşmenin denetlenmesine ilişkin de olabilir²⁴⁷. Postada elkoyma, resmi ve özel kuruluşların gönderileri hakkında uygulanabilir. Yine, postada elkoyma tedbiri kargo şirketlerinin gönderilerinin benzer şekilde otobüs firmalarının taşıdığı gönderiler hakkında da uygulanabilir²⁴⁸.

Postada elkoyma CMK md.129²⁴⁹ ile düzenlenmiştir. Buna göre, Kanun koyucu postada elkoyma kararı verme yetkisini kural olarak *hâkime*, gecikmesinde sakınca bulunan hallerde ise *Cumhuriyet savcısına* vermiştir. Kanun koyucu, genel arama tedbirinin aksine *kolluk amirine* yetki vermemiştir. Bu noktada, özel bir elkoyma tedbiri olarak, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde elkoyma ile benzer özellik göstermektedir. Öte yandan, CMK md.129 incelendiğinde, postada elkoyma tedbiri doğrudan ya da dolaylı olarak posta hizmeti veren kuruluşlar

²⁴⁷ Gökçen ve diğerleri, s. 483.

²⁴⁸ Ünver ve Hakeri, s. 926.

²⁴⁹ CMK md. 129 şu şekilde düzenlenmiştir; “Suçun delillerini oluşturduğundan şüphe edilen ve gerçeğin ortaya çıkarılması için soruşturma ve kovuşturmada adliyenin eli altında olması zorunlu sayılıp, posta hizmeti veren her türlü resmî veya özel kuruluştaki bulunan gönderilere, hâkimin veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının kararı ile elkonulabilir.”

hakkında uygulanabileceğinden söz konusu tedbirin bilgisayarlar yönünden uygulanması söz konusu değildir²⁵⁰.

1.3.3.2.4. İletişimin Tespiti, Dinlenmesi ve Kayda Alınması Tedbiri

CMK madde 135 ile iletişimin tespiti, dinlenmesi ve kayda alınması tedbiri düzenlenmiştir. CMK madde 135'in uygulanması için ortada bir iletişim aracı bulunması gerekir. Kişilerin yüz yüze yaptığı görüşmeye ilişkin alınan tedbir CMK md.135'in konusunu oluşturmamaktadır²⁵¹.

CMK'da yer alan her iki koruma tedbiri incelendiğinde; tedbirlerin konusuna ilişkin bir ayırım olduğu görülmektedir. CMK md. 134 ile düzenlenen bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kopyalama ve elkoyma tedbirinin konusu *bilgisayar, bilgisayar programı* ya da *bilgisayar kütüğüdür*. Dolayısıyla tedbir ancak bu cihazlar hakkında uygulanabilir. Ancak, iletişimin tespiti, dinlenmesi ve kayda alınması tedbirinin konusu iletişim olmakla beraber, bu iletişim maddi varlığa sahip bir bilgisayarla gerçekleştirebileceği gibi herhangi başka bir vasıta ile de gerçekleştirilebilir.

CMK md. 135'te yer alan iletişimin tespiti, dinlenmesi ve kayda alınması tedbiri niteliği itibariyle gizli uygulanması gerekir. Kişi, iletişim kurarken hakkında söz konusu tedbirin uygulandığı konusunda bilgisi olmayacaktır. Gerçekten de tedbirle ulaşılmak istenen amaç, hakkında tedbir uygulanan kişiden takip edildiği izlenimi uyandırmadan suça ilişkin bilgi edinmektir²⁵². Oysa, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirine başvurulması durumunda uygulama esnasında gizlilik unsuru aranmaz. Söz konusu tedbir uygulanırken, şüpheli ya da sanık konuya ilişkin bilgilendirilir.

Yine, iletişimin tespiti, dinlenmesi ve kayda alınması tedbirine başvurulabilmesi için ortada iletişim olması gerekir. Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kopyalama ve elkoyma tedbirine başvurma'nın ön koşulu iletişimin varlığı değildir²⁵³. Bilgisayarlar, bilgisayar programı ya da

²⁵⁰ Özbek ve diğerleri, s. 390.

²⁵¹ Öztürk ve diğerleri, CMK, s. 356.

²⁵² Gökçen ve diğerleri, s. 498.

²⁵³ Özbek ve diğerleri, s. 357.

bilgisayar kütüğünün iletişimde kullanılmamış olması halinde de CMK md. 134 kapsamında tedbire başvurulabilir.

Kanun koyucu iletişimin denetlenmesine ilişkin dinlenme, kayda alma ve sinyal bilgilerinin değerlendirilmesi konusunda tedbire başvurulması için madde metninde belli suç tiplerinin varlığını aramıştır. Bu anlamda, iletişimin tespitine ilişkin ayrıık düzenleme yapılmış ve iletişimin tespitine tüm suçlar yönünden başvurulabileceği düzenlenmiştir. Bilgisayarlarda, bilgisayar programı ya da kütüklerinde arama kopyalama ve elkoyma tedbirinde ise herhangi bir kısıtlama öngörölmemiştir. Söz konusu tedbire tüm suçlar yönünden başvurmak mümkündür.

Günümüz teknolojisinde kişiler arası ya da kitleler arası iletişimde sadece sesli ya da metin formatı kullanılmamaktadır. Artık, resimli, görüntölü farklı şekilde verilerden oluşan pek çok iletişim türü kullanılabilmektedir. Bu anlamda bilişim sistemleri iletişim amacıyla oldukça yaygın kullanılmaktadır. Bilişim sistemlerinin iletişimde kullanılması halinde hangi koruma tedbirinin uygulanması gerektiğine ilişkin öğretide ikili ayrıma gidilmiştir. Buna göre, bilişim sistemlerinde iletişim esnasında kullanılan verilerin akış halinde tespit edilmesi durumunda CMK md. 135; bilişim sistemlerinde verilerin durağan halde tespit edilmesi durumunda ise CMK md. 134 uygulanacaktır²⁵⁴.

Öğretideki görüşe²⁵⁵ ve Yargıtay kararına göre²⁵⁶, şüphelinin, internet ortamında sosyal medya uygulamaları ve çeşitli platformlarda gerçekleştirdiği iletişime ilişkin kayıtların aranması; CMK md. 135'e göre değil, CMK md. 134'e göre yapılması gerekir. Nitekim, kişinin iletişim sürecindeki görüşmeler ve dosya alışverişleri bilgisayarın kütüğüne kaydedilmektedir. Kayıt sonrası iletişimi ilişkin tüm detaylar CMK md. 134 kapsamındaki birer veriye dönüşmektedir.

CMK md.134 ile CMK md. 135 uygulanması arasında koruma tedbirinin amacı olan delilin oluşma anıyla alakalı bir ayrım bulunmaktadır. CMK md. 135 geleceğe yönelik düzenlenmiş iletişimin tespitine ilişkindir. CMK md. 135 ile geçmişte gerçekleşen bir iletişim dinlenmesi ve kayda alınması mümkün değildir. Ancak ileride gerçekleşecek olan iletişime ilişkin uygulanır. CMK md. 134 ise geçmişte oluşturulmuş dijital verilere dair uygulanır. Bu kapsamda; internet, sosyal medya ve

²⁵⁴ Dölger, s. 581.

²⁵⁵ Şahin, s. 280.

²⁵⁶ Yargıtay 16. CD. 24.04.2017 tarih, E.2015/3 K.2017/3 sayılı kararı.

üçüncü parti yazılımlar marifetiyle oluşturulan ve bilgisayar kütüğüne kayıt altına alınmış verilere ilişkin CMK md. 134 uygulama alanı bulacaktır²⁵⁷.

1.3.4. Tedbirin Temel Hak ve Özgürlüklerle İlişkisi

“Avrupa Birliği Genel Veri Koruma Tüzüğü” (GDPR), kişisel verilerin korunmasına ilişkin önemli bir düzenlemedir. Söz konusu tüzük’ün 4. maddesinde “*kişisel veri*” şu şekilde tanımlanmıştır. “*Kişisel veri tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgidir.*” Aynı maddenin devamında “*veri sahibi*” ise; “*tanımlanmış bir gerçek kişi özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir;*” şeklinde tanımlanmıştır. Bir bilgisayarın içinde yer alan verilerde arama ile bilgisayar ağlarında bulunan verinin araması farklı hususlar olup ayrı nitelikteki işlemlerdir. Kişisel verileri elde etmek için usulüne uygun arama kararı verilmesi gerekir²⁵⁸.

Teknolojinin gelişmesiyle birlikte kişisel veriler de önemli ölçüde dijitalleşmiştir. Bireyler kendilerine dair her türlü veri, belge, resim, video gibi içerikleri dijital ortamlarda oluşturmakta ve saklamaktadır. CMK’da yer alan bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama ve elkoyma tedbiri, temel hak ve özgürlükleri hüküm verilmeden önce önemli şekilde sınırlandırmaktadır²⁵⁹. Söz konusu tedbir özellikle, Anayasamızda düzenlenip koruma altına alınmış özel hayatın gizliliği ve korunması, mülkiyet hakkı gibi temel hak ve özgürlüklerle yakından ilişkilidir. Bilgisayarlarda, bilgisayar programları ve kütüklerinde arama ve elkoyma tedbiri niteliği itibarıyla devlet eliyle kişinin mülkiyet hakkını geçici olarak kısıtlayarak, bireyin özel alanına girilmesidir. Bu nedenle, söz konusu koruma tedbirine ilişkin özel bir düzenleme yapılması yerinde olmuştur.

Bilişim sistemlerinde yapılacak arama, şüphelinin kullanımında olan bilgisayarda gerçekleştirilir. Yapılacak arama, suça konu verinin bulunmasından ibaret

²⁵⁷ Yusuf Yaşar ve İsmail Dursun, “Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt: 19, Sayı: 3, 2013, s. 23.

²⁵⁸ Yenisey ve Nuhoglu, s. 429.

²⁵⁹ Duran, s. 182.

olması gerekir. Şüpheli tarafından kullanılmış tüm bilgisayarlarda arama yapılması yahut şüphelinin bilgisayarında suça ilişkin veriyle sınırlamaksızın sistemde yer alan tüm verilerde arama yapılması ölçülülük ilkesi bakımından tereddüte yol açacak özel hayatın gizliliğini ihlal mahiyeti kazanacaktır²⁶⁰. Nihayetinde, kişilerin kendine ait olan bilişim sistemleri, kişiler arası iletişim kayıtları, özel hayata ilişkin resim ve belgeler, okunan gazeteler, siyasi parti düşünceleri gibi pek çok ayrıntı barındıran sırdaşları gibidir²⁶¹. Kişinin bilişim sistemlerine ilişkin özel hayat beklentisi her somut olaya göre değerlendirilmesi gerekir. Örneğin, kişi bilişim sistemini satmış ya da herhangi bir şekilde rızası ile üçüncü kişiye devretmişse bu noktada özel hayat beklentisi kalmamıştır. Ancak kişi devir öncesi verilerini silmiş ise özel hayat beklentisinin sürdüğü söylenebilir²⁶².

Şirket bilgisayarları, prensip olarak şirket ihtiyaçlarına ve ticari faaliyetlere özgülenmiştir. Yenisey/Nuhoğlu'na göre, şirket bilgisayarlarındaki verilerin özel hayat alanına girmemesi nedeniyle bireyin ilgili bilgisayarda özel hayat beklentisi olamaz²⁶³. Ancak kanaatimizce, şirket bilgisayarı da olsa, bu bilgisayarda kişi özel bir dosya/dizin açmış ve bu dosyadan özel hayat beklentisi anlaşılıyor ise bu durumda CMK md. 134 hükümleri uygulanması gerekir.

Bir bilgisayar içerisinde yer alan tüm verilerin gelişigüzel açılarak içine bakılması özel hayatın gizliliğini ihlal mahiyetindedir²⁶⁴. AİHM; bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kopyalama ve elkoyma koruma tedbirinin usulüne uygun yürütülmemesi durumunu AİHS md. 8²⁶⁵'e göre incelemiştir. AİHM, özel hayatın gizliliğinin sınırlandırılması hakkında AİHS md.8/2'de yer alan şartları somutlaştırarak, müdahalenin; “*orantılı olması*”, “*demokratik toplumda gerekli*

²⁶⁰ Uğraş, s. 103.

²⁶¹ Rezan Epözdemir, “Bilişim Sistemlerinde Arama ve Elkoyma Tedbirleri”, **Terazi Hukuk Dergisi**, Cilt: 13, Sayı: 142, 2018, s. 91.

²⁶² Duran, s. 184.

²⁶³ Ayrıca mukayeseli hukukta 25.07.2008 tarihli US v. Edward Mosby kararında iş için kullanılan bilgisayarlarda “işe ilişkin davranışlar” açısından arama yapılması için hakim kararına gerek görülmemiştir; Yenisey ve Nuhoğlu, s. 450.

²⁶⁴ Yenisey ve Nuhoğlu, s. 443.

²⁶⁵ AİHS md. 8; “1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.” şeklinde düzenlenmiştir.

olması”, “*meşru amaç taşıması*”, “*kanunla öngörülmüş olması*” şeklinde ifade etmiştir²⁶⁶.

AİHM’nin bazı kararlarında bilişim sistemlerinde arama ve elkoyma tedbiri orantılı şekilde uygulanması gerektiğini belirterek, müdahalede ölçünün aşılmasını hukuka aykırı bularak amaçla uyumlu olmasını gerektiğini değerlendirmiştir²⁶⁷. AİHM bir kararında²⁶⁸, Smirnov isimli avukat müştekinin bilgisayarının, 6 günden daha uzun bir süre zarfında alıkonulmasının herhangi bir nedeni olmadığı, müştekinin bilgisayarının mesleğini ifa etmesi için kullandığı bir araç olduğunu ve elkoyma tedbirinin, müştekinin mesleki faaliyetlerini bozduğunu belirterek söz konusu tedbir ile Rus adli makamlarının toplumun genel çıkarları ile müşteki olan avukatın hakları arasındaki adil dengeye müdahalede başarısız olduğundan bahisle yapılan işlemi hukuka aykırı bulmuştur²⁶⁹.

AİHM, Ernst ve Diğerleri/Belçika kararında²⁷⁰, CD, bilgisayar ve bilgisayar belleklerinin bulunduğu pek çok eşyaya elkonulmasını ve fakat elkoymaya ilişkin başvurularda gerçek sebeplerinin bildirilmemesini AİHS md.8’in ihlali anlamına geldiğini değerlendirmiştir. Mahkeme, soruşturma esnasında aramalara ilişkin geniş terime yer verildiğini arama konusun girilecek yerin net bir şekilde belirtilmediğini, bu nedenle müdahalenin meşru amaçla orantısız olduğunu değerlendirmiştir.

CMK md.134 kapsamında uygulanan koruma tedbirinin ihlal ettiği bir diğer temel hak ise mülkiyet hakkıdır. Anayasa mahkemesi bir kararında²⁷¹; ilgili koruma tedbirinin mülkiyet hakkını ihlal etmemesi ve Anayasa’nın 13. ve 35. maddelerine uygun olabilmesi için, “*müdahalenin kanuna dayanması*”, “*kamu yararı amacı taşıması*” ve ayrıca “*ölçülülük ilkesi*” gözetilerek yapılması gerektiğine hükmetmiştir. Kanunilik ilkesini ararken CMK md. 134 ile yapılan düzenlemeyi yeterli görmüştür. Müdahalenin ceza muhakemesi esnasında maddi gerçeğin ortaya çıkarılması amacını taşıması nedeniyle kamu yararına dayalı meşru amacın varlığını da kabul etmiştir. Ölçülülük ilkesine uygunluğu ise, kamu makamlarınca mülkiyet hakkına yapılan

²⁶⁶ Yaşar ve Dursun, s. 31.

²⁶⁷ Değirmenci, Sayısal, s. 381.

²⁶⁸ AİHM Smirnov/Rusya Kararı; AİHM, [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-76823%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-76823%22]}), (11.04.2022)

²⁶⁹ Ünal, s. 131.

²⁷⁰ Yaşar ve Dursun, s. 31.; AİHM, [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-65779%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-65779%22]}), (11.04.2022)

²⁷¹ Anayasa Mahkemesinin 26.12.2018 tarih ve 2015/19961 numaralı bireysel başvuru kararı.

müdahaleyle gerçekleştirilmek istenen amaç ile bu amacı gerçekleştirmek için kullanılan araçlar arasında makul bir ölçülülük ilişkisinin varlığını araştırarak tespit etmiştir.

1.3.5. CMK md. 134'e İlişkin Yasa Değişiklikleri

1.3.5.1. 6526 Sayılı Yasa

6526 sayılı yasanın ile 11. maddesi²⁷² ile CMK md. 134'te iki önemli değişiklik yapılmıştır. Bunlardan birincisi, şüpheli hakkında arama kararı verebilmek için olması gereken şüphe derecesidir. Diğeri ise maddenin 4. fıkrasında yer alan yedekten yapılan kopyalama işleminin bir kopyasının şüpheliye veya vekiline verilmesine ilişkin husustur.

Kural olarak, soruşturma evresinde başvurulacak bir tedbir olan bilgisayarlar, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirine karar vermek için şüphe yönünden düzenlenme bulunmamaktaydı. Öğretide, bu durumda Alman CMK da yer aldığı gibi şüphe derecesinin *basit şüphe* seviyesinde olması gerektiğini savunan yazarların yanında *makul şüphenin* gerekeceğini savunanlar da olmuştur²⁷³.

6526 sayılı yasa ile öngörülen şüphe derecesi *kuvvetli şüphe sebebi* olmuştur. Yine, aynı yasa ile kuvvetli şüphe sebebinin *somut delillere* dayanması da aranmıştır. Böylece CMK md. 134'te yer alan tedbirin uygulama şartları sıkılaştırılmıştır.

Bilişim sistemlerine özgü koruma tedbiri kapsamında, bilgisayarlar veya bilgisayar kütüklerine elkoyma işlemi sırasında sistemde yer alan bütün verilerin yedeklemesi yapılır. Bu yedekten alınan kopya, 6526 sayılı yasa öncesinde şüpheli veya müştekinin talep etmesi durumunda kendilerine verilmekteydi. Ancak bu durum bilişim sistemlerine ilişkin verilerin hassas yapısı ve verilerin kolayca değiştirilebilme ihtimali karşısında şüpheliyi korumamaktaydı. Nitekim, şüphelinin bu hakkını bilmesi bir yana birçok avukat dahi söz konusu hakkı bilmemekteydi. Yasa değişikliği ile bu

²⁷² 6526 sayılı Kanun md. 11; “5271 sayılı Kanunun 134 üncü maddesinin birinci fıkrasında yer alan “soruşturmada,” ibaresinden sonra gelmek üzere “somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve” ibaresi eklenmiş ve dördüncü fıkrasında yer alan “İstemesi halinde, bu” ibaresi “Üçüncü fıkraya göre alınan” şeklinde değiştirilmiştir.”

²⁷³ Değirmenci, Sayısal, s. 350.

durum isteğe bağlı olmaktan çıkarılarak, zorunlu hale getirilmiştir. Bu anlamda, söz konusu düzenleme oldukça yararlı olmuştur.

1.3.5.2. 7145 Sayılı Yasa

7145 sayılı yasanın 16. maddesi ile CMK md.134'te yer alan koruma tedbirinin birinci ve ikinci fıkralarında değişiklik yapılmıştır. Birinci fıkrada yapılan değişiklik ile tedbire karar verme yetkisi Cumhuriyet savcısı yönünden düzenlenmiş, ikinci fıkra ile bilişim sistemlerine elkoyma için gerekli istisnai şartlara *işlemin uzun sürecektir* olması durumu da eklenmiştir.

7145 sayılı yasa öncesinde; bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kopyalama ve elkoyma tedbirine karar verme yetkisi mutlak olarak hâkime tanınmıştı. Buna göre, diğer şartların gerçekleşmesi durumunda cumhuriyet savcısı istemiyle, yetkili sulh ceza hâkimi söz konusu koruma tedbirine karar vermektedir. Bu durum, öğretilde bilişim teknolojilerindeki hız ve değişkenlikle, delillere müdahalede ivedilik gerektirmesi nedeniyle eleştirilmiş ve gecikmesinde sakınca bulunan hallerde cumhuriyet savcısının da koruma tedbirine karar verebilmesinin yerinde olacağı değerlendirilmiştir²⁷⁴.

OHAL döneminde ise; 668 sayılı KHK ile gecikmesinde sakınca bulunan hallerde cumhuriyet savcısına belli şartlarda CMK md.134'e başvurma yetkisi tanınmıştır²⁷⁵. OHAL döneminde KHK kapsamında beş ve on günlük süreler düzenlenmiştir. Cumhuriyet savcısı tarafından doğrudan karar verilmesi durumunda; söz konusu karar, beş gün içinde hâkim onayına sunulmak zorundaydı. Yine, hâkim kararını elkoymadan on gün içinde açıklamak durumundaydı. Nitekim; hâkim kararını açıklamazsa, bu durum zımni ret niteliğinde olup tedbirin kendiliğinden kalkması sonucunu doğurmaktaydı.

²⁷⁴ Başlar, Usul, s. 90.

²⁷⁵ 668 sayılı KHK md.3/1(j): "5271 sayılı Kanunun 134 üncü maddesi uyarınca bilgisayarlarda, bilgisayar programlarında ve kütüklerinde yapılacak arama, kopyalama ve elkoyma işlemlerine, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da karar verilebilir. Bu karar, beş gün içinde görevli hâkimin onayına sunulur. Hâkim, kararını elkoymadan itibaren on gün içinde açıklar; aksi halde elkoyma kendiliğinden kalkar. Kopyalama ve yedekleme işleminin uzun sürecektir olması halinde bu araç ve gereçlere elkonulabilir. İşlemlerin tamamlanması üzerine elkonulan cihazlar gecikme olmaksızın iade edilir."

7145 sayılı Kanun md.16 ile yapılan düzenleme²⁷⁶ doğrultusunda, CMK md. 134 günümüzdeki şeklini almış ve Cumhuriyet savcısına gecikmesinde sakınca bulunan hallerde CMK md. 134'e başvurma yetkisi tanınmıştır²⁷⁷. Ancak, Cumhuriyet savcısı gecikmede sakınca bulunan hali gerekçelendirmek durumundadır. Gecikmesi durumunda makul bir sakınca bulunmadığı halde Cumhuriyet savcısının koruma tedbirine başvurması hukuka aykırı olacaktır.

Öğretide²⁷⁸, yapılan değişikliklerle birlikte Cumhuriyet savcısına yetki verilmesi hususunda çekinceler dile getirilmiştir. Yazara göre, koruma tedbirine başvurunca henüz tedbir yerine getirilmeden yapılan hâkim incelemesi ile Cumhuriyet savcısının talimatı neticesinde hali hazırda yerine getirilmiş olan kararın incelemesi aynı titizlikle gerçekleşmeyecektir.

Yine, 7145 sayılı yasa ile yapılan düzenleme ile beş ve on günlük süreler kaldırılmıştır. Bu süreler yerine, Cumhuriyet savcısının kararını, yirmi dört saat içinde onaya sunması gerektiği düzenlenmiştir. Kanun koyucu, hâkime, yirmi dört saatlik karar verme süresi tanımıştır. Bu süre içerisinde karar verilememesi yahut hâkim tarafından Cumhuriyet savcısının kararının aksine karar verilmesi halinde çıkarılan kopyalar ve çözümü yapılan merinler derhal imha edilmesi gerekecektir.

7145 sayılı Kanun ile CMK md. 134'te yapılan bir diğer düzenleme elkoyma şartlarına ilişkindir. Yasa ile CMK'da yer alan koruma tedbiri yönünden bilişim sistemlerine elkoyma şartı genişletilmiştir. Buna göre, koruma tedbirinin uygulanma safhasında *işlemin uzun süreceği olması durumunda ilgili bilişim sistemine elkonulabilir.*

²⁷⁶ 7145 sayılı Kanun md. 16: "5271 sayılı Kanunun 134 üncü maddesinin birinci fıkrasında yer alan "Cumhuriyet savcısının istemi üzerine" ibaresi "hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından" şeklinde değiştirilmiş, fıkra da yer alan "hâkim tarafından" ibaresi madde metninden çıkarılmış, fıkra ya aşağıdaki cümleler eklenmiş ve ikinci fıkrasına "bilgilere ulaşılabilmesi" ibaresinden sonra gelmek üzere "ya da işlemin uzun süreceği olması" ibaresi eklenmiştir."

"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."

²⁷⁷ Öğretide, söz konusu tedbire sadece hâkim tarafından karar verilmesi gerektiğini değerlendirerek, cumhuriyet savcısının gecikmesinde sakınca bulunan hallerde dahi bu yetkiye sahip olmaması gerektiğini savunan yazarlar bulunmaktadır. Şen ve Eryıldız, s. 203.

²⁷⁸ Değirmenci, 7145, s. 151.

İşlemin uzun sürecektir olması durumunda yapılacak elkoyma tedbirini uygulayan kolluk kuvvetlerinin hangi gerekçelerle işlemin uzun sürdüğünü açıklayan bir tutanak tutması gerekmektedir.



İKİNCİ BÖLÜM

BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA ARAMA, KOPYALAMA VE ELKOYMA KORUMA TEDBİRİNİN ŞARTLARI VE UYGULANMASI

2.1. BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA KOPYALAMA VE ELKOYMA TEDBİRİNİN ŞARTLARI

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kopyalama ve elkoyma tedbirine başvurmak için Kanun koyucu, suç yönünden bir kısıtlama getirmemiştir. Bu anlamda, her suç tipi için uygun koşullar oluştuğunda söz konusu tedbire başvurulabilir.

Madde, kural olarak bir arama tedbiri niteliğindedir. Ancak, istisnai hallerde madde kapsamında elkoymaya da karar verilebilir. Bu yönüyle, söz konusu tedbire başvurabilmek için arama ve elkoyma yönünden ortaya konan şartların ayrı ayrı değerlendirilmesi Kanunun sistematığına uygun olacaktır.

2.1.1. Arama ve Kopyalama Yönünden

Bilgisayar ya da bilgisayar niteliğindeki cihazlarda yer alan veriler belli bir sistematik çerçevesinde saklanır. Örneğin, fotoğraf, video, doküman gibi belgeler; bilgisayarlarda dosyalar halinde dizinlenerek saklanır. Durumu somutlaştırmak adına; her bir dosyayı konut, verileri ise konutun içindeki eşyalar gibi düşünebiliriz. Bu verileri aramak konutun içinde yer alan eşyaları aramak gibidir. Konutta yer alan tek bir eşya için tüm konuta elkoymak gibi suça konu tek bir veri için tüm bilişim sistemine elkoymak hukuka aykırıdır²⁷⁹.

Bilgisayarlarda arama, sadece arama kararında gösterilen arama konusu ile sınırlıdır. Uzman personel aramayı tedbirin konusu veri ile sınırlı tutmalıdır. Bunun yerine tüm bilişim sistemlerinde yer alan tüm verilerin tek tek incelenmesi toplu arama kararı niteliğinde olup hukuka aykırıdır.

²⁷⁹ Yenisey ve Nuhoğlu, s. 436.

Kanun koyucu, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama tedbirine başvurabilmek için belli şartlar öngörmüştür. Söz konusu şartları aşağıda yer alan başlıklar altında incelemek uygun olacaktır.

2.1.1.1. Suç Dolayısıyla Yürütülen Bir Soruşturmanın Varlığı

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama tedbirine başvurabilmek için öncelikle soruşturmanın varlığı gerekmektedir. Gerçekten de yasa koyucu maddeyi düzenlerken “*bir suç dolayısıyla yapılan soruşturmada*” ibaresine yer vererek koruma tedbirine başvurulması için suça ilişkin soruşturmanın bulunması gerekliliğine açıkça yer vermiştir. Yine, söz konusu maddenin devamında *şüphelinin* kullandığı bilişim sistemlerine ilişkin düzenlemede bulunmuş ve fakat *sanık* sıfatı zikredilmemiştir. Öte yandan, tedbire karar verme yetkisi düzenlenirken de *hâkimin* yetkisi açıkça düzenlenmiş; *mahkemenin* yetkisine yer verilmemiştir.

Yasanın açık hükmü karşısında, mezkûr tedbire başvurma olanağı soruşturma evresi ile kısıtlı olup olmayacağı eş deyişle kovuşturma evresinde söz konusu tedbire başvurulup başvurulamayacağı hususu öğretide tartışılmıştır.

Yenisey/Nuhoğlu’na göre²⁸⁰, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama yapabilmek için evvela suça ilişkin soruşturma yapılması gerekir. Yine Kanun açık hükmüne göre bu tedbire sadece soruşturma evresinde başvurulabilir.

Ünver ve Hakeri ise²⁸¹, söz konusu koruma tedbirinin sadece soruşturma evresi yönünden düzenlenmiş olmasını hatalı olduğunu değerlendirmekte ve buna karşın uygulamada tedbirin kovuşturma evresinde de başvurulmasının kanunilik ilkesine aykırı olduğunu ve bu kapsamda toplanan delillerin hukuka aykırı olduğunu savunmaktadır.

Aldemir’e göre²⁸², söz konusu koruma tedbirine sadece soruşturma evresinde başvurulabilecek, kovuşturma evresinde koruma tedbirine başvurulamayacak, kamu davası açılması durumunda ise mahkeme CMK md.174-1/b doğrultusunda eksik delil toplanmasından bahisle iddianameyi iade edecektir.

²⁸⁰ Yenisey ve Nuhoğlu, s. 232.

²⁸¹ Ünver ve Hakeri, s. 937.

²⁸² Aldemir, s.179.

Yukarıda yer verdiğimiz bizim de katıldığımız görüşlerin²⁸³ ortak yönü, Kanunun açık düzenlemesine göre, söz konusu tedbire sadece soruşturma evresinde başvurulabileceği, kıyas yoluyla hükmün genişletilerek kovuşturma evresinde uygulanamayacağıdır. Ancak, kovuşturma evresinde CMK md. 134'e başvurma zorunluluğu doğduğu takdirde, aynı suça ilişkin yeniden soruşturma evresine dönülemeyeceğinden ortada yasal boşluk meydana gelecektir. Ayrıca, kovuşturma evresinde aleni bir duruşmada mahkemenin söz konusu tedbire karar vermesi halinde bilgi sistemleri kayıtlarının silinmesinin önü açılacak ve tedbir yarar sağlamayacaktır²⁸⁴. Gerçekten de gelişen teknoloji, delillerin hızlı ve geri dönülemez şekilde ortadan kaldırılmasına olanak sağlamaktadır. Tek bir komutla mahkemede bulunan kişi çevrimiçi her tür bilgi sistemine erişim sağlayabilmekte ve anında tedbire konu olacak verileri başka bir ortama taşıyabilmekte ya da ortadan kaldıracılabilmektedir. Bu nedenle, bilişim sistemlerine yönelik tedbirlerin, soruşturma evresinde yerine getirilmesi soruşturmanın etkinliği açısından önem arz etmektedir.

CMK md. 134'e kovuşturma evresinde başvurulabileceğini savunan yazarlar da bulunmaktadır. Bir görüşe²⁸⁵ göre, madde metninde mezkûr tedbire sadece soruşturma evresinde başvurulabileceği düşünülse de yargılama esnasında delil toplamaya engel bir hüküm olmaması, mahkemenin resen delil toplama yetkisinin bulunması nedenleriyle kovuşturma evresinde de söz konusu tedbire başvurmak mümkündür. Bir diğer görüşe²⁸⁶ göre ise; söz konusu koruma tedbirinin şartlarından birisinin suç soruşturmasının varlığı olmasına rağmen, bu şart dar yorumlanmamalı, kovuşturma evresinde eksik delil olması durumunda yine CMK md. 134 kapsamında tedbire karar verilebilmelidir. Başka bir görüşe²⁸⁷ göre ise, kamu davasının açılması için “yeterli şüphe” gerektiği, mahkemenin somut olayda yeterli şüphe görmemesi ve suçun sübuta ermesi için gerekli gördüğü koruma tedbirine istem üzerine yahut re'sen başvurabilecektir.

²⁸³ Aynı yönde görüş için bkz; Şen ve Eryıldız, s. 204.

²⁸⁴ Nur Centel ve Hamide Zafer, **Ceza Muhakemesi Hukuku**, Beta Basımevi, İstanbul, 2018, s. 459.

²⁸⁵ Şahin ve Göktürk, CMK-1, s. 355.

²⁸⁶ Özen ve Özocak, s. 63.

²⁸⁷ Yaşar ve Dursun, s. 10.

Yargıtay bir kararında²⁸⁸, yerel mahkemenin kararını bozmuş ve gerekçesinde sanığın suçlamayı kabul etmeyerek kullandığı modemın şifreli olduğunu, kötü niyetli kişiler tarafından şifresinin kırılıp kullanılabileceğini iddia etmesi karşısında, yerel mahkemenin konuyu araştırması gerekliliğine vurgu yapmıştır. Bu noktada, Yargıtay da CMK md. 134 tedbirine dolaylı olarak kovuşturma evresinde sanık hakkında uygulanabileceğine hükmetmiştir. Ayrıca, Yargıtay'ın pek çok kararında sanık ibaresine yer verilmiştir.

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kopyalama ve elkoyma tedbirine her suç tipi yönünden başvurulabilir. Ancak öğretide, mezkûr tedbire sadece belli suç tipleri için başvurulmasına ilişkin çeşitli görüşler bulunmaktadır. Esasen, kanun tasarısında iki yıl ve daha fazla cezayı gerektiren suçlar yönünden uygulanması öngörülse de daha sonda Adalet Komisyonu görüşmelerinde ilgili madde çıkarılmış ve suç tipi bakımından sınırlandırmaya yer verilmemiştir.²⁸⁹ Centel/Zafer'e göre²⁹⁰ tedbirin kişilik haklarına müdahale yoğunluğu göz önünde bulundurulduğunda, söz konusu koruma tedbirinin sadece belli suç tipleri yönünden uygulanmasına olanak sağlayacak uygun bir düzenleme yapılmalıdır. Bizim de katıldığımız başka bir görüşe²⁹¹ göre, bazı suç tipleri bakımından delillerin sadece

²⁸⁸ Yargıtay 8. CD. 14.05.2014 tarihli E.2014/3415, K.2014/12298 sayılı kararı “Osmaniye Valiliği Bilgi İşlem Şubesi servis sağlayıcılarının İsimtescil İnternet T.. A.Ş olduğu ve yapılan araştırmada söz konusu şirketin www.o....gov.tr web sitesine 31.03.2012 günü saat 19:38'de siber saldırı düzenleyen ve www.o...gov.tr web sitesine erişim yapan bilgisayarların IP numaralarının tespiti istenildiği ve İ. İ. T.. A.Ş'nin cevabı yazısında 31.03.2012 günü saat 19:38'den 19:39'a kadar ... numarası ile 31.03.2012 günü saat 19:38:02'de M.. D.. isimli şahsa ait sabit telefonla bağlantı sağlandığından bahisle açılan davada; yapılan soruşturma ve kovuşturma yetersiz olup olaya ilişkin deliller toplanmadan mahkumiyet hükmü kurulmuştur. Sanığın suçlamayı kabul etmeyerek kullandığı modemın şifreli olduğunu, kötü niyetli kişiler tarafından şifresinin kırılıp kullanılabileceğini savunması karşısında, sanığın internet hattına izinsiz giriş yapan olup olmadığının sanığın internet hattının bağlı bulunduğu internet sağlayıcısından sorulması, dosya içinde suça konu valiliğe ait siteye giriş yapan IP numaralarının ilgili birim tarafından bildirildiği ancak sitenin erişilmez hale getirilip getirilmediği, veri değiştirme, yoketme veya yeni veri yerleştirme yapıp yapılmadığına ilişkin bir tespiti rastlanmadığı anlaşılmakla, erişimin engellediği iddia olunan tarih/tarihler ve takip eden günlerde siteye erişimin ne zaman engellendiği sanık veya servis sağlayıcı tarafından bildirilen diğer IP numaralarından hangisi ile girişin yapıldığı araştırılmalı, siteye yapıldığı iddia olunan siber saldırının ne şekilde gerçekleştiği, niteliği, sitenin geçici veya daimi olarak erişilmez kılınıp kılınmadığı yahut mevcut verilerin yok edilip edilmediği veya varsa yerleştirilen resim, yazı v.s.nin neler olduğunun tespit edilip örnekleri de alınmak suretiyle dosya içine konulmalı, sanığın bilgisayarına el konulup hard disk incelenerek suça konu siteye ait bilgisayarlar arasında bağlantı ve veri akışı olup olmadığı saptanmalıdır.

Bu itibarla yukarıda açıklanan eksiklikler yerine getirilerek sonucuna göre tüm deliller birlikte değerlendirilip sanığın hukuki durumunun takdir ve tayini gerekirken eksik araştırmaya dayanarak yazılı şekilde hüküm kurulması”, “<https://www.hukukturk.com>”, (12.02.2022)

²⁸⁹ Şen ve Eryıldız, s. 208; Değirmenci, Sayısal, s.337.

²⁹⁰ Centel ve Zafer, s. 461.

²⁹¹ Değirmenci, Sayısal, s. 338.

bilişim sistemlerinde yer alması nedeniyle suç kataloğu düzenlenmesi durumunda bu suçların aydınlatılmasının olanaklı olmaması sebebiyle mevcut düzenleme yerindedir.

Yasa koyucu, CMK md. 134'e başvurulabilmesi için suç soruşturmasının varlığını aramıştır. Buna; 657 sayılı Devlet Memurları Kanunu'na göre yürütülen disiplin soruşturmaları, 5326 sayılı Kabahatler Kanunu kapsamında fiiller bakımından, 6413 sayılı Türk Silahlı Kuvvetleri Disiplin Kanunu kapsamındaki disiplin soruşturmalar, iç denetleme gibi idari işlemler kapsamında yürütülen faaliyetlerde söz konusu tedbire başvurulamaz²⁹².

Kanun yolları tüketilip hüküm kesinleştikten sonra somut olayda koşulları bulunması halinde olağanüstü kanun yollarından yargılamanın yenilenmesi söz konusu olabilir. CMK md. 320/2 "*Delillerin mahkemece veya naip hâkim tarafından veya istinabe suretiyle toplanması sırasında, soruşturmaya ilişkin hükümler uygulanır.*" şeklinde düzenlenmiştir. Bu noktada kanun koyucu adeta ceza muhakemenin yeniden yapılmasını öngörmüş ve delil toplanmasına ilişkin soruşturmaya ilişkin hükümlerin uygulanacağına hükmetmiştir. CMK md. 134 şüpheli hakkında soruşturma evresinde başvurulabilen bir koruma tedbiri olması nedeniyle yargılama yenilenmesi durumunda da CMK md. 134 hükümleri uygulanabilecektir.

2.1.1.2. Somut Delillere Dayanan Kuvvetli Şüphe Bulunması

Maddenin ilk halinde, tedbire başvurma şartları bakımından şüphe yönünden herhangi bir düzenleme bulunmamaktaydı. 6526 sayılı yasa²⁹³ ile madde metnine, "*somut delillere dayalı kuvvetli şüphe bulunma*" şartı eklenmiştir. Bu düzenleme ile kanun koyucu CMK md. 134'ün uygulanmasını daha da sıkı şartlara bağlayarak zorlaştırmıştır²⁹⁴. Buna göre, CMK md. 134'e dayanarak koruma tedbirine karar verilebilmesi için, kuvvetli şüphenin somut delile dayanması gerekmektedir.

6526 sayılı yasa öncesi, madde metninde açık bir şüphe derecesi bulunmadığından, CMK md. 134'ün uygulanması için aranması gereken şüphe

²⁹² İhsan Baştürk, "Bilgisayar Sistemleri ile Verilerinde Arama, kopyalama ve Elkoyma", **Fasikül Hukuk Dergisi**, Cilt: 2, Sayı: 9, 2010, s. 50; Değirmenci, Sayısal, ss. 333, 337.

²⁹³ 21 Şubat 2014 tarih ve 6526 sayılı Kanun; 6 Mart 2014 tarih ve 28933 Mükerrer sayılı Resmî Gazete'de yayımlanmıştır.

²⁹⁴ Özen ve Özocak, s. 63.

hususunda tartışma bulunmaktaydı. Bir görüş²⁹⁵, CMK md. 134 ile düzenlenen tedbirin arama ve elkoymanın genel hükümlerine tabi olmasından yola çıkarak söz konusu tedbirin uygulanması açısından makul şüphe gerekliliğini savunmaktaydı. Diğer bir görüş ise, CMK'da kıyas yasağı bulunmamasından bahisle, CMK md.135'te yer alan kuvvetli şüphe sebeplerinin kıyasen CMK md. 134 açısından da uygulanması gerektiğini savunmaktaydı.²⁹⁶ 6526 sayılı yasa ile, aranması gereken şüphe derecesi somut delile dayanan kuvvetli şüphe olarak belirlenerek konuya ilişkin belirsizlik ortadan kaldırılmıştır.

Kuvvetli şüphe, şüpheli ya da sanığın iddia edilen suçu işlediği hususunda somut vakıalarla desteklenmiş, dayanağı olan delillere göre mahkûmiyet kararı verilmesi kuvvetle muhtemel olduğu şüphe biçimidir²⁹⁷. Kanun koyucu, CMK md. 116'da yer alan genel arama tedbiri hakkında makul şüphe belirlerken, CMK md. 170 doğrultusunda kamu davası açılması için yeterli şüphenin varlığını aramıştır. Bu noktada CMK md. 134 ile düzenlenen bilişim sistemlerinde arama, kopyalama ve elkoyma koruma tedbirinin gerçekleştirilmesi için ise tüm bu şüphe derecelerinin üstünde olan somut delillere dayalı kuvvetli şüphenin varlığını aramıştır.

Öğretide, esasen kuvvetli şüphenin zaten somut delillere dayanması gerektiği ancak yasa koyucunun bu ibareyi de birlikte kullanarak bu hususu garanti altına almak istediği değerlendirilmektedir²⁹⁸.

Kanunda ya da öğretide, somut delil ve soyut delil ayrımı ya da somut delilin karşısında bu kavrama zıt anlam içeren başka bir delil ayrımı yapılmamıştır. Anglosakson hukuk sisteminde, somut delil-ikrar delili ayrımı yapılmış olsa da bizim de dahil olduğumuz Kıta Avrupası hukuk sisteminde böyle bir ayrım bulunmamaktadır. Somut delilden kasıt ulaşılabilir gerçekçi ve akılcı delillerin olması gerekliliğidir²⁹⁹.

Kuvvetli şüphenin, söz konusu koruma tedbirine ilişkin iki farklı yönü bulunmaktadır. Bunlardan birincisi soruşturmaya konu suçun şüpheli tarafından işlendiği yönünde kuvvetli şüphe bulunmasıdır. Diğerisi ise, arama yapılacak bilişim

²⁹⁵ Ünal, s. 100, 101; Özbek – Kanbur – Doğan – Bacaksız – Tepe, s. 395.'den aktaran Değirmenci, Sayısal, s. 350.

²⁹⁶ Baştürk, s. 26; Özen – Baştürk, s. 147.'den aktaran; Değirmenci, Sayısal, s. 351.

²⁹⁷ Dülger, s. 600.

²⁹⁸ Öztürk ve diğerleri, Koruma Tebdirleri, s. 34.

²⁹⁹ Dülger, s. 583.

sistemi üzerinde delil elde edileceğine ilişkin bulunan kuvvetli şüphe dir. Kişinin suçu işlediğine yönelik kuvvetli şüphe bulunması ve fakat delillerin ilgili bilişim sisteminde bulunacağına dair aynı derecede şüphenin bulunmaması durumunda CMK md. 134'ün uygulanması akılcı bir yaklaşım olmayacaktır³⁰⁰. Bu anlamda, CMK md. 134'ün uygulanması için bulunması gereken somut delillere dayalı kuvvetli şüphe hem suçun işlendiğine yönelik olması hem de suça konu delilin ilgili bilişim sisteminde bulunacağına yönelik olması gerekmektedir.

2.1.1.3. Başka Bir Şekilde Delil Elde Etme Olanının Bulunmaması

İkincilik ilkesi esasen oranlılık, ölçülülük ilkesinin bir alt dalıdır. Bu ilkeye göre, maddi gerçeği ortaya çıkarabilecek birden fazla delil varsa bu noktada öncelik sonralık ilişkisinin belirlenmesi gerekir. Öncelik belirlemede temel kriter, temel hak ve özgürlüklere müdahale yoğunluğu gözetilerek, en az müdahalede bulunulan tedbire öncelik verilmesi gerekir³⁰¹.

Başka suretle delil elde edilmesi imkanının bulunmaması hâli, Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik'te tanımlanmıştır. Söz konusu tedbire başvurabilmek için bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama tedbirinin *son çare* olması gerekir. Buna göre; söz konusu koşul, *“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 olmasını”* ifade eder.

Somut gerçeğe ulaşmak için öncelikle Kanun'da yer alan daha hafif tedbirlerin tümü uygulanmış ve sonuç alınamamış olması³⁰² ya da uygulansa dahi netice elde edilemeyeceğine ilişkin gerekçelendirilebilir ve makul bir beklenti olması gerekir³⁰³. Yine, kararların gerekçeli olması gerekliliğinin bir sonucu olarak; hâkim koruma

³⁰⁰ Değirmenci, Sayısal, s. 353.

³⁰¹ Değirmenci, Sayısal, s. 342.

³⁰² Özen ve Özocak, s. 62.

³⁰³ Şen ve Eryıldız, s. 191.

tedbiri kararını “*başka suretle delil elde etme imkanının bulunmadığına*” ilişkin gerekçelendirmelidir³⁰⁴. Ancak, uygulamada çoğu kararda kanun maddesi olduğu gibi tekrar edilmekte ve gerekçeli bir karar yazılmamaktadır³⁰⁵.

Başka bir şekilde delil elde etme olanağının olmaması durumunun, somut olaya nasıl uyarlanacağı yorumu önem kazanmaktadır. Söz konusu koşulun, dar yorumlanması halinde, soruşturma esnasında suça ilişkin delilleri elde etmek için mutlaka önce diğer koruma tedbirlerine başvurulacak; delil elde edilmesinin olanaksız olduğu anlaşıldığı vakit CMK md. 134’e başvurulacaktır. Ancak, söz konusu koşulun geniş yorumlanması durumunda ise, diğer tedbirlerin uygulanmasına gerek kalmaksızın, somut olayda CMK md.134 dışındaki tedbirlere başvurma delil elde edilmesine olanaksız olduğu açıkça anlaşılıyorsa, doğrudan bu tedbire başvurulabilecektir³⁰⁶. Örneğin, internette kumar oynatılma suçuna³⁰⁷ ilişkin başka tedbirlere başvurmak çoğunlukla anlamsızdır. Örneğimizde, dar yorumun uygulanması durumunda, Cumhuriyet savcısının ne olursa olsun öncelikle diğer tedbirlere başvurusu ve bu tedbirlerle delil elde edilememesi durumunda bilişim sistemlerinde arama tedbirine başvurulması beklenir. Geniş yorumda ise, Cumhuriyet savcısının, diğer tedbirlere başvurusunun, muhakeme açısından tehlikeli olması, delil elde etme olanağının neden bulunmadığının gerekçeleriyle birlikte makul sebepleri ortaya koyması durumunda doğrudan CMK md. 134 tedbirine başvurulmasını talep edebilecektir.

Öğretide CMK md. 134’te yer alan koruma tedbirine ilişkin; başka bir şekilde delil elde etme olanağının bulunmaması şartının gerekliliği tartışılmıştır. Bir görüşe göre³⁰⁸ , söz konusu tedbirin son çare olması gerekliliği kuralı yerinde olmakla beraber; bilişim suçlarına ilişkin soruşturmalarda da aynı kuralın uygulanmasının soruna neden olabileceğinden ayrık düzenlemeye yer verilmesi gerekir. Başka bir görüşe göre³⁰⁹; böylesine temel hak ve özgürlüklere doğrudan müdahale eden koruma tedbirleri açısından, söz konusu kısıtlamalara yer verilmesi isabetli olup, bu kısıtlama

³⁰⁴ Yenisey ve Nuhoğlu, s. 436.

³⁰⁵ Dülger, s. 584.

³⁰⁶ Değirmenci, Sayısal, s. 343.

³⁰⁷ TCK md. 228/3 “*Suçun bilişim sistemlerinin kullanılması suretiyle işlenmesi halinde üç yıldan beş yıla kadar hapis ve bin günden onbin güne kadar adli para cezasına hükmolunur*”

³⁰⁸ Yusuf Başlar, “Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri”, **Uyuşmazlık Mahkemesi Dergisi**, Cilt: 0, Sayı: 3, 2013, (Usul), s. 90.

³⁰⁹ Şen ve Eryıldız, s. 192.

ölçütünün ayak bağı olarak görülmeden uygulanmalıdır. Bir diğer görüşe göre³¹⁰ ise, bilişim suçlarına ilişkin genellikle başka şekilde delil elde etmek mümkün olmamakla beraber, yapılması gereken ilk iş sistemin bütünlüğü bozulmadan içindeki verilerin ve bağlantıların tespit edilmesidir. Bilişim suçlarında, başka suretle delil etme çabası sürerken bilişim sistemlerinden veri toplamak için çok geç kalınmış olunabilecektir.

Kanaatimizce, bilişim suçları ya da başkaca özgü suçlara ilişkin *son çare* kuralına istisna getirecek özel düzenlemeye ihtiyaç yoktur. Nitekim, sadece bilişim sisteminin kullanıldığı başka suretle delil elde edilemeyeceği açık olan söz konusu suçlarda, Kanun Koyucu bu tedbire doğrudan başvurulmasını engellemiştir. Hâkimin konuya ilişkin uygun gerekçe ile doğrudan söz konusu tedbire başvurulmasında yasal engel yoktur. Burada önemli olan husus; hâkimin objektif olarak başka suretle delil elde edilemeyeceğini takdir etmesi ve gerekçelendirmesidir. Öte yandan, söz konusu şarta istisna getirilmesi halinde, temel hak ve özgürlüklere müdahale eden bu koruma tedbirine istisna hükümlerinde yer verilen her suç tipi için doğrudan başvurulması sonucu doğacaktır. Bu durumda da bu özel düzenlemenin pek bir anlamı kalmayacaktır.

2.1.1.4. Hâkim Kararının Bulunması

Bir suç dolayısıyla yapılan soruşturma esnasında, bilgisayarlarda, bilgisayar programları ve kütüklerinde arama, kopyalama ve elkoyma tedbirine başvurulabilmek için diğer şartların da oluşması halinde, yetkili hâkim kararı bulunması gerekir. Kanun koyucu, gecikmesinde sakınca bulunan haller ile sınırlı kalmak kaydıyla Cumhuriyet savcısı tarafından da bu tedbire başvurulmasının önünü açmıştır. Ancak, Cumhuriyet savcısının bu tedbire karar vermesi halinde savcılık kararı yirmi dört saat içerisinde hâkim onayına sunulur. Sürenin dolması veya hâkim tarafından aksine karar verilmesi halinde çıkarılan kopyalar ve çözümü yapılan metinler derhâl imha edilir. Kanun koyucu, genel arama tedbirinde olduğu gibi CMK md. 134 kapsamında kolluk amirine arama kararı verme yetkisi vermemiştir.

³¹⁰ Dülger, s. 585.

Kanunda yer alan hâkim kararından kasıt, soruşturmanın yürütüldüğü yerdeki sulh ceza hâkimidir³¹¹. 6545 sayılı Kanun ile, 5235 sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanunda düzenleme yapılmıştır. Bu düzenleme ile, sulh ceza mahkemeleri kapatılarak sulh ceza hakimlikleri kurulmuş, yetki yönünden yargı çevresi düzenlenmiştir. Buna göre, sulh ceza hâkimliğinin yargı çevresi, bulundukları il merkezi ve ilçeler ile bunlara adli yönden bağlanan ilçelerin idari sınırları olarak belirlenmiştir. Sulh ceza hakimliği, bağlı bulunduğu yargı çevresinde dışında, CMK md. 134 kapsamında bilgisayarlarda bilgisayar programlarında ve kütüklerinde arama kopyalama ve elkoyma tedbirine müspet ya da menfi karar veremez.

Nitekim, Yargıtay önüne gelen bir dosyada, bir üniversitede iki öğretim üyesinin haklarında 2547 sayılı Yükseköğretim Kanunu md. 53(c)/1 uyarınca yapılan ilk soruşturma sırasında soruşturmacı tarafından Hatay Cumhuriyet Başsavcılığından söz konusu öğretim üyelerinin konutlarında, çalıştıkları bölüm odalarında, evlerinde üniversiteye ait tüm belge ve hard disklerin aranması ve el konulması konusunda karar aldırılmasının istenilmesi üzerine, Hatay Cumhuriyet Başsavcılığınca yapılan arama ve el koyma talebinin adı geçenlere isnat edilen fiillerin henüz somutlaşmadığından reddine dair Hatay 2. Sulh Ceza Mahkemesince verilen karara, soruşturmacı tarafından yapılan itiraz üzerine, Hatay Sulh Ceza Mahkemesinin yetki alanı içerisinde bulunmayan Kırıkhan İlçesinde bulunan yer yönünden de arama kararı verilemeyeceğinin gözetilmeden itirazın kabulüne karar verilmesini hukuka aykırı bulmuştur³¹².

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama yapılabilmesi için, mutlaka CMK md.134 hükümleri çerçevesinde karar olması gerekir. CMK md. 116 doğrultusunda verilen arama kararının geniş yorumlanarak bilgisayarlara da uygulanması hukuka aykırıdır. Nitekim, Yargıtay da aynı görüşü benimsemiş, önüne gelen bir dosyada³¹³; CMK md. 119 uyarınca, sanığın işyerinde

³¹¹ Aldemir, s. 181.

³¹² Yargıtay 7. CD, 27.02.2014 tarih, E.2014/2918, K.2014/3889 sayılı kararı; “Hukuk Türk”, <https://www.hukukturk.com/>, (20.02.2022)

³¹³ Yargıtay 19.CD 02.02.2016 tarih, E.2015/11396, K.2016/1087, sayılı kararı; “Bu açıklamalar ışığında; davaya konu olaya gelince, ... Cumhuriyet Başsavcılığı tarafından CMK'nın 119. maddesi uyarınca sanığın işyerinde arama yapılmasına yönelik verilen 26.4.2012 tarihli karar uyarınca yapılan aramada ele geçen hddisklerde kolluk görevlilerince yapılan inceleme sonucu 471 adet film bulunduğundan tespit edildiği ve CMK'nın 134 . maddesi uyarınca bilgisayar ve bilgisayar kütükleri

yapılan bir aramada, bilgisayar ve bilgisayar kütüklerinin de incelenmesi ve buradan çıkan deliller doğrultusunda mahkumiyetin kurulması üzerine, CMK md. 134 uyarınca verilen bir arama kararı olmamasından bahisle yerel mahkeme kararını hukuka aykırı bulmuştur. Yine, Yargıtay başka bir kararında³¹⁴, Hendek Sulh Ceza Mahkemesinin verdiği arama kararını CMK md. 134 kapsamında olmadığından bahisle, usule aykırı arama kararı sonucu elde edilen delile dayanarak verilen mahkûmiyet kararını bozmuştur. Yargıtay'ın bahse konu kararlarındaki değerlendirmelerine katılıyoruz. CMK md. 134'ün düzenlenme amacı temel hak ve özgürlüklere müdahale yoğunluğunun yüksek olduğu bilişim sistemlerinde arama ve elkoymanın sıkı şartlarla uygulanmasını sağlamaktır. CMK md. 116 ve devamında yer alan genel arama ve elkoyma tedbirleri doğrultusunda verilen karar sonucu bilişim sistemlerinde aram ve elkoyma tedbirinin uygulanması çalışmamıza konu koruma tedbirinin varlık amacına ters düşmektedir.

Yine, söz konusu tedbire başvurmak için Cumhuriyet savcısının istemi şarttır. Hâkim, istem olmaksızın doğrudan tedbire karar veremez. Ancak; CMK md. 163'e göre, suçüstü hâli ile gecikmesinde sakınca bulunan hâllerde, Cumhuriyet savcısına erişilememesi veya olay genişliği itibarıyla Cumhuriyet savcısının iş gücünü aşması durumu gibi istisnai hallerde Sulh ceza hâkimi de soruşturma işlerini yapmaya yetkili kılınmıştır. Burada sulh ceza hâkimi "savcılık" sıfatıyla görev yaptığından, bu durumda tedbir istemini sulh ceza hakiminin yerine getirmesi gerekir. Ancak tedbir kararını aynı yargı çevresindeki diğer sulh ceza hakiminin vermesi gerekir³¹⁵.

üzerinde arama yapılmasına dair hakim tarafından verilmiş bir karar bulunmadığı cihetle, arama sonucu 2 adet harddiskte bulunan 471 adet filmin hukuka aykırı şekilde elde edilmiş delil niteliğinde olması sebebiyle hükme esas alınamayacağı ve atılı suçlamayı kabul etmeyen sanık hakkında hukuka aykırı şekilde elde edilmiş bu delil dışında mahkumiyetine yeterli başkaca bir delil de bulunmadığı gözetilmeden, beraati yerine yazılı şekilde mahkumiyetine karar verilmesi ..."

<https://www.hukukturk.com/>, (20.02.2022).

³¹⁴ Yargıtay 7. CD. 10.12.2014 tarihli, E.2013/6138, K.2014/22341 sayılı kararı; "Sanığın yetkilisi olduğu Bilgisayar Güvenlik Sistemleri Ticaret Sanayi Limited Şirketi isimli işyerinde Hendek Sulh Ceza Mahkemesinin 2008/524 değişik iş sayılı arama kararı ile yapılan aramada ele geçirilen MSI marka bilgisayarda katılana ait Windows XP PRO ve OFFİCE 2003 PRO lisansız programların bulunması şeklinde gerçekleşen olayda, aramaya dayanak olan Hendek Sulh Ceza Mahkemesinin 2008/524 değişik iş sayılı arama kararında CMK'nın 134.maddesindeki bilgisayarda, bilgisayar kayıtlarında ve kütüklerinde arama kopyalama ve elkoyma yetkilerinin bulunmadığı, bu nedenle arama kararı usule aykırı olup anılan arama kararı gereğince elde edilen delile dayanılarak hüküm kurulamayacağı gözetilmeden sanığın beraati yerine mahkumiyetine karar verilmesi yasaya aykırı olup..." <https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/>, (20.02.2022).

³¹⁵ Şen ve Eryıldız, s. 204; Özen ve Özocak, s. 63.

Arama kararı veya emrinde bulunması gerekenler hususlar, CMK md. 119/2’de düzenlenmiştir. Buna göre ilgili karar veya emirde; aramanın nedenini oluşturan fiil, aranılacak kişi, aramanın yapılacağı konut veya diğer yerin adresi ya da eşya, karar veya emrin geçerli olacağı zaman süresi bulunması gerekir. CMK md. 134’te genel arama kararına ilave olarak daha sıkı şartlarda düzenlenmiştir. Bu sebeple, CMK md.119/2’de yer alan hususlara ilave olarak, CMK md.134’ün uygulaması bakımından, kuvvetli şüphe sebeplerini oluşturan etmenler ile başka suretle delil elde etmenin neden imkânsız olduğunu gösteren hususlara da yer verilmesi gerekir³¹⁶. Yine arama konusu bilişim sisteminin şüpheliye mülkiyetinde olmaması durumunda, şüphelinin kullandığına dair oluşan kanaatin de gerekçelendirilmesi ve kararda yer alması uygun olacaktır³¹⁷. Nitekim kanun koyucu şüphelinin kullandığı bilgisayara ilişkin tedbire karar verilebileceğini öngörmüştür. Aksi halde, söz konusu tedbir hukuka aykırı olacaktır.

Yargıtay önüne gelen bir dosyada³¹⁸, şüphe üzerine durdurulan sanığın rızasıyla teslim ettiği iddia edilen dijital materyallere ilişkin CMK md.134 uyarınca yazılı hâkimlik kararı olmadığı ve dijital materyallerin olay mahallinde imaj alınmadan, sanık ya da müdafisine bir kopya verilmeden el konulmasının CMK md. 134’e göre hukuka uygun yöntemlerle delil elde edilmediğinden bahisle kurulan mahkûmiyet hükmünü bozmuştur. Kanaatimizce, Yargıtay kararı yerindedir. Nitekim, temel hak ve özgürlüklere müdahale yoğunluğu yüksek olan söz konusu koruma tedbirinde hakimlik kararı yasal bir zorunluluktur. Ayrıca, olay mahallinde dijital materyalden yedek alınarak orijinalinin derhal şüpheliye verilmesi gerekir. Kanun koyucu madde ile bilişim sisteminden ziyade dijital veriye elkoymayı hedeflemiştir.

Konutta ve işyerinde CMK md. 116 vd. hükümlerince arama ve elkoyma uygulanırken, CMK md.134 kapsamında hâkim kararı olmaksızın bilişim sistemlerine yönelik arama ve elkoyma tedbiri uygulanamaz. Nitekim, CMK md. 116 vd. ile başlayan arama tedbirinde bilgisayarlara yönelik uygulama sonrasında CMK md. 134 ile arama kararı alınması hukuka aykırıdır. Olması gereken, önce CMK md. 134’e göre

³¹⁶ Değirmenci, Sayısal, s. 354; Ünal, s. 105.

³¹⁷ Değirmenci, Sayısal, s. 354.

³¹⁸ Yargıtay 16.CD. 10.10.2019 tarih ve E.2019/2637 K.2019/5904 sayılı kararı, Yargıtay 18.CD. 07.03.2016 tarih ve E.2015/24016 K.2016/4194 sayılı kararı.

hakimlik kararı bulunması ve akabinde tedbirin uygulanmasıdır. Yargıtay önüne gelen bir dosyada³¹⁹

İncelemeye konu olayda; İstanbul Anadolu 35. Sulh Ceza Mahkemesi'nin 17/04/2013 tarih ve 2013/510 değişik iş sayılı kararı ile sanığın evinde CMK 116-119 maddeleri uyarınca arama yapılmasına dair karar verildiği, bu karar kapsamında yapılan aramada sanığa ait iki adet bilgisayara el konulduğu, yine İstanbul Anadolu 36. Sulh Ceza Mahkemesi'nin 18/04/2013 tarih ve 2013/195 değişik iş sayılı kararı ile sanığın ikametinden ele geçen bilgisayar üzerinde inceleme yapılması ve kopya çıkarılmasına hükmedildiği anlaşılmakla, arama sonrası bilgisayarların yedeklemesinin yapılıp şüpheliye verildiğine dair bir ibareye tutanakta yer verilmediği gibi, 18/04/2013 tarih ve 2013/195 değişik iş sayılı kararın ise bilgisayarlara el konulmasından sonra alındığı, bu suretle CMK'nın 134. maddesi hükümlerine riayet edilmeyerek bilgisayar kütüklerinde bilirkişi incelemesi yaptırıldığı, bilgisayar kasasında hukuka aykırı yapılan bu arama ve el koyma sonucu elde edilen delillerin de hukuka uygun elde edilmiş delil niteliğinde olmadığı, delil değerlendirme yasağı kapsamında kaldığı kabul edilip...

gerekçesiyle hüküm kurmuştur. Buna göre, Yargıtay bilgisayara elkoyma işlemi gerçekleştikten sonra CMK md. 134'e göre karar alınmasını hukuka aykırı bulmuştur. CMK'da yer alan tedbirler hakkında, söz konusu tedbir uygulanmadan önce karar verilmesi gerekir. Zira, tedbir uygulandıktan sonra yetkili mercilerce de olsa tedbire karar verilmesi, ilgili koruma tedbirini hukuka uygun hale getirmez. Somut olayda, CMK md.116-119 doğrultusunda arama yapılmasına karar verilmesi, bilişim sistemlerini arama kapsamı dışında tutması gerekir. Ancak, kolluk tarafından bilgisayarlara el konulması hukuka aykırı olduğu gibi sonradan CMK md. 134 kapsamında karar alınması da mezkûr eylemin hukuka aykırılık sorununu ortadan kaldırmaz.

2.1.2. Elkoyma Yönünden

CMK md.134 ile bilişim sistemlerine yönelik arama ve elkoyma aynı maddede yer almasına karşın, söz konusu tedbir esasen arama tedbiridir. Elkoyma tedbiri

³¹⁹ Yargıtay 18.CD. 07.03.2016 tarih ve E.2016/8680 K.2018/5914 sayılı kararı.

bilgisayar programının şifrenmesi ve şifrelerinin çözülememesi, kopyalama tedbirinin çok uzun sürmesi gibi çok istisnai hallerde yerine getirilir. Bu durumda dahi, bilgi sistemlerinden gerekli kopyaların alınmasını müteakip gecikmeksizin iade edilmesi gerekir.

Madde kural olarak arama tedbiri olması ve elkoymanın istisnai olarak uygulanması gerekirken uygulamada elkoymanın da kural olarak uygulandığı görülmektedir. Bu durum öğretilerde ve yargı kararlarında tartışılmıştır.

Ünver ve Hakeri'ye göre³²⁰, söz konusu tedbirin elkoyma tedbiri olarak ele alınması, uygulamada hataya sebep olmakta, maddede yer alan istisnai koşullara titizlikle uymadan ve detaylı inceleme yapmaksızın doğrudan elkoyma işlemi yapılabilmektedir.

Dülger'e göre³²¹, kolluk kuvvetleri yaptıkları aramanın tamamına yakınında CMK md.134/2'yi doğrudan işletmekte, yeterli personel olmadığı, sistemin başında kopyalama işlemi gerçekleştirmeleri durumunda işlerini yetiştiremeyecekleri gibi mazeretlerle, koruma tedbirine konu bilişim sisteminde şifre bulunduğuna ilişkin tutanak tutarak yasaya uygun davrandıklarını düşünerek esasen yasanın arkasından dolanmaktadırlar. Ancak tutulan tutanaklarda, sistemde ne tür bir şifrenin bulunduğu, bu şifrenin neden bertaraf edilemediği bilişim uzmanlarınca neden sisteme girilemediği gibi hususlarda açık gerekçe yer almamaktadır. Bu doğrultuda elde edilen delil “*hukuka aykırı delil*” niteliğindedir. Hukuka aykırı deliller Anayasa md. 38 ve CMK md. 217/2 uyarınca hükme esas alınmamalıdır.

Bahse konu şifre çoğu zaman bilişim sisteminin başlatılmasında kullanılan basit bir şifre ya da programa erişim kısıtlaması sağlanması açısından şüpheli tarafından konulan bir şifre olmaktadır. Bu şifre şüpheliye sorulması halinde, şüpheli tarafından kolluk görevlileri ile paylaşılabilir ve sorun rahatlıkla ortadan kaldırılabilecektir. Nihayetinde, şüpheli tarafından şifrenin paylaşılması ve adli kolluğa kolaylık sağlanmaması durumunda elkoyma işlemine haklı bir gerekçe oluşturulabilecektir.

Şahin ise³²², adli kolluğun kanunun arkasından dolanarak uygun gerekçe oluşturmadan tutanak ile elkoyma işlemi neticesinde elde edilen delilin tamamıyla

³²⁰ Ünver ve Hakeri, s. 937.

³²¹ Dülger, s. 585.

³²² Şahin, s. 283.

hukuka aykırı bulunarak hükme esas alınmamasını isabetli bulmamaktadır. Yazar, bu şekilde elde edilen delillerin güvenilirliğinin ayrı bir sorun olarak değerlendirmekle beraber bu şekilde elde edilen delilin her durumda değerlendirme yasağı kapsamına alınmasını uygun bulmamaktadır.

Anayasa Mahkemesine yapılan bireysel başvuru neticesinde verilen bir kararın karşı oy gerekçesinde³²³; elkoyma işleminin gerçekleşmesi için gerekli koşullar ortaya konmuş ve bu koşullara uyulmaksızın, yedekleme işlemi yapılmadan ve çıkarılan yedeklerden birisinin şüpheli veya vekiline verilmeksizin yapılan elkoyma işleminin ve elkoyma neticesinde elde edilen delillere dayanarak verilen tutuklama kararının hukuka aykırı olmasından bahisle somut olayda hak ihlali olduğu sonucuna varılmıştır.

Kanaatimizce, hukuka aykırı uygulamanın herkes tarafından yapılması, ilgili eylemi hukuka uygun hale getirmez.

Madde düzenlemesinde yer alan elkoyma tedbirinde amaç bilişim sistemlerinde yer alan verilere elkoymadır. Bilgisayara fiziken elkoyma CMK md.134 uyarınca değil, CMK md.127’de yer alan genel elkoyma hükümlerine göre gerçekleştirilecektir³²⁴.

2.1.2.1. Arama, Kopyalama Tedbirine Karar Verilmiş Olması

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbiri niteliği itibarıyla arama tedbiridir. Arama bilişim sistemlerinde yer alan veriler üzerinde gerçekleştirilecektir. Arama sonrasında ortaya çıkan delil niteliğindeki verilere Kanunda yer alan istisnai şartlar mevcutsa elkoyma gerçekleştirilebilecektir. Bu anlamda; koruma tedbirinde arama kural, el koyma istisnai olarak düzenlenmiştir.

Bilişim sistemlerinde arama yapılabilmesi için öncelikle CMK md. 134 kapsamında arama kararı verilmesi gerekir. CMK md. 116’ya dayanarak bilişim sistemlerine ilişkin arama yapılması hukuka aykırıdır. Nitekim, üst araması esnasında

³²³ Anayasa Mahkemesi 2014/3129 numaralı bireysel başvurusuna ilişkin 27.10.2016 tarihli kararı, <https://kararlarbilgibankasi.anayasa.gov.tr/BB/2014/3129?BasvuruNoYil=2014&BasvuruNoSayi=3129>, (20.02.2022)

³²⁴ Aldemir, s. 186; Şen ve Eryıldız, s. 204.

dahi ortaya çıkan cep telefonunun bilişim özelliğine dair arama yapılması hukuka aykırı delil mahiyetinde olup yasak delil niteliğindedir³²⁵.

2.1.2.2. Şifrenin Çözülememesinden Dolayı Bilgisayara Girilememesi veya Gizlenmiş Bilgilere Ulaşılamamış Olması

CMK md.134 kapsamında yer alan bilişim sistemlerine elkoyma istisnai olarak düzenlenmiştir. Tedbirin bu şekilde düzenlenmesindeki amaç, bilgisayar ve kütüklerine mülkiyetini sonlandırmaksızın dijital verilere elkoymaktır³²⁶. Böylece, mülkiyet hakkını da ihlal etmeden koruma tedbiri gerçekleştirilecektir. Ancak, bazı istisnai durumlarda, arama yapıldığı esnada verilere ulaşmak zor ya da imkânsız olabilmektedir. Kanun koyucu, bilgisayara konulmuş herhangi bir şifrenin çözülememiş olmasını ya da verilerin gizlenmesi sebebiyle hedef veriye ulaşamama durumunu istisna olarak düzenlemiştir.

Bilgisayarların kodlanabilir ve karmaşık yapısından dolayı bazı durumlarda verilere erişmek kolay olmayabilir. Veriler bilgisayarda açık ya da kapalı kaynak kodlara sahip bir yazılım ile şifrelenmiş, silinmiş ya da bir şekilde gizlenmiş olabilir. Bu durumda, CMK 134 çerçevesinde verilmiş arama kararı icra edilirken o an için verilere ulaşarak veriler üzerinde arama yapmak mümkün olmayabilir. Bu durumda, şifrelerin çözülmesi gerekeceğinden daha detaylı inceleme yapmak adına bilgisayara, bilgisayar kütüğüne elkoymak gerekli olabilir.

Öğretide bir görüşe³²⁷ göre, bu düzenleme teknik olarak hatalıdır. Yazar, bilgisayarların yerinde incelenmesinin çoğu kez olanaksız olacağı gerekçesiyle şüphelinin mağdur olmayacağı şekilde tedbir alınarak bilgisayara elkonulması ve laboratuvar ortamında inceleme yapılması gerektiği kanaatindedir. Ancak, biz bu görüşe katılmıyoruz. Bilişim sistemlerinde yer alan veriler sisteme giriş yapılmaksızın yedeklenebilir. Bu anlamda verilerin o bilişim sistemi vasıtasıyla incelenme zorunluluğu bulunmamaktadır. Bilişim sistemlerinde şifre bulunması ve bu şifrenin kırılmaması durumunda dahi cihazın imajı alınabilmekte ve daha sonra üçüncü parti

³²⁵ Dülger, s. 589.

³²⁶ Öztürk ve diğerleri, Koruma Tebdirleri, s. 214.

³²⁷ Özen ve Özocak, s. 64.

uygulamalarla söz konusu şifre kırılıp inceleme yapılabilir³²⁸. Yine, bilişim sistemleri hakkında verilen her koruma tedbirinde doğrudan elkonup laboratuvar ortamına götürülmesi mülkiyet hakkını ölçüsüz şekilde ihlal edecektir. Zira, bilişim sistemlerinde yer alan verilerin incelenmesi için tüm bilişim sistemine elkoyma zorunluluğu bulunmamaktadır.

2.1.2.3. İşlemin Uzun Sürecek Olması

Bilişim sistemlerinde arama veya yedekleme yapılmasının uzun sürecek olması halinde; ilgili bilişim sistemine elkonulabilir. Söz konusu istisna maddenin ilk halinde bulunmamakta olup, 668 sayılı KHK'nın 3/j maddesi ile ilk defa düzenlenmiş ve 31.07.2018 tarihinde yürürlüğe giren 7145 sayılı Kanun ile yasal bir zemine kavuşmuştur.

İşlemin uzun sürecek olması koşulu oldukça sübjektif bir kriterdir. Kanun koyucu bu noktada, kime göre neye göre işlemin uzun süreceği hakkında objektif bir kriter belirlememiştir. Nihayetinde, her somut olaya göre işlem süresi değişiklik gösterecektir. Örneğin, 500 Gb boyutlu bir belleğin yedeklenmesi ile 12 TB boyutlu belleğin yedeklenme süresi eşit değildir. 500 Gb boyutlu bir bellek ortalama 1 saat içinde yedeklenirken 12 Tb boyutundaki bellek 24 saatte yedeklenmektedir³²⁹. Burada işlemin uzun sürme kriteri kopyalama, yedekleme işlemine konu cihazın boyutuna göre değerlendirilmesi gerekir.

Düşük boyutlu bir belleğin kopyalama süresinin ortalama on dakika olduğunu düşünelim. Bu durumda, her defasında sekizinci dakikada sistemin hata vermesi durumunda elkoyma işleminin gerçekleştirilip gerçekleştirilmeyeceği belli değildir. Nihayetinde, kopyalama işleminin uzun sürme koşulu gerçekleşmemiştir. Öte yandan, somut olayda çözülememiş şifre de bulunmadığı gibi, gizlenmiş verilere ulaşamama durumu da söz konusu değildir.

Yargıtay güncel tarihli bir kararında³³⁰, Ankara Cumhuriyet Başsavcılığı'nın verdiği

³²⁸ Uğraş, s. 130.

³²⁹ Değirmenci, 7145, s. 152.

³³⁰ Yargıtay CGK 22.09.2020 tarihli, E.2019/353 K.2020/367 sayılı kararı.

arama yapılacak kişi sayısının oldukça fazla olması, ülkenin içerisinde bulunduğu olağanüstü durum nedeniyle aramayı yapacak personel eksikliği, yine fazla arama yapılması nedeniyle alınacak dijital kopyaların yedekleneceği dijital veri deposu temininde aksaklık yaşanabileceği ve her kopya alınmasının oldukça uzun zaman alacağı sebebiyle, aramalarda elde edilecek bilgisayarlara, bilgisayar kütüklerine, cep telefonlarına, HD, DVD, CD, USB bellek, harici ve dahili hard disk vb. dijital tüm materyallerin mühürlü çuval, koli, delil poşeti vb. eşyalar içerisinde muhafaza altına alınması, delil torbası vb. eşyaların mühürlenirken birlikte imza altına alınması, mühürleme işleminin tutanak haline getirilmesi ve akabinde kopya çıkartılması için mühür açma işleminin şahıs veya avukatı nezaretinde tanzim edilecek tutanak haline getirilmesi ve kopya alınması akabinde gerekli teslim işleminin yapılması

şeklindeki talimatını CMK md.134/2 ye göre hukuka uygun bulmuştur³³¹.

Burada bir diğer önemli husus, elkoymaya konu olacak cihazın, suça ilişkin bilgileri içeren donanımdan (hard disk, usb bellek) ibaret olması gerekliliğidir. Aksi halde tüm bilişim sistemine elkonulması hem mülkiyet hakkını ölçsüz şekilde kısıtlayacak hem de suçun engellenmesi amacına hizmet etmeyecektir. Siber suç sözleşmesinde konuya ilişkin düzenleme bulunurken ulusal mevzuatımıza bu duruma özgü düzenleme bulunmamaktadır³³².

2.2. TEDBİRİN UYGULANMASI

CMK md.134, esasen bünyesinde üç farklı koruma tedbiri barındırmaktadır. Bunlar arama, kopyalama ve elkoymadır. Yasa koyucu, bilişim sistemleri üzerindeki incelemeyi kural olarak mülkiyet hakkını ihlal etmeksizin; cihazın kopyası üzerinden

³³¹ Kararın devamında Yargıtay'ın gerekçesi şu şekildedir; "27.07.2016 tarihinde yürürlüğe giren 668 sayılı KHK'nın 3/j maddesi ile; kopyalama ve yedekleme işleminin uzun sürecektir olması hâlinde bu araç ve gereçlere el koyulabileceğinin kabul edildiği, anılan düzenlemenin olağanüstü hâlin devamı süresince uygulandığı, sonrasında ise 31.07.2018 tarihinde yürürlüğe giren 7145 sayılı Kanun'un 16. maddesi ile CMK'nın 134. maddesinin 668 sayılı KHK'ya uygun olarak değiştirildiği hususları ile yapılan el koyma işlemine CMK 134/2. maddesinin izin vermesi, olağanüstü durumun varlığı dikkate alındığında kanuni düzenlemelerin 15.07.2016 tarihinde gerçekleştirilen darbe teşebbüsünden sonra değiştirilerek yedekleme işleminin uzun sürecektir olmasının el koyma işlemine sebep olarak gösterilmesi ile birlikte değerlendirildiğinde, CMK'nın 134/2. maddesine göre gerekli kopyaların alınması hâlinde el koyulan materyallerin iade edileceğinin belirtilmesi sebebiyle gerekli kopyaların alınamaması durumunda bu materyallerin de iade edilmesinin beklenemeyeceği," Yargıtay CGK 22.09.2020 tarihli, E.2019/353 K.2020/367 sayılı kararı.

³³² Yenisey ve Nuhoğlu, s. 441.

gerçekleştirilmesini öngörmüştür. Burada; verilerin hassas yapısı gözetilmiş, veri bütünlüğünün sağlanması amaçlanmıştır³³³. Bilişim sistemlerinde arama, kopyalama ve elkoyma işleminin gerçekleştirilmesi sürecinde adli bilişim uzmanının bulunması gerekmektedir³³⁴. Elektronik delillerin toplanmasında klasik delillerde olduğu gibi olay yeri ön plana çıkmakta ve olay yerine yapılan ilk müdahale elektronik delillerin sağlıklı toplanması açısından büyük önem kazanmaktadır³³⁵.

Yargıtay bir kararında³³⁶, CMK md. 134'ün ayrıkısı düzenlenmesi ve maddenin uygulama safhasının önemine değinmiştir. Yargıtay kararını gerekçelendirirken; CD, DVD, flash bellek, disket, harici ve dahili harddisk, bilgisayar özelliği içeren noktaları bakımından akıllı telefon ve benzerlerinden elde edilen ve tamamı "*dijital delil*" olarak adlandırılan delillerin; adil yargılanmanın sağlanabilmesi için, şüpheli veya sanıktan elde edilirken, kanun ile sınırları belirlenmiş ve teknik gereklilikler doğrultusunda toplanmasını ve yargılama makamlarına eksiksiz, bozulmamış halde sunulmasının gerektiğine değinmiştir. Bu doğrultuda sunulmayan dijital delillerin, kanunsuz delil olacağına ve hükme esas alınamayacağına karar vermiştir. Yargıtay'ın gerekçesine katılıyoruz. Nitekim dijital veri içeren tüm materyaller bilgisayar, bilgisayar kütüğü mahiyetindedir. Anılan dijital verilerin, yasa ile öngörülen teknik gerekliliklere uyulmadan alındığı takdirde, delillerin güvenliği tehlikeye girmektedir. Yine söz konusu kararla, CMK md. 134'ün uygulama safhasının önemini bir kez daha görüyoruz. Gerçekten de CMK md. 134 ün hukuka uygun olması için koruma tedbirine karar verilmesi safhasındaki usullerin yanında uygulama safhasındaki usuller de önem kazanmaktadır. Usulüne uygun toplanmayan dijital delillerin güvenilirliği tartışmaya açık olacağı gibi hükme esas alınmayacaktır.

³³³ Şen ve Eryıldız, s. 205.

³³⁴ Uğraş, s. 126.

³³⁵ Özen ve Özocak, s. 64.

³³⁶ Yargıtay 16. CD. 21.09.2017 tarih ve E.2015/2056 K.2017/5023 sayılı kararı.

2.2.1. Bilgisayarlarda, Bilgisayar Programları ve Kütüklerinde Arama ve Kopyalama

2.2.1.1. Genel Olarak

Bilişim sistemlerinde yapılacak aramanın konusu elektronik veridir. Elektronik verilerin toplanması sürecinde tıpkı klasik delillerdeki gibi, olay yeri önem kazanmaktadır. Delillerin sağlıklı toplanması, olay yerine ilk müdahalenin sağlıklı olması ile doğrudan ilişkilidir³³⁷. Adli bilişim sürecinin her aşaması titizlikle yürütülmeye muhtaçtır. Bilişim sistemlerine ilk müdahaleden muhakemenin sonuna kadar delil bütünlüğünün sağlanması gerekir³³⁸. Dijital delillerin mahkeme karşısında şüpheyi yer bırakmaksızın hükme esas alınabilmesi için ulusal mevzuata ve uluslararası standartlara uygun şekilde elde edilmiş olması gerekir³³⁹. Yine dijital delilin paketlenmesi, taşınması ve muhafazası için uygun ortam sağlanmalıdır. Dijital delile bu şekilde hassas yaklaşılmaması veride bozulmalara yol açacaktır. Örneğin; CD, DVD gibi medya ortamlarının aşırı basınç altında bırakılması, zımba teli basılması, aşırı sıcak ortama maruz bırakılması, uygunsuz yerlere etiket yapıştırılması, hassas şekilde taşınmaması kalıcı veri hasarlarına yol açabilecektir³⁴⁰.

Bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirin uygulanması; verilerin araştırılması, sorgulanması, elektronik veri depolama ortamında gerçekleştirilmektedir³⁴¹. Uluslararası hukukta da elektronik delil incelemesinde genel olarak 4 farklı yol izlenir. Bunlar³⁴²; bilişim sistemini arama ve ilgili veriyi kâğıda yazdırma, bilişim sistemini arama ve dijital yedeklemesini gerçekleştirme, bilişim sistemine uzaktan arama gerçekleştirerek elektronik kopyasını alma ve bilişim sistemini yerinde inceleyerek dijital kopyasını almaktır. Teknik olarak arama kararı uzaktan erişim ile gerçekleştirilebilse de CMK md. 134'ü incelediğimizde bilişim

³³⁷ Özen ve Özocak, s. 64.

³³⁸ Robyn Burrows, "Judicial Confusion And The Digital Drug Dog Sniff: Pragmatic Solutions Permitting Warrantless Hashing Of Known Illegal Files", **George Mason Law Review**, Cilt: 19, Sayı: 1, 2011, s. 259.

³³⁹ Mehmet Serkan Kılıç, "Elektronik Delillerin Hukuken Geçerliliği Açısından İlk Müdahalenin Önemine İlişkin Bir İnceleme", **Terazi Hukuk Dergisi**, Cilt: 10, Sayı: 102, 2015, s. 36.

³⁴⁰ Yusuf Başlar, "Elektronik Delilin Toplanması ve Muhafazası", **Hacettepe Hukuk Dergisi**, Cilt. 10, Sayı: 1, 2020, (Elektronik), s. 100.

³⁴¹ Duran, s. 225.

³⁴² Burrows, s. 259.

sistemlerinde yerinde arama, kâğıda yazdırma ve yedek alma prensiplerini benimsemektedir³⁴³.

Bilişim sistemlerinde arama işleminin kim tarafından gerçekleştirileceği Kanun'da açıkça düzenlenmese de CMK md. 63 doğrultusunda atanacak uzman kişiler tarafından diğer kişilerin huzurunda gerçekleştirileceğini söylemek mümkündür³⁴⁴. Bilişim sistemlerinde arama yapmak için olay yerine gitmeden önce ön hazırlık yapılması gerekir. Arama kararında yer alan bilgiler ışığında arama tekniği ve metodolojiyi önceden belirlemek gerekir³⁴⁵. Bilişim sistemlerine müdahalede bulunacak her türlü işlem tutanak altına alınmalıdır. Nitekim, bilişim sistemine yapılacak en küçük müdahale veri dosyalarında değişiklik meydana getirecektir. Bu şekilde şüphe halinde hem uygulanacak işlemler tekrar edilebilecek hem de hukuki güvenlik sağlanacaktır. Ayrıca olay yerinde, işin niteliğine göre dışarıdan müdahaleyi engelleyecek izolasyonun sağlanması önemlidir³⁴⁶.

2.2.1.2. İmaj Alma ve Kopya Üzerinden İnceleme

Yargılamaya konu olayın muhakeme esnasında aydınlatılması adına kullanılacak olan belge delili, orijinal olması gerekir. Nihayetinde belgenin sahte olup olmadığının tespiti ancak belgenin orijinali üzerinde yapılacak incelemeyle ortaya çıkarılabilir³⁴⁷. Basit bir kopya üzerinden delil incelemesinin yapılması olanaksızdır.

Yargıtay, içtihatlarında³⁴⁸ belge fotokopilerinin, aslı gibi olduğuna ilişkin onay bulunmadığı sürece hukuk düzeninde sonuç doğurmayacağına ilişkin hüküm kurmuştur. Ancak Yargıtay'ın bu yaklaşımı elektronik delillerde tamamen aynı şekilde uygulanması mümkün görünmemektedir.

Elektronik deliller ile diğer belge delilleri tam olarak aynı kapsamda değerlendirilemez. Adli bilişim uzmanlarının bilişim sistemlerinden delil elde ederken

³⁴³ Değirmenci, Sayısal, s. 360; Yaşar ve Dursun, s. 24.

³⁴⁴ Yaşar ve Dursun, s. 21.

³⁴⁵ Değirmenci, Sayısal, s. 361.

³⁴⁶ Nitekim, günümüz teknolojisi ile bluetooth, baz istasyonları marifetiyle bilişim sistemlerine müdahale etmek mümkündür. Kılıç, s. 36.

³⁴⁷ Başlar, Elektronik, s. 88.

³⁴⁸ “Sahteciliğin maddi konusunu oluşturan ve aslı elde edilemeyen belgenin aslına uygun olduğuna ilişkin onayının bulunmadığı ve bu durumuyla hukuksal sonuç doğurmayacağı gözetilmeden hükümlülük kararı verilmesi ... bozmayı gerektirmiştir.”; Yargıtay 6. CD, 3.11.1988 tarihli, E. 1988/7928 K. 1988/11809 T. sayılı kararı; Değirmenci, Sayısal, s. 140.

üzerinde çalıştığı bilişim sistemlerinde değişiklikler meydana getirebileceği bu durumu da delilin orijinalliği hakkında birtakım şüphe meydana getirebileceği değerlendirilmiştir³⁴⁹. Nitekim, bilişim sisteminin sadece başlatılması durumunda dahi, sistem birtakım bilgisayar servislerini başlatacak verinin kayıtlı olduğu harddiskte değişim meydana gelecektir. Hatta, otomatik yazılmış işletim sistemi servis yazılımı ya da üçüncü parti uygulamalarla yetkisiz sistem açılışında tüm veriler silinebilecektir. Bu duruma, yaygın şekilde çözüm olarak veride değişiklik meydana gelmemesi için bilişim sisteminin birebir kopyası alınarak bu kopya üzerinde inceleme yapılmasının uygun olacağı değerlendirilmektedir³⁵⁰.

Adli bilişim sürecinde, bilişim sistemlerinde yer alan verilerin birebir kopyalama işlemine *imaj (forensic image)* adı verilir³⁵¹. Birebir kopyalama işlemi için özel yazılım ve donanımlar kullanılmaktadır³⁵². Elektronik delillerden imaj alma işlemi, üç farklı seviyede yapılır. Bunlar, disk seviyesi imaj alma, bölüm seviyesi imaj alma ve dosya seviyesi imaj almadır³⁵³. Bölüm seviyesi ve dosya seviyesi imaj alma işlemleri sadece aktif dosyalar üzerinde gerçekleştiği için gizli sektörleri ve silinmiş verileri kapsamaz³⁵⁴. Disk seviyesi kopyalama işlemi birebir kopyalama işlemi olarak da anılır. Birebir kopyalama işlemi verinin bulunduğu bilişim sisteminde orijinalinde bulunan her sektör ve bitin (byte) kopyalanması anlamına gelir. Böylece, gizli sektör ya da silinen veriler de dahil olmak üzere bilişim cihazında yer alan tüm veriler kopyalanır³⁵⁵. Bu nedenle adli bilişimde birebir kopyalama işlemi standart hale gelmiş bir yöntemdir³⁵⁶. Birebir kopyalama işlemi yazılımsal yapılabileceği gibi donanımsal da gerçekleştirilebilir³⁵⁷. Donanımsal imaj alma, harici bir donanıma veri taşıyan belleğin yerleştirilmesi sonucu gerçekleşir. Söz konusu donanım, imaj alma işlemini gerçekleştirdiği esnada hash kodunu da otomatik olarak üretecektir. Yazılımsal imaj

³⁴⁹ Değirmenci, Sayısal, ss. 244–245.

³⁵⁰ Ahmet Serhat Şirikçi ve Nergis Cantürk, “Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi”, **Bilişim Teknolojileri Dergisi**, Cilt: 5, Sayı: 3, 2012, s. 30; Değirmenci, Sayısal, s. 245.

³⁵¹ Özen ve Özocak, s. 66.

³⁵² Şirikçi ve Cantürk, s. 30.

³⁵³ Başlar, Elektronik, s. 30.

³⁵⁴ Hüseyin Çakır ve Mehmet Serkan Kılıç, **Adli Bilişim ve Elektronik Deliller**, Seçkin Yayıncılık, Ankara, 2014, s. 172.

³⁵⁵ Şirikçi ve Cantürk, s. 30.

³⁵⁶ Çakır ve Kılıç, s. 172.

³⁵⁷ Başlar, Elektronik, s. 91.

alma işleminde ise, boot işlemi gerçekleştirilirken ilave bir yazılım marifetiyle bilgisayar üzerinden ilgili diskin imajını yeni bir veri ortamına aktarmaktadır³⁵⁸.

İmaj alma işleminin, sistem kapalıyken gerçekleştirilmesi gerekir. Kapalı sistemde imaj alınması sistemi ve veriyi koruyacaktır. Nitekim, sistemin açık olması durumunda delil güvenliği tehlikeye atılabilir³⁵⁹. Gerçekten de tuzak yazılımlar marifetiyle sistemin adli kolluk tarafından açılması ile sistem verileri kalıcı olarak silinebilir yahut başkaca kötücül düzenekleri tetikleyebilir. O nedenle, verinin bulunduğu bilişim sistemine müdahale konusunda çok titiz davranılmalıdır.

Bilişim sistemlerinde yer alan verilerin doğrudan incelenmesi yerine, imajının alınarak imajı üzerinde inceleme yapılmasının bir amacı da verilerin bütünlüğünün ve güvenilirliğinin sağlanmasıdır³⁶⁰. Veri güvenilirliği ve bütünlüğün sağlanamadığı durumlarda, soruşturmaya gölge düşecektir. Birebir imaj alma işlemi sayesinde, şüphelinin kullanmış olduğu bilişim sisteminde yer alan verilerin değişmediği, ekleme çıkarma yapılmadığı güvence altına alınmış olacaktır. Ayrıca, bilişim sisteminde yer alan verilerin delil toplama esnasında zarar görmesinin de önüne geçilecektir.

Yargıtay birçok kararında³⁶¹, yedekleme işleminden ne anlaşılmasına gerektiğine ilişkin açıklamaya yer vermiştir. Yargıtay’a göre, maddenin üçüncü fıkrasında belirtilen yedekleme işleminden, “*imaj alma*” işlemi anlaşılması gerekir. Nitekim imaj alma, dijital medyanın herhangi bir kısmının kopyalanması anlamına gelmez. İmaj olarak dijital medyada yer alan aktif, silinmiş veya artık alanlarında bulunan dijital verilerin, orijinal medyadaki haliyle bire bir aynı, *adeta aynadaki görüntüsü* gibi yedeklenmesi işlemidir.

Yine, Yargıtay başka bir kararında³⁶² ise imaj almanın önemine değinmiştir. Kararın gerekçesinde; “*Dijital delillere harici müdahalenin teknik olarak mümkün olması, çoğu zaman kim tarafından hangi tarihte müdahale yapıldığının da belirlenememesi karşısında, güvenli bir şekilde el konulup incelenebilmesi için mahallinde imaj alındıktan sonra orijinal medyanın şüpheliye bırakılması gerekmekte*

³⁵⁸ Çakır ve Kılıç, s. 173.

³⁵⁹ Şahin, s. 281.

³⁶⁰ Başlar, Elektronik, s. 89.

³⁶¹ Yargıtay’ın pek çok kararında aynı gerekçeye yer verdiği görülmektedir. Bkz; Yargıtay 16. CD 21.04.2016 tarih, E.2015/4672 K.2016/2330 sayılı kararı, Yargıtay CGK 04.02.2020 tarih, E.2019/286 K.2020/52 sayılı kararı, Yargıtay CGK 22.09.2020 tarih, E.2019/353 K.2020/367 sayılı kararı, Yargıtay CGK 25.02.2020 tarih, E.2016/544 K.2020/127 sayılı kararı.

³⁶² Yargıtay 16. CD. 21.09.2017 tarih ve E.2015/2056 K.2017/5023 sayılı kararı.

... ” ibaresine yer vererek olay yerinde yapılacak müdahalenin önemine ve imaj alma gerekliliğine yer vermiştir.

Yargıtay’ın yedekleme işlemine ilişkin hassas tutumunu önemli buluyoruz. Esasen yedekleme işleminin ne şekilde alınması gerekliliği en azından yönetmelikle düzenlenmelidir. Nihayetinde, yukarıda açıklandığı üzere imaj alma faaliyeti ile herhangi bir dosyayı kopyalamak oldukça farklı hususlardır. Bu anlamda; Yargıtay kararlarında Kanun’da yer alan yedekleme işleminden, imaj alma işleminin alınmasının anlaşılması gerekliliğine ilişkin tutumu oldukça yerindedir.

2.2.1.3. Özet Değer (Hash) Hesaplama

CMK md. 134 uyarınca verilen koruma tedbiri kararının uygulanması aşamasındaki en önemli hususlardan birisi, ilgili verinin muhakeme evresinde bütünlüğünün sağlanmasıdır³⁶³. Elektronik delil bütünlüğü, adli bilişim uzmanlarınca delile yapılan ilk müdahaleden, delilin mahkemeye sunulması ve incelenmesi aşamasının sonuna kadar değiştirilmemesidir³⁶⁴.

Hash değeri, veri depolama ünitesinin ilk sektörden başlayarak son sektöre kadar belli bir algoritmik programdan geçmesi ile üretilen, her diske ayrı özgün şekilde üretilen sayısal değerlerdir³⁶⁵. Hash değeri, değere ilişkin veriye özel parmak izi, DNA değeri gibi benzersiz bir değerdir³⁶⁶. Veri depolama birimine üretilen hash değeri veride en küçük bir değişiklik yapılması durumunda dahi değişime uğramaktadır³⁶⁷. Hash değeri, imaj alma işlemi esnasında ya da imaj alma işleminin bitmesini müteakip de uygulanabilir³⁶⁸. Ceza yargılaması devam ederken, delil bütünlüğü konusunda herhangi bir iddia atılması durumunda, adli bilişim uzmanlarının inceleme yürüttüğü imaj kopyası üzerinden yeniden hash değeri alınabilir. Bu üretilen hash değeri ile delil toplama esnasında üretilen hash değeri karşılaştırılır. İki değer aynı ise, veri bütünlüğünün korunmuş olduğu değerlendirilir³⁶⁹. Eğer hash değeri aynı değilse, veri

³⁶³ Değirmenci, Sayısal, s. 248.

³⁶⁴ Çakır ve Kılıç, s. 176.

³⁶⁵ Başlar, Elektronik, s. 93.

³⁶⁶ Murat Özbek, “Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları”, **1st International Symposium on Digital Forensics and Security**, Elazığ, 2013, s. 2.

³⁶⁷ Özen ve Özocak, s. 53.

³⁶⁸ Başlar, Elektronik, s. 93.

³⁶⁹ Başlar, Elektronik, s. 94.

bütünlüğünün bozulduğu, ilgili imaj dosyasının bozulduğu düşünülerek hükme esas alınamaz.

Kanun koyucu, madde metninde kopyalama ve yedek alma işlemini düzenlemiş ve fakat imaj alma ve hash değerinden bahsetmemiştir. Oysa, kopyalama işlemi verinin tamamının kopyalanması anlamına gelmemektedir. Yukarıda da ifade edildiği gibi, düzenlenmede yer alması gereken diskin tamamının uygun usullerle imaj alınması ve bu imajın da hash değeri ile doğrulanması gerekir. Uygulamada ise, kopyalama ve yedek alma işlemi, imaj alma ve hash değerinin belirlenmesi şeklinde gerçekleştirilir³⁷⁰. Öğretide, bu durum adli bilişim uzmanlarının *görevlerini düzgün yapma istekleri* ve *kendi iyi niyetleri* şeklinde yorumlanmış ve uygulamayı bu şekilde yapmamaları durumunda sorgulanabilecekleri yasal bir dayanak olmadığı değerlendirilmiştir³⁷¹. Bu duruma katılmakla beraber, adli bilişim uzmanlarının ileride delil değiştirdiklerine ilişkin olası iddiaları da bertaraf etmeyi hedeflediklerini değerlendiriyoruz.

Yargıtay kararlarında, sıklıkla *hash* değerinin alınmasına ilişkin bizim de iştirak ettiğimiz Özen/Özocak görüşüne³⁷² yer verilmiştir. Buna göre, delillerin alındığı safhada delil güvenliğinin korunması maksadıyla, işlemi yapan adli kolluk tarafından, bilgisayarın veri depolama birimi (hard disk) alındığı esnada öncelikle özet değeri (hash değeri) alınarak, bu değer yer aldığı tutanak tutulmalı ve tüm bu imaj alma, yedekleme vb. işlemler şüpheli veya vekilinin eşliği ile gerçekleştirilmelidir.

Koruma tedbirinin uygulamasında bazı durumlarda kolluk kuvvetinin imaj alma ve hash değeri hesaplamaya yarayan cihazın başka operasyonlarda kullanıldığı ve bu nedenle bu işlemin gerçekleştirilemeyeceğinden bahisle doğrudan elkoyma yapıldığı görülmektedir. Ancak bu usul şüphelinin hukuki güvenliğini tehlikeye sokmaktadır. Tedbirin böylesi sıkı şartlarla düzenlenmesinin karşısında bu şekilde bir yaklaşımı doğru karşılamak mümkün değildir. Bu nedenle, uzman kişilerin ilgili teçhizatını yanında bulundurmaları önem arz etmektedir.

Delile müdahale esnasında imaj ve hash değerinin alınması bu durumun da tutanak altına alınması şüpheliyi koruduğu gibi adli bilişim uzmanlarını da

³⁷⁰ Şahin, s. 281.

³⁷¹ Dülger, s. 589.

³⁷² Özen ve Özocak, s. 68.

koruyacaktır. Ancak, böyle önemli bir hususun herhangi bir görevlinin inisiyatife bırakılmaması gerektiği ve konuya ilişkin mevzuatta düzenleme yapılması gerektiği kanaatindeyiz.

2.2.2. CMK md. 134 Kapsamında Elkoyma Tedbirinin Uygulanması

2.2.2.1. Verilerin Yedeklemesinin Yapılması

Bilişim sistemlerinde yer alan veriler, hassas yapısı ile ön plana çıkmaktadır. Bu veriler işin uzmanları ya da kötü niyetli üçüncü kişilerce değiştirilebilecek niteliktedirler. Kanun koyucu söz konusu tedbirde kural olarak aramayı düzenlemiş, öngörülen istisnai durumlarda ise elkoyma işleminin yapılmasına olanak sağlamıştır. Ancak işin niteliği gereği hem şüpheli, sanığın korunması hem de suçun aydınlatılmasını sağlamak adına el konulan sistemdeki bütün verilerin yedeklemesinin yapılması ve yedeklemeden bir kopya çıkarılarak şüpheliye veya vekiline verilmesini bu durumun da ispat edilebilirliği sağlamak adına tutanağa geçirilmesine hükmetmiştir.

CMK md.134'te suça konu bütün verilerin yedeklemesinden bahsedilmiş ve fakat usuller açıkça Kanun'da ya da Yönetmelikte düzenlenmemiştir. Öğretide, yedekleme işlemi esnasında takip edilmesi gereken usuller değerlendirilmiştir. Öncelikle, yedekleme işlemi yapılacak bilişim sisteminin kolluk ya da bilişim uzmanlarınca üçüncü kişilere erişimi kapatılmalıdır³⁷³. İşin uzmanlarınca yedekleme uygulanırken tüm verilerin iki nüsha imajı alınır ve yedeklenen verinin hash değeri üçüncü parti uygulamalar marifetiyle çıkarılarak tutanak altına alınıp imzalanır³⁷⁴. Verinin bulunduğu dijital ortamın hash değeri alındıktan sonra, herhangi bir şekilde üçüncü kişilerce veri değişikliği meydana gelirse hash değeri değişecek delil niteliğini kaybedecektir. Öte yandan, muhakemenin ilerleyen evrelerinde şüphe duyulması halinde şüpheli veya vekiline teslim edilen ikinci nüsha hash değeri kontrol edilerek, delil olarak kullanılabilecektir. Böylece, delilin bütünlüğünün bozulması durumunda delile ulaşmanın ikinci bir şansı olabilecek ve ispat edilebilirlik sağlanacaktır.

³⁷³ Şahin, s. 280.

³⁷⁴ Dülger, s.581.

CMK md. 134 kapsamında, verilerin yedeklenmesinin düzenlenmiş olması oldukça yerinde olmuştur. Ancak uygulamada çoğu zaman elkoyma işlemi esnasında bir kopya çıkarılmamakta, ilgili cihaz delil torbasına konarak doğrudan muhafaza altına alınmaktadır. Mevzuat hükümleri bu kadar açık olmasına rağmen, uygulamadaki usuller, kamuoyunu meşgul eden bazı davalar da dahil olmak üzere çoğunlukla farklı seyretmektedir. Genellikle, CMK md. 134'e göre hüküm kurulduğunda kolluk kuvvetleri şifrenin kırılmadığına ilişkin tutanak tutmakta ve doğrudan elkoyma tedbirini uygulamaktadır. Bu vesile ile yedekleme işlemini kendi çalışma alanlarında gerçekleştirmektedir. Ancak, kolluk kuvvetlerince yapılan bu uygulama hukuka aykırıdır.

Anayasa Mahkemesine yapılan bireysel başvuruya ilişkin verilen bir kararın³⁷⁵ bizim de katıldığımız karşı oy gerekçesinde; başvurucunun evinde yapılan arama neticesinde ele geçirilen P. isimli veri tabanının yer aldığı TVDO'nun, kolluk tarafından yedeklenmesinin yapılmaması, yedeklerden bir kopyasının verilmemesi, TVDO'nun şifresinin bilahare emniyetçe tek taraflı açılması hususunun, CMK md.134'te yer alan emredici hükümlere aykırı uygulama olduğu, bu durumun Anayasa md. 38 ile teminat altına alınan "*Kanuna aykırı elde edilmiş bulgular delil olarak kabul edilemez*" hükmü karşısında *kanunsuz delil* olarak kabul edilmesi gerekmekte olup, bu kapsamda verilen tutuklama kararı da hukuka aykırıdır.

Uygulamada genellikle kolluk kuvvetlerince arama anında yedekleme yapılmadan cihaza elkonulmakta; daha sonra şüpheliden, tedbire konu bilişim sisteminin kapasitesine göre taşınabilir bellek talep edilmekte³⁷⁶ ve yedekleme işlemi bu cihaza yapılmaktadır. Bu usul açıkça hukuka aykırıdır. Olması gereken Kanun'da yer aldığı gibi öncelikle arama tedbirinin gerçekleştirilmesi, eğer istisnai şartlar mevcutsa o halde elkoyma tedbirine başvurulmasıdır. Elkoyma tedbirine başvurulacaksa bile, kolluk kuvvetlerinin bilişim sistemlerine ilk temasından, yedekleme³⁷⁷ işleminin gerçekleştirilmesi anına kadar şüpheli/müdafinin tedbire konu ilişim sisteminden ayrı kalmaması gerekir. Aksi halde, soruşturma evresine gölge düşecek ve toplanan tüm dijital veriler hukuka aykırı olacaktır. Nitekim, bilişim

³⁷⁵ AyM 27.10.2016 tarihli, 2014/3129 numaralı bireysel başvuru kararı.

³⁷⁶ Dülger, s. 588.

³⁷⁷ Uygulamada genellikle "*imaj alma*" olarak anılmaktadır. Yedekleme işlemi gerçekleştirildikten sonra mutlaka hash değeri alınarak yedeklerin üzerine yazılmalı ve kolluk kuvvetlerince onaylanmalıdır. Hash değerinin varlığı veri bütünlüğünün teminatıdır.

sistemlerinde yer alan veriler kolaylıkla değiştirilebilir, yeni veri eklenebilir ya da bir veri ortadan kaldırılabilir. Objektif ve ideal hukuk düzeninde, böylesi hassas veri yapısına sahip sistemde kötü niyetli kişinin müdahalesinin ortadan kaldırmaya yarayacak uygun tedbir alınmalıdır.

Yargıtay bir kararında³⁷⁸,

Adli Bilişim Şube Müdürlüğüince veri çıkarma işleminin uluslararası adli bilişim standartlarına uygun olarak yapılması, alınan imajların bir kopyası sanığa veya müdafisine verilmek, diğer kopyası ise incelenmek üzere iki ayrı hard disk içerisine export edilmesi, yapılan işlemler için imaj alma tutanağına, teknik inceleme ve export (veri çıkarım) raporuna bağlanması, imaj alma işlemi tamamlandıktan sonra ilgili materyallerin ağzı mühürlü delil torbasına konularak mühür kapatma ve teslim tesellüm tutanağının tanzim edilmesi, dijital delillere müdahaleyi önleyecek şekilde seri numaraları tutanağa yazılmak suretiyle usulüne uygun zapt edilip mühürlenmesi ve dijital delillere dışarıdan müdahale edildiğini gösterir herhangi bir bulguya rastlanılmaması hususları birlikte değerlendirildiğinde imaj alma işleminin usulüne uygun şekilde uzman kişiler tarafından dijital materyallerin delil olma niteliği korunarak gerçekleştirildiği anlaşıldığından sanıktan elde edilen elektronik deliller toplanırken kişisel verilerin ve özel hayatın gizliliğinin korunması ilkelerine aykırı davranılmamakla birlikte CMK'nın 134. maddesine uygun hareket edildiği, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma işlemi sonucu elde edilen delillerin CMK'nın 217. maddesinin ikinci fıkrası uyarınca hukuka aykırı delil niteliğinde olmadığı ve bu nedenle hükme esas alınabileceği kabul edilmelidir...

gerekçesiyle hüküm kurmuştur. Yargıtay'ın karar gerekçesinde CMK md. 134'ün uygulanması safhasına ilişkin bir takım somut kriterler ortaya koyduğunu görüyoruz. Yargıtay'ın ortaya koyduğu bu kriterlere katılmakla beraber, söz konusu kriterlerin niteliğine göre, Kanun ya da Yönetmelik'te detaylı şekilde düzenlenmesi gerektiğine inanıyoruz.

Yargıtay başka bir kararında³⁷⁹, mahalde yedekleme işleminin objektif olarak mümkün olmadığının kabulünün zorunlu olduğu hallerde, aramayı gerçekleştiren

³⁷⁸ Yargıtay CGK 22.09.2020 tarihli, E.2019/353 K.2020/367 sayılı kararı.

³⁷⁹ Yargıtay 16. CD. 21.09.2017 tarih ve E.2015/2056 K.2017/5023 sayılı kararı, Yargıtay 16. CD. 10.10.2019 tarih ve E.2019/2637 K.2019/5904 sayılı kararı.

kolluk görevlilerinin dijital delillere müdahaleyi önleyecek şekilde ilgili veri depolama biriminin seri numaralarının da tutanak altına alınarak mühürlenmesinin gerektiği, şüpheli veya müdafinin denetleme imkanı sağlanarak inceleme alanına kadar eşlik etmesine olanak sağlanması gerektiği, mümkün olan en kısa sürede şüpheli veya müdafinin huzurunda mühürün açılarak dijital ortamın derhal imajının alınması ve ilgisine imajlardan bir kopya ve orijinalinin teslim edilmesinin gerektiği, yine sanık veya müdafinin mühür açma sırasında olay mahallinde bulunmasına imkan olmadığı takdirde koruma tedbirine karar veren hakim huzurunda açılarak imaj alma işleminin bu sırada gerçekleştirilmesi gerektiğine aksi halde delillerin tartışılır hale geleceğine ve hükme esas alınmasının hukuka aykırı olacağına hükmetmiştir. Yargıtay'ın kararına katılmakla beraber, yedekleme işleminin objektif olarak mümkün olmaması hususunun kötüye kullanılabileceğini düşünüyoruz. Nitekim, uygulamada genellikle kolluk tarafından yedekleme işleminin gerçekleşmesinin mümkün olmadığı tutanağa bağlanarak bilişim sistemine doğrudan el konulduğunu sıklıkla görüyoruz.

2.2.2.2. Kopyalama ve Metin Haline Dönüştürme

CMK md. 134 kapsamında bilişim sistemlerinde uygulanan koruma tedbirinde kural, arama yapılan yerde kopyalama işleminin gerçekleştirilmesidir³⁸⁰. Bu işlem gerçekleştirilirken sistemdeki verilerin kopyası alınır, bir kopya şüpheli veya vekiline teslim edilir. Düzenleme bu yönüyle hem şüpheliyi korumakta hem de delilin bütünlüğünü sağlamaktadır. Öte yandan, kopyası alınan veriler incelenerek bu kayıtların çözümü yapıp metin haline getirilir³⁸¹.

Öğretide, CMK md. 134'ün uygulaması kapsamında metin haline getirilme hükmü eleştirilmiştir. Bir görüşe³⁸² göre, metin halinde verinin kâğıda yazdırılması işlemi maddi olarak imkânsız olmanın yanında uygulamanın da gereksiz olduğu savunulmuştur. Eleştiriye kısmen katılmakla beraber Kanun maddesinde yapılacak düzenleme ile sorunun ortadan kalkacağına inanıyoruz. Bilişim sistemlerinde arama, kopyalama ve elkoyma koruma tedbiri, genel arama ve elkoyma tedbirine kıyasen temel hak ve özgürlüklere daha fazla müdahale etmektedir. Zira, Kanun koyucu bu

³⁸⁰ Uğraş, s. 126.

³⁸¹ Uğraş, s. 126.

³⁸² Özen ve Özocak, s. 70.

durumu göz önünde bulundurmuş ve daha sıkı şartlara bağlamıştır. Bazı durumlarda bilişim sistemlerinde suça konu delil tek bir sayfa metin, tek bir resim gibi küçük boyutlu verilerden oluşabilir. Bu durumda, tüm bilişim sisteminin verilerini kopyalama, elkoyma işlemi ölçsüz olabilecektir. Somut olaya göre, hareket edilmesinin uygun olacağını, delilin makul olarak kolayca metin haline getirilebilecek durumlarda, bu yolun izlenmesinin uygun olacağını ve fakat binlerce sayfa doküman gibi yüksek boyutlu verilerde ise metin haline getirmek yerine TVDO ortamlarına uygun usullerde yedekleme yapılarak incelenmesinin uygun olacağını değerlendirmekteyiz.

Yargıtay da bir kararında³⁸³, bu konuya yer vermiş ve gerekçeli kararında şu ifadeleri kullanmıştır.

Mahkeme tarafından gerekçeli kararın 2. Kitap B bölümünde "Bilişim itirazları" başlığı altında yapılan "...Örneğin, CMK'nın 134/5. maddesinde belirtilen bilgisayar veya bilgisayar kütüklerine elkoymaksızın da sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır." tespitinun uygulamada yeri bulunmamaktadır. "Mahkememiz tarafından yaptırılan HTS raporu sadece bir DVD'ye sığan 3,5 Gb veri içeren excel tablo verisi Yargıtay denetimi yapılması aşamasında kullanılması için yaklaşık 6- 7 ayı bulan bir zaman içerisinde kâğıda bastırılabilmiş, her biri 500 sayfa olan 1300 civarında klasör oluşturulduğu yapılan uygulama ile müşahade edilmiştir.

Yargıtay önüne gelen somut olayda ilgili dijital veri, objektif olarak kâğıda basılamayacak kadar fazladır. Yargıtay'ın kararı, yüksek boyutlu verilerin metin haline getirmek yerine TVDO ortamlarına uygun usullerde yedeklemesinin yapılarak değerlendirilmesi gerektiğine ilişkin görüşümüzü desteklemektedir.

2.2.2.3. Elkonulan Eşyanın İadesi

CMK md. 134, kural olarak koruma tedbirinin mülkiyet hakkını sonlandırmayacak şekilde düzenlenmiştir. Ancak yukarıda açıklandığı üzere ötürü belli şartlar gerçekleşmesi durumunda bilişim sistemlerine elkoyma gerçekleştirilebilir.

³⁸³ Yargıtay 16.CD. 21.04.2016 tarihli, 2015/4672 E. 2016/2330 K. Sayılı kararı

İstisnai olarak elkoyma işleminin gerçekleşmesi durumunda, şifrenin çözümünün yapılması ve ardından gerekli kopyanın alınmasında sonra ilgili cihazlar gecikmeksizin iade edilmesi gerekir. Nitekim tüm koruma tedbirlerinde olduğu gibi bilişim sistemlerinde arama kopyalama ve elkoyma tedbiri de geçici nitelikte olması gerekmektedir.

Madde metni zikredilen şekilde olmakla beraber uygulamada bilişim sistem cihazlarına makul süreyi aşacak şekilde uzun süreler elkonulduğu görülmektedir. Konuya ilişkin gerekçe ise bilişim uzmanı personel sayısının yetersiz olması, dava dosyaları kapsamında bekleyen çok sayıda bilişim sistem cihazı olması, inceleme süresinin oldukça uzun olmasıdır. Kanaatimizce, bahsedilen gerekçelerin yanında asıl sorun kolluk tarafından elkoyma işlemine sıkça başvurulmasından ileri gelmektedir. Adli kolluk, yedekleme ve kopyalama işlemine öncelikle başvurması ve elkoyma işlemini istisnai uygulaması halinde elkonulan bilişim cihazları önemli ölçüde azalacak ve muhafaza altına alınan süre de azalacaktır. Tüm bunların yanında eğer nitelikli uzman personel sayısı yetersiz ise uygun miktarda uzman personelin istihdam edilmesi uygun olacaktır.

Bilgisayarlara ya da bilgisayar kütüklerine elkoyma işlemi gerçekleştirilmesi durumunda şifrenin çözülmesi ve gerekli kopyalama işlemi gerçekleştirilmesini müteakip elkoyma işlemi gerçekleştirilen sistemler gecikmeksizin iade edilmesi gerekir³⁸⁴. Elkoyma işlemi içinde veri olan donanımdan ibaret olması gerekir. Tüm bilgisayara elkoymak mülkiyet hakkına doğrudan zarar verebilecektir.

2.2.2.4. Suç Unsuru Barındıran Veri Kopyasının Durumu

Elkoyma işlemine konu olan bilgisayarlarda ya da bilgisayar kütüklerindeki bazı veriler suç unsuru barındırabilir. Yedeklemesi yapılan bilişim sistemlerinde suç unsuru ihtiva eden verilerin bir yedeğinin verilmesi yahut elkonulan cihazın olduğu gibi iade edilmesi durumunda suçun işlenmesine devam edilmesi mümkün olabilir. Örneğin, çocuk pornografisi ya da çalıntı olan kredi kartı bilgilerinin yedeklemesinin yapılarak bir nüshanın müdafî/şüpheliye verilmesi yeni sakıncalara yol açabilecektir. CMK md. 127 doğrultusunda eşya müsaderesine başvurulabileceği düşünülse de

³⁸⁴ Öztürk ve diğerleri, Koruma Tedbirleri, s. 214.

konuya özgü düzenleme yapılması kanunilik ilkesi açısından uygun olacağını düşünen yazarlar³⁸⁵ bulunmaktadır. Yine, yedekleme sonrası suç unsuru barındıran yedeklerin, sadece müdafie bir nüsha verilmesine imkân sağlayacak düzenleme yapılmasını öneren yazarlar³⁸⁶ da bulunmaktadır.

Öğretide bilişim sisteminin suç unsuru ihtiva eden veri barındırması durumunda yedekleme işleminin yapılma usulüyle ilgili öneride bulunulmuştur. Bu görüşe göre³⁸⁷, suç unsuru ihtiva eden verinin bulunduğu bilişim cihazının şüpheli/vekile iade edilmesi durumunun uygun olmadığı, bu sebeple bu verinin silinerek bilişim cihazının şüpheliye iade edilmesine imkân tanıyan düzenlemenin yapılmasının uygun olacağı değerlendirilmiştir.

Yargıtay bir kararında³⁸⁸; CMK md. 134 uyarınca elkonulan dijital verilerin, her ne kadar yedeklenen verilerin bir kopyası ile aslının şüpheliye veya vekiline verilmesini öngörmüşse de somut olayda hükümeti devirmeye ve anayasal düzeni cebren ilgaya teşebbüs edilmesi, olağan üstü halin varlığı, sanığın üzerine atılı suçun mahiyeti ve dijital materyallerde bulunabilecek bilgilerin niteliği nedeniyle TCK md.54/4 uyarınca ilgili dijital materyalde suça konu verinin olup olmadığı hususu yargılama sonunda anlaşılacağından söz konusu materyallerin yargılama sonuna kadar sanığa verilmemesi gerektiğine hükmetmiştir. Kanaatimizce de, suç unsuru ihtiva eden verinin şüpheliye iade edilmemesi gerekir. Zira aksinin kabulü, suçluyu suça teşvik etmekle sonuçlanacaktır.

2.3. TEDBİR SONRASI ELDE EDİLEN VERİLERİN YOK EDİLMESİ

Çalışmamıza konu koruma tedbiri kapsamında usulüne uygun verilen karar ile şüphelinin kullanımında olan bilişim sisteminde yer alan pek çok veri kopyalanmakta ve elkonulmaktadır. Kopyalanan bu veriler kişisel veri olabileceği gibi çok kıymetli ticari sır da olabilir. Yürütülen soruşturma sonrasında Cumhuriyet savcısı tarafından

³⁸⁵ Öztürk ve diğerleri, Koruma Tebdirleri, s. 216; Özen ve Özocak, s. 70.

³⁸⁶ Yazara göre, suç unsuru ihtiva eden bilişim sistemlerinin bir yedeğinin yeni suç işlemeyeceği varsayımıyla kişinin avukatına verilmesine imkân sağlayacak düzenleme yapılmalıdır. Bu vesile ile, hem delilin doğruluğunun teyit edilmesi sağlanacak hem de aynı ya da başkaca bir suç işlenmesinin önü kapatılacaktır. Dülger, s. 586.

³⁸⁷ Uğraş, s. 130.

³⁸⁸ Yargıtay CGK 22.09.2020 tarihli, E.2019/353 K.2020/367 sayılı kararı.

iddianame düzenlenebileceği gibi kovuşturmayaya yer olmadığına dair karar da verilebilir. Yine muhakeme sonucu beraat ya da mahkûmiyet kararı verilebilir. Bu durumda, şüpheliye ait hakkında yürütülen adli takibat sonlanacak ve elkonulan verilerin ve veri taşıyıcıların ne olacağı gündeme gelecektir.

CMK md. 134'ün madde metni göz önüne alındığında, adli takibatın sonlanması durumunda elkonulan verilerin ne olacağına ilişkin doğrudan düzenleme yapılmadığı görülecektir. Arama ve elkoyma tedbiri verilen bilişim sistem cihazının, failin mahkumiyeti halinde, mahkûmiyet kararı ile birlikte söz konusu cihazın iadesine karar verilebileceği gibi, cihazın suç unsuru ihtiva etmesi halinde TCK md. 54 uyarınca müsadereğine, KYOK ya da beraat kararında ise şüpheli/sanığa iadesine karar verilebilir³⁸⁹.

Bahse konu durumlarda bilişim sistem cihazlarına yukarıda anlatıldığı şekilde yaklaşılabilir. Ancak söz konusu cihazlardan alınan imajların ne olacağı belirsizliğini sürdürmektedir. Öğretide, CMK md.137/3 uyarınca tespit ve dinlemeye ilişkin kayıtların en geç on gün içinde yok edileceği düzenlenmişken; temel hak ve özgürlüklere yoğun müdahale içeren CMK md. 134 bakımından herhangi bir düzenlemeye yer verilmemiş olması büyük bir eksiklik olarak nitelendirilmiştir³⁹⁰. Yine, söz konusu soruna çözüm olarak ise CMK md. 137/3'ün kıyasen işletilebileceği, buna göre kovuşturmayaya yer olmadığı kararı verilmesini müteakip on gün içinde Cumhuriyet savcısı denetiminde yok edilmesi gerektiği ve bunun da tutanağa bağlanması gerektiği önerilmiştir³⁹¹.

Dülger³⁹² ise, konuyu farklı bir açıdan ele almış koruma tedbiri kapsamında alınan imajların günümüzde mahkeme ya da Cumhuriyet savcılarınca imha edilmesine ilişkin emir gönderdiklerini ancak iyi niyetle yapılan bu uygulamanın açık yasa maddesi olmaması karşısında hukuka aykırı olduğunu değerlendirmiştir. Yine yazara göre, söz konusu imajların koruma tedbiri neticesinde alındığı bu nedenle imajların imhasının da temel hak ve özgürlüklerle doğrudan ilişkili olduğu ve buna göre kısıtlamanın ancak Anayasa md. 13 doğrultusunda Kanunla yapılabileceğini belirmiş,

³⁸⁹ Dülger, s. 592.

³⁹⁰ Değirmenci, Sayısal, s. 380.

³⁹¹ Ünal, s. 127.

³⁹² Dülger, s. 593.

bu doğrultuda mahkeme kararı ya da savcılık emri ile değil açık düzenleme doğrultusunda imha işleminin gerçekleştirilmesi gerektiğini değerlendirmiştir.

2.4. TESADÜFEN ELDE EDİLEN DELİLLER

Tesadüfen elde edilen delil; yürütülmekte olan soruşturma veya kovuşturmayla ilgisi olmayan ancak, diğer bir suçun işlendiği şüphesini uyandırabilecek bir delil anlamında gelir. Söz konusu düzenleme, CMK md. 138 ile karşımıza çıkmaktadır. Madde metninde iki fıkra yer almaktadır. Birinci fıkroda, tüm koruma tedbirleri yönünden düzenleme bulunmakla beraber ikinci fıkroda sadece telekomünikasyon yoluyla yapılan iletişimin denetlenmesi sırasında elde edilen deliller yönünden düzenleme bulunmaktadır.

Adli ve önleme aramaları yönetmeliğinde söz konusu düzenleme bir miktar genişletilmiş, 10. madde ile yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmakla birlikte, karar veya yazılı emirde konu edilmeyen ancak diğer bir suçun işlendiği şüphesini uyandırabilecek deliller de tesadüfen elde edilen deliller arasında sayılacaktır.

Tesadüfen elde edilen delile arama esnasında sürpriz bir şekilde rastlanması gerekir. Bu tesadüfe arama esnasında arama emrinin çizdiği sınırlar içerisinde rastlanmış olması gerekir³⁹³. Kolluğun arama faaliyeti gerçekleştirdiği esnada suça ilişkin arama yaparken, arama faaliyetini yarıda bırakıp başka bir eşyayı araması durumunda tesadüfen delil edilmesinden bahsetmek mümkün olmayacaktır³⁹⁴.

Hukuk devleti ilkesi gereği adli kolluğun işlenen suça göz yumması beklenemez³⁹⁵. Arama esnasında tesadüfen delil elde edilmesi durumunda aramayı gerçekleştiren her kolluk görevlisi muhafaza altına alma kararı verebilir. Ancak muhafaza altına alma işleminin kolluk tarafından gerçekleştirilmesi durumunda, söz konusu durum gecikmeksizin Cumhuriyet savcılığına bildirilmelidir³⁹⁶. Nitekim bu düzenlemenin amacı koruma altına alınmadığı takdirde ortadan kalkabilecek delilin varlığını korumaktır³⁹⁷.

³⁹³ Özbek ve diğerleri, s. 329.

³⁹⁴ Değirmenci, Sayısal ,s. 448.

³⁹⁵ Değirmenci, Sayısal ,s. 450.

³⁹⁶ Özbek ve diğerleri, s. 330.

³⁹⁷ Değirmenci, Sayısal, s. 448.

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbiri gerçekleştirilmesini müteakip tesadüfen başka bir suça ilişkin delil tespit edilmesi mümkündür. Bu noktada, CMK md. 138 devreye girecek, arama kararında yer almayan diğer bir suçun işlendiği şüphesini uyandırabilecek bir delil elde edilirse; söz konusu delil muhafaza altına alınarak, durum derhal Cumhuriyet Savcılığına bildirilecektir³⁹⁸. Ancak bu noktada önemle belirtmek gerekir ki tıpkı yukarıda açıklandığı üzere arama, kopyalama ve elkoyma sırasında elde edilen verinin gerçekten tesadüfen elde edilmiş olması gerekir. Elkoyma işlemi gerçekleştirildikten sonra arama kararında yer alan suça odaklanılmalı bunun dışında yer alan verilere titizlikle yaklaşmalıdır.

Yine benzer şekilde genel arama ve elkoyma tedbiri uygulanırken de suça konu olacak bilişim sistemine tesadüfen rastlanabilir. Konuyu somutlaştırmak adına örnek verecek olursak, uyuşturucu ticareti şüphesi ile verilen genel arama kararında kredi kartı dolandırıcılığı da yapıldığı ve bu hususun olay mahallinde yer alan bilişim cihazları vasıtasıyla gerçekleştiği konusunda tesadüfi bir delile rastlanabilir. Bu noktada, yönetmelikle belirlenen usul ile Kanun'da düzenlenen usul hükümleri tam olarak örtüşmemektedir. Yönetmeliğe göre, söz konusu delil koruma altına alınacak, Cumhuriyet başsavcılığına derhâl bildirilerek el koyma işlemini gerçekleştirmek için Cumhuriyet savcısından yeni bir yazılı emir istenecektir. Cumhuriyet savcısına ulaşamadığı takdirde kolluk âmirinin yazılı emriyle kolluk görevlileri elkoyma işlemini gerçekleştirebilecektir. Ancak kanun koyucu CMK md. 134 ile bilişim sistemlerine elkoyma tedbirini istisnai olarak düzenlemiştir. Buna göre, yukarıda ayrıntılı olarak açıklandığı üzere öncelikle arama ve kopyalama işlemi gerçekleşecek; şartları oluşursa kural olarak hâkim, gecikmesinde sakınca bulunan hallerde ise Cumhuriyet savcısı tarafından elkoyma işlemi gerçekleştirebilecektir. Kanun koyucu kolluk amirine bilişim sistemlerine elkoyma yetkisi tanımamıştır. Bu anlamda, genel arama ve elkoyma tedbiri icra edilirken, tesadüfi olarak bilişim sistemine rastlanırsa bu iki hükmün birlikte işletilmesi uygun olacaktır. Zira tesadüfi olarak bilişim sistem cihazına rastlanıldığı takdirde, bu delilin koruma altına alınması Cumhuriyet Başsavcılığına bildirilmesi ve akabinde CMK md. 134'ün işletilmesi uygun olacaktır.

³⁹⁸ Öztürk ve diğerleri, Koruma Tebdirleri, s. 216.

2.5. TEDBİRE KARŞI KANUN YOLU

İtiraz; kural olarak hâkim kararları ve kanunun açıkça düzenlediği hallerde, nihai kararlardan evvel mağdur olduğunu ileri süren ilgililerin kararı veren mercie başvurusu üzerine, başka bir merci tarafından yeniden incelenmesinin sağlayan olağan kanun yoludur³⁹⁹. İtirazı inceleyen makam, verilmiş olan kararın hatalı olduğunu değerlendirirse; söz konusu kararı kaldırarak yerine yeni bir karar tesis edebilir⁴⁰⁰.

İtirazın konusunu hâkim kararı oluşturmakla beraber, istisnai hallerde mahkeme kararları hakkında da itiraz kanun yoluna gidilebilir⁴⁰¹. CMK md.134 kapsamında verilen tedbir kararına CMK md.267 hükümleri doğrultusunda 7 gün içinde itiraz edilebilir. Ancak, kararına itiraz edilen makam veya kararı inceleyen merci kararın geri bırakılmasına karar vermediği sürece, itiraz verilen kararın uygulamasını kendiliğinden durdurmaz⁴⁰². Ancak, kararı inceleyecek merci veya kararına itiraz edilen makam, itiraza konu kararın geri bırakılmasına karar verebilir.

CMK md.134'e göre; soruşturma evresinde sulh ceza hâkimi tarafından karar alınması durumunda, itiraz kanun yolunun uygulanmasında herhangi bir tereddüt bulunmamaktadır. Nitekim, yukarıda zikredildiği gibi tüm hakimlik kararlarına karşı itiraz yolu işletilebilir. Ancak, CMK md.134 kapsamında kovuşturma evresinde karar verilmesi durumunda itiraz yolu işletilemeyecektir. Nihayetinde, CMK md. 134'e ilişkin mahkeme kararı hakkında itiraz yoluna başvurmak için Kanun'da açık düzenleme yapılmış olması gerekir. CMK md. 134 incelendiğinde, böyle bir düzenleme olmadığı görülmektedir. Bu anlamda, ilgili bölümde yer verilen CMK md. 134'ün kovuşturma evresinde uygulanıp uygulanamayacağı sorunu burada da kaşıma çıkmaktadır. Söz konusu maddenin kovuşturma evresinde de uygulanması durumunda şüpheli ve sanık yönünden kullanılabilecek kanun yollarının ayrıştığı görülmektedir. Bir başka deyişle söz konusu koruma tedbirinin soruşturma evresinde uygulanması ile kovuşturma evresinde uygulanması arasında şüpheli ve sanığın hak arama hürriyeti farklılık göstermektedir. Buna göre, kanun koyucunun iradesinin

³⁹⁹ Özbek ve diğerleri, s. 726; Erdem ve diğerleri, s. 771; Cumhuriyet Şahin ve Neslihan Göktürk, **Ceza Muhakemesi Hukuku-2**, 12. baskı, Seçkin Yayıncılık, Ankara, 2022, s. 254; Mustafa Ruhan Erdem ve Candide Şentürk, **Ceza Muhakemesinde Kanun Yolları**, Seçkin Yayınevi, Ankara, 2018, s. 71.

⁴⁰⁰ Erdem ve diğerleri, s. 771.

⁴⁰¹ Özbek ve diğerleri, s. 727.

⁴⁰² CMK md. 267-271 arasında olağan kanun yollarından itiraz kurumu düzenlenmiştir.

CMK md. 134'ün sadece soruşturma evresinde uygulanması yönünde irade ortaya koyduğu kanaatindeyiz.

CMK md. 134 kapsamında, istisnai hallerde elkoyma işlemi de gerçekleştirilebilir. Bu durumda, elkoyma tedbirine karşı düzenlenmiş olan yasal çare olan CMK md. 127/4'e başvurulabilir⁴⁰³. Bu bağlamda, şüpheli veya bilişim sistem cihazının maliki elkoyma tedbirine karar verilmiş ise bu tedbirin gerekli olup olmadığına ilişkin değerlendirme yapılması hususunda talepte bulunabilecektir⁴⁰⁴.

2.6. HUKUKA AYKIRI KORUMA TEDBİRLERİ NEDENİYLE TAZMİNAT

AİHS'nin 5. Maddesi "*Herkes özgürlük ve güvenlik hakkına sahiptir. Aşağıda belirtilen haller dışında ve yasanın öngördüğü usule uygun olmadan hiç kimse özgürlüğünden yoksun bırakılamaz*" şeklinde düzenlenmiş ve maddede yer alan koşullara aykırı uygulama yapılması durumunda; "*aykırı bir yakalama veya tutma işleminin mağduru olan herkes tazminat hakkına sahiptir*" hükmüne yer verilerek, bireylerin tazminat isteme hakkı saklı tutulmuştur. Anayasamızda ise, kişi hürriyeti ve güvenliği üst başlığı ile 19. maddede kişinin hangi sebeplerle hürriyetinden yoksun bırakılabileceği belirtilmiş ve hukuka aykırı şekilde şüpheli veya sanıklara verilen zararın devletçe giderilmesi gerekliliği düzenlenmiştir⁴⁰⁵.

CMK'dan önce, 446 sayılı Kanunla hakkında haksız yakalama ve tutuklama tedbiri uygulananlara tazminat ödeme hususu CMK ile şartları kişi lehine genişletilerek yeniden düzenlenmiştir⁴⁰⁶. CMK md.141'de kişilerin suç soruşturması ve kovuşturması esnasında oluşan maddi ve manevi zararlarını hangi şartlarda devletten isteyebileceği düzenlenmiştir⁴⁰⁷. Madde metninde dijital yollardan elde

⁴⁰³ CMK md. 127/4 "*Zilyedliğinde bulunan eşya veya diğer malvarlığı değerlerine elkonulan kimse, hâkimden her zaman bu konuda bir karar verilmesini isteyebilir.*" şeklinde düzenlenmiştir.

⁴⁰⁴ Değirmenci, Sayısal, s. 381.

⁴⁰⁵ Erdem ve diğerleri, s. 654.

⁴⁰⁶ Özbek ve diğerleri, s. 446.

⁴⁰⁷ CMK md. 141'de devletin koruma tedbirleri nedeniyle tazminat ödeme yükümlülüğünün şartları düzenlenmiştir. Buna göre;

"Suç soruşturması veya kovuşturması sırasında;

a) Kanunlarda belirtilen koşullar dışında yakalanan, tutuklanan veya tutukluluğunun devamına karar verilen,

b) Kanunî gözetim süresi içinde hâkim önüne çıkarılmayan,

c) Kanunî hakları hatırlatılmadan veya hatırlatılan haklarından yararlandırılma isteği yerine getirilmeden tutuklanan,

edilen delillere ilişkin tazminat sebebi özel olarak düzenlenmemiştir⁴⁰⁸. Ancak, CMK md. 134 kapsamında, bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirinin hukuka aykırı uygulanması durumunda, CMK md.141 kapsamında koruma tedbirleri nedeniyle tazminat gündeme gelebilecektir. Nitekim, bilişim sistemlerinde arama ve elkoyma, özel bir arama ve elkoyma tedbiridir. Bu bağlamda, CMK md.141/1(i) bendinde ölçüsüz şekilde uygulanan arama tedbirinin de tazminata konu olabileceği düzenlendiğinden, söz konusu madde bilişim sistemlerinde arama ve elkoyma yönünden de uygulanabilir⁴⁰⁹. Yine, CMK md.141/1(j) bendinde, koşulları oluşmadığı halde eşyalarına, malvarlığına elkonulan veya korunması için gerekli tedbirler alınmayan durumlarda ve eşyası veya diğer malvarlığı değerleri amaç dışı kullanılan veya zamanında geri verilmeyen kişiler hakkında da tazminata hükmedilebileceği düzenlenmiştir. Öte yandan, ilişim sistemlerinde arama, kopyalama ve elkoyma tedbiri uygulanırken ilgili cihaza yazılımsal ya da donanımsal zarar verilebilir. Böyle bir durumda da tazminat hükümlerine gidilebilmesi gerekir⁴¹⁰.

2.7. TEDBİRİN HUKUKA AYKIRI UYGULANMASI NEDENİYLE CEZA HUKUKU SORUMLULUĞU GEREKTİREN HALLER

CMK md. 134'te yer alan koruma tedbiri özel hayatın gizliliği ve mülkiyet hakkının korunmasının sağlanması nedeniyle sıkı şartlara bağlanmıştır. Bu nedenle

-
- d) Kanuna uygun olarak tutuklandığı hâlde makul sürede yargılama mercii huzuruna çıkarılmayan ve bu süre içinde hakkında hüküm verilmeyen,*
e) Kanuna uygun olarak yakalandıktan veya tutuklandıktan sonra haklarında kovuşturmayaya yer olmadığına veya beraatlerine karar verilen,
f) Mahkûm olup da gözetim ve tutuklulukta geçirdiği süreleri, hükümlülük sürelerinden fazla olan veya işlediği suç için kanunda öngörülen cezanın sadece para cezası olması nedeniyle zorunlu olarak bu cezayla cezalandırılan,
g) Yakalama veya tutuklama nedenleri ve haklarındaki suçlamalar kendilerine, yazıyla veya bunun hemen olanaklı bulunmadığı hâllerde sözlü açıklanmayan,
h) Yakalanmaları veya tutuklanmaları yakınlarına bildirilmeyen,
i) Hakkındaki arama kararı ölçüsüz bir şekilde gerçekleştirilen,
j) Eşyasına veya diğer malvarlığı değerlerine, koşulları oluşmadığı halde elkonulan veya korunması için gerekli tedbirler alınmayan ya da eşyası veya diğer malvarlığı değerleri amaç dışı kullanılan veya zamanında geri verilmeyen,
k) Yakalama veya tutuklama işlemine karşı Kanunda öngörülen başvuru imkânlarından yararlandırılmayan,
Kişiler, maddî ve manevî her türlü zararlarını, Devletten isteyebilirler."

⁴⁰⁸ Erdem ve diğerleri, s. 654.

⁴⁰⁹ Değirmenci, Sayısal, s. 381.

⁴¹⁰ Ünal, ss. 129, 130.

tedbirin uygulanması esnasında sürecin hukuka aykırı işletilmesi durumunda TCK'da yer alan bazı suç tipleri gündeme gelebilmektedir.

Bilgisayarlarda, bilgisayar programları ve kütüklerinde arama kararı kural olarak sulh ceza hâkimi tarafından verilir. Söz konusu kurala istisna getirilmiş ve gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısına da karar alma yetkisi tanınmıştır. Ancak Cumhuriyet savcısına tanınan bu yetki Sulh Ceza Hakimine kıyasla daha sınırlıdır. Cumhuriyet savcısı gecikmesinde sakınca bulunan hallerde arama kararı verse de yirmi dört saat içinde söz konusu kararı hâkim onayına sunmalıdır. Yine hâkim de kararını yirmi dört saat içinde vermelidir. Hâkimin ret niteliğinde karar vermesi ya da süresi içinde karar vermemesi durumunda çıkarılan kopyalar ve çözümü yapılan metinler derhâl imha edilmesi gerekir. Eğer usulüne uygun imha işlemi gerçekleştirilmezse TCK md. 138'de yer alan verileri yok etmeme suçu gündeme gelecektir⁴¹¹.

CMK md. 134, özel hayatın gizliliği ile doğrudan ilişkilidir. Günümüzde kişiler özel hayatlarına ilişkin pek çok veriyi doğrudan bilişim sistemlerinde muhafaza etmektedirler. Bu anlamda, adli kolluk tarafından CMK md. 134 kapsamında yapılan arama titizlikle sürdürülmelidir. Bilgisayarlarda yapılan arama esnasında suça ilişkin veriden ziyade özel hayata ilişkin veriler de açılabilir. Bu noktada ikili bir ayırım yapılabilir. Özel hayata ilişkin veriler bilerek ve isteyerek açılması durumunda TCK md.134'te yer alan özel hayatın gizliliğine ihlal suçu meydana gelecektir. Ancak, söz konusu verinin suça ilişkin olduğu düşünülerek açılması ancak özel hayata ilişkin veri olduğu ortaya çıkması durumunda ilgili eylem taksirle meydana gelmesi ve TCK md. 134'ün ancak kasten işlenebilmesinden söz konusu suç meydana gelmeyecektir⁴¹².

Yine, kopyalama işlemi esnasında suçla bağlantılı olduğu düşünülmesine rağmen suçla herhangi bir bağlantısı olmayan verilerin kopyalanması durumunda TCK md. 135 ile düzenlenen kişisel verilerin kaydedilmesi suçu oluşabilir⁴¹³. TCK md. 135'in de kasten işlenebilir bir suç olması nedeniyle, suça ait olduğu düşünülerek taksirle yapılan kopyalama işleminde suç oluşmamaktadır.

Bilgisayarlarda bilgisayar programlarında ve kütüklerinde arama kopyalama ve elkoyma koruma tedbiri ile TCK'da yer alan bilişim sistemlerine girme suçu

⁴¹¹ Şahin, s. 281; Ünal, s. 127.

⁴¹² Şahin, s. 281.

⁴¹³ Şahin, s. 282.

arasında yakın bir ilişki bulunmaktadır. CMK md. 134 ile düzenlenen koruma tedbiri bilişim sistemlerine girme suçunun hukuka uygunluk nedenlerinden birisi olarak değerlendirilmektedir. Bu yönüyle CMK md. 134 ile düzenlenmiş sıkı şartlara uyulmaması durumunda hem koruma tedbirinde sınırın aşılmış olması durumu hem de ilgili delilin hukuka aykırı elde edilmiş olması ve hükme esas alınamaması gündeme gelebilecektir⁴¹⁴.

⁴¹⁴ Apiş, s. 80.

SONUÇ

Bilişim sistemlerinde yer alan delillere ilişkin arama, kopyalama ve elkoyma tedbiri klasik arama ve elkoyma tedbirine kıyasla çok daha titizlikle yürütülmesi gerekir. Günümüzde, bilişim sistemlerinde yer alan veriler kişilerin en hassas, en özel verilerinden oluşmaktadır. Bilişim sistemlerine yapılacak müdahale pek çok temel hak ve hürriyetin kısıtlanması anlamına gelmektedir. Çalışma konumuz olan bilişim sistemlerine özgü bu koruma tedbiri, özellikle mülkiyet hakkı ve özel hayatın gizliliği ile yakından ilişkilidir. Dijital delillere ilişkin koruma tedbirinde amaç bilişim sisteminin kendisine elkoymak değil, sayısal veriye elkoymaktır. Bilişim sistemleri, teknolojiyle birlikte hızla gelişmektedir. Bilişim sistemlerine ilişkin özel koruma tedbiri düzenlenmiş olması oldukça yerinde bir uygulama olmakla beraber bazı hususların yeniden ele alınarak düzenlenmesi gerektiği kanaatindeyiz. Çalışmamız sırasında incelediğimiz hususlara ilişkin bazı sonuçlara ulaşılmış bulunuyoruz.

Elektronik delil, dijital delil, sayısal delil, analog delil kavramları birbirinin yerine kullanılmakta ve karıştırılmaktadır. Elektronik delil, dijital delil ve analog delil olarak iki alt başlıkta incelenebilen üst bir kavramdır. Günümüzde; bilişim sistemlerinin dijital veri üzerine inşa edilmesinden ötürü, analog delil kavramı ortadan kaybolmakla beraber dijital delil kavramının kullanımı günden güne artacaktır.

Bilişim sistemlerine özgü koruma tedbiri Ceza Muhakemesi Kanununda, bilgisayar teriminin üzerine inşa edilmiştir. Bilgisayar, bilişim dünyasına giriş kapısı olmakla beraber, etrafımızda bilgisayar ile aynı işlevde pek çok donanım bulunmaktadır. Bu donanımlar, bir nevi bilgisayarın farklı bir formudur. Bu nedenle, bilgisayar daha özgü bir kavram haline gelmiştir. Öte yandan, Türk Ceza Kanunu da dahil olmak üzere, modern dünyada *bilişim sistemi* kavramı yaygın şekilde kullanılmaktadır. Bu bağlamda, CMK md. 134'ün *bilişim sistemi* teriminin üzerine inşa edilmesi hususunun hem terim birliğini sağlayacağını hem de daha kapsayıcı bir ifade olarak teknik açıdan da uygun olacağını değerlendiriyoruz.

CMK md. 134'ün madde metni incelendiğinde, koruma tedbirinin soruşturma evresinde şüpheli hakkında uygulanabileceği görülmektedir. Bu anlamda, söz konusu tedbirin kovuşturma evresinde sanık yönünden uygulanıp uygulanamayacağına ilişkin çalışmamızın ilgili bölümünde, öğretide yer alan tartışmalar ile Yargıtay

uygulamalarına geniş şekilde yer verilmiştir. Bu minvalde, söz konusu belirsizliğin giderilmesi ve koruma tedbirinin kovuşturma evresinde sanık yönünden de uygulanabilmesi için gerekli düzenlemenin yapılması gerektiğine inanıyoruz.

Bilişim sistemlerinde yer alan veriler günümüzde ilgili bilişim sisteminin dahili belleğinin yanında bulut bilişim sistemlerinde de saklandığı bilinmektedir. Bulut bilişim sistemlerinde yapılan veri aramaları sistemlerin niteliği itibarıyla uzak masaüstü bağlantısı ile gerçekleştirilebilmektedir. Mevcut düzenleme, daha çok yerinde arama sistemi üzerine inşa edilmiştir. Bu bağlamda, bulut bilişim sistemlerine özgü düzenleme yapılmasının uygun olacağını değerlendiriyoruz.

CMK md. 134'ün madde metninde yer alan yedekleme işleminin nasıl uygulanacağına dair usuller belirsizdir. Adli kolluk, genellikle tedbiri uygularken veri bütünlüğünü koruduğunu göstermek amaçlı, verinin imajını alarak hash değerini çıkarmakta ve yapılan işlemi tutanak altına almaktadır. Bu durum hem kolluğu hem de şüpheliyi korumaktadır. Kanaatimizce, söz konusu usulün işletilmesi kolluğun iradesine bırakılmamalı, gerekli düzenleme ile zorunluluk haline getirilmelidir.

CMK md. 134 kapsamında bilişim sistemlerine elkoyma, istisnai hallerde yerine getirilebilen bir tedbirdir. Kanun koyucu bu anlamda elkoyma şartlarından birisi olarak *işlemin uzun sürecektir* kriter olarak belirlemiştir. Ancak bu şart oldukça subjektif bir kriter olup yasanın arkasında dolaşmaya elverişlidir. İşlemin uzun sürmesi durumunun kime ve neye göre olduğu konusunda açıklık bulunmamaktadır. Bu nedenle, çoğu zaman kolluk tarafından işlemin uzun sürdüğüne ve sistemin hata verdiğine ilişkin tutanak tutularak doğrudan elkoyma işlemi yapılmaktadır. Bu bağlamda, söz konusu kriterin daha objektif açıdan ele alınarak düzenlenmesi gerektiğini kıymetlendiriyoruz.

CMK md. 134 kapsamında tedbire karar verilmesi için gerekli bir kriter de *“son çare”* olarak bilinen *başka bir suretle delil elde etme imkanının olmamasıdır*. Bahse konu kriter ilgili kısımda detaylı açıklandığı üzere tartışmalıdır. Somut olayda başka suretle delil elde edilemeyeceği objektif olarak belirlenebilirse doğrudan CMK md. 134'te yer alan tedbire başvurulabileceği kanaatindeyiz.

Söz konusu tedbirde ilgili dijital delilin metin haline çevrilmesine yönelik hüküm bulunmaktadır. Suça konu veri sadece bir resim, ufak bir metin gibi birkaç sayfaya basılacak kadar kısa ise bu tedbir anlamlı hale gelmektedir. Ancak bahse konu

veri sayfalar dolusu dokümandan oluşuyorsa bu hükmün uygulanabilirliği kalmamaktadır.

Çalışmamıza konu koruma tedbirine ilişkin bir eleştirimiz, tedbirin sonunda elde kalan verilerin ne yapılacağı hususunda yasal düzenlemenin bulunmamasıdır. Uygulamada konuya çeşitli çözümler getirilmeye çalışılsa da kişilerin yedeklenen ya da el konulan dijital verilerinin tedbir sonunda ne yapılacağına ilişkin bir düzenleme yapılması uygun olacaktır.

Adli ve önleme aramaları yönetmeliğinde bilişim sistemlerine yönelik uzaktan arama yapılabilmesine imkân veren hüküm bulunmaktadır. Kanunda ise böyle bir düzenleme yoktur. Bu anlamda, kanun ile yönetmelik hükümlerinin uyumlu hale getirilmesinin uygun olacağı kanaatindeyiz.

Bilişim sistemleri, teknolojinin gelişmesi ile gittikçe uzmanlık gerektiren bir alan olmuştur. Bu sistemlerin kullanılmasıyla işlenen suçların aydınlatılması da aynı şekilde uzmanlık gerektirmektedir. Bu anlamda, suça ilişkin kovuşturmanın yürütüleceği özel ihtisaslı bilişim mahkemelerinin kurulmasının suçların aydınlatılmasına önemli katkı sağlayacağı kanaatindeyiz.

KAYNAKÇA

KİTAP

Akpek, Ayça. **Tutuklamada Kuvvetli Suç Şüphesi**, Seçkin Yayıncılık, Ankara, 2020.

Aldemir, Hüsnü. **Adli Önleme Arama ve Elkoyma**, 2. Baskı, Seçkin Yayınevi, Ankara, 2018.

Antonopoulos, Nick ve Lee Gillam. **Cloud Computing**, 2. Baskı, Springer, Swindon UK, 2011.

Arıcı, Haydar Yener. **Adli Bilişim**, Seçkin Yayıncılık, Ankara, 2018.

Aydoğdu, Şeyhmus, Kadir Aba, Mehmet Kırtay, Gökçe Becit İşçitürk, Yıldız Özaydın ve Ozan Coşkunserçe. **Bilgisayara Giriş**, Pegem Akademi Yayıncılık, Ankara, 2017.

Çakır, Hüseyin ve Merhmet Serkan Kılıç. **Adli Bilişim ve Elektronik Deliller**, Seçkin Yayıncılık, Ankara, 2014.

Centel, Nur ve Hamide Zafer. **Ceza Muhakemesi Hukuku**, Beta Basımevi, İstanbul, 2018.

Dandamudi, Sivarama P. **Fundamentals of Computer Organization and Design**, Springer New York, 2013.

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

Döngel, Ali. **Bilgisayar Donanımı ve Elektronik**, 2. Baskı, Tuna Matbaacılık, Ankara, 2012.

Dölger, Murat Volkan. **Bilişim Suçları ve İnternet İletişim Hukuku**, 8. Baskı, Seçkin Yayınevi, Ankara, 2020.

Emmungil, Levent. **Bilgisayar Donanımı**, Ankara, 2010.

Erdem, Mustafa Ruhan ve Candide Şentürk. **Ceza Muhakemesinde Kanun Yolları**, Seçkin Yayınevi, Ankara, 2018.

Erdem, Mustafa Ruhan, Durmuş Tezcan ve Bahri Öztürk. **Dijital Ceza Muhakemesi Hukuku**, Seçkin Yayıncılık, Ankara, 2022.

Erdoğan, Yavuz. **Türk Ceza Kanununda Bilişim Suçları**, Legal Yayınevi, İstanbul, 2012.

Eryılmaz, Mesut Bedri. **Ceza Muhakemesi Hukuku Dersleri**, Seçkin Yayınevi, Ankara, 2012.

Göçmen, Özen Kaya. **Yakalama ve Gözaltı Koruma Tedbirleri**, Seçkin Yayıncılık, Ankara, 2021.

Gökçen, Ahmet, Murat Balcı, M. Emin Alşahin ve Kerim Çakır. **Ceza Muhakemesi Hukuku**, 5. Baskı, Adalet Yayınevi, Ankara, 2021.

Göksoy, Resul. **Ceza Muhakemesinde Dijital Delillerin Elde Edilmesi ve Güvenilirliğinin Sağlanması**, Seçkin Yayıncılık, Ankara, 2019.

Gözler, Kemal. **Türk Anayasa Hukuku Dersleri**, 15. Baskı, Ekin Yayınevi, Bursa, 2015.

Henkoğlu, Türkay. **Adli Bilişim**, 2. Baskı, Pusula 20 Teknoloji ve Yayıncılık, İstanbul, 2014.

Karagülmez, Ali. **Bilişim Suçları ve Soruşturma Kovuşturma Evreleri**, 5. Baskı, Seçkin Yayıncılık, Ankara, 2014.

Korkmaz, Muzaffer. **Koruma Tedbirleri Nedeniyle Tazminat Davaları**, Seçkin Yayıncılık, Ankara, 2019.

Messmer, Hans-Peter. **The Indispensable PC Hardware Book**, 4. Baskı, Pearson Education, Great Britain, 2002.

Özbek, Veli Özer, Koray Doğan ve Pınar Bacaksız. **Ceza Muhakemesi Hukuku**, 13. Baskı, Seçkin Yayıncılık, Ankara, 2020.

Özçatalbaş, Orhan, Gamze Döğerlioğlu ve Hasan Özmen. **Bilgisayar**, Ekin Yayınevi, Ankara, 2008.

Özgüler, Mehmet. **Bilgisayar Donanımı**, 3. Baskı, Akademi Yayınevi, Rize, 2007.

Öztürk, Bahri, Behiye Eker Kazancı ve Sesim Soyer Güleç. **Ceza Muhakemesi Hukukunda Koruma Tedbirleri**, 4. Baskı, Seçkin Yayıncılık, Ankara, 2021.

Öztürk, Bahri, Durmuş Tezcan, Mustafa Ruhan Erdem, Özge Sırma Gezer, Yasemin Saygılar Kırıt, Efser Erden Tütüncü, Özdem Özaydın, Derya Altınok Villemin ve Mehmet Can Tok. **Ceza Muhakemesi Hukuku**, 8. Baskı, Seçkin Yayınevi, Ankara, 2021.

Şahin, Cumhur ve Neslihan Göktürk. **Ceza Muhakemesi Hukuku-1**, 11. Baskı, Seçkin Yayıncılık, Ankara, 2021.

Şahin, Cumhur ve Neslihan Göktürk. **Ceza Muhakemesi Hukuku-2**, 12. Baskı, Seçkin Yayıncılık, Ankara, 2022.

Scott, Mueller. **Upgrading and Repairing PCs**, 15. Baskı, Que, Indiana, 2004.

Şen, Ersan ve H. Sefa Eryıldız. **Elkoyma**, Seçkin Yayıncılık, Ankara, 2017.

Ünver, Yener ve Hakan Hakeri. **Ceza Muhakemesi Hukuku**, 15. Baskı, Seçkin Yayıncılık, Ankara, 2019.

Yaşar, Osman ve Cengiz Otacı. **Ceza Muhakemesi Kanunu (2 Cilt)**, 10. Baskı, Seçkin Yayınevi, Ankara, 2022.

Yayla, Mehmet. **Ceza Muhakemesi Hukukunda İspat ve Şüphe**, Seçkin Yayıncılık, Ankara, 2016.

Yazıcıoğlu, Yılmaz. **Bilgisayar Suçları**, Alfa Basım Yayın Dağıtım, Bursa, 1997.

Yenisey, Feridun ve Ayşe Nuhoğlu. **Ceza Muhakemesi Hukuku**, 8. Baskı, Seçkin Yayıncılık, Ankara, 2020.

Yıldırım, Metin. **Genel ve Özel Ceza Soruşturması**, 2. Baskı, Adalet Yayınevi, Ankara, 2020.

MAKALE

Akın, Gülfer. “Belgede Sahtecilik Suçlarının Konusu Olarak Elektronik/Dijital Belge”, **Bilişim Hukuku Dergisi**, Cilt:3, Sayı: 1, 2021, ss. 76–138.

Aktaş, Batuhan. “Bilgisayarlarda, Bilgisayar Programlarında Ve Kütüklerinde Arama, Kopyalama ve Elkoyma Tedbiri Üzerine Bir İnceleme”, **Yeditepe Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 14, Sayı: 2, 2017, ss. 211–239.

Apiş, Özge. “Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Koruma Tedbiri”, **Yasama Dergisi**, Cilt:13, Sayı: 37, 2018, ss. 49–86.

Araalan, Cemal. “Digital Evidence in Turkish Law Türk Hukukunda Dijital Deliller”, **GSI Articleletter**, Cilt: 203, 2015, ss. 203–212.

Arslan, Çetin. “Dijital Delil ve İletişimin Denetlenmesi”, **Ceza Hukuku ve Kriminoloji Dergisi**, Cilt: 3, Sayı: 2, 2015, ss. 253–266.

Başlar, Yusuf. “Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri”, **Uyuşmazlık Mahkemesi Dergisi**, Cilt: 0, Sayı: 3, 2013, ss. 82–105.

Başlar, Yusuf. “Elektronik Delilin Toplanması ve Muhafazası”, **Hacettepe Hukuk Dergisi**, Cilt: 10, Sayı: 1, 2020, ss. 77–107.

Baştürk, İhsan. “Bilgisayar Sistemleri ile Verilerinde Arama, kopyalama ve Elkoyma”, **Fasikül Hukuk Dergisi**, Cilt: 2, Sayı: 9, 2010, ss. 23–32.

Burrows, Robyn. “Judicial Confusion And The Digital Drug Dog Sniff: Pragmatic Solutions Permitting Warrantless Hashing Of Known Illegal Files”, **George Mason Law Review**, Cilt: 19, Sayı: 1, 2011, ss. 255–290.

Çekiç, Burak. “Bilgisayar Verilerinde Arama, Kopyalama, Elkoyma Tedbirinin Hukuki Niteliği ve Benzer Kavramlar”, **Tekirdağ Namık Kemal Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 2021, Sayı: 1, 2021, ss. 153–185.

Değirmenci, Olgun. “Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbirinde (CMK m. 134), 7145 Sayılı Kanunla Yapılan Değişikliklerin Değerlendirilmesi”, **Terazi Hukuk Dergisi**, Cilt: 13, Sayı: 147, 2018, ss. 146–155.

Dereboylular, Özde. “Bulut Bilişim Bakımından Arama ve Elkoymaya İlişkin Hükümlerin Uygulanabilirliği”, **Ceza Hukuku Dergisi**, Cilt: 14, Sayı: 39, 2019, ss. 161–202.

Duran, Gökhan Yaşar. “Ceza Muhakemesi Kanunu’nda (CMK) Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma (CMK m.134)”, **Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 14, Sayı: 173, 2019, ss. 173–241.

Epözdemir, Rezan. “Bilişim Sistemlerinde Arama ve Elkoyma Tedbirleri”, **Terazi Hukuk Dergisi**, Cilt: 13, Sayı: 142, 2018, ss. 88–98.

Feyzioğlu, Metin. “Yasama Dokunulmazlığı”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: 42, Sayı: 1, 1991, ss. 22–45.

Gürel, Begüm ve İpek Mengilli. “Dijital Delil Kavramı ve Yargılamadaki Yeri”, **Leges Hukuk Dergisi**, Sayı: 139, 2021, ss. 78–108.

İşman, Aytekin. “Bilgisayarlar ve Eğitim”, **Sakarya Üniversitesi Eğitim Fakültesi Dergisi**, Cilt: 0, Sayı:2, 2001, ss. 1–34.

Karaca, Muhammet ve Ensar GÜL. “Kritik Altyapılara Yönelik Bilişim Suçları, Türkiye ve AB Uygulamaları”, **Bilişim Hukuku Dergisi**, Cilt: 3, Sayı: 1, 2021, ss. 1–30.

Keskin, Salih. “Bilişim Suçlarında Ceza Muhakemesi Kanununun 134. Maddesindeki Hükümlerin Uygulanmasında Yaşanan Aksaklıklar”, **Kırıkkale Üniversitesi Sosyal Bilimler Dergisi**, Cilt: 11, Sayı: 2, 2021, ss. 649–667.

Kılıç, Mehmet Serkan. “Elektronik Delillerin Hukuken Geçerliliği Açısından İlk Müdahalenin Önemine İlişkin Bir İnceleme”, **Terazi Hukuk Dergisi**, Cilt: 10, Sayı: 102, 2015, ss. 34–41.

Ölmez, Aslan. “Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Kopyalama ve Bunlara Elkoyma”, **Terazi Hukuk Dergisi**, Cilt: 4, Sayı: 30, 2009, ss. 40–52.

Özbek, Murat. “Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları”, **1st International Symposium on Digital Forensics and Security**, Elazığ, 2013, ss. 1-7.

Özen, Muharrem ve Gürkan Özocak. “Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)”, **Ankara Barosu Dergisi**, Cilt: 73, Sayı: 1, 2015, ss. 41–77.

Özkul, Davut. “Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi”, **Sayıştay Dergisi**, Cilt: 13, Sayı: 44, 2002, ss. 11–34.

Sümer, Seda Yağmur. “Ceza Muhakemesinde Mobil Telefona/Akıllı Telefona Elkoyma ve Müdahale İmkanları”, **İzmir Barosu Dergisi**, Cilt: 0, Sayı: 1, 2022, ss. 61–119.

Şahin, Cumhuri. “Ceza Muhakemesinde Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma”, **Yaşar Hukuk Dergisi**, Cilt: 1, Sayı: 2, 2019, ss. 271–286.

Sarsıkoğlu, Şenel. “Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı”, **Türkiye Adalet Akademisi Dergisi**, Cilt: 0 Sayı: 22, 2015, ss. 507–534.

Şen, Ersan. “Avukat, Hakim ve Savcıların Aranması”, **Ankara Barosu Dergisi**, Cilt: 0, Sayı: 2, 2013, ss. 333–343.

Şirikçi, Ahmet Serhat ve Nergis Cantürk. “Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi”, **Bilişim Teknolojileri Dergisi**, Cilt: 5, Sayı: 3, 2012, ss. 29–34.

Taşçı, Ufuk ve Ali Can. “Türkiye’de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014”, **Fırat Üniversitesi Sosyal Bilimler Dergisi**, Cilt: 25, Sayı: 2, 2015, ss. 229–248.

Thach, Liz. “Using Electronic Mail to Conduct Survey Research”, **Educational Technology**, Cilt: 35, Sayı: 2, 1995, ss. 27–31.

Uğraş, Dilek Özge. “Bilgisayarlarda, Bilgisayar Programlarında ve Bilgisayar Kütüklerinde Arama, Kopyalama ve Elkoyma”, **Türkiye Barolar Birliği Dergisi**, Cilt: 34, Sayı: 154, 2021, ss. 97–134.

Yaşar, Yusuf ve İsmail Dursun. “Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri”, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, Cilt: 19, Sayı: 3, 2013, ss. 3–34.

TEZ

Kaynakçıoğlu, Uğur. **Ceza Muhakemesinde Dijital Deliller**, (Yayınlanmamış Yüksek Lisans Tezi), Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2015.

Parlak, Oğuzhan Emre. **Türk Ceza Muhakemesinde Bilişim Sistemlerinde Arama, Kopyalama ve Elkoyma**, (Yayınlanmamış Yüksek Lisans Tezi), Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 2019.

Tanrıkulu, Cengiz. **Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma**, (Yayınlanmamış Doktora Tezi), Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2014.

Ünal, Osman Gazi. **Bilgisayarlarda, Bilgisayar Programlarında Ve Kütüklerinde Arama, Kopyalama ve Elkoyma**, (Yayınlanmamış Yüksek Lisans Tezi), Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara, 2011.

İNTERNET KAYNAKLARI

T.C. Anayasa Mahkemesi Kararlar Bilgi Bankası,
<https://kararlarbilgibankasi.anayasa.gov.tr/>, (20.02.2022)

AİHM Resmî Sitesi, <https://hudoc.echr.coe.int/>, (11.04.2022)

Horsman, Graeme. “ACPO principles for digital evidence: Time for an update?”, Forensic Science International: Reports, Cilt: 2, Sayı: 100076, 2020, ss. 1-6.
“Hukuk Türk”, <https://www.hukukturk.com/> (13.06.2022).

Williams, Janet. “ACPO Good Practice Guide for Digital Evidence”, 2011, ACPO, Association of Chief Police Officers, https://www.npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence_Vers%205_Oct%202011_Website.pdf, (03.10.2022).

Türk Dil Kurumu Sözlüğü, <https://sozluk.gov.tr/>, (03.10.2022).

Türkoğlu, İbrahim. BİL391 İşletim Sistemleri (Ders Notları), 2006, <http://eng.harran.edu.tr/~nbesli/OS/book1.pdf>, (03.10.2022)

U.S. Secret Service. “Best practices for seizing electronic evidence v.4.2”, 2007, <https://www.cwagweb.org/wpcontent/uploads/2018/05/BestPracticesforSeizingElectronicEvidence.pdf>, (15.11.2021)

European Union. “Electronic Evidence Guide a Basic Guide for Police Officers, Prosecutors and Judges V.2”, Cybercrime Division - Directorate General of Human Rights and Rule of Law, 2014, https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf, (22.03.2022)

Yargıtay Karar Arama, <https://karararama.yargitay.gov.tr/>, (20.02.2022)