

T.C.

İSTANBUL KÜLTÜR ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

CEZA MUHALEMESİNDE DİJİTAL DELİLLERİN İSPAT GÜCÜ

YÜKSEK LİSANS TEZİ
AYŞENUR KAYA
1600002450

Anabilim Dalı: KAMU HUKUKU
Programı: KAMU HUKUKU

Tez Danışmanı: Dr. Öğr. Üyesi Yasemin Filiz SAYGILAR

EKİM 2023

T.C.

İSTANBUL KÜLTÜR ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

CEZA MUHAKEMESİNDE DİJİTAL DELİLLERİN İSPAT GÜCÜ

YÜKSEK LİSANS TEZİ
AYŞENUR KAYA
1600002450

Anabilim Dalı: KAMU HUKUKU

Programı: KAMU HUKUKU

Tez Danışmanı: Dr. Öğr. Üyesi Yasemin Filiz SAYGILAR

Jüri Üyeleri:

Dr. Öğr. Üyesi Ezgi CANKURT

Dr. Öğr. Üyesi Özdem ÖZAYDIN

EKİM 2023

ÖNSÖZ

Teknolojinin gelişmesiyle birlikte hayatımızın her alanı dijitalleşmeye başlamıştır. Dijital aygıtların artan kullanımı, ceza hukukuna da etki etmiştir. Klasik olay yeri kavramı yerini, bilişim cihazlarının içerisindeki depolama alanlarına bırakmıştır. Bilişim cihazları suç işlemekte, suç unsurlarını depolamakta kullanılmaya başlamıştır. Bu durum, bilişim aygıtları kullanılarak işlenen suçlarla mücadele için önlemlerin alınması gereğini doğurmuştur. Bilişim Hukuku ve Ceza Muhakemesi hukukunun ortak kesişimi olan dijital deliller bu açıdan oldukça önemlidir.

Çalışmanın konusunu “Ceza Muhakemesinde Dijital Delillerin İspat Gücü” oluşturmaktadır. Bu çalışmada, klasik delillerin aksine farklı prosedür ve değerlendirme biçimleri olan dijital delillere ilişkin, araştırma yaparak farklı yönlerinin ortaya koyulması amaçlanmıştır.

Öncelikle, araştırma ve yazım sürecimde yardımlarını benden esirgemeyen danışmanım Dr. Öğr. Üyesi Yasemin Filiz Saygılar’a teşekkür ederim. Çalışmanın biçim almasında emekleri çok değerli.

Yazım sürecinde hep yanımda olan, bana konforlu bir ortam sağlayan, desteklerini her daim sürdüren aileme ayrıca teşekkür ederim.

Değerli fikirleriyle esere katkıda bulunan, beni her zaman destekleyip yanımda duran, yol arkadaşım Av. Osman Talha Yıldız’a da ayrıca teşekkür ederim.

Ayşenur KAYA

05.10.2023

İÇİNDEKİLER

ÖNSÖZ	i
İÇİNDEKİLER	ii
SİMGELER ve KISALTMALAR	vi
ÖZET	viii
ABSTRACT	ix
GİRİŞ	1

BİRİNCİ BÖLÜM

CEZA MUHALEMESİNDE İSPAT ARACI OLARAK DELİLLER

I. Genel Olarak	2
II. Delillerin Özellikleri	3
III. Delillerin Sınıflandırması	5
A. Beyan Delilleri	6
1. Şüpheli-Sanık Açıklamaları	6
a. İkrar	7
2. Tanık Açıklamaları	9
a. Tanıklıktan Çekinme	9
b. Tanıklara Yemin Verilmesi	10
c. Devlet Sırrı İçeren Bilgiler Hakkında Tanıklık	11
d. Tanıkların Dinlenmesi	11
e. Gizli Tanıklık ve Savunma Hakkı	12
f. Tanık Beyanının Delil Değeri	13
B. Belgeler	14
1. Yazılı Belge	14
2. Şekil Tespit Eden Belgeler	15
3. Ses ve Görüntü Tespit Eden Belgeler	15
4. Dijital Deliller	16

C.	Belirtiler	16
----	------------------	----

İKİNCİ BÖLÜM

DİJİTAL DELİLLER

I.	Genel Olarak	17
II.	Dijital Delillerin Deliller İçerisindeki Yeri	19
III.	Dijital Delillerin Kendine Özgü Özellikleri	20
IV.	Dijital Delillerin Elde Edilmesi ve Muhafazası	21
A.	Dijital Delillerin Bulunacağı Ortamlar	21
1.	Bilgisayarlar	21
2.	Veri Depolama Araçları	22
3.	Cep Telefonları ve SIM Kartı	23
4.	Bilgisayar Ağı	24
5.	Elektronik Posta İletileri	25
6.	Sosyal Medya	26
7.	Bulut Bilişim Sistemleri	27
B.	Dijital Delillerin Elde Edilme Aşamaları ve Adli Bilişim	27
1.	Dijital Verilerin Toplanması	28
2.	Arama Yapılması	31
a.	Yerinde Arama	31
b.	Off-site Arama	33
c.	Uzaktan Arama	34
d.	Bulutta Arama	35
3.	Elde Edilen Delillerin Muhafazası ve Taşınması	36
4.	Delillerin İncelenmesi Aşaması	36
5.	Çözümleme (Analiz) Aşaması	38
6.	Raporlama Aşaması	39
V.	Türk Hukukunda Dijital Delillerin Elde Edilmesi	40
A.	CMK m.134 Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma	40
1.	Genel Olarak	40
2.	Amaç	41
3.	Kapsam	41
4.	Somut Delillere Dayanan Kuvvetli Suç Şüphesinin Varlığı	43
5.	Başka Suretle Delil Elde Etmenin Mümkün Olmaması	45

6.	CMK m. 134'teki Aramanın Uygulanma Şartları	46
7.	İmaj Alma	48
8.	Elkoyma	50
9.	Arama Kararını Verecek Mercii	53
10.	İtiraz	53
B.	İletişimin Tespiti, Dinlenmesi ve Kayda Alınması	54
C.	Cumhuriyet Savcısının Genel Yetkisi	55
VI.	Avrupa Konseyi Siber Suç Sözleşmesinde Arama ve Elkoyma	55
VII.	Dijital Delillerin Elde Edilmesinin Bazı Temel Hak ve Özgürlüklerle	
İlişkisi		57
A.	Genel Olarak	57
B.	Özel Hayatın Gizliliği ile İlgisi	57
C.	Kişisel Verilerin Korunması ile İlişkisi	60
1.	Sosyal Medya ve Kişisel Veriler	61
D.	Haberleşme Hürriyeti	62
E.	İfade Özgürlüğü ile İlişkisi	63

ÜÇÜNCÜ BÖLÜM

DİJİTAL DELİLLERİN İSPAT GÜCÜ

I.	Genel Olarak	65
II.	Dijital Delillerin Kabul Edilebilirlik Şartları	65
A.	Sahihlik	66
B.	Dijital Delillerin Bütünlüğü	66
A.	Tekrar Ele Alınabilirlik	67
B.	Dijital Delillerin Doğrulanması	68
III.	Dijital Delillerin Doğrudanlık Problemi	69
A.	Ekran Görüntüsü	71
IV.	Delil Türleri Bakımından İspat	72
B.	Dijital Delillerin Güvenilirliğinin Sağlanması	73
1.	Hash Değeri	73
2.	Üst Veri Bilgisi	74
3.	Elektronik İmza	75
4.	Delil Zinciri	75
V.	Dijital Deliller ile Tek Başına Mahkûmiyet Kararı Verilebilme	76
VI.	Hukuka Aykırı Deliller	77
A.	Zehirli Ağacın Meyvesi Doktrini ve Dijital Deliller	78
VII.	Tesadüfen Elde Edilen Deliller	80

SONUÇ	82
KAYNAKÇA.....	85



SİMGELER ve KISALTMALAR

ADN : Advanced Digital Network

a.g.e : Adı Geçen Eser

AİHM: Avrupa İnsan Hakları Mahkemesi

AİHS: Avrupa İnsan Hakları Sözleşmesi

AY: Anayasa

AYM: Anayasa Mahkemesi

Bkz.: Bakınız

CD: Compact Disk

CD: Ceza Dairesi

CDN: Content Delivery Network

CMK: Ceza Muhakemesi Kanunu

DNA: Deoksiribo Nükleik Asit

DM: Direct Message

DVD: Digital Versatile Disk

E.: Esas

E.T.: Erişim Tarihi

GPS: Global Positioning System

HMK: Hukuk Muhakemeleri Kanunu

HTML: Hiper Metin İşaretleme Dili

IP: Internet Protocol Address

Jpeg: Joint Photographic Experts Group

K.: Karar

m.: Madde

Md: Madde

MİB: Merkezi İşlem Birimi

MOBESE: Mobil Elektronik Sistem Entegrasyonu

No: Numara

PDF: Portable Document Format

PGP: Pretty Good Privacy

PVSK: Polis Vazife ve Salahiyet Kanunu

RAM: Random Access Memory

RG: Resmi Gazete

ROM: Read Only Memory

S: sayfa

SBE: Sosyal Bilimler Enstitüsü

SMS: Short Message Service

URL: Uniform Resource Locator

USB: Universal Serial Bus

V.: ve

Vb.: Ve Benzeri

Vol: Volume

Yar.: Yargıtay

YKD: Yargıtay Kararları Dergisi

ÖZET

Çalışmamızın konusu, klasik deliller ile karşılaştırıldığında daha yeni bir delil türü olan dijital delillerdir. Dijital delillerin kendilerine has yapıları sebebiyle, bu delillerin elde edilışinden mahkeme önüne getirilmesine kadar olan sürecin ayrıntılı bir şekilde incelenmesi gerekmektedir. Dijital delillerin adli bilişim süreci, uzmanlık gerektiren bir alandır. Bu sürecin titizlik ile yürütölmesi muhakeme açısından büyük öneme sahiptir. Konunun adli bilişimle ilgili kısmını sınırlı tutmaya çalışarak, ceza muhakemesi hukuku açısından gerekli olan kısımlarını çalışmamızda ortaya koymayı hedefledik. Türk hukukunda dijital delillerin elde edilmesine yönelik mahallinde ve mahallinden uzakta aramayı kapsayan CMK m.134 hükmü çalışmamızın önemli bir kısmıdır. CMK m.134, Bilgisayar, Bilgisayar Programları ve Kütüklerinde Arama, Kopyalama ve Elkoyma, özel bir arama ve elkoyma türüdür. Bu tedbirin önemi, dijital delillerin elde edilmesinde arama ve elkoymanın usul hükümlerini ortaya koymasındır. Tedbir, temel hak ve özgürlükleri ihlal etmeyecek şekilde delillerinin elde edilmesini amaçlamaktadır. Dijital delillerin elde edileceğı bilişim cihazına, şifrenin çözölmemesinden dolayı girilememesi, gizlenmiş bilgilere ulaşılammaması veya işlemin süresinin uzun süreceğ olması hallerinde, bilişim cihazlarına elkonulabileceğdir. Dijital deliller, adli bilişim ile bağlantılı bir elde edilme sürecine tabidir bu sebepten, adli bilişime dair hususlar yeterince bilinmediğı takdirde bu durum uygulamada eksikliklere yol açabileceğdir. Adli bilişim sürecinden geçen dijital delillerin muhakemeye esas alınması için gerekli şartlar, bu delillerin tek başına mahkumiyet için yeterli olup olamayacağı, hukuka aykırı ve tesadüfen elde edilen delillerin durumu ispat kısmında açıklanacaktır. Çalışmamızın gerek teorik gerekse uygulama açısından fayda sağlamasını temenni ediyoruz.

ABSTRACT

The subject of our study is digital evidence, which is a newer type of evidence compared to classical evidence. Due to the unique nature of digital evidence, it is necessary to examine the process from the acquisition of this evidence until it is brought before the court in detail. The forensic informatics process of digital evidence is an area that requires expertise. The meticulous execution of this process is of great importance for the judgment. By trying to limit the part of the subject related to forensic informatics, we aimed to reveal the parts that are necessary in terms of criminal procedure law in our study. The provision of Article 134 of the Criminal Procedure Code, which covers on-site and remote searches for obtaining digital evidence in Turkish law, is an important part of our study. Article 134, Search, Copying and Seizure of Computers, Computer Programs and Logs, is a special type of search and seizure. This measure is important because it sets out the procedural provisions of search and seizure in obtaining digital evidence. The measure aims to bring evidence in a manner that does not violate fundamental rights and freedoms. Information devices may be seized in cases where the information device from which the digital evidence is to be obtained cannot be accessed due to the inability to decrypt the password, the concealed information cannot be accessed, or the process will take a long time. Digital evidence is subject to a process of acquisition in connection with forensic informatics; therefore, issues related to forensic informatics. If not sufficiently known, this situation may lead to deficiencies in practice. The conditions necessary for digital evidence that has gone through the forensic informatics process to be taken as a basis for the judgment, whether this evidence alone can be sufficient for conviction, and the status of evidence obtained illegally and incidentally will be explained in the proof section. We hope that our study will be beneficial both in terms of theory and practice.

GİRİŞ

Dijital deliller, dijitalleşmeyle birlikte ceza muhakemesine giren bir terimdir. Hayatlarımızın dijitalleşmesiyle birlikte, suçlar da dijitalleşmektedir. Dijital alanlarda, dijital cihazlar ile işlenen suçların sayısı azımsanmayacak kadar çoktur. Bu tür suçlarla mücadelede, klasik koruma tedbirleri yetersiz kalabilmekte, sonuca ulaştırmada başarılı olamamaktadır.

Eserde, dijital delillerin adli bilişim aşamaları, koruma tedbirleri ile ilişkisi, temel hak ve özgürlüklere etkisi ve ispat açısından durumu ele alınacaktır. Dijital delillerin kendine has yapısı ve tahrif olmaya elverişli olması sebebiyle bu delillerin elde edilışinden, şüpheli ya da sanığa iadesine kadar olan süreçte çok dikkatli bir şekilde muhafaza edilmelidir. Aksi takdirde, bu delillerin sahihliğinde şüphe oluşabilir, bu durum da delillerin muhakemede kullanılamamasına sebebiyet verebilmektedir. Bu tür problemlerin önüne geçebilmek için, adli bilişim uzmanlarının eğitimini almış kişilerden seçilmesi, bu aşamaları dikkatli bir şekilde yürütmeleri oldukça elzemdir.

Özel bir arama ve elkoyma türü olan CMK m.134 hükmü, Türk hukukunda dijital delillerin elde edilmesinde kullanılan başlıca tedbirlerdendir. Bu maddenin doğru bir şekilde anlaşılması ve uygulanması, temel hak ve özgürlükler açısından oldukça önemlidir. Bilişim cihazları içerisinde kişisel veriler ve özel hayata ilişkin bilgiler barındırmaktadır, tedbirin bu haklara zarar vermeden uygulanması gerekmektedir. Dijital deliller ile tek başına mahkumiyet kararı verilip verilemeyeceğinin tartışılması bu delillerin ispat değerin belirlenmesi açısından gereklidir.

BİRİNCİ BÖLÜM

CEZA MUHAKEMESİNDE İSPAT ARACI OLARAK DELİLLER

I.Genel Olarak

Ceza muhakemesinde, esas olarak, fiilin fail tarafından işlendiği veya işlenmediği konusunda, hukuk düzenince kabul edilen vasıtalarla yargılama makamının tam bir kanaate ulaşmasını sağlama çabasına *ispat* denir.¹ Ceza muhakemesinde deliller ispat vasıtalarıdır. Hakimin yargılama sırasında kanaatinin oluşmasında deliller, önemli bir yere sahiptir. Ceza yargılamasında hâkim olaya tanık olmamıştır; geçmişte olmuş bir olayı bugünün kaynakları yani deliller ile çözmeye çalışmaktadır. Deliller, olayı tekrardan kurgulayarak hakimin olay hakkında fikir sahibi olmasına yardımcı olurlar.

Ceza muhakemesinde benimsenen delil sitemi, vicdani delil sistemidir. Vicdani delil sistemi, hâkimin vicdani kanaatine göre delilleri değerlendirip karar vermesidir. Delillerin toplanmasından sonra olay ile bağlantısını ve karar üzerindeki etkisini belirlemek hakimin kanaatindedir. Vicdani delil sistemi, delil serbestliği ve delillerin serbestçe değerlendirilmesi ilkelerini kapsar. Ceza yargılamasında her şeyin delil olabilmesi anlamına gelen delil serbestliğine göre, maddi olay her tür delil ile ispatlanabilir. HMK'daki sadece belirli delillerin kesin delil sayılacağına ilişkin kural, ceza muhakemesi bakımından geçerli değildir, Ceza Muhakemesi Kanunu bu konuda bir sınırlandırma yapmamıştır.

¹ Bahri Öztürk, Durmuş Tezcan, Mustafa Ruhan Erdem, Özge Sırma Gezer, Yasemin F. Saygılar, Esra Alan , Özdem Özaydın, Efser Erden Tütüncü Derya Altınok Vıllemın ve Mehmet Can Tok, *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku*. (Ankara: Seçkin Yayıncılık, 2022) s.298.

Ceza hukukunun amacı insan haklarını gözeterek maddi gerçeğe, hakikate ulaşma faaliyetidir. Delil serbestisinden önce benimsenen kanuni delil sistemi ile, delillerin serbestisi kısıtlanmış, ceza hukukunun öncelikli amacını yerine getirilememesi sonucunu doğurmuştur. Kanuni delil sistemi yalnızca kanunun öngördüğü deliller ile somut olayın ispat edilebileceğini ifade etmekteydi, bu sebeptendir ki sistem, maddi gerçeğin ortaya çıkması bakımından yetersiz kalmıştır. Bu eksikliğin giderilmesi için delil serbestliği ilkesi kabul edilmiştir.

Delillerin serbestçe değerlendirilmesi ilkesi ise, hakimın delilleri değerlendirirken bağımsız olmasını ifade eder. Ceza muhakemesinde hiçbir şey kesin delil değildir, kesinlik değerlendirmesini hakim belirler. Bilirkişi raporları, kan izi gibi bilimsel deliller dahi hakimın kararını sınırlamaz ve bağlamaz, hakim bunları olayla birlikte değerlendirerek karar verir. Bu serbestlikler hakimın keyfî hareket edebileceği manasına gelmez. Hakim hangi delile dayanarak karar verdiğini kararda belirtmelidir.

Tüm bu açıklanan ilkelerden hareketle söylenebilir ki; delillerin değerini önceden belirlemek mümkün değildir, bu sebepten kanun koyucu delillere değer biçmemiş, bu görev hakime bırakılmıştır.² Somut olaya göre değerlendirmenin muhakemenin yürüyüşü bakımından daha güvenilir olduğundan hareketle delillere önceden ispat değeri yüklenmemiş ve bu değeri hakimın belirlemesi kabul edilmiştir.

II.Delillerin Özellikleri

Ceza yargılamasında her şey delil olabilir. Kanun delil türü bakımından sınırlamaya gitmemiştir; hukuka uygun elde edilmiş her şey delil olabilmektedir. Bununla birlikte, delillerin yargılamada esas alınabilmesi için bazı özellikleri taşıması gerekmektedir.

Delil olayı temsil etmelidir, bir diğer ifade ile olayla bağlantılı olmalıdır. İspat açısından yarar sağlamayan delil, olay bakımından değerlendirmede esas alınmaz. Bu tür deliller yalnızca yargılamanın uzamasına sebebiyet verirler ve sübuta etki etmezler.

²Feridun Yenisey ve Ayşe Nuhoglu, *Ceza Muhakemesi Hukuku*. (Ankara:Seçkin Yayıncılık,2022) s.536.

Delil beş duyu organı ile algılanabiliyor olmalıdır. Failin iç dünyasına yönelik tanımlamalar delil özelliği taşımaz.³ Bu özellik delilin mahkemede tartışılabilmesi açısından gereklidir. Tartışılmayan delilin karara etki etmesi mümkün değildir, değerlendirmeye esas alınamaz.

Delil akılcı olmalıdır. Rüya, kehanet gibi bilim dışı olan şeyler delil özelliği taşımaz. Delil olabilmesi için mantığa uygun olmalıdır. Örneğin kişinin olayın olacağı yaşanacağını öncesinde rüyasında görmesinin delil değeri yoktur.

Deliller hukuka uygun olmalıdır. Deliller elde edilirken hukuka aykırı yöntem ile elde edilmiş ise zehirli ağacın meyvesi de zehirlidir anlayışıyla elde edilen delil hukuka aykırı hale getirmektedir. Hukuka aykırı delilin olayı temsil etmesinin bir önemi bulunmamaktadır, hukuka aykırı deliller yargılamada kullanılamaz ve hükme esas alınamazlar.

Delil müşterek olmalıdır. Duruşmaya getirilmiş ve tartışılmış olan deliller muhakemeye etki sağlayabilirler. Duruşmaya getirme zorunluluğu doğrudanlık ilkesinden doğmaktadır. Delillerin duruşmada ikame edilmiş olması müşterekliğin sağlandığı anlamına gelmez, delilin ikamesi sadece “doğrudan doğrualığın” gerçekleştiği anlamına gelir. Müşterekliğin sağlanması ancak delilin mahiyeti hakkında tarafların iddia ve savunmasının dinlenmesi ve bir sentez yapılmasıyla sağlanmış olur.⁴

Doktrinde kimi yazarlar delilin ulaşılabilir olmasını da delil özelliği olarak kabul etmektedir.⁵ Delillerin ulaşılabilir olması delilin muhakeme bakımından esas alınabilmesi için gerekli bir kıstas olmakla birlikte, duruşmaya getirilemeyen delil, delil olma vasfında bir eksiklik oluşturmamaktadır. Yukarıdaki özelliklerin aksine delile ulaşamıyor oluşu her zaman kesinlik taşımamaktadır. Bazı delillerin günler hatta aylar yıllar sonra ortaya çıktığını göz önünde bulundurarak söylenebilir ki bu bir delil olarak değerlendirme engeli değil, hükme esas alma bakımından engeldir. Suç

³Mesut Bedri Eryılmaz, *Ceza Muhakemesi Hukuku Dersleri*. (Ankara: Seçkin Yayıncılık,2012) s.635.

⁴Fatih Birtek, *AIHM, Anayasa Mahkemesi ve Yargıtay Kararları Işığında Ceza Muhakemesinde Delil ve İspat*. (Ankara:Adalet Yayınevi,2017) s.64.

⁵ Bkz. Eryılmaz, s.636.; Şahin/Göktürk, s.23.

unsuruna ulaşamaması, o suç aletinin delil olarak değerlendirilemeyeceği anlamına gelmemektedir. Bu durum yalnızca delilin hükme etki etmesinin önüne geçmektedir. Bu özelliğin diğer delil olarak değerlendirilme şartlarından farkı, değişebilir nitelikte olmasıdır. Hukuka aykırı yöntem ile elde edilen delil hukuka uygun hale gelmemekte ya da akılcı olmayan delilin sonrasında düzelmesi mümkün değildir. Fakat delile ulaşamıyor olması, delilin esasına ilişkin bir eksiklik olmayıp, geçici bir durum arz edebilmektedir.

Hukukumuzda delillerin reddedileceği haller; hukuka aykırı bir şekilde elde edilmiş olması, hükme etki etmemesi ya da davayı uzatmak amacıyla yapılmış olması şeklinde sayılmıştır.

III.Delillerin Sınıflandırması

Delillerin sınıflandırılması bakımından öğretilerde birçok görüş bulunmaktadır. *Eryılmaz, Yenisey/Nuhoğlu, Öztürk/Tezcan*; beyan, belge ve belirti delili şeklindeki 3'lü tasnifi tercih etmiştir. *Centel/Zafer* ise şahsi delil ve maddi delil olan ikili ayrımı tercih etmiştir. Bu tasnif delilleri kaynağına göre değerlendirmektedir, kaynağı kişi olan sanık beyanı, tanık beyanı gibi deliller şahsi delil iken, tutanak, yazılı belge gibi kaynağı madde olan deliller ise maddi delillerdir.⁶

Delillere ilişkin bir diğer tasnif ise doğrudan doğruya ve dolaylı deliller şeklindedir. Bu sınıflandırma delillerin kaynağının doğrudanlığı üzerinedir. Beyan ve belge delilleri doğrudan doğruya delil olarak kabul edilirken, belirti delilleri dolaylı delil kabul edilmektedir. Dolaylı delil ispata ilişkin hususla birlikte, başka konuları da ispat edebilirler. Örneğin olay yerinde kişinin parmak izinin bulunması, olayı değil; sadece o kişinin orada bulunduğunu ispat eder.⁷

⁶ Cumhuriyet Şahin ve Neslihan Göktürk, Ceza Muhakemesi Hukuku-2.(Ankara:Seçkin Yayıncılık,2022) s.26.

⁷ Şahin/Göktürk, s.26.

Belirtmek gerekir ki bu tasnifler delillerin ispat deęerini esas almamaktadır; olayla baęlantılılıęı ve güvenilirlięi o delilin ispat deęerini belirler. Ceza hukuku bakımından delillerin birbirine üstünlüğü yoktur. Bir kağıt parçasına yazılmış mektup da delil deęeri taşıyabilir.

Delillerin sınıflandırılması bakımından çalışmada benimseyeceęimiz ayrım; beyan, belge ve belirti şeklinde olacaktır. Beyan delilleri; sanık beyanı ve tanık beyanı, belge deliller; ses tespit eden belge, yazılı belge, şekil tespit eden belge ve dijital delil, son olarak da belirti deliller ele alınacaktır.

A. Beyan Delilleri

1. Şüpheli-Sanık Açıklamaları

Şüpheli- sanık açıklamaları, soruşturma aşamasında ifade ve sorgudaki beyanları ifade eder. Ceza hukukunda deliller kural olarak soruşturma aşamasında toplandıęından, beyan delilleri soruşturma işlemleri olan ifade ve sorgudan elde edilir.

İfade, cumhuriyet savcısı veya kolluk tarafından alınır. Sorgu işlemi ise sulh ceza hakimlięi tarafından gerçekleştirilir. Kanunda ifadenin alınış yeri ve zamanıyla ilgili açıklama yapılmamıştır. Şüphelinin ifadesinin alınacağı yer kanunda açıkça belirtilmemiştir. Uygulamada çoğunlukla ifadelerin polis karakolu ya da Suça Sürüklenen Çocuklar bakımından savcının odasında alındığı görölmektedir. İfade zamanı bakımından sınırlama yoktur.

İfade davet üzerine veya yakalama sonucunda zorla getirilme şeklinde olabilir. CMK m.145'te ifadesi alınacak kişinin öncelikle davetiye ile çağrılacağı, gelmemesi halinde zorla getirileceęi belirtilmiştir. Ayrıca davetiyede çağırılma sebebinin açıkça belirtilmesi gerektięi de kanunda yer almaktadır. Davet üzerine ifade alınmasına gözaltı söz konusu deęildir. Gözaltına alma koşulları CMK 91.madde'de belirtilmiştir. Bu haller söz konusu olmadıęı için davet üzerine ifade vermeye gelen şüpheli hakkında gözaltı kararı verilemez.⁸

⁸Centel/Zafer, s.268.

İfadesi alınacak kişi çağrıya uymadığı halde, hakkında zorla getirme kararı verilir. Zorla getirme kararı istisnadır, kanun hangi hallerde verilebileceğini saymıştır; kişinin hakkında tutuklama kararı verilmesi, yakalama emri düzenlenebilmesi için yeterli nedenlerin bulunması veya çağrıldığı halde gelmemesi halleri. Zorla getirme kararında kişinin açık kimliği, üzerine atılı suç, eşkali ve zorla getirilme nedenlerinin olması gerekir.

İfade kolluk tarafından alınır. İfade ve sorguya alınmadan önce şüpheli veya sanığa hakları mutlaka hatırlatılmalıdır, bu haklar; yakınlarına haber verme hakkı, susma hakkı, lehine olan delillerin toplanmasını isteme, hakkındaki isnadı öğrenme hakkı ve müdafii yardımından yararlanma hakkıdır.

Yargıtay; “CMK’nın 191/3-c ve 147. maddeleri uyarınca sorguya çekilmesi gereken sanığa, bu maddeler ile tanınan savunma hakkına dair hakları hatırlatılmadan, hatırlatılmış ise de bu husus tutanağa geçirilmeden savunması alınıp yargılamaya devam edilerek hüküm tesisi usul ve kanuna aykırıdır.”⁹ şeklinde karar vermiştir. Yargıtay haklarının şüpheli veya sanığa eksik anlatılmasını veya tekrar ifade veya sorguya başvurulmasında tekrar hatırlatılmamasının aydınlatma yükümlülüğünün ihlali olarak kabul etmektedir.¹⁰

a. İkrar

Ceza hukukunda ikrar, şüpheli veya sanığın suçu işlediğine dair olan kabul beyanıdır. İkrarda şüphelinin veya sanığın suçu kendisinin işlediğini belirten beyanı basit ikrar olarak adlandırılırken, vakianın bir kısmını kabul etme veya farklı şekilde gerçekleştiğine dair olan kabuller tevilli ikrar olarak adlandırılmaktadır. Geçmişte ikrara büyük önem atfedilse de günümüzde değerlendirilmesi farklılık arz etmektedir. Tanıkların yalan beyanda bulunması cezalandırılırken, şüpheli için aynı cezai müeyyide uygulanmamaktadır. Cezalandırılma korkusu ile şüpheli veya sanığın yalan söyleyebileceği, gerçeğe aykırı ikrarda bulunabileceği öngörülmüştür. İkrar elde

⁹Yargıtay Ceza Genel Kurulu’nun 25.10.2016 tarihli, 2014/14-728 Esas, 2016/389 Karar numaralı kararında, sanığa haklarının hatırlatılması gerektiğini belirtme zorunluluğunu ortaya koymuştur. ; Özge Apış, “Güncel Yargı Kararları ve Yasa Değişikliği Işığında İfade Alma ve Sorgu Sırasında Şüpheli/Sanığın Hakları,” *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi* Haziran.2019: s.69.

¹⁰ Centel/Zafer,s.276.

edebilmek için hukuka aykırı yöntemlerin kullanılmasının önüne geçmek için susma hakkı, işkence ve kötü muamele yasağı gibi haklar kabul edilmiştir. Bu haklarla, kişinin kendi hakkında suçlayıcı beyanda bulunmasının zor oluşu göz önünde bulundurularak, iradi olmayan bir şekilde elde edilmesinin önüne geçilmek istenmiştir. İkrarın kabule değer olabilmesi için, özgür ve iradi olması koşuldur.¹¹

Modern ceza muhakemesinde sanığın itirafta bulunması ve ikrarı da delil olabilir ancak sanığın itiraflarının ve ikrarının doğruluğunun da delillerle saptanmış olması gerekir. Mahkeme sanığın suçlamayı kabullenip yaptığı açıklamalarla yetinmeyerek bunların doğru olup olmadığını da göstermelidir. Yargıtay bir kararında “*Başka kanıtlarla doğrulanmayan, oluşa ve maddi gerçeğe uygun düşmeyen, fenni kanıtlarla çelişen soyut ikrara dayalı hüküm kurulamaz.*” Şeklinde hüküm kurarak, sanığın ikrarının delillerle desteklenmesi ve sanığın itiraf ettiği bilgilerin doğru olup olmadığı incelenmesi gerektiğini belirtmiştir.¹² İkrarın delil değerinin belirlenebilmesi için belirli kıstaslar ortaya koyulabilir; suç konusu olaya ilişkin herkesin bilmesinin mümkün olmadığı detayların bilinmesi, bu açıklamaların farklı delillerle uyumlu olması ve çelişmemesi, ikrarın gerçekçi ve gerçekleşmesi mümkün olması bunlara örnek gösterilebilir.¹³

İkrar her zaman gerçeği yansıtmayabilir, maddi gerçeği aydınlatma niteliği taşımayabilir. İrade sakatlıkları sebebiyle kişi gerçeği yansıtmayan ikrarlarda bulunabilir ya da yalan beyanda bulunabilir. Bunu öngören hukuk sistemimiz yalnızca ikrarın mahkumiyete esas alınamayacağını kabul etmiştir. Yargıtay bu konuda; “*İkrar, tek başına kesin kanıt kabul edilemez. Çünkü bir kimsenin çeşitli nedenlerle ikrarda bulunması olanaklıdır. Yargıç önünde yapılan ikrarın dahi bağlayıcı olabilmesi için başka yan kanıtlarla doğrulanması gerekir. İkrarını geri alan sanığın önceki soyut ikrarına dayanılarak hiçbir zaman mahkumiyet kararı verilemez. Başka bir ifade ile kanıtla doğrulanan ikrar değerlidir. Soyut ikrar tek başına yeterli olamaz.*” ikrarın tek başına mahkumiyete esas olamayacağını değerlendirmiştir.¹⁴

¹¹Yar.CGK2.12.1991,1301/334,YKDTemmuz1992,s.1108;Öztürk/Tezcan/Erdem/Gezer/Saygılar/Alan/Özaydın/Tütüncü/Villemin/Tok, s.301

¹² Yargıtay 10 CD 12.7.2005 Tarih ve E.2004/24577 K.2005/8554 sayılı kararı; Devrim Aydın, *Ceza Muhakemesinde Deliller*. (Ankara: Yetkin Yayınları, 2015) s.64.

¹³Centel/Zafer, s.272.

¹⁴ Yargıtay 6.CD 2015/1932 E., 2018/1069 K.

2. Tanık Açıklamaları

Şüpheli ve sanık dışında herkes tanık olabilir. Mağdur veya şikayetçi de tanıklık yapabilir, bu kişilere de tanıklığa ilişkin hükümler uygulanır. Ancak yemin verilmez.¹⁵ 5271 Sayılı Ceza Muhakemesi Kanunu md.43/5'te tanığı dinleyebilecek kişiler sayılmıştır; Cumhuriyet savcısı, hakim veya mahkeme tanığı dinleyebilirken, kolluk huzurunda dinlenilmesi mümkün değildir. Ceza muhakemesinde tanık olarak dinlenecek kişiler tanıklık yaparken bazı haklara sahiptir; tanıklıktan çekinme, kendisi ve yakınlarının aleyhine açıklamada bulunmaktan çekinme, haklarını öğrenme korunma, tazminat ve masraflarını isteme hakkı. Tanıklık yapacak kişiye hakları hatırlatılmadan dinlenmesi halinde alınan beyan hukuka aykırı olacaktır.

a. Tanıklıktan Çekinme

Tanık her zaman tanıklık yapmaktan çekinebilir, bu hakkını kullanması sınırlandırılmamıştır. Tanıklıktan çekinme hakkı soruşturmanın her aşamasında kullanılabilir. Tanıklıktan çekinme hakkı, tanık dinlenilmeden önce kendisine hatırlatılır. Yargıtay bu hakkın hatırlatılmamış olmasını bozma sebebi saymıştır.¹⁶ Tanıklıktan çekinme halleri kanunda sayılmıştır. Kanun hükmü açıktır; yalnızca belirtilen hallerde tanıklıktan çekinme mümkündür. Tanıklıktan çekinme halleri iki sebeple oluşabilmektedir; mesleki sebepler ile çekinme ve kan-kayın hısımlığı sebebi ile çekinme.

Kan ve kayın hısımlığı sebebi ile tanıklıktan çekinebilecek kişiler; şüpheli veya sanığın nişanlısı, evlilik bağı kalmasa bile şüpheli veya sanığın eşi, şüpheli veya sanığın kan hısımlığından veya kayın hısımlığından üstsoy veya altsoyu, şüpheli veya sanığın üçüncü derece dahil kan veya ikinci derece dahil kayın hısımları ve şüpheli veya sanıkla aralarında evlâtlık bağı bulunanlar olarak belirtilmiştir.

Meslek sebebiyle tanıklıktan çekinebilecek kişiler; avukatlar veya stajyerleri veya yardımcılarının, bu sıfatları dolayısıyla veya yüklendikleri yargı görevi sebebiyle öğrendikleri bilgiler, hekimler, diş hekimleri, eczacılar, ebeler ve bunların yardımcıları

¹⁵ Doğan Soyaslan, *Ceza Muhakemesi Hukuku*. (İstanbul: Yetkin Yayıncılık, 2020) s.459.

¹⁶ Veli Özer Özbek, Koray Doğan ve Pınar Bacaksız, *Ceza Muhakemesi Hukuku*. (Ankara: Seçkin Yayıncılık, 2022) s.624. Bkz. Yargıtay 3. CD 2014/33375 E., 2015/11386 K., Yargıtay 3. CD 2013/32443 E., 2014/19466 K.

ve diğer bütün tıp meslek veya sanatları mensuplarının, bu sıfatları dolayısıyla hastaları ve bunların yakınları hakkında öğrendikleri bilgiler, malî işlerde görevlendirilmiş müşavirler ve noterlerin bu sıfatları dolayısıyla hizmet verdikleri kişiler hakkında öğrendikleri bilgiler şeklinde sayılmıştır.

Avukatlar, stajyerleri ve yardımcılarının dışındaki meslek gruplarında meslek sebebiyle çekinmesi, sınırlı bir çekinme halidir. Bu meslek gruplarının meslekleri sebebiyle öğrenmiş olduğu bilgilerin ilgilileri rıza verdiği takdirde, tanıklıktan çekinmeleri mümkün değildir.

Meslek ve kan-kayın hısımlığı sebebiyle çekinmenin haricinde kanun bir çekinme sebebi daha öngörmüştür; Anayasanın 38/5'inci fıkrasındaki *“Hiç kimse kendisini ve kanunda gösterilen yakınlarını suçlayan bir beyanda bulunmaya veya bu yolda delil göstermeye zorlanamaz.”* ibaresi Ceza Muhakemesi Kanunu'nun 48.maddesinde de belirtilmiştir. Kişilerin kanunda gösterilen yakınların aleyhinde beyanda bulunmaya yani tanıklık yapmaya zorlanamayacağı kanun tarafından koruma altına alınan bir tanıklıktan çekinme halidir. CMK m. 48'teki tanıklıktan çekinme sınırlı bir çekinmedir, tanıklıktan tamamen çekinme değil yalnızca kendisi ve yakınlarını suçlayıcı aleyhine olan hususlarda olan bir çekinme türüdür.

b. Tanıklara Yemin Verilmesi

Tanıklara dinlenmeden önce yemin verdirilebilir. Yemin verme yetkisi hakim ve mahkemeye aittir, soruşturma aşamasında Cumhuriyet savcısının da yemin verme yetkisi vardır. Fakat kollukların yemin verme yetkisi yoktur. Tanıklara tek tek yemin verdirilir. Yemin verilmesi gereken bir tanıkların yeminsiz dinlenmeleri bozma nedenidir.¹⁷ Yeminin şekli belirlidir, kısaltılmış yeminler hukuka aykırı niteliğe sahiptir. Tanıklık yaptığı sırada 15 yaşını doldurmamış olanlar, ayırt etme gücüne sahip olmayan kişiler ve yargılama konusu suça iştirak veya suç konusu delilleri değiştirme, gizleme veya yok etmekten sanık ya da hükümlü olan kişiler yeminsiz olarak dinlenir. Yemin yalnızca bir kez verilir, tanığın tekrar dinlenmesi halinde ikinci kez yemin verilmesi istenmez.

¹⁷ Soyaslan, s.470. Bkz. Yargıtay 4CD 2021/11451 K., Yargıtay 4CD 2021/24425 K.

c. Devlet Sırrı İçeren Bilgiler Hakkında Tanıklık

Tanıklık konusu bilgilerin devlet sırrı niteliğini taşıması halinde; tanık, sadece mahkeme hâkimi veya heyeti tarafından zâbıt kâtibi dahi olmaksızın dinlenir. Cumhurbaşkanının tanıklığında devlet sırrı niteliğinde bir beyan olduğunu kendisi belirler, mahkemeye bildirmesinde takdir yetkisi kendisine aittir.

d. Tanıkların Dinlenmesi

Duruşmaya davet edilen tanık bakımından hakim değerlendirmede bulunur; eğer davayı uzatmak amacı taşıyor ya da dava ile alakasız bir tanık ise tanık dinlemeye ilişkin talebi ret edebilir. Bu durum hakim delilleri serbestçe değerlendirebilmesi hakkının bir yansımasıdır. Bu durumun istisnası, duruşma gününde mahkeme huzurunda hazır olan tanıklardır, hazır olan tanığın davayı uzatma amacı taşımadığı açık olduğundan mahkemece dinlenir.¹⁸

Tanığa beyanda bulunmadan önce görevleri anlatılır. Sanık-şüphelilerin yalan beyanda bulunması cezalandırılmamışken, tanıkların yalan beyanda bulunmasının cezai müeyyidesi bulunmaktadır. Tanığa, yalan tanıklık yapması halinde cezalandırılacağı bu sebepten gerçeği söylemesi gerektiği beyanından önce söylenir. Doğruyu söyleyeceğine dair yemin edeceği tanığa bildirilir. Ceza hukukunda yemin hukuk yargılamasında olduğu gibi bir delil şekli değil, beyanın güvenilirliğini ölçme aracıdır.

Tanık beyanda bulunurken sözü kesilmez, çapraz sorgu yöntemi tanık beyanını tamamladıktan sonra uygulanır. Tanığa soru sorma sistemi ve sözü kesilmeden dinlenmesi düzenlemesi bu sebepten birbiriyle çelişmez. Tanık beyanlarının doğruluğunu tespit etmede kullanılan araçlardan birisi de doğrudan soru sorma hakkıdır. Tanığa soru yöneltebilecek kişiler; cumhuriyet savcısı, avukat, sanık, katılan ve toplu mahkemelerde heyette bulunan hakimlerdir.

Doğrudan soru sorma hakkı beyan delilinin sağlamlaştırması açısından önemli bir araçtır. Soru sorma sırasında tanığın olayla ilgili bilgisi ölçülecek, olaya ne kadar hakim olduğu anlaşılacaktır. Tanık yalan beyanda bulunuyorsa da bu durum soru sorma sırasında verdiği cevaplardan veya jest ve mimiklerinden anlaşılabilir.

¹⁸ Birtok, s.169.

Tanıklara soru sorulması ve yüzleştirilmesi Avrupa İnsan Hakları Sözleşmesinde yer alan haklardan silahların eşitliğine uygulama alanı sağlamaktadır.

e. Gizli Tanıklık ve Savunma Hakkı

Gizli tanıklık, yalnızca Ceza Muhakemesi Kanunu'nun suç saydığı fiilleri işlemek amacıyla kurulan bir örgütün faaliyeti çerçevesinde işlenen alt sınırı iki yıl veya daha fazla hapis cezasını gerektiren suçlarda veya terör örgütünün faaliyeti çerçevesinde işlenen suçlar bakımından mümkündür. Gizli tanıklık statüsü, amaç suç olan örgüt faaliyetleri çerçevesinde işlenen suçlar için mümkün olup, araç suç niteliğindeki örgüt kurma, yönetme ve üye olma suçlarında gizli tanık dinlenemez.¹⁹ Buna göre;

- Yargılamaya konu suçun örgütlü suçlardan olması
- Tanık olarak dinlenecek kişilerin tanıklığı, kendileri veya yakınları açısından ağır bir tehlike oluşturması,
- Bu tehlikenin başka türlü önlenmesi mümkün değil ise tanık gizli tanık olarak dinlenebilir.

Gizli tanığın dinlenmesi, Tanık Koruma Kanunu ve Ceza Muhakemesi Kanunu'nda belirtilen sınırlar içerisinde yapılabilir. Tanık Koruma Kanunu, gizli tanık dinlenirken ses ve görüntüsünün değiştirilebileceği gibi, duruşma salonuna getirilmeyecek şekilde de dinlenebileceğini düzenlemiştir. Duruşma salonuna getirilmeden tanığın beyanının dinlenmesi hususunda, kanun koyucu bir şekil şartı getirmemiş, uygulayıcıya bu alanda serbestlik tanımıştır. Bu serbestliğin sınırını Ceza Muhakemesi Kanunu 58. Madde ile çizilmiştir; Gizli tanığın beyanları duruşmada hazır olanlara kimlik bilgileri anlaşılmayacak şekilde okunur.

Tanığa soru sorulmasının sınırı kimliğini açığa çıkaracak sorular olmamasıdır, bununla birlikte hakim soru sorulmamasına da karar verebilir. Kanun metninde böyle bir açıklama yapılmış olsa da bu durumun adil yargılanma hakkına etki etmesi muhtemeldir.

¹⁹Osman Yaşar ve Cengiz Otacı, *Yeni İçtihatlarla Uygulamalı ve Yorumlu Ceza Muhakemesi Kanunu 1.Cilt.* (Ankara: Seçkin Yayıncılık, 2022) s.444.

Sanık veya şüpheliye tanık beyanına karşı savunma imkanı tanınmadan, gizli tanığın beyanının dinlenilmesi ve muhakemeye esas alınması, savunma hakkını sınırlar niteliktedir. Gizli tanıklık hakkındaki AİHM kararları, gizli tanığın hayati güvenliği ve savunma hakkı arasında adil bir denge kurulmasını istemektedir. Yaşam hakkı ve adil yargılanma hakkı hukuk düzeni bakımından aynı derece önem verilmesi ve korunması gereken haklardır. Gizli tanıklık statüsü tanığın yaşam hakkını korurken, sanığın tanığın beyanlarına karşı savunma yapabilmesi, soru sorabilmesi adil yargılanmanın bir gereğidir. Bu iki hak arasında bir hiyerarşi bulunmamaktadır bu sebeptendir ki AİHM haklar arasında denge kurulması gerektiğini belirtmektedir. Adil yargılanma hakkı korunmaksızın davada adil bir yargılama sonucu beklenemeyeceği gibi, tanıklık yapacak olan kişilerin yaşam hakkını korumak da bir o kadar önemli bir konu olup, bu husus devletin pozitif yükümlülüğü içerisinde yer almaktadır.

f. Tanık Beyanının Delil Değeri

Kanun koyucu tanık beyanı ile hüküm kurulabilmesine imkan tanımıştır. Fakat hüküm kurulurken tek delil tanık beyanı ise, tanığın tekrar dinlenmesi gerektiği kabul edilmiştir. Tanığın önceki beyanının duruşmada okunabilmesi için tek delilin tanık beyanı olmaması gerekmektedir. Yani bu tanığın tutanağa geçmiş ve duruşmada tutanaktan okunan beyanını destekleyen başka delillerin de bulunması gerekir. Hüküm, duruşmada okunan tanık dinleme tutanağı ve diğer delillere dayanmak zorundadır. Zira eğer olayın delili bir tanığın açıklamalarından ibaret ise bu tanık duruşmada mutlaka dinlenir. Yani olayın tek delili olan bir tanığın duruşma dışında alınan beyanını içeren tutanaklara dayanılarak hüküm kurulamaz.²⁰ AİHM içtihatlarına göre istinabe şeklinde tanıklar dinlenirken sanık veya müdafii soru sorma hakkı tanınmamış ve yalnızca buna dayanılarak hüküm kurulmuş ise adil yargılanma hakkı ihlal edilmiş olmaktadır. Bu beyanlara karşı itiraz hakkının tanınmış olması ihlal sonucunu değiştirmez.²¹

²⁰Atila Oğuz Boyalı AYM Kararı B. No: 2013/99, 20/3/2014. Aym tek delilin tanık beyanı olduğu hallerde tanık dinlenilmeden hüküm kurulamayacağına karar vermiştir.; Centel/Zafer, s.310.

²¹Aydın, s.73.

B. Belgeler

1. Yazılı Belge

Yazılı belgeler, yazı içeren belgeleri ifade eder. Yazılı belgelerin olayı temsil etmesi delil olmaları bakımından yeterli olmaktadır. Yazılı belgelerin, anonim olması, el yazısı bir belge olması, imza taşıması gibi özellikler belge olma niteliğini engellemez. Bu tür özellikler yalnızca belgenin ispat değeri bakımından zayıflık sağlamaktadır. Yazılı belgeler; otopsi raporu, ifade ve sorgu tutanakları, tanık beyanları, noterce düzenlenen belgeler vb. şeklinde yazılı olan tüm belgeleri kapsar.

Kanun koyucu belgeleri duruşmada anlatılması zorunlu (md.209), duruşmada okunması yasak olan (md.210, 148/4) ve sadece okunmasıyla yetinilebilecek (md 211) belgeler şeklinde üçlü bir ayrıma tabi tutmuştur.²² Duruşmada okunması zorunlu olan belgeler naip veya istinabe yoluyla alınan sanık, tanık beyanları vb. deliller olmaktadır. Duruşmada okunmayacak belgeler, olayın tek delilinin tanık beyanı olduğu durumlarda geçerlidir. Bu durumda tanığın vermiş olduğu beyan okunmakla yetinilemez, mutlaka dinlenilmesi gerekmektedir. Ayrıca şüphelinin müdafî olmaksızın kollukça alınan ifadesi de yine şüpheli veya sanık tarafından mahkeme önünde doğrulanmadıkça duruşma sırasında okunamaz. Son olarak sadece okunmasıyla yetinilecek belgeler ise tanık veya sanığın suç ortağının ölmüş ya da akıl hastalığına tutulmuş olduğu ya da bu kişilerin yeri bulunamamışsa, tanık veya sanığın suç ortağının duruşmada bulunması çeşitli sebeplerden mümkün değilse ya da tanığın ifadesi önem arz etmiyorsa olması halindedir.

Bir belge veya yazının delil olarak kullanılabilmesi duruşmada okunmasına bağlıdır.²³ Yazılı belgenin okunması gerekir ibaresinden anlaşılması gereken yazılı belgelerin duruşma sırasında okunması ve tartışılması olmalıdır. Taraflarca tartışılmayan bir delilin muhakemeye esas alınması mümkün değildir.

²² Yaşar/Otacı, s.1967.

²³ CMK m. 209 gerekçesi.

2. Şekil Tespit Eden Belgeler

Yazılı belgeler yargılamaya konu olaylarla ilgili okunmak suretiyle bilgi verirken şekil tespit eden belgeler ise belirli şekiller vasıtasıyla görülmek suretiyle bilgi verirler.²⁴ Resim, fotoğraf, kroki, plan ve benzeri şekil içeren belgeler örnek olarak gösterilebilir.

Şekil tespit eden delillerde dikkat edilmesi gereken hususlardan biri orijinalliktir. Gelişen teknolojiyle beraber dijital belgeler üzerinde değişiklik yapmak mümkün ve kolay hale gelmiştir. Belgelerin orijinal olması ispat bakımından önem taşımaktadır.

3. Ses ve Görüntü Tespit Eden Belgeler

Ses ve görüntü kayıtlarının çeşitli elektronik aygıtlarla kaydedilmesi sonucunda ortaya çıkan delilleri ifade eder. Film şeridi, teyp kaseti, video ve CD kasetleri, bilgisayar CD ve disketleri, taşınır bellekler, MOBESE kameraları ve işyerlerindeki özel kameralar ses ve görüntü tespit eden belgelerdir.²⁵

İçerik itibarıyla sağlamlığı ve olayı temsil kabiliyeti test edilmiş olup duruşma sırasında ortaya konularak süjeler tarafından tartışılmış olan ses ve görüntü kayıtları pekâlâ delil olarak kullanılabilir. Nitekim usul kurallarına riayet edilerek ve hukuka uygun bir şekilde elde edilen filmler, teyp bantları, video kasetleri, bilgisayar disketleri gibi ses ve görüntü kayıtlarının belge delili olduğunda bir şüphe bulunmamaktadır.²⁶

CMK m.147 ve m.219 hükümlerinde ses ve görüntü kaydına alınmayla ilgili hükümler bulunmaktadır. 147. Madde fıkrasına göre ifade ve sorgunun alınması sırasında teknik imkanlardan yararlanılır. 219. Maddenin lafzından bunun seçimlik bir durum olduğu ortaya çıkmaktadır; duruşmanın kaydının teknik araçlarla alınması halinde bunun yazılı tutanağa dönüştürüleceği belirtilmiştir. Duruşmaların kayda alınması zorunlu olmamakla birlikte, böyle bir seçenek de bulunmaktadır. Bu tür ses ve görüntü kayıtları yazılı tutanağa dönüştürüldüğünde, yazılı belge delili haline gelmektedir.

²⁴ Muhammet Sefa Çetin, *Kovuşturma Evresinde Belge Delillerin İkamesi ve Değerlendirilmesi*. (Ankara: Seçkin Yayıncılık,2021) s. 85.

²⁵Eryılmaz, s. 645.

²⁶ Çetin, s. 88.

4. Dijital Deliller

Dijital delillere ilerideki bölümlerde ayrıntılı bir şekilde yer verileceğinden açıklama yapılmayacaktır.

C. Belirtiler

Belirti delilleri ispat bakımından dolaylı bir vasıtaadır. Parmak izi, fren izi, saç teli vb. bulgular belirti deliline örnek olarak gösterilebilir. Bu tür deliller tek başına anlam ifade etmese de olay çerçevesinde değerlendirildiğinde maddi gerçeğin ortaya çıkmasına yardımcı olmaktadır.²⁷

Belirti delillerinden Alibi delili, diğer delillerle desteklendiğinde kişinin suçsuzluğunu ortaya koyan bir delil türüdür. Alibi, atılı suçun gerçekleştiği sırada şüphelinin olay yerinde bulunmadığı anlamına gelen belirti delili türüdür.²⁸ Bu durum şüphelinin olay yerinde bulunmadığını ispatlasa da atılı suçu işlemediği yönünde dolaylı bir delil sayılmaktadır.

²⁷ Öztürk/Tezcan/Erdem/Gezer/Saygılar/Alan/Özaydın/Tütüncü/Villemin/Tok, s.337.

²⁸ Öztürk/Tezcan/Erdem/Gezer/Saygılar/Alan/Özaydın/Tütüncü/Villemin/Tok, s.336.

İKİNCİ BÖLÜM

DİJİTAL DELİLLER

I. Genel Olarak

Gelişen teknolojiyle birlikte, her geçen gün hayatımızdaki teknolojik imkan ve aletlerin sayısında artış yaşanmaktadır. Günümüzde sosyal hayatımızın nerdeyse her alanında yaptığımız işlemlerin dijital bir yönü mevcuttur.²⁹ Taşınır ve taşınmazların satışının gerçekleştiği web siteleri, e- devlet sistemi, sosyal medya platformları buna örnek olarak gösterilebilir. Yaptığımız işlemler sonucunda oluşacak sayısal verilere kişisel verilerimiz de girmektedir. Kimlik bilgilerimiz, tüketim alışkanlıklarımız, gelir-gider-harcama dengemiz gibi birçok önemli bilgiyi internet ve bilişim cihazları üzerinden yaptığımız işlemlerle sanal ortama taşımaktayız. Hayatımızın bu denli dijitalleşmesinin sonucu olarak suçlar da dijitalleşmiştir. Suçlular bilişim cihazlarını araç olarak kullanarak suç işlemekte, bu cihazlarda suç unsurlarını depolamaktadırlar. Suçların işlenme şekli ve yerinin değişmesi ceza hukukunun da bu duruma uyum sağlamasını gerektirmiştir, suçla etkin bir şekilde mücadele için tedbirler öngörülmüştür. Kolluk, hakim, savcının yapacağı işlemler de bu suçlara müdahale edilebilecek uygunluğa getirilmiştir. Kolluk, hakim veya savcının teknolojik olanaklardan yararlanması koruma tedbirleri bakımından da gerçekleştirilmiştir.³⁰ CMK 134 ve 135. Maddelerinde yer alan koruma tedbirleri de teknolojinin gelişimiyle birlikte ceza muhakemesi bakımından kabul edilmiştir. Suç soruşturmasında fiziki delillerin yanında bu cihazlar içerisindeki dijital deliller de maddi gerçeğin ortaya çıkarılmasında gerekli hale gelmiştir. Eserin ana konusunu oluşturan bu delil türünü gerek hukuki gerek teknik anlamda inceleyip, hukukumuz için yeni bir kavram olan dijital delillerin ispat gücünü irdeleyeceğiz.

²⁹Değirmenci, s.131.

³⁰ Av. Aynur Tuncel, “Ceza Muhakemesi Hukunda İspat Konferansı,” *İstanbul Barosu*, <https://www.youtube.com/watch?v=7hl1pxgKwEQ> ,(E.T: 01.05.2023).

Dijital delil kavramının tanımlamadan önce veri kavramından bahsetmek gerekir. 5070 sayılı Elektronik İmza Kanunu’nun 3-a maddesinde ise verinin tanımı “Elektronik veri, elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtlar” şeklindedir. Dijital veriler bilişim aygıtları içerisinde yer almaktadır. Veriler olayla bağlantıları ortaya koyulduğunda delil olma niteliğine haizlerdir. Her dijital delil veridir fakat her dijital veri dijital delil değildir.

Dijital deliller, elektronik ortamda yer alan, somut olayı temsil etme gücüne sahip verilerdir. Bu deliller kişiler tarafından oluşturulabileceği gibi, bilgisayar tarafından oluşturulmuş olması ya da başka bir cihazdan aktarılmış olması mümkündür.³¹

Doktrindeki dijital delil ve elektronik delil arasındaki farklılık ve kullanılacak olan terim problemini çözmek adına Değirmenci’nin “*Elektronik delil ifadesiyle kapsayıcı bir terim olarak analog veya sayısal ortamda tutulan ve muhakeme konusu maddi olayı temsil edici bilgi veya veriyi ifade etmekteyiz[...] Buna karşın analog delillerin, hayatın her alanından gün geçtikçe silinmesi, sayısal delillerin hakimiyetinin artması ve sayısal delillerin toplanması ve muhafazasındaki özelliklerden dolayı*”³² dijital delil teriminin kullanılması gerektiği görüşüne katılmaktayız. Bilgisayarların hayatımıza girmesiyle birlikte analog deliller yerini dijital delillere bırakmıştır. Dijital delil teriminin, elektronik delil yerine tercih edilme sebebi ise, dijital delilin anlam olarak daha yakın olmasındandır. Elektronik delil, sayısal delile göre daha üst bir kavram olmakla birlikte, gelişen teknoloji içerisinde sayısal delillerin yaygınlaşması sebebiyle dijital delil (sayısal delil) kavramını kullanmak daha yerinde olacaktır.

³¹ Yusuf Başlar, “Elektronik Delil ve Ceza Yargılamasında Kabul Edilebilirliğine İlişkin Bir İnceleme,” *LHD*.2018: s.1665.

³² Olgun Değirmenci, *Ceza Muhakemesinde Sayısal (Dijital) Delil*. (Ankara: Seçkin Yayıncılık, 2014) s. 130.

II.Dijital Delillerin Deliller İçerisindeki Yeri

Ceza Muhakemesi Kanunu, dijital delillerin delil sınıflandırmasına yönelik bir düzenleme içermemektedir. Delilleri beyan belge ve belirti olarak üç grup şeklinde kabul ettiğimiz sınıflandırmada, dijital deliller bazen belirti, bazen de belge delilleri niteliğindedir.³³

Nuhoğlu ve Yenisey'e göre dijital veriler belge delili niteliğindedir; “Bilişim sisteminde yer alan elektrik yükleri cihazlarla okunarak anlamlandırılabilir. Bilişim teknolojisi içerisinde irade açıklaması içeren ve düzenleyeni teknik yöntemlerle tespit edilebilen bu tür veri grupları teknik anlamda belge niteliğindedir. Bu tür belgeler özellikle bilgisayarlardan yararlanarak ve bilgisayar programları (word, excel vb.) kullanılarak düzenlenir ve belli bir isim altında kaydedilerek bilgisayarın içinde saklanır.”³⁴

Öztürk ve Tezcan'a göre ise dijital verilerin delil olması usulüne göre doldurulup muhafaza altına alınmış ve yine usulüne uygun bir şekilde mahkemeye delil olarak sunulmuş bulunup bulunulmamasına göre ikili bir ayırım yapmak gerekir;³⁵ “Filmler, teyp bantları, video kasetleri, bilgisayar disketleri gibi araçların içeriği muhakeme konusu olay hakkında, delil olabilecek bir düşünceyi ihtiva ediyor ve yukarıda açıklanan koşulları taşıyorsa bunların belge olduğundan şüphe etmemek lazım gelir.³⁶ Ses ve/veya görüntü bantları usulüne göre doldurulup muhafaza altına alınmamış ve yine usulüne uygun bir şekilde mahkemeye delil olarak sunulmuş değilse, HİÇBİR ŞEKİLDE, tanıklık veya ikrar gibi delil vasfına haiz olamaz. Ancak bir belirti olarak değer taşıyabilir.”³⁷

Delilleri doğrudan veya dolaylı delil olarak ikiye ayıran tasnife göre ise dijital delillerin yeri değişiklik göstermektedir. Elektronik delil bazen doğrudan delil (bir saldırı olayını kaydeden sayısal kameradaki veri), bazen dolayısıyla delil (bilgisayara hukuka aykırı erişim suçunda, erişilen bilgisayarda bulunan sayısal izler)

³³ Değirmenci, s.130.

³⁴ Yenisey/Nuhoğlu, s. 576.

³⁵ Öztürk/Tezcan/Erdem/Gezer/Saygılar/Alan/Özaydın/Tütüncü/Villemın/Tok, s.333.

³⁶ Öztürk/Tezcan/Erdem/Gezer/Saygılar/Alan/Özaydın/Tütüncü/Villemın/Tok, s.333.

³⁷ Öztürk/Tezcan/Erdem/Gezer/Saygılar/Alan/Özaydın/Tütüncü/Villemın/Tok, s.334.

olabilecektir.³⁸ Bu sebeple dijital delilleri doğrudan ya da dolaylı delil olarak bir grubun içine sokmak doğru olmayacaktır. Maddi olaya göre dijital delilin doğrudanlığı değişiklik gösterecektir.

III.Dijital Delillerin Kendine Özgü Özellikleri

Dijital delillerin yapısı klasik deliller ile karşılaştırıldığında farklılık göstermektedir. Dijital deliller bilişim cihazları içerisinde sanal ortamlarda yer almaktadır. Sanal bir yapı içerisinde bulunmaları sebebiyle bu delilleri elde etmek için kullanılan arama ve elkoyma tedbirleri de farklılık göstermektedir.

- Dijital deliller kolayca kopyalanabilirler. Bu tür delillerin kolayca kopyalanabilir yapıya sahip olması bazı olumsuzluklara sebep olabilmektedir.
- Kolayca değişebilme, silinme gibi delilin sahliliğine şüphe düşürebilecek eylemleri yapmak mümkündür. Bu delillerdeki değişikliğı tespit etmek her zaman kolay olmamaktadır; adli bilişim uzmanlarının incelemeleri sonucunda bunlar fark edilebilmektedir.
- Delillerin elde edilirken ve sonrasında çok dikkatli bir şekilde korunması gereklidir. Korunamayan deliller dış etkenler sonucu bozulabileceklerdir.
- Sayısal deliller fiziki deliller gibi yargılama makamlarına sunulduklarında görüntülenemeyebilirler, bu delillerin görüntülenebilmesi için farklı vasıtalara ihtiyaç duyulmaktadır. Sayısal delillerin verilerden oluşması sebebiyle bilgisayar monitörü, yazılımlar vb. yardımcı araçlar ile görüntülenebilmesi mümkün olmaktadır.³⁹
- Dijital delillerin fiziki delillere göre avantajlı olduğu durumlar mevcuttur; depolama, elde etme ve muhafaza açısından dijital deliller kolaylık sağlamaktadır.⁴⁰

³⁸ Değirmenci, s.130.

³⁹ Rafael FERNÁNDEZ DE PAİZ ve Jesús Ángel SUÁREZ RAMOS, Dijital Delillerin Değerlendirilmesi. Hâkim ve Savcı Adaylarının Staj Verimliliğinin ve Etkinliğinin Arttırılması Projesi,2020, s.3.

⁴⁰ Çetin Araalan, “Türk Hukukunda Dijital Deliller,” *GSI Articleletter*.2015: s.206-207.

IV.Dijital Delillerin Elde Edilmesi ve Muhafazası

A. Dijital Delillerin Bulunacağı Ortamlar

Gelişen teknolojinin hayatımızın her alanına girmesiyle birlikte dijital verilerin muhafaza edildiği alanlarda da genişleme ve büyüme söz konusudur. Akıllı telefonlar, bilgisayarlar gibi elektronik cihazlar üzerinden neredeyse tüm işlemlerimizi gerçekleştirebildiğimiz göz önünde bulundurulursa, dijital delil niteliğinde olan verilerin ne denli geniş bir alana yayıldıkları anlaşılabilmektedir.

Dijital delillerin bulunacağı ortamların başında bilgisayarlar gelmektedir. Nitekim, Ceza Muhakemesi Kanunu da arama tedbirini “Bilgisayar, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma” olarak adlandırılmıştır.

Sayısal delillerin bulunduğu ortamlar bilgisayar ile sınırlı değildir. Mobil iletişim cihazları, akıllı televizyonlar, navigasyon cihazları, akıllı evler vb. birçok elektronik aygıt içerisinde dijital veri barındırmaktadır.

1. Bilgisayarlar

Uzun süreli veya geçici olarak veri depolama ve işleme özelliğine sahip birimler, bilgisayardan elde edilen sayısal deliller bakımından öncelikle kontrol edilecek alanlardır.⁴¹ Bilgisayarlarda veri saklayan birimleri; rastgele erişimli bellek (Random Access Memory- RAM), sadece okunabilen bellek (Read Only Memory- ROM), ön bellek (Cache Memory) ve sabit bellekler (hard disk) şeklinde ifade edebiliriz. Bu belleklerden bazıları verileri geçici olarak tutar ve herhangi bir şekilde cihaza enerji veren gücün kesilmesi durumunda söz konusu veriler kaybolur. Buna örnek olarak rastgele erişimli bellek ve ön bellek verilebilir.⁴²

Sabit disk ve RAM sayısal delillerin depolandığı alanlardandır. Sabit disk harici olabileceği gibi bilgisayar içerisinde de olabilir. Sabit diskte veriler kalıcı olarak depolanır, depolama işlemi için enerjiye ihtiyaç bulunmamaktadır.⁴³

⁴¹ Değirmenci, s.144.

⁴² Değirmenci, s.144.

Uçucu veri sabit diskte değil, RAM’de depolanmaktadır. Uçucu veriler bilgisayarın enerji kaynağından bağlantısı kesildiğinde kaybolan verilere verilen isimdir. RAM (Random Access Memory), geçici olarak verileri barındırma özelliğine sahiptir. RAM, bu tür verileri işlemcinin erişimine hazır bulundurur, elde edilen sonuçların depolama birimlerini sağlayan bilgisayar bölümüdür.⁴⁴

Sadece okunabilen bellekler bilgisayar ilk açıldığında MİB’ne hangi işlemleri yapması gerektiğini aktaran komutlar dizgesini içerisinde barındırır. Sadece okunabilen bellekler, özel bir içeriğe sahiptirler ve özel programları barındırmaktadırlar. Sadece okunabilen bellekler, kalıcı bellek türlerindendir, bazı modelleri yeniden yazılabilir olsa da çoğunlukla üzerinde bir değişiklik yapılamaz ve gücün kesilmesi durumunda üzerindeki verileri muhafaza ederler. Bu bellekler, bilgisayar açıldığı zaman, bilgisayarın düzgün bir şekilde çalışıp çalışmadığını kontrol etmek için birtakım testler yaparlar. Belleğin parçası olan ve ROM BIOS olarak isimlendirilen birim, bilgisayar sisteminin açılışını gerçekleştirmektedir.⁴⁵ ROM’lar, adlarından da anlaşılacağı üzere sadece okuma amacıyla kullanılır ve verinin kullanıcı tarafından işlenmesini engellemeyi amaçlar.⁴⁶

Ön bellekler, MİB tarafından bellek işlemlerinin hızlandırılması için tasarlanmış özel ve yüksek hızlı belleklerdir. MİB, ön bellekte bulunan komut veya verilere, sabit bellekte bulunan komut ve verilere oranla daha hızlı ulaşabilmektedir. Bu bağlamda rastgele erişimli bellek de bir ön bellek türüdür.⁴⁷

2. Veri Depolama Araçları

Veri depolama araçları bilgisayardan ayrı olarak bulunan ve bilgisayara veya bilgisayardan veri aktarımı sağlayan araçlardır. CD, DVD, Bluray, hafıza kartları, USB bellekler, dijital fotoğraf makineleri veri depolama araçlarına örnek verilebilir. Taşınır bellekler, hafif yapıları sebebiyle taşımaya elverişli depolama araçlarıdır. Bu aygıtlar, bilgileri depolamak için enerji kaynağına ihtiyaç duymazlar.

⁴⁴ Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku*. (Ankara: Seçkin Yayıncılık, 2023) s.675.

⁴⁴ Göksoy, s. 27.

⁴⁵ Değirmenci, s.145.

⁴⁶ Dülger, s. 629.

⁴⁷ Değirmenci, s.145.

Veri depolama araçları yüksek hızda veri okuyabilirler. Kullanımları yaygın olan veri depolama araçları, dijital delillerin elde edilmesinde başvurulan öncelikli aygıtlardan biridir.⁴⁸

3. Cep Telefonları ve SIM Kartı

Cep telefonları gerek mevcut gerek silinmiş kısa mesajları (SMS), telefon rehberi kayıtları, son aramalar listeleri gibi kanıtları barındırmaktadır. Kapasitesine bağlı olarak, müzik ve fotoğraf dosyaları, videolar, kelime işlemci program ve belgeleri de saklayabilmektedirler. Akıllı telefonlar her bakımdan bilgisayarlara benzerlik gösterdiklerinden; bilgisayar incelemelerinde kullanılan metotlar ve incelemeler, bu cihazlar üzerinde de yapılabilmektedir.⁴⁹

Taşınabilir aygıtların bazı modellerinde, gücün tamamen kesilmesi halinde üzerinde yüklü program ve veriler kaybolarak cihaz fabrika ayarlarına dönebilmektedir. Ayrıca, bazı cep telefonları ve cep bilgisayarlarına önceden yazılım yüklenmek suretiyle, gerektiğinde (Örneğin çalınma durumunda) uzaktan erişim yöntemiyle kullanılamaz hale getirebilmekte ve üzerindeki verilere ulaşılması kısıtlanabilmektedir. Bu tür yazılımların, cihazlara el konulması sonrasında aktif hale getirilerek, üzerindeki mevcut dijital delillerin kaybolması olasılığına karşı dikkatli olunmalıdır.⁵⁰

Mobil cihazlar, suç işlemede araç olarak kullanılabileceği gibi, suç delillerinin bulunduğu yer olarak da karşımıza çıkmaktadır.⁵¹ İskoçya'da Ore Operasyonu adli soruşturma esnasında birçok şüphelinin taşınabilir telefonlarında çocuk pornografisi görüntüleri ortaya çıkarılmıştır. Bu görüntülerin bir kısmı internet ortamından indirilen görüntüler iken bir kısmı da taşınabilir telefonda bulunan sayısal kamera vasıtasıyla oluşturulmuştur.⁵²

⁴⁸ Başlar, s. 79.

⁴⁹ Dülger, s.632.

⁵⁰ Türkay Henkoğlu, *Adli Bilişim, Dijital Delillerin Elde Edilmesi ve Analizi*. (İstanbul: Pusula Yayıncılık, 2014) s.271.

⁵¹ Göksoy, s. 76.

Suça konu deliller bazen mobil cihazın saklama alanında bulunurken bazen de mobil cihazlarının içerisindeki SIM kartları içerisinde depolanabilmektedir. Ayrıca SIM kartları sayesinde suça konu cihaza dair birçok bilgi elde edilebilmektedir. SIM kartlardan elde edilebilecek veriler; Kişiler Bilgisi, Konum, Servis Bilgileri ve mesajlardır.⁵³ Telefon rehberi ve arama bilgileri kullanıcı SIM kartını aktif olarak kullanıyorsa yani SIM kart seçiliyse erişilebilecek bilgilerdendir. Telefon rehberi SIM kartta depolanmaktadır; SIM kart kullan seçeneği seçilmemişse bu bilgilere ulaşamaz.⁵⁴ SIM kartlar vasıtasıyla elde edilebilecek verilerin en önemlilerinden biri konumdur. Kullanıcı mobil servis sağlayıcının baz istasyonları ile konum bilgileri üzerinden iletişime geçer. Mobil aygıtlar baz istasyonlarından aldıkları sinyalleri izlerler ve iletişimi sürekli tutmaya göre yapılandırılmıştır.⁵⁵

4. Bilgisayar Ağı

Bilgisayar ağları üzerinde bulunan veriler akış halinde bulunan verilerdir. Bu yüzden söz konusu verilerde gerçek zamanlı inceleme veya sistem çalışırken inceleme yapmak gereklidir.⁵⁶ Bilgisayar ağından birçok verinin elde edilmesi mümkündür fakat verilerin delil olarak kabul edilmesi için uzmanlar tarafından anlaşılır hale getirilmeleri gereklidir.⁵⁷

Bilişim sistem araçlarının üzerindeki verilerin incelenmesi, cihaz açık olmasa bile her zaman mümkünken, ağ üzerindeki verilerin incelenmesi ancak belli zamana ilişkin ağ trafiğinin yakalanarak (snapshot) daha sonra detaylı olarak incelenmesi ile mümkündür. Dolayısıyla bir anın analizi olduğu için özet değer alınması ve özet değerlerin karşılaştırılması mümkün olmamakta, canlı ağ trafiği her an ağ üzerindeki verilerde değişiklik yaratmaktadır.⁵⁸

⁵³ Değirmenci, s.143.

⁵³ Erhan Akbal ve Şengül Doğan, “SIM Kartların Dijital Delil Olarak İncelenmesi ve Analizi,” *Karaelmas Fen ve Mühendislik Dergisi*.2017: s.368.

⁵⁴ Akbal/Doğan, s.370.

⁵⁵ Akbal/Doğan, s.370.

⁵⁶ Değirmenci, s.149.

⁵⁷ Başlar, s. 82.

⁵⁸ Değirmenci, s.150.

Günümüzde kısıtlı kaynakları daha verimli kullanmak amacıyla, bilgisayarların birbiri ile bağlantılı olduğu ve kaynakları paylaştığı yerel alan ağlarının yaygın olarak kullanıldığı söylenebilir. Bilgisayarların bir ağ yapısı içerisinde olması, bir bilişim suçunun işlenme şeklini ve sonucunu değiştirebilmesi açısından önemlidir. Bir verinin güvenli ağ üzerinden nasıl alınabildiği sorusuna aranan cevaptan, bir saldırının hangi bilgisayar üzerinden (dolaylı olarak kim tarafından) yapıldığına dair oluşacak kanaate kadar birçok anahtar/ipucu başlangıcı, bilgisayarın girdiği yerel alan ağları içinde karşılaştığı ağ aygıtları ile ilgili Windows kayıt defteri elde edilebilmektedir.⁵⁹

5. Elektronik Posta İletileri

Elektronik postalar dijital delillerin bulunabileceği ortamlardan biridir. Teknoloji kullanımıyla birlikte iletişimin internet üzerinden yapılması da yaygınlaşmıştır. Kişiler gerek iş hayatı gerekse özel hayatlarında iletişim aracı olarak elektronik posta iletilerini kullanmaktadır. Elektronik postaların alındı ve gönderildi bilgileri bir suç soruşturmasında önem arz edebilmektedir. Somut delil oluşturması açısından elektronik posta iletilerinin bu tür bilgilere başvurulabilmektedir. Ayrıca kişilerin birbirlerine göndermiş oldukları elektronik posta metinlerinin de sayısal delil olarak kullanılabilmesi mümkündür. Elektronik posta iletilerine farklı dosya türlerinin ek olarak eklenebilmektedir. Bu tür ekler de dijital delil olarak adlandırılacaklardır. Elektronik postalar alıcıya ulaşmaya kadar geçmiş olduğu sunucularda izler bırakabilmektedir. Bu tür izlerin tespiti halinde bunlar da dijital delil olarak kullanılabilir.⁶⁰

Teknik olarak zararlı kod içeren bir e-postanın nereden geldiğinin tespit edilmesi mümkündür. E-posta sunucusu üzerinde, gönderilen ve alınan e-postalara ait gönderici ve alıcı bilgilerinin (gönderen bilgisayar ve sunucunun IP adresleri ve gönderici/alıcı e-posta adresleri) kayıtları tutulmaktadır. ⁶¹Bu kayıtların resmi yoldan istenmesi halinde e-posta hizmetini sağlayan servis sağlayıcıdan elde edilmesi, aradan birkaç yıl gibi çok fazla zaman geçmediği müddetçe mümkündür. Ayrıca, e-postanın geldiği servis sağlayıcıdan, e-postayı gönderen adres sorgulanmak suretiyle kullanıcıya ve sonrasında ilgili kullanıcıya hangi saatlerde ve hangi telefon numarasına

⁵⁹ Henkoğlu, s. 140.

⁶⁰ Değirmenci, s.153.

⁶¹ Henkoğlu, s.121.

bağlı bilgisayara/modeme servis hizmeti sağlandığını öğrenmek suretiyle adres bilgilerine ve kimlik bilgilerine dahi ulaşmak mümkün olabilmektedir.

6. Sosyal Medya

Sosyal medya platformlarının sayısının artması ile kullanıcı sayısında da kayda değer bir artış yaşanmıştır. Sosyal medya platformlarının günlük kullanım sürelerinin bu denli artması, sosyal medyayı hayatımızın gözlemcisi konumuna taşımıştır. Sosyal medya üzerinde sayısal verilerimiz depolanmaktadır; kişiden kişiye gönderilen mesaj veya iletiler, takip eden kişilerin görüntüleyebildiği içerikler ve son olarak da açık hesapların herkes tarafından görüntülenebilen paylaşımlar⁶² sayılabilecek verilerdendir.

Sosyal medya şirketlerinin topladıkları bilgiler ya da üçüncü parti şirketlerle ortak çalışarak tuttukları bilgiler birlikte değerlendirildiğinde, herhangi bir kişiyle ilgili cezai kovuşturma yapıldığında, sosyal medya üzerinden toplanacak elektronik verilerin, kişilerin sadece IP adresleri, sisteme erişim saatleri ve kullanıcı kimlik bilgileriyle sınırlı olmadığı, kullanıcının internet erişimiyle ilgili her türlü bilgi tutularak kayıt altına alındığından (sisteme erişilen cihazın bilgileri de dahil) , işlenen suçun niteliğine göre bu kişinin internet üzerinden işlenen suça konu ile ilgili bilgi toplayıp toplamadığı, suçun işlendiği sırada gerçek lokasyon bilgisinin tespiti açısından bu bilgiler kullanılabilir. Bu durumda da bilişim sistemleri ve sosyal medya üzerinden elektronik delil toplanması sırasında delil toplanacak yerlerin sınırlarının, çok daha geniş olduğu anlaşılmaktadır.⁶³ Big Data denilen bu bilgilerin sınırı iyi belirlenmelidir. Büyük veri, geleneksel yazılım araçları ve teknolojileri kullanılarak analiz edilmesi ve yönetilmesi zor olan ya da mümkün olmayan muazzam büyüklük ve çeşitlikteki dijital verileri ifade etmektedir.⁶⁴ Büyük veri sayesinde bir kişinin neredeyse gerçek zamanlı olarak takip edilmesiyle sınırlı kalınmayıp, o kişinin tutum ve davranışlarının analizi suretiyle psikolojik durumu dahi öngörülebilmektedir.⁶⁵

⁶² Göksoy, s. 106.

⁶³ Servet Yetim, *Ceza Muhakemesi Hukuku Kapsamında Sosyal Medyadan Elektronik Delil Toplama ve Değerlendirme (Facebook Örneği)*. (Ankara:Seçkin Yayıncılık, 2016) s.516.

⁶⁴ Durmuş Tezcan, Özge Sırma Gezer, Yasemin F. Saygılar Kırıt, Elif Altınok Çalışkan, Esra Alan, Özdem Özaydın, Efser Erden Tütüncü, İdris Güzel, Nilüfer Köker, Derya Altınok Vilemin ve Mehmet Can Tok, *Dijital Ceza Muhakemesi Hukuku*. (Ankara: Seçkin Yayıncılık, 2022) s.562.

⁶⁵ Tezcan/Gezer/Kırıt/Çalışkan/Alan/Özaydın/Tütüncü/Güzel/Köker/Vilemin/Tok, s.562.

7. Bulut Bilişim Sistemleri

Bulut bilişimde sayısal delil olarak kullanılabilir veri, kullanıcı tarafından yüklenen veya bulutta programlar üzerinde işlenen veriler olabilir. Burada yer alan verinin, bulut hizmeti sağlayan kuruluş tarafından birden fazla sunumcu üzerinden kullanıcının isteği halinde kullanıcının hizmetine sunması söz konusudur. Bulut bilişimde yer alan veri, tek bir sunumcu üzerinde depolanmamaktadır. Bununla birlikte bulut bilişimin en önemli özelliği, bulut bilişim hizmeti sunan kuruluşun hizmet sözleşmesinde belirtilen durumlar hariç olmak üzere, sunumcuların bulundurduğu veriyi, ulaşma hakkı bulunan kişiler başka kişilere aktarmamasıdır.⁶⁶

Bulut sistemi üzerinde yapılacak dijital delillerin incelenmesi esnasında; aynı ortamda bulunan ve suç konusu olmayan verilerin de açık hale gelmesi, farklı bir hukuksal problemin oluşmasına neden olabilecektir. Diğer taraftan, inceleme esnasında herhangi bir suç ile ilişkisi bulunmayan dosyaların yapısında da (son erişim zamanı vb.) değişiklik meydana geleceği için, daha sonra yapılacak herhangi bir incelemede delil niteliğinde değerlendirilmeyecektir.⁶⁷

B. Dijital Delillerin Elde Edilme Aşamaları ve Adli Bilişim

Dijital delillerin elde edilmesi, arama ve elkoyma ile başlayıp, mahkeme huzuruna getirildiğinde sonlanan bir süreçtir. Bu sürece adli bilişim aşamaları denilmektedir. Adli bilişimin amacı sayısal delilleri tarafsız bir şekilde inceleyerek mahkemeye sunmaktır. Adli bilişim faaliyeti yorum içermeyen, objektif ve teknik bir yöntemdir.⁶⁸ Adli bilişim aşamalarına ilişkin birçok metodoloji mevcuttur. Biz çalışmamızın kapsamını aşmamak için birkaç tanesini ele almakla yetineceğiz.

“Adli Bilişim Soruşturma Süreci (Computer Forensic Investigative Process)” modelini Mark Pollitt tarafından önerilmiştir. Bu model dört aşamadan oluşur; elde etme,

⁶⁶ Değirmenci, s.158-159.

⁶⁷ Türkay Henkoğlu ve Özgür Külcü, “Bilgi Erişim Platformu Olarak Bulut Bilişim: Riskler ve Hukuksal Koşullar Üzerine Bir İnceleme,” *Bilgi Dünyası*, 2013: s.72. (E.T:10.05.2023) <<https://www.openaccess.hacettepe.edu.tr/xmlui/bitstream/handle/11655/10734/94-828-1-PB.pdf?sequence=1>>.

⁶⁸ Muharrem Özen ve Gürkan Özocak, “Adli Bilişim, Elektronik Deliller ve Bilgisayarda Arama ve Elkoyma Tedbirinin Hukuki Rejimi”, *Ankara Barosu Dergisi*, 1.2015:s.45.

tanımlama, değerlendirme ve kabul.⁶⁹ Elde etme aşamasında verinin teknik ve hukuki gereksinimleri gözden geçirilir. Tanımlama aşamasında, verinin metin haline getirilmesi gerçekleştirilir. Bu metin haline getirme işlemi daha çok teknik bir işlemdir. Değerlendirme aşamasında, verinin hukuk sùjelerince anlaşılır hale getirilmesi ile tamamlanmış olur. Kabul aşamasında ise, verinin incelenmesi son bulup mahkemeye teslim edilir.⁷⁰

“Adli Bilişim Araştırma Çalıştayı Soruşturma Modeli (Digital Forensic Research Workshop Investigative)” 2001 yılında ilk defa toplanan Adli Bilişim Araştırma Çalıştay’ında önerilen metodolojidir. Tanımlama, muhafaza, toplama, inceleme, analiz ve sunum aşamalarından oluşmaktadır. Tanımlama aşamasında suç eylemlerinin tespiti yapılmaktadır. Muhafaza aşamasında, olay yeri muhafaza işlemi gerçekleştirilmektedir. Toplama aşamasında, arama kararının alındıktan sonra deliller toplanmaktadır. İnceleme aşamasında veriler incelenmektedir. Analiz aşaması elde edilen verilerin delil haline getirildiği, anlamlandırıldığı aşamadır. Sunum aşaması ise mahkemeye delillerin teslim edildiği aşama olmaktadır.⁷¹

Tüm metodolojilerde ortak olan aşamalar; verilerin toplanması, incelenmesi, analizi ve raporlanması olarak karşımıza çıkmaktadır. Biz de çalışmamız bakımından bu şemayı kullanarak genel hatlarıyla dijital delillerin elde edilme aşamalarına yer vermeyi amaçlamaktayız.

1. Dijital Verilerin Toplanması

Dijital verilerin elde edilmesi yani toplanması aşaması hukuki bir işlem olmakla birlikte, bu işlemin adli bilişimi ilgilendiren teknik boyutu da mevcuttur. Hukuki işlemin sağlıklı bir şekilde gerçekleştirilmesi için adli bilişim uzmanları veya eğitimli personel tarafından bu aşama gerçekleştirilmelidir.

Dijital delillerin kolayca bozulabilir yapılarının olduğu unutulmamalıdır. Bu sebepten dijital delillerin elde edilme aşaması titiz bir şekilde yürütülmelidir. Nitekim aramanın

⁶⁹ Göksoy, s.119.

⁷⁰ Değirmenci, s.165-166.

⁷¹ Değirmenci, s.166-167.

hukuka uygun olabilmesi için arama kararında bulunması gereken unsurların eksiksiz bir şekilde yer alması ve arama işleminde kararın dışına çıkılmaması gerekliken, teknik hususlar da göz ardı edilmemelidir.

Verileri toplanmaya başlamadan önce öncelikle arama kararının alınması gerekmektedir. Arama kararı verilere erişme ve onları inceleme hakkını veren bir karardır. Arama kararı olmaksızın verilere erişilmesi ve üzerinde inceleme çalışmaları yapılması mümkün değildir.⁷² Alınacak arama kararında aranacak cihazlar belirlenmeli ve o cihazlar üzerinde aramaya yoğunlaşılmalıdır. Bu bağlamda klasik arama tedbirinde olduğu gibi bilişim sistemlerinde yapılacak aramalarda da bir suça ilişkin herhangi bir delil değil arama talebinde bireyselleştirilmiş delil aranmalıdır.⁷³

Bilişim cihazlarında yapılacak olan arama öncelikle aranacak bilgisayar, ikincil olarak atılı suç üzerinde yoğunlaşmalıdır. Ev ya da iş yerindeki tüm bilgisayarların aranması hukuka uygun değildir. Suç şüphesi olan bilgisayar özelleştirilmeli ve yapılacak olan aramada bu bilgisayara yoğunlaşılmalıdır. Ayrıca, bilgisayarda yapılacak aramada da sınırsız bir arama gerçekleştirilmemelidir.⁷⁴ Günümüzde bilgisayarlar kişilerin özel hayatına ilişkin bilgi ve verileri depolayan araçlar konumundadır. Bu araçlar üzerinde yapılacak olan sınırsız bir arama bu haklara müdahale teşkil etmektedir.

Bilgisayarda yapılan aramalarda, bazı sebeplerden belirlilik ilkesini uygulamak mümkün olmamaktadır. Bilgisayarın yalnızca bir kısmında arama yapılması delillerin elde edilememesi sonucunu doğurabilmektedir. Failler, dosya tipi değiştirmek, dosyaları şifrelemek vb. yöntemler ile delilleri gizleyebilmektedir. Bu sebepten yalnızca bir dosya türü üzerinden yapılan arama bize istediğimiz sonucu vermeyebilir. Nitekim Değirmenci bu görüşü destekler nitelikte “*Bilişim sistemlerinde sayısal delilin aranması hususunda mutlak suretle sınırlamalar getirilmelidir. Ancak bu sınırlamalar dosya türleri bakımından değil arama yapılacak bilişim aracı ile aramaya neden olan fiil bakımından olmalıdır.*”⁷⁵ diyerek aramanın özelleştirilmesini vurgulamıştır.

⁷² Burak Çekiç, “Bilgisayar Verilerinde Arama, Kopyalama, Elkoyma Tedbirinin Hukuki Niteliği ve Benzer Kavramlar,” *NKÜ Hukuk Fakültesi Dergisi* 2021: s.163.

⁷³ Değirmenci, s.197.

⁷⁴ Değirmenci, s.197.

⁷⁵ Değirmenci, s. 199.

Dijital delillerler toplanmadan önce olay yerinin muhafazası gerçekleştirilmelidir. Olay yerini muhafaza altına almak, söz konusu bilişim araçlarına fiziki veya uzaktan erişimi engellemek anlamına gelmektedir. Dolayısıyla olay yerinin güvenliği alındığı andan itibaren, yetkisiz hiç kimse olay yerinde bulunan bilişim araçlarına fiziksel olarak erişme olanağı bulamayacağı gibi söz konusu araçlara, kablolu veya kablosuz ağlardan da ulaşma olanağı bulmamalıdır.⁷⁶ Olay yerinin güvenliğini sağlamak delillerin değiştirilme riskine karşı alınması zorunlu tedbirlerdendir. Soruşturma konusu suç ile ilgisi bulunan kişilerin, olay yerinde bulunan bilişim araçlarına erişimi engellenmelidir. Bu durum sayısal delillerin kasten veya sehven tahrifini veya yok edilmesini engelleyecektir. Şüphelinin, bilişim araçlarına erişiminin engellenmesi, delillerin bütünlüğünün sağlanması açısından önemlidir. Nitekim Internet üzerinden, tek tuşa dokunmak üzere bilişim sisteminin tamamında yer alan verileri silebilen programlara ulaşmak mümkündür.⁷⁷

Dijital delillerin elde edilmesi sırasında yapılan işlemlerin tutanağa geçirilmesi önem arz etmektedir. Tutanaklar, dijital delilleri güçlendirmektedir. Hem soruşturma aşamasında hem de kovuşturma aşamasında mahkemeye kolaylık sağlamaktadır. Tutanak tutma işlemi, soruşturma aşamasında, delillerin bütünlüğünün korunduğunun, adli bilişim aşamasının eksiksiz bir şekilde yerine getirildiğinin ispatı olurken, kovuşturma aşamasında, delilin kaynağının kontrolünde ve delile ilişkin itirazlara karşı kullanılabilmesi mümkündür.⁷⁸

Dijital delillerin toplanması sırasında adli bilişime ilişkin dikkat edilmesi gereken hususlar şunlardır;

- Delillerde parmak izi bırakmamaya dikkat edilmelidir.
- Yapılan işlemler için denetim zinciri oluşturulmalı, işlemler kayıt altına alınmalıdır.
- Olay yeri incelemesinde adli bilişim ilkelerine uyulmalı, çalışır durumda olan cihazlar ve uçucu verilere öncelik verilmelidir.

⁷⁶ Değirmenci, s.212.

⁷⁷ Değirmenci, s.213.

⁷⁸ Begüm Gürel ve İpek Mengilli, “Dijital Delil Kavramı ve Uygulamadaki Yeri,” *Leges Hukuk Dergisi*.2021: s.87.

- Delilin bozulmamasına özen gösterilmelidir. Delili bozabilecek program veya sistemlere dikkat edilmelidir. Bilişim cihazının ekran görüntüsü alınarak cihaz şifresi kaldırılmalıdır.
- Laboratuvar ve bilirkişi incelemesinde büyük zorluklar yaşatabilecek programların (PGP, TrueCryp vb.) varlığı araştırılmalı ve bu tür programların kurulu olması halinde, durumu açıklayan bir tutanak hazırlanmalı ve kamera kaydı altında canlı inceleme yapılmalıdır. Canlı inceleme konunun uzmanı tarafından yapılmalı ve yapılan tüm işlemler ayrıca dokümanlara kaydedilmelidir.
- Olay yerindeki açık bilgisayarların kapatma işlemi esnasında işletim sisteminin durumu mutlaka göz önünde bulundurulmalıdır. Windows işletim sistemleri (WinNT, W2K, WinXP, Vista, Win7) bilgisayarın fişini çekmek suretiyle kapatılırken, Windows sunumcuları, Linux ve Macintosh bilgisayarlar normal kapatma işlemi (*Bilgisayarı Kapat- Shutdown*) uygulanarak kapatılmalıdır. Dizüstü bilgisayarlar kapatılırken dikkat edilmesi gereken husus, bataryanın çıkarılmasıdır.
- İmaj alınırken, adli bilişim standartlarına uygun programlar (FTK Imager, En Case vb.) kullanılmalı ve orijinal delilin birebir kopyası (“sector by sector”, “bit to bit”) alınmalıdır. İmaj alma işleminde, adli bilişim standartlarına uygun olarak tek yönlü yazma işlemi yapabilen donanımsal disk kopyalama cihazları veya aynı özellikte yazılımlar tercih edilebilmektedir.
- İmaj alınması amacıyla kullanılan donanımsal araçları ya da yazılımların, birebir kopya alma, imajı istenen büyüklükteki parçalara bölebilmeye, arızalı disklerin imajını alabilme ve karşılaşılan tüm hataları kaydedebilme, “olayın adı, imaj alan kişiye ait bilgiler, tarih/saat bilgileri ve disk etiket bilgileri” gibi bilgileri kaydetme yeteneklerine mutlaka sahip olması gerekir.⁷⁹

2. Arama Yapılması

a. Yerinde Arama

Yerinde arama ya da mahallinde arama, bilişim cihazının bulunduğu yerde aramanın gerçekleştirildiği arama türüdür. Yerinde arama, uygulamada çoğunlukla tercih edilen bir yöntem olsa da bazı dezavantajları mevcuttur. Bunlardan ilki aramanın uzun süre almasıdır. Arama işlemi çeşitli sebeplerden uzun sürebilmektedir; veri depolama

⁷⁹ Henkoğlu, s.23-24.

birimlerinin genişliği, şifrelenmiş veya gizlenmiş verilerin bulunması bunlara örnek olarak verilebilir. Depolama birimlerinin büyük olması ise aranan verinin bulunamamasına ya da eğer kopyalama işlemi gerçekleştiriliyorsa bu işlemin uzun sürmesi sonucunu ortaya çıkarabilir. İşlemi yapan kolluğun şifrelenmiş veya gizlenmiş verileri elde edebilmesi için gerekli teknik bilgisi ya da aygıtı olmayabilir. Bu tür hallerde, mahallinde arama yapılması zaman kaybına sebep olabilmektedir.⁸⁰

Dezavantajlarının yanında, mahallinde arama yapılmasının zorunlu olduğu haller de mevcuttur. Uçucu veriler gibi bilgisayar kapandığında kaybolabilecek veriler bakımından yerinde arama yapılması daha uygundur. İnternet ağından elde edilecek olan verilere erişim için bilgisayarın açık ve çalışır durumda olması gereklidir. İnternet ağından elde edilecek deliller için de yerinde arama yapılması gereklidir.⁸¹

Yerinde (On-Site) aramada, aramanın icrası için genellikle iki yöntem uygulanmaktadır. Birinci yöntem, daha çok basit bir arama yöntemi olarak bilişim sisteminde yer aldığı bilinen bir verinin aranması amacıyla kullanılır. Bu yöntemde, kolluk kuvvetleri bilişim sistemine erişir ve içeriğini kontrol eder. Bu yöntemin tercih edilmesi durumunda, arama video kaydına alınmalı ve yapılan tüm işlemlere ilişkin kayıt tutulmalıdır. Bu yöntemin, bilgisayarda yer alan dosyaları veya üst verileri değiştirmesi kuvvetle muhtemeldir. Her ne kadar, yazma bloklama cihazlarının kullanılması ile bilişim sisteminin belleğinde bir değişiklik yaratması önlenebilir olsa da söz konusu yöntemin de eğitimli kişiler tarafından uygulanması gereklidir. Bu yöntem karşımıza son derece zaman kaybına neden olan bir yöntem olarak çıkmaktadır.

İkinci yöntem ise beraberinde getirmiş olduğu veri bütünlüğünü sağlama avantajından dolayı tercih edilen bir yöntemdir. Bu yöntemde, yerinde arama yapılmasına rağmen, öncelikle bilişim aygıtının belleğinin birebir kopyası alınmakta, tüm arama işlemleri ilgili kopya üzerinden yapılmaktadır.⁸² Bu yöntemin tercih edilmesi delil bütünlüğünü korumak açısından daha yerindedir. Birebir kopya üzerinde yapılan işlemlerde, verinin aslı korunmuş olur.

⁸⁰ Değirmenci, s.222.

⁸¹Göksoy, s. 128.

⁸² Değirmenci, s. 223.

b. Off-site Arama

Mahallinden uzakta arama, yerinde arama yapılmasının ya da verilerin birebir kopyasının alınmasının mümkün olmadığı hallerde söz konusu olmaktadır.⁸³ Aranacak verilere olay yerinde ulaşılması bazı durumlarda mümkün olmamaktadır; şifrelenmiş dosyalar ya da aranan verinin bulunmasının zaman aldığı zamanlarda mahallinden uzakta arama yapılması zorunlu olabilmektedir.

Aranacak verilerin bulunmasının zaman alması iki halde mümkündür, ilki dosyanın gizlenmiş, silinmiş ya da şifrelenmiş olmasıdır, ikincisi ise depolama alanında çok fazla dosya olması halindedir. Şifrelenmiş, gizlenmiş ya da değiştirilmiş dosyaları tespit etmek için adli bilişim uzmanları ve uygun bilgisayar programları gereklidir. Adli bilişim uzmanları programlar vasıtasıyla kolayca bu tür dosyalara ulaşabilirken, sıradan kolluk kuvvetinin bu işlemi yapması mümkün değildir. Bu işlemin olay mahallinde yapılması uzun zaman alacağından bahisle anılan hallerde mahallinden uzakta arama yapılabilir. ⁸⁴

Mahallinden uzak arama yapılması zorunlu olan hallerin bulunabileceğinin kabulüyle birlikte, elkonulan cihazlardan elde edilecek olan kişisel verilerin hak ihlallerine sebebiyet verebileceği, bunun da özel hayatın gizliliğini etkileyen bir husus olduğu göz önünde bulundurulmalıdır. Adli bilişim uzmanları arama yöntemlerini seçerken kendi rahatlarını değil, şüpheli veya mağdur haklarının korunmasının mümkün olduğu yöntemi seçmelidir. ⁸⁵

Mahallinde aramada aramaya şüpheli ve müdafinin katılması ve arama gerçekleşirken orada bulunabilmesi mümkünken, mahallinden uzakta arama laboratuvarında gerçekleştirilmektedir. Şüpheli ve müdafii aramaya katılamamakta, yapılan arama işleminin tespiti ancak tutanakla mümkün olabilmektedir. Nitekim olay yerinin dışında yapılan aramalarda kasten ya da sehven delillerin değiştirilme olasılığı mevcuttur. Doğruluk ve güvenilirlik açısından mahallinde arama daha şeffaf bir yöntemdir. Hukuka aykırı işlemlerin gerçekleştirilmesine açık olan mahallinden uzakta aramaların denetiminin güçlendirilmesi gereklidir.

⁸³Göksoy, s. 129.

⁸⁴ Değirmenci, s.224.

⁸⁵ Göksoy, s.129.

Nitekim bu konuda Şahin; “Mahalde yedekleme ve yedekten kopya verme olanağının bulunmadığının objektif olarak kabulünde zorunluluk bulunan hallerde, aramayı yapan kolluk birimince dijital delillere müdahaleyi önleyecek şekilde, seri numaraları tutanağa yazılmak suretiyle usulüne uygun olarak zapt edilip mühürlenerek, şüpheli veya müdafinin istemesi halinde nezaret etme ve denetleme imkanı sağlanarak inceleme mahalline kadar eşlik etmesi sağlanmak ve bu yerde şüpheli veya müdafinin hazır bulunmasına imkan verildikten sonra mümkün olan en kısa süre içinde mühür açılıp, dijital medyanın derhal imajının alınarak ilgisine de imajlardan bir kopya ve orijinal medya teslim edilerek, yine sanık veya müdafinin mühür açma işlemi sırasında hazır bulunmasının mümkün olmadığı hallerde, mühür açma işleminin arama ve el koyma kararını veren (veya onaylayan) hakim huzurunda açılarak imaj alma işleminin bu sırada yapılması yoluna gidilerek inceleme yapılması halinde 134/2 ye ve hukuka uygun bir süreç izlenmiştir.⁸⁶” şeklinde görüş belirtmiştir. Şahin’in önerisine katılmaktayız, mahalden uzak aramalarda titiz bir süreç izlenmesi delillerin güvenilirliği pekiştirmiş olacaktır.

c. Uzaktan Arama

Uzaktan arama, bilgisayarının sabit diski veya başka bellekleri üzerinde yapılan, bilgisayarıda arama yapılan kişinin haberi olmadığı bir arama türüdür. Türk hukukunda uzaktan erişimle arama düzenlenmemiştir. Avrupa Konseyi Siber suç Sözleşmesinin 32. Maddesi uzaktan erişimle arama yapılmasına imkan tanımıştır. Uzaktan arama doktrinde tartışmalı olan bir arama türüdür. Bunun sebebi, arama sırasında şüphelinin bilgisinin olmamasıdır. Şüphelinin bilgisi olmadan gerçekleştirilen koruma tedbirleri hukukumuzda mevcuttur. Tedbir kapsamında yapılacak olan aramanın sınırlarının temel hak ve özgürlere zarar verecek ölçüde geniş olması problem teşkil etmektedir.

Tedbirle şüphelinin bilgisayarından ortam dinlemesi yapılabilmekte, web kamerası ile izlenebilmekte, elektronik postaları denetlenebilmekte ve bilgisayarın sabit diski dahil tüm alanlarına erişilebilmektedir. Bu denli geniş bir alanın izlenmesi ve bunun yapılırken kişinin bilgisi dahilinde olmamasının yetki aşımına sebebiyet vermesi muhtemeldir. Şüphelinin tedbirden haberi olmadığı için, şüpheli toplanan delilleri

⁸⁶ Cumhuriyet Şahin, “Ceza Muhakemesinde Bilgisayarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma(CMK m.134),” *Yaşar Hukuk Dergisi* Temmuz. 2019: s. 283-284.

inceleyememektedir. Arama sırasında denetimin mevcut olmaması, kolluk veya üçüncü kişiler tarafından hukuka aykırı müdahalelerin yapılmasının önünü açmaktadır.⁸⁷ Tarafların delillere ulaşamaması, bu delillere itiraz etme imkanlarını ortadan kaldıracaktır.

Uzaktan arama iki şekilde gerçekleştirilebilmektedir; bunlardan ilki bilgisayara yazılım yüklenmesi şeklinde gerçekleşirken diğeri ise, internet veya diğeri bilişim ağları üzerinde bilişim sistem aracına bağlanmak suretiyle⁸⁸ gerçekleşmektedir.

d. Bulutta Arama

Bulutta arama; bilgisayar yazılım ve donanımlarının dosyaları saklamak için kullanıldığı bir tür bilişim hizmeti alt yapısıdır. Program ve verilerin bilgisayar ya da disklerde saklama zorunluluğu olmadan internet ortamında bir depolama aracında saklandığı sistem olarak adlandırmak mümkündür. Bulut bilişimin tercih edilme sebepleri maliyetinin az olması, erişim kolaylığı ve saklama alanı kapasitesinin sınırlanmamasıdır.⁸⁹

Bulut bilişime kaydedilen verilere ulaşmak için cihaza gerek kalmamaktadır. Bulut hizmetlerinde sağlanan hizmetin sürekliliği, bulut hizmetini kullanan kişilerin bulut yazılımına internet ağı üzerinden uzaktan erişim sağlayarak kullanabilmesi gibi kolaylıklar da sağlamaktadır. Bulutta arama, bulut depolama ve saklama sisteminde delil niteliğinde saklanan verilerin, teknolojinin gelişmesinin de etkisiyle kullanıcılar aracılığı ile daha hızlı bir şekilde arama yapılarak, çok kısa sürede istenilen delile ulaşmayı sağlamaktadır. Bulut sistemlerinde bulundurulanan verilen tek bir birimde depolanmazlar, birden çok depolama birimine yayılmaları mümkündür.⁹⁰ Veriler farklı depolama birimine yayılmış olsalar da yapılacak arama tüm depolama alanında değil, sadece bulut hizmeti kullanıcısı şüphelinin hesabı içerisindeki veriler bakımından olacaktır. Bu sınırın aşılması, kişilerin özel hayatlarına ilişkin verilerin gizliliğinin ortadan kalkmasına sebep olur.

⁸⁷ Özen/Özocak, s.50.

⁸⁸ Değirmenci, s.226.

⁸⁹ Göksoy, s.131.

⁹⁰ Göksoy, s.131.

Bulutta arama yapılması Türk hukukunda açıkça düzenlenmemiş olsa da doktrinde CMK m.134 hükmü kapsamında uygulanabileceğini belirten görüşler mevcuttur.⁹¹Bulut sistemi kullanıcılara sanal bir alan sağlar. Bu alan üzerinde arama yapılması CMK m.134 hükmüne aykırılık teşkil etmez. Madde hükmü sadece bilişim cihazlarında kaydedilmiş verilere değil, internet ağı üzerinde depolanan verilerin de elde edilebilmesini kapsamaktadır.

3. Elde Edilen Delillerin Muhafazası ve Taşınması

Adli bilişimin bir sonraki aşaması elde edilen dijital delillerin nakledilmesidir. Dijital deliller kolayca bozulabilir yapıları gereğince dikkatli bir şekilde korunmalı ve taşınması gerçekleştirilmelidir. Dijital verilerin taşınması sırasında şunlara dikkat edilmelidir;

- Dijital cihazlar, dikkatli bir şekilde taşınmalıdır; ısı, ses vb. cihazlarda tahrife sebep olacak eşyalardan uzak tutulmalıdır. Dik bir şekilde taşıyarak olası sarsıntılara karşı korunmalıdır. Manyetik alandan etkilenmeleri engellenmelidir. Tozdan, nemden, ısıdan ve sıvıdan uzak tutulmalıdır.
- Eşyalara dokunurken dikkatli davranılmalıdır, cihazlar üzerinde parmak izi ve DNA kalmamalıdır.
- Pille çalışan cihazlara özen gösterilmelidir, pillerin yerinden çıkması veri kaybına sebep olabilir. Bu durum gözetilerek pili olan cihazların incelemesi kısa bir sürede yapılması gerekir. ⁹²

4. Delillerin İncelenmesi Aşaması

İnceleme aşamasında, arama sonucunda elde edilen delillerin olay ile bağlantısı ortaya koyulur, soruşturma açısından gerekli olabilecek deliller çıkarılır. Toplanan veriler üzerinden ayıklama işlemi yapılır. Bu aşama, veri halindeki delillere anlam kazandırılmaya çalışılan aşamadır. ⁹³

⁹¹ Bkz. Değirmenci, s.242-243.; “Burada kullanıcıya ait veriler bulunmakta ve söz konusu verilerin kişilerin bilişim sistemlerinde tutulması ile bulut bilişimde tutulması arasında herhangi bir fark bulunmamaktadır. Bu nedenle CMK m.134 uyarınca alınacak bir arama kararı ile bulut bilişimde arama yapma imkanı bulunmaktadır.”

⁹²Göksoy, s. 135-136.

⁹³ Değirmenci,s.256.

İnceleme aşamasında öncelikle planlama yapılır; elde edilen veriler içerisinde olaya etki sağlayabilecek olanların nerede olabilecekleri araştırılır, bu sayede çalışmaya başlanmadan önce hangi alana bakılması gerektiğine ilişkin şablon oluşturulmuş olur. Planlama yapılması adli bilişim uzmanının yol haritasını belirler.⁹⁴

Bir diğer inceleme işlemi, yapılanların dokümente edilmesidir. İncelenen verilerin her aşamasının kayıt altına alınması delili denetlenebilir kılar. Elde edilen verilerin usulüne uygun yöntemlerle incelenip incelenmediği ancak bu tür yazılı kayıtlarla anlaşılabilir. Kayıt altına alma işlemi ayrıca, kamera kaydı şeklinde de gerçekleştirilmelidir.

İnceleme işlemi imaj üzerinden gerçekleştirilmektedir. Orijinal veri üzerinden yapılan inceleme verinin tahrifine sebebiyet verebilecektir. İncelemede, silinmiş, gizlenmiş, değiştirilmiş, şifrelenmiş verilere ulaşılması ve ortaya çıkarılması amaçlanmaktadır. Bu aşamada yapılacak olan çalışmalar sayesinde, daha önce fark edilemeyen olgular ortaya çıkarılarak yeni delillere ulaşılabilir.⁹⁵

Gizlenen, değiştirilen, şifrelenmiş veya silinmiş verilerin anlaşılması, bulunması veya geri getirilmesi için çeşitli araçlar kullanılmaktadır. Bunlardan biri de anahtar kelime arama yöntemidir. Elektronik medya üzerinde anahtar kelime yazılarak arama yapılır. Fakat anahtar kelime ile arama yöntemi her zaman yeterli bir yöntem olmamaktadır, teknik sebepler (yazılım tarafından yakalanamayan kelimeler) ya da anahtar kelimenin somut olay ile bağlantılı olmayan dosyalarda da bulunması hallerinde yöntem, sonuca ulaştırma bakımından yetersiz kalabilmektedir.⁹⁶ Bu yöntemin bir diğer avantajı ise, yalnızca atılı suça ilişkin verilerin inceleniyor olmasıdır. Yazılan anahtar kelime ile yapılan aramada sadece eşleşme sağlayan veriler tespit edildiğinden, şüpheli kişilerin özel hayat mahremiyeti ihlal edilmemiş olmaktadır.⁹⁷

⁹⁴ Başlar, s.224.

⁹⁵ Başlar, s.223

⁹⁶ Çekiç, s.164.

⁹⁷ Başlar, s.226.

Silinen verilerin kurtarılması ise farklı prosedürlere sahiptir. Silinen verilerin geri getirilmesi kimi durumlarda mümkünken kimi hallerde mümkün değildir. Dosyalar silindiğinde, sabit diskte bu tür dosyalar için ayrılan alanda beklerler. Yeni bir veri, silinen verinin üzerine yazılmadığı sürece bu alanda yerlerini korurlar. Bu tür hallerde silinen verileri geri getirmek mümkündür. Fakat sabit bellek üzerinde bulunan veri üzerine veri yazılırsa, yazılımsal olarak geri getirilmesi mümkün değildir. Sabit diskin kurtarılmasının son yolları, sabit diskin kazınması veya elektron mikroskopuyla bakılmasıdır, bu yöntemlerin dezavantajları yapılan işlemler sonucunda sabit diskin zarar görecektir. ⁹⁸

Şifrelenmiş verilerin çözümü de bu aşamada gerçekleşmektedir. Şifreleme yöntemi parola olabilmektedir. Parolanın çözülmesi olay yerinde mümkün olamayabilir, şifrenin çözümünü adli bilişim uzmanları gerçekleştirir. İkinci bir şifreleme yöntemi ise kriptografidir. Kriptografi yönteminde veriler şifre girilmediği sürece anlaşılabilir bir halde kalacaktır. Bu yöntem verilere erişme yolunda engel teşkil etmektedir. Kriptolu dosyalarda adli kopya alınması durumunda, alınan kopya da kriptolu olacak ve verilere erişilemeyecektir. Kriptolu dosyalarda kriptoların çözülerek sonrasında kopya alınması gerekmektedir. ⁹⁹

Son olarak üzerlerinde değişiklik yapılmış verileri incelemekte fayda var. Steganografi adı verilen veriler, üzerinde değişiklik yapılmış verileri ifade etmektedir. Bu yöntem sayesinde bir dosya türü hakkında yapılan aramada, aranan veri gizlenerek bulunması güçleştirilmektedir. Dosya türünün değiştirilmesi en yaygın kullanılan dosya gizleme yöntemlerinden biridir. Bu yöntem ilk görüşte dosyaları gizlemekle birlikte, adli bilişim yazılımlarıyla kolayca fark edilmesi mümkündür. ¹⁰⁰

5. Çözümleme (Analiz) Aşaması

Analiz aşamasında, hangi delillerin soruşturma kapsamındaki maddi olayı aydınlatmak için yeterli olduğu belirlenir. Toplanan veriler arasında işe yarayanlar çıkarılarak, suçla bağlantılı olan deliller ilgili mercilere sunulur. ¹⁰¹ Bu aşama ispata yönelik bir aşamadır. Verilerin delil değeri, suç bakımından hukuki değeri ortaya

⁹⁸ Değirmenci, s. 259.

⁹⁹ Çekiç, s.173.

¹⁰⁰ Değirmenci, 260.

¹⁰¹Göksoy, s. 136.

koyulur. Analiz aşamasının inceleme aşamasından farkı, bu aşamada delillerin hukuki değerinin belirleniyor olmasıdır. Verilerin suç soruşturmasına konu olay bakımından değeri bu aşamada anlaşılmaktadır. Analiz işlemi ispata yönelik bir işlem iken, inceleme işlemi daha teknik bir aşamadır.¹⁰²

Analiz aşaması her suç bakımından farklıdır. Her suça özgü farklı suç unsurlarını içeren verilerin tespit edilmesi amaçlanır. Bu aşama yargılama sjelerine suça ilişkin fikir vermeyi amaçlar.¹⁰³ Bu işlem yapılırken arama sırasında çıkartılan imaj ile analiz aşamasına kadar gelmiş imaj üzerinden hash değeri karşılaştırması yapılır. Hash değerlerinin birbiriyle örtüşmemesi delilin btnlğne şphe dşrebilmektedir.

6. Raporlama Aşaması

Raporlama aşaması adli bilişim evrelerinin son aşamasıdır. Bu aşamada elde edilen veriler toplanmış, tasnif edilmiş, maddi olayı aydınlatmada işe yarar olan veriler ayrılmış olarak rapora dklr. Bu rapor ile adli bilişimin teknik dili ile hukuk sjeleri tarafından anlaşılamayacak olan bilgiler anlaşılır hale getirilir.¹⁰⁴ Raporlama aşamasında delillerin hukuka uygun şekilde toplanmış ve değeriendirilmiş olması, delillerin muhakemeye esas alınabilmesini etkilemektedir. ngrlen usul kanunlarına uygun bir şekilde toplanmayan deliller, mahkeme tarafından esas alınmaz.¹⁰⁵ Adli bilişim uzmanları tarafından hazırlanan raporlara ilişkin hukukumuzda iki hkm bulunmaktadır; CMK m.209 ve 214.

CMK m. 209'a gre rapor, duruşmada anlatılması zorunlu belgeler arasında yer almaktadır. Nitekim delillerin mşterek olması ilkesi gereğince muhakemede tartışılmamış delillerin esas alınması hukuka aykırıdır. Hazırlanan raporun anlatılarak, somut olaya etkisi ortaya koyulmalıdır. CMK m.214'e gre ise, raporu hazırlayan adli bilişim uzmanlarının gerekli grlmesi halinde raporun aıklanmasına ynelik olarak dinlenebileceklerine ilişkindir. Hakim, rapor ile baėlı deėildir, vereceėi kararı rapora uygun olmak zorunda deėildir. Fakat rapor somut olayı aydınlatıcı nitelikte olduėunda yan delillerle desteklendiėinde hakimin rapora dayanarak mahkumiyet veya beraat hkm vermesi mmkn olmaktadır.

¹⁰²Başlar, s.233.

¹⁰³ Başlar, s.233.

¹⁰⁴ Başlar, s.239.

¹⁰⁵ zen/zocak, s.55.

V.Türk Hukukunda Dijital Delillerin Elde Edilmesi

A. CMK m.134 Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma

1. Genel Olarak

5271 Sayılı CMK'nın 134. Maddesinde düzenlenen ve hüküm altına alınan "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" tedbiri bir tür koruma tedbiridir.¹⁰⁶ Söz konusu koruma tedbiri, CMK'nın 116. ve 123. maddelerinde düzenlenen "arama" ve "elkoyma" koruma tedbirlerinin özel bir şekli oluşturmaktadır.¹⁰⁷ CMK'da arama ve elkoymaya ilişkin düzenlemeler, 134. Maddede düzenlenmemiş ya da söz konusu koruma tedbirleri ile çelişmemiş olması halinde bu koruma tedbiri bakımından da uygulanabilecektir. Örneğin CMK m. 134'te aramanın gece yapılıp yapılamayacağı düzenlenmemiştir. Genel arama hükümlerine göre gece vakti arama yapılamaz. Bu hüküm bilgisayar, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbiri bakımından da uygulanabilecektir.

CMK m.134, öncelikle arama ve kopyalama, ikincil olarak elkoyma tedbiri düzenlenmiştir. Elkoyma tedbirinin uygulanması için ek koşullar belirtilmiştir. Bu zorlaştırıcı şartlar iki amaca ilişkindir; temel hak ve özgürlüklere en az zarar verecek tedbirleri uygulamak ve kişilerin bilişim cihazlarını kullanmamaları sonucunda iş ve

¹⁰⁶ "CMK m.134 (1) Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine karar verilir. 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.

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözilememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.

(4) Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

(5) 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."

¹⁰⁷Hüsnü Aldemir, *Adli-Önleme Arama ve Elkoyma*. (Ankara:Adalet Yayınevi,2019) s.158.

özel hayatlarının zarara uğramamasıdır.¹⁰⁸ Kişiyi özel olarak addedilen bilgisayar kayıtlarındaki kişisel ve özel bilgiler, temel insan hakları arasında bulunmakta ve bireylerin özel hayatlarını ilgilendirmektedir. Özel hayatın gizliliği ve korunması, Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesinde düzenlenmiş ve yine bu madde ile bireylerin özel hayatının korunması güvence altına alınmıştır. Bu nedenle yasa koyucu özel hayata ilişkin hakkın kısıtlanması sonucunu doğuran bilgisayarlarda arama ve elkoyma tedbirini özel olarak düzenlemiş ve sıkı koşullara bağlamıştır.¹⁰⁹

2. Amaç

CMK'nın 116. maddesinde düzenlenen genel arama tedbirinde amaç, suç delillerinin elde edilmesidir. Genel aramada, kişilerin üstü, eşyası, evi ya da aracı aranmaktadır. Buralarda atılı suçlara ilişkin delil elde edilmesi amaçlanarak arama yapılmaktadır. CMK 123. maddesinde düzenlenen genel elkoyma tedbirinin amacı ise sonucunda elde edilen ve suç delilinin müsadere edilinceye kadar korunmasıdır.

CMK'nın 134. maddesinde düzenlenen arama ve elkoyma tedbirleri, CMK 123. maddeden farklı olarak bu tedbirin asıl amacı suç delillerinin elde edilmesi ve elde edilen suç delillerinin korunmasıdır. Burada bahsettiğimiz koruma tedbirinin amacının ise elde edilen elektronik delilin aslının ve/veya bir kopyasının muhafaza altına alınmasını sağlamaktır.¹¹⁰ Amaç bakımından farklılık gösteren CMK m.134'teki arama tedbiri, genel aramanın uygulanamadığı bir alan olan bilgisayar, bilgisayar programları ve kütüklerinde yapılacak arama bakımından hükümler içerir.

3. Kapsam

CMK m.134/1'in madde metninde tedbirin “bilgisayar, bilgisayar programları ve kütüklerinde” uygulanabileceği ifade edilmiştir. Bilgisayarlar, kendi işlemcisiyle ve kendi hard diskinde bulunan yazılımlarla birçok türden işlemi yapabilir ve bir belleği olan bu aygıtlar, dış ortamdan ve bir başka cihazlardan aldıkları verileri depolarlar.

¹⁰⁸Batuhan Aktaş, “Bilgisayarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Tedbiri Üzerine Bir İnceleme,” *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi* Şubat. 2017: s.228.

¹⁰⁹Ali Parlar ve Mustafa Öztürk, *Ceza Yargılamasında Arama ve Elkoyma*. (İstanbul: Aristo Yayınevi,2019) s.191.

¹¹⁰ Başlar, s. 156.

Her türlü belge ve dosyayı “işleyen dönüştüren, bunlardan yeni sonuçlar üreten ve kullanıcıya sunan, veri iletişimi sağlayarak başka yerlerdeki bilgilere ulaşabilmeyi sağlayan ve genel amaçlı olarak üretilen bir veri işlem aygıtı”¹¹¹olarak tanımlanabilir.

“Bilgisayar” terimi, sadece günlük dilde bilgisayar olarak adlandırılan cihazları değil, amaçsal yorumla işletim sistemi kullanan akıllı telefon olarak adlandırılan cihazları, tabletleri, giyilebilir akıllı aksesuarları (saat, gözlük gibi) ve benzer diğer aletleri de kapsar. Fonksiyonel yaklaşım ve amaçsal yorum, akıllı telefon, tablet gibi aletlerin de bilgisayar olarak kabul edilip, CMK 134. maddesi kapsamında değerlendirilmesini zorunlu kılmaktadır. ¹¹²CMK m.134 kapsamındaki aranabilecek bilişim cihazları veya programlarını tek tek saymak belirlilik ilkesi açısından faydalı olacaktır fakat her geçen gün gelişen teknoloji sebebiyle bunu gerçekleştirmek ve güncel tutmak mümkün olmayacaktır. Bu sorunun çözümü tüm bilişim cihaz/programlarını kapsayacak şablon çizmek yerinde olacaktır.¹¹³

CMK’nın 134. maddesinin uygulanmasında e-postaların da özel olarak ele alınması gerekir. ¹¹⁴ E-posta, bilgisayarlar ve buna benzer diğer akıllı cihazlar aracılığı ile gerçekleştirilen bir elektronik iletişim yöntemidir. E-postalar aracılığı ile delil elde etmek gerektiğinde, CMK’nın 134. ve 135. Maddelerindeki koruma tedbirleri göz önünde bulundurulmalıdır. Bu maddeler arasında yapılacak olan seçimde belirleyici kıstas olarak, durağan nitelikte mi yoksa akış halinde mi veri elde edilmesi amaçlandığıdır. CMK’nın 134. Madde gerekçesinde durağan halde olan cihazda arama yapılması terimi yer almaktadır. Bu gerekçeden yola çıkarak söylenebilir ki, iletişim araçlarıyla yapılan bir iletişimin sonlanması ve verinin durağan hale gelmesiyle CMK m. 134 hükmü uygulanacaktır. Bu husus e-postalar bakımından da geçerlidir. Bilişim sistemine kaydedildiğinde artık bu elektronik postalar CMK m.134 konusu haline gelecektir.¹¹⁵

¹¹¹Mert Karakoyunlu, *Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri*.(İstanbul:Legal Yayıncılık,2022) s. 42.

¹¹² Yaşar/Otacı, s.1107.

¹¹³ Başlar, s.159.

¹¹⁴Karakoyunlu, s. 141.

¹¹⁵Karakoyunlu, s.141.

Bilgisayar programı, maddi varlığı olmayan ancak maddi varlıklar arası iletişim kurarak bilgisayarın bir bütün halinde çalışmasını sağlayan, veri alan, depolayan, ileten, işleyen, gösteren, oynatan çeşitli dillerle oluşturulan komutlar dizisidir.¹¹⁶

Bilgisayar kütüğü, bilişim sistemlerinde herhangi bir verinin saklandığı mantıksal depolama birimine verilen ¹¹⁷isimdir. CMK 134. maddede yer alan “bilgisayar kütüğü” kavramı, bilgisayarla oluşturulan verilerin tutulduğu yer olarak geniş bir anlam içeriğine sahiptir, veri içeren donanımları hatta uzak depolama araçlarını da kapsar.¹¹⁸

Bir cihazın bilgisayar kabul edilmesi ile CMK 134.maddenin sağladığı inceleme usulüne tabi olması aynı şey değildir. Bir cihazın bilgisayar olup olmadığı, Sanal Ortamda İşlenen Suçlar Sözleşmesi’nin 1/a bendindeki bilgisayar tanımına göre çözülür. Bir cihazın CMK m.134 kapsamında olup olmadığı ise hem bilgisayar kavramına girip girmediği hem de dijital veri içerip içermediğine göre çözülür. Dijital veri içeren her cihaz, CMK 134. maddesi kapsamındadır.¹¹⁹

4. Somut Delillere Dayanan Kuvvetli Suç Şüphesinin Varlığı

Arama kararı verilebilmesi için madde lafzında iki tane şart bulunmaktadır. Bunlardan ilki, somut delillere dayanan kuvvetli şüphe sebeplerin varlığı, diğeri ise başka suretle delil elde etmenin mümkün olmamasıdır. Tedbirin uygulanması için aranan şüphe derecesi kuvvetli suç şüphesidir. Kamu davası için yeterli şüphe aranırken, CMK m.134’nin uygulanması için bu şüphe derecesi yeterli olmamış, kanun koyucu daha yüksek bir suç şüphesi gerektirdiğini belirtmiştir.¹²⁰

Kuvvetli şüphe, bilgisayarda, programda ya da kütükte arama kararı vermeden önce var olan, şüphelinin yüklenen suçu büyük bir olasılıkla işlemiş olduğunu gösteren somut delildir. Bu şüphe hali, aynı zamanda suça ilişkin daha ileri seviye delillerin de var olabileceğine ve çok güçlü olasılıkla bunların, şüphelinin kullandığı bilgisayarda /programda/kütükte bulunduğu, objektif bir gözlemciyi ikna edecek boyutta olmalıdır. Şüphelinin kullandığı bilgisayarda/programda/kütükte suça ilişkin deliller

¹¹⁶ Yaşar/Otacı, s. 1108.

¹¹⁷Değirmenci, s.52.

¹¹⁸ Yaşar/Otacı, s. 1107.

¹¹⁹ Yaşar/Otacı, s.1108.

¹²⁰Benek, s.383.

olabileceğine dair somut ve güçlü kanıtlar yoksa “bir de bilgisayarda/programda/kütükte bakalım, acaba oradan ne çıkacak” düşüncesiyle arama yapılamaz.¹²¹

Kuvvetli şüphe hem şüphelinin suçu işlediği hem de aranacak olan bilişim sisteminde delil bulunacağı yönünde olmalıdır. ¹²² Arama kararı ancak şüphelinin kullandığı bilgisayar, bilgisayar programı ya da kütüğünde suç delillerinin bulunma olasılığının yüksek olduğu durumlarda verilmelidir. Aranacak delil ve arama yapılacak bilgisayar arasında bağlantı bulunmalıdır. Dijital delil ve elde edildiği bilişim cihazı arasındaki kişi bağlantısını kurmak kolay olmamaktadır. Gelişen teknolojiyle bir başka bilişim cihazını yazılımlar aracılığıyla kullanmak mümkün olmaktadır. Delilin bulunduğu ya da suçun işlendiği bilişim cihazının, suç sırasında şüpheli tarafından kullanılmamış olması mümkündür. ¹²³

Şüphelinin suçu işlendiği yönünde kuvvetli bir suç şüphesi olmalıdır. Bu durum karşısında mahkûmiyete esas teşkil edebilecek kesin ve inandırıcı bir kanı henüz var olmamış olsa da eldeki deliller bakımından failin mevcut söz konusu suçun işlendiği yönünde kuvvetli ve makul şüphe boyutunu aşan, kesin ve inandırıcı kanaatin oluşması gerekmektedir. ¹²⁴ Ancak bu hallerde arama kararı verilmesi kişi bakımından hak ihlali sonucunu oluşturmaz. Aksi halde kişinin bilgisayarında yapılacak olan arama, keyfi olup hukuka aykırı hale gelecektir. Somut delillere dayanan kuvvetli şüphe sebeplerin varlığının aranması, aramanın özel hayatın gizliliğini ihlal etmemesi bakımından güvence oluşturur.

¹²¹ Yaşar/Otacı, s. 1114.

¹²² Şahin,s.274.

¹²³ Başlar, “Elektronik Delil ve Ceza Yargılamasında Kabul Edilebilirliğine İlişkin Bir İnceleme,” s.1667.

¹²⁴ Dülger, s.584.

5. Başka Suretle Delil Elde Etmenin Mümkün Olmaması

Temel hak ve hürriyetlere müdahale eden bu tedbir, her koruma tedbirinde olduğu gibi hüküm verilmeden önce uygulama alanı bulmaktadır. Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbiri kişinin özel hayatı ile bağlantılı bir koruma tedbiridir. Nitekim tedbir uygulandığında kişilerin bilişim cihazlarında depoladıkları mahremiyet içeren veriler de elde edilmekte ve açığa çıkmaktadır.¹²⁵

Bu tedbir, başka suretle delil elde etmenin imkansız olduğu durumlarda kullanılarak, fail hakkında delil elde etmek amacı doğrultusunda uygulanmaktadır. İşlenmiş olan bir suçu açığa çıkartmak amacıyla, birden fazla tedbire başvurulabilecek durumlarda öncelikle, bireyin temel hak ve hürriyetine en az müdahale teşkil edebilecek olan tedbire başvurulması oranlilik ilkesinin bir gerekliliğidir. Temel hak ve özgürlüklere daha az müdahalede bulunan bir tedbirle delil elde edilebiliyor ise bu tedbiri uygulamak gereklidir. Son çare prensibi, başka şekilde delilleri elde etmenin mümkün olmadığı hallerde tedbirin uygulanmasını ifade etmektedir.

Nitekim bu şartın gerçekleşmesi için, diğer koruma tedbirlerinin tek tek uygulanması ve sonuç vermemesine gerek yoktur. Diğer tedbirlere başvurulması sonucunda delil elde edilmesinin mümkün olmadığına ilişkin kuvvetli bir ihtimal bulunması halinde, ilk çare olarak da bu tedbire başvurulması mümkün ve hukuki olmaktadır.¹²⁶

Bilişim cihazları ile bağlantılı suç ve tedbirlerde suç unsurlarına ulaşabilmek ancak bilişim cihazlarının incelenmesi ile mümkün olmaktadır. Bu tür suçlarda genellikle başka türlü delil elde etmek halihazırda mümkün olmamaktadır.¹²⁷

¹²⁵ Özbek/Doğan/Bacaksız, s.362.

¹²⁶ Aktaş, s.223.

¹²⁷ Benek, s.385.

6. CMK m. 134'teki Aramanın Uygulanma Şartları

Kanun bu koruma tedbirinin uygulanması için bir suç sınırlandırılması getirmemiştir. Yalnızca bilişim suçları değil, her tür suç bakımından koruma tedbiri uygulanabilmektedir. Ceza muhakemesinde amaç maddi gerçeğe ulaşmaktır. Somut delillere bağlı “kuvvetli suç şüphesi sebeplerinin varlığı” şartı ile uygulanması kısıtlanan CMK m.134'e bir de sadece belli başlı suçlar için başvurulabileceğini kabul etmek, ceza kanunlarının maddi gerçeğe ulaşma amacının önünde ciddi bir engel teşkil edecektir.¹²⁸

CMK md. 134'te yer alan koruma tedbirinin soruşturma aşamasında uygulanması konusunda birlik olup, kovuşturma aşamasında da uygulanabilirliği öğretide tartışmalı olan bir konudur. Bir kısım yazarlar tedbirin sadece soruşturma aşamasında uygulanması gerektiğini¹²⁹ aksi halde tedbirden beklenen faydanın gerçekleşmeyeceğini ifade etmektedir. Tedbir kovuşturma aşamasında uygulandığında, bu durumun sanık tarafından bilinecek olması tedbirin uygulanmasını olumsuz yönde etkileyecektir. Sanığın tedbirin uygulanacağını farkında olması halinde, delilleri değiştirime, gizleme veya yok etme olasılığının yüksek olacaktır.¹³⁰ Delillerin toplanması kural olarak soruşturma evresinde gerçekleşmektedir. Nitekim madde lafzında yer alan “bir suç dolayısıyla yapılan soruşturmada” ve “şüpheli” ifadeleri de tedbirin soruşturma aşamasında uygulanması gerektiğini gösteren ifadeler olduğu savlarını tamamlayıcı rol üstlenmektedir.

Koruma tedbirinin kovuşturma aşamasında da uygulanabilir olması gerektiğini savunan yazarlar mevcuttur.¹³¹ Ceza muhakemesinde kural olarak delillerin elde edilmesi soruşturma aşamasında gerçekleşiyor olsa da kovuşturma aşamasında delil toplamaya ilişkin herhangi bir usul kuralı mevcut değildir. Hakim somut olayı aydınlatmak için kovuşturma aşamasında da delil toplayabilmektedir.

¹²⁸ Karakoyunlu, s. 146.

¹²⁹ Yenisey/Nuhoglu, s.428, Şahin/Göktürk, s.335.

¹³⁰Nur Centel ve Hamide Zafer, *Ceza Muhakemesi Hukuku*. (İstanbul: Beta Yayınevi, 2020) s.489; Karakoyunlu, s.144.

¹³¹ Bkz. Özen/Özocak s.62., Değirmenci, s.334., Şahin, s.278.

Sonuç olarak, CMK m.134'ün yalnızca soruşturma evresinde uygulanabileceğine ilişkin öngörünün kanun lafzından çıkartılmasının terkedilerek, kanunilik ve kıyas yasağı gereği maddenin soru işareti bırakmayacak şekilde tekrar düzenlenmesi gerekmektedir.¹³²

Arama kararı özelleştirmelidir. CMK md.134 bakımından dosya kapsamında özelleştirme mümkün olmamakla birlikte; aranacak bilgisayar, aranacak alan kararda belirtilmelidir. Suç ve tedbirin uygulanacağı bilişim cihazı eşleştirilmesi yapıp, bu durumun arama kararında belirtilmesi gereklidir.¹³³ Aksi halde arama keyfi bir hale gelecektir.

Arama kararında, evde, işyerinde vb. yerlerde bulunan bütün bilgisayarların aranmasından bahsedilemez, bu tür bir uygulama orantısız olacaktır. Aranacak olan bilgisayar şüphelinin kullandığı bilgisayar olmalıdır. Şüphelinin kullandığı bilgisayar olması yeterlidir, malik olma veya zilyetlik gerekli değildir. Bir yerde birden fazla bilgisayar olması halinde, hangisinin şüpheli tarafından kullanıldığını belirlemek kolay olmayabilir. Kolluğun, şüphelinin hangi bilgisayarı kullandığı tespit etmesi için, kabul edilebilir ölçüde bir çaba sarf etmesi gerekir. Hiçbir çaba sarf etmeksizin tüm bilgisayarların (ve bilgisayar niteliğindeki cihazların) aranması, kopyalanması ve bunlara elkonulması hukuka uygun değildir, en azından üçüncü kişiler yönünden tazminat talep etme şartları oluşur.¹³⁴

CMK.'nın 134. Maddesinin kabul ediliş amacı gözetildiğinde, genel olarak ev veya iş yerinde arama kararı alınması, arama yerinde bulunan bilgisayar veya bilgisayar kütüklerinde aramayı kapsamaz. Söz konusu arama sonucunda CMK.'nın 134. maddesi kapsamında bir arama gerekli olursa bu yönde yetkili hakimden usulüne uygun olarak arama kararı alınması veya gecikmesinde sakınca bulunan hallerin varlığı halinde Cumhuriyet savcısı tarafından bir arama kararı verilmesi gerekir. Bilgisayarda, bilgisayar kütüklerinde arama yapılmasına ilişkin bir hüküm içermeyen arama kararına dayanılarak yapılan aramada ele geçirilen bilgisayar kayıtları hükme esas teşkil etmez.¹³⁵ Yargıtay bir kararında, “Sanık tarafından işletilen iki ayrı

¹³² Aktaş, s.222.

¹³³ Başlar, s.163.

¹³⁴ Yaşar/Otacı, s.1114-1115.

¹³⁵ Aldemir, s.162-163.

işyerinde arama yapılmasına karar verilmesine karşın, aynı işyerinde bulunan bilgisayarlar üzerinde arama yapılabilmesine olanak tanıyan hükümlere göre verilmiş bir arama kararı bulunmadığı anlaşılmakla, işyerinde bulunan bilgisayarlar üzerinde yapılan arama sonucunda elkonulan ve içerisinde müşteki firmaya ait lisanssız yazılımların olduğu belirtilen harddiskler ve CD'ler hukuka aykırı delil niteliğinde olup hükme esas alınamayacağı”¹³⁶,na karar vermiştir. Bu şekilde düzenlenmiş olan genel arama kararı ile, bilgisayarda arama yapılması halinde elde edilen deliller hukuka aykırı olacaktır.

Ayrıca belirtmek gerekir ki, CMK m.134 bakımından önleme araması yapmak mümkün değildir. Her ne kadar CMK m.134 özel bir adli arama türü olsa da yasa koyucunun sadece adli aramalarda bilişim sistemlerinde veri aranmasını özel kurallara bağlamak niyetinin bulunduğu, önleme aramalarında özel bir düzenleme getirmediğinden, PVSK m.9 kapsamında bilişim sistem araçlarında da her türlü arama yapılabilir olduğunu ileri sürmek, temel hak ve hürriyetlere orantısız bir müdahale teşkil edecektir. Suç işlenmesinin önlenmesi amacıyla usulüne uygun arama yapan kolluk kuvvetleri, bilişim sistem araçlarında işlenen bir suçun delillerinin bulunduğu veya bizzat ilgili aracın suçun işlenmesinde kullanıldığı konusunda bir şüpheyne sahip olursa ilgili araca el koyacak ve ancak CMK m.134'teki diğer koşullar sağlanarak alınan karar üzerine ilgili araçlarda arama mümkün olacaktır.¹³⁷

7. İmaj Alma

İmaj birebir kopya anlamına gelmektedir. İmaj alma işlemi iki farklı şekilde gerçekleştirilebilmektedir; bölümlerin kopyalanması ve adli kopyalama işlemi. Bölümlerin kopyalanmasında diskin belirlenen kısımlarının kopyalanması gerçekleştirilmektedir. Bölüm kopyalama işlemi sırasında kullanılan imaj programının özelliğine bağlı olarak, alınan imajın başlık ve yapılandırma bilgileri değişiklik göstermektedir. Bu nedenle, bölüm kopyalama tekniği de adli bilişimde kullanılması doğru olan bir yöntem olarak kabul edilmemektedir.¹³⁸

¹³⁶ Yargıtay 19. CD, 6.5.2015, 2015/2092-1175; Şahin, s.275.

¹³⁷ Değirmenci, s.336.

¹³⁸ Henkoğlu, s.50.

Elektronik verinin kopyası ancak imaj şeklinde alındığında geçerli olmaktadır. Basit kopya üzerinden yapılacak olan inceleme geçerli olmayacaktır. Bu durum usule uygun kabul edilmeyecektir. Aynı şekilde normal kopya da birebir kopya yerine geçmediğinden bu tür kopyaların üzerinden yapılan bilirkişi incelemeleri geçersiz olacaktır. ¹³⁹ Delil ihtiva etmesi muhtemel bilgisayar sistemleri üzerindeki incelemeler, sistemin veri depolama birimlerinin birebir alınmış kopyaları üzerinde gerçekleştirilmelidir. Delilin aslı üzerinde yapılacak inceleme bozulmasına sebep olabilmektedir. Delilin birebir kopyası da bu sebepten aslı gibi sayılmaktadır. ¹⁴⁰

Dijital deliller insan müdahalesi olmaksızın da değişebilmektedir. Bilişim sisteminin otomatik güncellemeleri, yedeklemeleri sonucunda bu verilerde değişiklik meydana gelebilecektir. Bilgisayarın açık-kapalı durumunun değiştirilmesi, tarama yapmak, kopyalama gibi faaliyetler bilişim cihazlarında izler bırakarak değişikliğe sebep olabilirler. ¹⁴¹ Dijital delillerin bilinçli ya da bu gibi durumlarda sehven değiştirilmesinin önüne geçmek için, öncelikli cihazın adli kopyası alınmalıdır. Bilişim cihazından alınan imajdan, veri üzerinde değişiklik yapılmışsa bu durum anlaşılabilir.

Madde metninde arama ve elkoyma için farklı terimlere yer verilmiştir. Arama sırasında kopya alınması, elkoyma sırasında ise yedekleme yapılması öngörülmüştür. Uygulamada ayrı ayrı bu işlemler yapılmamakta, yalnızca adli imaj kopyası alınmaktadır. Alınan kopyalardan şüpheli ve müdafine verilmesiyle işlem tamamlanmaktadır. Adli kopya yedeklemenin gereksinimlerini de kapsamaktadır. ¹⁴²

Adli kopyalama işlemi, dijital delillerin elde edilmesi bakımından uygulanabilir olan bir yöntemdir. Bu yöntem, tüm dosyalara erişim ve kopyalama imkanı sunmaktadır. Bilişim suçları faillerinin veri gizlemek için kullandıkları yöntemlerle etkin mücadele için adli kopyalama işlemi gereklidir. Birebir kopyalama işleminin, diskte bulunan tüm alanları fiziksel anlamda kopyalamasının yanı sıra ikinci bir özelliği, her bir dosyaya ait oluşturulma, değiştirilme ve erişilme tarihlerinde herhangi bir değişiklik

¹³⁹ Başlar, s.209.

¹⁴⁰ Şenel.Sarsıkoğlu “Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı”, *Türkiye Adalet Akademisi Dergisi*, Sayı. 22, Temmuz 2015: s.440.

¹⁴¹ Çekiç, s. 157.

¹⁴² Çekiç, s,175.

yaratmamasıdır. Mantıksal kopyalama işleminde, kopyalanan dosya üzerinde herhangi bir değişiklik yapılmasa dahi, kopyalama tarihi, kaynak ortamdan farklı olacaktır.¹⁴³

İmaj almaya yönelik uygulamada bazı eksiklikler mevcuttur. Bunlardan ilki terim problemidir. Yedeğin alınması ve kopya alınması gibi işlemler imaj alma işlemiyle tam olarak örtüşmemektedir. Yedekleme işleminde boş sektörlerin kopyası alınamadığından delilin bütünlüğü zarar görmektedir.¹⁴⁴ Bu terimsel problemin düzenlenmesi gerekir. Ayrıca yönetmelikle imaj alma işleminin kim tarafından, nasıl, ne zaman yapılacağına ilişkin açıklamalara yer verilmelidir.

İkinci eksiklik ise imaj alma mahallidir. İmaj alma işleminin mahallinde yapılıp, alınan imaj kopyasının birini de şüpheli ve müdafine verilmesi gerekirken, uygulamada bu şekilde gerçekleşmeyebilmektedir. Bu durumun başlıca sebepleri adli bilişim uzmanlarının ve teknik ekipmanların yetersizliğidir.¹⁴⁵ Elkoyma öncesinde ya da sırasında alınan adli kopyalar hukuka uygunken, elkoyma gerçekleştirildikten sonra alınan adli kopyaların güvenilirlikleri tartışmalı olacaktır.

8. Elkoyma

Bilgisayar veya bilgisayar kütüklerinde arama kararının icrası için, şüpheliye ait bilgisayara el konulması zorunlu değildir. Ancak bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılabilmesi ya da işlemin uzun süreceği olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir(CMK m.134/2).

Yukarıda belirtilen üç halden biri veya birkaçı bulunması halinde, nedeni belirterek elkoyma işlemi gerçekleştirilebilir. Elkoyma tedbiri uygulanırken bilişim cihazındaki tüm verilerin yedeklenmesi gerekir. Yedekleme işlemi elkoyma tedbirinden önce veya elkoyma sırasında yapılabilecekken, sonrasında yapılması koruma tedbirinin güvenilirliğini olumsuz yönde etkileyebilecektir.¹⁴⁶ Usulüne uygun bir elkoyma kararı olmadan arama mahalli dışında gerçekleştirilen imaj alma işleminin hukuka aykırı

¹⁴³Değirmenci, s.246.

¹⁴⁴ Şahin, s.281.

¹⁴⁵ Şahin, s.284.

¹⁴⁶ Aktaş, s.233.

olduğu ve bu suretle elde edilen deliller hükme esas alınamayacağı kabul edilir.¹⁴⁷ Adli kopyalarının mahalinde alınması delilin güvenilirliğini etkileyen bir husus olduğundan kural olarak imaj alma olay mahalinde yapılmalıdır. Elkoyma gibi istisna hallerde ise adli kopyanın laboratuvarında alınması zorunlu hale gelmektedir.

Uygulamada tedbiri uygulayacak adli bilişim personelinin yetersizliği ve arama işleminin uzun süreceğinden bahisle olay yerinde yalnızca kopyalama işleminin yapıldığı, gerekli incelemenin ise, bilişim laboratuvarlarında gerçekleştirildiği görülmektedir.¹⁴⁸ CMK m.134'te yer alan elkoyma hükmünün düzenlenme amacı arama ile kopyaların alınmasının mümkün olmadığı hallerde elkoyma tedbirinin uygulanmasıyla tedbirin uygulamasının sekteye uğramamasıdır. Madde bakımından elkoyma halleri sınırlı sayıda sayılmıştır; işlemin uzun sürmesi, şifrelenmiş belgelere erişim sağlanamaması veya gizlenmiş bilgilere ulaşılamaması. Bu haller mevcut değil ise, diğer bir deyiş ile arama sırasında kopyalar alınmışsa elkoyma tedbiri uygulanmayacaktır.¹⁴⁹ Elkoymanın tedbir bakımından kural değil, istisna olduğu göz önünde bulundurularak karşılaşılan bu soruna gerekli düzenlemeler yapılarak çözüm bulunması gerekmektedir.¹⁵⁰

CMK md. 134/2; “Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.” demektedir. El konulan cihazların iade edilmesi halinde suç unsuru içeren delilleri barındıran cihazların iade edilip edilmeyeceği hususu ele alınmalıdır. Madde metninde cihazlarda suç unsuruna rastlanıp rastlanmadığına ilişkin bir ayrıma gidilmediğinden her türlü aygıtın iade edileceği anlaşılmaktadır. Madde hükmü anlaşılır olsa da her durumda uygulanabilir değildir. Suç unsuru içeren dijital delillerin, şüpheliye iade edilmesi hukuk sistemlerince benimsenen bir yöntem değildir. Bu sorunun çözümü iç hukukta düzenlenmemiştir. Ancak Avrupa Konseyi Siber Suç Sözleşmesi'nin 19/3-d bu konuyla ilgili bir düzenlemesi mevcuttur; suç unsuru veya suç aracı olan veriler erişemez ve kullanılamaz hale getirilmelidir. İlgili madde kopyaları alınan verilerin silinebileceğini de ayrıca düzenlemiştir.¹⁵¹ İç hukukumuzda suç unsuru içeren bilişim

¹⁴⁷ Aldemir, s.166.

¹⁴⁸ Aktaş, s.229.

¹⁴⁹ Aktaş, s.232.

¹⁵⁰ Başlar, s.171-172.

¹⁵¹ Başlar, s. 173.

cihazlarının iadesi bakımından bir boşluk olduğundan, tarafı olduğumuz Avrupa Konseyi Siber Suç Sözleşmesi'nin ilgili hükmünün uygulanabileceği görüşündeyiz.

CMK'nın 134. Maddesi uyarınca usulüne uygun bir karar olmamasına rağmen, aynı Kanunun 119 ve devam maddeleri uyarınca alınan arama kararına istinaden, yapılan adli arama sırasında, bilgisayar kasalarına da el konulması (bilgisayar içeriği ile ilgili herhangi bir inceleme ve tespit yapılmamak şartı ile) adli aramayı hukuka aykırı hale getirmez.¹⁵²

Genel arama kararında kişinin konutu aranırken bilgisayarına elkonulmasını engelleyen bir hüküm mevcut değildir. Fakat bu halde, bilgisayarda veri araması gerçekleştirilemeyeceğinden, bilgisayarda arama için hakim kararı alınması gerekecektir.¹⁵³

Uygulamada mobil cihazlara basit elkoyma hükümleri uygulanarak elkonulduğu görülmektedir. Bilişim cihazlarına ilişkin düzenlenmiş CMK m.134 tedbiri bu cihazlar bakımından özel hüküm olup, genel hüküm olan CMK m.123' ü uygulamak mümkün değildir¹⁵⁴. Fakat mobil cihazların CMK m.134 tedbiri kapsamında olup olmadığı doktrinde görüş ayrılığı yaşanan bir husustur. Doktrindeki baskın görüş cep telefonları ve bilgisayarların gerek özellik gerek kullanım alanı olarak iç içe geçmesi sebebiyle koruma tedbiri kapsamında sayma eğilimdedir.¹⁵⁵ Aksi görüşte olan yazarlar ise cep telefonlarının tedbir kapsamında değerlendirilemeyeceğini belirtmektedir.¹⁵⁶ CMK m. 134 metninin daha açık bir şekilde düzenlenmesi gerekmektedir, tedbire

¹⁵² Aldemir, s.164-165.

¹⁵³ Ateş Benek, s.401.

¹⁵⁴ Seda Yağmur Sümer, "Ceza Muhakemesinde Telefona/Akıllı Telefona Elkoyma ve Müdahale İmkanları," *İzmir Barosu Dergisi*, 2022:s.105.

¹⁵⁵ Bkz Göksoy, s. 155; Dereboylular Özde, "Bulut Bilişim Bakımından Arama ve Elkoymaya İlişkin Hükümlerin Uygulanabilirliği", *Ceza Hukuku Dergisi*, Yıl:14, Sayı:39, 2019, s. 184; Borekçi Çağrı, "Bilgisayarlar, Bilgisayar Programlarında ve Kütüklerinde; Arama, Kopyalama ve Elkoyma", (Yayımlanmamış Yüksek Lisans Tezi), Bahçeşehir Üniversitesi, İstanbul, 2020, s. 75; Öztürk Bahri/ Kazancı Eker Behiye/ Güleç Soyer Sesim, *Ceza Muhakemesi Hukukunda Koruma Tedbirleri*, Seçkin Yayıncılık, Son Değişikliklerle Güncellenmiş ve Gözden Geçirilmiş 3. Bası, Ankara 2019, s. 202. Benzer görüşte olan Baştürk'e göre; sayısal olarak kaydetme ve işleme yeteneğine sahip bulunan tüm araçlar ve yine bilişim ağı CMK m. 134 kapsamındadır. Bakınız: Baştürk İhsan, "Bilgisayar Sistemleri ile Verilerinde Arama, Kopyalama ve Elkoyma", *Fasikül Hukuk Dergisi*, Sayı:9, Ağustos 2010, s.28. Yine Bostancı/Benzer'e göre;CMK m.134'ün düzenlemenin dijital veri bulunduran tüm cihazları kapsayacak şekilde düzenlenmesi gerekmektedir. Bakınız: Bostancı Ümit/ Benzer Recep, "Türk Hukuk Sisteminde Bilgisayarlar, Arama, Kopyalama ve El Koyma", *International Journal of Human Sciences*, Cilt: 12, Sayı: 2, 2015, s.1222.; Sümer, s.87.

¹⁵⁶ Bkz.Yaşar/Dursun, s. 15-17.; Sümer,s.105.

ilişkin birçok eksiklik bulunmaktadır; adli bilişime ilişkin açıklamalar, tedbirin hangi bilişim cihazlarının kapsadığına ilişkin açıklamalar örnek olarak verilebilir. Tedbirin hangi bilişim cihazlarını kapsadığına ilişkin en azından çatı bir başlık oluşturulması gerekmektedir.¹⁵⁷

9. Arama Kararını Verecek Mercii

Bu tedbirin uygulanabilmesine karar verme yetkisi değişiklikten önce sadece hakimde bulunmaktaydı. 25.7.2018 tarih ve 7145 s. Kanunla değişik CMK m.134/1 gereğince gecikmesinde sakınca bulunan hallerde 134'üncü maddede belirtilen tedbirlere Cumhuriyet savcısı tarafından da karar verilebilmesine imkan sağlanmak suretiyle, delillerin biran evvel elde edilebilmesi ve suçla etkin mücadele edilebilmesi amaçlanarak değişiklik yapıldı.¹⁵⁸ Arama kararını verme yetkisi hakim ve gecikmesinde sakınca bulunan hallerde savcıdadır, kolluk kuvvetlerinin karar verme yetkisi bulunmamaktadır. Savcı tarafından verilen arama kararında, kararın 24 saat içerisinde hakim onayına sunulması şartı aranmaktadır. Hakim bu süre içerisinde karar vermek zorundadır aksi halde çıkarılan kopyalar ve çözümü yapılan metinler derhal imha edilir. Hakimin kararının olumsuz olması ya da süresi içerisinde karar vermemesi hallerinde arama hukuka aykırı hale gelecektir.

10. İtiraz

CMK md. 134 çerçevesinde Cumhuriyet savcısı tarafından verilen kararlara karşı başvuru yolu bulunmamaktadır. Tedbire karşı başvuru yolları, Cumhuriyet savcısının kararının hakim onayına sunulması veya doğrudan hakim tarafından karar verilmesi hallerinde gündeme gelmektedir. Hakim tarafından verilen kararlara karşı da özel bir itiraz usulü mevcut olmayıp, CMK md. 267 ve devamında düzenlenen genel itiraz yapılması mümkündür. CMK m.35 kanunda ayrıca bir düzenleme olmadığı hallerde itiraz usulünü düzenlemiştir, tedbir bakımından da bu hükme dayanarak itiraz yapılması mümkündür. CMK m. 134 bakımından itiraza ilişkin süre bulunmadığından, m.35'te belirtilen kararın öğrenildiği tarihten itibaren yedi gün içinde itiraz edilebilmesi kabul edilmelidir.¹⁵⁹

¹⁵⁷ Sümer, s.109.

¹⁵⁸ Özbek/Doğan/Bacaksız, s.371-372.

¹⁵⁹ Göksoy, s.172.

B. İletişimin Tespiti, Dinlenmesi ve Kayda Alınması

Sayısal delil sadece bilişim sistemlerinde depolanan veya işlenen durağan verilerden oluşmamaktadır. Bilişim sistemleri aracılığıyla işlenen veya saklanan veri, sistemler arasında transfer edilmektedir. Söz konusu transfer esnasında elde edilen verilerin de sayısal niteliği bulunmaktadır.¹⁶⁰ Bu tür verilere akış halindeki veriler denilmektedir.

Durağan verilerin elde edilmesinde CMK m.134'te tedbirinin uygulanırken, akış halindeki veriler için CMK.135'te yer alan tedbir uygulanmaktadır. Akış halindeki sayısal verileri iki grup olarak değerlendirdiğimizde, bunlardan ilki, kişi tarafından üretilen ve iletişim haline geçirilen verilerdir. İkinci grup ise, sistem tarafından üretilen ve ileti haline getirilen verilerdir.¹⁶¹ Bilişim cihazlarında yer alan veriler kişiler tarafından oluşturulabileceği gibi, sistemin kendiliğinden oluşturması da mümkündür.

Bilişim cihazlarından elde edilecek veriler bakımından ilk belirlenmesi gereken verilerin akış halinde mi yoksa durağan halde mi olduklarını saptamaktır. Akış halindeki verilere örnek olarak anlık mesajlaşma uygulamalarından gönderilen mesajlar verilebilir. İletişim sırasındaki mesajlaşmalar için CMK m.135 hükmü uygulanırken, kayıtlı mesajların elde edilmesi için CMK m.134 hükmü uygulanacaktır.¹⁶² CMK m. 135 tedbirinin uygulanması, bilişim sistemine girerek uzaktan arama yapılmasını kapsamaz.¹⁶³ CMK m. 135'in gerekçesinde bilgisayar işlemekte iken içeri girilmesine karşılık, CMK m.135 akış halindeki verileri kişinin bilgisayarına girmek suretiyle ele geçirilmesine olanak tanımamaktadır. CMK m.135 tedbiri ortam dinlemesi, uzaktan arama gibi tedbirleri sağlayan bir madde değildir. Bu tedbir kararıyla yalnızca kişilerin iletişimi dinlenebilir, tespit edilebilir. Uzaktan arama tedbiri Türk hukukunda düzenlenmemiştir, bu sebepten uzaktan erişimle bir bilgisayara girilip arama yapılması hukuka aykırı olacaktır.¹⁶⁴

¹⁶⁰ Değirmenci, s.382

¹⁶¹ Değirmenci, s.383.

¹⁶² Göksoy, s.175.

¹⁶³ Değirmenci, s.384.

¹⁶⁴ Değirmenci, s.384-385.

CMK m.135'te sayılan katalog suçlar arasında bilişim suçları bulunmamaktadır. Bu sebepten tedbirin uygulaması bilişim suçları bakımından mümkün olmayacaktır. Ancak, katalog suçların bilişim cihazları aracılığıyla işlendiği hallerde tedbire başvurmak mümkün olacaktır.¹⁶⁵

C. Cumhuriyet Savcısının Genel Yetkisi

Türk hukukunda bazı sayısal deliller Cumhuriyet savcısının genel delil toplama yetkisi kapsamında elde edilebilecektir. Özellikle diğer koruma tedbirlerinin alanına girmeyen, daha çok üçüncü kişilerde bulunan sayısal ortamdaki veriler Cumhuriyet savcısı tarafından elde edilebilecektir.¹⁶⁶ Bu kapsamdaki verilere örnek olarak sosyal paylaşım sitelerindeki bazı veriler, sayısal kameralardaki veriler, bankalar gibi üçüncü kişilerde bulunan veriler gösterilebilir.¹⁶⁷

VI. Avrupa Konseyi Siber Suç Sözleşmesinde Arama ve Elkoyma

Siber Suçlar Sözleşmesi, vatandaşları siber suçlara karşı korumak için 2001 yılında Avrupa Konseyi tarafından kabul edilen bir anlaşmadır. Siber suçların soruşturulması, kovuşturulması ve cezalandırılmasında üye devletler arasında iş birliği için yasal bir çerçeve ve mekanizmalar sağlar. Sözleşme, dijital teknoloji yoluyla işlenen suçlara ilişkin uluslararası iş birliği için bir model haline geldi, siber suçlardaki artışa ve dijital teknoloji aracılığıyla işlenen yeni suçlardaki artışa doğrudan bir yanıt olarak kabul edildi.¹⁶⁸

Türkiye sözleşmeyi 10 Kasım 2010 tarihinde kabul etmiştir. Sözleşmenin kanun ile uygun bulunması 02.05.2014 tarihinde gerçekleşmiştir. Bu tarihe kadar sözleşme onaylanmadığı için yürürlüğe girememiştir. Resmî gazetede yayımlanmasıyla birlikte

¹⁶⁵ Göksoy, s. 176.

¹⁶⁶ Değirmenci, s.387.

¹⁶⁷ Değirmenci, s.387.

¹⁶⁸ Nasuh Buğra Karadağ, Avrupa Konseyi Siber Suçlar Sözleşmesi: Genel Bakış, < <https://nasuhbugrakaradag.av.tr/avrupa-konseyi-siber-suclar-sozlesmesi-genel-bakis/#:~:text=Siber%20Su%C3%A7lar%20S%C3%B6zle%C5%9Fmesi%2C%20vatanda%C5%9Flar%C4%B1%20siber,bir%20%C3%A7er%C3%A7eve%20ve%20mekanizmalar%20sa%C4%9Flar.>> (E.T.: 06.06.2023).

sözleşme hukukumuz bakımından bağlayıcılık kazanmıştır.¹⁶⁹ Avrupa Konseyi Siber Suç Sözleşmesi'nin uluslararası siber suçlarla mücadele açısından büyük önemi vardır. Elektronik veriler bilgisayarla bağlantılı suçlarda ana bir rol üstlenmektedir. Bu bağlamda, suça yönelik fiillerin tespiti ile suç faillerinin tespit edilmesine yönelik ülkelerarası ortak bir tutum belirlenmiştir.¹⁷⁰

Siber Suç Sözleşmesi'ne baktığımızda, sayısal delillerin elde edilmesine yönelik bazı koruma tedbirlerinin düzenlendiği görülmektedir. Bu koruma tedbirleri;¹⁷¹

- Saklanan bilgisayar verilerinin korunmasının kolaylaştırılması (madde 16),
- Trafik bilgilerinin korunmasının kolaylaştırılması ve kısmen açıklanması (madde 17),
- Üretim talimatı (madde 18)
- Saklanan bilgisayar verilerinin aranması ve bunlara el konulması (madde 19)
- Trafik Bilgilerinin gerçek zamanlı olarak toplanması (madde 20)
- İçerikle ilgili bilgilere müdahale edilmesi (madde 21)¹⁷²

Sözleşmenin 19. Maddesi, bilgisayardaki verilerin arama ve elkoymasını düzenlemektedir. Madde metninde arama yapma yetkisi ulusal sınırlar olarak belirtilmiştir, uluslararası sınırlara çıkılması gereken durumlarda ülkeler arası iş birliği yolunun benimsenmesi gerektiği belirtilmiştir. Madde ayrıca, başka bilgisayarlarda atılı suç bakımından şüphe mevcutsa soruşturmanın bu bilgisayarları kapsayacak şekilde genişletilebilmesine izin vermiştir. Aranılan bilgisayarlara elkonabileceği de ayrıca düzenlenmiştir.¹⁷³

¹⁶⁹ Başlar, s.126-127.

¹⁷⁰ Başlar, s.118.

¹⁷¹ Değirmenci, s.302.

¹⁷² Değirmenci, s.302.

¹⁷³ Başlar, s.124.

VII.Dijital Delillerin Elde Edilmesinin Bazı Temel Hak ve Özgürlüklerle İlişkisi

A. Genel Olarak

Sayısal delil elde etme amacına yönelik bilişim sistemlerinde arama ve elkoyma tedbirleri, Anayasada belirtilen birçok temel hak ve özgürlük ile doğrudan bağlantılıdır. Bilişim sistemlerinde kişisel verilerin saklanması, kişinin özel hayatına ilişkin bilgileri bilişim sistemlerinde bulunmasından dolayı özel hayatın gizliliği hakkı ile bağlantı kurulabilecektir. Bilişim sistemlerinin sadece veri depolamak ve işlemek için değil, veri iletişimi için de kullanıldığı göz önüne alınırsa, bilişim sistemlerinde arama ve elkoyma tedbirinin kişinin haberleşme gizliliğini ihlal edeceği açıkça görülecektir. Kişiler arası haberleşmede bilişim sistemlerinin gün geçtikçe artan kullanımı da bilişim sistemleri arasındaki haberleşmeye müdahaleyi, haberleşmenin gizliliğini ihlale neden olmaktadır. İkinci nesil web sayfalarının gelişmesi, kişilerin bilgi tüketicisi yerine bilgi üreticisi olması, kişilerin web sayfalarının içeriğini belirlemesi kişilerin düşüncelerini toplumun her kesimine açıklaması hakkı ile bağlantılı olarak değerlendirilecektir. Son olarak bilişim sistemlerinde kişiyi tanımlayan verilerin tutulması ve işlenmesi, bilişim sistemlerinde arama durumunda kişisel verilerin usulüne uygun olarak korunması ve kişinin kendi kişisel verileri üzerindeki serbestçe tasarruf hakkı (kişisel verilerin geleceğini belirleme hakkı)'nın ihlaline sebep olabilecektir.¹⁷⁴

B. Özel Hayatın Gizliliği ile İlgisi

Anayasa'nın Özel Hayatın Gizliliği ve Korunması Başlığı altında yer alan özel hayatın gizliliği 20. Maddede düzenlenmiştir. Özel ve aile hayatı gizlidir. Herkes bu haklara saygı gösterilmesini isteme hakkına sahiptir. Bu hak sınırsız bir hak değildir, kanun bazı sınırlamalar getirmiştir. Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin söz konusu olduğu hallerde, bu hak sınırlandırılabilir. CMK m. 134 tedbirinde kişilerin özel ya da iş bilişim aygıtları aranmakta ve el konulabilmektedir. Özel hayatın gizliliğine müdahale teşkil eden bu uygulama gerçekleştirilirken, hakim veya gecikmesinde sakınca bulunan hallerde savcı kararı ile işlem yapılabileceği hüküm altına alınmıştır. Savcı kararını 24 saat içerisinde hakime sunmalı, bu yöndeki karar

¹⁷⁴ Değirmenci, s.89.

ise 48 saat içerisinde verilmelidir. Aksi halde elkoyma kararı ortadan kalkar. Kanun koyucu bu düzenleme ile öncelikle kanunumuzu Avrupa İnsan Hakları Sözleşmesine uygun hale getirmeyi amaçlamıştır. Kişilerin özel hayatını kapsayan eşyalarına el konulmasının süreye bağlanmamış olması ya da bu sürenin hak ihlaline neden olabilecek bir süre olması temel hak ve özgürlüklerle bağdaşmamaktadır.

AİHS’te özel ve aile hayatına saygı hakkı 8. Maddede koruma altına alınmıştır. AİHS madde hükmüne göre, herkes, özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir. Hakkın sınırlandırılma sebepleri, 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 hallerinde uygulanabilmektedir. AİHM, AİHS’e taraf devletlerin bir suça ilişkin delil elde etme amacıyla arama ve elkoyma tedbirine başvurabileceğini kabul etmektedir. Arama ve elkoyma, AİHS’in 8’inci maddesine göre özel hayat hakkına müdahale teşkil etmesine rağmen, söz konusu önlemleri açıklamak için kullanılan nedenlerin ilgili ve yeterli olduğu ve hedeflenen amaca göre orantısız olmadığı durumlarda bir ihlalden de bahsedilemeyecektir. AİHM içtihatları incelendiğinde, aramaların “*yasal*” olması ile “*keyfiliği ve istismara karşı usul açısından yeterli mekanizmalara sahip*” olması hususlarına odaklandığı görülmektedir.¹⁷⁵

Koruma tedbirleri genel olarak hak ve özgürlüklere müdahalede bulunmaktadır. Müdahalenin gerçekleştiği hallerde bakılması gereken husus, bu müdahalenin haklı olup olmadığıdır.

AİHS müdahalenin hukuka uygun olup olmadığı şu şartlar ışığında değerlendirmektedir;

-Müdahale kanunlara uygun mu?

-Meşru bir amacı var mı?

-Demokratik bir toplumda gerekli mi?¹⁷⁶

¹⁷⁵ Değirmenci, s.97;AİHM Funke v. Fransa

¹⁷⁶ Ursula Kilkelly, “Özel Hayat ve Aile Hayatına Saygı Gösterilmesi Hakkı”. İnsan Hakları El Kitapları, no.1,2001, s.14.

<https://inhak.adalet.gov.tr/Resimler/Dokuman/10122019113948ozel_hayat.pdf>. (E.T:02.03.2023).

Bu şartlar bakımından genel değerlendirme yapılacak olursa, müdahalenin kanunlara uygun olup olmadığını ölçmek için dayanılması gereken maddeler başlıca şunlardır, Ceza Muhakemesi Kanunu m.134, Anayasa madde 20, AİHS m.8 ve ilgili yönetmeliklerdir. Ceza Muhakemesi Kanununda bilgisayar, bilgisayar program ve kütüklerinde arama yapılmasına ilişkin bazı öncül kurallar mevcuttur. Bunlar, somut delillere dayanan kuvvetli suç şüphesi ve son çare olma prensibinin yansıması olan başka şekilde delil elde edilememesidir. Bu şartlar, koruma tedbirinin uygulanmasını zorlaştırıcı koşullar olup, keyfiliğin önüne geçmektedir. Bununla birlikte, kararı verebilecek merciler kanunda açıkça belirtilmiştir. Bu mercilerin dışında verilen ya da yapılan tedbirler kanuna uygun olmayacaktır. Delillerin nasıl elde edileceği, imaj alınma zorunluluğu, elde edilen kopyanın şüpheli ve/veya müdafine verilmesi zorunluluğu ilgili maddede düzenlenmiştir. Kanunda belirtilen şartlara uygun olarak yapılan CMK m.134 arama ve elkoyma müdahaleleri hukuka uygun olacaktır. Aramanın ilgili maddesi dışında, Anayasaya da aykırı olmamak zorundadır. Yapılan aramanın temel hak ve özgürlükleri ihlal etmeden gerçekleştirilmesi gereklidir.

Meşru amaç, madde kapsamında maddi gerçeğin ortaya çıkarılması olmaktadır. Bilgisayar, bilgisayar program ve kütüklerinde aramada kişilerin bilişim cihazlarında arama yapılmak suretiyle atılı suç şüphesine ilişkin delil elde etmek amaçlanmaktadır. Deliller, muhakemenin ilerleyişi ve hükmün kurulması bakımından vazgeçilmez bir öneme sahiptir. Fakat bir soruşturma kapsamında olmayan devlet ya da özel kişilerce yapılan dijital delillerin toplanması ve değerlendirilmesi meşru amaca hizmet etmeyecektir. CMK m. 134'te ancak soruşturma aşamasında bu tedbire başvurulabileceği ifade edilmiştir.

Demokratik toplumda gerekli olup olmadığının değerlendirilmesinden anlaşılması gereken temel hak ve özgürlüklere daha az müdahale eden tedbirlerin uygulanması mümkün ise, bunların uygulanması olmaktadır. Teknolojinin gelişmesiyle suç delilleri de dijital bir hal almıştır. Yalnızca bilişim suçlarında değil, diğer suç tiplerinde de mahkumiyet ya da beraat hükmünün kurulabilmesi için dijital delillere ihtiyaç duyulabilmektedir. Genel arama ve elkoyma tedbirleri her olay bakımından yeterli olmayabilmektedir.

C. Kişisel Verilerin Korunması ile İlişkisi

Bilişim teknolojilerindeki gelişmeler sonucunda, geçmişte mümkün olmayan bazı yeni yöntemlerle verilere ulaşmak mümkün hale gelmiştir. Birbirinden bağımsız verilerin bir araya getirilebilmesi, veri madenciliği, veri eşleştirme yöntemleriyle yeni verilerin üretilmesi gibi birtakım gelişmeler günümüzde kişisel verilerin öneminin artması ve bunun doğal bir sonucu olarak korumanın artmasına sebebiyet vermiştir.¹⁷⁷

Kişisel verilerin korunması, Anayasa'nın 20. Maddesi tarafından hüküm altına alınmıştır. 2010 yılına kadar kişisel verilerin korunması bir temel hak olarak Anayasa'da yer almamaktaydı. 2010 yılında yapılan Anayasa değişikliğiyle Anayasa madde 20'ye eklenen 3. fıkrayla, kişisel verilerin korunması ilk kez anayasal güvenceye bağlanmıştır.

Anayasa md. 20/3; *“Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.”*¹⁷⁸

AİHS’de kişisel verilerin korunması madde 8. ile koruma altına alınmıştır. Bir kamu makamı tarafından bir kişinin özel hayatına ilişkin bilgilerin arşivlenmesi, özellikle bu bilgi bir kişinin uzak geçmişini ilgilendiriyorsa veya politik görüşü ifşa eden ve bu itibarla daha yüksek bir koruma seviyesini haklı kılan özel hassas veri kategorileri içerisine giriyorsa AİHS md. 8 anlamında bir müdahale teşkil eder.¹⁷⁹

¹⁷⁷ Anayasa Mahkemesi Kararı, 25.12.2014, E.2014/74, K.2014/201, RG:23.05.2015, s.29364.; Halil Kalabalık, *İnsan Hakları Hukuku*. (Ankara: Seçkin Yayıncılık,2017) s. 462.

¹⁷⁸ Gülay Arslan Öncü, *Özel Yaşama ve Aile Yaşamına Saygı Hakkı Anayasa Mahkemesine Bireysel Başvuru* El Kitapları Serisi- 8.(Strasbourg:Avrupa Konseyi,2019)s.86.<https://www.anayasa.gov.tr/media/5604/ozel_yasam_hakki.pdf> (E.T:21.02.2021).

¹⁷⁹ Avrupa Konseyi,Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi Özel Hayata ve Aile Hayatına, Konuta ve Haberleşmeye Saygı Hakkı, 2019,s.41. <https://www.echr.coe.int/Documents/Guide_Art_8_TUR.pdf> . (E.T: 28.03.2023).

Güvenlik güçlerince belli kişiler hakkında sistematik olarak veri toplanması ve arşivlenmesi, bu veriler kamusal bir yerde toplansa veya sadece kişinin mesleki ya da kamusal faaliyetlerini ilgilendirse dahi, bu kişilerin özel hayatına bir müdahale kapsamında değerlendirilmelidir. Bir kişinin aracına iliştirilen GPS cihazı ile kişinin bulunduğu yerler ve kamusal alandaki hareketleri ile ilgili verinin arşivlenmesi özel hayata müdahale olarak görülmüştür.¹⁸⁰

Kişisel verilerin depolanması ve imhasına ilişkin düzenlemeler yapılmalıdır. Bu hususta Avrupa sözleşmesi 6. Maddesinde düzenlendiği gibi verilerin toplanmasını belirleyen esaslar ortaya konulmalıdır. Kişilerin ırkı, siyasi görüşü, dini ve diğer inançlarını ortaya koyan verilerin toplanması yasaklanmalıdır.¹⁸¹

1. Sosyal Medya ve Kişisel Veriler

Sosyal medya platformu kullanıcısının; sosyal medyada kullandığı adı, müstear adı, cinsiyeti, yaşadığı ülke, yaşadığı şehir, doğum tarihi sevdiği sözler, eklenen şehirler, (hesabın statüsü ve tarihçesi) hoşlandığı ve hoşlanmadığı şeyler, e-posta adresi, (üyelik boyunca kullanılan eskiler ve yeni adresleri) ilişki durumu, iş ve eğitim durumu, (okuduğu okullar ve kurs gördüğü yerler) yaşadığı yer, kişinin kendisi ile ilgili sosyal medya platformuna yüklediği sertifikalar[...] kişinin aktif oturumları sırasındaki sistem tarafından otomatik olarak tutulan tarih, saat, zaman dilimi, cihaz bilgisi, IP adresi,[...] kişinin belirttiği beğeniler, retweetler, ilgi alanları, zaman tüneline koyduğu diğer verilere dayanarak kullanıcıyı hedeflemeye dahil eden konuların listesi,[...], kişinin direct mesaj olarak (DM) sohbette yaptığı konuşmaların geçmişi¹⁸² ve benzeri kişisel veriler, sosyal medya platformlarınınca tutulan ortak verilerdendir.¹⁸³

Sosyal medya şirketleri genellikle cezai ve ulusal güvenlikle ilgili konularda bağlı bulundukları usulü dairesinde talep edilmesi durumunda veri paylaşımında bulunmaktadır. Sunulan bu verilerin her zaman için doğru olması, sosyal medya şirketleri tarafından garanti edilmemektedir. Bunun en önemli sebebi ise bu sosyal

¹⁸⁰ Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi Özel Hayata ve Aile Hayatına, Konuta ve Haberleşmeye Saygı Hakkı, s. 47

¹⁸¹ Kalabalık, s.475.

¹⁸² Yetim, s.299.

¹⁸³ Yetim, s.298.

medya platformlarında tutulan verilerin büyük bir oranının sosyal medya kullanıcıları tarafından sisteme işlenmesi, değiştirilmesi, güncellenmesi veya silinmesidir. Bu verilerin veri tabanına işlenmesi sırasında herhangi bir şekilde, kimlik doğrulama ya da veri güvenliğinin ve veri bütünlüğünün sağlanmasıyla ilgili elektronik imza ya da benzeri herhangi bir teknoloji kullanılmadığı için sosyal medya şirketleri tarafından ibraz edilen bu verilerin doğruluğu ve bütünlüğü garanti edilmemektedir.¹⁸⁴ Bu bakımdan, sosyal medyadan elde edilen delillerin güvenilirliğini saptamak kolay değildir. Değiştirilmiş olma ihtimali delillerin tahrifi sonucunu oluşturacaktır ki bu da yargılamada kullanılamamasına sebebiyet vermektedir. Sosyal medya şirketlerinden talep halinde ya da hakim veya savcının soruşturma aşamasında delil toplamak amacıyla kendiliğinden yaptığı araştırmalarda, aranan delilin yanında, soruşturma ile ilgisi olmayan kişisel verilerin de elde edilmesi mümkün olabilmektedir. İç hukukumuzda, CMK m.134 kapsamında elde edilen verilerin imhası düzenlenmemiştir. Madde hükmünde yalnızca elkonulan cihazların iadesinden bahsedilmiştir. Fakat imaj alma işlemiyle, bilişim cihazlarından içerik kopyası çıkarılmaktadır. Bunlar incelemeyi yapan kollukta kalmaktadır. Kişilere dair bu denli kapsamlı ve detaylı kişisel verilerin içirme ihtimalinin olduğu verilerin imhasının düzenlenmemiş olması eksikliklerdir.

D. Haberleşme Hürriyeti

Haberleşme hürriyeti, Anayasamızın 22'nci maddesinde koruma altına alınmıştır. İlgili madde incelendiğinde, haberleşme hürriyetine vurgu yapmaktan başka haberleşmenin gizliliğinin de altı çizilmiştir. Haberleşme kavramı açıkça posta yoluyla gönderilen gönderileri içermekle birlikte, teknolojik gelişmelere uygun olarak geniş yorumlanmak suretiyle elektronik haberleşmeyi de içermektedir.¹⁸⁵ Haberleşme hürriyeti gerek Anayasamızdaki düzenleniş tarzına gerekse de AİHS'in 8'inci maddesinde düzenleniş tarzına bakıldığında özel hayatın gizliliği kapsamında özel hayatın dokunulmaz alanını oluşturan bir alan iken aynı zamanda da bağımsız bir hak oluşturmaktadır.¹⁸⁶

¹⁸⁴ Yetim, s.320.

¹⁸⁵ Değirmenci, s. 98.

¹⁸⁶ Değirmenci, s. 98.

Teknolojilerde özellikle de elektronik mesajlar (e-postalar), internet kullanımı ve bilgisayar sunucularında saklanan veri, hard diskler ve disketler dahil olmak üzere, Madde 8 kapsamını girer.¹⁸⁷ CMK m.134 kapsamında yapılan arama ve elkoyma tedbirinden elde edilen deliller haberleşme niteliği taşıyabilmektedir. Daha önce belirtildiği üzere, e-postaların durumu durağan veri olması halinde CMK m.134'e girerken, akış halinde olması hallerin de CMK m. 135 hükümleri uygulanmaktadır. E-posta yaygın kullanılan bir iletişim aracı olmakla birlikte, bu iletilere yapılan müdahale haberleşme hürriyeti bağlamında değerlendirilmelidir. Kişinin özel ya da iş hayatına ilişkin e-posta, Whatsapp, Skype vb. iletişim uygulamalarından yapmış olduğu haberleşmenin devlet tarafından dinlenmesi ve tespit edilmesi ihlallere sebebiyet verebilmektedir.

E. İfade Özgürlüğü ile İlişkisi

Bir ülkede demokrasinin anlamına ve kurallarına uygun şekilde yaşanması ve varlığını sürdürmesi ancak çoğunluk düşüncesi dışındaki ifadelere müdahale edilmemesiyle mümkün olabilir. Bireyin bakış açısına Devletin ve çoğunluğun hoşgörüsü, demokratik siyasi sistemin önemli bir dayanağını oluşturur.

AIHM Handyside- Birleşik Krallık davasında (1976) ifade özgürlüğünün niteliklerini şöyle belirtmiştir: “[...] İfade özgürlüğü [...] yalnızca lehte olduğu kabul edilen veya zararsız ya da önemsiz görülen bilgi ve düşünceler için değil, aynı zamanda devletin veya toplumun bir bölümü için saldırgan, şok edici veya rahatsız edici bilgi ve düşünceler için de uygulanır. Bunlar çoğulculuğun, hoşgörünün ve açık fikirliliğin gerekleridir ki; [...]”¹⁸⁸

İfade özgürlüğü her türlü ifadeyi özgürlük kapsamında saymıştır. Hakka yönelik sınırlandırmalar içerik bakımından değildir. AIHM içtihatlarına bakıldığında bu tutumun benimsendiği görülebilir, mahkeme her tür ifadeyi korumaktadır. Bu hakkın kanunlardaki karşılığına bakıldığında da yaklaşımın bu yönde olduğu görülecektir.¹⁸⁹

¹⁸⁷ Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi Özel Hayata ve Aile Hayatına, Konuta ve Haberleşmeye Saygı Hakkı, s.100.

¹⁸⁸ Erkan Tanju, *AIHM Kararları Işığında Basın ve İfade Özgürlüğü*. (Ankara: Seçkin Yayıncılık,2017) s.179-180.

¹⁸⁹ Ulaş Karan, *İfade Özgürlüğü Anayasa Mahkemesine Bireysel Başvuru El Kitapları Serisi-2*. (Ankara:Avrupa Konseyi,2018) s.6.

Anayasa Mahkemesi internetin modern demokrasilerde başta ifade özgürlüğü olmak üzere temel hak ve özgürlüklerin kullanılması bakımından önemli bir araçsal değere sahip bulunduğunu belirtmiştir.¹⁹⁰ Mahkeme'ye göre internet ortamında düşüncelerin paylaşılması daha az maliyete sahiptir bu sebeple daha yaygın kullanıma sahip olmaya başlamıştır.¹⁹¹ İnternetin kendine has bazı özellikleri halkın haber alma özgürlüğünü pekiştirir niteliktedir. İnternetin, belirli bir alan sınırının olmaması, geçmişe yönelik arşiv tutması, geniş kullanıcı ağına ulaşabilmesi gibi özellikleri halkın haberleşme ve haber alma özgürlüğünü kullanmakta araç haline getirmiştir. İnternet sınırları kaldırarak herkesin bu haklara erişebilmesi ve kullanmasına imkan sağlamıştır.¹⁹² Mahkeme internetin ifade özgürlüğünün güvencesi altında olduğunu kabul etmiştir.¹⁹³ Mahkeme'ye göre internet özgürlüğü demokratik toplum için oldukça önemli bir yere sahiptir, bu sebepten kamu makamlarının internete dair düzenlemelerde dikkatli olması gerekmektedir.¹⁹⁴ Kişiler, internet üzerinde hem etkin olarak düşüncelerini paylaşabilmekte hem de başkalarının düşüncelerine ulaşabilmektedir. Kişiye ait bilişim sistemlerinde arama ve elkoyma yapılması kişilerin ifade özgürlüğü ile doğrudan bağlantılıdır. Ayrıca ifade özgürlüğü, kişilerin iletişim aygıtları ile gerçekleştirebilecekleri haklardandır. Akış halindeki veriler üzerindeki müdahalelerin kişilerin düşüncelerini açıklama özgürlüğüne yönelik olduğu açıktır.¹⁹⁵

< https://www.anayasa.gov.tr/media/3545/02_ifade_ozgurlugu.pdf>.(E.T:28.03.2023).

¹⁹⁰ AYM, Yaman Akdeniz ve Diğerleri Kararı, B. No: 3986, 2/4/2014, § 39; Karan, s.54.

¹⁹¹ AYM, Ali Kılık Kararı, B. No: 2014/5552, 26/10/2017, § 55; Karan, s 54.

¹⁹³ AYM, Medya Gündem Dijital Yayıncılık Ticaret A.Ş. Kararı, B. No: 2013/2623, 11/11/2015, § 34; Karan, s 54.

¹⁹³ AYM, Medya Gündem Dijital Yayıncılık Ticaret A.Ş. Kararı, B. No: 2013/2623, 11/11/2015, § 34; Karan, s.54.

¹⁹⁴ AYM, Ali Kılık Kararı, B. No: 2014/5552, 26/10/2017, § 82; Karan,s .54.

¹⁹⁵ Değirmenci, s.102.

ÜÇÜNCÜ BÖLÜM

DİJİTAL DELİLLERİN İSPAT GÜCÜ

I. Genel Olarak

Günümüz ceza muhakemesinde geçerli olan ispat sistemi, ceza muhakemesinin amacına paralel olarak kabul edilen *vicdani delil* sistemidir. Vicdani delil sistemi tabiri, her şeyin delil olarak kabul edilme serbestliğini, hem de delillerin serbestçe değerlendirilmesi serbestliğini ifade eder. Maddi gerçeğin araştırıldığı ceza muhakemesinde, belli hususların belli delillerle ispatı zorunlu tutulmadığı gibi, yargıç da tarafların sunduğu delillerle bağlı ve sınırlı değildir. Bu nedenle ceza muhakemesinde her şey delil olabilir.

Fiziksel delillerin delil olarak kabul edilebilmesi için gerekli özellikler dijital deliller bakımından da geçerlidir. Dijital deliller de tıpkı fiziki deliller gibi, olayı temsil etmeli, sahihliğinden emin olunmalı, akılcı olmalı, hukuka uygun olmalı ve müşterek olmalıdır. Olayı temsil etmeyen bir veri, dijital delil niteliğine haiz değildir, muhakemeye esas alınamaz. Dijital deliller hukuka uygun yöntemlerle elde edilmiş olmalıdır; yasak usullerle elde edilen dijital deliller hükme esas alınamaz. Müşterek olma özelliği ise delillerin mahkeme huzurunda tartışılmış olmasını ifade eder.

II. Dijital Delillerin Kabul Edilebilirlik Şartları

Dijital delillerin ispatının mümkün olabilmesi için hem hukuki hem teknik anlamda bazı şartlar bulunmaktadır. Delillerin muhakemeye esas alınabilmesi için gerekli olan bu şartlar, sahihlik, bütünlüğünün sağlanması, tekrar ele alınabilirlik ve delillerin doğrulanmasıdır. Delillerin değerlendirilme ilkelerinden yola çıkarak oluşturduğumuz bu bölümde dijital delillerin kendine özgü özellikleri bağlamında mahkeme tarafından değerlendirilirken dikkat edilen hususlar üzerinde durulacaktır.

A. Sahihlik

Delillerin değişmemiş, tahrif edilmemiş olması onların sahih bir başka anlatımla orijinalliklerini korudukları anlamına gelir. Dijital deliller yapıları gereği değişmeye, bozulmaya elverişli delillerdir. Delilin şüpheli/sanık tarafından değil, bir başka kişi tarafından oluşturulmuş ya da değiştirilmiş olması ihtimali ispata muhtaç ve yargılama bakımından elzem bir husustur.

Sahihlik, sayısal delilin kabul edilebilirliği kararının verilebilmesi için merkez bir rol üstlenmektedir. Sahihlik bakımından oluşacak şüphe delilin yargılamaya esas alınmamasına sebebiyet verebilmektedir. Sahih olmayan deliller esas alınarak kişi hakkında mahkumiyet kararı verilemez. Yargılama bakımından bu denli hayati olan kriterin doğrulaması, adli bilişim uzmanları tarafından gerçekleştirilmektedir. İlk görüşte orijinal görünen delillerin, adli bilişim uzmanlarınca incelendiğinde, değiştirilmiş oldukları ortaya çıkabilmektedir. Bilgisayarda bulunan bir kaydın kimin tarafından girildiğini, bilgisayarın kaydı işleme alırken doğru çalışıp çalışmadığı ve kayıt eğer çıktı şeklinde ise çıktı ile kaydın aynı olup olmadığı hususları ispata muhtaçtır.¹⁹⁶

Sahihlik incelemesinde değerlendirilmesi gereken birçok etken vardır. Olay- şüpheli bağlantısı, delil-bilişim cihazı gibi ikili bağlantıların gerçekçiliği ortaya konulmalıdır. Bilişim sistemi ile o sistemin sahibi arasında her zaman bir ilişki kurulamamaktadır. Kimi zaman suç işlenen bilgisayar şüphelinin bilgisayarı değil, herhangi bir bilgisayar olmaktadır. Kötücül yazılımlar kullanarak herhangi bir bilişim aygıtının araç olarak kullanıldığı suçlarda, şüpheliyi tespit etmek her zaman mümkün olmamaktadır.¹⁹⁷

B. Dijital Delillerin Bütünlüğü

Elektronik delilin bütünlüğü ilkesi, elektronik delilin ilk andan itibaren gerek fiziki gerek elektronik bakımdan değişime uğramadığını ifade etmektedir.¹⁹⁸ Elektronik delilin bütünlüğünün sağlanması işlemi genellikle kriptografi teknikleri kullanılmak

¹⁹⁶ Değirmenci, s.139.; United States v. Vela, 673 F.2d 86; Karar için bkz.Romano, s.1750.

¹⁹⁷ Değirmenci, s.176.

¹⁹⁸ Başlar,s.94.

suretiyle gerçekleştirilmektedir.¹⁹⁹ Delillerin fiziksel olarak bütünlüğünün korunması, elde edilme aşamasından itibaren fiziksel şartlarının korunmasını ifade eder. Sayısal deliller tahrife, fiziksel delillerden daha fazla açıktırlar. Dijital verilerin dış etkenlerle (ısı, nem, kırılma vb.) geri döndürülemeyecek şekilde yok olma olasılıkları mevcuttur. Bunun yanında failer veya bir üçüncü kişi tarafından değiştirilme, gizlenme veya yok edilme ihtimalleri de bulunmaktadır. Verilerin tahrif edilme olasılığına karşı önlemler alınmalıdır. Dış etkenlerden korunması için, veri depolama aygıtlarının elkonulması ve taşınması sırasında dikkatli davranılmalıdır. Aşırı ısıya ya da nemli ortama maruz bırakılmamalıdır. Dış etkenlerin yanında fail ya da üçüncü kişiler tarafından da delillerin bilerek ya da sehven değiştirilmesi söz konusu olabilmektedir.

Elektronik deliller nitelikleri itibarıyla her zaman itiraza konu edilebilirler. Bu sebeple elde edilen elektronik delilin orijinal hali yapılabilecek bütün itirazları ortadan kaldıracak mahiyette bütünlüğü bozulmadan muhafaza altına alınmalı ve korunmalıdır. Bu şekildeki bir koruma işleminin gerçekleşebilmesi için, elektronik delillerin toplanmasından raporlanmasına kadar geçen süreçte delil koruma zincirine azami derecede riayet edilmelidir.²⁰⁰

A. Tekrar Ele Alınabilirlik

Dijital delilin sübuta etki edebilmesi için tekrar ele alınabilir olması gereklidir. Elde edilen sonucun tesadüfen değil, başka uzmanlarca incelendiğinde de aynı sonucu veriyor olması, doğruluğunun ortaya koyulması açısından gereklidir. Tekrar elde alınamayan bulgular tesadüfen o sonucu vermiş olacağından yargılamada kullanılamaz.

Bu konuda uzman bir kişinin müdahale etmesi, gerektiğinde yöntemleri değiştirmesi, alternatifler uygulaması, çıkan sonuçları kendi aralarında çaprazlama bir şekilde değerlendirme gerekebilecektir. Elektronik delillerin ortaya koyulması işlemleri genelde sosyal bir olayla ilgili kanaat belirtmekten ve sübjektif bir sonuç üretmekten ziyade, objektif ve matematiksel bir yaklaşımla, çoğunlukla, tek doğrusu olan, aynı yöntemlerle aynı sonuna ulaşılan prosedürler içerir.²⁰¹ Elde edilen, ortaya çıkarılan,

¹⁹⁹ Başlar,s.95.

²⁰⁰ Yetim,s.106.

²⁰¹ Yetim, s.109.

görünür belirgin hale getirilen, şifresi çözülen elektronik deliller ile ilgili, delil incelemesinde bulunan uzmanın dışında başka bir uzman da aynı yazılım ve donanımları yahut da alternatif yazılım ve donanımları kullanmak suretiyle aynı neticeyi elde edebiliyor ise delillerin tekrarlanabilir olma özelliğine sahip olduğu, elde edilen neticenin değişken olmadığı, kişilerin bu işlemleri yaptıkları sırada objektif metotlar kullandıkları ve sağlıklı sonuçlara ulaştıkları varsayılacaktır.²⁰²

B. Dijital Delillerin Doğrulanması

Elde edilen delillerin teknik ve hukuki anlamda doğrulanması gerekir. Delilin elde edildiği bilişim cihazının kontrol edilmesi ve şüpheli ile bağlantısının, bilişim cihazının şüphelinin kullandığı ve atılı suçlamanın işlendiği zamanda da şüpheli tarafından kullanıldığı hususlarının doğrulanması gerekir. Toplanan delillerin değiştirilmemiş olması özellikle çok önemlidir. Adli bilişim uzmanlarının titizlikle çalışma göstermesi, adli bilişim aşamalarının kayda alınması sürecin kısmen de olsa denetlenebilmesi için önemlidir. Elektronik delilin doğrulanması için incelemesi ve analizinin yapıldığı laboratuvar ortamının standartlara uygun olup olmadığı hususu ele alınmalıdır.²⁰³

Bazı elektronik sistemler, elektrik kaynağıyla ilişki kesildiğinde önceki bir verinin üzerine yazma işlemi yapabilmektedir.²⁰⁴ Bu tür durumlarla karşı karşıya kalmamak için eğitilmiş adli bilişim uzmanları eşliğinde arama gerçekleştirilmelidir. Arama sırasında CMK'nın 120.maddesinde sayılan kişilerin hazır bulunması, yapılan bütün faaliyetlerin bu kişilerin huzurunda yapılması, gerçekleştirilen her türlü işlemin hiçbir adım atılmaksızın kayıt altına alınması, yapılan işlemlerin resimlerinin çekilmesi, mümkünse video kayıtlarının yapılması, elde edilen delillerin bütün özelliklerinin (marka, model, renk, defo, belirgin diğer vasıfları, kim tarafından kullanılmakta olduğu gibi) kayıt altına alınması, mümkünse olay yerinde adli imaj işlemi tamamlanarak elde edilen delilin özet değerinin olay mahallinde tespit edilmesi gerekir.²⁰⁵

²⁰² Yetim, s.109.

²⁰³ Başlar, s. 96.

²⁰⁴ Karakoyunlu, s.81.

²⁰⁵ Yetim, s.108.

Son olarak delillerin doğrulanması bakımından ele alınması gereken husus ise insanın adli bilişimdeki rolüdür. Adli bilişimde analiz aşamasına kadar işlemler bilgisayarlar tarafından yapılmaktadır. Bilgisayarların yanılma payı oldukça düşüktür, hatalı sonuçları insan eliyle gerçekleştirilen işlemler oluşturmaktadır. Hatalı sonuçların birçok sebebi vardır; uygun tekniklerin kullanılmaması, delillerin değiştirilmiş olması ya da değerlendirmeyi yapan mahkemenin bilgi yetersizliği örnek olarak verilebilir.²⁰⁶ Bu tür hatalarla karşılaşmamak için eğitimli adli personellerin yetiştirilmesi ve bu alanda kullanılması gerekmektedir. Yapılan işlemler kaydedilmeli ve rapor olarak mahkemeye sunulmalıdır.

III.Dijital Delillerin Doğrudanlık Problemi

Doğrudanlık ilkesi, delilin mahkeme önüne getirilip tartışılması anlamına gelmektedir. CMK m.217’de doğrudanlık ilkesi ele alınmıştır; “*Hâkim, kararını ancak duruşmaya getirilmiş ve huzurunda tartışılmış delillere dayandırabilir. Bu deliller hâkimin vicdanî kanaatiyle serbestçe takdir edilir.*” Doğrudanlık, yargılamayı yapan hakimin olay hakkındaki kanaatini şekillendirme süreci ile ilgili bir ilkedir. Bu ilke gereğince yargılamayı yapan hakim veya mahkeme; delil, sözlü ise dinleyecek, yazılı ise okuyacak, eşya veya iz şeklinde ise görecektir. Ancak bu şekilde elde edilen ve değerlendirilen deliller hükme esas alınabilecektir.²⁰⁷ Ceza yargılamasında maddi gerçeğe ulaşma zorunluluğu muhtemel deliller arasında daima en iyisinin tercih edilmesini gerektirir. En güvenilir yol olayı olabildiğince kaynağından yani ilk elden öğrenmektir. Olayı bizzat yaşamamış olan yargılama makamı olay hakkında zaten dolaylı olarak bilgi sahibi olmaktadır. Maddi gerçeğe ulaşmak açısından hadiseye olabildiğince yakın bağlantısı olan, dolaylılığı en az düzeyde bulunan delillerin kullanılması gerekir. Örneğin, mahkeme, bir trafik kazasıyla ilgili olarak trafik kaza tespit tutanağını düzenleyen kişiyi tanık olarak dinlemek yerine mahallinde keşif yapmalıdır.²⁰⁸

²⁰⁶ Göksoy, s.178.

²⁰⁷ Doğan Gedik, *Ceza Muhakemesinde İspat ve Şüphenin Sanık Lehine Yorumlanması*. (Ankara: Adalet Yayınevi,2022) s.46.

²⁰⁸ Gedik, s.48

Dijital delillerin doğrudanlığını ele aldığımızda, delillerin aslının mahkeme önüne getirilmesi her zaman mümkün olmadığını görmekteyiz. Dijital delillerin bir kısmı yardımcı araçlarla görüntülenebilirken, bir kısmının aslının mahkeme önüne getirilmesi mümkün olmamaktadır. Bu durum delillerin dolaylılığını arttıran bir faktör olarak karşımıza çıkmaktadır. Dijital deliller yapıları gereği soyut özellikte olduklarından bu delillerin görüntülenebilmesi için vasıta bazı araçlara gereksinim duyulmaktadır. Monitör, yazıcı vb. araçlarla bu deliller mahkeme tarafından değerlendirilebilecektir.

Asıllarının mahkeme önüne getirilememesi ise incelemenin delilin aslı üzerinden yapılmamasındandır. Dijital deliller adli bilişim aşamasından geçerken, delilin aslı değil adli kopyası alınmaktadır. Asıl delilin bozulmasının önüne geçmek için inceleme işlemleri adli kopya üzerinden gerçekleştirilmektedir. Mahkeme önüne getirilen delil aslında delilin aslı değil, adli kopyası olmaktadır. Dijital delil bir görüntü kaydı olduğunda, bu delil mahkeme tarafından izlenebilir ve delilin aslı dolaylı da olsa mahkeme tarafından değerlendirilmiş olur. Fakat bilişim cihazlarından yapılan mesajlaşmalar ya da bilgisayarlara yüklenen zararlı yazılımlar gibi deliller mahkeme önüne getirilememekte, bunların ya bir kopyası ya da metin haline getirilmiş hali mahkemeye sunulmaktadır.

Dijital delillerde bir diğer dolaylılık hali ise, delillerin adli bilişim sürecinden geçerek mahkeme önüne gelmesidir. Bilişim sisteminde yer alan özellikle belirti niteliğindeki delillerin soruşturma aşamasında savcılık, kovuşturma esnasında ise mahkeme tarafından incelenmesi ve değerlendirilmesi çoğu zaman mümkün olmayacaktır. Bilişim sisteminde yer alan verinin, işlendiği iddia edilen suçun delili olup olmadığı, delil niteliğinde ise doğru ve inanılır olup olmadığı hususlarının tespiti için teknik bilgiye ihtiyaç duyulabilecektir. Bilişim sisteminde bulunan verinin çıkarılarak, olayı temsil ediciliğinin özel ve teknik bilgiyi gerektirdiği durumlarda, söz konusu teknik bilgiye savcı veya yargıç her zaman sahip bulunamayacaktır.²⁰⁹ Bu durumda ilgili delilin değerlendirilmesi için teknik bilgisi ve uzmanlığı ile yargıca yardımcı olacak bilirkişilerden²¹⁰ yararlanılabilecektir

²⁰⁹Değirmenci, s.402.

²¹⁰ Değirmenci, s.402.

Görüşümüz, müşterekliği ihlal etmeyecek ölçüde, maddi gerçeğin ortaya çıkmasına yardımcı olacak delillerin asıllarının getirilmesi mümkün olmadığı hallerde getirilen kopyaların değerlendirmeye esas alınmaması gerektiği yönündedir. Adli kopyalama işlemi birebir kopya sağladığından, adli uzmanlar tarafından cihazlar üzerinden alınan imajlar aslıyla aynı sayılma eğilimindedir. Nitekim Değirmenci adli bilişim aşamalarında birebir kopya alınıp bunun üzerinden işlem yapıldığı için, belgenin orijinalini yani aslının bir önemi kalmadığını ifade etmektedir.²¹¹ Yardımcı araçlar vasıtasıyla görüntülemeye her ne kadar dolaylılık artsa da delillere erişebilmek ancak bu halde mümkün olduğundan daha dolaysız bir yöntem bulunana kadar bu yöntemin benimsenmesi zorunlu gözükmektedir. Dolaylı bir şekilde mahkeme huzuruna getirilen kopyaların adli kopya olmasına dikkat edilmeli, adli kopya dışındaki kopyaların ise nasıl elde edildiğine göre değerlendirme yapılmalıdır.

A. Ekran Görüntüsü

Uygulamada hakaret, tehdit, şantaj veya özel yaşamın ihlali suçları son yıllarda yoğunlukla facebook, Twitter gibi sosyal paylaşım siteleri üzerinden ya da elektronik postalar aracılığıyla işlenmekte, suçun mağduru da şikayet dilekçesine genellikle buna dair (örneğin facebooktaki hesabın ekran görüntüsünü içeren) bir çıktıyı eklemekte, bu çıktı esas alınarak facebook profilinin sahibi görünen kişi şüpheli olarak dinlenmekte, hakkında dava açılabilir. ²¹²

Ekran görüntüsü, görüntü sergileme aracı olan monitör/ ekran vasıtasıyla bireylere ulaşan ışık demeti yansımasıdır. Ekrandaki bu görüntünün siber ortamda sayısal olarak anlık birebir nüshasının alınması işlemine ise “ekran görüntüsü almak/ yakalamak” (=printscreen, screenshot) denmektedir. Başta bilgisayar olmak üzere birçok elektronik cihaz (örneğin akıllı telefonlar) bir ekrana sahiptir. Bu ekrana yansıyan görüntü ve siber ortamdaki veri karşılığı aslında başlı başına bir çıktıdır(=output). Ekran görüntüsü çıktılarını ikiye ayırarak incelemek gerekir. ²¹³

²¹¹ Değirmenci, s.140.

²¹² Gedik, s.140.

²¹³ Gedik, s.140.

Bunlardan ilki, ekran görüntüsü sayısal çıktılardır. Işık demeti yansımasıyla oluşan ve ekrana yansıyan anlık görüntülere ekran görüntüsü dijital/ sayısal çıktısı adı verilmektedir. Herhangi bir işleme tabi tutulmayan bir bilgisayarda masaüstü görüntüsü bile aslında arka planda çalışan programlar nedeniyle ve halihazırda bir görüntüyü yansıttığı için çıktı sayılmaktadır. Ekran görüntüsü dijital/ sayısal çıktıları geçici olduklarından ve o an itibariyle ekran görüntüsünün videoya kaydedilmesi veya ekran görüntüsünün yakalaması yapılmadığı sürece tekrar edilebilir nitelikte değildir. Bu nedenle de ceza muhakemesinde ispat aracı olmak için zayıftırlar.²¹⁴

Bir diğer ekran görüntüsü çıktı türü ise ekran görüntüsü fiziki/yazıcı çıktılarıdır. Bunlar, ekrandaki görüntünün yakalanması ve fotoğraf çekilmesi sonrasında bir yazıcı yardımıyla görüntünün kağıt vb. materyal üzerine yazdırılmasıdır. Bazen bu çıktı bir web sitesinin o andaki görüntüsü olabilmektedir. Bir web tarayıcısı açıkken doğrudan fiziki çıktı alınması halinde URL linki ve çıktı tarihi, fiziki çıktı üzerinde yazmaktadır. Fakat bu bilgilerin fiziki çıktı üzerinde yer alması yeterli değildir; ek deliller ile URL linkinin ve URL linkine bağlı adreste bulunan görüntünün doğrulanması gerekmektedir.²¹⁵

IV.Delil Türleri Bakımından İspat

Dijital belgenin hangi delil türü olduğuna göre ispat bakımından gücü değişecektir. Dijital delil ses ve görüntü kaydeden araçlardan elde edilmiş ise, bu delillerin mahkeme önünde dinlenmesi ya da izlenmesi mümkün olabilmektedir. Örneğin bir suç anına yönelik kamera kaydını hakim izleyerek bu konuda karar verebilecektir. Öğretideki baskın görüş, ses veya görüntü kayıtları olan delillerin, tek başına hüküm vermek için yeterli olmadığına yöneliktir.²¹⁶

²¹⁴ Gedik, s.140.

²¹⁵ Gedik, s.140.

²¹⁶ Değirmenci, s.395.

Dijital delil belirti olabilir. Sistemde yer alan suçun işlendiğine ilişkin kayıtların belirti delili olduğunu ifade edebiliriz.²¹⁷ Sistemde yer alan günlük kayıtları, bir suçun işlendiğini veya kimin tarafından işlendiğini çoğu zaman doğrudan ortaya koymamaktadır. Hatta bilişim sistemine bir kullanıcı kodu ile ulaşıldığı, söz konusu kayıtların ilgili kullanıcı tarafından kaydedildiğinin sistem tarafından teyit edilmesi durumunda bile, suç failinin doğrudan kullanıcı kodunun sahibi olduğu ileri sürülemeyecek, diğer delillerle desteklenmesi gerekecektir.²¹⁸

Ve son olarak, elde edilen dijital delil bir belge delili olabilir. Sosyal medya üzerinden gerçekleştirilen DM’ler, paylaşımlar, elektronik posta aracılığıyla gerçekleştirilen konuşmalar suç unsuru içerebilmektedir. Her dijital delilde bakılması gereken sahlilik durumu belge delilleri bakımından da geçerlidir. Bu tür belgeler değıştirilebilir ve silinebilir nitelikte olmakla birlikte tahrife aşıktırlar. İmaj alınırken bu delillerin hash değeri kontrol edilmelidir. Asıl belge yapılacak olan değışikliğin imajı ya da belgenin çıktısından anlaşılabilmesi zor olup, belgenin güvenilirliğini zarara uğratabilecektir.

B. Dijital Delillerin Güvenilirliğinin Sağlanması

1. Hash Değeri

Hash değeri hesaplama işlemi belli bir verinin belli bir algoritmaya göre verdiği sonuçtur. İmajı alınan donanımın delil niteliğinin bozulmadığı ve elde edilen imaj dosyasının kesinliği “hash değeri”²¹⁹ hesaplanarak ortaya koyulur. Bu sonuç verideki en ufak bir değışiklikte değışecektir ve elde edilen sonuç benzersizdir(unique). İmajı alınan donanımdaki bütün verilerin hash değeri, imaj dosyasının hash değeri ile eşleştğinde delil bütünlüğünden ve doğrulamasından bahsedilebilir.²²⁰ Hash değeri karşılaştırılarak üzerinde inceleme ve analiz yapılan imajın değışip değışmediği kontrol edilir.²²¹ Hash değerine ilişkin dijital delillerin DNA’sı şeklinde benzetmeler yapılmaktadır.²²²

²¹⁷ Değirmenci, s.393.

²¹⁸ Değirmenci, s.393.

²¹⁹ Akarslan, s. 126.

²²⁰ Akarslan, s. 127.

²²¹ Karakoyunlu, s.112.

²²² Dölger, *Bilişim Suçları ve İnternet İletişim Hukuku*, s.688.

Hash değerinin doğruluğu adli bilişim uzmanının raporundaki ve sabit diskin imajının alındığı sırada oluşan hash değerinin karşılaştırılmasıyla sağlanmaktadır. Bu iki değer aynı olmaması halinde, yapılan analize itiraz edilebilecektir. Rapordaki ve imaj alınırken oluşan hash değerinin aynı olmaması sonucunda bu durum elde edilen delillerin geçerliliğini de etkileyecektir. Hash değerinin bir diğer kullanım alanı dosya eşdeğerliği karşılaştırmasıdır. Bu yöntem özellikle çocuk pornografisine ilişkin soruşturmalarda, daha önceden özet değeri bilinen çocuk pornografisine ilişkin görüntülerin şüphelinin bilgisayarında olup olmadığı veya şüpheli tarafından dağıtılıp dağıtılmadığının kontrolünde kullanılmaktadır.²²³

Uygulamada hash değerine dair bazı aksaklıklar yaşanabilmektedir. Bu aksaklıkların sebebi, hash değerinin gereğince takip edilmesinin ihmal edilmesi ve kontrol sağlanmamasındandır. Bazen delillerin elde edilmesi ve imaj alma işlemleri sırasında kolluk birimleri tarafından elde edilen ve rapora işlenen hash değerinin, bilirkişi raporunda yer alan hash değerinden farklı olduğu durumlarla karşılaşmaktadır. Bu durum, bilirkişinin incelemiş olduğu imajın gerçeğinden farklı olduğu ve imaj üzerinden elde edilen bulguların adli bilişim açısından delil değeri taşımadığı tartışmalarına yol açacaktır.²²⁴ Bu açıklamalardan sonra belirtilmelidir ki, karşılaştırılan hash değerlerinin aynı çıkması doğrudan verinin değiştirilmediği anlamına gelmemektedir.²²⁵

2. Üst Veri Bilgisi

Üst veri bilgisi, gömülü veri veya meta verisi, kullanıcının doğrudan görmediği verileri açıklayıcı bilgiler taşıyan sistem bilgileridir. Dijital delillerin yazıcıdan çıktı şeklinde alınması delili tam olarak yansıtmamasına sebep olacaktır; delil üzerindeki üst veri çıktıda gözükmeyeceğinden inceleme sırasında üst veri bilgisine erişim mümkün olmayacaktır. ²²⁶Bu veriler bir fotoğrafın çekildiği tarih ya da yer (GPS)kaydı veya elektronik postanın gelirken izlediği güzergah gibi çok çeşitli bilgileri içerebilirler. Veriler aynı zamanda dosyanın güvenliği açısından da tutulabildikleri için, dosyanın değiştirilip değiştirilmediği veya hangi bilgisayarda hazırlandığı gibi bilgileri

²²³Değirmenci, s.251.

²²⁴Başlar, s. 216.

²²⁵ Irmak Erdoğan, “Ceza Muhakemesi Hukunda İspat Konferansı,” *İstanbul Barosu*, <https://www.youtube.com/watch?v=7hl1pxgKwEQ>, (E.T: 01.05.2023).

²²⁶ Çekiç, s.157.

içerebilirler.²²⁷ Microsoft Office Word dosyaları üstveri bilgisi olarak dokümanı kullanan son 10 kullanıcıya ait bilgiler içerir. Benzer şekilde PDF (portable document format) dosyaları, hangi yazılım ile nasıl (Office dosyasının çevrilmesi-convert gibi) ve nerede (Macintosh üzerinde gibi) oluşturulduğu bilgisine sahiptir. JPEG dosyaları ise fotoğrafın çekildiği makineye ait marka ve model bilgisini içerir.²²⁸

3. Elektronik İmza

Elektronik imzanın kişiye münhasır olması sebebiyle delil doğrulama yöntemi olarak karşımıza çıktığını görmekteyiz. Elektronik imza sahibinin, kimliği, imzanın geçerliliği ve doğruluğunu göstermektedir. Belge niteliğindeki sayısal delillerin, belge sahibi ile ilişkisinin kurulması güçtür. Özellikle güvenli elektronik imza ile sayısal belgeyi oluşturanın tespit edilemediği durumlarda, belge sahibi konusunda ceza yargıcında bir şüphe oluşacaktır.²²⁹ Belgenin bir başkası tarafından oluşturulduğu iddiasında bu iddianın da aydınlatılması gerekmektedir. Dijital deliller dijital ortamda bulunduğundan, fiziksel deliller gibi el yazısı ile karşılaştırmak mümkün olmayacaktır.

Elektronik imza, imzalanacak verinin imza sahibi dışında değiştirilememesi yönünde güvence sağlamaktadır. Her elektronik imza kendine özgü niteliktedir. Elde edilen verilerin hangi tarihte kim tarafından imzalandığı ya da belgede bir değişiklik yapıldıysa bunu kimin tarafından yapıldığı noktasında elektronik imzadan yararlanılmaktadır.

4. Delil Zinciri

Delilin elde edildiğinden itibaren delil takip formuna yapılan işlemlerin işlenmesi işlemine delil zinciri ya da koruma zinciri denilmektedir. Koruma zinciri hem dijital delil hem de dijital delilin bulunduğu bilişim cihazıyla ilişkili bir kavramdır. Bu sebeple koruma zincirinin yalnızca dijital delillere ilişkin değil, aynı zamanda delilin elde edildiği cihaza da uygulanması gereklidir.²³⁰

²²⁷ Hüseyin Çakır ve Mehmet Serkan Kılıç, *Adli Bilişim ve Elektronik Deliller*. (Ankara:Seçkin Yayıncılık,2014)s.150.

²²⁸ Çakır/Kılıç, s.152.

²²⁹Değirmenci, s.134.

²³⁰ Başlar, s.221.

V.Dijital Deliller ile Tek Başına Mahkûmiyet Kararı Verilebilme

Dijital delillerin orijinalliği ve güvenilirliği uygulamada çokça karşımıza çıkan bir problemdir. Dijital delillerin kim tarafından, ne zaman oluşturulduğu, oluşturulduğundan bu yana değişikliğe uğrayıp uğramadığını ilk bakışta tespit etmek mümkün olmamaktadır. Dijital verilerin tek başına mahkumiyet kararına esas olamamalarının altında yatan neden budur; dijital delillerin güvenilirlikleri tespit edilemediğinde yan deliller, dijital delili güvenilir hale getirmektedir. Yan deliller ile bütüncül bir değerlendirme yapılması muhakeme açısından daha sağlıklı olacaktır.²³¹

Yargılamadaki tek delilin dijital delil olduğu hallerde, bu delilin güvenilirliğin teyit edilmesi, en ufak bir şüphe halinde sanığın beraatine karar verilmesi gerekmektedir. Bu yaklaşımın altında yatan ilke şüpheden sanık yararlanır ilkesidir. Şüphenin sanık aleyhine yorumlandığı hallerde, şüphelinin masum olması durumunda cezalandırılması söz konusu olmaktadır. Nitekim Yargıtay şüphelinin tereddüde mahal vermeyecek şekilde suçu işlediğine yönelik bir belirleme yapılması gerektiğine karar vermiştir.²³²

Doktrinde dijital deliller ile tek başına mahkumiyet kararı verilemeyeceğini savunanlar olduğu gibi,²³³ tek başına mahkumiyet kararı verilebileceğini savunanlar²³⁴ da mevcuttur. Dijital delillerin yargılamada tek başına mahkumiyete esas olamayacağına ilişkin görüşlerde ortak olan, delillerin tahrif edilme olasılıkları yani sahilikleri üzerinden olmaktadır. Yargıtay bir kararında, *“Dijital delilin yapısı gereği manipülasyona açık olduğu bilinmektedir. Diğer delil türlerine göre özellik arz eden bazı yönleri olmakla birlikte dijital delil de sonuçta, deliller hiyerarşisinin kabul edilmediği, delil serbestisinin benimsendiği ceza muhakemesi sistemimizde bir ispat aracıdır. İspat aracı olan delilin değerlendirilmesinde, Ceza Muhakemesi Hukuku'nda bir delil için öngörülen nitelikleri taşıyıp taşımadığı nazara alınıp, genel olarak; somut olayın özellikleri, yüklenen suçun işleniş biçimi, dosyadaki diğer deliller gibi*

²³¹ Arslan, s.263.

²³² Arslan, s.263.; Yargıtay 13. CD, 14.01.2013, 2011/28624, 2013/172

²³³ Özbek, Veli Özer. “Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi”, *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, Cilt. 59, Sayı. 1-2, (2001): s. 185-186. Kızılyar, Murat. “Ceza Yargılamasında Dijital Verilerin Delil Değeri”, *Adalet Dergisi*, Sayı. 50, (Eylül 2014): s. 79; Benzer şekilde bkz. Arslan, s. 263.; Orta, Mesut. “Bilişim Suçlarında İspat”, 1. Polis Bilişim Sempozyumu, Ankara, 21-22 Ekim 2003:s. 290.

²³⁴Sarsıkoğlu, 444.

*hususlar gözetilip, özel olarak da; delilin temsil ettiği olayın niteliği, ele geçiriliş yeri, şekli ve zamanı, bu delilin sair karakteristik özellikleri gibi hususlar göz önünde bulundurulmalıdır.”*²³⁵ delillerin manipölasyonlara açık nitelikte oluşunun ispat aracı olarak değerlendirilmesinin önüne geçmemesi gerektiğini belirtmiştir.

Hukukumuzda sahih olmayan delillerin tek başına mahkumiyete esas olmadıkları gibi delil olarak da kullanılmaları mümkün değildir. Usulüne uygun elde edilmiş hukuka uygun delillerin bu anılan şüpheleri taşımadığı varsayılırsa, bu delillerin tek başına mahkumiyete karar verememesine ilişkin engel de kalkmış olacaktır²³⁶

VI.Hukuka Aykırı Deliller

Hukuka aykırı deliller, hukuka aykırı yöntemlerle elde edilmiş delillerdir. Hukuka aykırılık, temel hak ve özgürlükler (işkence, insanlık dışı müdahale) bakımından olabileceği gibi, usul hükümlerine aykırılıklar da (imaj almadan bilgisayarda arama yapılması) olabilecektir. Hukukumuzda hukuka aykırı deliller kullanılamaz, karara esas alınamaz. Öyle ki mahkeme verdiği kararda, hangi delillerin hukuka aykırı olduğunu belirtmek zorundadır. Bu durum hukuk güvenliğini tesis etmektedir. Hüküm, verilen kararın hukuka aykırı bir delile dayandırılmamış olduğunu alenileştirmektedir.

CMK m.134 bakımından incelemede öncelikle ele alınması gereken hukuka aykırılık imaj almadır. Adli imaj kopyası, sayısal delilin güvenilirliğini sağlamak için gereklidir. İmaj alınmadan arama yapılması hukuka aykırı olacaktır. Adli kopya alınmaksızın arama yapılması halinde asıl veriler üzerinde işlem yapılmış olacaktır. Asıl veriler üzerinde işlem yapılması o delilin değişikliğine sebebiyet verecek, güvenilirlikleri ortadan kalkmış olacaktır. Adli kopyalarının şüpheli ve müdafine verilmemesi de yine tedbiri hukuka aykırı hale getirecektir.

²³⁵ Başlar, “Elektronik Delil ve Ceza Yargılamasında Kabul Edilebilirliğine İlişkin Bir İnceleme,” s.1678-1679.; Yargıtay 9. CD. 09.10.2013, E. 2013/9110, K. 2013/12351.

²³⁶ Başlar, “Elektronik Delil ve Ceza Yargılamasında Kabul Edilebilirliğine İlişkin Bir İnceleme,” s.1678.

Madde de yer alan Cumhuriyet savcısının yetkisi sınırsız bir yetki olmayıp, yalnızca gecikmesinde sakınca bulunan hallerde mevcuttur. Bu yetki devrinin yapılmasında hukuka uygun davranılması gereklidir aksi halde yapılan arama ve elkoyma hukuka aykırı hale gelebilecektir. Ayrıca bu yetkiye sahip Cumhuriyet savcısının da kararını 24 saat içerisinde hakim onayına sunması gereklidir. Hakimin 24 saat içerisinde karar vermesi gerektiğine dair düzenleme açıktır, hakim belirtilen süre içerisinde karar vermediği takdirde elde edilen kopyalar ve metinler imha edilmek zorundadır. Bu hükme uyulmaması halinde elde edilen deliller hukuka aykırı hale gelecektir.

A. Zehirli Ağacın Meyvesi Doktrini ve Dijital Deliller

Zehirli ağacın meyvesi doktrininin çıkış noktası, hukuka aykırı elde edilen deliller kullanılmak suretiyle ya da bu deliller sayesinde elde edilen ikincil nitelikte delillerin yargılamada kullanılıp kullanılmayacağı sorununun çözümünü bulma isteğidir.²³⁷ Doktrindeki baskın görüş, hukuka aykırı arama, elkoyma, sorgu, ifade gibi işlemler ile elde edilen delilleri hukuka aykırı saymakla birlikte, hukuka aykırı işlem neticesinde ulaşılan diğer delilleri de hukuka aykırı saymaktadır. Yapılan ilk hukuka aykırı işlem ağacın gövdesini, elde edilen diğer deliller ise meyvelerini temsil etmektedir.

Bu yaklaşım Anglosakson sisteminde benimsenmiş olup, Kıta Avrupası sisteminde de uygulandığı ülkeler mevcuttur. Anglosakson sisteminde zehirli ağacın meyvesi doktrini olarak yer alan yaklaşımın amacı “kolluk güçlerini disipline alma”, Kıta Avrupa’sındaki hukuka aykırı delillerin uzak etkisindeki amaç ise “temel hak ve özgürlükleri korumaktır.” Anglosakson sisteminde kolluğu disipline alma amacını taşıyan yaklaşım, Amerika Birleşik Devletlerindeki polislerin aşırı güç kullanımları sonucu haklarında dava açılmasını önlemek için benimsenmiştir. Polisin hukuka aykırı yöntemlerle elde ettiği deliller muhakemede kullanılırsa, polis bu eylemlerine aynen devam edecek bu durum da kişilerin hak ihlallerine sebebiyet verecektir. Delillerin dışlandığı halde ise, polisin delili elde ederken harcadığı tüm çaba boşa gideceğinden bu yöntem ile polisi hukuka aykırı müdahaleden uzak tutmak amaçlanmıştır. Kıta Avrupa’sında daha çok bireysel haklar önem arz ettiğinden bireysel olarak kişileri

²³⁷ Hamid Köse, “Delil Değerlendirme Yasakları Bakımından Zehirli Ağacın Meyvesi Doktrini,” *Türkiye Adalet Akademisi Dergisi*.2022:s.168.

korumak amacıyla dışlama kuralı uygulanmaktadır. Sistem kişinin temel hak ve özgürlüklerini merkeze alarak, kişinin haklarının ihlal edilerek elde edilen delilleri dışlar.²³⁸

AİHM'in bu yöndeki önemli kararlarından olan Gäfgen v. Almanya'da mahkeme yasak yöntemlerle elde edilen delilleri dışlarken, türev delilleri dışlamamış ve bu delillerle karar verilmesini AİHS m.6 'ya aykırı bulmamıştır. Mahkeme delillerin kabul edilebilirliğinin değerlendirmesini ulusal mahkemelere bırakmakla, ulusal mahkemenin kararlarının keyfi olup olmadığını ve ikrar delilinin güvenilirliğinin değerlendirmesinde mahkemelerin sağladığı güvencelerin yeterli olup olmadığını denetlemiştir.²³⁹ Mahkeme türev delillerin dışlanmasına ilişkin kamu ve mağdur menfaati dengesini gözetmektedir. İkincil nitelikteki delillerin dışlanması halinde kamu ve mağdurun zarar göreceğinden bahisle bu delilleri hukuka aykırı olarak kabul etmemektedir.²⁴⁰ AİHM bu kararında zehirli ağacın meyvesi de zehirlidir doktrinini benimsememiştir.²⁴¹

Hukukumuzda ise, hukuka aykırı delillerin kullanılamayacağına ilişkin birçok düzenleme mevcuttur (AY. m.38/6, CMK m.148,217/2,206/6,289/1-i). AY m. 38/6 ve CMK m. 217/2 karşısında delillerin elde edilişi sırasında herhangi bir şekilde hukuka aykırılığın yapılmış olması, söz konusu delillerin hükme esas alınmasına kesin bir şekilde engeldir.²⁴² Hukuka aykırı delillerle birlikte, türev deliller de dışlanmaktadır. Yargıtay hukuka aykırı delillerin uzak etkisini kabul ettiği bir kararında; "*Hukuka aykırı şekilde elde edilen dolayısıyla ulaşılan deliller, ister hukuka aykırı, isterse hukuka uygun yolla elde edilsin, hukuka aykırı delil olacaktır. Öğretide baskın görüşün bu yönde olduğunu görüyoruz. Bu duruma 'hukuka aykırı delilin dolaylı etkisi, uzak etkisi' ya da 'zehirli ağacın meyvesi de zehirlidir' denilmektedir.*" Bu kararın tam tersi yöndeki Yargıtay'ın hukuka aykırı delillerin uzak etkisini kabul etmediği kararları da mevcuttur.²⁴³

Dijital delillerin elde edilmesinde kullanılan arama ve elkoyma tedbirlerinin hukuka aykırı olması halinde, bu arama ve elkoyma sonucu elde edilen deliller de hukuka

²³⁸ Güçlü Akyürek, "Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu," *TBB Dergisi* 2012: s. 65.

²³⁹ Dülger, *Ceza Muhakemesi Hukukunda Dışlama Kuralı ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağacın Meyvesi Öğretisi)*. (Ankara:Seçkin Yayıncılık,2014) s.105.

²⁴⁰ Pınar Palabıyık, "İşkence Tehdidi ile Ulaşılan Maddi Bulguların Delil Olarak Değerlendirilmesine İlişkin Avrupa İnsan Hakları Mahkemesi Karar Tahlili (Gäfgen v. Almanya)," *İstanbul Aydın Üniversitesi Hukuk Fakültesi Dergisi*, 2016:s.194.

²⁴¹ Palabıyık,s.188.

²⁴² Metin Köse, "Amerikan Ceza Muhakemesi Hukukunda Hukuka Aykırı Delillerin Dışlanması," *Hacettepe Hukuk Fakültesi Dergisi*, 2019:s.181.

²⁴³ Yargıtay 19. CD. 09.11.2015. E.2015/12122, K.2015/6823, Yargıtay 7. CD. 24.02.2010 E.2007/10087, K.2010/6022.

aykırı olacaktır. Elde edilen deliller sayesinde ulaşılan türev delillerin de hukuka aykırı olup olmadığını değerlendirmek gereklidir. Görüşümüz elde edilen türev delillerin de hukuka aykırı olacağı yönündedir. Hukuka aykırı deliller muhakeme tarafından kabul edilmiyor ise zaten bu hukuka aykırı delil sayesinde elde edilen deliller de hukuka aykırı olacaktır.

Mahalin dışında yapılan aramalarda, arama laboratuvarında gerçekleşmekte, yerinde arama gibi şüpheli, müdafii olay yerinde bulunmamaktadır. Olay yerinin dışında yapılan bu incelemelerin güvenilirlikleri oldukça düşüktür. Denetim mekanizması olmadan bilişim cihazları üzerinde inceleme yapılmaktadır. Bu gibi denetimin olmadığı hallerde yapılan incelemeler sonucu elde edilen deliller hukuka aykırı olabileceği gibi, bu deliller ile ulaşılan diğer türev delillerin de muhakemede kullanılamamasına sebebiyet verebilecektir.

VII.Tesadüfen Elde Edilen Deliller

Tesadüfen elde edilen deliller, devam etmekte olan bir soruşturma esnasında ya da soruşturmanın tamamlanması ve iddianame tanzim edilmesi ile geçilen kovuşturma aşamasında başvurulmuş koruma tedbirlerinin uygulanması ile ele geçirilen ve dava konusu bir suç dışında başka bir suçun da işlendiğini gösteren delillere verilen isim olarak adlandırılmaktadır. Kısaca bir delilin soruşturma ya da kovuşturma konusu başka bir suçun işlenmesiyle ya da başka bir suçun işlendiği şüphesini ile elde edilen deliller, arama, el koyma, iletişimin dinlenmesi ve iletişimin kayda alınması koruma tedbirlerinin uygulanması sırasında elde edilen deliller, tesadüfen elde edilmiş delillerdir.

5271 sayılı Ceza Muhakemesi Kanunu'nda Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi başlığı altında ve 138. Maddesinde olan tesadüfen elde edilen deliller hüküm altına alınmıştır.²⁴⁴

²⁴⁴ Madde 138 – (1) Arama veya elkoyma koruma tedbirlerinin uygulanması sırasında, yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan ancak, diğer bir suçun işlendiği şüphesini uyandırabilecek bir delil elde edilirse; bu delil muhafaza altına alınır ve durum Cumhuriyet Savcılığına derhâl bildirilir. (2) Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi sırasında, yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan ve ancak, 135 inci maddenin altıncı fıkrasında sayılan suçlardan birinin işlendiği şüphesini uyandırabilecek bir delil elde edilirse; bu delil muhafaza altına alınır ve durum Cumhuriyet Savcılığına derhâl bildirilir.

CMK m.134 tedbirini gerçekleştiren uzmanlar, soruşturma konusu suç hedef olarak işlemlerini gerçekleştirmelidir.²⁴⁵ Nitekim, uzmanların yetkili hale getiren arama kararı olup, kararda fiil ve dayanağı da açıkça belirtilmiştir.²⁴⁶ Arama sırasında atılı suçun dışına çıkılmamalı, keyfi bir şekilde soruşturma genişletilmemelidir. Tesadüfen elde edilen deliller sebebiyle soruşturmayı genişletmek yapılan işlemleri hukuka uygun hale getirmemektedir.²⁴⁷

Başka bir suç işlendiği yönündeki şüphe halinde, eğer tesadüfen bir delil elde edilmiş ise, sadece bu delilin değerlendirilmesi yapılmalıdır. Tedbirin öngörülen şartlar dahilinde gerçekleştirilmesi sırasında başka suçların da işlenmiş olabileceği şüphesini doğuran delillere ulaşılması halinde, aramanın tedbir konusu araçlar dışında da uygulanmaya başlaması ya da kopyalama işleminin tüm verileri içerecek şekle dönüştürülmesi, aramaya adeta bir keşif araması niteliği kazandıracak, temel hak ve özgürlüklere hukuka aykırı bir müdahale teşkil edeceği gibi artık elde edilen delillerin tesadüfiliğinden de bahsedilemeyecektir.²⁴⁸ Sınırlı ve ölçülü bir uygulamanın benimsenmemesi halinde, tedbirin, suç soruşturmasının dışına kayması ve delillerin hukuka aykırı hale gelmesi muhtemeldir.²⁴⁹

²⁴⁵ Karakoyunlu, s.181.

²⁴⁶ Karakoyunlu, s.181.

²⁴⁷ Başlar, s.181.;

²⁴⁸ Karakoyunlu, s.181.

²⁴⁹ Başlar, s.181.

SONUÇ

Her yönüyle ele almak istediğimiz dijital deliller, sayısal ortamda bulunan verilerden oluşmaktadır. Delil olma özellikleri değerlendirildiğinde bu delillerin hukuka uygun bir şekilde elde edilmiş, akılcı, olayla bağlantılı, müşterek olduğu durumlarda delil olma vasfını taşıdıklarında şüphe yoktur. Fakat bu delillerin tek başına hüküm kurmak için yeterli olmadığı, diğer delillerle desteklenmesi gerektiği doktrinde baskın olan görüştür. Bu delillerin kendine özgü yapısı, elde ediliş tarzlarını etkilemektedir. Dijital delillerin istenen sonuçları verebilmesi için öncelikle adli bilişim kısmının düzenlenmesi gerekmektedir. Eğitimli uzmanların bu aşamayı gerçekleştirmesi, her aşamada detaylı bir şekilde yapılan işlemlerin raporlanması, adli bilişim aşamasının şeffaf olması için önem arz etmektedir. Ayrıca, hakim ve savcının bu aşamaya daha etkin katılımı, elde edilen delilleri güvenilirliği açısından önemlidir. Adli bilişim uzmanlarının delilleri değerlendirirken hangi metodolojiyi tercih ettiği de hazırlanan raporlarda belirtilmelidir.

Bilişim suçları ve bilişim yoluyla işlenen suçlarla etkin mücadele için kanuni düzenlemeler gereklidir. CMK 134 hükmü bu koruma tedbirini düzenlemekle birlikte, kanunda boşluklar mevcuttur. Dijital delillerin öne çıkan özellikleri kolayca tahrif olabilme ve güvenilirlik problemidir. Kolayca tahrif olmanın önüne geçmek için alanında uzman kişiler tarafından delillerin elde edilip, muhafaza altına alması gereklidir. Bu delilleri değerlendirme yetkisi CMK’da savcıya verilmişse de bu eksik bir düzenlemedir. Delillerin elde ediliş aşamasından raporlanması aşamasına kadar hakim ve savcının etkin bir şekilde bulunması gerekmektedir. Gerekli yasal düzenlemelerle birlikte, denetimin yoğunlaştırılması gerekmektedir. Düzenlenen tek denetim hash değeri bakımından olmaktadır. Alınan imaj üzerindeki hash değeri ile inceleme sonucundaki hash değeri karşılaştırılarak sağlama yapılmaktadır. Bu yöntem hata payına sahip bir yöntemdir. Delilin elde edilmesi arama, aleni ve denetlenebilirken, en az onun kadar önemli olan adli bilişim aşaması kullanılan adli bilişim metodolojileri bir giz olarak kalmaktadır. Bu durumun düzeltilmesi gereklidir.

Mahallinden uzakta yapılan aramaların istisna olmaktan çıkıp neredeyse kural haline gelmiş olması uygulamanın hatalı olduğunu gözler önüne sermektedir. Elkoyma şartlarına uyulmaksızın, keyfi olarak bilişim sistemlerine elkonmaktadır. Bu durum hukuka aykırıdır, kanun elkoyma hallerini düzenlemiştir. Uygulayıcıların da bu kurallara riayet ederek hareket etmesi gerekmektedir.

Bir başka eksiklik ise CMK m.134 açısından dır. Madde metninde elde edilen delillerin kopyalarının imha edilmesiyle ilgili bir düzenleme bulunmamaktadır. Nitekim m.135 bakımından elde edilen deliller yönünden ayrı bir kanun maddesi bulunurken, bu tedbir bakımından olmaması eksiklik dır. Kişisel verilerin devlet tarafından tutulması kanunlara bağlanmış, temel hak ve özgürlükler açısından değerlendiriliyorken, bu düzenlemenin kanunlarımızda düzenlenmemiş oluşu temel hak ve özgürlükleri ihlal eder niteliktedir. Kopyası alınan bilişim cihazlarının kopyalarının durumunun belirsiz oluşu hukuka aykırı bir durum arz etmektedir. Bu eksikliğin en kısa sürede yasa koyucular tarafından giderilmesini temenni ediyoruz.

Sonuç olarak, çalışmamızda sayısal delillerin nitelikleri, elde ediliş yöntemleri, Türk Hukukundaki karşılığı, ispat bakımından değeri irdelenmiştir. Sayısal delillerin kendine özgü özelliklerinin bilinerek, yapılan işlemlerin bu hususlar gözetilerek yapılması gereklidir. Fiziki delillerden ayrı koruma ve muhafaza etme şekline sahiptirler. Dijital delillerin zayıf yönleri, özgü özellikleri bilinirse, bu delillerin muhakemeye katkısının olma olasılığı daha fazla olacaktır. Nitekim, bu tür deliller kolayca bozulabilir, bu bozulma da muhakeme bakımından hiçbir sonuç vermemelerine sebebiyet verir. Muhakemede sayısal delillerin kullanılabilmesi için çok dikkatli bir şekilde korunmalı, şüpheli veya üçüncü kişilerin değıştirme, yok etme olasılıklarına karşı kısa bir sürede soruşturma aşamasında arama işlemi yapılmalıdır. Bu delillerin korunmasında büyük görev adli bilişim uzmanlarına düşmektedir. Adli bilişim uzmanları, delilin toplanması aşamasından raporlama aşamasına kadar dikkatli ve titiz bir süreç yürütürlerse, delilin hem bozulma olasılığı ortadan kalkacaktır hem de muhakemede kullanılabilecektir. Aslında delilin ispat bakımından değeri ifade etmesi için adli bilişim uzmanının yaptığı çalışma hayati öneme sahiptir. Adli bilişim uzmanının hakime sunmuş olduğu raporla birlikte artık hukuki süreç başlamaktadır. Dijital delillerin elde edilmesinde yararlanılan tedbirler, koruma tedbirleri olmaları sebebiyle temel hak ve özgürlükleri sınırlar niteliktedir. Burada dikkat edilmesi

gereken, orantılılığa uygun bir şekilde tedbirlerin uygulanması ve hak ihlaline sebebiyet vermemek için tedbir ve hak arasında denge sağlanmasıdır.

Son olarak, dijital delillerin ispat bakımından değeri eserde tartışılmıştır. Elde edilen delillerin hukuka aykırılıkları halinde, diğer hukuka aykırı deliller gibi geçersiz olacak ve yargılamaya esas alınmayacaktır. Genel kanaat dijital delillerin tek başına mahkumiyet kararı vermeye yeterli delil olamayacağı yönündedir. Bu durumun bir sebebi, delillerin değiştirilmiş olma ihtimalidir. Bu hususu ele almak yerinde olsa da yaklaşım şekli hatalıdır. Dijital delilin doğruluğu ve bütünlüğü üzerinde bir şüphe mevcutsa bu onun delil olma niteliğini etkileyen bir husustur. Fakat doktrindeki baskın görüş, bütünlüğü şüpheli delilleri delil olarak kabul etmekle birlikte, mahkumiyet kararı vermek için şüpheli bulmaktadır. Dijital delillerin tek başına hükme esas olmaması için herhangi bir kanun ya da hukuki ilke mevcut değildir. Her olay bakımından ayrı değerlendirme yapıldığından bu tür bir yaklaşım muhakeme açısından her zaman sağlıklı sonuç vermeyecektir. Olay bakımından değerlendirme yapılmadığında, delilin sahliliğinden emin olunduğu hallerde, dijital delilin tek başına hükme esas olabilecektir.

KAYNAKÇA

- Akbal, Erhan ve Şengül Doğan. «SIM Kartların Dijital Delil Olarak İncelenmesi ve Analizi.» *Karaelmas Fen ve Mühendislik Dergisi*, 2017: 364-374.
- Aktaş, Batuhan. «Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Tedbiri Üzerine Bir İnceleme.» *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi*, Şubat 2017: 211-239.
- Akyürek, Güçlü. «Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirmesi Sorunu.» *TBB Dergisi*, 2012: 61-82.
- Aldemir, Hüsnü. *Adli-Önleme Arama ve Elkoyma*. Ankara: Adalet Yayınevi, 2019.
- Apiş, Özge. «Güncel Yargı Kararları ve Yasa Değişikliği Işığında İfade Alma ve Sorgu Sırasında Şüpheli/Sanığın Hakları.» *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, Haziran 2019: 53-85.
- Araalan, Çetin. «Türk Hukukunda Dijital Deliller.» *GSI Articleletter*, 2015: 203-212.
- Arslan, Çetin. «Dijital Delil ve İletişimin Denetlenmesi.» *CHKD*, 2015: 253-266.
- Aydın, Devrim. *Ceza Muhakemesinde Deliller*. Ankara: Yetkin Yayınları, 2015.
- Ayhan, Zeynel Abidin. «Ceza Muhakemesinde Dijital Deliller.» *Yüksek Lisans Tezi*. Ankara: Atılım Üniversitesi, 2022.
- Başlar, Yusuf. *Ceza Yargılamasında Elektronik Deliller*. Ankara: Yetkin Yayınları, 2016.
- . «Elektronik Delil ve Ceza Yargılamasında Kabul Edilebilirliğe İlişkin Bir İnceleme.» *LHD*, 2018: 1655-1688.

- Benek, Neslihan Ateş. «Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma.» *Ceza Hukuku ve Kriminoloji Dergisi*, 2022: 367-411.
- Birtek, Fatih. *Ceza Muhakemesinde Delil ve İspat*. Ankara: Adalet Yayınevi, 2017.
- Bucak, Yeşim. «Adli Bilişim ve Türk Ceza Hukukunda Bilgisayarda Arama.» *Yüksek Lisans Tezi*. İstanbul: Üsküdar Üniversitesi, 2019.
- Centel, Nur ve Hamide Zafer. *Ceza Muhakemesi Hukuku*. İstanbul: Beta Basım Yayıncılık, 2021.
- Çakır, Hüseyin ve Mehmet Serkan Kılıç. *Adli Bilişim ve Elektronik Deliller*. Ankara: Seçkin Yayıncılık, 2014.
- Çekiç, Burak. «Bilgisayar Verilerinde Arama, Kopyalama, El Koyma Tedbirinin Hukuki Niteliği ve Benzer Kavramlar.» *NKÜ Hukuk Fakültesi Dergisi*, 2021: 153-186.
- Çetin, Muhammet Sefa. *Kovuşturma Evresinde Belge Delillerin İkamesi ve Değerlendirilmesi*. Ankara: Seçkin Yayıncılık, 2021.
- Değirmenci, Olgun. *Ceza Muhakemesinde Sayısal (Dijital) Delil*. Ankara: Seçkin Yayıncılık, 2014.
- Dülger, Murat Volkan. *Bilişim Suçları ve İnternet İletişim Hukuku*. Ankara: Seçkin Yayıncılık, 2023.
- . *Ceza Muhakemesi Hukukunda Dışlama Kuralı ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağacın Meyvesi Öğretisi)*. Ankara: Seçkin Yayıncılık, 2014.
- Erdoğan, Irmak. «Dijital Delillerin Karşılaştırılmalı Hukukta Değerlendirilmesi.» *Ceza Muhakemesinde İspat Konferansı*. İstanbul: İstanbul Barosu, 2023.
- Eryılmaz, Mesut Bedri. *Ceza Muhakemesi Hukuku Dersleri*. Ankara: Seçkin Yayınları, 2012.
- Gedik, Doğan. *Ceza Muhakemesinde İspat ve Şüphenin Sanık Lehine Yorumlanması*. Ankara: Adalet Yayınevi, 2022.
- Göksoy, Resul. *Ceza Muhakemesinde Dijital Delillerin Elde Edilmesi ve Güvenilirliğinin Sağlanması*. Ankara: Seçkin Yayıncılık, 2019.

- Gürel, Begüm ve İpek Mengilli. «Dijital Delil Kavramı ve Uygulamadaki Yeri.» *Leges Hukuk Dergisi*, 2021: 78-108.
- Henkoğlu, Türkay. *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi*. İstanbul: Pusula Yayıncılık, 2014.
- Henkoğlu, Türkay ve Özgür Külçü. «Bilgi Erişim Platformu Olarak Vulut Bilişim: Riskler ve Hukuksal Koşullar Üzerine Bir İnceleme.» *Bilgi Dünyası*, 2013: 62-86.
- Kalabalık, Halil. *İnsan Hakları Hukuku*. Ankara: Seçkin Yayıncılık, 2017.
- Karakoyunlu, Mert. *Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri*. İstanbul: Legal Yayıncılık, 2022.
- Karan, Ulaş. *İfade Özgürlüğü Anayasa Mahkemesine Bireysel Başvuru El Kitapları Serisi-2*. Ankara: Avrupa Konseyi, 2018.
- Kilkelly, Ursula. *Özel Hayat ve Aile Hayatına Saygı Gösterilmesi Hakkı*. 2001.
- Konseyi, Avrupa. *Avrupa İnsan Hakları Sözleşmesi Madde 8 Rehberi Özel Hayata ve Aile Hayatına, Konuta ve Haberleşmeye Saygı Hakkı*. 2019.
- Köse, Hamid. «Delil Değerlendirme Yasakları Bakımından Zehirli Ağacın Meyvesi Doktrini.» *TAAD*, 2022: 165-202.
- Köse, Metin. «Amerikan Ceza Muhakemesi Hukukunda Hukuka Aykırı Delillerin Dışlanması.» *Hacettepe Hukuk Fakültesi Dergisi*, 2019: 159-195.
- Öncü, Gülay Arslan. *Özel Yaşama ve Aile Yaşamına Saygı Hakkı Anayasa Mahkemesine Bireysel Başvuru El Kitapları Serisi-8*. Strasbourg, 2019.
- Özbek, Veli Özer, Koray Doğan ve Pınar Bacaksız. *Ceza Muhakemesi Hukuku*. Ankara: Seçkin Yayınları, 2022.
- Özen, Muharrem ve Gürkan Özocak. «Adli Bilişim, Elektronik Deliller ve Bilgisayarda Arama ve Elkoyma Tedbirinin Hukuki Rejimi.» *Ankara Barosu Dergisi*, 2015: 43-77.
- Öztürk, Bahri, Durmuş Tezcan, Mustafa Ruhan Erdem, Özge Sırma Gezer, Yasemin Filiz Saygılar, Esra Alan, Özdem Özaydın, Efser Erden Tütüncü, Derya Altınok

Villemın ve Mehmet Can Tok. *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku*. Ankara: Seçkin Yayınları, 2022.

Palabıyık, Pınar. «İşkence Tehdidi ile Ulaşılan Maddi Bulguların Delil Olarak Değerlendirilmesine İlişkin Avrupa İnsan Hakları Mahkemesi Karar Tahlili(Gäfgen v. Almanya).» *İstanbul Aydın Üniversitesi Hukuk Fakültesi Dergisi*, 2016: 173-197.

Parlar, Ali, Mustafa Öztürk. *Ceza Yargılamasında Arama ve Elkoyma*. İstanbul: Aristo Yayınevi, 2019.

Rafael FERNÁNDEZ DE PAIZ, Jesús Ángel SUÁREZ RAMOS. *Dijital Delillerin Değerlendirilmesi*. Eğitim, Intra, 2020.

Sarsıkoğlu, Şenel. «Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı.» *TAAD*, Temmuz 2015: 427-454.

Soyaslan, Doğan. *Ceza Muhakemesi Hukuku*. İstanbul: Yetkin Yayıncılık, 2020.

Sümer, Seda Yağmur. «Ceza Muhakemesinde Telefona/Akıllı Telefona Elkoyma ve Müdahale İmkanları.» *İzmir Barosu Dergisi*, Ocak 2022: 61-119.

Şahin, Cumhur ve Neslihan Göktürk. *Ceza Muhakemesi Hukuku-2-*. Ankara: Seçkin Yayıncılık, 2021.

Şahin, Cumhur. «Ceza Muhakemesinde Bilgisayarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma(CMK m.134).» *Yaşar Hukuk Dergisi*, 2019: 271-286.

Tanju, Erkan. *AİHM Kararları Işığında Basın ve İfade Özgürlüğü*. Ankara: Seçkin Yayıncılık, 2017.

Tezcan, Durmuş, Mustafa Ruhan Erdem, Oğuz Sancakdar ve Rıfat Murat Önok. *İnsan Hakları El Kitabı*. Ankara: Seçkin Yayıncılık, 2021.

Tezcan, Durmuş, Özge Sırma Gezer, Yasemin Filiz Saygılar Kırıt, Elif Altınok Çalışkan, Esra Alan, Özdem Özaydın, Efser Erden Tütüncü, İdris Güzel, Nilüfer Köker, Derya Altınok Villemın ve Mehmet Can Tok. *Dijital Ceza Muhakemesi Hukuku*. Ankara: Seçkin Yayıncılık, 2022.

Tuncel, Aynur. «Delillerin Doğrudan Doğrualığı ve Dijital Deliller.» *Ceza Muhakemesinde İspat Konferansı*. İstanbul: İstanbul Barosu, 2023.

Yaşar, Osman ve Cengiz Otacı. *Yeni İctihatlarla Uygulamalı ve Yorumlu Ceza Muhakemesi Kanunu 1.Cilt*. Ankara: Seçkin Yayıncılık, 2022.

Yenisey, Feridun ve Ayşe Nuhoğlu. *Ceza Muhakemesi Hukuku*. Ankara: Seçkin Yayınları, 2022.

Yetim, Servet. *Ceza Muhakemesi Hukuku Kapsamında Sosyal Medyadan Elektronik Delil Toplama ve Değerlendirme (Facebook Örneği)*. Ankara: Seçkin Yayıncılık, 2016.

