TÜRKİYE CUMHURİYETİ

ANKARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

KAMU HUKUK ANABİLİM DALI

CEZA MUHAKEMESİNDE DİJİTAL DELİLLER

DOKTORA TEZİ

DANIŞMAN

Doç.Dr. Güneş OKUYUCU ERGÜN

HAZIRLAYAN

Khalil AFANDAK

ANKARA-2021

TÜRKİYE CUMHURİYETİ

ANKARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

KAMU HUKUK ANABİLİM DALI

CEZA MUHAKEMESİNDE DİJİTAL DELİLLER

DOKTORA TEZİ

DANIŞMAN

Doç.Dr. Güneş OKUYUCU ERGÜN

HAZIRLAYAN

Khalil AFANDAK

ANKARA-2021

TÜRKİYE CUMHURİYETİ

ANKARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

KAMU HUKUK ANABİLİM DALI

CEZA MUHAKEMESİNDE DİJİTAL DELİLLER

Doktora Tezi

Tez Danışmanı: Doç.Dr. Güneş OKUYUCU ERGÜN

Tez Jürisi Üyeleri

Adı ve Soyadı	İmzası
Prof. Dr. Muharrem ÖZEN	**.....**
Prof. Dr. Devrim GÜNGÖR	**.....**
Doç. Dr. Güneş OKUYUCU ERGÜN	**.....**
Doç. Dr. EzgiAygün EŞİTLİ	**.....**
Doç. Dr. Önder TOZMAN	**.....**

Tez Sınavı Tarihi: 26/08/2021

TÜRKİYE CUMHURİYETİ ANKARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Bu belge ile, bu tezdeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplanıp sunulduğunu beyan ederim. Bu kural ve ilkelerin gereği olarak, çalışmada bana ait olmayan tüm veri, düşünce ve sonuçları andığımı ve kaynağını gösterdiğimi ayrıca beyan ederim.(……/……/2021)

KHALIL AFANDAK

İÇİNDEKİLER

İÇİNDEKİLER ..... **İ**
ŞEKİLLER ve TABLOLAR LİSTESİ ..... **İV**
KISALTMALAR LİSTESİ ..... **V**
GİRİŞ **1**

BİRİNCİ BÖLÜM
CEZA MUHAKEMESİNDE DELİL KAVRAMI

I. CEZA MUHAKEMESİNDE İSPAT VE DELİLLER **5**
A. İspat ve Delil Kavramı 8
B. Delillerin Özellikleri 16
1. Gerçekçi Olması 21
2. Akla Uygun Olması 21
3. Olayı Temsil Edici Olması 22
4. İspat Bakımından Önemli Olması 23
5. Hukuka Aykırı Olmaması 23
6. Müşterek Olması 24
7. Erişilebilirlik 25
C. Delil Çeşitleri 26
1. Beyan Delilleri 29
2. Belge Delilleri 33
3. Belirtiler 35
4. Dijital Veriler 37
II. CEZA MUHAKEMESİNDE DELİLLERİN DEĞERLENDİRİLMESİNİN TARİHSEL GELİŞİMİ: MUHAKEME SİSTEMLERİ VE İSPAT SAFHALARI **43**
A. Muhakeme Sistemleri 45
1. İtham Sistemi 45
2. Tahkik Sistemi 46
3. Karma Sistem (İşbirliği) 47
B. Delil Safhaları 48
1. Erken Safha 48

2. Kanuni Safha 49
3. Vicdani Kanaat Safhası 50
4. Bilimsel Safha 51

İKİNCİ BÖLÜM
DİJİTAL DELİL

I. BİLİŞİM KAVRAMI VE BİLİŞİM YOLUYLA ELDE EDİLEN VERİLER.. 52
A. Kavram ve Tanımlar 52
B. Bilişim Yoluyla Elde Edilen Veriler 59
1. Dijital Veri Kavramı 59
2. Dijital Verilerin Delil Olarak Kullanılması 69
C. Dijital Veri ve Dijital Belge Kavramları 81
II. DİJİTAL VERİLERE ERİŞEBİLMEK AÇISINDAN BİLİŞİM SİSTEMİNDE KULLANILAN CİHAZLAR 86
A. Bilgisayar Sistemleri 86
B. Bilgisayarı Oluşturan Unsurlar 88
1. Mikroişlemci- CPU 88
2. Dahili Bellek (İnternal Memory Storage) 90
a. RAM 91
b. ROM 93
c. Çevre Giriş-Çıkış Birimleri 94
C. El Bilgisayarları 96
D. Dijital Verilerin Depolandığı Cihazlar 97
E. Veri Depolama Cihazlarının Hash Değeri 101
F. İnternet Sistemleri 104
1. İnternetin Tarihi Gelişimi 104
2. İnternetin Teknik Yapısı 107

ÜÇÜNCÜ BÖLÜM
CEZA MUHAKEMESİNDE DİJİTAL DELİLLERİN ELDE EDİLMESİ VE DEĞERLENDİRİLMESİ

I. DELİLLERİN ELDE EDİLMESİ VE DEĞERLENDİRİLMESİ 112
II. DİJİTAL DELİLLERİN ELDE EDİLMESİ VE DEĞERLENDİRİLMESİ 121

A. Ceza Muhakemesi Çerçevesinde Dijital Delillerin Kabul Edilebilirliği Meselesi 121
B. Dijital Delillerin Doğrulanması ve Dijital Delillere İlişkin Hukuki Kurallar .. 126
1.Türk Ceza Muhakemesi Kapsamında Dijital Delillerin Elde Edilmesine İlişkin Kurallar 127
a. CMK 134. Maddenin İncelenmesi 128
b. AİHM'in Bilgisayar Aramalarına İlişkin Kararları 135
c. Bilgisayarlarda Yapılacak Aramalar Sonucu Elde Edilecek Tesadüfi Deliller 140
d. CMK 134. Madde Kapsamında Getirilen Hukuki Düzenlemeye Aykırılık 143
e. İletişimin Denetlenmesi Yoluyla Dijital Delil Elde Edilmesi..... 146
f. Teknik Araçlarla İzleme Tedbiri Yoluyla Dijital Delil Elde Edilmesi..... 158
g. Cumhuriyet Savcısının Genel Soruşturma Yetkisi Çerçevesinde Elde Edilen Dijital Deliller 161
2.Yabancı Hukuk Sistemlerinde Dijital Delillere İlişkin Kurallar 163
3.Dijital Delillere İlişkin Uluslararası Kurallar 169
III. ..... TÜRK CEZA MUHAKEMESİ KAPSAMINDA DİJİTAL DELİLLERİN DEĞERLENDİRİLMESİ 172
A. Dijital Delillerin Hukuki Geçerliğinin İncelemesi 173
B. Delil Değerlendirme İlkeleri..... 176
1.Delillerin Re'sen İncelenmesi 176
2. Delillerin Doğrudan Doğruya İncelenmesi..... 177
3. Delillerin Serbestçe Değerlendirilmesi..... 179
4. Delillerin Bütün Olarak Değerlendirilmesi 182
5. Şüpheden Sanığın Yararlanması..... 184
6. Delillerin Doğrulanması İlkesi 186
7. Delillerin İnkar Edilmemesinin İncelenmesi..... 187
8. Delillerin Tekrar ele Alınabilirliği..... 188
9. Delillerin Doğruluğu İlkesi..... 189
C.CMK KAPSAMINDA DİJİTAL DELİLLERİN DEĞERLENDİRİLMESİ..... 190
SONUÇ 207
KAYNAKÇA.....213
ÖZET 236
ABSTRACT 237

ŞEKİLLER ve TABLOLAR LİSTESİ

Şekil 1. Mikroişlemci ve bölümleri 90

Şekil 2. Bilgisayarlardaki Salt Okunur Bellek (ROM), EPROM ve EEPROM 94

Şekil 3. Bilgisayar Giriş ve Çıkış Birimleri..... 95

Şekil 4. El Bilgisayarı 96

Şekil 5. USB Bellek Çeşitleri 99

Şekil 6. Hanelerde ve bireylerdeki bilgisayar kullanımı ve internet erişim oranları 106

Tablo 1. Dijital Delil Değerinin Belirlenmesi 72

KISALTMALAR LİSTESİ

AİHS : Avrupa İnsan Hakları Sözleşmesi

AİHM : Avrupa İnsan Hakları Mahkemesi

BM : Birleşmiş Milletler

CMK : Ceza Muhakemesi Kanunu

CMUK : Ceza Muhakemeleri Usulü Kanunu

HMK : Hukuk Muhakeme Kanunu

HSYK : Hakimler ve Savcılar Yüksek Kurulu

HSK : Hakimler ve Savcılar Kurulu

k.k : kabul edilemezlik kararı

m.d : madde

MSB : Milli Savunma Bakanlığı

OHAL : Olağan Üstü Hal

Para : paragraf

RG : Resmi Gazete

TBMM : Türkiye Büyük Millet Meclisi

TCK : Türk Ceza Kanunu

TMK : Türk Medeni Kanunu

YCGK : Yargıtay Ceza Genel Kurulu

TDK :Türk Dil Kurumu

GİRİŞ

Dijital delil, elektronik veya manyetik ortamları tarafından iletilen veya kaydedilen bir suçun bilgilerine denilmektedir. Elektronik delillerin ilgili birimlere sunulması ile beraber ise dijital delillendirme oluşmaktadır. Dijital deliller çok farklı türlerde ortaya çıkmaktadır.

Dijital delillerin fiziksel diğer delillerden farklı yönleri uygulamada bazı sorunları da beraberinde getirmektedir. Bu sorunların başında bu delillerin güvenilirliğine ilişkin soru işaretleri gelir. Dijital verilerde değişiklik, silme ve yenisini oluşturma gibi işlemler çok hızlı ve kolay bir şekilde yapılabilmektedir. Bu nedenle bu delillerin bütünlüğünü sağlamak oldukça zordur. Bu çerçevede Ceza Muhakemesinde dijital delillerin delil değeri de bu çalışmanın önemli ayaklarından birini oluşturur. Ceza muhakemesinde delillerin güvenilirliğinin sağlanması açısından benimsenen kurallar da çalışmanın yine önemli bir bölümünü oluşturmaktadır. Bu bağlamda bu çalışma, 5271 sayılı Ceza Muhakemesi Kanunu ağırlıklı olacak şekilde, dijital delillere ilişkin muhakeme kurallarını ele almaktadır.

Türk Ceza Muhakemesi açısından dijital delillerin elde edilmesi yöntemlerine işaret eden mevzuat 5271 sayılı Ceza Muhakemesi Kanunu ve kanunun uygulanmasına yönelik olarak çıkarılmış yönetmeliklerdir. Bu çalışma da bu mevzuat kapsamında dijital delillerin elde edilmesi, korunması ve değerlendirilmesine ilişkin bir çerçeve çizme amacı taşımaktadır.

Bu doğrultuda çalışmada ilk olarak delil kavramı ele alınacak, ceza muhakemesinde ispat ve delil kavramları incelenerek delil çeşitleri ve delillerin özellikleri ortaya koyulacaktır. Ayrıca çalışma boyunca yapılacak olan değerlendirmelere ışık tutabilmesi açısından ceza muhakemesinde delillerin değerlendirilmesinin tarihsel gelişimi de ele alınacaktır.

İkinci bölümde ise Dijital delil kavramı derinlemesine incelenecektir. Bu çerçevede ilk olarak Ceza muhakemesinde yeni bir alan olduğu savunulabilecek bilişim kavramı ve bilişim yoluyla elde edilen veriler üzerinde durulacaktır. Dijital veri kavramı ve bu verilerin delil olarak kullanılması tartışmaları da bu bölümde ele alınacaktır. Bu çerçevede dijital delillere ulaşabilmek adına kullanılan cihazlar ve sistemler de ceza muhakemesi alanında bu delillerin kullanılıp kullanılmayacağı tartışmasını aydınlatması açısından incelenecektir.

Üçüncü bölümde ise genel olarak delillerin elde edilmesi ve değerlendirilmesi üzerinde durulduktan sonra "dijital delillerin elde edilmesi ve değerlendirilmesi" hususları ortaya koyulacaktır. Ceza Muhakemesinde dijital delillerin elde edilmesi ve değerlendirilmesi konusu tezin en önemli ayaklarından birini oluşturmaktadır. Bu kısımda ağırlıklı olarak Türk Ceza Muhakemesinde dijital delillerin nasıl elde edildiği ortaya koyulacaktır. Bu çerçevede CMK m. 134, CMK m. 135, CMK m. 140 ve Cumhuriyet Savcısının genel soruşturma yetkisini düzenlemekte olan CMK m. 160 ve 161 öne çıkan usullerdir.

CMK m. 134 "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El Koyma"nın hukuki rejimini düzenlemektedir. Bu hususta, 134. madde ve ilgili yönetmelik maddeleri incelenmek suretiyle bu yolla elde edilen dijital delillerin delil değeri ve bu delillere uygulanacak hukuki rejim ortaya koyulmaktadır.

CMK m.135-138 ise "Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi"ni düzenlemektedir. Bu kapsamda m. 135'te (1) "şüpheli veya sanığın telekomünikasyon yoluyla iletişimi dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi", (2) "şüpheli veya sanığın mobil telefonunun yerinin tespiti" ve (3) "Şüpheli ve sanığın telekomünikasyon yoluyla iletişiminin tespiti" şeklinde üç ayrı tedbir öngörülmektedir. Bu tedbirler yoluyla elde edilen dijital deliller, içeriklerin nasıl

saklanacağı, hukuka uygun delil olarak kabul edilebilmesi için taşıması gereken şartlar bu başlık altında değerlendirilecektir.

CMK m. 140'ta düzenlenen "Teknik Araçlarla İzleme Tedbiri" de dijital delillerin elde edildiği bir usuldür. Bu tedbir çerçevesinde elde edilen delillerin değeri, tedbirin şartları, delillerin muhafazası ve uygulamadaki teknik problemler gibi hususlar da bu tedbir kapsamında ele alınacaktır.

Dijital delillerin elde edilmesini ve muhakemede bu delillere başvurulmasını öngören bu uygulamalar dışında, CMK'nın 160 ve 161. Maddelerinde düzenlenmiş olan Cumhuriyet Savcısının genel soruşturma yetkisi de dijital delillerin elde edilmesinde bir yöntemdir. Örneğin sosyal medya yoluyla işlenen bir tehdit suçunun tespit edilmesinde ve bu suça ilişkin dijital delillerin elde edilmesinde Cumhuriyet Savcısı bu kapsamdaki yetkisini kullanacaktır.

Dijital delillerin hukuki rejimini ortaya koyarken ağırlıklı olarak bulunduğumuz hukuk sistemindeki kurallara başvurmak gerekmektedir. Bununla birlikte yabancı hukuk sistemlerindeki örneklere değinmek de konuyu zenginleştirecektir. Bu kapsamda Avrupa'da, ABD'de, Avustralya, Hollanda, İsviçre gibi ülkelerde hukuk sistemlerinde dijital delillerin hukuki rejimine de değinilmektedir.

Ek olarak, Dijital delillere ilişkin uluslararası alanda yapılan çalışmalar da çalışmanın konusuna katkı sağlayacağı ölçüde ele alınmıştır. Avrupa Siber Suç Sözleşmesi, OECD'nin çeşitli ilke kararları, IOCE (International Organization on Computer Evidence) organizasyonunun öngördüğü standartlar, Avrupa Konseyi Siber Suçlar Sözleşmesi bu uluslararası düzenlemeler arasında olup bu çalışma kapsamında da ele alınmaktadır.

İzleyen bölümde, Türk Ceza Muhakemesi kapsamında elde edilen dijital verilerin değerlendirilmesi üzerinde durulmaktadır. Genel olarak delillerin değerlendirilme ilkeleri çerçevesinde dijital deliller bu kısımda incelenmektedir. Dijital

delillerin hukuki geçerliliğinin incelenmesi önemli aşamalardan biridir. Hakime yönelik olarak delil değerlendirme ilkeleri olan delillerin re'sen incelenmesi, delillerin doğrudan doğruya incelenmesi, delillerin serbestçe değerlendirilmesi, delillerin bütün olarak değerlendirilmesi, şüpheden sanığın yararlanması, delillerin doğrulanması ilkesi, delillerin inkar edilmemesi, delillerin tekrar ele alınabilmesi ve delillerin doğruluğu ilkesi kapsamında dijital deliller bakımından özellik gösteren noktalar bu bölümde ortaya koyulmaktadır.

Son olarak da CMK kapsamında dijital delillerin nasıl değerlendirildiği ortaya koyulmaya çalışılmaktadır. Yargıtay kararları ışığında delillerin hangi şartlarla hükme esas alınabileceği ve hakimin değerlendirmesinde nasıl bir yeri olması gerektiği gösterilmeye çalışmaktadır. Dijital delillerin suistimale çok yatkın deliller olduğu tespitine yönelik çözümler bu bölümde ele alınmaktadır. Bu bağlamda dijital delillerin tek başlarına hükme esas kabul edilebilecek delil niteliği taşıyıp taşımadığı, hangi şartlarla bu niteliği taşıyabileceği değerlendirilmektedir. Bu çalışma boyunca cevaplanmaya çalışılan temel sorulardan biri de budur. Nitekim, dijital deliller için önemli olan nokta ne kadar kuvvetli oldukları değil ne derece güvenilir olduklarıdır.

BİRİNCİ BÖLÜM

CEZA MUHAKEMESİNDE DELİL KAVRAMI

I. CEZA MUHAKEMESİNDE İSPAT VE DELİLLER

Bir bireyin yapmış olduğu fiilin suç olduğu şüphesi üzerine yapılmış olan ve bu şüphenin doğru ya da yanlış olduğunu belirlemeye yönelik sürdürülmüş olan faaliyet ceza muhakemesi olarak tanımlanmaktadır[1]. Ceza muhakemesinde öncelikle bir suçun işlenip işlenmediği incelenmektedir. Sonrasında da eğer bu suç işlenmişse kim tarafından işlendiği ve bu suça karşı o kişiye ne yapılması gerektiği belirlenmektedir[2]. Ceza muhakemesinde ortak faaliyeti oluşturan alt faaliyetler şu şekilde sıralanmaktadır. Bunlar;

-İddia,

-Savunma,

-Yargılama'dır.

Ceza yargılamasında ortak faaliyeti teşkil eden diğer faaliyetlerden iddia ve savunma beraber değerlendirilerek yargılama ortaya çıkmaktadır[3]. Bir kişinin ceza muhakemesinde özgürlüğünün kaybile karşı karşıya kalması, bunun sonucunda da maddi gerçeğin aranması bu faaliyetin amacı haline gelmektedir[4].

[1] N. Kunter ve diğerleri, 2010, s.13; Öztekin Tosun, **Türk Suç Muhakemesi Hukuku Dersleri Cilt I Genel Kısım**, 4. Bası, İstanbul, Acar Matbaacılık, 1984, s. 5; Erdener Yurtcan, **Ceza Yargılaması Hukuku**, 11. Baskı, İstanbul, Vedat Kitapçılık, 2005, s. 4.
[2] B. Öztürk ve diğerleri, 2010, s. 33; C. Şahin, 2011, s. 19.
[3] N. Centel, H. Zafer, 2011, s.3; Yener Ünver ve Hakan Hakeri, **Ceza Muhakemesi Hukuku**, Adalet Yayınevi, Ankara, 2012, s.2; Veli Özer Özbek, M. Nihat Kanbur, Koray Doğan, Pınar Bacaksız, İlker Tepe, **Ceza Muhakemesi Hukuku**, Ankara, 2012, s. 42.
[4] N. Kunter, 1981, s.21; E. Yurtcan, 2005, s. 4; Ş. Sarsıkoğlu, 2013, s. 694.

Ceza muhakemesinin ana amacını Yargıtay maddi gerçeğin kesintiye uğramadan ortaya konulması olarak belirlemiştir[5].

Ceza muhakemesinin bu amacına ulaşılabilmesi için özellikle geçmişte yaşanmış olayların deliller aracılığı ile ortaya konulması sağlanmalıdır[6]. Bu noktada maddi gerçeğin ortaya çıkarılabilmesi için özellikle olayla ilgili bulunan tanıklar, belgeler ve olaylardan arta kalan izlerin tespit edilmesi sağlanmaktadır. Sonrasında da bu bulunanlar ceza muhakemesinde kullanılmaktadır[7].

Ceza muhakemesi içerisinde hukuki delillerin sınırlandırılması kabul edilmemektedir. Ceza muhakemesinde özellikle maddi gerçek aranmakta ve buna bağlı olarak vicdani ispat sistemi kabul edilmektedir. Ceza muhakemesi içerisinde her şey delil olarak kullanılmaktadır. Bu nedenle delillerin ayrıntılı bir şekilde toplanması gerekmektedir. Ceza muhakemesi içerisinde bir olayın gerçekleştikten sonra o olayla ilgili uyuşmazlık noktalarını ispat etmek için kullanılan araçlara delil adı verilmektedir. Ceza muhakemesi içerisinde ispat edilmesi gereken iki tür uyuşmazlık türü olduğu belirlenmiştir. Bu uyuşmazlıklar aşağıda belirtilmektedir. Bunlar;

-Maddi ceza konuları,

-Ceza muhakemesi hukuku konularıdır.

Maddi ceza konularına örnek olarak; suç işlenip işlenmediği, eğer bir suç işlenip kimin işlendiğinin belirlenmesi verilebilmektedir[8]. Ceza muhakemesi konularına örnek

[5] Bkz.Yargıtay Ceza Genel Kurulu'nun 19.04.1993 tarih, E.1993/6-79, K.1993/108 sayılı kararı; Yargıtay 4. Ceza Dairesi'nin 06.11.2007 tarih, E.2007/8601, K.2007/8929 sayılı kararı, http:// www.kazanci.com/kho2/ibb/giris.htm Erişim Tarihi: 01.06.2017

[6] N. Kunter ve diğerleri, 2010, s. 1325; M. Koca, 2006, s. 207.

[7] D. Soyaslan, 2010, s. 428; Nevzat Toroslu ve Metin Feyzioğlu, **Ceza Muhakemesi Hukuku**, Savaş Yayınevi, Ankara, 2009, s. 176; V. Bıçak, 2011, s. 430; Hakan Karakehya, "Ceza Muhakemesinde Maddi Gerçek", **Eskişehir Barosu Dergisi 2006,** 10, s. 97.

[8] Ali Şafak, Vahit Bıçak, **Ceza Muhakemesi Hukuku ve Polis**, Roma Yayınevi, 2005, s.277.

ise; bir sanığın eşi olmasına göre tanık olmadan çekilmek istemesi ve hakikaten bu kişinin tanığın eşi olmasi veya olmamasının tespiti verilebilmektedir[9].

Ceza muhakemesi hukukunda; maddi gerçek aranmaktadır ve bunun yanında vicdani kanaat ilkesi kabul edilmektedir. Bu olay neticesinde de delillerinin sınırlandırılması kabul edilmemektedir. Ceza muhakemesi içerisinde her şeyin delil olması kabul edilmektedir. Hakimin vicdani kanaat ilkesine göre her şey delil olarak kabul edilmesi sağlanarak, delillerin serbestçe değerlendirilmesi sağlanmalıdır. Bu delilleri taraflar ileri sürebilecekleri gibi mahkemenin de kendiliğinden toplaması da mümkün olmaktadır.

Ceza muhakemesi hukuku içerisinde delillerin yargıç tarafından serbest şekilde değerlendirilmesi gerekmektedir. Bir şeyin delil olarak kabul edilebilmesi için öncelikle bu delilin ispatı konusunda hakimde vicdani kanaatin oluşmasına bağlıdır.

Delillerin ispat noktasında bazı özelliklerinin bulunması gerekmektedir. Delillerin özellikleri şu şekilde sıralanmaktadır. Bunlar;[10]

-Delillerin ceza davasini teşkil eden olayının bir kısmını ispat edebilecek vasfi olması gerekmektedir (CMK madde 206/2-b),

-Delillerin tum duyularımızla anlaşılabilecek fiziki bir niteliğe sahip olması gerekmektedir,

-Deliller elde edilebilir olmalıdır,

-Delillerin sağlam ve güvenilir olması gerekmektedir,

-Delillerin akılcı olması gerekmektedir,

-Delillerin bilim tarafından kabul edilebilir düzeyde olması gerekmektedir[11],

[9] Feyzullah Avcı, **Ceza Yargılamasında Özel Hayatın Gizliliği Hak ve Hürriyetinin Hukuka Aykırı Olarak Elde Edilen Deliller Nedeniyle İhlal**, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya, 2006, ss.66-67.
[10] N. Centel, H. Zaferi, 2011, s.207.
[11] Bkz.AY madde 38/6; CMK madde 206/2-a, 217

-Delillerin hukuka uygun yollardan elde edilmiş olması gerekmektedir.

İspat araçlarının delil olarak sayılması için olayı yansıtmasına gerek yoktur. Yansıtma; delilin bilime, maddi gerçeğe ve hukuka uygun olması demektir. Eğer bir delil bu koşulları taşımıyorsa teknik olarak bu delil olarak kabul edilmemektedir. Bu nedenle bu tür araçlarla hükme varılması mümkün değildir[12].

Ceza yargılamasının ana amacı; kesintiye uğramadan maddi gerçeğin orataya çıkarılmasıdır. Bu amaç Yargıtay'ın 19.04.1993 tarihinde verdiği önemli bir kararında ortaya çıkmıştır[13].

A. İspat ve Delil Kavramı

Açılan bir davada bir hukuk kuralının uygulanabilmesi için, bu kuralın dayandığı hususların olayda gerçekleşip gerçekleşmediğinin belirlenmesi gerekmektedir. Taraflar iddia ve savunmalarını mahkeme tarafından desteklenmek istedikleri gerekçeye dayandırmalrı gereklidir[14].Bu iddialar taraflar arasında tartışılırsa, onların kanıtılmaları gereklidir. Davaya taraf olan her birinin lehinde sonuçlanması, hukukta bulunan oalyın ispat edilmesine bağlıdır. Bir konu delil araçlari ile açıklanırsa buna ispat denir[15]. Bir şeyin ispatlanmasının hukuki tanımı; ihtilafli mevzunun gerçek olup olmadığı hakkında hakime kanaat verecek delil ve karineleri sunmak, onun dikkatini bu kunuya çekmek olarak tanımlanmaktadır[16].

Bir ispat süreci, davacı ve davalının bir olayın varlığına veya yokluğuna genel bir bakış sunma ve kanuni gerekliliklerini yerine getirme girişimidir[17]. Yargıç bir olayın olgusunu ikna etmeye yönelik bir faaliyet olarak kabul edilen kanıt, aslında adli işlem

[12] Bahri Öztürk, **Ses veya Görüntü Kaydeden Araçlarla Yapılan Tespitlerin Ceza Muhakemesi Hukukunda Değeri**, Prof. Dr. Seyiullalı Edis'e Armağan, 2000, s. 9
[13] Yargıtay CGK. 19.04.1993, 6-79/108, YKD Ekim 1993, s. 1564 vd.
[14] Bilge Umar, Ejder Yılmaz, **İspat Yükü**, İstanbul, Kazancı Matbaacılık, 1980, s.1.
[15] Ejder Yılmaz, **Hukuk Sözlüğü**, Ankara, Yetkin Yayınları, 1996, s.5.
[16]**Türk Hukuk Lügatı**, Ankara, Türk Hukuk Kurumu Yayını, 1991.
[17] Salih Şanver, "Vergi Hukukunda İspat", **Vergi Dünyası 1983**, 21: s.52.

sürecini tanımlar. Olayın doğruluğuna yargıcın ikna etme çalışması olarak kabul edilen ispat, gerçekten yargılama faaliyetin sürecin tanımlamaktadır[18]. Duruşma sırasında taraflar, hakimi verdikleri delillerle ikna etmeye çalışırlar. Bir duruşmda, taraflar iddiaların ve savunmaların çeşitli gerçeklere dayandırmak zorundadırlar. davacının tarafındadır[19]. Eğer varlıkların gerçekliği hakkında uyuşmazlık bulunursa, iddiayı ileri süren taraf vakıaların gerçek olup olmadığını ispat etmek zorundadır. Yasal olarak belirli hususlar hariç, yargıç hukuksal sonuçun önüne gelişinde, onlarin doğup doğmadığını belirleyebilmesi için, sonucun varlığını iddia eden dava tarafı olayın meydana geldiğini ispatlamalıdır. Açılan bir davada kendini haklı bullan tarafın vakıaların doğruluğu hususnda hakimi ispat etmeye ççalışmasına asıl ispat denilir. Davanın karşı tarafı yargıçta yaranan ihtimali kanaati sarsıntıya salmak kendi iddiasına inandırmaya çalışmasına karşı ispat denilir[20]. İspat sonucu bir olayın maddi şekli için hangi yasal kurallar uygulanması gerektiğinde, işin yorum tarafını oluşturur[21]. Bir durumda, taraflar davayı yalnızca dayandıkları gerçeklerin doğru olduğunu ya da diğer tarafın iddia ettiği gerçeklerin doğru olmadığını kanıtlayarak, davanı kazanır ya da kaybederler. Eğer bir davada davacı, iddiasında haklı olmasına rağmen, iddiasını dayandırdığı vakıaları ispat kanıtlayamazsa, karşı tarafda bunun tam aksini ispatlayabilirse, davayı kaybeder. Bu sebeple, olayi açıklaması olarak kabul edilebilecek ispat davalarda daha önemlidir.

Mesele, hakimi davanın gerçeklerinin doğru olup olmadığına ikna etmek için faaliyetleri ve belgeleri kanıtlamaktır.Bu faaliyetler ve belgeler, hem vakayı etkileyebilecek nitelikte olmalıdır hem de davanın nihai sonucuna ulaşılmak için, hakimin kanaatini uyandıracak nitelikte olmalıdır. İspat sürecinde olan bır dava

[18] Nihal Saban, **Vergi Hukuku**, İstanbul, Beta Yayınevi, 2006, s.74.
[19] Yavuz Atar, **Vergi Hukuku**, Konya, Mimoza Yayınları, 2000, s.171.
[20] Baki Kuru, Ramazan Arslan, Ejder Yılmaz, **Medeni Usul Hukuku**, Genişletilmiş 12. Baskı, Ankara, Yetkin Yayınları, 2003, ss.421-422.
[21] M. Kamil Mutluer, **Vergi Genel Hukuku**, İstanbul Bilgi Üniversitesi Yayınları, 2006, s.64.

taraflarının arasında olan ihtilaflı olaydır. Bu olay dış dünyadaki maddi olay veya insan aleminde meydana gelen manevi olay da olabilir[22]. Bu olay yargıcın önünde olan ihtilafi uygulamasına hukuki kuralara ait maddi unsuru açıklayıp ve onun bilinmesine olanak sağlayan iddialardır. Dava taraflarının iddia ettikleri gerçekler, sadece bir ispatın konusu olmaktadır.İspatı gerektiren gerçekler, davanın çözümünü etkileyen yasal olarak önemli gerçeklerdir. Bir anlaşmazlığın çözümünde bazı olayların doğrudan ve dığerleri ise dolaylı olarak etkisi vardır. Kanunlara dayanan vasıtasız vakıa, hukuki bir sonucun ortaya çıkması için ön koşuldur. Bilvasita ehemmiyeti olan vakıa ise hukuk kuralının uygulanması sonucu koşul vakıasının gerçekleşmiş olduğu sonucunu ortaya çıkaran dığer vakıadır. Bu tur vakıalara belirti vakia denir[23]. yargıç delili incelenmesinde, takdiri yetkisine dayanarak, bir olayi belirtile ispat olmasını kabul edebilir. Yargıç bir davada yasayı otomatik olarak uygular. Tarafların olay için hangi kanunun geçerli olduğunu kanıtlamaları gerekmez. Ama ağer dava taraflarının her birisi örf ve adet yasalarına dayandığı zaman onu ispatlamak zorundadır[24]. Yine HUMK'un 76. maddesinde istisnai olarak "devletler özel hukukuna ilişkin bir davada iddiasını bir kanun hükmüne dayandıran taraf bunu ispat etmekle yükümlüdür", yasası devam ediyor. Hakimler Türk kanunlarının ihtilaf kurallarını ve bu kurallar çerçevesinde yetkili yabancı hukuku resen uygulamaktadır. Bunu 5178 sayılı MÖHÜHHK,un ikinci maddesine göre yapmiştir. Hakim dava taraflaraından bu konudaki yabancı yasaların içeriğini belirlemede yardım alabilir.Sonuç olarak, yabancı hukuka başvurmuş olan tarafa yüklenen ispat yükü yerini yardım yükümlülüğüne bırakmıştır.

Bir hukuk kuralının uygulanabilmesi, kendilerine hukuki sonuçu olan olayin somut olarak gerçekleşmesine bağlıdır. Hukuk kurallarının soyut olarak düzenledikleri

[22] M. Kamil Yıldırım, **Medeni Usül Hukukunda Delillerin Değerlendirilmesi**, İstanbul, Kazancı Hukuk Yayınları, 1990, s.114.
[23] Hakan Pekcanıtez, Oğuz Atalay, Muhammet Özekes, **Medeni Usül Hukuku**, Ankara, Yetkin Yayınları, 2005, s.344.
[24] H. Pekcanıtez ve diğerleri, a.g.e., s.349.

olaylar, somut olarak gerçekleşmedikçe o hukuk kuralının uygulanması mümkün değildir. Hakim bir davada ihtilafli olayın gereğini tespit ettikten sonra, bu olayın davahı veya davacı tarafından ispat edileceği meselesi ile karşı karşıya kalır. İşte ispatı gereken çekişmeli olayların hangi tarafça ispat edilmesi gerektiği sorunu da karşımıza ispat yükü kavramını çıkarır[25]. Davanın ispatı yükümluluğu; dava taraflarının her hangisi bir vakıanı iddia edip sonucun kendi lehinde olmasını istemesi, o tarafın ispata mecbur tutulmasına denir. İspat yükü kendisine düşen taraf, iddiasını ispat edemediği takdirde davayı kaybetme riski altındadır[26]. Her hukuk kuralındaki ispat yükünü, o kuraldan yaralanacak kimse taşıyacaktır. Diğer bir deyişle iddiayı ispat etme yükü kime aitt olmasının tespiti bir nevi o olayı düzenleyen hukuk kuralının hangi taraf lehine sonuç doğurduğunun tespitidir[27].

İspat yükü belirsizliğin riskinden ibarettir[28]. Belirli bir olayın meydana gelip gelmediğini ispatı yükü, davacı bulunan tarafa usuli bir yüktür. Talebini kanıtlama yükümlülüğüne sahip olan tarafın bir yükümlülüğü değil sadece bir görevi vardır. Bu yükü yerine getirmeyen kimse hakkında herhangi bir yaptırım uygulanamaz. Bu sebeple genellikle ispat mükellefiyetinden değil de ispat külfetinden (yükünden) söz edilir. Mükellefiyetin yerine getirilmesi zorunludur. Oysa ispat yükü kendisine düşen taraf bir vakıyanın ne olduğunu kanıtlayamıyorsa, davanın dığer tarafı ya da hakim onun ispatının ondan taleb edemez ve ispat yüküne yükümlu olan iddasını ispat edememiş sayılır. Davacının bu durumda olduğu anda, davası ispat edememiş sayılıp ve onun davası reddedilir[29]. İspat yükü konusunda genel kural TMK'nun 6.maddesinde yer alan; "kanunda aksine bir hüküm bulunmadıkça, taraflardan her biri, hakkını dayandırdığı olguların varlığını ispatla yükümlüdür", hükmü ile düzenlenmiştir. Bu hükme göre, bir

[25] B. Kuru ve diğerleri, 2003, s.423.
[26] Süheyla Şenlen Sunay, **İdari Yargılama Usulüne Hakim Olan İlkeler Karşısında İspat ve Delil Hususları**, İstanbul, Kazancı Matbaacılık, 1997, s.28.
[27] Selami Şengül, "Özel Hukukta ve Vergi Hukukunda Delil Sistemi", **Maliye Dergisi 1987**, 47, s.70.
[28] B. Umar, E. Yılmaz, 1980 s.37.
[29] B. Kuru ve diğerleri, 2003 s.422.

davada ileri sürdüğü bir iddiadan kendisine bir hakk talab eden kimse, o dayandığı vakıanı ispatını gerekmektedir. Bu noktadan hareketle davacı davasını dayandırdığı, davalı ise savunmasını haklı göstermek için dayandığı vakıaları ispat etmelidir. Yani bu hükümden ispat yükünün ilk olarak davacıda olduğu anlaşılmaktadır. Ancak bu genel kuralın istisnaları mevcuttur. Burada önemli olan husus tarafların hukuki durumu değil, dayandıkları vakıaları ispat etmeleri gerektiğidir. Davada ispat yükü herhangi bir tarafa düştüğü gözetmeksizin delil göstermişse, bu durumda hakimin ispat yükünün hangi tarafa ait olduğunu araştırmasına gerek yoktur. yargıç başlangıçta her tarafın sunduğu delilini tetkik etmekle yükümlüdür[30]. Tarafların gösterdiği delillerin incelenmesiyle dava aydınlanmış ve hakimde dava konusu olayla ilgili bir kanaat oluşmuşsa yine ispat yükünün tespitine gerek kalmaz. Buna karşılık gösterilen delillerin incelenmesi sonucu hakimde dava ile ilgili tam bir kanaat oluşmaması durumunda, ispat yükünün önemi kendini gösterir. Bu durumda ispat yükünün hangi tarafa ait olduğunun saptanması gerekir ve ispat yükü kendine düşen taraf da dava konusu olayı ispatlamalıdır. Hâkim, sunulan delilleri dava hakkında karar vermesi için yeterli olup olmayacağına karar vermelidir. Bu durumda hakim, davanın har hangi tarafin ispat yükünü olmasını düşündügü zaman, o taraf ihtilafi kunusu olan vakianı ispat istemesi gerekir[31].

İspat yükü ile ilgili en önemli kunu, hangi olay için ispat yükünün kime düştüğüdür. Bunu belirleyen kurallara ispat yükü kuralları denir. İspatın yükünün paylaşmasına göre olayın ispatının mümkün olmadığı ve hakimin bir tarafın aleyhine çıkan kararın tehlikesinin önlemesi için, hangi olay bakımından kimin üzerinde bulunduğunun belirlenmesi gerekir. İspat yükünü, nesnel ve öznel ispat yüküne ayırmak mümkündür. Nesnel ispat yükü, olgusal iddiaların ispatsız kalmasının sonuçlarına yönelik sorunun yanıtını verir. Yani burada taraflardan hangisinin belirsizliğin yükünü taşıyacağı sorusuna yanıt aranır. Diğer yandan öznel ispat yükü ise, tarafların davayı

[30] B. Kuru ve diğerleri, 2003 s.424.
[31] B. Kuru ve diğerleri, 2003 s.425.

kaybetmelerini önlemek amacıyla çekişmeli olaylara ilişkin delil ileri sürme yüklerini ifade eder. Başka bir deyişle, taraflardan hangisinin mahkemeye delil sunma yükü altında bulunduğu, öznel ispat yükü kavramı ile açıklanır[32]. Hakim önceden ispat yükünün subjektif sonradan objektif olmasını belirlemelidir. Davada önceden her hangı bir tarafa ispat yükü düşeese o taraf iddiasını ispat edecektir. Davanın diğer tarafı, ispat yükü olan Tarafdan, iddiasının kanıtlamsını bekleyebilir.İspat yükü olan taraf, iddiasını doğrulayamazsa, karşı taraf iddiasını ispatına gerek kalmaz ve o vakıa ispat edilememiş kabul edilir. Ancak ispat edilmesi istenmeyen taraf, ispat etmesi gereken tarafın iddiasını ispat etmesini beklemeyebilir ve tarafın iddia ettığı konunun gerçek olmadığının ispat için delillerini mahkemeye sunula biliyor. Buna karşı delil denir[33]. Yani "karşı delil", ispat yükü kendisine düşmeyen tarafın gösterdiği delildir. Karşı delil gösteren taraf bu davranışıyla ispat yükünü üzerine almış sayılmaz. Fakat ispat yükünü taşıyan tarafın iddialarını ispat etmesini güçleştirir ve iddialarını çürütmeye çalışır[34].

Olağan bir duruma dayanan taraf iddiasını ispat etmek zorunda olmayıp ispat yükü olağan durumun tersini iddia eden tarafa düşer. Genel kuraldan ayrı olarak kanun bazı hallerde ispat yükünün kime düştüğünü belirtmiş olabilir. Bu durumda kanunda gösterilen taraf ispat yükünü taşır. İddiasını yasal bir karineye dayandıran taraf da iddia konusu olan ve uygulanacak hukuk kuralında yer alan vakıayı doğrudan ispatla yükümlü değildir. Dava tarafları çekişmeli vakıanı ispat yükünün hangi tarafa düştüğüne dair ispat yükü sözleşmesini yapabilirler. Taraflar haklarında serbestçe tasarruf edebildikleri gibi uyuşmazlık konusu hakkın ispatı konusunda da serbestçe tasarruf edebilirler. Dava sürecinde yapılan ispat yüküne dair sözleşme, her iki tarafında sözleşme hususunda özgürce tasarruf haklarının bulunması ve vakıaların

[32] Mithat Sancar, "Vergi Yargısında Dava Malzemesinin Toplanması ve İspat yükü", **Mali Hukuk 1989**, 24, s.53.
[33] B. Kuru ve diğerleri, 2003, s.430.
[34] B. Umar, E. Yılmaz, 1980, s.7.

belirlenmiş olması sonucundan geçerlilik kazanır. İspata ilişkin emredici hukuk kurallarına aykırı ispat sözleşmesi yapılamaz[35].

İspat yapılırken birtakım vasıtalardan yararlanılır. İspatlamada kullanılan bu vasıtalara ispat vasıtaları denilir. İspat vasıtaları ise delillerdir. İspat vasıtalarının geçerliliği, bunların kullanılmalarına hukuken izin verilmiş olması şartına bağlıdır[36]. Dolayısıyla da nelerin delil olabileceği, bunların nasıl kullanılacağı, ispat güçleri, hukuk dallarına göre ayrı ayrı düzenlenmiştir.

Delil kelimede, reberlik eden ve kılavuzluk anlamına gelmektedir[37]. Hukuk bilimide ise delil, dava tarafları arasında doğruluğu tartışmalı olan vakıanın doğruluğuna hakimi inandırmak için kullanılan vasıtaları ifade eder[38]. Taraflar arasında gerçekliği tartışmalı olan vakıaların doğruluğuna hakimi inandırma faaliyeti ispat olarak adlandırıldığına göre delil kavramı, ispat kavramı içinde yer alır. Çözümlenmesi gerekli olan kunuda tarafların, hukukun ona tanıdığı hakkın doğumuna ilişkin vakiaların gerçekliğini ispat etmek suretiyle, karşı taraf ise bunun aksini ortaya koyarak davanın kazanılması için ispat faaliyetlerine girişirler. Bir davada olayların ispatında kullanılan vasıtalara delil denir[39]. Deliller ispat faaliyetinde kullanılmaktadır. Bunun yanında kanıtlar, mahkeme dışında gerçekleşmiş ise temsili olarak yargılamaya aktarılmaktadır ve bu şekilde kullanılmaktadır[40].

Delil, yargılama hukukunun tüm dallarında ortak konudur. Nitekim Hukuk Usulü Muhakemeleri Kanunu'nun 238. maddesinde delil; "davanın halline tesir edebilecek münazaalı hususların ispatı için başvurulan vasıtalardır", şeklinde tanımlanmıştır. Bu tanımlamaya göre delil, taraflar arasında ihtilaflı olan vakıalar

[35] H. Pekcanıtez ve diğerleri, 2005s.365.
[36] Adnan Tezel, "Türk Vergi Hukukunda İspat ve Delil Sistemi", **Yaklaşım 1997,** 56, s.12.
[37] Ferit Develioğlu, **Osmanlıca-Türkçe Ansiklopedik Lügat**, 3. Baskı, Ankara, 1978
[38] Necip Bilge, Ergun Önen, **Medeni Yargılama Hukuku Dersleri**, 3. Baskı, Ankara, Sevinç Matbaası, 1978, s.492.
[39] S. Şengül, 1987, s.69.
[40] H. Pekcanıtez ve diğerleri, 2005, s.379.

hakkında gösterilir. Taraflar arasında tartışmasız anlaşmazlıklar gösterilmesine gerek yoktur. Dava tarafları arasındaki ihtilafsız vakıa kunusunda bir delilin gösterilmesine gerek yoktur. Tarafların üzerinde anlaştıkları veya ikrar ettikleri vakıalar ile herkes tarafından bilinen ya da öğrenilmesi mümkün olan hususlar, ihtilaflı kabul edilmez. Maddi hukuk, bir hakkın doğumunu belirli olayların gerçekleşmesine bağlamıştır. Delilin konusunu da bu maddi olaylar teşkil eder. Bu olaylar iddia ve savunmanın kaynağını oluşturan, iddia ve savunmanın dayandığı olaylardır. Hukuk kuralları ise delilin konusunu teşkil etmez. Bu kuralları hakim zaten re'sen göz önüne almaktadır.

Delillerin ispat gücü onların türüne yada biçimlerine göre değişmemektedir. Delillerin ispat gücü anlaşmazlık konusu olayın yapısına uygun olup olmamasına bağlı olarak farklılaşmaktadır. Buna bağlı olarak delillerin olayı aydınlatacak nitelikte olup olmaması da büyük önem taşımaktadır.

Yargılama noktasında delil gösterme yükü; özellikle mahkemenin aleyhte karar verilmesi tehlikesini ortadan kaldırmak amacıyla tarafların doğruyu göstermesi amacıyla gerçekleştirilmektedir. İddia makamı iddiasını ispat etmekle yükümlüdür. Bu nedenle delillerde yargılama esnasında büyük önem taşımaktadır. Delillerin doğruluğu veya yanlışlığı da mahkeme tarafından bağımsız olarak tespit edilmektedir.

Delil gösterme yükü, taraflardan birinin kendi aleyhine verilmesi muhtemel bir kararı engellemek amacıyla delil göstererek, kendi iddiası doğrultusunda hakimde kanaat uyandırma ödevi şeklinde de tanımlanabilir. Delil gösterme kuralları ile ispat işinin biçimi ve yöntemi düzenlenir. Delil gösterme, yargısal bir kavram olarak kaşımıza çıkmaktadır. Yargılama hukuku içerisine delil gösterme kuralları da girmektedir. Genellikle belirli bir olayı kanıtlama yükümlülüğü olan bir taraf o olay için delil gösterme yükünü taşımaktadır. İspat yükü sabit olmasına rağmen delil

gösterme yükü, yargılamanın gidişine ve yargıcın değerlendirmesine göre taraf değiştirir[41].

B. Delillerin Özellikleri

Hakim, önüne gelen bir uyuşmazlıkta hem maddi olayı hem de hukuki sorunu çözmek durumundadır. Delil geçmişe ilişkin bir gerçeği ifade etmektedir. Hakim dosya üzerinde geçmişi incelemekte ve geçmiş hakkında bir karar vermektedir[42]. Yargılama hukukunda maddi gerçeğe ulaşmak için hakimin kanaatinin serbestçe oluşması arandığından hakime gerçeğe uygun olanı gösterecek her şey delil sayılabilir. Ama o şeyin ispat aracı yani delil olmasıda başka ve bu vasıtanın hakimim kararında esas olmasıda başka şeydir. Çünkü delil olan şeylerin hepsi hükme temel teşkil etmez. Bu nedenle delil olabilecek şeylerde bazı özellikler aranmaktadır.

Ceza muhakemesi sistemi içerisinde karar verecek olan hakim vicdani delil sistemi içerisinde bir suçun aydınlatılabilmesi için her şeyi delil olarak kullanabilmektedir. Ceza muhakemesi içerisinde bir şeyin delil olarak kullanılıp değerlendirilebilmesi hakimin kanaatine bağlı olarak değişmektedir. Bu nedenle delilleri değerlendiren hakimdir. Medeni hukuk içerisinde delil bakımından uygulanan sistem kanuni deliller sistemi söz konusudur. Bu kesin deliller hukuki uyuşmazlığın çözümünde büyük önem taşımaktadır. Eğer uyuşmazlık; kesin delil ise çözümlenirse hakimin takdir yetkisine başvurulmaz bu kesin delile göre hareket edilir[43]. yargıç delillerin değerlendirmesinde tam ve sınırsız bir yetkisi yoktur. Mahkemede bir şeyin delil olup ve hakim tarafından kabul edilmesi için bazı özellik ve nitelikleri taşımaları gerekmektedir. Bu nedenle YCGK'nun vermiş olduğu bir kararda "delillerin gerçek, akla uygun ve realist olması, olayın bir bütünü veya parçasını kapsaması gerektiği

[41] B. Umar, E. Yılmaz, 1980, s.32.
[42] Yusuf Karakoç, **Türk Vergi Yargılaması Hukukunda Delil Sistemi**, DEÜ Hukuk Fakültesi Döner Sermaye İşletmesi Yayınları, 1997, s.11.
[43] Mehmet Akif Tutumlu**, Medeni Muhakeme Hukukunda Delillerin İleri Sürülmesi**, 4. Baskı, Ankara, Seçkin Yayınevi, 2007, s.28.

belirtilmektedir. Deliller olmadan bir akım varsayımlara dayanılarak sonuca ulaşılması ceza muhakemesinin amacına kesinlikle aykırıdır"[44]. Bu şekilde Yargıtay delillerin sahip olması gereken özelliklerinin ana hatlarını çizerek hukuk sisteminde bunlara uyulması gerektiğini belirtmiştir.

Ceza muhakemesinde kullanılan delillerin muhakeme konusu olayla ilişkilendirilerek olayı ispat etmesi ya da çürütmesi sağlanmalıdır. Muhakeme konusu olayla ilgisi olmayan delillerin muhakeme içerisinde yer alması mümkün değildir. Bu nedenle muhakeme konusu olayla ilgili ve ilişkili delillerin kullanılması gerekmektedir. Bu delillerin bazı özellikleri bulunması gerekmektedir. Bu özellikler;

-Delillerin maddi bir gerçeğinin ortaya çıkarılmış olması ve fayda sağlaması gerekmektedir.

-Delillerin ispat edici nitelikte olması gerekmektedir.

Delillerin bu özellikleri taşıması da kanuni bir zorunluluk olarak görülmektedir. Bu nedenle ceza muhakemesinde bu özellikleri taşıyan delillerin kullanılması gerekmektedir.

Cezai takibatta, deliller özellikle mantıklı olup ve güvenilir bir kaynaktan elde edilmelidir. Bazı şeylerin delil olması beklenemez. Orneğin; dedikodular, safsatalar, falcılık veya psikolojik kehaneti gibi akla ve mantığa aykırı veriler. İnsanların beş duyusuyla elde ettiği bilgilerin bazıları tesadüf eseri doğru olabilmektedir. Ancak yasa gereği, belirli bir mantık filtresinden aktarılan sonuç mantıklı olabilir[45]. Kaynağı belirli olmayan ve temeli ortada olmayan verilerin delil olma husuiyeti bulunmamaktadır. Bu nedenle delillerin içeriğinin de güvenilir olması gerekmektedir. Buna örnek vermek gerekilirse; ceza muhakemesinin farklı aşamaları içerisinde tanıklar birbirleriyle

[44] Bkz.Yargıtay CGK, E. 1993/6-79, K.1993/108, T. 19.04.1993 (YKD C.19, S.10, Ekim 1993, s.1565).
[45] E. Ernest Hirşt, **Pratik Hukukta Metot,** 4. baskı, Ankara, Banka ve Ticaret Hukuku Araştırma Enstitüsü Yayınları, 2005, s. 83.

çelişkili olarak beyan vermişlerse o zaman bu tanıkların beyanı güvenilir kabul edilmemektedir.

Delillerin başka bir özelliği de müşterek olması olarak bilinmektedir. Buradaki müştereklik; bir ceza davası içinde öne sürülmüş olan deliller muhakemenin bütün taraflarca bilinmesi ve tartışılabilmesi olarak tanımlanmaktadır. Fakat eğer davaya bakan hakimin özel olarak elde ettiği, kişisel yönden edinmiş olduğu bunun yanında da mahkeme önüne getirilmeyen veriler delil olarak kabul edilmemektedir[46]. Eğer taraflar delili bilmiyorlarsa bu delillere itiraz etmeleri ve tarafların bu delillere ilişkin olarak etkili savunma yapılmasi imkansızdır[47].

Bir cezai yagılama sayesinde ceza ile adalet sistemi çalışmakta ve bunun sonucunda da adalet tecelli etmektedir. Bu sistem içerisinde hukuk dışı bir eylem bulunmamaktadır. Hukuki süreçin yerine getirilmesi, delilin toplanmasında, yargı makamına sunmasında ve takdir edilmesinde mutlaka zorunludur. Yasaya uygun olmayan şekilde elde edilen delillerin kabul edilemeyeceği Anayasa'nın 38. maddesi ve 6. fıkrasında belirtilmiştir.

Ceza muhakemesinde kullanılan belirli ilkeler bulunmaktadır. Bu ilkeler;

-Delillerin serbestisi ilkesi,

-Deliller üzerinde hakimin takdir yetkisi.

[46] Bahri Öztürk, Mustafa Ruhan Erdem, **Uygulamalı Ceza Mahkemesi**, 10. Baskı, Ankara, Seçkin Yayıncılık, 2006, s.453-454.
[47] Veysel Dinler, **Ceza Muhakemesinde Delillerin Toplanması**, Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara, 2009, s.11.

Ceza muhakemesinde delil serbestisi ilkesi sınırsız olarak kabul edilmemektedir. Bu noktada da bazı kimi özelliklerin sahip olması sağlanmalıdır[48]. Buna göre delillerin özellikleri aşağıdaki şekilde sıralanmaktadır, bunlar;

-Delillerin gerçekçi olması sağlanmalıdır.

-Delillerin geçmişte bulunan somut olayları temsil edici nitelikte bulunması gerekmektedir. Ceza yargılamasında bulunan delil kanıtlanmış olaylarınan ilgilidir. Bu nedenle deliller bir olayın tamamın veya bir kısmın yansıtmalıdır. Bu nedenle ortaya çıkan deliller bu olayın tamamını veya bir kısmını yansıtmalıdır. Bu nedenle delillerin güçlü ve güvenilebilir belirtiler taşıması gerekmektedir.

-Delillerin akılcı olması sağlanmalıdır. Deliller gerçek, makul, gerçekçi ve nesnel özelliklere dayanan verilerle kanıtlanması sağlanmalıdır.

-Delillerin mevcut olması gerekmektedir.

-Delillerin muşahhas bir şekilde elde edilmesi ve hakimin takdirine verilmesi gerekmektedir.

-Delillerin kanuna uygun şekilde bulunması gerekmektedir.

-Delillerin kanuna uygunluğu iki şekilde ortaya çıkmaktadır. Buna bağlı olarak delillerin hem kanuna uygun yolla elde edilmesi ve kanuna uygun nitelikte olmasının sağlanması gerekmektedir. Bazı deliller; kanun kapsamında elde edilmesine rağmen, mahkeme makamı tarafından delil olarak kabul edilmeyebilmektedir. Bunun nedeni de delillerin içerikleridir. Buna örnek olarak doktorlar doktor unvanı ile hastalarından öğrendikleri bilgileri hukukki yollarla ellde etseler bile, bu kişilerin izinleri olmadan mahkemeye sunamazlar. Delil elde etme yöntemleri yasa dışı ise, delil olarak

[48] N. Toroslu, M. Feyzioğlu, 2009, s.170.

kullanılması yasaktır. Ceza Muhakemesi Kanunun 148. maddesinde hangi şekilde elde edilen delillerin delil olarak kullanılamayacağı belirtilmiştir. Bunlar;

-Bireyin özgür iradesine dayanılmayacak şekilde kötü davranılarak elde edilen deliller,

-İşkence yoluyla elde edilen deliller,

-İlaç verme yoluyla elde edilen deliller,

-Yorma ve aldatma yoluyla elde edilen deliller,

-Cebir uygulama ve tehdit yoluyla elde edilen deliller,

-Tehditte bulunularak elde edilen deliller,

- Bir kişinin iradesini veya manevi müdahalesini veya yasadışı menfaatlerin vaatlerini ihlal eden belirli araçlar kullanılarak elde edilen deliller,[49]

Bu deliller bir ceza mahkemesinde delil olarak kabul edilemez.

-Delillerin müşterek olması gerekmektedir. Bu nedenle delillerin içeriğini sadece mahkeme makamını bilmesi yeterli değildir. Bu delillerin muhakemenin taraflarının da bilmesi sağlanmalıdır. Ceza muhakemesinde buna delillerin müşterekliği ilkesi adı verilmektedir.

Delillerin muhakeme tarafları tarafından tartışılması gerekmektedir. Buna bağlı olarak hakimler kişisel bilgiye dayanılarak hükmün tesis edilmemesi sağlanmalıdır. Dava konusu vakıa ilgili olarak davanın gidişatı hakkında kişisel bilgisi olanyargıç görevinden ayrılarak mahkemede şahitlik yapabilir[50].

[49] N. Toroslu, M. Feyzioğlu, 2009, s. 171.
[50] Metin Feyzioğlu, **Ceza Muhakemesi Hukukunda Tanıklık**, Ankara, 1996, s.64.

1. Gerçekçi Olması

Bir şeyin delil olarak kabul edilebilmesi için gerçek dünyanın, gerçeğin bir parçası olması gerekmetedir. Bu kapsamda delil; gerçekçi, beş duyu organımızla algılanabilecek somut bir yapısı olmalıdır. Beyan ve belge delilleri ile birlikte belirtilerin de dış dünyada varlığı nedeniyle aranılan özelliğe sahip oldukları konusunda tereddüt edilmemelidir[51].

2. Akla Uygun Olması

Ceza muhakemesinde deliller, tarihsel gelişim içinde çeşitli aşamalardan geçmiş ve özellikle ilkel aşamada muhakeme çoğu zaman akıldışı delillere dayanılarak sonuçlandırılmıştır. Bu doğrultuda örneğin, kuşun güneye uçması sanığın suçu işlediğini, kuzeye uçması işlemediğini ifade edebilmiştir[52]. Bugünkü gelinen aşama açısından akılcı olması delilin en önemli özelliklerinden biridir. Hâkimin vicdani kanaate ulaşmasında maddi gerçeğin araştırılması yolunu mantık kuralları göstermektedir. Bu kapsamda delillerin bilimsel olması akla ve mantığa uygun olması gerekmektedir. Örneğin, yargıç kararını bir falcının kehanetleri sonucunda vermez. Yine şekli deliller, ancak şekli gerçeği gösterdiklerinden maddi gerçeği araştıran ceza muhakemesi bunlarla yetinemeyecektir[53].

Delilin akla ve mantığa uygun olması ve bilimsel olarak kabul görmesi gerekir. Delin'in maddi gerçeği akla uygun, gerçekçi ve objektif niteliklere dayanan verilerle ispat edilebilir özellikte olması gerekmektedir. Yani aklın, mantığın ve bilimin kabul edemediği şeyler delil olamaz[54]. Delinin akıllıcılık özelliği, bilimsel açıdan kabul edilebilir bir nitelik taşımasını da beraberinde getirir. Hakimin kararına temel teşkil

[51] N. Kunter ve diğerleri, 2010, s.1328.
[52] Ö. Tosun, 1984, ss.4-5.
[53] N. Kunter ve diğerleri, 2010, s.1329.
[54] Cumhur Şahin ve Neslihan Gökturk, Ceza Muhakemesi Hukuku II, 2. Basım, Ankara: Seçkin Yayıncılık, 2013, s. 19

eden falcının kehanetine veya yaygınca kabul edilen asılsız inançlara dayandırması delilin akılcılığı özelliği ile bağdaşmaz. Zira gerek falcının kehaneti gerekse toplumun benimsediği asılsız inançlar akıl yoluyla izah edilemez[55]. Dolayısıyla ceza muhakemesinde akla dayanmayan şeyler delil olarak nitelendirilemez.

3. Olayı Temsil Edici Olması

Deliller, bir olayı temsil etmek özelliği olmalıdır. Buna göre ispat aracının olayın bir parçası olması veya olayı yansıtması gerekmektedir. Olayı herhangi bir boyutuyla temsil etmeyen deliller, yargılama konusunda ilgisiz olmaları nedeniyle rededilirler. Olayı temsil edilecek, geçmişte yaşanması olayı anlatabilme ve canlandırabilme özelliğini ifade etmektedir. Delinin sağlam ve güvenilir olması da yine olayı temsil edileceğin bir unsurudur[56].

Deliller uyuşmazlık konusu olan olayı temsil etmelidir. Delilin olayı temsil etmesi, delil olarak kullanılmak istenen aracın olayın bir parçası olarak görülmesidir. Bunun yanında delilin olayı temsil etmesi olayı yansıtmasını ifade etmektedir. Buna bir örnek vermek gerekirse bir adam öldürme suçunda olay yerinde bırakılmış olan suç aletinin olayın bir parçası olduğu görülmektedir. Suçu beş duyusuyla algılayan ve şahit olan bir kişinin olayı anlatması oalyın nasıl gerçekleştiğini ortaya koymaktadır[57].

Temsil edilecek hususa, yargılama konusu olayın tamamı esas alınarak karara bağlanmalıdır. Dolaylı delilerin olayı temsil ediciliği başlarına düşünüldüğünde zayıf görülebilir, ancak Sair delilerle birlikte ele aldığını takdirde olayın ispatına yardımcı olabilecekleri kanaatine varılır. Bazen dolaylı bir delil tek sonucua değil, birden fazla sonuca götürülebilir.

---

[55] Bıçak, s. 429.
[56] Şahin ve Göktürk, s. 20.
B. Öztürk ve diğerleri, 2010, s.279.[57]

İspatlanması gereken bir olayın bir bölümünü temsil etmeyen vasıtanın delil olarak değeri yoktur[58]. Aynı zamanda bir delilin olayı temsil edici olabilmesi için sağlam ve güvenilir olması da şarttır[59]. Bir delilin güvenilir olup olmadığını hâkim değerlendirecektir.

4. İspat Bakımından Önemli Olması

Delilin ispat açısından önemli olması bir diğer deyişle bir faydasının bulunması gerekir. İspatına ihtiyaç duyulan hususlarla ilgili deliller ispat bakımından önemlidir[60]. CMK'nın 206/2-b maddesi gereğince de, delil ile ispat edilmek istenilen olayın karara etkisi yoksa delilin ortaya konulması reddolunacaktır.

5. Hukuka Aykırı Olmaması

Delillerin en önemli özelliklerinden biri de delilin hukuka aykırı olmaması gereğidir. Ceza muhakemesinde maddi gerçeğin araştırılması gayesi mutlak olarak görülmemelidir. Bu bağlamda, gerçeğin somut olarak ortaya konulması herhangi bir maliyetle elde edilebilecek kesin bir değer değildir, yani bazı değerlelr somut gerçeklerden daha önemlidirBu nedenle, maddi gerçeklerin, insan hakları ve insan onuru gibi temel değerleri koruyarak ve yasal yollarla ortaya konmalıdır. Bu doğrultuda hukuka uygun olmayan kanıtların ceza muhakemesinde delil olarak değerlendirilmesi mümkün değildir. İnsan haklarını teminat altına alan, toplumsal güvenliği sağlayan, ve hukuk kurallarına bağlı olan bir hukuk devletinde hukuka aykırı delillere yer verilmemelidir. Anayasa'nın 38/6. maddesinde yer alan kanuna aykırı olarak elde edilmiş bulguların, delil olarak kabul edilemeyeceği; CMK 206/2-a maddesinde yer alan kanuna aykırı olarak elde edilmiş delillerin ortaya konulamayacağı; CMK 217/2. maddesinde yer alan yüklenen suçun, hukuka uygun bir şekilde elde edilmiş her türlü

[58] N. Kunter ve diğerleri, 2010, s.1330.
[59] N. Kunter ve diğerleri, 2010, s.1331.
[60] N. Kunter ve diğerleri, 2010, s.1331.

delille ispat edileceği düzenlemeleri gereği deliller hukuka uygun yollardan elde edilmiş olmalıdır. Bu durumda, vicdani kanıt sistemin sınırını oluşturan hukuka aykırı deliller, ceza muhakemesinde hiçbir aşamada kullanılamayacak, dolayısıyla vicdani kanaate ve hükme de esas alınamayacaktır.

6. Müşterek Olması

Deliller müşterek olmalıdır. Hâkimin şahsi ve özel bilgisi delil olamaz, dolayısıyla delilin içeriğinin sadece hâkim tarafından öğrenilmesi yetmez. Delilleri hâkim ile birlikte taraflar da öğrenmeli ve kolektif hüküm verme faaliyetine katılabilmelidir[61]. Delillerin müşterekliği ya da kolektifliği bunu gerektirir[62]. Delinin sadece hakim tarafından öğrenilmesi yetmemektedir, uyuşmazlığın tarafları da bu konuda bilgi edinmeleri gerekmektedir ve mütalaaları ile kollektif hüküm verme faaliyetine katılmalıdırlar. Sadece bir tarafından bilgisinde kalan deliler, müşterek delil kazanamaz. Müştereklik duruşma açılarak sağlanmalıdır. Hakimin tek bilgi kaynağı duruşmadır. Vicdanı kanaat, kollektif ispat aracına dayanılarak oluşturulan özgür kanaattır. Hakim kanaatini, ancak duruşmada irad ve ikame edilmiş ve tartışılmış delillerle dayandırabilir[63]. Delil olacak her belge duruşmada okunmalı, hükme (vicdanı kanaate) esas alınacak her beyan duruşmada tartışılmalı.

CMK 217/1. maddesinde de "hâkim, kararını ancak duruşmaya getirilmiş ve huzurunda tartışılmış delillere dayandırabilir" denilmek suretiyle delillerin duruşmada tartışmaya açılarak müşterekliğinin sağlanması hususu hüküm altına alınmıştır. Hâkimin vakıa hakkında kişisel bilgisine dayanarak karar vermesi delillerin müşterekliği (kollektifliği) hususna ters düşmektedir[64]. Bu ilke çerçevesinde deliller toplandıktan

[61] N. Kunter ve diğerleri, 2010, s.1332.
[62] Yener Ünver, "Ceza Muhakemesinde İspat C.M.K. ve Uygulamamız", **Ceza Hukuku Dergisi2006,** 1(2), s.119.
[63] Ünver, Yener, Ceza muhakemesinde İspat ve Uygulamamız (İspat ve Uygulamamız) Ceza Hukuku Dergisi, sç 2,Aralık 2006,sç 119.
[64] Y. Ünver, a.g.m., s.120.

sonra ilgili herkesin duruşmaya ve her delil açısından görüş, iddia ve savunmalarını açıklamaya davet edilmeleri zorunludur[65].

7. Erişilebilirlik

Elde edilmeyen bir şeyin olayı temsil edici (ispat edici) özelliğinden yararlanabilmek mümkün değildir. Bir bulgu veya beyanı, Ispata elverişli olup olmadığının değerlendirebilmesi için öncelikle bu bulgu veya beyana ulaşılmış olması, muhakemece bilinmesi gerekmektedir. Bu yönüyle erişebilirlik, bulunması gereken bir özelliktir. Erişilmeye bir delinin, duruşmada tartışılması mümkün olmadığı gibi, duruşmada tartışılmayan bir delile dayanılarak da hüküm kurulması adil yargılanma hakkına aykırıdır[66]. Elde edilmeyen, erişilmeye bir delinin olayı temsil edildiği niteliği tam olarak bilinmeyecek gibi, olayı temsil edicilik özelliği bulunsa dahi özelliğinden faydalanamaz[67].

Delilin erişilebilir olması, somut olarak elde edilerek muhakemenin takdirine sunulabilir olmasını ifade eder. Ulaşılmasına asla mümkün olmayan veya belirsiz bir süre elde edilemeyen bir delil ceza yargılamasında kullanılamaz. Buna göre sanığın suç ortağının veya olay tanığının ölmesi, akıl hastalığına tutulmuş olması veya bulunduğu yerin öğrenilmemesi, bu kişilerin herhangi bir genel nedeniyle duruşmada hazır bulunmasının belirsiz bir süre için imkansız olması gibi durumlarda ortağının veya olay tanığının beyanını duruşmada elde etmek mümkün olmayacaktır [68].

Soruşturma veya kovuşturma aşamasında ulaşılmayan, elde edilmeyen bir bulgu veya beyanın olayla ilgili olup olmadığı ya da diğer bir değişle olayı temsil edip etmediği her zaman bilinemez. Ancak soruşturma aşamasında ulaşılıp da, delil olduğuna karar verilen ve zorlayıcı nedenlerle kovuşturma aşamasında tekrar incelenmeyen

[65] Y. Ünver, 2006, s.121.
[66] Şahin/Göktürk, C.II, sç 26. Centel/Zafer, s. 211.
[67] Toroslu/Feyzıoğlu, s. 171.
[68] Şahin ve Göktürk, sç 19-20, Özocak, s. 111.

(duruşmaya getirilmeyen) bulgular senin niteliğini devam ettirir. Çünkü bu bulgular, cumhuriyet savcısı tarafından değerlendirilmemiş (mevcudiyet şartı saklanmış) ve fakat sonradan duruşmaya getirilmemiştir. Nitekim CMK m. 211 bu gerçekten hareketle, zorlayıcı nedenlerle duruşmaya getirilen tanıkların daha önceki dinleme tutanaklarının veya yazdıkları belgelerin duruşmada okunmasıyla yeteneğinle bileceğini hüküm altına almıştır. Bir delil elde etmek mümkün olmamış ise, o delinin ikamesinden vazgeçilebilir[69].

Delilin mevcudiyeti sağlanıp da, delil olarak Kabul edilmesinden (değerlendirilmesinden) sonra dosyada muhafazası gerekir. Hüküm verilmiş ve kesinleşmiş olsa dahi, olağanüstü kanun yoluna müracaat edilebilme imkanı bulunduğundan, delillerin muhafazası zorunludur. Ancak zorunlu hallerde, bir kez değerlendirildikten sonra bir daha ele geçirilmeyen beyan veya duygular yerine, bunlara ilişkin tutanaklar okunarak duruşmada tartışıldıktan sonra vicdanı kanaate(hükme esas olabilmesi de mümkündür(CMK m.211).

C. Delil Çeşitleri

Doktrinde delillerin sınıflandırılmasına ilişkin çeşitli tasnifler yapılmıştır. Bu kapsamda deliller; sanık beyanı, tanık beyanı, bilirkişi mütalaası, keşif ve belgeler;[70] ya da şüpheli-sanık açıklamaları ve ikrar, şahitlerin izahatları yazılı belgeler, görüntü ve ses kaydeden araçlarla yapılmış olan kayıtlar ve belirtiler;[71] bundan başka bireysel anlatımlara dayanan deliller ve kişisel anlatım biçimi dışındaki deliller (Belirtiler)[72] şeklinde sınıflandırmalara konu olmuşlardır. Yine deliller; sanık açıklamaları, tanık açıklamaları, sanık ve tanıktan başka kişilerin açıklamaları, yazılı açıklamalar (belgeler), görüntü ve (veya) ses kaydeden araçlarla açıklama ve belirtiler şeklinde

[69] Kantar, sç 146.
[70] E. Yurtcan, 2005, s.269.
[71] V.Ö. Özbek ve diğerleri, 2012, s.604.
[72] Ö. Tosun, 1984, s.1

tasnif edilmiştir[73]. Alman doktrininde ise ispat araçlarının tanık, bilirkişi, belge ve görünüşe dayalı ispat aracı olmak üzere dört türe ayrılarak incelendiği de görülmektedir[74].

Medeni usul hukukunda deliller, hakimi bağlayıcı nitelikte olan kesin deliller ve hakimin serbestçe takdir yetkisine sahip olduğu takdiri deliller olmak üzere ikiye ayrılmaktadır. İkrar, kesin hüküm, yemin ve senet kesin deliller sınıfına; tanık, bilir kişi, keşif ve özel hüküm sebepleri ise takdiri deliller sınıfına girmektedir. Hukukumuzda senetle ispatı zorunlu olan hukuki işlemlerin uygulama alanının genişliği ile birlikte, ikrar ve yemin delillerinin karşı tarafın iradesine bağlı olması nedeniyle senet, hukuk yargılamasındaki ispat araçlarının belki de en önemlisidir[75].

Delilleri kaynaklarına göre, kaynağı kişiye dayanan deliller (sanık, tanık ve bilirkişi) ve kaynağı nesneye dayanan deliller (belge ve belirti delilleri) olarak ikiye ayırmanın da mümkün olduğu ifade edilmiştir[76]. Görüldüğü üzere, ceza muhakemesinde deliller, doktrinde çeşitli şekillerde tasnif edilmekle birlikte, çoğunlukla, beyan delilleri, belge delilleri ve belirtiler olmak üzere üç başlık altında sınıflandırılmaktadır[77].

Delillerin ispat gücüne ilişkin hiyerarşik bir sınıflandırma yapma amacında olmaksızın konunun sistematik olarak ele alınması açısından doktrindeki yaygın görüş çerçevesinde delil çeşitleri aşağıda ele alınacaktır. Bununla birlikte, hangi sınıflandırma esas alınırsa alsın, delil serbestliğinin geçerli olduğu ceza muhakemesinde, akla gelebilecek her unsurun delil olabileceği ve bu delilleri yargıcın özgürce kabul edebileceği unutulmamalıdır[78].

[73] B. Öztürk ve diğerleri, 2010, s.280.
[74] Y. Ünver, H. Hakeri, 2012, s.100.
[75] B. Kuru ve diğerleri, 2003, s.52.
[76] N. Centel, H. Zafer, 2011, s.201.
[77] N. Kunter ve diğerleri, 2010, s.1343
[78] V.Ö. Özbek ve diğerleri, 2012, s.633.

Mahkemenin hükme varark çözdüğü olayı ispatlayan deliller, doğrudan doğruya delil; ana vakıya bağlı yan vakıları olayları açıklayan deliller ise dolaylı delil olarak adlandırılmaktadır[79]. Mesela, A'nın B'ye ateş ettiğini gören tanığın beyanı asıl olayı ispatlayacak nitelikte olmakla birlikte, A'nın B'nin öldürüldüğü dükkanda parmak izinin bulunması ise asıl olaya bağlı olan A'nın olay yerinde bulunduğunu ispat edebilecektir. Bu doğrultuda beyan ve belge delilleri doğrudan delil, belirtiler ise dolaylı delil niteliğindedir. Ancak ifade etmek gerekir ki, mahkeme olayı kendisi görmediği için olay her halükarda dolaylı olarak ortaya konulmaktadır. Bu nedenle de ceza muhakemesinde tüm deliller aslında olayı dolaylı olarak temsil etmekte olup sadece bu dolaylılığın derecesi farklı olabilecektir. Bir delilin doğrudan doğruya olması veya dolaylı olması, o delilin hâkimde vicdani kanaat uyandırmasının derecesi ile ilgili değildir[80]. Dolayısıyla belge ve beyan delilleri ile belirtiler arasında bir mahiyet farkı bulunmadığını kabul etmek gerekir.

Bu kapsamda ceza muhakemesinde hiçbir delil türünün tek başına ispat kuvvetine sahip olmadığı, bunları destekleyen başka delillerin de bulunması gerektiği görüşüne katılıyoruz. Hâkim olayı doğrudan gördüğünü anlatan tanığın beyanını hiçbir değerlendirmeye tabi tutmaksızın hükmüne dayanak yapamayacağı gibi, olayı dolaylı olarak ispat eden bir delili de ispatta kullanmaması, hükmünde bu delile dayanmaması söz konusu olamaz[81]. Bu noktada hâkim, delillerin serbestçe değerlendirilmesi çerçevesinde, olayın mahkeme önünde tekrar canlandırılmasını sağlayan delilleri eşit bir şekilde ve bir bütün olarak değerlendirerek vicdani kanaate ulaşacaktır. Doğrudan delil-dolaylı delil ayrımını bu doğrultuda ve yukarıdaki açıklamalar ışığında kabul etmek gerekir. Aşağıda kısaca beyan delilleri, belge delilleri ve belirtilerin temel özelliklerine değinilecektir.

[79] N. Centel, H. Zafer, 2011, s.199-200.
[80] N. Centel, H. Zafer, 2011, s.201.
[81] Ali Kemal Yıldız, **Ceza Muhakemesinde İspat ve Delillerin Değerlendirilmesi**, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Doktora Tezi, İstanbul, 2002, s.137.

1. Beyan Delilleri

Uyuşmazlık konusu maddi olaya ilişkin açıklamalar beyan delilini oluşturur[82]. Beyanın delil olabilmesi için olayla ilgisi bulunan, olay hakkında doğrudan bilgi sahibi olan kişi tarafından verilmiş olması gereklidir[83]. Beyanların içeriğini sanık, tanık, mağdur gibi kişiler tarafından söylenen sözler oluşturmaktadır.

Şüpheli veya sanık beyanı savunmaya ilişkin olmakla birlikte maddi gerçeği bulma gayesi bakımından aynı zamanda delil niteliği taşımaktadır. Ceza Muhakemesi Kanunu'nun ikinci maddesinde şüphelinin güvenlik güçleri tarafından ifadesinin alınması ve Cumhuriyet Savcısı tarafından soruşturma kapsamınsdaki suçla hakkında dinlenmesini esasa almaktadır. Şüpheli veya sanığın yargıç veya mahkeme tarafından soruşturma ya da kovuşturma kapsamında dinklenmesine sorgu denilmiştir. CMK'nın 147. maddesi, şüphelinin veya sanığın ifadesinin alınmasında uyulacak esasları ve haklarını belirtmiştir. CMK'nın 191. maddesinde de duruşmada sanığın sorguya çekilmesinde 147. maddeye atıf yapılmış ve bu maddedeki hakların bildirileceği hüküm altına alınmıştır. Bununla birlikte, 148. maddede, şüphelinin ve sanığın beyanının özgür iradesine dayanması şartı getirilmiş ve yasak sorgu yöntemleri gösterilmiştir. Sanığın ifade vermesi ya da sorguya çekilmesi sırasında kendi özgür iradesiyle beyan etmesi şart olarak görülmektedir. Şüpheli ya da sanığa ifadesi alınırken irade özgürlüğünü engelleyici nitelikte yapılan davranışlar varsa şüpheli ya da sanığın ifadesi geçersiz olacaktır. Şüpheli ya da sanığın irade özgürlüğünü engelleyici davranışlar aşağıda sıralanmaktadır. Bunlar;

-Kötü davranış,

-İşkence,

[82] N. Centel, H. Zafer, 2011, s.201

[83] Feridun Yenisey, "Ceza Muhakemesi Hukukunda (Hukuka Uygun Bir Şekilde Elde Edilmiş) Delil", **Ceza Hukuku Dergisi 2007**, 2(4), s.19.

-İlaç verme,

-Yorma,

-Aldatma,

-Cebir ve tehditte bulunma,

-Bazı araçları kullanma,

-Bedensel ve ruhsal müdahalelerin yapılması.

Şüpheli, sanık ya da tanıkların yasak usüllerle ve özgür iradeye dayanmayan şekilde vermiş oldukları ifadeleri kendi özgür iradeleriyle verilmiş olsa da, delil sayılmayacaktır.

Kovuşturma aşamasında olay hakkında yapılan açıklamalar, olayı hâkimin zihninde canlandırmak bakımından beyan delilleri niteliğindedir. Bununla birlikte, soruşturma sırasında beyan delili özelliği bulunan izahatlar kovuşturma süresince belge delili olarak okunabilecek ve mahkeme önünde tekrarlandıkları takdirde bu evre için de beyan delili özelliği taşıyacaklardır[84]. İfade etmek gerekir ki, soruşturma aşamasında beyan delili niteliği taşıyan açıklamalar bakımından bir özellik söz konusudur. Ceza Muhakemeleri Kanunu'nun 148/4 maddesine göre müdafi hazır bulunmadan kollukça ifadesinin alınması eğer hakim veya mahkeme huzurunda şüpheli yada sanık tarafından doğrulanmazsa hüküm esas alınmayacaktır. Bu nedenle bu kanun maddesinin iyi şekilde değerlendirilmesi gerekmektedir. Eğer mahkeme içerisinde yapılmış olan sorguda müdafi hazır bulunmadan kolluk tarafından dalınan ifadenin içeriği reddedilirse eğer bu ifade olayın kovuşturması evresinde delil olarak nitelenmeyecektir. Bu nedenle şüpheli ya da sanığın sorgusu yapılırken müdafinin hazır bulunması gerekmektedir.

Ceza muhakemesinde yargılanan uyuşmazlığın konusu olan eylemin doğrudan doğruya beş duyusu ile algılamış olan kişinin belleğindeki bilgileri kovuşturma

[84] N. Centel, H. Zafer, 2011, s.201.

esnasında mahkemede anlatmasına tanık beyanı denilmiştir[85]. Ceza muhakemesine göre ehliyet şartı aranmaksızın herkes tanık olabilmektedir[86]. Ceza muhakemesinde tanık beyanı en çok başvurulan delillerden biri olarak görülmektedir. Fakat tanık beyanı çok fazla güven verici olarak görülmemektedir. Bunun nedenleri şu şekilde sıralanmaktadır. Bunlar;

-Tanıkların yalan söyleyebilmeleri,

-Tanıkların çekinme durumu,

Bu nedenlerin ortadan kaldırılması için kanun koyucu belirli önlemler almıştır. Bu önlemler şu şekilde sıralanmaktadır. Bunlar;

-Tanıkların yemin etmesi,

-Tanıkların ayrı ayrı dinlenilmesi,

-Tanıkların yüzüne karşı ve alenen beyanda bulunmaları,

-Yalan beyanın suç olarak kabul edilmesi[87].

Tanıklık yapmak kamu hukukunda yer alan toplumsal bir ödev olmakla birlikte, tanıklık yapacak kişinin adli makamların önüne gelme, yemin etme ve bildiklerini doğru olarak söyleme gibi birtakım ödevleri bulunmaktadır. Bununla birlikte, tanıklar, tanıklıktan çekinme, cevap vermekten çekinme, haklarını öğrenme, tazminat ve masraf alma ve korunma hakkı gibi birtakım haklara sahiptir[88].

Ceza Muhakemeleri Kanunu'nun 45. maddesine göre bazı tanıklara tanıklıktan çekinme hakkı tanınmıştır. Sanıkla yakın aile ilişkisi bulunan kimselerin aileleri hakkında yalan beyanda bulunmamak yada yakını aleyhine beyanda bulunmak arasında tercih yapma zorunda bırakılmaması, aile içerisindeki güven ilişkisinin zedelenmemesi

[85] N. Kunter ve diğerleri, 2010, s.1346.
[86] N. Toroslu, M. Feyzioğlu, 2009, s. 179.
[87] N. Toroslu, M. Feyzioğlu, 2009, s. 180.
[88] N. Centel, H. Zafer, 2011, s.229.

için tanıklıktan çekinme hakkı tanınmıştır. Ceza Muhakemeleri Kanunu'nun 46. maddesine göre ise meslek ve sürekli uğraşıları nedeniyle bazı kimselere tanıklıktan çekinme hakkı verilmiştir (CMK m. 210/2)

Son olarak, özellikle suç örgütünün faaliyeti çerçevesinde işlenen suçlar bakımından tanıklık ödevinin yerine getirilmesi tanık veya yakınları için tehlike teşkil edebilecektir. Bu kapsamda ceza muhakemesinde tanıkların korunması amacıyla tedbirler alınabilmesi mümkündür[89]. Tanıkların korunması ile ilgili bir prosedür hazırlanmıştır. Bu prosedürün hazırlanma nedeni bazı tanıkların, kendilerinin veya çevrelerindeki yakınlarının hayatının korunması, beden bütünlüğü ve bunun yanında mal varlığı ciddi şekilde tehlikede bulunan kişilerin korunması olarak belirlenmiştir.

CMK'nın 58. maddesinde tanığın korunması müessesesi düzenlenmiştir. Bu konuda 27.12.2007 tarihinde kabul edilen 5726 sayılı Tanık Koruma Kanunu'nda üçüncü kişi tanıklar ve mağdur tanıklar ile bu kişilerin Kanun'da sayılan yakınları hakkında uygulanacak koruma tedbirleri gösterilmiş, tedbire karar verilmesi ve tedbirin uygulanması düzenlenmiştir. İfade etmek gerekir ki, gizli tanık dinlenmesi ile adil yargılanma hakkının ihlali arasında ince bir çizgi bulunmaktadır ve tanığın korumak için alınan tedbirler çoğu zaman sanığın savunma hakkını kısıtlayabilmektedir ve bu yüzden adil yargılanmaya gölge düşmektedir. Tanığın korunması sanığın savunma haklarını hiçbir şekilde ihlal etmemelidir ve bu bakımdan tanık ve yakınlarının korunması ile sanığın savunma hakkı arasında adil bir denge kurulması son derece önemlidir.

CMK'nın 58. maddesinin 3. fıkrası ile sanığın ve diğer kişilerin soru sorma hakkı güvence altına alınmıştır. Yine Tanık Koruma Kanunu'nun 9/10. maddesinde haklarında koruma tedbiri kararı alınan tanıkların dinlenmesine ilişkin hükümlerin

[89] Bahri Öztürk, **Yeni Yargıtay Kararları Işığında Delil Yasakları**, Ankara, Ankara Üniversitesi Siyasal Bilimler Fakültesi İnsan Hakları Merkezi Yayınları, 1995, s. 304.

savunma hakkını kısıtlayacak şekilde uygulanamayacağı hüküm altına alınmıştır. Bununla birlikte, AİHM kararları da göz önüne alındığında, yalnızca gizli tanık beyanlarından hareketle mahkumiyet hükmü verilmesi de kabul edilemez. Bu doğrultuda gizli tanık beyanları inandırıcı ve pekiştirici başka delillerle desteklenmedikçe tek başına mahkumiyet hükmüne dayanak olamayacaktır.

2. Belge Delilleri

Resmi ya da özel belge niteliği taşıyan tüm evrak, yazı, ses ve görüntü kayıtları belge delillerini oluşturmaktadır. Belge delilleri üçe ayrılmaktadır. Bunlar şu şekilde sıralanmaktadır.

-Yazılı belgeler,

-Şekil tespit edilen belgeler,

-Ses tespit eden belgeler[90].

Belge delillerinin beyan delillerine göre daha objektif ve güvenilir olduğu bilinmektedir. Fakat belge delillerinin sahteliği de karşı taraf tarafından iddia edilebilecektir. Bu nedenle belge delilleri konusunda dikkat edilmesi gerekmektedir.

Yazılı belgeler; somut olayı tespit ederek, olayın yazıya döküldüğü belgeler olarak tanımlanmaktadır[91]. Bir işletmede bir memurun görevi nedeni ile düzenlemiş olduğu belge resmi belge olarak adlandırılmaktadır Adı geçen belgelerden ayrılan diğerleri özel belge olarak adlandırılmaktadır. Resmi belgelerin ispat gücünün özel belgelerin ispat gücünden fazla olduğu bilinmektedir[92].

Yazılı belgeler sağlamlıkları ve güvenilirlikleri açısından üçe ayrılmaktadır. Bu belgeler şu şekilde sıralanmaktadır. Bunlar;

[90] N. Kunter ve diğerleri, 2010, s.1385.
[91] Y. Ünver, H. Hakeri, 2012, s.117.
[92] N. Toroslu, M. Feyzioğlu, 2009, s. 192.

-Aksi sabit oluncaya kadar geçerli olan yazılı belgeler[93],

-Sahteliği sabit oluncaya kadar geçerli olan yazılı belgeler.

Aksi sabit oluncaya kadar geçerli olan yazılı belgelerin içeriğinin gerçeği yansıttığı yolunda bir karine kabul edilmiş olup aksinin ispatının mümkün olduğu dile getirilmiştir. Sahteliği kanıtlanan kadar olayla ilgili belgelerin kapsamının gerçeği gerçeği yansıttığı söylenmektedir. Bu karine güçlü bir karine olarak kabul edilmiştir. Belgenin sahte olduğu ispat edildiği noktada bu karine çürütülecektir.

Bir olayı temsil eden ve belli bir biçimde belgeler de bulunmaktadır. Bu belgeler aşağıdaki şekilde sıralanmaktadır. Bunlar[94];

-Fotoğraf,

-Resim,

-Kroki,

-Plan vb.

Bu tür belgelerin de sahtelik iddiasıyla karşılaşması mümkün olup bunların da güvenilirliğinin denetlenmesi gerekmektedir.

Ceza muhakemesinde her şeyin delil olarak kabul edilebileceği bilinmektedir. Bu noktada ses ve görüntü kayıtlarının da birer delil olarak kullanılabileceği bilinmektedir. Ses ve video kaydı ile oluşturulan belgeler de bulunmaktadır. Bu belgeler; ses ve görüntü tespit eden belgeler olarak tanımlanmaktadır[95]. Bu tür kayıtlar da belge niteliğinde görülmektedir. Bununla birlikte, bant kayıtlarının yazılı olmadığı ve

[93] N. Kunter ve diğerleri, 2010, s.1385.
[94] N. Kunter ve diğerleri, 2010, s.1386.
[95] N. Kunter ve diğerleri, 2010, s.1387.

okunma kabiliyetinin de bulunmadığı için belge olarak kabul edilmeyeceği bilinmektedir. Fakat bantlar keşif konusu olabilecek şeyler olarak düşünülmektedir[96].

Bant kayıtları yanlarında inandırıcı ve pekiştirici deliller bulunmadıkça tek başına mahkumiyet hükmüne dayanak olmayacaktır. Bu nedenle Yargıtay tarafından da suçu tek başına ortaya koymasına yetecek belgeye sahip olmayan iletişimin tespit tutanakları hariç kanıt bulunamamsı yüzünden bozma kararı verilmiştir[97]. Bununla birlikte, bu kayıtlatın ancak sahteliği konusunda hiçbir şüphe bulunmadığı hallerde delil olarak kabul edilebileceği, aksi halde diğer deliller ile birlikte değerlendirme kapsamına alınmaması gerektiği ifade edilmektedir[98]. Bu tür delillerin ceza muhakemesinde sınırlı bir ispat gücüne sahip oldukları bilinmektedir.

Görüntü veya ses tespit eden belgeler, özel hayata ve kişilik haklarına müdahale söz konusu olduğunda farklı bir öneme sahiptir. Özellikle delil elde edilmesi veya şüphelinin yakalanması için başvurulmuş olan bir tedbir olarak iletişimin kontrol edilmesi özel hayatın gizliliğini ihlal etmektedir ve bu sebeple bir takım sıkı koşullara bağlanmıştır. Kanun koyucu bu koşulları kabul ederek iletişimin denetlenmesi yoluyla delil elde etmenin istisnai bir yol olduğunu vurgulamaktadır. Dolayısıyla kurallara uyulmadan, hukuka uygun olmayan şekilde elde edilen bu tip belgelerin delil olarak kabul edilmesi mümkün değildir.

3. Belirtiler

Belge ve beyan dışında kalan diğer delil türü olan belirtiler; genel olarak keşif ile ortaya çıkabilecek ve olaydan geriye kalan her türlü iz ve eserler olarak tanımlanmaktadır. Bu deliller hakkında hüküme varılması gereken ana olayla ilintili yan

[96] E. Yurtcan, 2005, s.338.
[97]YCGK, E.2010/8-134, K.2010/217, T. 9.11.2010

[98] Serap Keskin, **Ceza Muhakemesi Hukukunda Temyiz Nedeni Olarak Hukuka Aykırılık**, İstanbul, Alfa Yayınları, 1997, s.175.

olayları açıklamaktadır[99]. Örnek vermek gerekirse; suç yerinde kalan ayakkabı veya bardak üzerindeki parmak izi asıl olayı tek başına açıklamasa da şüphelinin olay yerinde bulunduğunu ispat edebilecektir bu nedenle büyük önem taşımaktadır. Bununla birlikte, belirtilerin olay örgüsünün birer parçasını teşkil eden maddi vakalar olduğu ve bunların ispatının yine deliller tarafından gerçekleştirilebileceği ifade edilmektedir[100].

Bilim ve teknolojide yaşanan hızlı ve kapsamlı gelişmeler, ceza muhakemesinde de yaygın bir şekilde kullanılmaya başlamıştır. Bilimsel gelişmelere bağlı olarak, örneğin bir saç telinden bir kişinin suç yerinde olup olmadığının tespiti gibi olanaklar doğdukça belirtilerin önemi daha da artmıştır[101]. Bununla beraber; belirtilerin anlamlandırılarak, bir diğer deyişle konuşturulabilmesi çoğu zaman keşif veya bilir kişi incelemesi ile mümkün olmaktadır[102] .

Belirtiler ikiye ayrılmaktadır. Bunlar;

-Tabii belirtiler,

-Suni belirtiler.

Tabii belirtiler; sanığın iradesi dışında olayı tabi bir şekilde temsil eden belirtilerdir. Suni belirtiler ise eylemin iradesi veya bir kişi tarafından belirli bir amaç için hazırlanan belirtilerdir. Bu kapsam içerisinde olay yerinde kalan parmak izi veya kan tabii belirtiye, bir biletin işaretlenmesi ise kullanıldığını göstererek suni belirtiye örnek olarak gösterilebilmektedir[103].

[99] N. Centel, H. Zafer, 2011, s.200.
[100] Fulya Eroğlu, **Beden Muayenesi ve Vücuttan Örnek Alma Suretiyle Elde Edilen Delillerin İspat Değeri,** Yeditepe Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2009, s.6.
[101] Ö. Tosun, 1984, s.10.
[102] N. Centel, H. Zafer, 2011, s.201; Cumhur Şahin ve Neslihan Göktürk, **Ceza Muhakemesi Hukuku II**, 2. Baskı, Ankara, Seçkin Yayınevi, 2013, s.47
[103] Y. Ünver, H. Hakeri, 2012, s.118.

4. Dijital Veriler

Günümüzde dünyada bilgi üretme ve üretilen bilgiye erişme hızı günden güne artmaktadır. Buna bağlı olarak insanların günlük yaşamında da büyük değişiklikler yaşanmaktadır. Bu yaşanan değişimin en önemli nedeni olarak bilgi ve iletişim teknolojileri görülmektedir. Bilgi ve iletişim teknolojileri bireylerin günlük alışkanlıklarını da etkilemektedir. Bilgi ve iletişim teknolojileri eğitimden ticarete, bankacılıktan iletişime kadar tüm sektörleri olumlu yönde etkileyerek hayatı kolaylaştırmaktadır. Birçok kavram elektronik sözcüğünün e harfi ile birleşerek kullanılmaya başlamıştır. Bu kavramlara örnek olarak; e-posta, e-devlet ve e-imza verilebilmektedir. Dijital ortam içerisinde birçok yerde bilgi üretilmektedir. Bu bilginin üretildiği gibi dijital ortam içerisinde saklanması gerekmektedir. Bu nedenle bilgi güvenliğine karşı oluşan risk ve tehditlerin çözümlenmesi ve bilginin dijital ortam içerisinde rahat bir şekilde korunması sağlanmalıdır.

Bilgi ve iletişim teknolojisi içerisinde birçok risk ve tehditler bulunmaktadır. Birçok bilgi ve iletişim teknolojisini kullanan kişi risk ve tehditlerin ne kadar ciddi olduğunun bilincinde değildir. Fakat bu risk ve tehditler kullanıcıları büyük maddi kayıplara uğratabilmektedir. Bunun yanında kullanıcıların dijital ortam içerisinde sahip oldukları bilgilere izinsiz olarak erişim mümkün olduğundan dolayı buna karşı güvenlik önlemleri geliştirilmiştir. Kullanıcıların bilgilerinin silinmesi ve değiştirilmesi maddi ve manevi kayıpların ortaya çıkmasına zemin hazırlamaktadır. Bu hasarların önlenebilmesi için bilgi ve iletişim teknolojileri ile ilgili güvenlik önlemlerinin geliştirilmesi sağlanmalıdır[104].

Bilgi dünyada sürekli değişen ortam içerisinde dolaşmaktadır. Bu bilginin sürekli erişebildiği ortam içerisinde bilginin gönderildikten sonra gizlilik içinde

[104] Köksal Özenç, "Bilgi ve iletişim teknolojilerinde kişisel ve kurumsal bilgi güvenliğinin sağlanması", **Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı**, 13-14 Aralık 2007, Ankara, s.52

bozulmadan, değiştirilmeden ve başkalarının eline geçmeden güvenli bir şekilde iletilmesine bilgi güvenliği adı verilmektedir[105]. Bilgi güvenliği kavramı eski zamanlarda öncelikle yazılı ve basılı platformlarda yer alan bilgilerin fiziksel olarak güvenliği sağlanmasıydı[106]. Dünyada bilgi güvenliği ile ilgili süreç bilişim teknolojileri açısından değerlendirilmektedir. Bu nedenle bilgi güvenliği düşünülünce artık dijital veri güvenliği kavramı düşünülmeye başlamıştır. Dijital veri güvenliği; elektronik ortam içerisinde bulunan verilerin bütünlüğü bozulmadan, izinsiz erişimlerden saklanarak aktarılması için bilgi işleme ortamlarının güveniğinin sağlanması olarak tanımlanmıştır[107].

Dijital veri güvenliğini dünyada tehdit eden birçok etmen bulunmaktadır. Bu etmenler aşağıdaki şekilde sıralanmaktadır;

-Dünyada meydana gelen doğal afetler nedeniyle güç kaynakları, kamera sistemleri ve telefon santrallerinin arızalanması,

-İnternet üzerinde e-posta, internet bankacılığı ile çevrim içi alışveriş ve donanımda ortaya çıkan sorunlar,

-Bilgisayar virüsleri,

-Dijital ortamda yetkili erişimlerin kötü şekilde kullanılması.

Bilgi güvenliğini oluşturan zincirin en zayıf halkası olarak insan kaynaklı tehditler görülmektedir[108]. Bu tehditler bazı noktalarda bilinçsizce ya da yeterli eğitime

[105] A. Howard Schmidt, **Building a Mosaic Of Security For A Better World, Security Matters**. USA, Aspatore Books, 2004, s.25

[106] Türkay Henkoğlu, Bülent Yılmaz, "Avrupa Birliği (AB) Bilgi Güvenliği Politikaları", **Türk Kütüphaneciliği 2013**, 27(3), s.451-471.

[107] Gürol Canbek, Şeref Sağıroğlu, "Bilgi, Bilgi Güvenliği Ve Süreçleri Üzerine Bir İnceleme", **Politeknik Dergisi 2006**, 9(3), s.165-174

[108] Andreas E. Wagner, Carole Brooke, "Wasting Time: The Mission İmpossible With Respect To Technologyoriented Security Approaches Electronic", **Journal of Business Research Methods 2007**, 5(2), ss.117-124.

malik olmadan çıkabileceği gibi, bilinçli olarak sisteme zarar verilmesi olarak da görülebilmektedir[109].

Symantec[110] tarafından yayımlanmış olan 18. *İnternet Güvenlik Tehdit Raporu (ISTR*) verilerine göre 2012'de gerçekleşen siber saldırılar, bir önceki yıla göre % 42 artmıştır bu da göstermektedir ki internetle ilgili dünya üzerinde büyük tehditler bulunmaktadır. 18. İnternet Güvenlik Tehdit Raporu'na göre Avrupa ülkeleri arasında Türkiye değerlendirildiğinde istem dışı eposta (spam) saldırılarında beşinci olduğu, olta saldırılarında sekizinci olduğu, virüs saldırılarında da beşinci sırada olduğu görülmektedir. Dünyada ve Türkiye'de dijital veri güvenliğine yönelik olarak yapılan ampirik araştırmaların önemi her geçen gün artmaktadır. Bu nedenle bu çalışmaların yapılması için bilgi ve iletişim teknolojileri ile ilgili çalışan yazılımcılar teşvik edilmektedir.

Bilgi güvenliği konusunda birey, kurum ve kuruluşlar önceden önlem almak yerine ciddi bir sorun ortaya çıktığında bu sorunu ortadan kaldırmak için acil önlem planları geliştirmektedir. Bu nedenle bilgi güvenliği konusunda farkındalığın arttırılmasına ihtiyaç bulunmaktadır. Bilgi güvenliği ile ilgili özellikle kurumlarda yönetim seviyesindeki kişilerin bir sistem kurmalarının sağlanması için farkındalıklarının arttırılması gerekmektedir[111].

Bilişim teknolojilerinde çok büyük bir gelişme yaşanmaktadır. Bu gelişmenin sonucunda da bilişim teknolojileri insan hayatına birçok kolaylık sağlamıştır. Bankacılıkla ilgili her türlü internet üzerinden yapılmaktadır. Para çekme, yatırma, kredi karıyla yapılan her türlü işlem ve akla gelmeyen bir çok işlem biilişim

[109] Mehmet Tekerek, Bilgi Güvenliği Yönetimi, **KSÜ Fen ve Mühendislik Dergisi 2008**, 11(1), s.132.
[110] Symantec, **Internet Security Threat Report**. http://www.symantec.com/content /en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf (25.09.2017).
[111] Meltem Kocamustafaoğulları, **Bilgi Güvenliği Farkındalığı Ve Uygulama Seviyesi Değerlendirmek İçin Bilgi Güvenliği Prototip Uygulaması,** Yayımlanmamış Yüksek Lisans Tezi, Çankaya Üniversitesi, Fen Bilimleri Enstitüsü, Ankara, 2013, s.58.

teknolojileri sayyesinde gerçekleşmektedir. Bunun doğal bir sonucu olarak bilişim güvenliği oratya çıkmıştır. Yıllar ilerledikçe bilişim güvenliğini tehdit eden faktörlerde bir artma görülmektedir. Günümüzde de en önemli suçların başında bilişim suçları gelmektedir.

Bilişim suçları çok geniş bir alana yayılmış ve günden güne artan bir hızda büyümeye devam etmektedir. Bu nedenledir ki bilişim suçları ile ilgili bir sınır çizilmemiştir. Bilişim suçları ile ilgili yerli ve yabancı literatürde birçok tanım görülmektedir. Bilişim suçu ile ilgili Amerikan Adalet Departmanı'nın yapmış olduğu tanıma göre bilişim suçu; ceza kanunu ihlal eden, bilgisayar teknolojisi bilgilerini içeren bilgileri araştırılması suç olarak kabul edilmiştir[112].

Bilgisayarla ilintili suçlarla ilgili olarak Amerika Birleşik Devletleri Kanunları incelendiğinde yargılanabilecek şekilde bazı illegal eylemler tanımlanarak, yorumlanmaktadır. Bu nedenle ülkelerin ulusal güvenlik bilgilerinin, banka ve finans bilgilerinin, eyaletler arası ve uluslararası ticaret bilgilerinin büyük bir özenle korunması gerekmektedir[113].

Bilişim suçu Teksas Ceza Kanunları'na göre; bilgisayara, bilgisayar sistemlerine ve bilgisayar ağlarına sahibinin izni olmadan girmek olarak tanımlanmaktadır. Bilişim suçu ile ilgili bu tanım dar bir tanım olarak görülmüştür[114]. Türkiye'de Ankara Emniyet Müdürlüğü tarafından yapılmış olan çalışmalara göre bilişim suçlarında yıllar içerisinde büyük bir artış gözlenmektedir.

Bilişim suçları incelendiğinde bu suçların büyük bir çoğunluğunun internet üzerinden işlendiği görülmektedir. Bilişim suçları içerisinde en sık karşılaşılan suçlar aşağıdaki gibi sıralanmıştır. Bunlar;

[112] USDOJ, **U. S. Department of Justice**, FBI LAw Enforcement Bulletin, August, 2004, s.22.
[113] USC, **Title 18 of the US Code, in Chapter 47**, Section 1030, 2002, s.12.
[114] TPC, **Texas Penal Codes Section,** 2002

-Çocuk pornografisi,

-Kredi kartı dolandırıcılığı,

-Bilgi hırsızlığı,

-Sistemlere izinsiz erişim,

-Telif haklarının ihlali olarak görülmektedir.

Bir bilişim suçu ile ilgili olarak elektronik ve manyetik bir ortam üzerinden iletilmesi sağlanan ve bu ortam içerisinde saklanan veriler dijital kanıt olarak adlandırılmaktadır. Dijital delillerin ilgili birimlere sunulmasına ise dijital delillendirme adı verilmektedir. Dijital delillendirme ceza muhakemesinde de yoğunlukla kullanılmaktadır.

Dijital deliller aşağıda sıralanmaktadır. Bunlar;

"-Veri dosyaları,

-Kurtarılmış silinmiş dosyalar,

-Kayıp alanlardan kurtarılmış veriler,

-Dijital fotoğraf ve videolar,

-Sunucu kayıt dosyaları,

-E-Posta,

-Chat kayıtları,

-İnternet geçmişi,

-Web sayfaları,

-Kayıt logları,

-Abone kayıtları"

Normal delillere göre dijital delillerde bazı sıkıntılar bulunmaktadır. Bu sıkıntılar aşağıda şu şekilde sıralanmaktadır[115].

-Dijital delillerin bir bütün olması gerekmektedir. Dijital delilleri oluşşturan dijital bilgiler kolayca silinip, değiştiği yenisi oluşturalabilme gibi eylemlerle işlem yapılabildiği için bu delillerin bütünlüğünü sağlamak zordur. Bu nedenle bu delillerle ilgili güvenlik önlemlerinin alınması gerekmektedir.

-Dijital delillerin doğrulanması gerekmektedir. Eğer bir sanık yada şüpheli dijital deliller ile yakalanmışsa o delillerin o kişiye ait olduğunun mahkeme sürecinde tespit edilmesi gerekmektedir. Bu delil olarak ele geçirilen dijital delillerin aynısı herhangi bir kişi tarafından fa oluşturulmuş olabilir. Özellikle şüpheli ya da sanık adı geçen dijital delillerin güvenlik güçleri tarafından yapıldığını iddia edebilmektedir. Bu nedenle elde edilen dijital delillerin şüpheli ya da sanığa ait olduğunun kesinlikle mahkeme sürecinde teyitinin yapılması gerekmektedir.

-Dijital delillerin inkar edilememesi gerekmektedir. Sanık ve şüpheli ile beraber ele geçirilen dijital delillerin sanık ve şüpheli tarafından delilin alındığı medyanın, delilin ele geçirildiği zaman ve delilin içeriği gibi bütün unsurlarının sanık ya da şüpheli tarafından inkar edilememesi gerekmektedir. Bununla ilgili güvenlik önlemlerinin alınması sağlanmalıdır.

-Dijital delillerin doğru olması gerekmektedir. Sanık yada şüpheli ile beraber ele geçirilen dijital delillere ulaşılma noktasında kullanılan teknikler ve kullanılan bilgilerin doğruluğunun da mahkeme tarafından ispat edilmesi gerekmektedir. Bu şekilde dijital delillerin doğruluğu kabul edilmiş olacaktır.

[115] Chet Hosmer, "Providing The Integrity of Digital Evidence With Time", **International Journal of Digital Evidence 2002**, 1, s.55.

-Dijital delillerin daha sonradan ele alınabilir olması gerekmektedir. Sanık yada şüpheli ile beraber ele geçirilen dijital delillerin üçüncü kişiler tarafından incelenebilir durumda olması gerekmektedir.

Dijital deliller ele geçirildiğinde göze çarpan etkenler şu şekilde sıralanmaktadır. Bunlar;

-İnternet ile ilgili özel dosyalar,

-Elektronik aygıtlar,

-Geniş alan ağları,

-Kuruluş kaynakları,

-Bilgisayarlar,

-Yedekleme üniteleri,

-Veri havuzları,

-Yazılımlar,

-E-postalar,

-Bir sistem içerisinde yapılan işlemleri gösteren kayıtlar, geçmiş bilgiler ve erişim listeleri.

II. CEZA MUHAKEMESİNDE DELİLLERİN DEĞERLENDİRİLMESİNİN TARİHSEL GELİŞİMİ: MUHAKEME SİSTEMLERİ VE İSPAT SAFHALARI

Bu bölümde muhakeme sistemlerinin geçmişten günümüze doğru gelirken nasıl evrildiğini ve delilerin bu evrilme sürecindeki değişiminden bahsedilmiştir. Ceza yargılaması hukuku kurumlarının tarihçesi, ceza yargılamasında ispat prensipleri hakkında yol gösterici olacaktır. Hukuk kuralları süreç içerisinde ihtiyaçlar karşısında değişir ve gelişir. Değişim ihtiyacı toplumun sosyo-ekonomik ihtiyaçları doğrultusunda olmaktadır. Ancak bu değişim her zaman aynı ivme ile devam etmez. Hukuk kuralları

değişim yaşarken geçmişten büsbütün kopmaz. Önceki ve sonraki yapılar arasında hep bir devamlılık söz konusudur. Bugünü anlamak bu kurumların tarih sürecindeki değişimini ve gelişimini anlamakla mümkün olacaktır .[116]

Ceza muhakemesi, hukuk tarihi içerisinde bir takım insan hak ve hürriyetleri doğrultusunda değişmiştir. Ceza adaleti, yargılama faaliyetine katılan süjelerin hak ve hürriyetleri veya toplumsal düzenin devamını koruma endişesine göre şekil almaktadır. Günümüzden geçmişe dönüp baktığımızda ceza yargılama yaygın görüşe göre üç safhadan geçmiştir. Bunlar "*itham*", "*tahkik*" ve "*karma veya işbirliği*" sistemi olarak tasnif edilmektedir. Bu değişim ve dönüşüm elbette ki ülkelerin siyasi, sosyal ve iktisadi yapasına bağlı olarak gerçekleşmiştir.[117] Bu yargılama sistemlerindeki dönüşüm yargılamanın bütününe yansımıştır.Mahkemenin süjelerinden ispat prensiplerine kadar bütün ceza yargılamasının kurumlarına sirayet etmiştir. İspat ve delil de tarih içerinde çeşitli aşamalardan geçmiştir. Bu safahatlar çeşitli tasniflere göre sınıflandırılmıştır. Doktrindeki yaygın sınıflandırma "*ilkel delil*", "*dinsel delil*", "*kanuni delil*", "*vicdani delil*" ve adli bilimlerin gelişmeleri doğrultusundaysa "bilimsel delil" olacak şekilde beş kısma ayrılarak yapılmaktadır. İspat da delilden bağımsız olarak tasnife tabi tutulduğunda "*ilkel safha*", "*dinsel safha*" ve "*akılcı safha*" olarak üçe ayrılmaktadır. Delillerin, ispat prensiplerine göre ayrımı ise "*ilkel delil*", "*kanuni delil*", "*delil serbestliği*" ve "*vicdani delil*" olmak dört safhaya ayrılmaktadır.[118]

Bu değişim tarihsel süreç içerisinde her ülke için eş zamanlı olmamıştır. Ülkeden ülkeye değişim farklı zamanlarda olmakla birlikte aynı safhalar da birbirinitakip eder gibi gerçekleşmemiştir. Kıta Avrupası'nda bu süreç etnik, dinsel ve kanuni safhayı vicdani safha takip ederken, İngiltere'de ve sonra da Amerika'da jüri sistemi takip etmiştir. Jüri sitemi ile akli muhakeme, akılcı delil, vicdani kanaat ve ispat

[116]Centel N, Zafer H. Ceza Muhakemesi Hukuku, 10. Bası, İstanbul, Beta Basım Yayım Dağıtım, İstanbul, 2013: 18-47; 680-9.
[117]Soyaslan D. *Ceza Muhakemesi Hukuku*, 5. Baskı, Ankara, Yetkin Yayınları, 2014: 71-6.
[118]Aydın D. Ceza Muhakemesinde Deliller, Ankara, Yetkin Yayınları, 2014: 15- 88.

sistemi şekillenmeye başlamıştır. Daha sonra sanık haklarının gelişmesiyle sanık, yargılama içerisindeki nesne konumundan yargılamanın bir süjesi konumuna erişerek diğer ülkelere örnek olmuştur. İngiltere' de başlayan bu iyileşmeler sonraki yıllarda Fransa'ya oradan da Kıta Avrupası'na yayılmıştır. Günümüzde adil yargılanma ve insan haklarına dair uluslararası belge ve sözleşmeler ortak bir yargılama kültürünün oluşmasına katkı sağlamaktadır. Oluşan bu ortak yargılama kültürünün bugünkü sonucu; maddi vakayı temsil eden, mahkemeye getirilebilen, kolektif, akılla kavranabilen ve hukuka uygun olarak elde edilmiş olan delillerin yargılama makamının vicdani kanaatine göre serbestçe değerlendirilebilir olmasıdır.[119]

A. Muhakeme Sistemleri

İnsanın tarihsel süreç içindeki değişimi, muhakeme sistemlerine de yansımıştır. Bilinenden günümüze kadar geçen muhakeme süreçleri aşağıda aktarılmıştır.

1. İtham Sistemi

Bilinen ilk ve en eski yargılama sistemidir. Ancak çıkış kaynağı bilinmemektedir. İtham sistemi, suçtan zarar gören bireyi ilgilendirdiği dönemde ortaya çıkmıştır. Yani yargılamayı kişilere bırakan, taraf yargılaması şeklinde zuhur eden bir sistemdir .[120]Tarihte en belirgin izleri Roma'nın ilk dönemlerinde ve Kıta Avrupası feodalitesinde görülmüştür. Bugün Anglo-sakson ülkelerde (İngiltere ve Amerika Birleşik Devletlerinde) uygulanmaktadır.[121] Bu yargılama sistemi kamusal bir yargılamadan ziyade özel yargılamaya benzemektedir. Hakim, kamu görevlisi olmayıp halkın içinden taraflarca seçilip azledilen bir statüdedir. Ancak süreç içerisinde hakim kamu otoritesi tarafından seçilmektedir. Süreç içerisinde bu yargılamaya jüri sistemi de

[119]Aydın D. Ceza Muhakemesinde Deliller, Ankara, Yetkin Yayınları, 2014: 15- 88.
[120]Özbek VÖ, Kanbur MN, Doğan K, Bacaksız P, Tepe İ. Ceza Muhakemesi Hukuku, 7.Baskı, Ankara, Seçkin Yayıncılık, 2015: 45-8; 672-39.
[121]Yayla M. Ceza yargılamasında ispat için yenilmesi gereken şüphe; Türkiye ve Amerika Birleşik Devletleri sistemlerinin incelenmesi, *Ankara Barosu Dergisi*, 2013, 3: 291-13.

entegre edilmiştir. Bu sistemde, yargıyı harekete geçiren mağdurun kendisidir. Yani hakim kendiliğinden harekete geçmez. Hakim, hakem konumundadır. Tarafların karşılıklı mücadele etmelerinde süreci eşit yönetmektedir.

Yargılama çekişmeli, aleni ve sözlüdür.[122] Taraflar, birbirlerinin iddialarına karşı savunma yapmaktadır. Yargılamada her delil konuşulur. Hakim, tarafların ortaya koymuş oldukları delillerle bağlıdır. Hakim bizzat işin içinde değildir. Hakim re'sen delil araştırması yapmaz ancak taraflar eşit konumdadır. Deliller, davacı ve sanığın huzurunda sunularak tartışılırdı .[123] Hakim, suçun cezasını vicdani kanaatine göre verdiği tahmin edilmektedir. Sistem liberal ve demokratik siyasal rejimlere daha uyumludur. İtham sistemindeki ispat prensibi ise, tatbik edildiği dönemlerin inanışlarına ve gelişmişliğine bağlı olarak önceleri akıl dışı ve dini delile dayanıyorken, zaman içerisinde vicdani ispat prensibine doğru evrilmiştir.[124]

2. Tahkik Sistemi

Ortaçağ Avrupası'nda "*Engizisyon Mahkemeleri*" nde Kabul edilen "kanuni delil; ikrar" esaslı gizli ve yazılı yapılan yargılama, tahkik(soruşturma) sistemi olarak kabul edilir. Bu yargılama sisteminde esaslı bir yargılama faaliyeti yürütülür ve bütün yargılamayı hakim yapar. Fail bu sistemde süje değil, "*nesne*"dir.[125] Kilise'nin bu sistemi uygulamasının altında yatan neden "*Tanrı adına*" ve "*Tanrıyı temsil etme ve yanılmazlık*"tır. Bu sistemin tipik yanı hakimin maddi vakaya doğrudan el koymasıdır.[126] Tahkik sistemi, kanuni bir delil olan ve delillerin kraliçesi addedilen

[122]Birtek F. AİHM, Anayasa Mahkemesi ve Yargıtay Kararları Işığında Ceza Muhakemesinde Delil ve İspat, Ankara, Adalet Yayınevi, Ankara, 2016: 255- 579.
[123]Altunkaş A. Hukuka Aykırı Delil Teorisi Işığında İfade Alma Ve Sorgu, Sosyal Bilimler Enstitüsü Hukuk Yüksek Lisans Programı, Yüksek Lisans Tezi, İstanbul: İstanbul Bilgi Üniversitesi, 2006.
[124]Özbek VÖ, Kanbur MN, Doğan K, Bacaksız P, Tepe İ. Ceza Muhakemesi Hukuku, 7.Baskı, Ankara, Seçkin Yayıncılık, 2015: 45-8; 672-39.
[125]Özbek VÖ, Kanbur MN, Doğan K, Bacaksız P, Tepe İ. Ceza Muhakemesi Hukuku, 7.Baskı, Ankara, Seçkin Yayıncılık, 2015: 45-8; 672-39.
[126]Soyaslan D. *Ceza Muhakemesi Hukuku*, 5. Baskı, Ankara, Yetkin Yayınları, 2014: 71-6

"*ikrar*"ı sağlamak için her türlü işkenceyi meşrulaştırmıştır.[127] Bu sistemde ikrar için yapılan işkence karşısında kişi suçlu değil ise zaten onu Tanrı koruyacaktır. Bu sistemin en önemli delili "*ikrar*"dır. Diğer yandan kilise, ikrarı arınma, bu dünyada günahtan kurtulma yolu olarak görmekteydi. Bu sistem, adaletin gerçekleşmesine olanak veren bir sistem değildir. Fail, yargılamanın süjesi olmadığından savunma hakkı kısıtlanmıştır.[128]

3. Karma Sistem (İşbirliği)

Yukarıda değinilen iki yargılama sistemindeki olumlu kısımlarının geliştirilmesi ile ortaya çıkan yargılama sistemine karma system veya iş bilirliği sistemi denilmektedir. İtham istemi, kişiyi, iddia ve savunmayı; tahkik sistemi ise yargılama makamını üstün.[129] Karma sistem ise, yargılama faaliyetinde bunları birer süje olarak kabul edip birlikte çalışmayı esas almıştır. Bu sistem, 1789 Fransız İhtilali'nden sonra "tahkik" yargılamasına tepki olarak doğmuştur. Bu sistemin prensipleri şunlardır: 1- Şüpheli/sanık yargılamanın objesi değil süjesidir. Şüphelinin/sanığın bazı hak ve yükümlülükleri vardır. 2- Delilleriyle bağlı olmayıp, maddi gerçeğin araştırılması esastır.[130] Yargılama faaliyetinin kapsamına bakıldığında ise yargılama herkese açık ve alenidir. Ayrıca yargılama sözlü ve çekişmelidir. Mahkemeye getirilen her delil kolektif olarak tartışılır. İddialara karşı savunma hakkı. Delillerin serbestçe eğerlendirilip vicdani kanaate ulaşmaya uygun koşullar sağlayan, işbirliği içerisinde maddi uyuşmazlığı çözme yetkisini hakim veya jüriye bırakan bir ispat prensibine sahiptir.[131]

[127]Birtek F. AİHM, Anayasa Mahkemesi ve Yargıtay Kararları Işığında Ceza Muhakemesinde Delil ve İspat, Ankara, Adalet Yayınevi, Ankara, 2016: 255- 579.
[128]Soyaslan D. *Ceza Muhakemesi Hukuku*, 5. Baskı, Ankara, Yetkin Yayınları, 2014: 71-6.
[129]Yayla M. Ceza yargılamasında ispat için yenilmesi gereken şüphe; Türkiye ve Amerika Birleşik Devletleri sistemlerinin incelenmesi, *Ankara Barosu Dergisi*, 2013, 3: 291-13.
[130]Özbek VÖ, Kanbur MN, Doğan K, Bacaksız P, Tepe İ. Ceza Muhakemesi Hukuku, 7.Baskı, Ankara, Seçkin Yayıncılık, 2015: 45-8; 672-39.
[131]Birtek F. AİHM, Anayasa Mahkemesi ve Yargıtay Kararları Işığında Ceza Muhakemesinde Delil ve İspat, Ankara, Adalet Yayınevi, Ankara, 2016: 255- 579.

B. Delil Safhaları

İnsanın dünyadaki serüvenine uygun gelişme gösteren yargılama sisteminde delili de çeşitli safhalardan geçirmiştir. Bu bölümde delilin geçirdiği safhalar aktarılmıştır.

1. Erken Safha

Tarihin erken dönemlerinde, ceza yargılamasında delillerin elde edilmesi ve değerlendirmesi konusunda gelişmiş bir usul yoktu. Suçluluğu baştan Kabul edilen kimselerin yargılanması muhakeme şeklinde olmayıp; suçsuzluğu daha çok bir takım testlere tabi tutarak belirlemeye çalışırlardı. Eski dönemlerde suç daha çok ilahi güçlere karşı işlenmiş kabul edilir ve bu suçların cezasını da yine ilahi güçlerin vereceğine inanılırdı. Eğer kişi masumsa zaten korunacağı inancı hakimdi. Örneğin ateşe atılmış veya zehir içirilmiş biri masum ise ilahi güçlerin bu kimseyi koruyacağına inanılırdı. Eski dönemlerde ilkel sayılacak yol ve yöntemler kullanılmaktaydı. Ancak bu erken dönemlerde suçun tanıkla ispat edildiği de bilinmektedir. Buna rağmen delillerin olayı temsil edip etmediği, doğruluğu gibi bir sorunla uğraşılmıyor, eğer böyle bir sorun ortaya çıkarsa da bu sorun yine ilahi güçlere havale ediliyordu. Erken dönemde hakimler hukuk bilgisi görmüş ve hakimliği meslek edinmiş kimseler değildi. Hakimler, tarafların üzerinde uzlaştığı kimselerden seçilir veya ilahi güçleri temsil ettiklerine inanılan kimselerden olurdu. Bu dönemde bilinen delil ikrar ve tanıklıktır. Olup bitenleri anlamaya çalışan hakim, ikrar (ya da yemin) ve tanık beyanları ile yetinmek zorundaydı. Yalan yere ikrar, yemin ya da şahitliğin cezasının da yine ilahi güçler tarafından verileceğine inanılırdı. Ancak sürecin ilerlemesi ile yozlaşan bu müessesenin bir takım usullere dayandırılması zaruri olmuştur. Bunun neticesinde hangi olayların

hangi delillerle ispatlanabileceği, tanık sayısı gibi düzenlemelere gidilmiş ve en temel delil "*ikrar*" olmuştur.[132]

2. Kanuni Safha

Sosyal hayatın ve bilgi düzeyinin gelişip artması sonucu yargılama faaliyetlerinde de akli yöntemlere başvurulmaya başlanmıştır. Toplumsal hayatı düzenleyen kanunlar yapılmaya başlandığında ceza yargılamasında ispat araçlarının neler olduğuna dair bir takım kurallar getirilmiştir. Hangi hallerde hangi delillere başvurulacağı, delil yasaklarının neler olduğu gibi düzenlemelerin yapıldığı görülmektedir. Getirilen bu düzenlemelerle hakimin keyfiliğini önlemek, akıl dışı delillere başvurmamak, kanunda gösterilen defilerle hukuki uyuşmazlıkların çözülmesi amaçlanmıştır. Örneğin kanunda öngörülen biçim ve tanık sayısının eksikliği ile karar verilecek olursa ispattan bahsedilemeyecektir. Bu dönemde deliller tam, eksik, basitkarmaşık, yazılı-sözlü gibi formlarda tanımlanmıştır. Kanunda sayılan delillerin sayısına ulaşıldığında tam ceza, eksik ulaşıldığında da eksik ceza verildiği de görülmüştür. Dolayısıyla bu döneme kanuni delil dönemi denilmektedir. Yani kanun, delil sistemini kanunda saymakla belirtmiştir. Örneğin zina suçunun ya ikrar ya da belli sayıda tanık beyanı ile ispat edilmesi gerektiğinin kanuna yazılması gibi. Zamanla birçok kurumda olduğu gibi bu kurumda da yozlaşmalar ortaya çıkmıştır. Uyuşmazlık sadece kanunda açıkça sayılan delillerle ispat edilebildiği için bu delillerin uydurulmaya başlandığı görülmüştür. Sitemin çökmesi üzerine delil serbestliği ve vicdani delil sistemine doğru evrilme başlamıştır. Bugünkü prensiplere ulaşılması uzunca bir zaman almıştır.[133]

[132]Aydın D. Ceza Muhakemesinde Deliller, Ankara, Yetkin Yayınları, 2014: 15- 88.
[133]Aydın D. Ceza Muhakemesinde Deliller, Ankara, Yetkin Yayınları, 2014: 15- 88.

3. Vicdani Kanaat Safhası

Aydınlanma ile hukukta aklileştirme ve Fransız Devrimi'nin de katkısıyla her şeyin delil olabileceği, delillerin akla ve mantığa uygun olması, hâkimlerin herhangi bir delille bağlı olmaması gerektiği anlayışı benimsenmiştir. Bu sistemde uyuşmazlığın çözümünde yargı makamını delillerle sınırlandırmamıştır. Aksine yargılama makamının, delillerin ne kadar güvenilir olup olmadığına, hükme esas alınıp alınmayacağına dair karar vermede özgür olduklarını teminat altına almıştır. Vicdani kanaat, yargılama konusu uyuşmazlığın ispat edilmesi için yetkili makam açısından oldukça önemli bir ölçüttür. Hakimin, vicdani kanaate varması demek; vardığı sonucun doğru olduğuna, kendisinin ve akıl sahibi herkesin de Kabul edeceği şekilde şüphenin yenilmesidir.[134] Vicdani kanaatin bir takım niteliklerini ortaya koymak gerekir. Şöyle ki;

1. Vicdani kanaat, bir sezgi değildir. Tanımlanmasına, sözcükleredökülebilmesine ve yazıya geçirilebilmesine olanak verilmelidir.

2. Vicdani kanaat masumiyet karinesi ile doğrudan ilişkilidir.

3. Vicdani kanaate, bir muhakeme faaliyeti sonucunda ulaşılmış olması gerekir.

4. Vicdani kanaat kovuşturma evresinde delillerin ortaya konulup tartışılmasından sonra ortaya çıkar.

5. Hakimin vicdani kanaate ulaşması kendisi açısından yeterli olmayıp, bu kanaatin denetlenebilir olması da gerekmektedir. 6. Vicdani kanaat "suçlu" veya "suçsuz" şeklinde bir değer yargısı içermelidir.

[134]Bıçak V. Suç Muhakemesi Hukuku, 2. Baskı, Ankara, Seçkin Yayıncılık, Ankara, 2011: 46-70; 423-520.

7. Vicdani kanaat, yenilmiş bir şüphenin varlığına bağlıdır.[135] Anayasamızın 138. maddesinin 1. fıkrası "*Hakimler, görevlerinde bağımsızlardır; Anayasaya, kanuna ve hukuka uygun olarak vicdani kanaatlerine göre hüküm verirler*" der. Ayrıca 5271 sayılı Ceza Muhakemesi Kanunun 217. Maddesinde "*Hakim, kararını ancak duruşmaya getirilmiş ve huzurunda tartışılmış delillere dayandırabilir*" hükmü mevcuttur. Burada vicdani kanaat bütün bileşenleri ile birlikte sayılmıştır

4. Bilimsel Safha

Vicdani kanaatle bahsedilen, hakimin kendi bilgi ve aklıyla delilleri .[136]değerlendirmesi, keyfiliği ve sübjektifliği değildir. Genelde bilim ve tekniğin ilerlemesi, özelde de adli bilimlerde yaşanan gelişmeler hakimin sübjektif değerlendirmeler yapmasının önüne engel çıkarmıştır. Adli bilimlerin, delil toplamada, delilleri incelenmede kullandığı yöntemlerin sonuç elde etmeye olanak tanıması bunun gerekçesidir. Delilden sanığa ulaşma ispatın bilimsel araştırmaya olanaklı hale gelmesiyle olmuştur. Maddi vakayla bağlantılı olarak elde edilen iz-emareler (DNA profili, parmak izi, balistik) bilimsel analizlerle uyuşmazlığın aydınlatılmasını kolaylaştırmıştır. Adli bilimler maddi vakanın oluşuna da izahat getirmede oldukça yetkin olduğunu defalarca kanıtlamıştır. Bilimsel delillerin taşıdığı bir risk var ki; o da hakimin delilleri serbestçe takdir etme otoritesini sınırlamasıdır. Deliller hukuka uygun olarak elde edilmiş ise doğruluğu aksi ispat edilene kadar geçerlidir. Aynı zamanda bu doğruluğun kesin biçimde olayla ilgisi ve şüpheli ile olan bağı da ortaya konulmalıdır. Örneğin maktulün giysilerinden elde edilen saç tellerinin kime ait olduğu tespit edildikten sonra, bu saç tellerinin maktulün giysilerine ne şekilde bulaşmış

[135]Bıçak V. Suç Muhakemesi Hukuku, 2. Baskı, Ankara, Seçkin Yayıncılık, Ankara, 2011: 46-70; 423-520.
[136]Aydın D. Ceza Muhakemesinde Deliller, Ankara, Yetkin Yayınları, 2014: 15- 88.

olabileceğinin saptanması gerekmektedir. Saç telinin kime ait olduğunun tespiti sadece bütünün bir parçasıdır.[137]

İKİNCİ BÖLÜM

DİJİTAL DELİL

I. BİLİŞİM KAVRAMI VE BİLİŞİM YOLUYLA ELDE EDİLEN VERİLER

A. Kavram ve Tanımlar

Teknolojik gelişmelere paralel olarak şekillenen bilişim hukukunun anlaşılabilmesi için öncelikle "bilişim", "bilişim teknoloji","bilişim ağı" "bilişim sistemi", "yazılım", "donanım" ve "adli bilişim" olarak adlandırılan kavramların tanımlanması gerekir.

Bilişim:*"insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik*"[138] ifadesiyle tanımlanmıştır. Başka bir tanıma göre ise; "*bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemler"* bilişim olarak isimlendirilmiştir[139].

Bilişim teknolojisi: Bilginin elektronik ortamda düzenli ve akıcı bir şekilde işlenmesine aracılık eden çağımızın en hızlı ve kullanışlı teknolojisi, bilişim

[137]Aydın D. Ceza Muhakemesinde Deliller, Ankara, Yetkin Yayınları, 2014: 15- 88.
[138] TDK, **Bilişim,** Genel Türkçe Sözlük, Erişim Tarihi: 13.11.2017. http://www.tdk.gov.tr/index.php?option=com_gts&kelime=B%C4%B0L%C4%B0%C5%9E%C4%B0M
[139] Sacit Yılmaz, "5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar", **TBB Dergisi 2011**, 92, ss. 62-100.

teknolojisidir. Bilgisayarlar, internet, banka kartları, dijital yayınlar, cep telefonları bilişim alanındaki teknolojik ürünlerden bazılarıdır[140].

Bilişim ağı: "Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı"nın 2/c bendinde bilişim ağı: *"En az iki bilişim sistemi arasında veya bir bilgisayar ile bir çevre birimi arasında veri iletişimini ve karşılıklı etkileşimi her türlü iletişim tekniği ile sağlayan ortamı,"*[141] ifaden terim olarak tanımlanmıştır.

Bilişim sistemleri:*5237 sayılı Türk Ceza Kanunu'nun* gerekçesinde, *"Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir."*[142] biçiminde tanımlanmıştır. Donanım ve yazılımların biraraya gelerek verilerin işlenmesini sağlayan sisteme bilişim sistemleri adı verilebilir. ***Donanım,*** bilişim cihazının yapısını oluşturan her bir parçası; ***yazılım*** ise bilişim cihazının çalışmasını sağlayan işletim sisteminden oluşan sistem yazılımları ile bu sisteme bağlı olarak çalışan ve kullanıcı için tasarlanan uygulama programlarıdır. Örneğin, bir bilgisayarın klavyesi, anakartı, cep telefonunun tuşları elle tutulan kısımları donanım, bu cihazlardaki verilerin değerlendirilmesini sağlayan windows ve ekranın dokunmatik olmasını sağlayan programlar sistem yazılımları, office, Acrobat reader ya da bir kayıt silici olarak yüklenen program ise uygulama yazılımı olarak sayılabilir.

Adli bilişim (computer forensic): Bilişim cihazlarının yasal delil elde edilmesi için incelenmesi işlemine adli bilişim adı verilebilir. Tanımı ayrıntılı olarak ifade etmek gerekirse; depolanmış veya şifrelenmiş bilgi, delil niteliğini taşıyan verilerin

[140] Şükrü Haluk Akalın, "Bilişim Türkçesi",**Türk Dili Dil ve Edebiyat Dergisi 2002**, TDK yayını, ss.472-481.
[141] "Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı", Erişim Tarihi: 12. 11.2017, http://www.tbd.org.tr/bilisim-agi-hizmetlerinin-duzenlenmesi-ve-bilisim-suclari-hakkinda-kanun-tasarisi/
[142] "Türk Ceza Kanunu Madde Gerekçeleri", Erişim Tarihi: 12. 11. 2017, www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc.

tanımlanması, toplanması, incelenmesi ve korunması amacıyla analitik ve araştırmacı özel analiz tekniklerinin kullanılması şeklinde tanımlanabilir[143]. Daha önceki zamanlarda, soruşturma ve kovuşturma yürüten yargıç ve savcılar delil olarak özel kağıt belgeleri kullanmaktaydılar. Ancak teknolojinin gelişmesiyle birlikte şimdilerde bilgisayar, telefon, hard disk, USB, CD, DVD gibi çeşitli elektronik aletlerin çeşitli suçlarda delil niteliği taşıması adli bilişim alanın doğmasına neden olmuştur[144].

Adli bilişim; "*Disketlerden, sabit disklerden ve çıkartılabilir disklerden delil elde etme amacıyla veri kurtarma işlemi olan ve elektronik delillerin muhteva ettiği bilgileri, delil inceleme süreçlerini, hukuki ve etik sorumlulukları göz önünde bulundurarak, delilin bütünlüğünü koruyarak ve maddi gerçeği açığa çıkarmak amacıyla; kopyalama, belirleme, çözümleme, yorumlama ve belgelemesüreçlerinin bütünü…"*[145] olarak da tanımlanmıştır.

Adli bilişim; bilişim suçları, bilgi güvenliği açıkları, ulusal güvenlik tedbirleri ve bilgisayar suiistimalleri karşısında, suçlunun ortaya çıkarılması amacıyla gereken sayısal delillerin bulunması ya da adli delilleri eksiksiz ve yorumsuz bir şekilde sunmak için adli analizler ve çalışmaların yapılmasıdır[146]. Adli bilişimi ilgi alanlarına göre "bilgisayar adli bilişimi", "ağ ve internet adli bilişimi", "gömülü cihazlara ait adli bilişim" ve "sosyal ağ adli bilişimi" olarak dört alt gruba ayırmak da mümkündür[147].

Teknolojik gelişmeler, özellikle ticaret, haberleşme, alış-veriş gibi birçok kişisel faaliyetlerle birlikte özel firmalar ya da devlet kurumlarının veri depolama ve kurumsal işleyişlerini bilgisayar sistemleri, dijital aletler ve internet ağları üzerinden yapmasına

[143] "Computer Forensics World", Erişim Tarihi: 14. 11. 2017, http://www.computerforensicsworld.com/
[144] Muharrem Özen ve Gürkan Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)",**Ankara Barosu Dergisi 2015**, 1, 42-77
[145] M. Özen, G. Özocak, 2015, ss.44-45.
[146] Yong-Ho Kim, Kunam J. Kim, A **Forensic Model on Deleted-File Verification for Securing Digital Evidence,** 2010 International Conference, Information Science and Applications (ICISA); Şeref Sağıroğlu, Mehmet Karaman, "Adli Bilişim", **Telepati Dergisi 2012**, 203, ss. 62-63.
[147] M. Özen, G. Özocak, 2015, s.45.

olanak sağlamıştır. Ortaya çıkan bu kolaylıklar beraberinde yeni bir suç ortamını da şekillendirmiştir. Bilişim sistemlerinin gelişmişliği ve internetin kolay ulaşılabilir olması, özellikle nakit transferleri başta olmak üzere çeşitli suçların işlenmesine de imkan sağlamaktadır.

Bilgisayar ağları aracılığıyla bir başkasına veya bir devlete karşı gerçekleştirilen dolandırıcılık, şantaj, sahtecilik, bilgi hırsızlığı, hizmeti engelleme, zararlı yazılım, sosyal mühendislik saldırıları, cinsel istismar, siber terörizm ve siber savaş gibi eylemler suç ve suçlunun tanımlanmasını zorlaştırmaktadır. Bu tip suçlar daha çok bilişim suçları olarak tanımlansa da hem ulusal hem de uluslararası doktrinde farklı isimler altında incelenebilmektedir.

Bilişim sistemleri, bilgisayarlı elektronik makineler ve internet ağlarının bir araya gelmesine olanak sağlayan sistemlerdir. Bu sistemler aracılığıyla işlenen suçlar "Bilgisayar suçları", "bilişim suçları", "internet suçları" "ileri teknoloji suçları" "dijital suçlar" ve "siber suçlar" gibi benzeri terimlerle adlandırılabilmektedir[148]. Bu terimler içerik olarak birbirinden ayrı olsa da tamamını kapsayacak ifade en geniş anlamlı olan "bilişim suçları" kavramıdır. Bununla birlikte bilişim teknolojisinde meydana gelen gelişmeler bu alanda yeni suç şekillerinin ortaya çıkmasına yol açtığı için tanımların da devamlı değişmesine neden olmaktadır. Bu nedenle her zaman tüm suçları içerisine alan bir tanımlama yapmak mümkün olmamaktadır[149].

Bilgisayar ve bilişimin birbirinden farklı olması nedeniyle "bilgisayar suçu" ile "bilişim suçunun" da farklı olduğu ileri sürülebilmektedir[150]. Ancak, pratikte bilgisayarın en yaygın bilişim aracı olması bilişim suçları ifadesinin kullanılmasını da haklı çıkarabilir. Bilgisayar suçlarının tanımlanmasına yönelik ulusal ve uluslararası

[148] Hakan Hekim ve Oğuzhan Başıbüyük, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", **Uluslararası Güvenlik ve Terörizm Dergisi 2013**, 4(2), s.136
[149] B. Zakir Avşar, Gürsel Öngören, **Bilişim Hukuku**, Yayın No: 270, Türkiye Bankalar Birliği, 2010, İstanbul, s.123.
[150] Yılmaz Yazıcıoğlu, "Bilişim Suçları",**Hukuki Perspektifler Dergisi 2004,** 2, s. 142.

hukuk doktrininde fikir birliği bulunmamakla birlikte OECD'nin yaptığı bir tanımlamaya göre sağlayan bir sistem aracılığıyla yasa dışı, ahlaka uygun olmayan şekilde ya da yetki alanının dışında eyleme geçirilen her türlü davranış olarak tarif edilmiştir[151].

Bilişim suçları ise bir bilgisayar veya ağına yönelik olarak veya onların kullanılmasıyla verilerin otomatik şekilde işlenmesi, saklanması, tasnif edilmesi, terkibi ve iletilmesi ile ilgili ve bilişim alanı içinde gerçekleştirilen suçlardır[152]. Bilişim ortamlarında işlenen suçlar "bilgisayar suçları" (computer crimes), "bilgisayarla ilgili suç" (computer-related crime), "bilgisayar ihlalleri" (computer abuse), "yüksek teknoloji suçları" (high-tech crimes), "İnternet suçları" (internet crimes)[153] olarak adlandırılabildiği gibi "bilişim sisteminin kendisine karşı işlenen suçlar" ve "bilişim sistemi ile işlenen suçlar olarak da gruplandırılabilmektedir[154].

Siber suçlar olarak adlandırılan suçların tanımlanmasında da çeşitli yorum farklılıkları bulunmaktadır. "Siber uzay" ve "internet" kavramları birbirinin yerine kullanılsa da gerçekte aynı anlamlara gelen kavramlar değildir. Siber uzay, hem interneti hem de intranet ve benzer diğer ağları kapsayan geniş anlamlı bir kavramdır. Bu nedenle intranet ortamında gerçekleşen bir suç, siber suçlardan sayılabilirken internet suçlarına girmemektedir[155].

Siber suçlar; network ya da bilgisayar sistemleri kullanılarak gerçek, çalınmış veya sanal kimlikli profesyonel kullanıcıların sınırları belirgin olmayan dijital dünyada gerçekleştirdikleri illegal faaliyetlerdir. Bu suçların işlenme şekillerine bakacak olursak;

---

[151] Ulrich Sieber, **Legal Aspects of Computer Related Crimes,** Erişim Tarihi: 12. 11. 2017 http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf, Ocak 1998.
[152] Levent Kurt, **Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması,** Ankara: Seçkin Yayınevi, 2005, s.53.
[153] Oğuz Turhan, **Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar),** Planlama Uzmanlığı Tezi, 2006, Ankara, ss.28-29.
[154] B. Z. Avşar, G. Öngören, 2010, s.123.
[155] O. Turhan, 2006, s. 26

kara para aklama, vergi kaçırma, hırsızlık, dolandırıcılık, kimlik bilgilerinin çalınması, sahtecilik, telif haklarının ihlal edilmesi, siber terörizm, siber savaş, sabotaj, casusluk, siber taciz, siber zorbalık, çocuk pornografisi, çocukların ifsadı, ırkçılık, nefret söylemi, dinin aşağılanması gibi eylemlerin siber alemde gerçekleştirilmesinden ibarettir[156].

İleri teknolojik bilişim yöntemleri kullanılarak işlenen siber suçlar aşağıdaki yöntemler kullanılarak gerçekleştirilebilir;

- *"Hizmetin Engellenmesi saldırıları (Denial of Service- Distributed Denial of Service),*
- *Kötücül Yazılımlar: Bilgisayar virüsleri, kurtçuk (worm), truva atı (trojan), klavye izleme (key logger), istem dışı olarak gönderilen ticari tanıtım (adware), bilgi toplayan casus / köstebek (spyware) yazılımlar*
- *Yemleme (phishing) ve İstemdışı elektronik posta (spam),*
- *Şebeke trafiğinin dinlenmesi (sniffing ve monitoring)."*[157]

Siber suçları suçun kaynağı, hedefi, kazanım amacı, bilgi sisteminde meydana getirdiği hasar ve elde edilen sonuç açısından farklı şekillerde gruplandırabiliriz[158]. "Devlet ve kamu düzenine karşı işlenen suçlar", "Mal varlığına ve kişilere karşı işlenen suçlar"; "Ekonomik değeri olan suçlar", "Güvenlik ihlali olan suçlar"[159], "Ahlaka karşı işlenen suçlar" ve "İnsanlığa karşı işlenen suçlar" bunlardan bazılarıdır[160]. Bilişim suç şekillerini yapılan saldırılardan elde edilen sonuca göre de; eylemci saldırılar, siber casusluk (siber ispiyonaj), siber suçlar (siber korsanlık), siber sabotaj, siber terör ve siber savaş olarak da sınıflandırılabilir[161].

---

[156] Servet Yetim, "Siber Suçlar, Yargılama Yetkisi ve Yeni Bir Model Önerisi",**TAAD 2014**, 5(17), s.183
[157] Mustafa Ünver, Cafer Canbay, Ayşe Gül Mirzaoğlu, **Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler,** Ankara, 2011, ss.8-21.
[158] Murat Güngör, **Ulusal Bilgi Güvenliği: Strateji Ve Kurumsal Yapılanma, Kalkınma Bakanlığı, Bilgi Toplumu Dairesi Başkanlığı**, Ankara, Yayın No: 2919, Uzmanlık Tezi, 2015, s.43-51.
[159] İbrahim Balcıoğlu, "İnternet Kullanımı ve Getirip Götürdükleri",**Somuncubaba Dergisi 2014,** s.67.
[160] S. Yetim, 2014, s.183.
[161] M. Güngör, 2015, ss.46-48.

Amerikan doktrinine göre bilişim suçları (siber suçlar)'nın on iki basamak altında değerlendirilmelidir. "Bunlar; mülkiyete karşı hırsızlıklar, verilere veya hizmetlere karşı gerçekleştirilen hırsızlıklar, giriş ihlalleri, veri sahtekârlığı, insan hataları sonucu oluşan ihlaller, gasp, sır aleyhine ihlaller, sabotajlar, maddi kısımlara yönelik hırsızlıklar, evraklarda gerçekleştirilen sahtekârlıklar, bankamatik kartları konusundaki hırsızlıkları, manyetik kartların şifreleri hususunda gerçekleştirilen eylemlerdir"[162].

Avrupa Komisyonu tebliğine göre ise siber suçlar: "Elektronik ağlar vasıtasıyla işlenen klasik suçlar", "Elektronik medya üzerinde yayınlanan yasa dışı içeriğe ilişkin suçlar" ve "Elektronik ağlara has suçlar"[163] olarak ifade edilmiştir. *TCK 5237 Sayılıkanunda* "Bilişim suçları (bilişim alanında işlenen suçlar) ve Bilişim sistemleri aracılığıyla işlenen suçlar (özel hayata ve hayatın gizli alanına karşı işlenen suçlar)" olarak gruplandırılırken;

TCK 5237 Sayılı kanunun Onuncu Bölümü "Bilişim Alanında Suçlar" ile ilgilidir. *243. Maddede*, bilişim sisteminin tamamına veya bir kısmına hukuka aykırı biçimde girilerek orada kalmayı sürdürmesi, sistemin içerisinde yer alan bilgilerin yok edilmesi veya değiştirilmesi bilişim sistemine girme suçu olarak ifade edilmiştir. 244. Madde ise sistemi engelleme, bozma, verileri yok etme veya değiştirmesi ile ilgilidir. Bu madde de bilişim sisteminin işleyişini ve verilerini kısıtlayan ya da yok eden, değiştiren veya erişimi engelleyen sisteme başka bilgi yerleştiren, var olan bilgileri başka bir yere aktaran kişinin bilişim suçu işlediği kabul edilmiştir[164].

[162] B. Z. Avşar, G. Öngören, 2010, s.124.
[163] H. Hekim, O. Başıbüyük, 2013, s.137.
[164] RG: **Bilişim Alanında Suçlar. Onuncu Bölüm**, Türk Ceza Kanunu, Kanun No. 5237, 26.9.2004.Erişim Tarihi: 14. 11. 2017, http://www.resmigazete.gov.tr/eskiler/2004/10/20041012.htm.

B. Bilişim Yoluyla Elde Edilen Veriler

1. Dijital Veri Kavramı

İngilizce karşılığı "data" olan "veri" kavramı TDK'ya göre: *"Olgu, kavram ya da komutların, iletişim, yorum ve işlem için elverişli biçimsel ve uzlaşımsal bir gösterimi. Elverişlilik, kişiler ya da özdevimli makinelerle iletişim, yorum ya da işleme uygunluk biçiminde düşünülür*"[165] olarak ifade edilmiştir. (https://sozluk.gov.tr/). Çeşitli disiplinlerde farklı anlamlara gelen "veri" kavramı bilişim alanında kişilere has özel bilgiler ve dijital ortamlarda bulunan bilgilerle ilgilidir. *Avrupa Siber Suç Sözleşmesi'ne* göre veri; "*belirli durumların, bilgilerin kaydı ya da bir bilgisayarın bir işlemi gerçekleştirmesini sağlayacak biçimleri de içeren bilgisayar sistemince icra edilebilecek bir işlemler bütünü olarak tanımlanmıştır*."[166] Başka bir ifade ile veri; depolamak, işlemek ve kullanmak için kurulu bir bilişim sistemi tarafından gerçekleştirilen temel unsurdur[167].

Bilgisayarlı ortamlarda daha çok "kişisel veri"lerden söz edilmektedir. İnsanların bir banka hesabı açması, bir uçuş rezervasyonu yaptırması gibi durumlarda vermek zorunda olduğu adı, adresi, kredi kartı numarası, telefon numarası gibi hayati kişisel bilgileri kötü niyetli kişilerin eline geçebilir. Bu nedenle uluslararası bir sorun olarak görülen kişisel verilerin korunması ile ilgili yönetmelik ve direktif metinleri Avrupa Komisyonu tarafından 4 Mayıs 2016'da kabul edilerek yayınlanmıştır. AB üyesi ülkelerin 6 Mayıs 2018'e kadar ulusal yasalarını buna göre düzenlemesi istenmiştir. Bu kuralların amacı, vatandaşların ve işletmelerin kişisel verilerinin kontrolünü sağlamasıdır. AB, yasalarına göre, kişisel veriler ancak meşru bir amaç için yasal olarak

---

[165] TDK, **Veri,** BSTS/Bilişim Terimleri Sözlüğü 1981, Erişim Tarihi: 14.11.2017 http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5a0aee1d5bd5d8.31054914

[166] S. Yılmaz, 2011, s.72

[167] R. Yılmaz Yazıcıoğlu, **"Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi", Hukuk ve Adalet: Eleştirel Hukuk Dergisi** 2004, 1(1), s.227.

toplanabilir ve toplanan bu veriler de yanlış kullanımlara karşı koruma altına alınmalıdır. Bu amaç doğrultusunda kişisel verilerin AB'nin her yerinde yüksek bir koruma standardına sahip olması için çıkartılan kurallar, suistimallere karşı şahsın şikayet etme ve tazminat alma hakkına imkan tanımaktadır[168].

T.C.K.'nın 135. Maddesinde kişisel veri tanımlanmasa da 2 nolu fıkrasında, *"Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse*"[169] ifadesi kullanılarak kişisel veriden kastın ne olduğu anlatılmaya çalışılmıştır.

"6698 Sayılı Kişisel Verilerin Korunması Kanunu", 24/3/2016 tarihinde yasalaşmıştır. Bu kanunun Madde 3. maddesinde kişisel verinin *"Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi"*, kişisel verilerin işlenmesinin ise "*Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hâle getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem*i" ifade ettiği bildirilmiştir[170].

Dijital, kelimesinin sıfat anlamı "sayısal" fiziki anlamı ise "verileri bir ekran üzerinde elektronik olarak gösteren" olarak tanımlanmıştır[171]. Sayı saymak için kullanılan "digitus" (parmak) kelimesinden türemiş olan dijital kavramı, verileri elektronik ortamda üretmek, işlemek veya saklamak anlamlarına gelir. Dijital veya

---

[168] European Commission, **Justice, Data protection, Protection of Personal Data** http://ec.europa.eu/justice/data-protection/. Erişim Tarihi: 14.11.2017

[169] T.C.K. 135. madde: (Değişik: 21/2/2014 – 6526/3 md.)

[170] "6698 Sayılı Kişisel Verilerin Korunması Kanunu", 24/3/2016. RG. Tarih: 7/4/2016 Sayı : 29677

[171] TDK, **Dijital,** Genel Türkçe Sözlük, Erişim Tarihi: 14.11.2017. http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5a0b14bd475791.42195834

dijitalleştirme ifadesi bilgisayar ortamında verilerin 1 ve 0'lardan oluşan bilgisayar diliyle sayısallaştırılmasıdır[172]. Bu tanımlamaya göre dijital veriden kasıt sayılarla ilgili veriler olduğu anlaşılmaktadır. Bununla birlikte dijital veri kavramı içerisine metin, resim, ses kaydı ve videonun da girdiği bildirilmektedir[173].

Dijitalleştirme işlemi *"elektronik sistemlerce algılanamayan yapılandırılmamış belge ve fotoğraflarla, analog ortamdaki müzik ya da videoların sayısal ortamda depolanan imajlara dönüştürülmesi işlemi"* olmasıdır. Bu çerçevede müzik ve sinema eserleri, kitaplar, dergiler, fotoğraflar, skaynerler, dijital ses kaydediciler, dijital kameralar aracılığıyla bilgisayara kolayca taşınarak aktarılarak dijital hale getirilmektedir[174].

Fotoğraf makinesi, kamera, cep telefonu, laptop, manyetik banka kartları, hard disk, flaş bellek, pc, cd, dvd, sim kart gibi cihazlar dijital delillerin arandığı cihazlardır. Bu nedenle dijital veriler, "elektronik ortamlarda bulunan ve elektronik aygıtlar aracılığı ile okunabilen saklanabilen veriler"[175] olarak tanımlanmıştır. Cihazların elektronik aletler olması nedeniyle "dijital veri" yerine "elektronik veri" terimi de kullanılsa da dijitalleşmekten esas maksat bilgisayar diliyle kodlanmış verilerdir.

Genellikle birbirlerinin yerine kullanılan dijital (sayısal) delil kavramı ile elektronik delil kavramı arasında önemli bir farklılık bulunmaktadır. Dijital kanıtlarda sayılar temel alınarak, çalışan ve elektronik cihazlarda saklanan verilerden oluşan kanıtlardır. Elektronik, elektronların hareketlerine göre uygun devreler yapılmasıyla ilgilidir. Bu alandaki cihazlar analog (örneksel) elektronik ve dijital (sayısal) elektronik

---

[172] Yavuz Selim Şener, **Fikri Mülkiyet Hukukunda Dijital Veri Tabanlarının Korunması**, İstanbul Kültür Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi, İstanbul, 2013, s.18

[173] Eoghan Casey, **Digital Evidence and Computer Crime: Forensic Science, Computer and The Internet,** London, Academic Press, 2011, s. 3-32.

[174] Y.S. Şener, 2013, s.18

[175] Yılmaz Şimşek, Muharrem Durmaz ve Nurullah Karataş, **Dijital Delil Yöntemi,** Ankara, Polis Akademisi Yayınları, 2012, s.13-19.

aygıt şeklinde ikiye ayrılır. Elektronik delil ifadesi dijital delilleri de kapsayan bir üst konsept olarak değerlendirilmiştir[176].

Elektronik deliller, *"bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen soruşturma açısından değeri olan bilgi ve verilerdir."* Bu verilerin gizil bir yapıya sahip olması uzmanlar ve uygun aletlerle analizini zorunlu kılmaktadır[177].

Dijital bilgi muhafaza edebilen veya elektronik devre akımları ile çalışan disket, disk, CD, bilgisayarlar, cep telefonları, PDA cihazları, flash bellekler, SIM kartlar gibi bilgisayarda kullanılan dâhili ya da harici donanımlardan elde edilen veriler "Elektronik Delil" olarak adlandırılır. Bazen bu adlandırma yerine, bilgisayar sistemleriyle kayıt edilen ya da iletilen veriler, bir suçun nasıl olduğu ya da suçtaki kritik unsurların yerlerinin belirlendiği ya da çürütüldüğü veriler "sayısal delil" olarak da isimlendirilmektedir[178].

Elektronik veya manyetik bir ortam üzerinden iletilen ya da bu ortamlara kaydedilen her türlü veri dijital veri çeşidi olarak değerlendirilebilir. Bu veriler; yazı, resim, ses, görüntü, sinyal, grafikler, çizimler, tablolar, bilgisayar programları, iletişim kayıtları, elektronik postalar, elektronik mesajlar, gizli ve şifreli dosyalar ve bunların silinme, değiştirilme ve erişimi ile ilgili bilgileri, son kullanılan ve sık kullanılan internet siteleri ve içerikleri, ağlara erişim kayıtları, IP bilgileri, donanımlara ait seri veya kullanım numaraları, yazılımlara ait sürüm bilgileri dijital veri çeşidi olarak sayılabilmektedir[179].

---

[176] Şenel Sarsıkoğlu, "Ceza Muhakemesinde Delil Ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı",**TAAD, 2015**, 6(22), ss.427-454.
[177] M. Özen, G. Özocak, 2015, s.59.
[178] Jerry Chisum, **Crime Reconstruction and Evidence Dynamics, Presented at theAcademy of Behavioral Profiling,** Monterey, 1999, s.9.
[179] Murat Kızılyar, "Ceza Yargılamasında Dijital Verilerin Delil Değeri",**Adalet Dergisi 2014,** 50, s. 72-89.

Elektronik aletlerdeki işletim sisteminin kayıt defteri bölümü adli bilişim uzmanlarınca incelendiğinde bilgisayarın genel bilgileri, sistem kayıtları, kayıt defteri, silinen verilere ulaşılması, kurulu yazılımlar, zararlı yazılım ve uygulamalar, geçici dosyalar, üst veri bilgileri, internet geçmişi, e-posta dosyaları, konuşma kayıtları, kablosuz ağ bağlantıları dijital delil niteliğindeki verilerin ele geçirilebileceği alanlardır[180]. Örneğin işletim sisteminin kayıt defterinden elde edilecek aşağıda sıralanan bilgiler dijital delil verilerini aydınlatacak niteliğe sahiptir.

- *"İşletim sistemi bilgileri,*
- *Kullanıcı bilgileri,*
- *Güvenlik bilgileri,*
- *Son kullanılan doküman listesi (MRU),*
- *Bilgisayara takılmış USB Bellekler,*
- *Bilgisayar üzerindeki donanım bilgileri,*
- *Bilgisayarda tanımlanmış kullanıcı gruplar bilgileri,*
- *Kullanıcılara ait şifrelerin belli bir algoritmadan geçirilmiş şekli,*
- *Bilgisayarın açılma kapatılma ve ne kadar çalıştığına ait kayıt bilgileri,*
- *Bilgisayarda yüklü yazılımlara ait bilgiler,*
- *Bilgisayardaki aktif veya pasif tüm servisler,*
- *Hangi yazı fontlarının sistem tarafından desteklendiği listesi,*

[180] Hüseyin Çakır, Mehmet Serkan Kılıç, "Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bir Bakış",**Polis Bilimleri Dergisi 2013**,15(3), ss.23-44.

- *Hangi dosya uzantılarının sistem tarafından desteklendiği listesi*."[181]

Teknolojik gelişmelerin çok hızlı bir şekilde yaşandığı günümüz şartlarında bilgisayar teknolojisi ile çalışan birçok elektronik aygıt üretilmektedir. Günlük hayatta kullanılan cep telefonları, bilgisayar çeşitleri, ses veya görüntü cihazları, hatta televizyonlar belirli hafızaları olan ve ulusal ya da uluslararası iletişim kurulan aletlerdir.

Adli bilişim uygulamalarında ceza muhakemesi hukukunda delil niteliğindeki veriler daha çok kişisel bilgisayarlarla birlikte cep telefonları, Xbox vb. oyun konsollarındaki görüşme kayıtları, USB bellekler, dijital ses ve video kayıt cihazları gibi elektronik cihazlardan sağlanmaktadır. Ancak en çok dijital delillere ulaşım yolu kişisel bilgisayarlardır. Bunun nedeni kişisel bilgisayarlarda internet gezinti bilgilerinin, silinmiş dosyaların, sistem loglarının, kullanıcı hesaplarının ve büyük miktarda şifrelenmiş verilerin bulunmasıdır. Son zamanlarda akıllı telefonların popülerleşmesi ve bilgisayarın çoğu özelliğini taşıması da telefonlarda dijital delillerin aranmasını gerekli kılmıştır[182].

Bilgisayar ya da elektronik cihazlar donanım ve yazılımları sayesinde yüklenen verileri işleyebilen, depolayabilen ve ihtiyaç durumunda tekrar ulaşımı sağlayabilen aygıtlardır. Bu aygıtlarda kullanılan yazılımlar programcıların hazırladığı komut ve donanımları harekete geçirme özelliğine sahiptir. Elektronik cihazların donanım ve yazılımları arasındaki komut alış verişi, aygıtlarda dijital verilerin üretilmesine ya da indirilen verilerin değişik biçimlere dönüştürülmesine aracılık eder. Bu bilgilerin geçiş

[181] H. Çakır, M.S. Kılıç, 2013, s.30.
[182] M. Özen, G. Özocak, 2015, s.47

yolları ve saklandığı alanlar dijital ortam olarak adlandırılmaktadır. Her dijital veri komutlarla ya da kullanıcı isteğine göre geçiş yolunda bir iz bırakır[183].

1990'lı yıllardan itibaren hayatımızın hemen hemen her alanına giren bilgisayarlı elektronik aletler günlük hayatımızı ve işlerimizi kolaylaştırması açısından daha çok tercih edilmektedir. Bu aletler vasıtasıyla bir kişiye ya da kuruma ait veriler depolanabilir, veriler analiz edilebilir, işlerin yapılma komutları iletilebilir ve denetlemeler yapılabilir durumdadır. Bununla birlikte insanlar alış veriş, eğlence, dijital sosyal alanlara katılma gibi faaliyetleri bu cihazlar aracılığıyla yapabildiği gibi sosyal grupları harekete geçirme, uzak bir bilgisayardaki kişilerin özel bilgilerine ulaşma, bilgisayar sistemlerinin çalışmasını engelleme, verileri bozma veya değiştirme gibi suç sayılabilecek eylemleri de gerçekleştirebilmektedir. Bilgisayarlı sistemlerde gerçekleştirilen tüm işlemler silinse bile geride kayıtlar ve izler bırakabilmektedir. Bu özellik sayesinde masum bir şekilde kaybedilen veriler geri getirilebildiği gibi, suç işlendiği durumlarda da kasıtlı bir şekilde silinse bile uzman kişi ve programlar sayesinde geri getirilerek kişinin aleyhine delil olarak kullanılabilmektedir. Bilgisayarlı elektronik aletlerden elde edilen dijital delillerin incelenmesi ile soruşturma sırasında şüphelinin suç işlediğine dair en küçük bir ize rastlanması bile ceza muhakemesinde büyük bir vakanın çözülmesine aracı olabilmektedir[184].

Hukuki açıdan delillerin elde edilmesi için izlenen yöntemlerdeki süreç dijital delillerle ilgili verilerin toplanmasında da geçerlidir. Bu nedenle her türlü izin ve onayda izlenecek prosedüre uyulması, delillerin yasal olması ve kullanılabilirliği yönüyle diğer delillerin toplanmasındaki gibidir. Ancak, bilgisayar ortamındaki delil değeri olan verileri toplamak, şüphelinin bilgisayarındaki verilerin kopyalanması ve içindekilerin adli makamlara belge şeklinde sunulması değildir. Dijital delillere ulaşmak

[183] M. Kızılyar, 2014, s.81
[184] Larry E. Daniel ve Lars E. Daniel, "Digital Forensic: The Subdisciplines",**Digital Forensic for Legal Professions 2011**, ss.17-23.

herkesin yapabileceği bir iş değildir, yapılan hatalı işlemler delillerin yok edilmesine bile yol açabilir. Bu nedenle dijital delil toplama işlemi, bilişim uzmanı personelin teknik yöntem ve uygun programları kullanması ile gerçekleştirilir.

Dijital delilleri elde etmek için arama ve el koyma işlemi sırasında bilgisayardan veri alınması, bilgisayarın dondurulması, verilerin kopyalanması, klonlanması, bilgisayarın kapatılması ve laboratuvara götürülmesine kadar geçen sürecin titizlikle yapılması ve delillerin kaybolmaması, silinmemesi ve değiştirilmesine fırsat verilmemesi sağlanmalıdır[185].

Dijital delillere ulaşılırken ilk olarak delillerin yer aldığı ortam boşaltılmalı ve bu durum kamera ile izlenmelidir. İnternet bağlantıları varsa verilerin silinme riskine karşı kapatılıp kapatılmamasına karar verilmeli, bilgisayar açılacaksa plastik eldivenler kullanılmalı, bilgisayarlar götürülmeyecekse mevcut durum gerekli programlar kullanılarak kopyalanmalı ve analiz edilmeli, elde edilen veriler adli birimlerin anlayacağı bir şekilde teknik terimlerden arındırılarak rapor halinde sunulmalıdır[186].

Dijital veriler, elektronik aygıtların veri depolama alanları ve önbelleklerinde depolanır. İnternet ya da diğer alan ağları üzerinden aktarılan verileri ya da veri yollarını da bu alanlarda araştırmak gerekir. Verilere ulaşma ve elde etme yöntemleri verinin bulunduğu kaynağa göre farklılık gösterir. Bu nedenle "*Dijital delillere ulaşmada ve bunları delil olarak kullanılabilecek duruma getirmede; tespit, yedekleme, örnek alma (kopyalama), imaj alma, işaretleme, çözümleme, tanımlama ve delil belgesine dönüştürme gibi süreçler izlenir.*"[187]

Dijital delillere ulaşma sürecini genellikle "ön inceleme" ve "olay yeri tespiti", "delil toplama", "analiz ve raporlama" şeklinde dört ana bölüme de ayırabiliriz. Ön

[185] Simson Garfinkel, "Digital Forensics Research: The Next 10 Years", **Digital Investigation 2010**, 7, ss.64-73.
[186] M. Özen, G. Özocak, 2015, s.52.
[187] M. Kızılyar, 2014, s.83.

inceleme ve olay yeri tespitinde şüphelinin bilgisayarının bulunduğu ortam fotoğraflanmalı, internete bağlı ise kesilmeli, bilgisayarın açılması ve kapatılması teknik bir şekilde yapılmalı, bilgisayar kapatılmadan önce uçucu delil niteliği taşıyan veriler kopyalanmalı, ekran görüntüsü alınmalı, tüm deliller teknik gereklere uyularak kopyalanmalı, kopyalanan verilerin de *hash* değerleri de alınmalıdır[188].

Delil toplama işleminde; olay yeri incelemesi ile bulunan dijital delillerden kopyalanmış verilerin erişim yetkisi ve veri bütünlüğü olup olmadığı kontrol edilir, silinmiş veriler varsa kurtarılır, şifrelenmiş veriler çözülür. Veriler üzerinde yapılacak tüm analizler ve incelemeler klonlanmış verilerde yapılır. Bilgisayardaki normal, şüpheli, gizli, şifrelenmiş, şifre korumalı, geçici ve swap dosyaların tamamı incelenmelidir. Ayrıca uygulamalar ve uygulamaların kullandığı dosyalar ve işletim sistemi dosyaları da analiz edilmelidir. Powergrep gibi programlarla txt dosyaları içinde aramalar yapılmalıdır. Pornografi suçuyla ilgili bir arama gerçekleştiriliyorsa video ve ses dosyaları daha dikkatli araştırılmalıdır[189]. Ayrıca, steganografi yöntemi ile imaj dosyaları içerisine veri gizlenebildiği için şüphelinin teknik becerisi dikkate alınarak bu tür verilerin analizi de uygun programlar kullanılarak yapılmalıdır[190].

Dijital delil toplama işleminde genellikle elektronik aygıtların imajının alınması yöntemi kullanılmaktadır. İmaj alma işlemi, kullanıcıların sistemi yeniden yüklemeleri durumunda önceki kurulu sistemin aynısı olacak bir şekilde yeniden yükleyebilmelerine imkan sağlayan bir işlemdir. Bu işlem için geliştirilmiş yazılımlar, mevcut sistemin ayrıntılı bir şekilde yedeklenmesini ve elektronik aygıta yeniden kurulmasını sağlamaktadır[191].

---

[188] Ş. Sağıroğlu, M. Karaman, 2012, ss.64-65.
[189] M. Özen, G. Özocak, 2015, s.54.
[190] Robert Altschaffel, Stefan Kiltz, Jana Dittmann, "From the Computer Incident Taxonomy to a Computer Forensic Examination Taxonomy",**Fifth International Conference on IT Security Incident Management and IT Forensics, 2009.**
[191] M. Kızılyar, 2014, s.83.

Delillerin analizi aşaması yapılırken verilerin elde edildiği bilgisayarda analiz yapılmamalı, klonlanmış veriler analiz edilmeli, orijinal veri ile analiz edilen veri arasında doğrulama yapılmalı, analizde kullanılan her türlü aygıt ve program raporlanmalı, ele geçirilen her türlü aygıt ve veri saat ve tarihiyle birlikte kayıt edilmelidir. Ayrıca, bilgisayarın *unallocated, file slack, swap space* veya *slack space* gibi alanlarında geçmişi ait veriler olacağı unutulmamalı ve analizi yapılmalıdır[192]. CMK'ya ve ilgili yönetmeliklere göre toplanan ve analizi yapılan delillerin son aşaması teknik terimlerden mümkün olduğunca arındırılarak savcılık makamına rapor halinde sunulmalıdır.

Bilgisayarlar büyük miktarda veriye sahip ve kendine özgü logları oluşturan aletlerdir. Dijital teknolojinin revaçta olduğu günümüz dünyasında birçok yazışma e-posta üzerinden gerçekleştiği için bu e-postaların kullanıcı yazışmaları da adli makamlar için çok önemli bir dijital delil hükmündedir[193]. Teknolojinin hızlı bir şekilde geliştiği günümüz dünyasında kiralanan araçlar, toplu taşımalar veya taşımacılık sistemlerinin GPS sistemleri ile entegre edilmesi sayesinde ziyaret edilen yerler, favori yerler ve aranılan yerlerin zaman bilgisinin tutulması birçok adli olayda aydınlatıcı bilgi verebilir[194].

Belirli bir sistem içerisinde kurulu olan *Local, Wan* veya *İnternet* ağ trafiği, cep telefonlarının servis sağlayıcılara ait fatura veya CDR (call detailed record) adı verilen arama detay bilgileri, telefonlarda kullanılan *skype, WhatsApp, tango, viber* vb ücretsiz haberleşme yazılımlarının incelenmesi ile de dijital delillere ulaşılabilir. Özellikle arama detayında şüphelinin konuşma süresi, arama saati ve arama sıklığı gibi veriler suçun belirlenmesine aracılık edebilir. Diğer yandan PDA, USB Bellek, dijital müzik

[192] Daniel Ayers, "A Second Generation Computer Forensic Analysis System", **Digital Investigation2009**, 6(42), s.34; Ş. Sağıroğlu, M. Karaman, 2012, s.65.
[193] Ş. Sağıroğlu, M. Karaman, 2012, ss. 63-64
[194] David Last, **Computer Analysts and Experts – Making the Most of GPS Evidence**, Erişim Tarihi: 25.11.2017, http://articles. forensicfocus.com/2012/08/27/computer-analysts-and-experts-makingthe-most-of-gps-evidence/,

oynatıcıları, ses kayıt cihazları ve taşınabilir diskler birçok şifreli veri ile beraber kroki, çocuk pornosu, ses kayıtı, uygunsuz videoların saklandığı ve izlendiği yerler olması nedeniyle dijital delillere ulaşma adına incelenmesi gereken cihazlardandır[195].

Sosyal ağlar, sohbet siteleri, forumlar, bloglar şahısların birbiriyle iletişim kurmasına olanak sağlayan ,ve bilgi paylaşılan alanlardır. "*Facebook, Twitter, Myspace, Linkedin, Ekşi Sözlük"* gibi birçok sosyal paylaşım sitesinde kişilerin yapmış oldukları paylaşımlar, bu paylaşımlara verilen tepkiler, iletişimler, aşağılamalar ve tehditler, bulundukları gruplar, grup hareketleri vb. çoğu iletişimle ilgili eylemler, belirtilen mail kutularına veya kullanmış oldukları uygulamalar vasıtasıyla sistemlerine ulaşmaktadır. Bu iletiler ya da kullanılan sosyal ağlardaki hareketlerde dijital verilerin ulaşılacağı alanlardır[196].

2. Dijital Verilerin Delil Olarak Kullanılması

Dijital bir verinin delil olabilmesi için, o verinin usule göre elde edilmiş olması gerekir. Bu nedenle ele geçirilemeyen dijital veriler delil olarak kullanılamaz. Dijital verinin varlığı ile ilgili tanık beyanı olmasına rağmen ele geçirilemeyen dijital veri, delili dijitallikten çıkarır ve beyana dayalı delil haline getirir. Ele geçirilen dijital verinin veya e-posta içeriğinin delil olabilmesi için kime ait olduğunun belirlenmesi ve içeriğin doğrulanmasına ihtiyaç vardır. Diğer delillere göre dijital delillerin bozulması, değişikliğe uğratılması sık rastlanan bir durumdur. Bu nedenle delilin geçersizliği veya sahte olduğuna yönelik iddialar çok sık bir şekilde ileri sürülebilir. Dijital delillerin delil olarak değerlendirilmesi için teknik ve fiziksel özelliklerinin bozulmadan ulaşılması gerekmektedir. Ayrıca dijital delil değeri, delilin hukuk kuralları çerçevesinde ele

[195] M. Özen, G. Özocak, 2015, s.49.
[196] M. Özen, G. Özocak, 2015, s.50.

geçirilmesine, suça konu olan olayla ilgisine, olayın aydınlatılmasını doğrudan veya dolaylı etkileyecek olmasına bağlıdır[197].

Muhakeme makamlarının dijital delili kabul etmesi için öncelikle veriler arasında bütünlük ve doğruluğunun sağlanıp sağlanmadığına bakmaktadır. Doğruluğu sağlanamayan verilerin dijital delil değeri olmaz. Bu nedenle klonlanan veriler ile orijinal veriler arasında tutarsızlık olmaması gerekir. Deliller kanunda öngörülen sürece ve usule uygun edinilmişse adli makamlarca delil değeri olduğuna hükmedilebilir[198].

Bilgisayarlı elektronik aletlerden elde edilen dijital verilerin hangi aygıttan elde edildiği veya kim tarafından kullanıldığı, ne zaman oluşturulduğu, ne zaman değiştirildiği genellikle sistem kayıtlarından belirlenebilir. Ancak, verilere ait bilgiler çeşitli programlar veya işlemlerle değiştirilebilir. Bu nedenle dijital veri ele geçirildiğinde imajlarının alındıktan sonra bir kopyasının şüpheliye teslim edilmesi, tutanağa geçirilmesi gerekir. Bu işlem sayesinde delil üzerinde yapılan değişiklikler delil değerini etkileyeceği için şüphelideki veriler ile alınan imajlar arasında farkın olup olmadığı analiz edilerek sahte iddialarının önüne geçilebilir[199].

Dijital delillerin incelenmesi imaj üzerinde yapılacağından orijinal disk ile imajın algoritma değerlerinde farklılığın oluşmasının deliller üzerinde oynandığına işaret edeceği bilinmelidir. Bu nedenle orijinal veriler ile incelenen veriler arasında algoritma değerlerinin birbirini tutmaması delil değerini yitirmesine neden olacaktır[200].

Dijital verilerin delil değeri taşıması için orijinal olmasının yanı sıra başkaca delillerle de desteklenmesi gerekebilir. Veriyi içeren dosya adının, kullanıcı adının diğer kişiye has özelliklerin olup olmadığının belirlenmesi suç isnadı açısından delilin

[197] M. Kızılyar, 2014, ss.86-88
[198] M. Özen, G. Özocak, 2015, ss.54-55
[199] M. Kızılyar, 2014, ss.86-88
[200] Y. Şimşek ve diğerleri, 2012, ss.79-80

değerini belirler. Dijital verilerin delil değeri; kapsadığı veriler, oluşturulma biçimi, erişimle ilgili bilgiler gibi suç ve suçluya ait özelliklerin ilişkisine bağlıdır[201].

Uygulamada karşı karşıya kalınan en önemli sorun "dijital delillerin güvenilirliği"dir. Dijital verinin "delil" değeri bu delillerin orijinalliği ile ilgili olduğu için Yargıtay aldığı bir kararda; "sanığın işyerine ait güvenlik kamerası kayıtlarının orijinalliğine ve bu kayıtlara ekleme yapılıp yapılmadığına ilişkin olarak bir bilirkişiden rapor istenmesi gerektiğine işaret edilmiş, aksi yöndeki uygulama bozma nedeni kabul edilmiştir."[202]

Usulüne uygun olmayan ses ya da görüntü tespit eden belgeler hukuka aykırı delil oldukları için dijital delil olarak kullanılamaz. Diğer yandan bu deliller usulüne uygun olarak elde edilmiş olsa bile çoğu doktrine göre tek başına mahkumiyet kararı verdirecek delil değeri olamaz. Başka delillerle desteklenmesi gerekir[203].

Avrupa Siber Suç Sözleşmesine göre ise sanal ortamlarda bulunan dijital verilerinin, ceza muhakemesi hukukunda delil değerinin olduğu ve bu delillerin diğer maddi delillerle eşdeğer olarak adli birimlerce kullanılması gerektiği bildirilmiştir[204].

Dijital delillerin diğer deliller gibi bir takım özelliklere sahip olması adli makamlarca delil değerlerini değiştirecektir. Bu deliller; kabul edilebilir olmalı, akıl ve mantık kuralları ile bağdaşmalı, gerçekçi olmalı, bilimsel kurallara uymalı ve ispatlanabilir olmalıdır. Maddi gerçeğe ulaşılmaya çalışılan konuyla ilgili mahkemeyi aydınlatıcı ve konunun çözüme kavuşmasını sağlayıcı olmalıdır. Dijital bilgiye ulaşma

[201] M. Kızılyar, 2014, ss.86-88
[202] Çetin Arslan, "Dijital Delil ve İletişimin Denetlenmesi",**CHKD 2015**, 3(2), 253-266 (6. CD, 19.07.2010, 2010/6992, 2010/13757)
[203] B. Öztürk ve diğerleri, 2010, s.430
[204] Daniele Cangemi, "Procedural Law Provisions Of The Council Of Europe Convention On Cybercrime",**International Review of Law Computers &Technology 2004**, s, 165

şekli, saklama ve değerlendirmesi hukuka aykırı olmamalıdır. Ayrıca, delil denetlenebilmeli ve tekrar incelendiğinde aynı sonucu vermelidir[205].

Dijital delillerin "Güven seviyesi" (confidence level), analizler sırasında elde edilen bulguların nitelik ve niceliklerine göre sınıflandırılmasıdır. Bu sınıflandırma sayesinde "aslına uygunluğunu", "kaynağını" ve "kullanıcı ilişkisini" belirlenerek dijital delilin hangi güven seviyesinde olduğu belirlenebilmektedir. Bununla birlikte dijital adli analiz biliminde karşılaşılan en önemli sorun yorumlama ve kesin karar verme aşamalarında tanımlı bir matematiksel formülün bulunmamasıdır. Dijital delillerin hangi kriterlere göre ve hangi kategoride değerlendirilmesi gerektiği adli uzmanın tecrübe ve bilgisine dayanarak yapıldığından nesnel olmayan bir sınıflandırmadır. Bu nedenle de farklı uzmanlar farklı sonuçlar çıkarabilir. Bununla birlikte aşağıdaki tabloda bulunan değerlendirme aşamaları güven seviyesi ve karar aşaması için faydalı olabilecek bir varsayımdır.

Tablo 1. Dijital Delil Değerinin Belirlenmesi[206]

Güven Seviyesi	Tanım	Nitelik Sınıflandırması
G0	Bulgu bilinen doğrularla çelişiyor, tespit hiçbir şekilde kabul görmüyor.	Tamamen Yanlış
G1	Bulgu ciddi şekilde sorgulanıyor. Cevaplanamayan soru veya sorular bulunmakta.	Şüpheli
G2	Bulguların manipüle edilmesi zor, bununla birlikte açıklanamayan tutarsızlıklar ve delil bütünlüğünü etkileyen eksiklikler mevcut.	İhtimal Dâhilinde
G3	Bulgunun manipüle edilmesi imkânsız veya aynı sonuca ulaştıran çok sayıda manipüle edilebilme ihtimali düşük bulgu var.	Kuvvetle Muhtemel
G4	Birden çok bağımsız otorite tarafından manipüle edilmesinin imkânsız olduğu türde bulgular mevcut. Bununla birlikte geçici veri kaybı gibi çok ufak belirsizlik ihtimalleri var.	Neredeyse Kesin
G5	Bulgunun doğruluğu ve kesinliğine hiçbir şüphe yok, bulgunun manipüle edilmesi imkansız.	Kesin

[205] Halid Özkan, **Ceza Muhakemesinde Ekran Görüntüsü Çıktılarının Delil Niteliği**, **Karşılaştırmalı Güncel Ceza Hukuku Serisi:15, Ceza MuhakemesiHukukunda Delil ve İspat,** Ankara, 2014. s.268.
[206] Emin Çalışkan, **Zararlı Yazılımların Etkisinde Dijital Adli Delillerin Güvenilirliği,** İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, İstanbul, 2013, s.117-118.

Bu tabloya göre yapılabilecek delil değeri analizi hayali bir "e-posta ile tehdit edilme" davası olarak incelemek gerekirse;

"*G5: Müzekkerede incelenmesi talep edilen dijital delillerin ilgili sabit disk imajında tespit edilmesi. Tespit edilen bu delillerdeki isimlerin, e-postalar ve benzeri diğer delillerin içeriklerinin ve resim/fotoğraf vb. materyallerin görsel inceleme sonucunda aynı delil olduğunun anlaşılması.*

G4: Kullanıcı bilgisi, oturum bilgisi, e-posta hesabı veya IP adresi gibi verilerin, bilgisayarı incelenen şahsı işaret etmesi. Bağımsız otoritelerin bu gibi verilerde güven seviyesinin neredeyse kesin olduğuna dair tespitlerinin olması, bu alanda yayınlamış çeşitli makalelerin uluslararası camiada kabul görmesi.

G3: Sabit disk imajında tespit edilen ve tehdit içeren e-postaların, bilgisayarın kullanıcısı tarafından gönderildiğine dair olan gönderici adı, gönderenin e-posta sunucu IP'si gibi verilerin varlığı veya aynı tarihlerde oluşturulduğu tespit edilen ve e-posta içeriğiyle tutarlı birçok dosyanın sabit diskte bulunması.

G2: Sabit disk imajında ilgili tarihlerde hazırlandığı tespit edilen, üst verilerinin tarih ve kişi bilgileri ile tutarlı olduğu bir dosyanın tespiti. Bununla birlikte tehdit amaçlı gönderildiği iddia edilen e-posta kayıtlarının bulunmaması.

G1: İlgili imajda tehdit için kullanılmış olabilecek çeşitli internet sayfaları, bazı kişisel veriler ve sosyal medya araştırmalarına dair tespitlerin bulunması. Bununla birlikte tehdit için gönderildiği iddia edilen metin dosyasının veya e-postanın bulunmaması.

G0: Sabit disk imajında iddia edilen tehdit içeriğine veya öncesinde yapılmış olabilecek muhtemel araştırmalara dair hiçbir izin bulunmaması."[207]

Bu sınıflandırmanda anlaşıldığı gibi dijital verilerin delil değeri oldukça karmaşık bir analiz ve sübjektif sayılabilecek yorumlamalara dayanmaktadır. Bununla birlikte bu tip bir sınıflandırma dijital adli analiz uzmanının tespitlerini hem daha kolay anlaşılır hale getirecek hem de belirli bir standart halinde sunulması adli birimlerin yorum farkını en aza indirebilecektir.

Bilişim cihazlarının hayatı kolaylaştırarak sağladığı çok sayıdaki yararlarının yanı sıra birçok suçun işlenmesi ve suçun gizlenmesine zemin hazırlayıcı teknik niteliğe sahip olması gibi zararlı yanları da bulunmaktadır. İnsanlar, özellikle internet vasıtasıyla elindeki verileri başkalarıyla paylaşabilmekte, dijital ajandalarına suç teşkil edecek veriler girebilmektedir. Bilişim alanındaki bilgi ve becerileriyle kısa zaman içerisinde evinde oturduğu yerden dünyanın diğer ucundaki bir kullanıcı ya da kurumun verilerini ele geçirebilmekte, işleyişini engelleyebilmekte ya da insanların kişisel hesaplarından gizlice para transferi yapabilmektedirler. Kullanıcılar tarafından yapılan usulsüz faaliyetler elektronik aletleri kullanılarak gerçekleştirildiği için soruşturma ve kovuşturma birimlerince bu cihazlarda dijital verilere ulaşıldığı durumda konuyla ilgili suç aydınlatılabilmektedir.

Teknolojinin gelişmesi ve bilişim alanında meydana gelen suçların artışı, ceza hukukunda da bir takım düzenlemelerin yapılmasına neden olmuştur. Bu düzenlemelerden biri de dijital verilerin delil olarak kullanılması için gereken usül ve mevzuat kriterleridir. Bu konuda AİHM ve Yargıtay içtihatlarında da dijital delillerin bireylerin temel hak ve hüriyetlerinin özünü ihlal etmemesi veya bu hakların ağır müdahalelere uğramaması da bir kriter olarak alınmıştır Temyiz mahkemeleri delillerin

[207]E. Çalışkan, 2013, s.118.

kaknuna uygun olarak elde edilmesi, hukuka aykırı olmaması, gerçekliği ve güvenirliğini inceleyerek usule ve mevzuata uygun bulması halinde dijital verilerin delil olmasını hukuka aykırı bulmamaktadır[208].

CMK madde 116'da "*Yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe varsa; şüphelinin veya sanığın üstü, eşyası, konutu, işyeri veya ona ait diğer yerler aranabilir*" hükmü ile dijital delillerin toplanması da makul şüphe kapsamında değerlendirilebilir. Ancak, bu karar bilgisayar ve bilgisayara özelliklerine sahip cighazlar dışındaki diğer delillerin toplanması ile ilgilidir.

Bu aygıtlardaki verilerin kanıt olarak toplanmasıı amacıyla özel hayata ağır müdahale olabileceği için CMK 134. Maddede özel olarak düzenleme yapılmış, diğer kanıtlardan farklı olarak özel bir usul ve yargıç kararı ile delil toplanması yasalaştırılarak AİHM[209] kararlarına uyacak paralel hükümler getirilmiştir[210].

Dijital delillerin elde edilmesinde özel hayatın gizliliği esas alınarak CMK'nın genel arama ve el koyma hükmünden ayrılmıştır. Kanuni müdahalenin şartları belirlenmiş ve arama ve el koyma işlemi için hakim kararı şart koşulmuştur. Ayrıca suç

[208] M. Kızılyar, 2014, s.86-88

[209] AİHM, İkinci Daire, Başvuru no:58223/10; http://www.fap.hsyk.gov.tr/dosyalar/aihm-karar.html; C.A.Ç./Türkiye, *"Başvuranın, savcılık tarafından aleyhinde sunulan delil unsurlarının geçersiz olduğuna ve sonuç olarak tutuklanmasını haklı gösterecek makul şüphelerin bulunmadığına ilişkin iddiasıyla ilgili olarak, AİHM soruşturma dosyasında bir yandan aleyhte olan delil unsurlarını oluşturan dijital belgelerin gerçekliğini doğrulayan bilirkişi raporları, diğer yandan savunma makamı tarafından sunulan ve bu delillerin inandırıcılığına değinen aksi yönde kanaat bildiren bilirkişi raporlarının yer aldığını kaydetmektedir. Öncelikle ceza soruşturması prosedürünün sonraki aşamasında, başvuranın ileri sürdüğü gibi, delil unsurlarının inandırıcı olup olmadığını veya bunların kendisine iftira atma niteliği taşıyan sahte bir unsur olup olmadığını tespit etme yükümlülüğü ulusal yargı organlarına aittir. Şüphelilerin bulunduğu aşamada gereken olguları ispat etme seviyesiyle ilgi olarak Sözleşmenin 5 inci maddesinin birinci fıkrasının gerekleri dikkate alındığında, AİHM, ceza dosyasının, başvuranın kovuşturulmasına neden olan suçu islemiş olabileceği konusunda objektif bir gözlemciyi ikna edebilecek bilgiler içerdiği kanaatindedir. Dolayısıyla, başvuranın Sözleşmenin 5 inci maddesi, birinci fıkrası, (c) bendi uyarınca, bir suç işlemiş olabileceğine dair hakkında makul şüphe oluşturacak 'inandırıcı nedenlere' dayanarak yakalanıp tutuklandığına karar vermek gerekmiştir"*

[210] M. Kızılyar, 2014, s.84-86

şüphesi olması ve başka şekilde delile ulaşma olası olmadığı için bilgisayarları arama ve el koyma tedbiri getirilmiştir[211].

"CMK 134". Maddeye göre;

"(1) Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması 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) İstemesi halinde, bu 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."[212]

Bu hükümlere uygun elde edilmeyen dijital verilerin delil olarak kullanılmasının yasal olmadığı çeşitli Yargıtay kararlarından da anlaşılmaktadır[213]. Dikkat edilirse

[211] V.Ö. Özbek ve diğerleri, 2012, s.380.
[212] CMK, 134. Madde

"CMK 134. Maddede" bilgisayarlarla ilgili hükümler bulunmaktadır. Ancak, bilgisayar özelliği taşıyan elektronik aygıtların da bu hükme tabi olacağı yorumu yapılabilir. Bununla birlikte bilgisayar ve bilgisayar özelliği taşımayan diğer elektronik aygıtlarla ilgili arama ve el koyma işlemlerinin "CMK 116 ve 129". Maddelerindeki genel hükümlerine göre yapılabileceği de unutulmamalıdır[214].

Dijital deliller maddi ve bilimsel deliller gibi genellikle belirti olarak değerlendirilmektedir. Bununla birlikte dijital delilin doğruluğunun tespiti halinde belge niteliğinde "belge delili" olarak kabul edilebilir. Ayrıca, dijital deliller "belirti" olarak kabul edilse bile belirtilerin sıhhati iyice araştırıldığında diğer deliller gibi değerlendirildiği unutulmamalıdır[215].

Ses ya da görüntü tespit eden belgelerin delil niteliği taşıyıp taşımadığı tartışmalıdır. Bunun sebebi bu verilerin kolaylıkla değiştirilebilir olmasıdır. Bu sebeple ses ya da görüntü tespit eden araçlarla elde edilmiş belgelerin ispat gücünün zayıf olduğu[216], tek başına mahkumiyet kararı verilemeyeceği sadece belirti olarak kabul edilebileceği başka delillerle de desteklenmesi gerektiği ifade edilmektedir[217]. Dijital delillerin delil olarak değerlendirilmesi için elde edilen dijital sistemin hepsinin incelenmesi, uzmanlar tarafından doğrulanması gerekir.

---

[213] Yargıtay Sekizinci Ceza Dairesinin 24/10/2013 tarih ve E.2012/21817, K.2013/25428 sayılı kararında; *"Sanığın kullandığı bilgisayar üzerinde usulünce imaj alma işlemi yapılarak sonucunda çıkan veri bütünlük (hash) değerlerinin tesbit edilmemiş bulunması, IP numarasının kullanılan bilgisayarı göstermeyip internetle olan bağlantıyı göstermesi, sanığın bilgisayarlarında yapılan incelemede, bu bilgisayar kütüğünden marma-riskoleji-k12.com adresine bağlantı yapıldığının tespit olunamaması 'hack' proğramına rastlanmasının sikayetçiye ait siteye müdahele edildiğini göstermeyeceği, kesin delil bulunmadan varsayımlarla hüküm kurulamayacı gözetilmelidir."* Yargıtay Onüçüncü Ceza Dairesinin 01/10/2013 tarih ve E.2012/17470, K.2013/26886 sayılı kararında da; *"Sanığa ait olan modem ve bilgisayar kasaları ile dosyanın, bütünüyle bilişim suçlarından anlayan tercihen bilgisayar mühendisi bir bilirkişiye tevdi edilerek bilgisayarlara bağlı modem türlerinin tespit edilmesi, modem hatlarının kablosuz olması durumunda hattın güvenliği için gerekli önlemlerin alınıp alınmadığı, internet bağlantısına dışarıdan girilip girilemeyeceği, IP numarasının değiştirilmesinin mümkün olup olmadığı, bilgisayarlara virüs gönderilerek bilgilerinin alınıp alınmadığı suça konu işlemin ne şekilde nereden yapıldığı konularında rapor düzenlettirilmesi, sonucuna göre tüm deliller çerçevesinde sanığın hukuksal durumunun değerlendirilmesi gerekirken, bu konularda kovuşturma genişletilmeden eksik inceleme ile yazılı şekilde karar verilmesi, bozmayı gerektirmiştir."*

[214] M. Kızılyar, 2014, s.86

[215] N. Toroslu, M. Feyzioğlu, 2009, s. 196.

[216] N. Toroslu, M. Feyzioğlu, s. 196.

[217] B. Öztürk ve diğerleri, 2010. s.429-430.

Elektronik ortamda bulunan plan, çizim, kroki, film, fotoğraf, ses kaydı, görüntü gibi deliller gözlem ya da duyum ile doğruluğu tespit edilen deliller olarak değerlendirmek gerekir. Bu nedenle ceza yargılamasında bu tip delillerin kendilerine has özellikleri dikkate alınarak işleme tabi tutulmalıdır[218].

Yargıtay'ın 22.2.2000 tarihli kararında *"teyp bantları, kaydedilen sözlerin kime ait olduğunun şüpheye yer bırakmayacak şekilde saptanmasının teknik olarak mümkün bulunmaması nedeniyle tek başlarına delil değeri taşımazlar*" ifadesiyle ses verilerinden oluşan dijital delilin tek başına kullanılamayacağını göstermiştir. Dijital delillerle ilgili çekinceler yönünden "Yargıtay 11. Ceza Dairesi'nin" aldığı bir kararda E-posta yoluyla virüs gönderilerek bir şirketin bilgisayarlara zarar verildiğine yönelik iddialar karşısında dijital delillerin elde edilmesinde kurallara dikkat edilmesi, delillerin kendilerine özgü yapıları sebebiyle tedbirli davranılması gerektiğinin altı çizilmiştir[219]. Bununla birlikte

[218]Y. Ünver, H. Hakeri, 2012, s.24.

[219]http://www.bilisimhukuk.com/2010/01/dijital-delillere-yargitaydan-ince-ayar/, *"- Virüs içeren bir e-posta veya e-postaların şikayetçinin bilgisayarlarına virüs bulaştırması sonucu doğacak zararın, şirketin gönderdiği e-postalar aracılığıyla başka adreslere virüs göndererek başka bilgisayarlara zarar vermesi ve kendi bilgisayarlarının sistem dosyalarını silerek çalışamaz duruma getirip iş ve zaman kaybına neden olması karşısında, virüslü veya virüssüz bir e-postayı gönderen bilgisayarı bulmanın mümkün olduğunu,*

- E-postayı gönderen bilgisayarın IP numarası, e-postayı gönderen sunucu bilgisayarın IP numarası, gönderici ve alıcı adreslerinin, e-posta almayı ve göndermeyi sağlayan e-postanın sunucu bilgisayarlarının tuttuğu günlük kayıtlarında saklandığını, servis sağlayıcı firmaların bir süre sonra bu kayıtların olduğu dosyaları silebildiğini, bu bilgilerin servis sağlayıcı firmalardan resmi yollarla istenilerek öğrenilebileceğini,

- E-posta sağlayıcı şirketin günlük (log) kayıtları mevcutsa gönderici eposta adresini, e-postanın yazılıp yola çıkarıldığı ilk bilgisayarın IP numarasını ve IP numarasının sahibi servis sağlayıcı firmanın isminin bulanabileceğini, servis sağlayıcı firmadan da, günlük kayıtları mevcutsa verilen tarih ve saat için bu IP numarasının kullanıcısının öğrenilebileceğini,

- Şayet e-postanın yola çıkarıldığı sistemin IP numarası e-posta sağlayıcı şirketten öğrenilemezse ve e-postayı gönderen adres .....@yahoo.de olarak bulunursa Yahoo şirketinden; başka bir adres çıkarsa o e-posta adresini sağlayan servis sağlayıcıdan, bu adresi kullanan kişinin sistemde kayıtlı kimlik bilgileriyle, mevcutsa günlük kayıtlarından bu adres aracılığıyla e-posta gönderip almak için sisteme erişildiğindeki tarih ve saatler ile erişilen IP numaralarının öğrenilebileceğini,

- Bu kullanıcı telefonla bağlanan bir ev kullanıcısı ise bağlanılan telefon numarasından kimliğinin kolaylıkla bulunabileceğini,

"Yargıtay'ın 9. Ceza Dairesinin 10 Eylül 2012'de" verdiği başka bir kararda ise dijital verileri delil olarak kabul ettiğini beyan etmiştir. Yargıtay, dijital delillere göre mahkumiyet hükmü kurmuş olan ilk derece mahkemenin kararını onayarak dijital verilerin somut olayları aydınlatma özelliği nedeniyle delil olmasını kabul etmiş bulunmaktadır. "Yargıtay'ın 9 Ekim 2013 tarihli 2013/9119 Esas", "2013/12351 Karar sayılı kararında" Yargıtay ceza muhakemesindeki delil serbestisi ilkesinden bahisle dijital delillerin de delil olarak kabul edilebileceği bildirilmiştir. Dijital delillerin dünya üzerinde de farklı yargılama usullerine göre artık kuvvetli deliller olarak kabul edildiği görülmektedir. Bununla birlikte dijital delillerin ne derece kuvvetli olduklarından ziyade ne derece güvenilebilir olduklarının tartışılması ve ona göre hükme esas olup olamayacağına karar verilmesi gerekir[220].

Bazı durumlarda sadece olayla ilgili elde edilen delilin dijital olması, delilin çok titiz bir şekilde değerlendirilmesini gerekli kılar. Şüphenin sanık aleyhine yorumlanması masumiyeti zedeleyeceği ihtimal dahilindedir. Bu nedenle dijital delillerin hükme esas alınması bu tür davalarda insan hakları açısından daha büyük sorunlar oluşturacaktır.

- Gerçeğin kuşkuya yer vermeyecek şekilde belirlenmesi açısından; öncelikle e-posta yolu ile virüs göndererek sistemine zarar verilmiş bir bilgisayarda incelemenin, olayın hemen akabinde yapılması ya da inceleme yapılacak bilgisayarın veya bilgisayara ait veri içeren ünitelerin, olaydan sonra inceleme yapılana kadar hiç kullanılmaması gerektiği,

- İncelenecek bilgisayarın diskine bazı bilgilerin yazılması, değişmesi veya silinebilmesini önlemek ve söz konusu diskin bütünlüğünü sağlamak için bilgisayarda virüslü dosya üzerinde inceleme yaparken ilk işlem olarak, söz konusu dosyanın birebir (sector-by-sector) yedeğinin alınması (yani incelemenin orijinal dosya üzerinde yapılmaması), daha sonra ikinci olarak alınan birebir yedeğin değiştirilip değiştirilmediğini tespite yarayacak zaman ve bütünlük kontrolü imkanı sağlayan değerin (hash) belirlenmesi,

- Bir e-postanın kimden geldiğinin tespiti için de, ilk olarak e-postayı gönderen IP adresinin bulunması (örneğin; şikayetçiye gelen e-postanın seçeneklerinden e-posta üst bilgisinin belirlenmesi ve bu üst bilginin uzman kişiler tarafından incelenmesi veya şikayetçiye gelen e-postanın göndericisinin ya da alıcısının e-posta sunucusunun sahibi şirkete belirtilen tarih ve saatte bahse konu e-postanın hangi IP adresinden gönderildiğinin sorulması,

- Daha sonra da bulunan IP adresinin belirtilen tarih ve saatte hangi abone tarafından kullanıldığının ve o abonenin açık adres ve kimlik bilgilerinin talep edilmesi ve bulunan IP adresini kullanan abonenin sanıkla bağlantısının araştırılması gerektiği"

[220]Elif Gökşen, **Türk Ceza Muhakemesinde Dijital Verilerin Delil Değeri,** Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, 2014, s.114-122.

Yargıtay 13. Ceza Dairesi'nce verilmiş 2013 tarihli bir kararda; *"müştekiye ait iş yerinde bulunan güvenlik kamerasından elde edilen görüntülerin olayın tek delili olması nedeniyle, bu görüntülerin donanıma sahip bilirkişi veya kurumlara incelettirilerek görüntülerdeki kişinin sanık olup olmadığının tereddüde mahal vermeyecek şekilde belirlenmesi gerektiğine*" işaret edilmiş, "*aksi yöndeki uygulamanın bozma nedeni sayılacağı"* ifade edilmiştir[221]. Bu nedenle dijital delillerin hükme esas kabul edilmesinde azami derecede dikkat edilmesi, doğruluğundan şüphe duyulmaması, tekrar edilen farklı uzman ve programlarca yapılan analizlerde hep aynı sonucu vermesi aranmalıdır.

Özetlenecek olursa dijital verilerin delil olarak kullanılabilmesi ve hukuken geçerli olabilmesi için delilin ispatında kullanılan özelliklerine benzer bazı temel niteliklere sahip olması gerekir. Bu özellikler aşağıdadır;

- ***"Dijital delillerin bütünlüğü:*** *Elde edilen dijital verilerin sonradan değiştirilmesi, silinmesi veya yenisinin oluşturulması delilin bütünlüğünü bozmaktadır. Bu durum elde edilen delilin hash değeri ile belirlenmektedir.*
- ***Dijital delillerin doğrulanması:*** *Dijital deliller ele geçirildikten sonra mahkeme sürecinde verilerin gerçekten o kişiye ait olup olmadığı doğrulanmalıdır.*
- ***Dijital delillerin inkar edilememesi:*** *Ele geçirilen dijital delillerin adli bilişim aşamasında yapılan işlemler sırasında gerekli raporlandırma ve belgelendirme işlemleri ile delilin şahsa ait olduğu ve inkarının mümkün olmaması gerekir.*
- ***Dijital delillerin doğruluğu:*** *Dijital delillerin ele geçirilmesi esnasında kullanılan tekniklerin ve kullanılan bilgilerin doğruluğunun ispatı gerekir.*
- ***Dijital delillerin daha sonra ele alınabilirliği:*** *Dijital deliller oluşturulduktan sonra, bu delilleri üçüncü bir şahıs her zaman için inceleyebilmesi ve değerlendirebilmelidir.*

[221] Ç. Arslan, 2015, s. 263.

- ***Akla uygunluk ve kabul edilebilirlik:*** *Bir şeyin delil niteliği taşıması için en basitinden sorgulanan konuyu aydınlığa ulaştıracak olması gerekir. Ayrıca, o delilin mahkemeye sunulabilmesi için de kanuni kısıtlaması veya yasağı olmamalıdır.*

- ***Gerçeklik ve hakikilik:*** *Elde edilen dijital delil soruşturmaya esas konu ile doğrudan ilişkisi olmasıdır.*

- ***Tamam ve eksiksiz:*** *Delilin birden fazla perspektifi işaret etmesi durumunda, sanığın suçsuzluğunu ispat edecek deliller de toplanmalıdır.*

- ***Güvenilirlik, itimat edilebilirlik:*** *Delil toplama ve inceleme prosedürleri sırasında yapılan işlemler delilin doğruluğu ve gerçekliği ile ilgili şüphe uyandırmamalıdır.*

- ***İnanılabilirlik:*** *Elde edilen ve adli birimlere sunulan deliller anlaşılabilir ve inanılabilir özelliklere sahip olmalıdır.*

- ***Tekrar Edilebilirlik:*** *Adli birimlere delil olarak sunulan tüm değerlendirme sonuçlarına aynı yöntemler kullanılarak farklı kişilerce, farklı yerlerde ve zamanlarda da ulaşılabilmelidir."*[222]

C. Dijital Veri ve Dijital Belge Kavramları

"Veri" kavram olarak İngilizce'den dilimize geçen "data" kelimesinin karşılığı olup farklı disiplinlerde birbirinden değişik anlamlara gelse de genel olarak herhangi bir konudaki bilgi anlamından kullanılabilir. "Dijital veri", fiziken bulunan bilgilerin bilgisayar dilindeki sayısal düzemde bir ve sıfır rakamları kullanılarak ifade edilmesidir. "Dijital belge" ise dijital verilerin tek başlarına ya da bir araya gelmesiyle oluşturdukları anlam bütünlüğünün bir olay, konu ya da görüşü temsil niteliği taşımasıdır[223].

[222] Ahmet Ekim, **Bilişim Suçlarında Sayısal Delillerin Toplanması, Muhafaza Edilmesi, İncelenmesi Ve Raporlanması,** Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, İstanbul, 2013, s.6-7

[223] Mustafa Göksu, **Hukuk Yargılamasında Elektronik Delil (1086 Sayılı HUMK ve 6100 Sayılı HMK Çerçevesinde),** Ankara: Adalet Yayınevi, Nisan 2011, s.13.

"Belge" ifadesi ise TDK'ya göre; "*bir gerçeğe tanıklık eden yazı, fotoğraf, resim, film vb., vesika, doküman"* anlamına gelmektedir[224]. Veri ile belgeye karşılaştırdığımızda belgenin verilerin bir araya gelmesiyle meydana gelen bir bütünü ifade ettiği anlaşılabilir. Belgenin bir bütün olması delil olarak kullanılmasına olanak sağlarken dijital verilerin parçalardan oluşması, çoğu zaman olayın tamamını temsil etmemesi delil niteliğini tartışmalı hale getirmiştir. Bununla birlikte diğer delilleri destekler mahiyette olmaları verileri "belirti-emare" olarak kullanılmasının yolunu açarken, verinin konu bütünlüğüne sahip olması, vakayı aydınlatacak bilgiler içermesi tek başına delil olarak kullanılmasını da mümkün kılabilmektedir[225].

Ceza hukukunda belge kavramına en fazla resmi evrakta sahtecilik suçuyla ilgili olarak karşılaşılmaktadır. Bir kimsenin bir olay, olgu, duygu ve düşüncenin bir nesne üzerine bilinen anlaşılır bir dilde çizgi, sayı, yazı ve şekil ile ifade etmesi belge anlamına gelir. Belgeden söz edilebilmesi için yazının bir içeriğinin bulunması ve birisine ait olması gerekir. Evrakta sahtecilik incelemelerinde yazının kimin tarafından yazılmış olduğu da bizzat yazının yazılış şeklinden anlaşılmalıdır[226].

Türk Ceza Kanunu'nda açıkça belge kavramının tanımlaması bulunmasa da TCK'nın 204. Madde gerekçesinde "belge" kavramı şu şekilde ifade edilmiştir:

"*Belge, eski dilimizdeki 'evrak' kelimesi karşılığında kullanılmakta olup, yazılı kağıt anlamına gelmektedir. Bu bakımdan, yazılı kağıt niteliğinde olmayan şey, ispat kuvveti ne olursa olsun, belge niteliği taşımamaktadır.*

Kağıt üzerindeki yazının, anlaşılabilir bir içeriğe sahip olması ve ayrıca, bir irade beyanını ihtiva etmesi gerekir.

[224] TDK. **Belge,** Türk Dil Kurumu, Güncel Sözlük, Erişim Tarihi: 26.11.2017 http://www.tdk.org.tr,
[225] M. Göksu, 2011, s.12
[226] E. Gökşen, 2014, s.12

Bu yazının belli bir kişiye veya kişilere izafe edilebilir olması gerekir. Ancak, bu kişilerin gerçekten mevcut kişiler olması gerekmez. Bu itibarla, gerçek veya hayalî belli bir kişiye izafe edilemeyen yazılı kağıt, belge niteliği taşımaz. Kağıt üzerindeki yazının belli bir kişiye izafe edilebilmesi için, bu kişinin ad ve soyadının kağıda eksiksiz bir şekilde yazılması ve kağıdın bu kişi tarafından imzalanmış olması şart değildir."[227] Yargıtay'a göre de belge; hukuki birkaarrı içeren bir hakkın oluşmasına ve bir olayın ortaya çıkmasına aracılık eden yazı anlamına gelmektedir[228].

HMK 199/1. Maddeye göre belge; "*Uyuşmazlık konusu vakıaları ispata elverişli yazılı veya basılı metin, senet, çizim, plan, kroki, fotoğraf, film, görüntü veya ses kaydı gibi veriler ile elektronik ortamdaki veriler ve bunlara benzer bilgi taşıyıcıları bu Kanuna göre belgedir.*"[229]

TCK'da doğrudan belge kavramının tanımlanması nedeniyle uygulamada genellikle doktrine göre hareket edilmektedir. Bu nedenle madde gerekçesi, Yargıtay tanımlaması ve doktrin görüşlerine göre belgeden söz edilebilmesi için; "belge yazılı olmalıdır", "belgenin belli bir içeriği bulunmalıdır" ve "belgeyi düzenleyen belli olmalıdır"[230].

Belge yazılı olmalıdır: Bir olayın kanıtlanmasına elverişli araç ve alfabe kullanılarak hazırlanmalıdır[231]. Evrak hazırlanırken kullanılan dilin önemi yoktur, esas olan anlaşılır olmasıdır, yazı bilgisayar, daktilo ya da el yazısı ile yazılmış olabilir[232].

[227] "Türk Ceza Kanunu Madde Gerekçeleri", www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc.
[228] Bkz. Yargıtay 6. CD. 4.7.1983, 2707/3846,
[229] 6100 SAY. HMK, Belge ve Senet (Madde 199-224).
[230] E. Gökşen, 2014, s.14-15.
[231] İsmail Malkoç, **Açıklamalı Yeni Türk Ceza Kanunu Özel Hükümler (170-345), II. Cilt,** Ankara: Malkoç Kitabevi, 2006, s. 1280.
[232] Zeki Hafızoğlulları, Muharrem Özen, **Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar,** Ankara: Us-A Yayıncılık, 2012, s.163.

Bir olayı anlatan resim ya da fotoğraflar bir görüşe göre varaka olarak kabul edilirken, diğer görüşe göre bu dokümanlar yazılılık sayılamaz[233].

Belgenin belli bir içeriğinin bulunmalıdır; belge bir olayın nakledilmesini ya da bir iradenin beyanını içermeli ve içeriğin hukuki sonuçlar doğuracak niteliğe sahip olması gerekir[234]. Ayrıca, belgenin bir sürekliliği olacağı için kar ya da kuma yazılanlar belge hükmüne geçmez[235].

Belgeyi düzenleyen belli olmalıdır; TCK'nın madde gerekçesinde "*Bu yazının belli bir kişiye veya kişilere izafe edilebilir olması gerekir. Ancak, bu kişilerin gerçekten mevcut kişiler olması gerekmez. Bu itibarla, gerçek veya hayalî belli bir kişiye izafe edilemeyen yazılı kağıt, belge niteliği taşımaz. Kağıt üzerindeki yazının belli bir kişiye izafe edilebilmesi için, bu kişinin ad ve soyadının kağıda eksiksiz bir şekilde yazılması ve kağıdın bu kişi tarafından imzalanmış olması şart değildir."*[236]Belge, düzenleyen kişi belirlenebilmeli ya da teşhis edilebilmeli. Yazıyı yazanın bir kişi ya da makam olduğunun anlaşılması yazının kimliği anlamına geldiği için yazarı belli olmayan belgeler hukuken kabul edilemeyen evraklardır[237].

Bir belgede bulunması gereken yukarıda açıklanan üç önemli özellik açısından düşünüldüğünde dijital belge kavramında önemli sorunlar ortaya çıkmaktadır. Öncelikli olarak bir yazının belge olmasında zorunlu olarak görülen aidiyetin dijital belgede nasıl tespit edileceği önemli bir sorundur. Adli bilişim işlemleri sırasında analiz edilen verilerin belge olabilmesi için aidiyetlerinden kuşku duyulmaması gerekir. Dijital delillerle ilgili en önemli problem verinin hazırlayanının kesin bir şekilde belirlenememesi nedeniyle çoğu adli vakada dijital veri üzerinden hüküm

[233] Durmuş Tezcan ve Mustafa Ruhan Erdem, **Teorik ve Pratik Ceza Hukuku,** İzmir, Şafak Matbaacılık, 2002, s. 282.
[234] Nevzat Toroslu, **Ceza Hukuku Özel Kısım,** Ankara: Savaş Yayınları, Ekim 2008, s. 223.
[235] D. Tezcan ve M.R. Erdem, 2002, s. 283
[236] "Türk Ceza Kanunu Madde Gerekçeleri", www.ceza- bb.adalet.gov.tr/mevzuat/maddegerekce.doc
[237] D. Tezcan ve M.R. Erdem, 2002, s. 282; Z. Hafızoğulları ve M. Özen, 2012, s.163.

verilememektedir. Bir bilgisayardan elde edilen Word belgesinin bilgisayar sahibi tarafından yazılıp yazılmadığında önemli bir sorundur. Zira kişisel bilgisayara başkasının erişerek yazmış olma ihtimali dahi şüphelinin suçsuz olabileceğini göstermektedir. Bu nedenle sadece bir dijital veriyi hükme esas kabul etmek ya da bilgisayardan çıkan bir verinin bilgisayar sahibine ait olduğu düşüncesi peşin hüküm vermeye neden olabilecektir. Elektronik aygıtlarda bulunan yazıların yazıcılar aracılığıyla klasik anlamda yazılı belge haline dönüştürülmesi belgenin yazılı olması zorunluluğunu sağlayabilir. Ancak dijital verilerin bir anlam bütünlüğü oluşturması ve söz konusu olayı temsil edebilme özelliğine sahip olmakla birlikte teknolojik aletlerden elde edilmesi bir sorun olarak görülmektedir. Değişen koşullar gereğince işlevsel olarak belge hükmüne geçen farklı türdeki dijital verilerin belge olarak kabul edilmesi mümkün olabilir[238].

Doktrinde bazı yazarlara göre bilişim sistemlerinden elde edilen belgeye "veri tespit eden belge" tanımlaması yapılmıştır. Bu nedenle CMK'nın 134. maddesi bağlamında ele geçirilen dijital belge kopyalarının da veri tespit eden belgeler hükmünde olduğu kanaati yaygındır. Örneğin, e-postalarla ilgili veri tespit eden belge oluşturmanın değişik iletişim süreçlerinde gerçekleştirilebileceğine dikkat çekilmektedir[239].

Yazılı belgelerle yürütülen ticari işlemler, resmi kurum yazışmaları, "elektronik belge" olarak adlandırılan bir formatta geçerlilik kazanmış durumdadır. Bu belgelerin hukuk sisteminde de dijital belge hükmünde değerlendirilmesi olağan bir durumdur. Bu tip belgelerin elektronik imza yoluyla imzalanmış olması ispat ve delil olma problemini ortadan kaldırmış görülmektedir. Elektronik imza Almanya, Singapur, ABD gibi ülkeler

[238] E. Gökşen, 2014, s.17.
[239] V. Bıçak, 2011, s. 460

ile 2004'den itibaren de Türkiye'de uygulanmaktadır[240]. Şifreleme yöntemleri aracılığıyla, elektronik olarak imzalanan bir belge, sadece elektronik imzanın sahibi olan kimse tarafından düzenlendiğini gösterir. Bu yüzden belgenin bir kimliği yani yazanı bulunmuş olur. Ancak burada önemli bir sorun elektronik imzanın kötü niyetli kişilerce ele geçirilmiş olma ihtimalinin olmasıdır. Yargıtay kararlarına göre belgenin "5070 sayılı Elektronik İmza Kanununa" uygun bir şekilde elektronik imzası olmalı, ıslak imzanın eksik veya bozuk olması da iade nedeni sayılmamaktadır[241].

II. DİJİTAL VERİLERE ERİŞEBİLMEK AÇISINDAN BİLİŞİM SİSTEMİNDE KULLANILAN CİHAZLAR

A. Bilgisayar Sistemleri

Bilgisayar sözcüğü, İngilizce'de hesaplamak anlamına gelen "computer"in Türkçe karşılığıdır. Kişisel bilgisayarlar olarak adlandırılan PC'yi (Personel Computer) ilk kez 1981 yılında IBM firması üreterek dijital dünyanın tüm insanlığın hizmetine girmesine büyük katkı sunmuştur.[242]

Bilgisayar; çok sayıdaki bilgileri depolayabilen, bilgileri işleyebilen, belirli komutlara ve programlara göre işlem gerçekleştirebilen, otomatik çalışabilen, sıralı işlemleri gerçekleştirebilen, iletme özellikleri bulunan, programlanabilir nitelikteki elektronik veya manyetik akımlarla çalışan elektronik aygıtlardır[243].

"Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı"na göre bilgisayar, bilişim ağı, bilişim ortamı ve bilişim sistemlerinin tanımı şu şekilde ifade edilmiştir:

---

[240] Gürsel Öngören, **İnternet Hukuku**, Öngören Hukuk Yayınları, İstanbul, 2006, s. 86-87.
[241] Bkz. Yargıtay 14. CD., 14/4/2014 T., 2012/7985 E, 2014/5302 K. (www.kazanci.com.tr).
[242] Hayati Pallı, **Türk Hukukunda Ve Mukayeseli Hukukta Bilişim Suçları**, Erciyes Üniversitesi. Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Kayseri. 2008, s.6-10.
[243] Charles Doyle **Computer Fraud And Abuse Laws: An Overview Of Federal Criminal Laws,** Nova Science Publishers, Newyork 1998, s. 1.

"b) Bilgisayar: Belleğindeki programa uygun olarak aritmetik ve mantıksal işlemleri yapabilen, karar verebilen, yürüteceği programı ve işleyeceği verileri ezberinde tutabilen, çevresiyle etkileşimde bulunabilen araçları,

c) Bilişim ağı: En az iki bilişim sistemi arasında veya bir bilgisayar ile bir çevre birimi arasında veri iletişimini ve karşılıklı etkileşimi her türlü iletişim tekniği ile sağlayan ortamı,

ç) Bilişim ortamı: Bilişim sistemi ve bilişim ağından oluşan toplam ortamı,

d) Bilişim sistemi: Bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistemi,"[244] ifade etmektedir.

Yukarıdaki tanımlamalara göre bilgisayarlar ile diğer elektronik aletler arasındaki en önemli fark bilgiyi işleyebilmesi, programlanabilmesi ve enformatik amaçlı kullanılmasıdır. Bu özellikleri sayesinde bilgisayarlar; bilgilerin depolanmasına, depolanan bilgiye istenildiğinde tekrar ulaşılmasına, bilginin başka ortamlara aktarılmasına, içerisinde bulunan programlar donanımı vasıtasıyla hesap ve analiz yapılabilmesine, ses ve görüntünün kaydedilmesi ve iletilmesine aracılık sağlayan ve teknolojik kapasitesi devamlı değişen gelişmiş bilişim teknolojisi bir alettir.

Teknolojik gelişmelerin baş döndürücü bir hızda ilerlediği günümüz dünyasında bilgisayar nitelikli aygıtların hem yapısal hem de işlevsel özellikleri çok sık bir şekilde değişmektedir. Bu nedenle bilgisayar kelimesinin tanımı da her geçen gün değişebilmektedir.[245] Örneğin bilim adamlarının canlı organizmalara dijital veri yüklemeleri günümüzde yaşanan gelişmelerdir.[246] Bu açıdan değerlendirildiğinde

[244] "Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı", 2006 http://www.tbd.org.tr/bilisim-agi-hizmetlerinin-duzenlenmesi-ve-bilisim-suclari-hakkinda-kanun-tasarisi/
[245] Ramazan Doğan, 5237 sayılı türk ceza kanununda bilişim suçları, Adalet Yayınevi, Ankara, 2014, s. 8.
[246] Yavuz Erdoğan, Türk Ceza Kanununda Bilişim Suçları, Legal Yayıncılık, İstanbul, 2013, s. 21.

bildiğimiz donanıma sahip olmayan ancak dijital verilerin yüklenebildiği ve bu verilere göre hareket ettiği belirlenen organik bilgisayarların olması bilgisayar ile ilgili tanımlamaları yetersiz bırakmaktadır. *"Bilgisayar ve başka aygıtlar vasıtasıyla işlenecek suçlarla ilgili yargılamalarda suçta kanunilik ve tipiklik ilkesi uyarınca suçun unsurları belirlenirken en başta kavram boyutuyla değerlendirme yapılacak olması, kavramlar arasındaki sınırların belirlenmesini zorunlu kılmakta, maddi ceza hukukunda kıyas yapmanın mümkün olmaması nedeniyle teknolojik gelişime uygun yeni yasalar yapmanın zorunlu olduğu sonucuna varılmaktadır.*"[247]

B. Bilgisayarı Oluşturan Unsurlar

Bilgisayarlar donanım (Hardware) ve yazılım (Software) olmak üzere iki ana kısımdan oluşur. Donanım; sabit disk, mikroişlemci, bellek, ekran, klavye, fare, yazıcı, joystick ve tarayıcı gibi fiziksel kısımlardır. Yazılım ise donanımı oluşturan parçaların çalışma kural ve komutlarını sağlayan, yüklenen verileri işleyerek sonuçlar çıkaran, elde edilen bu sonuçları kullanıcılara sesli ve görsel olarak sunan program, veri ve protokoller gibi fiziksel niteliğe sahip olmayan kısımlardır.

Günümüzde bilgisayarlar sistemlerini merkezi işlemci ünitesi (central processing unit- CPU), dahili bellek, ağa bağlı diğer bilgisayarlarla veri akımını sağlayan diğer cihazlar, disk sürücü olarak ayırabiliriz.[248]

1. Mikroişlemci- CPU

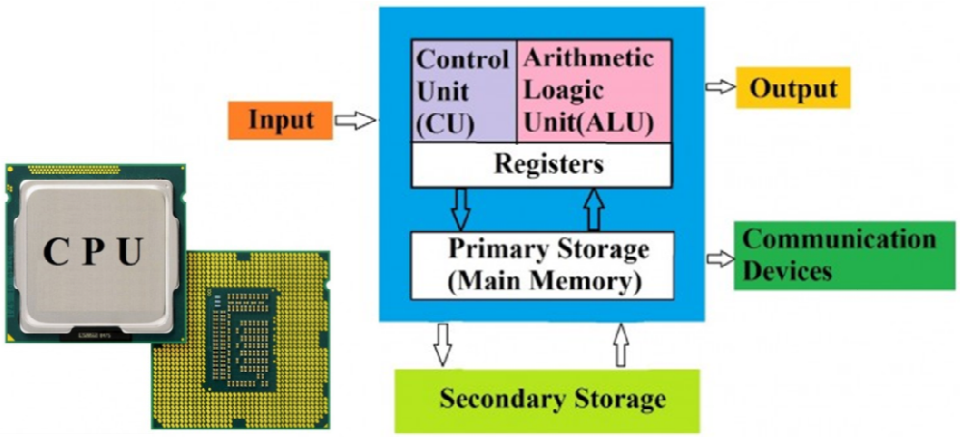
CPU, bilgisayarın "merkezi işlem birimi", "işlemci" ya da "ana işlemci" olarak da isimlendirilir. Bu donanım parçası, bilgisayardaki program direktiflerini yorumlayarak verinin işlenmesini sağlayan, programlanabilirlik özelliğe sahip tümleşik devrelerden ibarettir. Tümleşik devre, yarı iletken maddeden ibaret ince bir yüzey

[247] H. Pallı, 2008, s.6-7.
[248] Mustafa Topaloğlu, **Bilişim Hukuku,** Adana: Karahan Kitabevi, 2005, s. 3.

üzerine yerleştirilmiş ve küçültülmüş devredir. Bu devrenin yerleştirildiği yarı iletken madde ise yonga, çip, mikro çip, mikro devre, entegre devre adıyla da bilinir[249].

CPU veya Merkezi İşlem Birimi, tüm talimatları yerine getiren, aritmetik, mantıksal ve temel giriş / çıkış işlemleri gerçekleştiren bilgisayarın beyni hükmündeki kısımdır. Bir Bilgisayar sisteminin hızını daha yüksek işlemci hızıyla performansın kademeli olarak artmasıdır. İşlemci hızı MHz (Mega Hertz) ve GHz (Giga Hertz), yani saniyede talimatların sayısı ile ölçülür[250].

Mikro işlemci, bilgisayarın giriş birimlerinde gelen veriler üzerinde mantıki işlem yapılması, yapılan işlemlerin denetlenmesi ve işlem sonucunun da geçici bir süreyle saklanmasını sağlar. Mikroişlemcinin ana görevi kayıtlı komut serileri olarak da adlandırılan programların yürütülmesini sağlamaktır. Program, bilgisayar belleğinde saklanan seri sayılar ile gösterilir. Mikro işlemciler, kod çözme (decode), yürütme (execute), işlemi getirme (fetch) ve geri yazma (writeback) olarak dört aşamada işlemi gerçekleştirir[251].



CPU (Central Processing Unit)

[249] Murat Volkan Dülger, **Bilişim Suçları,** Seçkin Yayıncılık, Ankara, 2004, s. 39
[250] Information Q, **CPU (Central Processing Unit) Computer processors and its Work,** 2016, Erişim Tarihi: 28. 11.2017 https://www.informationq.com/central-processing-unit/
[251] M.V. Dülger, 2004, s. 39

Şekil 1. Mikroişlemci ve bölümleri[252]

Mikro işlemci denetim birimi, yazmaç, matematiksel yardımcı işlemci, komut besleme birimi, dahili ön bellek, adres yolu ve veri yolu denetleyicilerinden oluşmaktadır. Denetim birimi gerçek komutları işletir; yazmaç komut biriminin doğrudan bağlandığı bellek birimleridir. Matematiksel yardımcı işlemci trigonometri ve logaritmik fonksiyonların yapılmasını sağlar; komut besleme birimi komutları sıraya sokarak komut birimine gönderir, dahili ön bellek sık kullanılan komutların tutulmasını sağlar; adres yolu ile veri yolu deneticileri ise dış dünya ile bağlantıyı sağlayan alanlardır[253].

CPU, bir programın tüm işlemlerini ve işlevlerini yerine getiren bir bilgisayarın vazgeçilmez bir parçasıdır. Her komutun yürütmeden önce geçmesi gerektiği için işlemci olarak adlandırılmıştır. İşlemcinin hızı, saniyede talimat sayısını gerçekleştirmek için hızın saat frekansına bağlıdır. Talimatlara göre herhangi bir giriş veya çıkış cihazı okunur, yürütülür ve monitör ekranında görüntülenir. Bilgisayarların CPU kelime boyutu 8, 16, 32, 64 ve 128 bit'dir. CPU mikro işlemciler, Anakart üzerinde bulunan yuvalarına yerleştirilen CPU'nun performansı RAM boyutuna, veri yolu hızına ve ön bellek boyuta bağlıdır. Çalışma performansına göre soğutucu veya fan ile soğutulması gerekir[254].

2. Dahili Bellek (İnternal Memory Storage)

Dahili belleği; rastgele erişimli bellek (random access memory-RAM), salt okunur bellek (read only memory- ROM) ve veri depolama hafızası (disk space) olarak adlandırılan depolama alanları oluşturur.

---

[252] Information Q, 2016, CPU

[253] A. Caner Yenidünya, Olgun Değirmenci, **Mukayeseli Hukuk ve Türk Hukukunda Bilişim Suçları**, Legal Yayıncılık, İstanbul, 2003, s.22-23.

[254] Information Q, 2016, CPU.

a. RAM

Rastgele erişimli bellek, mikro işlemcili sistemlerin geçici veri deposudur. Bu donanım kısmı bilgisayarın ana hafızası veya birincil depo, yükleme, gösterme, uygulamaları yönlendirme ve veriler için üzerinde işlem yapılan çalışma alanıdır. Bu alan hem yazılabilir hem de okunabilir özelliğe sahiptir. Bu nedenle bilgisayar çalıştığı sürece çalışan ancak güç kesiminde üzerine yazılan ve depolanan bilgileri silen, erişimin ardışık olmadığı, rastgele düzenlendiği, bununla birlikte veri okuma hızının fazla olduğu bir bellek türüdür[255].

RAM'lar dinamik (DRAM) ve statik (SRAM) olmak üzere ikiye ayrılır. DRAM, transistör ve kapasitör içeren hücrelerden oluşur, anakart üzerinde daha az yer kaplar, depolanan bilgileri otomatik olarak saniyede binlerce kez yenileme özelliğine sahiptir. EDO DRAM (Extended Data Output Dynamic RAM), bellekten içerik okuma zamanını artırmak ve erişim yöntemini geliştirmek için kullanılan bir RAM çeşididir. SRAM, çok yönlü transistör içeren bellek hücrelerinden oluşur, güç sağlandığı müddetçe verileri korur, DRAM'dan daha pahalı ve bilgileri yenilemesi de gerekmemektedir. Cache memory adı verilen ön bellek çeşidi ise CPU ile RAM arasında yer alan çok yüksek hızda 2MB'a kadar veri depolama özelliği bulunan oldukça da pahalı bir bellek türüdür[256].

Bilgisayarların daha fazla performans göstermesi için RAM'ın kapasitesinin de büyük olması gerekir. Birden fazla program çalışırken, sistem yavaşlar ve aşırı sabit disk kullanımı meydana gelir. RAM yetersizliği sabit diskin daha fazla kullanılmasını ve aşırı çalışarak ses yapması (disk trashing) ve ısınmasına neden olur. Çalıştırılmak istenen program sahip olunan RAM'dan daha büyük boyutlarda ise belirli aralıklarla

[255] M.V. Dülger, 2004, s.40; A.C. Yenidünya ve O. Değirmenci, 2003, s.24.
[256] Information Q, 2017, **Computer Memory Overview,** Erişim Tarihi: 28.11.2017 https://www.informationq.com/computer-memory-overview/

sabit diskten transfer yapılması gerekir. Özellikle büyük bilgisayar oyunları, tasarım programlarında bu sorunlarla karşı karşıya kalınabilir[257].

Bilgisayarların işlem yapma sırasında program kodları ve veri tutmak için RAM belleği kullanılır. Bu bellekteki bilgilere uçucu bilgiler de denilir. RAM verileri sayesinde bilgisayarın bir ağa veya internete bağlandığı internet protokol adresi, bağlandığı diğer bilgisayarlar ve bağlantı kapıları belirlenebilir[258]. Ayrıca, bilgisayarın ne kadar süredir açık olduğu, işletim sisteminin kurulma tarihi, zamanı, kayıtlı sahibi de tespit edilebilir. Bu nedenle bilgisayarın elektrik gücü kesildiğinde RAM'daki bilgiler kurtarılamayacağından dijital delil arama el koyma işlemi sırasında bu bilgilerin ekran görüntülerinin alınması, bilgisayarın ne kadar zamandır açık olduğu, geçerli kullanıcı bilgileri, başka bilgisayarlarla bağlantı olup olmadığının tespit edilmesi ve gerekli kopyalama işleminin yapılması önem arz etmektedir.

[257] Bilişim Dergisi, **Bellek Seçimi,** 2014, Erişim Tarihi: 28.11.2017, https://bilisimdergisi.wordpress.com/2014/01/27/bellek-secimi/#more-291

[258] Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku,** Ankara, Seçkin Yayıncılık, Kasım 2013, s. 680.

b. ROM

Salt okunur bellek, bilgisayarın ilk açılışında işletim sisteminin çalışması için gerekli komutların verilmesini ve çalıştırılmasını sağlayan yazılımın yüklü olduğu bellektir. Bilgisayarların fonksiyonları için ihtiyaç duyulan ve içeriği değiştirilemeyen, sadece okunabilen verilerin depolandığı bellek türüdür. Bilgisayara gelen güç kesilse bile ROM etkilenmez ve veri kaybı oluşmaz. ROM, bilgisayar açıldığında veya "reset"lendiğinde işletim sistemini sabit diskten RAM'a yüklemeyi düzenleyen BIOS (Basic Input/Output System- temel giriş çıkış sistemi)" adı verilen özel bir program içerir. BIOS bilgisayarla kullanıcı arasında bilgi alışverişini sağlayan kısımdır. Örneğin, ROM'da bulunan programlar sayesinde klavye üzerindeki harflere basıldığında ekranda basılan harf çıkar. Aksi durumda her harf için bir komut yazılması gerekir[259].

BIOS, üretim sırasında programlanır daha sonra yeniden yazılamaz. ROM'ları yapısına göre 4'e ayırabiliriz. PROM, boş olarak üretilen ve son test sırasında bir kereliğine programlanabilen ROM'lardır.

Programmable ROM (PROM)'lar video oyun konsolları, cep telefonları, implante edilebilir tıbbi cihazlar ve yüksek tanımlı multimedya arayüzlerinde bulunmaktadır.

Erasable Programmable ROM (EPROM), PROM'a benzer, ancak güçlü ultraviyole ışığa maruz bırakıldığında silinebilir, sonra yeniden yazılabilir. Bu yüzden, Ultraviyole Değiştirilebilir Programlanabilir ROM (UV EPROM) olarak da bilinir.

[259] A.C. Yenidünya ve O. Değirmenci, 2003, s.23-24; M.V. Dülger, 2004, s. 40.

Electrically Erasable Programmable ROM (EEPROM); EPROM'a benzer, ancak elektrikle silinebilir, daha sonra elektriksel olarak yeniden yazılabilir ve yanma işlemi elektrik darbelerine maruz bırakılarak geri döndürülebilir[260].

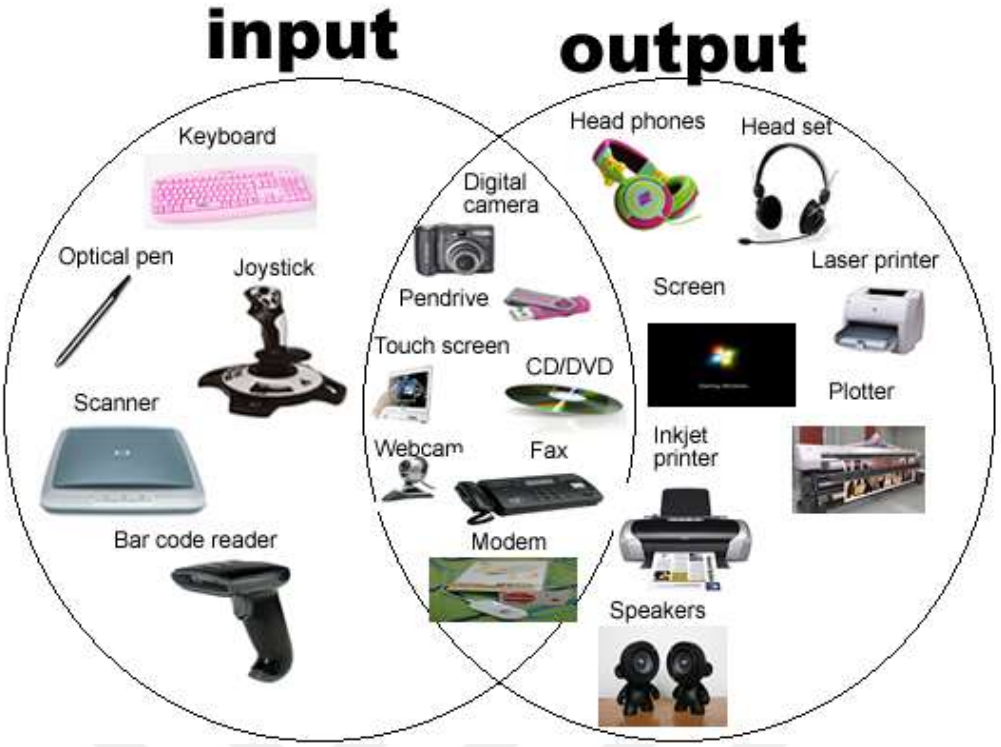
*MPROM (masceble programmable read only memory-maske programlı ROM)*özel bir programın ya da verinin maskelenmesi maksadıyla üretici tarafından programlanan bir ROM çeşididir[261].

Şekil 2. Bilgisayarlardaki Salt Okunur Bellek (ROM), EPROM ve EEPROM[262]

c. Çevre Giriş-Çıkış Birimleri

Çevre giriş- çıkış birimleri; klavye, fare, disket sürücü, CD-ROM sürücü, tarayıcı, kamera gibi cihazlardan oluşur. Bu birimler bilgisayar teknolojinin gelişmesine bağlı olarak doğru orantılı bir şekilde değişiklik gösterir[263]. Klavye ve fare sadece veri girişi sağlarken, disket sürücü, CD-ROM sürücü, tarayıcılar, kameralar, sabit disk, eksternal diskler gibi aygıtlarla hem veri girişi hem de veri çıkışı yapılabilir. Yazıcı ise sadece veri çıkışının yapıldığı bir unsur olup işlenen verilerin sonuçlarının fiziksel belgeye dönüştürüldüğü aletlerdir.

[260] Information Q, 2017
[261] Bilişim Dergisi, **ROM Bellek ve Çeşitleri,** 2014, Erişim Tarihi: 28. 11.2017 https://bilisimdergisi.wordpress.com/2014/01/27/rom-bellek-ve-cesitleri/#more-285
[262] Bilişim Dergisi, ROM Bellek ve Çeşitleri, 2014.
[263] M.V. Dülger, 2004, s. 40; A.C. Yenidünya, O. Değirmenci, s. 25.



Şekil 3. Bilgisayar Giriş ve Çıkış Birimleri[264]

"Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı Taslağı"na göre giriş-çıkış birimleri; *"e) Çevre birimler: Bilgisayara bağlanabilen, veri saklayıcılarını, veri giriş araçlarını, veri çıkış araçlarını ve veri giriş çıkış araçlarını"* ifade etmektedir[265]. Bu araçların hem sayısı hem de teknolojik özellikleri gün geçtikçe giderek artmakta ve daha fonksiyonel hale gelmektedir. Dijital kameralar, tarayıcılar, yazıcılar, CD, DVD, Flash bellekler, harici diskler GİBİ bilgisayar giriş çıkış birimlerinin kendilerine has bir kapasitede bellekleri bulunmaktadır. Bilişim suçları açısından bu aygıtların ve özellikle bazı yazıcı ve tarayıcıların geriye dönük hafızalarının olduğu delil toplama sırasında unutulmamalıdır.

[264] Computer In-put and Out-put, Erişim Tarihi: 28.11.2017 https://www.thinglink.com/scene/787328284789571584

[265] "Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı Taslağı", 2006, 2/e bendi.

C. El Bilgisayarları

El bilgisayarları, normal bir bilgisayarın özelliklerinin hemen hemen çoğunluğunu taşıyan bilgisayarlardır. Taşınabilir bilgisayarlara göre her ortamda rahatlıkla bulundurulabilmesi, avuç içine sığabilecek büyüklükte olmaları tercih sebepleri arasındadır. Bu bilgisayarlar internete erişimlerinin olması halinde çeşitli ofis programlarını çalıştırabilir, adres ve telefon bilgileri, ajanda, internet erişim kayıtları ve silinmiş verileri içerebilir[266].

Şekil 4. El Bilgisayarı[267]

El bilgisayarları donanım olarak 4,8 inç büyüklüğünde dokunmatik ekranlı, Atom işlemcili, 3G, webcam, 8 GB dahili hafıza gibi özellikleri vardır. USB girişi olmayan bu bilgisayarların, sesli görüşmeyi de desteklemeyebilir[268]. El bilgisayarları, cep bilgisayarı ve PDA (Personal Data Assistant) ismi ile de anılmaktadır. Bu cihazlar ülkemizde 2009'lu yıllarda popülerleşmeye başlasa da günümüzde akıllı telefonların teknik özelliklerinin artması PDA kullanımını oldukça sınırlamış durumdadır. PDA'lar ile, kelime işlem (Word), hesap tablolama (Excel), powerpoint sunularını görüntüleme,

[266] M.V. Dülger, 2013, s.682.
[267] Ücretsiz Bilgisayar Dergisi, 2010, Erişim Tarihi: 28. 11.2017, http://pdfdergi.com/4840/her-ele-bir-bilgisayar/
[268] Ücretsiz Bilgisayar Dergisi, 2010.

internete girme, e-posta alma ve gönderme, anında mesajlaşma, multimedya fonksiyonları (Müzik çalma, video görüntüleme) PIM fonksiyonları (Takvim, adres defteri, yapılacaklar listesi, notlar, harcamalar vs), hesap makinesi, saat, alarmlar, ses kaydı, kamerası olan modellerde fotoğraf çekme ve video kaydı, telefon özelliği varsa telefon görüşmeleri, SMS ve MMS gibi fonksiyonları yerine getirmektedir[269]. Günümüzde bu cihazlar daha çok cep telefonları ile bütünleştirilerek "akıllı telefon" adı verilen cihazlarla hayatımıza girmiştir[270].

Adli bilişim açısından değerlendirildiğinde PDA'lar bir bilgisayarda yapılan işlemlerin neredeyse hepsi yapılabildiğinden dijital delillerin aranması açısından önemli bir aygıttır. Ayrıca normal bilgisayara bağlanarak veri giriş çıkışı yapılabilme özelliği nedeniyle bilgisayarlara yapılan işlemlerin aynısının PDA'lara da yapılması unutulmamalıdır. Bellekleri, batarya ile muhafaza edilen bu aletlerin batarya ömürlerinin azlığı dijital delillerin kaybolmasına neden olabilir. Bu nedenle delilleri toplayan veya inceleyen personelin bu konuda dikkatli olması gerekir.

D. Dijital Verilerin Depolandığı Cihazlar

Bilgisayar ve diğer elektronik aygıtlar arasında veri transferi yapmak ya da depolamak maksadıyla hafıza kartı, CD-ROM, DVD-ROM ve USB bellek gibi çeşitli taşınabilir aygıtlar bulunmaktadır. Bunların dışında kullanım amacı başka olmasına rağmen yine dijital verilerin depolanmasına aracılık eden fotoğraf makineleri, video kameralar, taşınabilir müzik çalarlar, fotokopi makineleri, faks, tarayıcı, yazıcı ve cep telefonları da adli bilişim açısından önem arz eden cihazlardır.

[269] PDA ne demek? 2007, Erişim Tarihi: 28.11.2017, http://mobilyazilar.blogspot.com.tr/2007/01/pda-ne-demek.html

[270] Eoghan Casey, Benjamin Turnbull, **Digital Evidence on Mobile Devices, Chapter 20,** In: Casey, Eoghan, "Digital Evidence and Computer Crime: Forensic Science, Computer and The Internet", London: Academic Press, 2011, Third Edition. p.1

Hafıza Kartı: Dijital aletlerin hemen hemen hepsinde ek bellek olarak kullanılan aygıtlardır. Hafıza kartları; memory stick, memory card, flash card, compact flash card, smart media card, smart media floppy, floppy disk adaptör gibi isimlerle de anılmaktadır. Hafıza kartlarının ana güç kaynağından ayrıldıktan sonra verileri kaybetmeme ve silinmiş verilerin geri getirilmesine imkan vermesi dijital delillerin aranması açısından önemli özelliğidir.

CD/DVD ve Blu-Ray: CD (Compact disk) ve DVD (Digital versalit disk) olarak adlandırılan materyaller elektrik, manyetik ve dijital verilerin depolanmasında kullanılmaktadır. 2000'li yılların başında ortaya çıkan mavi-mor lazer ışınları ile yazılıp okunabilen Blu-Ray'ler CD ve DVD'ye göre hem çok daha fazla veri depolama kapasitesine sahiptirler hem de verilerin çözünürlük kalitesi daha yüksektir. CD, DVD ve Blu-Ray'lerde yazma işleminden sonra veriler silinemez ve değiştirilemez, ancak bu materyaller RW uzantılı ise üzerine kayıt yapıldıktan sonra tekrar değişiklikler yapılabilmektedir. Bu açıdan dijital delil olarak toplanan delillerin tekrar yazılabilen olup olmadıklarının belirlenmesi ve orijinalliklerinin belirlenmesi açısından delil değerini değiştirebilmektedir. Ayrıca, iddia edilen tarihlerde ilgili kişilerin kullandığı her türlü bilgi depolama medyası, CD ve DVD'nin içeriklerindeki dokümanların hazırlandığı kaynak sistem, el yazısı, parmak izi, seri numarası, üretici bilgisi, yazma hızı gibi fiziksel özellikleri delilin ispatlanması açısından önem arz etmektedir[271].

Taşınabilir Bellek: Günümüz teknolojisinde birbirinden farklı çeşitleri bulunan taşınabilir bellekler aslında hafıza kartlarının şekil değiştirmiş türleridir.En kapsamlı hafıza alanlarına sahip olan taşınabilir bellek harici (eksternal) disklerdir. Bu disklerin küçültülmüş formları olan USB bellekler, kolay taşınmaları ve veri aktarımında kolaylık sağlaması, yazılıp siline bilmesi nedeniyle birçok alanda kullanılan belleklerdendir. Dış görünüşleri açısından çeşitli şekillere sokulabilen bu bellekler özellikle usulsüz veri

[271] E. Casey, 2011, s, 220.

transferlerinin yapıldığı, illegal verilerin depolandığı belleklerden olması, bu cihazları önemli bir delil elde etme aracı haline getirmiştir. Özellikle üreticilerin USB'lere kalem, anahtarlık, bilezik, mandal, oyuncak, çakmak gibi (Şekil 5) birçok obje görüntüsü vermesi hem satılabilirliğini hem de gizlenebilirliği artırmaktadır. Adli bilişim açısından arama ve el koymalarda şüphelinin bulunduğu alanlardaki hemen hemen her materyali bu açıdan kontrol edilmesi dijital delilin ele geçirilmesine aracılık edecektir. Bu nedenle personelin USB bellek çeşitleri açısından bilgilendirilmesi önemli bir durumdur.

USB, İngilizce Universal Serial Bus (evrensel seri veriyolu) kelimelerinin kısaltmasıdır. USB bellekler, girişine uyumlu cihazlara ya da ara bağlantı yollarıyla bilgisayar, televizyon, kamera, cep telefonu gibi aletlere bağlanabilmektedir. Bağlandığı cihaz tarafından tanınan USB'ler üzerinden veri giriş çıkışı yapılabilmektedir. USB'lerin veri taşıma kapasitesi, üretiminde tanımlanan kapasitesine bağlıdır. İlk çıktığı yıllarda çift rakamlı MB'lara sahip olan USB'ler şimdilerde üç rakamlı GB kapasite olacak şekilde üretilmektedir.

Şekil 5. USB Bellek Çeşitleri

Dijital Kamera, Fotoğraf Makinesi ve Mp3 Çalar:Dijital Kameralar ve fotoğraf makineleri, fotoğraf ve video görüntülerinin oluşturulması, düzenlenmesi ve

depolanmasını sağlayan elektronik cihazlardandır. Mp3 gibi müzik çalmaya yarayan aletlerin de kendilerine has bellekleri olması USB gibi kullanılmasına aracılık etmektedir. Bu cihazlardan diğer dijital aletlere bağlanarak veri transferi yapılabilmesi, ekternal hafıza kart girişlerinin olması ve cihazlardaki dosyaların kimliği, tarih ve zaman bilgilerinin bulunması potansiyel delil olmasına yol açmaktadır[272].

Yazıcı, Tarayıcı, Faks ve Fotokopi Makineleri:Bu cihazlarında kendilerine hasveri depolama alanları bulunmaktadır. Cihazların teknolojik özelliklerine göre son yazdırılan ya da daha fazla veriye doğrudan ulaşma şansı olabilmektedir. Bu nedenle yazıcı, tarayıcı, faks ve fotokopi makineleri de delil oluşturulabilecek veri alanlarıdır[273].

Cep Telefonları:Günümüz dünyasında dijital teknoloji çok hızlı gelişen bir döneme girmiştir. Bu teknolojik yeniliklerden en çok etkilenen aygıtlardan biri de cep telefonlarıdır. Son 10 yılda meydana gelen değişikliklerle cep telefonları da tıpkı bilgisayarlar gibi özellikler kazanmıştır. Özellikle PDA'ların gelinen noktada cep telefonlarına evrildiği söylenebilir[274]. Cep telefonlarının akıllı hale getirilmesi, dokunmatik ekran özelliğine sahip olması, bilgisayarlar, kameralar, fotoğraf makineleri, tarayıcılar, müzik çalarlar, ses kaydedici cihazlar vasıtasıyla yapılan işlemlerin yapılabilmesi kullanılabilirliğini artırmış durumdadır.

Cep telefonlarının kendine has bir işletim sistemi, dahili ve harici belleğinin olması, arama kayıtları, rehber bilgileri, mevcut veya silinmiş kısa mesajları, fotoğraf, video[275], ses dosyalarını içermesi, internet bağlantısı yapılabilmesi, ücretli ya da ücretsiz birçok uygulamanın indirilmesi ve kullanılabilmesi, uydu teknolojilerinden yararlanılarak kullanım alanlarının tespit edilebilmesi, özel programlarla dinlenebilir ve takip edilebilir olması bu cihazların dijital delil aranacak cihazlar arasında öncelikli hale

[272] M.V. Dülger, 2013, s. 681.
[273] M.V. Dülger, 2013, s.682.
[274] E. Casey and B. Turnbull, 2011, s.1
[275] M.V. Dülger, 2013, s.681.

gelmesine neden olmuştur. Özellikle internetten sosyal medya yazışmalarının, bankacılık ve alış-veriş işlemleri gibi faaliyetlerin cep telefonları ile yapılması suç çetelerinin veya suça meyilli insanların da istedikleri ortamda istedikleri saatte harekete geçmelerine yol açmaktadır. Bu nedenlerle günümüzde akıllı cep telefonlarında dijital delile rastlanma olasılığı bilgisayarlardan bile daha fazla olabileceği düşünülebilir.

E. Veri Depolama Cihazlarının *Hash* Değeri

İmajı alınan verilerin tek yönlü kriptografik özeti olarak da ifade edilen *"hash"*değerine dijital dosyaların parmak izi denilebilir. Donanım tabanlı imaj alma araçları imajı alınacak diske fiziksel olarak erişim yapar ve sabit disk üzerindeki dosya sistemlerine bağlı kalmaksızın imajını alır ve *hash* değerini hesaplar. *Hash* değerinin alınması (hashing) o veriyi temsil eden sayısal bir verinin matematiksel algoritmalar kullanılarak üretilmesidir[276].

İmaj alma işlemi sırasında kullanılan yazılımlar otomatik olarak 2 farklı *hash* ibaresi içeren metin belgesini elde ederler. Bu değerlerden "*acquisition hash*" dijital materyalin incelemeden önce, dijital delil inceleme cihazında yer alan doğrulama algoritmasıdır. "*Verify hash*" ise inceleme sonrasında dijital materyalin delil bütünlüğünün bozulmadığını gösterir. Bu değerleri belirlemek için kullanılan yazılımlardan MD5 *hash* değeri, 32 karakter uzunluğunda 0-9 ve a-f karakterlerinden oluşan bir değerdir (Örn, MD5: e8359ebbe97f3bae584c76971059c35b). SHA1 de yine aynı karakterlerden oluşur, ancak 40 karakter uzunluğundadır (Örn, SHA-1: 5dbd53e4e7b0f6b8dd19d084af57722da83018e9)[277].

[276] John Ashcroft, Deborah J. Daniels, Sarah V. Hart, **Forensic Examination of Digital Evidence: A Guide for Law Enforcement**, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, 2004, s. 40.
[277] Mehmet Serkan Kılıç, **Elektronik Deliller ve Yapısal Özellikleri**, Edit: Çakır H. ve Kılıç M.S., "Adli Bilişim ve Elektronik Deliller", Seçkin Yayıncılık, Ankara, 2014, s.139-155.

Hash değeri belli bir uzunluktaki şifreli özetin tek yönlü olmasıdır, bu nedenle eski haline çevrilmesi mümkün değildir. Yani, *hash* değeri alınmış bir belgeyi açarak tek bir nokta eklenmesi dahi tekrar *hash* değeri alınmasında durumunda aynı sonucu vermemesidir. Bunun sebebi, *hash* algoritmasında yapılan kodlama dosya veya diske özel ve tektir. Dijital cihazlardaki farklı uzunluktaki metni, yazıyı, mesajı ve diğer dokümanları belli teknik yöntemler kullanılarak matematiksel işlemden geçirme işlemi sonucunda bu verileri temsil kabiliyetinde yeni matematiksel ve alfabetik bir özet değer elde edilmiş olur[278].

Hash algoritmasının belirlenmesi açısından en fazla kullanılan standard 128 bit MD5 (Message-Digest algorithm 5) ve 160 bit SHA-1 (Secure Hash Algorithm)'dir[279]. Bunlardan MD5'in 2010 yılından itibaren güvensiz olduğu deklare edilmiş, bunun yerine SHA1, SHA2 ve en güvenli yeni standart SHA3157 algoritmalarının kullanılması önerilmiştir. Bu algoritmalarla yapılan değerlendirmeler hem verilerin kopyalandığı boş sabit disk hem de kopyası alınan orijinal sabit disk için ayrı ayrı hesaplatılmakta ve verilerin aynılık oranı raporlanmaktadır[280].

El koyma sırasında alınan *hash* değeri alınan dijital verilerin adli bilişim uzmanı tarafından analiz edilebilmesi için tutanaklarda yazan değerlerin doğru olup olmadığı kontrol edilmektedir. Orijinal disk ile imaj dosyalarının *hash* (özet) değerlerini gösteren algoritmanın farklılığı ikisinden birinde ya da her ikisi üzerinde de oynama yapıldığı anlamlarına gelebilir. Bu nedenle, *hash* değeri raporda belirtilerek bir nevi sanal mühür yapılarak dijital veriler koruma altına alınmış olur[281].

---

[278] Robyn Burrows, **Judicial Confusion and The Digital Drug Dog Sniff: Pragmatic Solutions Permitting Warrantless Hashing of Known Illegal Files,** George Manson Law Review, 2011, 19,1, s.261.

[279] Türkay Henkoğlu, **Adli Bilişim Dijital Delillerin Analizi**, 1. Bası Pusula Yayınları, İstanbul 2011, s.55.

[280] "The Secure Hash Algorithm Directory MD5, SHA-1 and HMAC Resources", Erişim Tarihi: 28. 11.2017, http://www.secure-hash-algorithm-md5-sha-1.co.uk/

[281] Y. Şimşek ve diğerleri, 2012, s. 79-80.

Dosya üzerinde en ufak bir değişiklik yapılması durumunda *hash* değeri baştan sona değiştiği için dijital delil olarak yedeklenen verilerin bütünlüğü açısından önemli bir kriterdir[282].Ancak, verilerin orijinal olup olmaması açısından tek başına yeterli değildir. *Hash* değeri, delillerin kopyalanmasından sonra delil olarak sunulurken analiz edilen kopyanın orijinali ile arasındaki farklılığın belirlenmesi için kullanılır. Analizler sırasında veriye ilişkin *hash* değerinin değişmemiş olması verinin orijinal olduğunu gösterse de, *hash* değerinin değişmiş olması orijinal olmadığı anlamına da gelmeyebilir[283]. *Hash* değerinde meydana gelen değişiklikler depolama aygıtında meydana gelen mekanik bozulmalardan, RAM arızasından, bozuk sektörlerden, kullanılan yazılımdan kaynaklanabilir. Zira, herhangi bir değişiklik yapılmasa bile farklı zamanlarda alınan *hash* değerlerinin birbirinden farklı çıkabildiği de görülmektedir[284]. *Hash* değerinin kesin delil olarak görülmemesi, CMK'da yer almaması, Yargıtay'ın bir kararında *hash* değeri alınmamış olsa bile dijital delillerden elde edilen belgelerin delil olacağını kabul ederek mahkûmiyete esas alınmasını hukuka uygun bulmasına yol açmıştır[285].

Hash değeri zorunlu olmasa da yine de şüphelinin bilgisayarından delillerin alındığı sırada işlemi yapan görevli, bilgisayarın hard diskine el koyacağı zaman öncelikle *hash* değerini alması ve tutanak ile bunu güvenli hale getirmesi gerekir. Aksi taktirde veriler daha sonradan kolaylıkla değiştirilerek şüphelinin aleyhine deliller ortaya çıkartılabilir. Bu nedenle şüpheli ya da avukatının yanında bu işlemin yapılması doğrunun ortaya çıkartılmasında önemli bir adım olacaktır. CMK 134. Madde ele geçirilen verilerin kağıda dökülmesi verilerin güvenliği açısından zorunlu gösterilse de çok büyük dosyalardan ibaret olan ve fiziksel kağıda dökmesi mümkün olmayan bir

[282] M. Özen, G. Özocak, 2015, s.50.
[283] M. Kızılyar, 2014, s.86.
[284] E. Gökşen, 2014, s.27.
[285] Bkz. Yargıtay Kararı, "9. C.D.'nin 10.09.2012 tarihli ve 3282/ 8981 sayılı"

istektir. Bu nedenle elektronik delillerin nasıl toplanacağı yeniden düzenlenmeli ve *hash* değeri alınması gibi teknik zorunluluklar yasada yer almalıdır[286].

F. İnternet Sistemleri

Kişisel bilgisayarların üretiminden itibaren günlük hayatımıza giren bilgisayarlı sistemler internetin ortaya çıkmasıyla birlikte farklı bir boyut kazanmıştır. Başlangıçta sadece verileri depolama ve bazı günlük rutin işlemlerin yapıldığı bilgisayarlar internetin tüm dünya üzerinde önemli bir ağ kurması ile hem dünyanın her tarafındaki insanlarla iletişim kurulmasına hem de ihtiyaç duyulan bilgiye daha hızlı ve çok fazla çaba sarf etmeden ulaşmaya neden olmuştur. Günümüzde akıllı telefonlar, tablet bilgisayarlar ve özellikle sosyal medya platformlarının yaygınlaşması ve internete daha kolay ulaşım imkanının sağlanması günümüzün önemli bir kısmını bu aletlerin başında geçirmemize yol açmıştır. Bu kadar fazla kullanımı olan aletlerin internet ağları sayesinde etkileşimli veri aktarımına aracılık etmesi dijital delillerin toplanmasında da önemli arama noktaları haline getirmiştir.

1. İnternetin Tarihi Gelişimi

1957 yılında Rusya'nın Sputnik uydusunu uzaya göndermesi ABD Savunma Bakanlığı'nın ulusal güvenlik gerekçesiyle sadece tek bir bilgisayardan ağ oluşturma fikri, "Advanced Research Project Agency (ARPA)" adı altında bir birimin oluşturulmasını sağlamıştır. ARPA'nın esas kurulma amacı, haberleşme sistemlerinin kullanılamaz hale getirilmesi durumunda ulusal komuta merkezi olan Başkanlık'tan balistik füze üslerinin çalışmasını sağlayan emirlelri vererk savaşı başlataıp sevki sağlayan iletişim sistemi kurulmasıdır. Daha sonraki süreçte farklı sistemleri birbirine bağlamak için "ARPANET" adlı bir askeri bilgisayar kurularak silahlı kuvvetler, savunma sanayii müteahhitleri ve savunma konuları ile ilgili araştırmalarda bulunan

[286] M. Özen, G. Özocak, 2015, ss.68-70.

üniversitelerin bilgisayar merkezleri arasına bilgi alış verişini yapacak bir ağ (network) kurulmuştur[287].

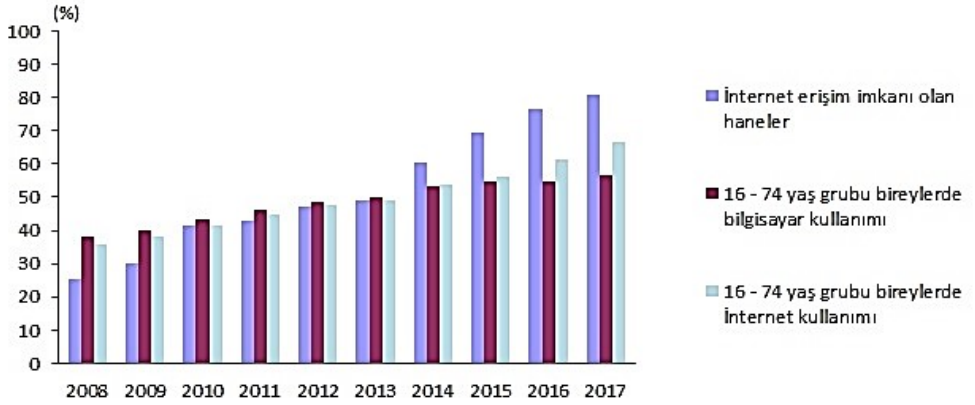
1968–1984 tarihleri gelişmiş ülkelerin ARPANET adı verilen bu ağa akademik olarak da olsa dahil olması internetin bulunuşunu hızlandırmış bu dönemde internet sadece üniversiteler, askeri ve devletin diğer üst düzey kuruluşları arasında kullanıma sunulmuştur. World Wide Web (www) internet ağının temelleri 1980'in sonlarında atılmıştır. İnternet, INTERnational ve NETwork kelimelerinin birleşiminden oluşan dünyadaki bilgisayar ağlarını birbirine bağlayan ağ olarak tanımlanmıştır. 1990 yılının başlarında kamuoyuna açılan internette grafik tabanlı tarayıcı kullanıma sunulmuş, 1995 yılından itibaren de hızla yayılmıştır. 1993 – 1995 yılları arasında internetin tamamen ticari alana açıldığı söylenebilir[288]. Türkiye'de ise ilk internet bağlantısı 12 Nisan 1993 tarihinde Türkiye Bilimsel ve Teknik Araştırma Kurumu (TÜBİTAK) destekli bir proje kapsamında "Orta Doğu Teknik Üniversitesi (ODTÜ)" tarafından gerçekleştirilmiştir[289].

İnternet, tarihi gelişim açısından diğer teknolojilere göre çok hızlı bir şekilde geliştirilmiş, halka açılmasıyla birlikte 50 milyon kullanıcıya ulaşması ancak 4 yılı almıştır. "Global Web İndex" verilerine göre 2015 yılına göre 2016 yılında %10'luk bir artışla 354 milyon kişi interneti kullanmaya başlamıştır. 2016 yılı internet kullanıcı sayısı dünya nüfusunun yarısından fazla, internete bağlanan kişi sayısı 3.77 milyar, sosyal medyayı kullanan kişi 2.80 milyar, mobil cihaz kullan kişi sayısı 4.92 milyar, mobil sosyal medya kullanıcı sayısı 2.56 milyar olarak belirlenmiştir. Mobil kullanıcısı sayısının da her yıl artış gösterdiği ve 2016 yılında %5 (22 milyon)'lik bir artışla Dünya

[287] B. Z. Avşar, G. Öngören, 2010, s.30.
[288] Peter Sommer, Ian Brown, **Reducing Systemic Cybersecurity Risk, OECD Multi-Diciplinary**, Erişim Tarihi: 29.11.2017, Issues International Futures Program, 2011, www.oecd.org/dataoecd/57/44/46889922.pdf, s.17.
[289] Şaban Cankat Taşkın, **Bilişim Suçları**, İstanbul: Beta Yayıncılık, Kasım 2008, s. 14.

nüfusunun neredeyse 2/3'nün mobil cihaz kullandığı ve hayatımızın bir parçası haline geldiği görülmektedir[290].

TÜİK'in 2017 "Hanehalkı Bilişim Teknolojileri Kullanım Araştırması"nda her on haneden sekizinin internet erişimine sahip olduğu, internet kullanım oranının %66,8; bilgisayar ve internet kullanımı oranı 16-74 yaş grubundaki bireylerde sırasıyla %56,6 ve %66,8 olarak belirlenmiştir. Nisan 2017 verilerine göre bu kullanıcılardan %80,7'sinin evden internete erişim yaptığı, hanelerin %40'ının ADSL, kablolu İnternet, fiber vb. ile %72,4'ünün ise mobil bağlantı ile internete erişim sağladığı tespit edilmiştir[291].



Şekil 6. Hanelerde ve bireylerdeki bilgisayar kullanımı ve internet erişim oranları[292]

Günümüzde "Kablosuz bağlantı" ya da "Wi-Fi" en çok kullandığımız internet bağlantı teknolojisi haline gelmiştir. Kablosuz ağlar, mobil araçların birbiri ile bağlantı oluşturmasını ve kullanıcıların sinyal aldığı her yerde özgürce işlem yapmasını sağlamaktadır. Bu teknoloji günümüzde her türlü bilgisayar, cep telefonu, televizyon ve diğer gelişmiş teknolojik aletlerde kullanılabilir hale getirilmiştir. Web teknoloji ile internetten sınırsız bilgiye eşirim imkanı bulan kullanıcılar anlık mesaj programları,

[290] Simon Kemp, **Digital in 2017: Global Overview.** Erişim Tarihi: 29.11.2017, https://wearesocial.com/blog/2017/01/digital-in-2017-global-overview.
[291] TÜİK. **Hanehalkı Bilişim Teknolojileri Kullanım Araştırması,** 2017, Sayı: 24862, 18 Ağustos 2017. Erişim Tarihi: 29.11.2017. http://www.tuik.gov.tr/HbPrint.do?id=24862
[292] TÜİK, 2017.

bloglar, e-posta sunucuları, sosyal medya platformları ile vakit geçirmektedirler. İnternetin bu kadar yaygınlaşması ve hayatımızda birçok şeyi kolaylaştırmasının yanı sıra bazen de içinden çıkılamaz ve hayatımızı alt üst edecek sorunlara neden olabileceğini unutmamak gerekir. Örneğin, internet ortamında paylaşılan bir yazıya öfkelenip yapılan bir yorum yargılanmaya sebep olabileceği gibi, kişisel bilgisayarda saklanan özel görüntülerin ele geçirilmesi ve önemli bir proje sonuçlarının virüs ya da uzaktan bağlanarak bilgisayarımızdan alınması mümkün olan sorunlardır. Bilgisayar korsanlarının kredi kartı bilgilerinin, banka hesaplarının, sosyal medya hesaplarının ele geçirilmesi ise günümüz şartlarında insanın hayatını karartacak bir durumdur. İnternet ortamının sınırsızlığı, bilgi alış verişi, veri transferlerinin çok kısa zaman içerisinde dünyanın bir diğer ucuna aktarılması, internet bağlantısının ortak (wi-fi) ile sağlanması ve daha birçok bilişim alanında yapılabilecek işlemler internet sunucularının, internet kullanıcı hesaplarının dijital deliller açısından değerlendirilmesini zorunlu hale getirmiştir.

2. İnternetin Teknik Yapısı

Internet her biri kendi içinde bağımsız yönetilen, denetlenen otonom ağlardan oluşmuştur. Bu açıdan bakıldığında, tek tek denetlenebilen ancak global anlamda idaresi ve kontrolünün tam olarak gerçekleşmemesidir. İnternete bağlı bilgisayarlar kendileri bağımsız bir şekilde çalışırken diğer taraftan diğer sistemlerle iletişim kurabilmektedir. Bu arada sistemde kaç tane bilgisayar olduğu, çalışıp çalışmadığı, internete bağlanıp bağlanmadığı ise bilinememektedir[293].

Teknik açıdan incelemek gerekirse internet, bilgisayarların birbirine bağlanarak oluşturdukları ağdır. Bu ağ içerisinde bulunan bilgisayarların birbirleriyle haberleşmesi ve veri transferini yapabilmesi ancak TCP/IP (Transmission Control Protocol/İnternet

[293] B. Z. Avşar, G. Öngören, 2010, ss.29-30

Protocol) protokolü adı verilen ortak bir dil ve kurallar bütünüyle gerçekleşebilmektedir[294]. TCP mesajların doğru yere ulaştırılmasını sağlarken, IP ise adresleme sisteminden yani kullanıcının coğrafi konumunun belirlenmesinden sorumludur. TCP'lere örnek verilecek olursa, internet üzerinden dosya alma/gönderme protokolü "FTP, File Transfer Protocol", elektronik posta iletişim protokolü "SMTP, Simple Mail Transfer Protocol", internet üzerindeki başka bir bilgisayarda etkileşimli çalışma için geliştirilen login protokolü "TELNET protokolü", WWW ortamında birbirine bağlanmış farklı türden objelerin iletilmesini sağlayan protokol "Hyper Text Transfer Protocol-http" olarak adlandırmaktadır[295].

İnternet Servis Sağlayıcısı internete bağlanılan her bilgisayara benzersiz bir IP adresi vermektedir. IP adresi, bir bilişim ağında ya da internette uç noktalara tahsis edilen benzersiz bir kimlik numarasıdır. IP adresi, bilişim ağı üzerindeki cihazın tanımlanmasını ve cihazın coğrafi olarak yerinin bilinmesini belirleme fonksiyonuna sahiptir[296]. Hangi bilgisayarın hangi IP adresini kullandığı İnternet Servis Sağlayıcı kayıtlarında mevcut olduğu için adli işlemlerde bilişim cihazları sahip oldukları IP adresi kullanılarak takip edilebilir. IP adresi, IP v4 için 32 bit boyutunda ve noktalarla ayrılmış şekilde 0-255 aralığında değişen dört adet sekiz bitlik sayı ile gösterilir (örneğin 192.167.10.47). IP adresleri dinamik veya statik olabilmektedir. Statik IP kişiye ait olan bir IP adresi olup bilgisayara tanımlanır. Dinamik IP ise her internete bağlandığında sunucu tarafından atanır ve her defasında değişebilir. IP adreslerinin dağıtımı her ülkede belirli merkezlerce yapılmaktadır[297].

World Wide Web (www), birçok internet hizmetini birleştiren bir araçtır. Yazı, resim, ses, video, animasyon gibi pek çok veriyi etkileşimli olarak kullanılmasını

[294] P. Sommer, I. Brown, 2011, s.11-17
[295] B. Z. Avşar, G. Öngören, 2010, s.32-33.
[296] Eric Laykin, **Investigative Computer Forensics The Practical Guide for Lawyers, Accountants, Investigators, and Business Executives**, USA, 2013, s.43.
[297] Larry L Peterson, Bruce S. Davie, **Computer Networks a System Approach**, 5th Edition, USA, 2012, s.203.

sağlayan çoklu bir hiper ortam sistemidir. Bu veriler anacak bir web tarayıcı ile görüntülenebilmektedir. Web Browser (web tarayıcısı), internet üzerindeki tüm verilere ulaşmak için kullanılması gerek bir uygulamadır (Microsoft Internet Explorer, Mozilla, Firefox, Safari gibi...).

Domain Name, "DNS, Domain Name System/ alan adı sistemi", aslında bir TCP/IP protokolüdür. İnternete bağlanan bilgisayar ve bilgisayar sistemlerinin bir ismi vardır. DNS, 'host' olarak adlandırılan internete bağlı tüm birimlerin yerel olarak bir ağaç yapısı içinde gruplandırmasını sağlar. Her internet adresinin ilk kısmı domain'in network adresini, son kısmı ise makinenin (host) numarasını verir. İnternet adresleri sonunda her ülkeye göre bir adlandırma bulunur. Örneğin, "tr" Türkiye, "de" Almanya, "uk" İngiltere'yi gösterirken, DNS ve benzeri uygulamaları oluşturan ABD'nin internet adreslerinde özel bir takı kullanılmaz. Bununla birlikte ABD kuruluşları için "us" takısı da oluşturulmuştur. İnternet adresleri ülkelere göre ayrıldıktan sonra üst düzey alan adları "com", "edu", "gov" gibi daha alt bölümlere ayrılır. Ticari alanlar "com", eğitim kurumları "edu", hükümet kurumları "gov", ticari olmayan ve hükümete de bağlı olmayanlar "org", Internet omurgası görevi bulunanlar "net", askeri kurumlar "mil", telefon numaralarının bulunabileceği yerler "num", ters DNS sorgulaması yapılacak alanlar ise "arpa" ile gösterilmektedir[298].

İnternet servis sağlayıcı (Internet service provider- ISP); internet hizmetinin oluşturulduğu uluslararası ağın merkezinde birbirine bağlanmış, yüksek hızlı iletişim yapabilen bilgisayarlara verilen isimdir. İnternet servis sağlayıcılar kullanıcıların internete bağlanması, iletişim kurması ve diğer her türlü işlemin yapılmasını sağlayan internetin anahtarını elinde tutun süjelerdir[299].

[298] B. Z. Avşar, G. Öngören, 2010, s.33-36.
[299] A.C. Yenidünya, O. Değirmenci, 2003, s. 37.

İnternet süjeleri "Telefon/telekomünikasyon idareleri", "Sunucu", "Servis sağlayıcılar" ve "Kullanıcılar"dan oluşmaktadır.

İnternet bağlantıları telefon hatları üzerinden gerçekleşmektedir. Bu nedenle her ülkenin Telefon/telekomünikasyon idaresi bu hatların kontrolünden sorumludur. Hatları kiralayan İnternet Servis Sağlayıcıları bir sunucu (server) kullanmaktadır. Sunucu bir bilgisayar ya da program olabilir. Sunucunun ehemmiyeti yayınlanan verilere kaynaklık teşkil etmesidir. Özel veya tüzel kişiler servis sağlayıcı ile yaptığı anlaşma gereği bir sunucuda herhangi bir veriyi depolayabilmekte ve yayınlayabilmektedir. Internet Servis Sağlayıcı veya özel bir sunucunun, başkasına ait olan bilgiyi kendi bilgisayarında depolaması ve internette yayınlaması işlemine hosting olarak adlandırılır[300].

Karşılaştırmalı hukukta internet suçları açısından sağlayıcıların işlevlerine göre "İçerik sağlayıcı", "Servis Sağlayıcı" ve "Erişim Sağlayıcı" olması cezai sorumluluğu belirlemede önemli bir ayrıntıdır.

Internet Erişim Sağlayıcılar "Internet Access Provider – IAP"; başkasına ait içeriklere kullanıcıların erişimini sağlar. Verilerin depolanması erişim sağlayıcıya ait değildir.

Internet Servis Sağlayıcılar "Internet Service Provider- ISP"; İnternet'e bağlanmak isteyen kişilerin bu bağlantıda bir giriş kapısı olarak kullandıkları servis sağlayıcının bilgisayarlarıdır. Sahip oldukları internet bağlantısını ücret karşılığında kullandırırlar ayrıca yayınlanacak verileri kendi sunucularında da depolayabilme özelliğine sahiptirler.

Internet İçerik Sağlayıcılar "Internet Content Provider- ICP"; bir bilgi veya belgeyi üreterek internet ortamında yayınlanmasını düzenleyen kişi veya kuruluşlardır.

[300] Sevil Yıldız, "Suçta Araç Olarak İnternetin Teknik Ve Hukuki Yönden İncelenmesi", **Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 2007**, 17, ss.609-623.

Kullanıcılar ise internetten etkin bir şekilde faydalanan, yayınlanan bilgi ve belgeleri izleyen, okuyan ve kendi bilgisayarlarına yükleyen gerçek ya da tüzel kişiliklerdir[301].

İnternet ortamında ya da internet kullanılarak işlenen suçlar "Siber suçlar", "Dijital suçlar", "İnternet suçları", "Bilişim suçları", "İleri Teknoloji Suçları" gibi değerlendirme kriterine göre de değişebilen adlandırmalarla anılmaktadır. İnternet aracılığıyla işlenen suçlar mevcut ceza kanunlarında tanımlanmış klasikleşmiş suç çeşitlerindendir. (Sövme, hakaret, dolandırıcılık gibi.) Siber uzay ortamında işlenen bu suçlarda internet sadece bir aracı olduğu için ceza hukuku normlarına göre yapılır. İnternet ortamında işlenen suçlar ise özel teknikler kullanılarak başkasının bilgisayarındaki verilere zarar vermek bir web sitesinin işleyişini bozmak, yayını değiştirecek eylemler yapmak, yayını çalışamaz hale getirmek, bilgisayarı çalışamaz hale getirmek, virüs bulaştırmak gibi eylemlerdir[302].

[301] Hasan Sınar, **İnternet ve Ceza Hukuku**, İstanbul, Beta Yayınları, 2001, s.41-43.
[302] S. Yıldız, 2007, s. 615-620.

ÜÇÜNCÜ BÖLÜM

CEZA MUHAKEMESİNDE DİJİTAL DELİLLERİN ELDE EDİLMESİ VE DEĞERLENDİRİLMESİ

I. DELİLLERİN ELDE EDİLMESİ VE DEĞERLENDİRİLMESİ

Ceza muhakemesi hukukunda yer alan delil serbestliği ilkesi[303] nedeniyle, yargıcın somut gerçeğe ulaşabilmek amacıyla her türlü delilden faydalanması gerekmektedir[304]. Başvurulacak olan delillerin birtakım özelliklerinin bulunması gerekmektedir. Ceza muhakemesinde deliller, vicdani delil sistemine göre yargıcın kanıt olarak gösterilen delillerin argümanlarının vakıayı gerçekten ispat etmeye yeterli olup olmadığına yönelik özgürce yaptığı değerlendirmeye göre kabul edilmektedir[305]. Bununla birlikte ceza muhakemesinde delil serbestisi prensibine tam olarak uyulduğu söylenemez. Ceza muhakemesi hukukunda öncelikle delillerin taşıması gereken birtakım özellikler bulunmaktadır. Ceza yargılamasında delillerin sahip olması gereken özellikler özetle şu şekilde sıralanabilir:[306]

"i) Deliller gerçekçi olmalıdır.

ii) Deliller akılcı olmalıdır.

iii) Deliller olayı temsil edici olmalıdır.

iv) Deliller sağlam ve güvenilir olmalıdır.

v) Deliller elde edilebilir olmalıdır.

vi) Deliller ispat bakımından önemli olmalıdır.

vii) Deliller kanuna (hukuka) uygun olmalıdır"

[303] Süheyl Donay, **Ceza Yargılama Hukuku**, İstanbul, Beta Yayınları, 2010, s.54.
[304] Sedat Bakıcı, **Olaydan Kesin Hükme Kadar Ceza Yargılaması ve Ceza Kanunu Genel Hükümler**, Ankara, Adalet Yayınevi, 2000, s.226.
[305] N. Toroslu, M. Feyzioğlu, 2009, s.177.
[306] N. Kunter ve diğerleri, 2010, ss.1328-1329.

Mevzuat incelendiğinde hukuka aykırı delilin tanımın yapılmadığı görülmektedir. Bu konu ile ilgili değişik kavramlar görülmektedir. *Anayasa'nın 38/6 maddesinde* "kanuna aykırı olarak elde edilmiş bulgular", *5271 sayılı Ceza Muhakemesi Kanunu'nun(CMK) 206/2. maddesinde* "kanuna aykırı olarak elde edilmiş delil", *230/1 maddesinde* ise, "hukuka aykırı yöntemlerle elde edilen deliller" terimleri kullanılmaktadır. CMK'nın 288. maddesinde hukuka aykırılık, "bir hukuk kuralının uygulanmaması veya yanlış uygulanması" şeklinde tanımlanarak temyiz nedenleri arasında görülmüştür.

Ceza muhakemesi kitapları incelendiğinde muhakame etmenin amacının somut gerçeğe ulaşmak olduğu yazılıdır[307]; ancak hukuk devleti ilkesinin gelişmesi, uluslararası anlaşmalar sonucunda ülkelerin egemenlik alanlarının[308] azalması dikkate alındığı zaman somut gerçeğe her ne koşulda olursa olsun ulaşılamayacağı da anlaşılmış ve ceza muhakemesinde özellikle insanların temel hak ve hürriyetlerini koruyan delil serbestliği ilkesine kısıtlamalar getirilmiştir[309].

Delile ulaşma konusunda getirilen kısıtlamalara delil elde etme yasağı, söz konusu delillerin hüküm sırasında ele alınması ise delil değerlendirme yasağı olarak adlandırılmaktadır[310]. Yargıtay'ın sıklıkla karşılaştığı temyiz taleplerinin çoğu, hukuka uygun olmayan biçimde toplanan delillere dayandırılarak mamhkumiyet verildiği gerekçesiyle yerel mahkeme kararlarına karşı kanuni yollara müracaat edildiği gözlemlenmektedir.

Delillerin elde edilmesinde uygulanacak prosedür ile ilgili kurallar şu şekilde belirtilmektedir. Bunlar;

---

[307] Eralp Özgen, **Ceza Muhakemesinin Yenilenmesi**, Ankara, Ankara Üniversitesi Hukuk Fakültesi Yayınları, 1968, s.3.
[308] Yusuf Şevki Hakyemez, **Mutlak Monarşilerden Günümüz Egemenlik Kavramı**, Ankara, Seçkin Yayınevi, 2004, s.35.
[309] Erdener Yurtcan, **Yargıtay Kararları Işığında Hukuka Aykırı Delillere Dayanma Yasağı**, İstanbul Üniversitesi Hukuk Fakültesi, 1998, s.519.
[310] B. Öztürk, M.R. Erdem, 2006, s.249.

-İlk işlemin yapılmasının sağlanması,

-Elde edilen delillerin korunmasının sağlanması.

Bu nedenle delillerin elde edildiği noktalara giriş ve çıkışların kontrol altına alınması sağlanmalıdır. Dijital delilleri bilişim uzmanları elde etmek için uğraşmaktadırlar. Bu nedenle bilişim uzmanları olay yerine geldiğinde herkesin ortamdan uzaklaştırılması gerekmektedir. Bundan sonra yapılacak işlem olay yeri ile ilgili resimlerin çekilmesidir. Olay yerinde delil olarak nitelenen tüm materyale numara verilerek bu materyaller etiketlenmelidir. Olay yerinde eğer bir bilgisayar bulunuyorsa bu bilgisayar kapatılmadan önce çalışır halde iken sistemden hafızada olan delillerin elde edilmesi ve bu bilgilerin kayda geçirilmesi sağlanmaktadır. Olay yerinin de birçok açıdan fotoğrafı çekilmektedir.

Bilgisayar sisteminin bağlantı kablolarının ve bağlı bulunduğu portların fotoğraflanması sağlanmalı; bilgisayarın göstermiş olduğu tarih ve zaman bilgilerinin de kaydedilmesi gerekmektedir. Bu bilgiler not alınırken gerçek tarih/zaman bilgileri de beraber not alınmalıdır. Bilgisayar içinde bulunan veriler kaydedilirken bu yapılan işlemler görsel ve yazılı olarak kayda alınmalıdır. Bu da delillerin doğrululuğunu mahkeme süresince kabul ettirecektir. Bilgisayar içinde bilgileri taşıyan donanım parçaları üzerinde doğrudan çalışmak yerine imajının alınması gerekmektedir.

Olay yerinde delil bulmak için yapılan araştırmaların donanım üzerinde yapılmaması, alınan kopyalar üzerinde durulmamsı daha uygun olacaktır. Bu da dijital delillerin güvenliği için sağlanacak durumlardan birini oluşturmaktadır.

Adli bilişimde bire bir yapılan kopyalama işlerime imaj ya da imaj alma adı verilmektedir. Bu kopyalama yapılırken sistemdeki tüm veriler özel yazılım kullanılarak alınarak başka bir ortamda örneği alınıp incelemesi yapılmaktadır. Bu işlem yapılırken kullanılan en önemli husus imaj alma işlemi sırasında kopya edilecek sistemin hemen

çalıştırılmaması gerekmektedir. Bilgisayarın açıldıktan sonra işletim sisteminin çalışmasına ilintili olarak yeni bilgilerin işlenmesi nedeniyle önceki veriler kaybolabilir. Hangi tür aygıtın hangi donanım için kullanılacağının, hangi prosedürün izleneceğinin bilişim uzmanı tarafından iyi bilinmesi gerekmektedir[311].

Sanık ya da şüphelinin bulunduğu olay yerinde bir bilgisayar bulunuyorsa bu bilgisayara ilk müdahaleyi adli bilişim alanında uzman olan kişinin yapması gerekmektedir. Eğer bilinçsiz bir kişi müdahale ederse delillerin bütünlüğü bozulacak veya elde edilebilecek çok önemli bilgilerin elde edilememesi gibi bir sonuçla karşı karşıya kalınacaktır[312].

Bilgisayar ve bilgisayar depolama ortamlarının çok iyi bir şekilde incelenmesi gerekmektedir. Bilgisayar depolama ortamları ile ilgili olarak aşağıdaki unsurların bilinmesi sağlanmalıdır. Bunlar:

-Toplam kapasitenin belirlenmesi,

-Partition sayısı, kapasite ve dosya sistemi bilgilerinin tespit edilmesi,

-Kullanıcı bilgilerinin kayda alınması,

-İşletim sistemi kurulum tarihinin belirlenerek kayda alınması,

-Bilgisayarın son kullanım tarihinin belirlenerek kayda alınması sağlanmalıdır.

Adli bilişim uzmanının bilgisayarın içindeki tarih ve zaman ile gerçek tarih ve zamanı beraber not etmesi gerekmektedir. Eğer bir zaman farkı varsa hazırlayacağı raporda bu zaman farkına da işaret etmelidir[313].

---

[311] Emrah Duman, **Bilgisayarlarda ve Bilgisayar Ağlarında Delil Toplama ve Türkiye'deki Uygulama Sorunları**, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, 2012, s.38.
[312] Hüseyin Çakır, Ercan Sert, **Bilişim Suçları ve Delillendirme Süreci**, O. Ö. Demir ve M. Sever (Der.), Örgütlü Suçlar ve YeniTrendler, Ankara, Polis Akademisi Yayınları, 2011, s.167.
[313] Dave Garza, **Investigating Hard Disks, File and Operating Systems,** ABD, EC-Council Press, 2010, s.2-4.

Olay esnasındaki en önemli adımlar; kullanıcı bilgilerinin elde edilmesinin sağlanması, profilin çıkarılması olarak belirlenmektedir. Bunlar bu çalışma esnasında en çok zaman harcanan kısmı oluşturmaktadır[314].

Somut gerçeği ortaya çıkarmak, uyuşmazlık sonucu verilen hükümle verilen karara arasındaki tutarlılığı sağlamak ceza muhakmelerinin temel amacıdır. Özgen'e göre bu durum şöyledir: " *Ceza muhakemesinin amacı olan maddi gerçek ise aralarında bağ bulunan birkaç hakikatin ortaya çıkarılmasını gerekli kılar*." Buna göre hakikate ulaşmak için

"i) İddia edilen fiil işlenmiş midir?

ii) Bu fiil, kanunların öngördüğü ve ceza müeyyidesine bağladığı bir suç mudur?

iii) İşlendiği ve kanunen suç olduğu tespit edilen fiili iddia edilen şahıs mı işlemiştir?

iv) Bu fiili işlemiş olan şahıs sorumlu mudur?" sorularının yanıtlanması gerekir[315].

Temel amacın somut gerçeğe ulaşmak olduğu için, soruların doğru şekilde cevaplanması "her şeyin her şeyle ispat olunabileceği" neticesi ortaya çıkmaktadır[316]. Buna "delil serbestisi" adı verilmektedir. Medeni muhakemeden farklı olarak, ceza muhakemesinde "kanuni delil sistemi"nden değil, "vicdani delil sistemi"nden söz edilir[317].

Ceza Muhakemeleri Kanunun 206. maddesinde "Delillerin ortaya konulması ve reddi" 207. maddesi "Delil ve olayın geç bildirilmesi", 216. maddesi "Delillerin

[314] Markus K. Rogers, James Goldman, Rick Mislan, Timothy Wedge, Steve Debrota, **Computer Forensics Field Triage Process Model, Conference of Digital Forensics, Security and Law**, Las Vegas Nevada, 2006, s.34.
[315] E. Özgen, 1968, s.3
[316] Faruk Erem, **Ceza Usülü Hukuku**, Ankara, Ankara Üniversitesi Hukuk Fakültesi Yayınları, 1964, s.316.
[317] Mehmet Gödekli, **Terörizmin Finansmanı Suçu,** Atatürk Üniversitesi Yüksek Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, Erzurum, 2013, ss.177-178.

tartışılması", 217. maddesi "Delillerin takdir yetkisi" hakkındaki hükümleri içine almıştır.

Delillerin ortaya konulması Ceza Muhakemeleri Kanunu'nun 216. maddesinin 1. fıkrasında düzenlenmiştir. Sanığın sorguya çekilmesinden sonra, dellillerin sunulması gerekmektedir. Delil bir ispat aracı olarak görülmektedir.

Delillerin ileri sürülmesi; sanık veya şüpheli ile olay ile ilgili olan kişilerin gösterecekleri deliller haricinde olayın sorulması ve incelenmesi için hakim ve mahkeme tarafından ileri sürülen bütün deliller olarak ifade edilmektedir[318].

Deliller, mahkemeye katılan şahısların bir vakıayı daha sonra tekrar yaşayarak aktarmalarını sağlayan araçlardır[319].

Delillerin ortaya konulması, hazır bulunan delillerin muhakemeye katılan kişilerce kullanılmaya başlanmasıdır[320].

Vasıtasızlık ilkesi; muhakemenin ya da hakimin kararını delilerle doğrudan doğruya temasa geçilerek verilmesi olarak ifade edilmektedir. Kararı verecek olan mahkeme ya da hakim; delilleri sözlü olarak dinler, yazılı olarak okur ve bu delilleri kayda alır. Bunun sonucunda tanıklarda mahkemede hakim tarafından dinlenilir. Tanıkların önceki ifadelerinin yanında tekrar sözlü olarak mütalası istenir. Sanık daha önce sorgulansa bile, mahkeme salonunda sorgusunun yeniden yapılması gerekmektedir[321].

Ortaya konulmak istenen delilinin gerekçeli sebebi belirtilmelidir. Çünkü ortaya konuş sebebi açıklanmayan bir delilin ortaya konulmasının reddi ihtimali mevcuttur.

---

[318] Bkz. Yargıtay İçtihadı Birleştirme Kurulunun 09.10.1940 gün ve 1938/38-1940/79 Sayılı Kararı.
[319] Öztekin Tosun, **Türk Suç Muhakemesi Hukuku Dersleri, C.II, Muhakemenin Yürüyüşü,** İstanbul, 1976, s.739.
[320] Ö. Tosun, a.g.e., s.740.
[321] B. Öztürk, M.R. Erdem, 2006, s.374.

Bir delilin mahkeme tarafından dikkate alınması için bazı şartların sağlanması gerekmektedir. Bu şartlar;

-Delilin olayı temsil etmesi,

-Delilin akla ve maddi gerçeğe uygun olması,

-Delilin hukuka uygun olması gerekmektedir[322].

Bütün deliller toplandıktan sonra kamu davası açılması, mahkemenin delil toplamakla uğraşmaması, tarafların dosyada yer almayıp da dikkate alınmasını istedikleri delilleri danışmadan önce mahkemeye bildirmeleri gerekmektedir.

Fakat mahkeme önüne getirilmeyen bir delilin varlığını tespit edebilir veya bir konuda araştırmaya ihtiyaç duyabilmektedir. Ceza Muhakemeleri Kanunu'nun 217. maddesinde "duruşmaya getirilmiş" delillere dayanılmasından söz edilmesi de mahkemeye delil araştırmak yükümlülüğü yüklenmemesi gerektiğini göstermektedir. Fakat duruşmanın amacı gerçeğe ulaşmak olduğu için mahkemenin kendiliğinden delil toplaması mümkündür.

Öztürk'de mahkemenin ileri sürülen delillere bağlı olmadığını, kendiliğinden delil araştırabileceğini ifade etmiştir. Yaşar'da mahkemenin kendiliğinden duruşma aşamasında delil toplamasının mümkün olduğu görüşündedir. Özbek-Doğan ise bu hususun tartışmalı olduğunu CMUK'nun 214. maddesindeki hakime bu yetkiyi veren 214. maddesi hükmünün CMK'nda bulunmadığından hakimin kovuşturma evresinde tanık ve bilir kişi çağrısına yetkisinin olmadığının söylenebileceğini ifade etmişlerdir. İddianamenin iadesi kurumunun da bu sebeple kabul edildiği düşünülebilmektedir. Aynı eserin bir başka yerinde de CMK'nun getirdiği en önemli yenilikler doğrudan soru sormak imkanının geliştirilmiş olması ve hakimin resen delil toplama imkanlarının kısıtlanması olarak gösterilmiştir. Ancak aynı hukukçular, maddi gerçeğin araştırılması

[322] B. Öztürk, M.R. Erdem, 2006, s.375.

ilkesi de dikkate alınarak mahkemenin kendiliğinden (re'sen) delil araştırmasının kabul edilmesi gerektiği, yasaya bu konuda açık hüküm konulmasının yararlı olacağı görüşündedirler[323].

Ortaya konulması istenen bir delil CMK'nun 206. maddesinin 2. fıkrasına göre aşağıdaki hallerde ret edilmektedir. Bunlar;

-Deliller kanuna aykırı olarak elde edilmişse reddedilmektedirll

-Delillerin ispat edilmesi istenen olayla ilgisi yoksa deliller reddedilmektedir.

-Delillerin istemi davayı uzatmak için yapılmışsa deliller reddedilmektedir.

Delilin ortaya konulmasının reddi kararı ret gerekçesiyle birlikte duruşma tutanağına kaydedilmelidir. Bu şekilde hem davanın ilgilileri delilin ortaya konulmasının neden kabul edilmediğini öğrenmiş olmaktadırlar hem de temyiz incelemesinde bu reddin haklılığı red gerekçesi ile birlikte ele alınarak değerlendirilecektir[324].

Kanuna aykırı bir şekilde delil elde edilmişse delil hükme esas alınamaz. Hukuka aykırı delil elde edilmesi de bir suç oluşturmaktadır.

Kanuna aykırı şekilde bulunan delillerin kabul edilemeyeceği Anayasa'nın 38. maddesinde belirtilmiş ve hüküm altına alınmıştır. Eğer deliller hukuka aykırı yöntemlerle elde edilmişse bu delillerin de hukuka uygun şekilde elde edilmediği için delil olamayacağı CMK'nın 289. maddesi 1. fıkrası i bendinde belirtilmiştir.

Hukuka aykırı olarak delil elde edilişlerinin doğrudan ya da dolaylı olmasının hiçbir anlamı bulunmamaktadır. Dikkate alınması gereken nokta, delil veya delillere elde ulaşma esnasında hukuka uygun davranılıp davranılmadığıdır. İşkence ile alınan

[323] Veli Özer Özbek, **CMK İzmir Şerhi Ceza Muhakemesi Kanunun anlamı Açıklamalı Gerekçeli İçtihatlı,** Pegem Yayınları, 2002, ss.751-752, 806.
[324] Serap Keskin Kiziroğlu, "Ceza Muhakemesi Hukukunda Aykırı Deliller", **Güncel Hukuk Dergisi 2007**, s.32-35.

itiraf , sayede ulaşılan suç aleti ve başka önemli deliller hukuka aykırı şekilde elde edilmişse cceza muhakemelerinde kulanılamaları ve hükümde esasa aalınmaları olasılık dışıdır[325].

Her ne şşekilde olursa olsun gerçeğe ulaşmak reddedilmiştir[326].Herhangi bir temel hak ihmal edilmeksizin basit bir hukuku aykırılık ile delil elde edilmesi durumunda dahi bu delilin hükme esas alınmasının mümkün olamayacağını belirten Demirbaş'a göre; bu hüküm (CMUK: m.254/2) ceza adalet sistemi bakımından büyük sıkıntıların doğmasına neden olacaktır.

Hukuka aykırı şekilde toplanan delillere örnekler aşağıdaki gibi verilmektedir. Bunlar şu şekilde sıralanmaktadır;

-Deliller özel hayatın gizliliğini ihlal edecek şekilde toplanmışsa bu deliller hukuka aykırı olarak nitelenmektedir.

-Deliller insanlık ve onur kırıcı işkence ile elde edilmişse bu deliller hukuka aykırı olarak nitelenmektedir.

-Deliller ajan ve provokatör kullanılarak elde edilmişse bu deliller hukuka aykırı olarak nitelenmektedir.

-Duruşmaya gelmeyen, yazılı olarak sunulup, açıklanmayan tanık beyanları hukuka aykırı delil olarak kabul edilmektedir.

[325] Bahri Öztürk, "Yeni Ceza Muhakemesi Kanunu'nda Delil Yasakları", **Hukuki Perspektifler Dergisi 2005,** s.135.
[326] E. Yurtcan, 2005, s.460.

II. DİJİTAL DELİLLERİN ELDE EDİLMESİ VE DEĞERLENDİRİLMESİ

A. Ceza Muhakemesi Çerçevesinde Dijital Delillerin Kabul Edilebilirliği Meselesi

AİHM, Schenk v. İsviçre davasında, AİHS'nin, 6. Maddesi kapsamında "adil yargılanma hakkını" güvence altına alırken delillerin kabul edilebilirliğiyle ilgili bir düzenleme yapmamış, delillerin kabul edilebilirliğinin yerel mahkemelerin görevi olduğunu ifade etmiştir (par. 46)[327].

Ceza muhakemesinin temel amacı somut gerçeğe ulaşmak, uyuşmazlık sonucunda verilen hüküm ile işlenen eylem arasında tutarlılığın sağlanmasıdır. *Özgen*'e göre, ceza muhakemesi hakikate ulaşmak için; "*i) İddia edilen fiil işlenmiş midir? ii) Bu fiil, kanunların öngördüğü ve ceza müeyyidesine bağladığı bir suç mudur? iii) İşlendiği ve kanunen suç olduğu tespit edilen fiili iddia edilen şahıs mı işlemiştir? iv) Bu fiili işlemiş olan şahıs sorumlu mudur?"* sorularına yanıtlar bulmaktır[328].

Medeni muhakemeye göre ceza muhakemesi ilgili tarafların ileri sürdükleriyle bağımsız bir şekilde geçmişte ne olduğuyla ilgilenerek gerçek olan şeye ulaşmayı hedefler. Bu kapsamda maddi gerçekliğe ulaşmak için ceza muhakemesi kanunun delil yasakları sınırı dışındaki her şeyi delil olarak kabul etmektedir[329]. Ceza muhakemesinde delillerin kabul edilebilirliğinin sınırını elde edilen delilin hukuka aykırı yöntemlerle ele geçirilmemiş olmasıdır. Özellikle Anglo-Amerikan hukuk sisteminde yargılamalarda jürinin nihai kararı önemli bir yere sahip olduğundan gerçeğe aykırı ya da davada kullanılamayacak delillerin jüri karşısına çıkarılmamasına dikkat edilir. ABD Federal Delil Kuralları doğrultusunda elektronik delillerin hukuk yargılamasında kabul

[327] Mehmet Gödekli, "Türk Ceza Muhakemesinde Maddi Gerçeğe Ulaşmanın Ön Koşulu Olarak Hukuka Aykırı Delillerin Değerlendirilmesi Yasağı"**,Ankara Üni. Hukuk Fak. Dergisi 2016**, 65(4), s.1872.
[328] M. Gödekli, 2016, s. 1819
[329] G. Akyürek, 2012, s. 61.

edilebilir olabilmesi için "ilgililik", "önemli olma", "doğrulama" ve "en uygun delil olma" özelliğinin bulunması gerekir[330].

Amerikan hukuk sistemde delillerin kabul edilebilirliğinin ölçüsünde sunulan delil;

- Jüri üzerinde adil olmayan bir önyargının oluşmasına neden olmamalıdır,

- Delilin ilavesi davaya konu olan olayı aşarak başka tarafa çekilecek nitelikte olmamalıdır,

- Delilin jüriyi yanlış yönlendirme ihtimali olmamalıdır,

- Delil duruşmanın gereksiz bir şekilde uzamasına neden olmamalı ve zaman kaybı oluşturmamalıdır.

Bunların yanı sıra olayın taraflarından birisinin mahkemeye sunulan bir delil karşısında böyle bir delilin ortaya çıkabileceğini haklı gerekçelerle hiç tahmin etmemesi durumunda bir haksızlık ve zarara uğrama durumunun ortaya çıkması hakimin deliller ilgili ve önemli bile olsa onları kabul edilebilir olarak değerlendirmeyebilecektir. Ayrıca, bilimsel yollarla elde edilen dijital delillerin de kabul edilebilirlik şartlarına uyması gerekir[331].

İngiliz hukuku da Amerikan hukukundaki gibi delillerin kabul edilebilirliği ve ilgililiğin olay ile ilişkili olmasına dikkat etmektedir. Bununla birlikte delilin ilgili olmasıyla o delilin kabul edilebilir olmasının aynı olmadığı bilinmelidir. Bunun nedenine mantıksal açıdan yaklaşıldığında ilgililik uyuşmazlık ile delil arasında ortaya çıkan bağ iken kabul edilebilirlik hukuki bir tartışma konusudur[332]. Delilin kabul

[330] M. Göksu, 2011, s.105.
[331] John C. Klotter, **Criminal Evidence**, Cincinnati: Anderson Publishing Company, 1980, ss. 94-104.
[332] Adrian Zuckerman, **The Principle of Criminal Evidence**, Oxford: Oxford University Press, 1989, s.47

edilebilirliğinde İngiltere hukukunda "bilirkişi tanıklığı" oldukça önemlidir. Hakim bilirkişinin dijital delilin olayla ilgisinin bilimsel yoldan açıklanmasını dinleyerek gerçek olana ulaşmada o delilin kanıt olup olmayacağına karar vermektedir. Delillerin aleniliği prensibi gereğince yargılamanın geleceğini belirleyecek delilin herkes tarafından anlaşılabilmesine ve tartışılabilmesine de imkan sunulmalıdır. Bu nedenle mahkeme salonunda dijital verilerin delil olup olmadığının tartışılabilmesi için salonların bu tartışmayı yapmaya uygun teknoloji ile donatılması gerekir[333].

"1978 tarihli Meiri v. Israel" kararından itibaren "İsrail Yüksek Mahkemesi" hukuka aykırı delilleri ceza yargılamasında dikkate alınması gerektiğini ancak bu delillerin hükme etkisinin mahkemenin taktirine bırakılması gerektiği yönünde içtihatta bulunmuştur. 2006 yılında "Issacharov v. Chief Military Prosecutor" kararında bu içtihat değişerek mahkemelerin hukuka aykırı delilleri kabul etmeme yetkisinin bulunduğu kabul edilmiştir[334].

Türk Ceza Muhakemesi bakımından esas olan şey delil yasakları dışında her şeyin delil olarak kabul edilmesi nedeniyle delillerin kabul edilebilirliğine yönelik tartışmaya önem verilmemektedir. Bununla birlikte *CMK'nın 170. maddesi 2. Fıkrasında*: *"soruşturma evresi sonunda toplanan deliller, suçun işlendiği hususunda yeterli şüphe oluşturuyorsa; Cumhuriyet savcısı, bir iddianame düzenler."* ifadesinin bulunması delillerin Cumhuriyet Savcısı tarafından değerlendirilebileceğini göstermektedir. Bu açıdan bakıldığında Cumhuriyet savcısı "delil" niteliğindeki hukuka uygun her türlü bilgi, belge, veriyi inceleyerek kamu davası açıp açmamaya yetkili kişidir[335]. CMK'nın Cumhuriyet savcısına verdiği bu yetki kapsamında savcının hukuka

[333] Ian Walden, **Computer Crimes and Digital Investigations**, Oxford: Oxford University Press, 2007, ss. 387-389.
[334] Binyamin Blum, **Doctrines Without Borders: The 'New' Israeli Exclusinary Rule and the Dangers of Legal Transplantation**, Stanford Law Review, Vol: 60, No: 6, April 2008, s. 2135-2136.
[335] Hasan Tahsil Gökcan, "Cumhuriyet Savcısının Delilleri Değerlendirme Yetkisi ve Yargıtay Uygulaması", **Ankara Barosu Dergisi 2012**, Ankara, Ocak http://www.ankarabarosu.org.tr/siteler/ankarabarosu/tekmakale/2012-1/2012-1-9.pdf

aykırı delilleri ayıklaması bilhassa kendi sorumluluğunda olması nedeniyle iddianame hazırlarken elde edilen delilin hukuka uygun olup olmadığını kontrol etmeli, kanıt değeri taşımayan bilgi ve belgelerle iddianame hazırlamamalıdır.

Türk hukukunda hakim hükmünü verirken delillerin ispat edilip edilmediğine baktığından delillerin hukuka aykırı olmaması, müşterek olmasına dikkat etmektedir. Bu nedenle Cumhuriyet savcısının iddianame düzenlemeden önce delilleri hukuka uygunluk süzgecinden geçirmesi ve daha sonra iddianame düzenlemesi hukuksal bir gerekliliktir[336]. Hakimin yargılama sonunda vereceği kararının akılcı ve bilimsel açıdan kabul edilebilir olabilmesi için hangi delillerin verilen kararı etkilediğini açıklaması gerektiğinden[337], herhangi bir şeyin delil olabilmesi için belli bir konunun ispatına aracılık etmesi, hukuka uygun olması ve yargıcın vicdani kanaate ulaşmasına yardımcı olup olmayacağının dikkate alınması gerekir[338]. Bununla birlikte gerekçelerini açıklamak koşuluyla yargıç delilleri tespit etmek ve değerlendirilme sürecinde serbestiye sahip olduğu ve bu sisteme vicdani delil sistemi denildiği de teoride öğretilen bir durumdur[339]. Medeni yargılamalarda şekillere bağlı kanıt yöntemine başvurulurken, ceza yargılamalarında yargıcın delilleri değerlendirmede tamamen bağımsız ve delillerin değerlendirilmesinde serbestliği bulunmaktadır. Bu durumda ceza hâkimi delil olarak ileri sürülen hususların delil olarak kabul edilebilirliğini bir diğer ifadeyle ispat değerini serbestçe takdir etme yetkisini "delillerin serbest değerlendirilmesi ilkesi" gereğince kullanabilmektedir[340].

---

[336] Fatih Birtek, "Cumhuriyet Savcısı'nın Delilleri ve Fiili Takdir Yetkisi", Prof. Dr. Nur Centel'e Armağan, **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 2013**, 19(2), s. 955

[337] Ş. Sarsıkoğlu, 2015, ss.432-433.

[338] V.Ö. Özbek ve diğerleri, 2012, s. 657

[339] Metin Feyzioğlu, **Ceza Muhakemesinde Vicdani Kanaat**, Yetkin Yayınları, Ankara, 2002, s.49; N. Kunter ve diğerleri, 2010, s. 1327; Bkz. CMK m. 217/1: "*Hâkim, kararını ancak duruşmaya getirilmiş ve huzurunda tartışılmış delillere dayandırabilir. Bu deliller hâkimin vicdanî kanaatiyle serbestçe takdir edilir."*

[340] Mahmut Koca, "Ceza Muhakemesinde Hukuka Aykırı Delilleri Değerlendirme Yasağı", **Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi 2000,** 4(1-2), s. 105.

Türk hukuk sisteminde delilin kabul edilebilmesi için hukuka aykırı olmaması kabul edilmiş olsa da *Yargıtay 7. Ceza Dairesi'nin 03.07.2013 tarih, E.2013/5127, K.2013/17549*[341] *sayılı kararında* arama kararı olmadan sanığın araba bagajında ele geçirilen kaçak parfümlerin topluma vereceği zararın kişiye vereceği zarardan fazla olması durumunda delil olarak kullanılabileceği kararı verilerek insan haklarını korunurken hukuk devletindeki adaleti ve hukuki güvenliği zedelemenin mümkün olmadığı gösterilmiştir.

Yargıtay'ın delillerin kabul edilebilirliğine yönelik vermiş olduğu başka bir kararda da AİHM kararları doğrultusunda bu hususun iç hukuk bağlamında ele alınması gereken bir sorun olduğu şu şekilde vurgulanmıştır: "*Avrupa İnsan Hakları Sözleşmesi, iç hukukun ve ulusal yargının yetki alanına giren delilerin kabul edilebilirlikleri veya bunların değerlendirilmeleriyle ilgili konularda bir kural koymamaktadır. (Garcia Ruiz/İspanya Davası, 21.01.1999, §28). Sözleşmede, delillerin kabul edilebilirliğinin belirlenme yöntemini gösteren ve hangi kanıtların kabul edilebilir olduğunu belirleyen bir kural yoktur (Schenk/İsviçre Davası, 12 Temmuz 1988, §45-46; Teixeira de Castro/Portekiz Davası, 09 Haziran 1998, §34; Heglas/Çek Cumhuriyeti Davası, 01 Mart 2007, §84). Mahkemenin yerleşik içtihadına göre kanıtların kabulü ve değerlendirilmesi öncelikle ulusal mahkemelerin görevidir (Van Mechelen ve Diğerleri/Hollanda Davası, 23 Nisan 1997, §50; Rachdad/Fransa Davası, 13 Kasım 2003, §23).*"[342]

Dijital adli delillerin güvenilirliği ve kabul edilebilirliği, adli bilişim uzmanları tarafından verilen raporlar bağlamında ele alınsa da hukuksal açıdan geçerliliği sorgulanabilmektedir. Bunun en önemli sebebi bilişim teknolojilerinin durağan olmayan yapısından ve delillere etki eden çok sayıda unsurun bulunmasından

[341] Bkz. Yargıtay 7. Ceza Dairesi'nin 03.07.2013 tarih, E.2013/5127, K.2013/17549
[342] M. Kızılyar, 2014, s.88. Bkz. Yargıtay Dokuzuncu Ceza Dairesinin 09/10/2013 tarih ve E.2013/9110, K.2013/12351 sayılı kararı

kaynaklanmaktadır. Dijital delilin kabul edilebilirliğindeki en büyük sorun "delil karartma", "zararlı yazılımlar" ya da herkesin bilmediği teknolojilerle müdahalelerin olmasıdır. Bu nedenle dijital adli delillerin kabul edilebilmesi için delilin geçerliliği, delilin aslına uygunluğu, delilin bütünlüğü, delilin kaynağı, delilin kullanıcı ilişkisi, delilin inandırıcılığı, delilin tekrar incelenebilirliğinin tespit edilmesi gerekir[343].

Dijital delillerin kabul edilebilirliğiyle ilgili olarak Cumhuriyet savcısının delillerin hukuka uygunluğunu incelemesi, ispatlanıp ispatlanamayacağını tespit etmesi gerekir. Dijital verilerin delil niteliğini taşıyıp taşımadığı yetkisi soruşturma aşamasında Cumhuriyet savcılığında, kovuşturma aşamasında ise mahkemelerdedir. Bu yetkilerini kullanırken bilişim uzmanlarının verdikleri raporları göz önünde bulundurmaktadırlar. Ancak, bilişim uzmanların elde edilen verilerin hukuka aykırılık taşıyıp taşımadıklarını, delil niteliğine sahip olup olmadığını, ispat gücünü, suçun işlendiğiyle ilgili yeterli şüphe oluşturup oluşturmadıklarını tespit edecek bir eğitime sahip olmamaları hazırladıkları raporun hukuksal açıdan değerlendirilmesini eksik bırakmaktadır.

B. Dijital Delillerin Doğrulanması ve Dijital Delillere İlişkin Hukuki Kurallar

Delillerin hukuka uygunluğu gösteren en önemli kriterlerden biri delilin doğrulanmasıdır. Yani delilin iddia edilen "şey" olup olmadığının ispat edilmesidir. Örneğin, tanığın mahkemeye tanık olarak gelen kişinin tanık olarak gösterilen kişi olup olmadığının resmine ve kimlik bilgilerine bakılarak tespit edilmesi, atılan bir imzanın kişiye ait olup olmadığının bilirkişi raporlarıyla belirlenmesi işlemleri delilin doğrulanması işlemleridir[344]. Dijital delillerin doğrulanmasında ise dijital delillerin kolay zarar görebilmeleri, değiştirilebilmeleri veya yok edilebilmeleri gibi kendilerine

[343] E. Çalışkan, 2013, ss.94-106.
[344] M. Göksu, 2011, s.170

özgü özellikleri nedeniyle oldukça büyük sorunlara yol açabilir ve doğrulama çoğu zaman yapılamayabilir.

Türk Ceza Muhakemesi açısından dijital delillere ilişkin getirilen kurallar "CMK 134. maddede", bilgisayarlar, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma başlığında ele alınmıştır. Ayrıca CMK m. 135 ve 140'ta düzenlenen koruma tedbirleri yoluyla da dijital deliller elde edilmektedir. Ancak dijital delillerin muhakeme hukukuna etkisiyle ilgili verilerin delil değeri konusunda yol gösterecek bir kurallar bütünü hukukumuzda bulunmamaktadır. Bununla birlikte tüm dünyada olduğu gibi ülkemizde de ele geçirilen dijital deliller artık klasik delillerden daha fazla hale gelmiştir.

Elektronik delillerin doğası gereği değiştirilebilmesi ve taklit edilebilmesi mahkemenin bu delilleri kabul edebilmesi için öncelikli olarak delilin doğrulanmasını istemesi gerekir. Bu nedenle bir davada elektronik delil sunulması halinde hâkimin, deliller üzerinde inceleme yapması, delilin doğruluğu konusunda tarafların anlaşamaması halinde mutlaka bilirkişiden yardım alınması yoluna girmesi gerekir[345].

Dijital delillerin doğrulanması ile ilgili muhakeme yapabilmek için çalışmamızda öncelikle CMK kapsamında Türk Ceza Muhakemesi detaylandırıldıktan sonra yabancı hukuk sistemlerinin dijital delil doğrulamaya yönelik geliştirdikleri hukuki düzenlemelerle birlikte uluslararası kurallardan da bahsedilmiştir.

1. Türk Ceza Muhakemesi Kapsamında Dijital Delillerin Elde Edilmesine İlişkin Kurallar

Bu başlık altında öncelikli olarak CMK 134. Madde incelenecek, ardından AİHM'nin bilgisayar aramalarına ilişkin kararları irdelendikten sonra bilgisayarlarda

[345] John D. Gregory, "Authentication Rules and Electronic Records", **The Canadian Bar Review 2002,** 81(3), s. 537.

yapılacak aramalar sonucu elde edilecek tesadüfi deliller ve CMK 134. Madde kapsamında getirilen hukuki düzenlemeye aykırılık konuları ayrıntılı bir şekilde ifade edilecektir. Ardından "İletişimin Denetlenmesi" ve "Teknik Araçla İzleme" koruma tedbirleri yoluyla elde edilecek dijital verilere ilişkin bir çerçeve oluşturulmaya çalışılacaktır.

a. CMK 134. Maddenin İncelenmesi

Türk Ceza Muhakemesi kapsamında dijital deliller ve adli bilişim alanına ilişkin hukuki nitelikteki metinler "Adli ve Önleme Aramaları Yönetmeliği" ve "Suç Eşyası Yönetmeliği" ve CMK'nın 134. Maddesidir. "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El Koyma" başlığını içeren CMK 134. Madde, bilgisayarlarda arama ve el koymanın hukuki rejimini düzenleyen bir maddedir. Hangi şartlar altında bilgisayar incelemesine başvurulacağı, incelemenin hangi kapsamda yapılacağına değinilen CMK 134. Maddesinin işletilebilmesi için ilk fıkrada vurgulanan "başka suretle delil elde etme" imkanının bulunmaması gerekir. Burada dikkat edilmesi gereken özellik arz etmeyen delil ve kaynakları bakımından CMK 119. Maddenin uygulanacak olması, bilişim suçları ya da klasik suçlara ait delillerin bilgisayarda bulunması durumunda ise CMK 134. Maddeye göre hareket edilmesi gerektiğidir.[346]

CMK 134. Maddenin gerekçesinde bilgisayar program ve kütüklerinde arama yapılmasının şartları şu şekildedir[347]: (www.tbmm.gov.tr)

"1. İki yıl veya daha fazla hürriyeti bağlayıcı cezayı gerektiren cürümler hakkında yapılan soruşturmalarda bilgisayarda, bilgisayar programlarında ve bilgisayar kütüklerinde arama, kopyalama ve aygıta geçici olarak elkoyma yapılabilir.

[346] M. Özen, G. Özocak, 2015, ss.60-61
[347] CMK Madde Gerekçeleri, www.ceza-bb.adalet.gov.tr/mevzuat/cmkmaddegerekce.doc.

2. Bunun için, söz konusu işleme başvurulmasının zorunlu olması yani bunun bir 'ultima ratio' çare oluşturması gereklidir.

3. Bu hususta kararın mutlaka hâkim tarafından ve gizli olarak verilmesi gerekir. Bu karar, soruşturma evresinde sulh ceza hâkimi tarafından gizli olarak verilecektir.

4. Arama sonucu, suçla ilgili bilgi metin hâline getirilecektir.

5. Bilgiler şifreye bağlanmış ise ve bu nedenle giriş yapılamıyorsa, çözümün yapılabilmesi için araç ve gereçlere, aygıta geçici olarak elkonulabilir. Çözümden hemen sonra bilgisayardaki bilgilere zarar vermeden aygıtın ilgilisine hemen geri verilmesi gerekir."[348]

CMK'nın 134. Maddesi kapsamında arama yapabilme, delillere el koyma veya kopyasını alabilmek için birinci fıkra gereğince;

- Öncelikle bir suç soruşturması açılmış olması gerekir,
- Somut delillere dayanan kuvvetli suç şüphelerinin olması gerekir.
- Başka suretle delil elde edilme imkanı olmaması gerekir.
- Son olarak da Cumhuriyet Savcısı talep etmeli, hakim de bu istemi onaylayan bir karar vermelidir. Gecikmesinde sakınca olan hallerde Cumhuriyet Savcısı karar verir.
- Maddenin gerekçesinde "İki yıl veya daha fazla hürriyeti bağlayıcı cezayı gerektiren cürümler hakkında yapılan soruşturmalar" şartının geçmesi dikkat edilmesi gereken önemli bir husustur.

[348] 5271 Sayılı CMK, ***"Madde 134*** *- (1) Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir."*

Şüphelinin bilgisayar aramasına başvurulabilmek ya da el koymak için *"somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı"* ve *"başka suretle delil elde etme imkanının bulunmaması"* şartlarının aynı anda aranması kanun koyucunun kişisel verilerin ihlal edilmesini engelleme isteğinden kaynaklanmaktadır. Bu nedenle bilgisayar aramaları başvurulacak en son tedbir olarak öngörülmüştür. Kanunun lafzına dikkat edilecek olursa *"başka suretle delil elde etme imkanının bulunmaması"* şartı suçun bilgisayarda işlenmiş olabildiği durumları işaret etmektedir. Bu nedenle bilgisayarla suç işlendiğinden şüphelenilen soruşturmalar olması ve bilgisayarlarda arama yapılacak verilerin de suçun konusunu oluşturan veriler olması gerekir. Baştürk'e göre "somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı" şartı, uluslararası hukukta "beyond the reasonable doubt" olarak ifade edilen makul şüphenin ötesine geçen, bir suçun işlendiğine yönelik çok güçlü işaretler taşıyan bulgular için yapılan bir tanımlamadır[349].

"Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El Koyma" tedbirinin uygulanmasına karar verme yetkisi 2018 yılında yaoılan değişikliğe kadar yalnızca hakimdeydi. 25.7.2018 tarihinde 7145 sayılı kanunla CMK'da yapılan değişiklik, gecikmesinde sakınca bulunan hallerde savcının da bu kararı alabilmesini sağlamaktadır. CMK m.134/1'de de "*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. (Ek üç cümle: 25/7/2018-7145/16 md.) Cumhuriyet savcısı tarafından verilen kararlar yirmi dört saat içinde hâkim onayına sunulur. Hâkim*

[349] İhsan Baştürk, "Bilgisayar Sistemleri ile Verilerinde Arama, Kopyalama ve El Koyma", **Fasikül 2010,** 9, s.25.

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." demektedir. Bu doğrultuda gecikmesinde sakınca bulunan bir hal varsa savcı karar verecek, ancak yirmidört saat içerisinde hakim onayına sunulacaktır. Yine yirmidört saat içerisinde hakim kararını verecektir. Süre dolar veya hakim aksi yönde karar verirse elde edilen tüm deliller imha edilir.

Bu tedbirin uygulanması için alınması gereken kararda önem taşıyan bir husus da bu kararın elkoyma öncesinde alınması gerekmesidir. Yargıtay da bu görüştedir: *"Sanığın, babası ... üzerine kayıtlı olan internet hattı üzerinden şirketteki işinden ayrıldıktan sonra şirkete ait sisteme girip bloke ettiğinden bahisle açılan davada; katılanın şikayet dilekçesi ekinde ibraz ettiği deliller dışında delil toplanmayıp bilirkişi raporundan da anlaşılacağı üzere katılanın ibraz ettiği LOG kayıtlarında başka IP'lerin de yer aldığı halde araştırılmaması ve her ne kadar hard diskte 'gkavak' kullanıcı adı ve tespit edilen IP numarasına rastlanmışsa da* ***el konulduktan 4 gün sonra CMK'nın 134. Maddesine göre bilgisayar kütüklerinde arama kararı verilmesi nedeniyle sanığın bilgisayarından hukuka aykırı olarak elde edilen delillerin hükme ve incelemeye esas alınamayacağından*** *suç tarihi itibariyle bilişim sistemine girip kalmaya devam ettiğine dair delil bulunamaması karşısında mahkemenin kararında bir isabetsizlik görülmemiştir"*[350]

134. madde kapsamında yapılacak bir arama veya el koyma işleminin kanuna uygun yapılabilmesi için bilgisayarlar, bilgisayar kütükleri veya bilgisayar programları olması kanun maddesinin başlığından ve içeriğinden de anlaşılmaktadır. Bununla birlikte günümüz teknolojisi dikkate alındığında pek çok cihazın teknolojik olarak gelişmiş olduğu ve tıpkı bir bilgisayar gibi çalıştığı göz önüne alınacak olursa kanunun lafzen bilgisayardan bahsetmesi diğer depolama ve bilgisayar programlarını çalıştırma

[350] Yargıtay 8. Ceza Dairesi, 29.11.2017, 2016/10741 Esas Sayılı, 2017/13486 Karar sayılı kararı.

özelliği olan cihazlarından bahsetmemesi kanunun önemli bir eksikliği olarak görülmelidir[351]. Kanun lafzen bilgisayardan bahsetse de uygulamada cep telefonları, akıllı cep telefonları, müzik çalarlar ve diğer depolama özelliği bulunan aletlere de el konulduğu bilinmektedir.

134. maddenin ikinci fıkrasına göre; *"(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması 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."*

Bu maddede doğrudan bir el koyma zorunluluğu getirilmemiş, *"şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması"* durumunda el konulma işleminin yapılacağı vurgulanmıştır. Madde her ne kadar lafzi olarak kişisel verilerin korunması amacıyla bilgisayar aranması ve el konulması son çare olarak görülse de uygulamada hukuki olarak kabul edilemeyecek gerekçelere dayandırılarak menkul mala el koyar gibi davranıldığı yönünde eleştiriler bulunmaktadır[352].

134. madde 2. Fıkraya göre öncelikli olarak bilgisayarda yerinde inceleme (arama) yapılmalıdır. Ancak, şifrenin kırılamamsından dolayı bilgisayara girilememesi veya gizlenmiş bilgilerin elde edilememesi halinde bilgisayarlara el konulabileceği bildirilmektedir. Özen ve Özocak'a[353] göre bu hüküm teknik olarak hatalı olup bilgisayarlarda yerinde inceleme genellikle yapılamamaktadır. Bu tedbirin doğru uygulanışı ancak şüphelinin mağduriyetinin önlenmesi ve delilleri koruyucu önlemlerin

[351] Serap Keskin Kiziroğlu, Fulya Eroğlu, İlker Tepe, Hazırlık Kolokyumu Bölüm III Ceza Muhakemesi Türkiye Ulusal Grup Raporu, AIDP XIX. Dünya Kongresi, "Bilgi Toplumu ve Ceza Hukuku Hazırlık Kolokyumları", **Suç ve Ceza Ceza Hukuku Dergisi2013**, 1, s.91.
[352] Y. Ünver, H. Hakeri, 2012, s.580.
[353] M. Özen, G. Özocak, 2015, s.63

alınmasından sonra bilgisayara el konularak teknik uzmanlarca laboratuvar ortamında incelenmesine imkan tanınmasıdır.

CMK 134. Maddede belirtilen hususlar "Adli ve Önleme Aramaları Yönetmeliği"nin 17. Maddesinde de aynen tekrar edilmiş sadece 3. Fıkraya bir cümle daha eklenerek bu işlemin bilgisayar ağları ve uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanabileceği belirtilmiştir. Yönetmelikte çıkarılabilir donanımlardan kastın CD, DVD, Flash Bellek ve cep telefonları gibi veri saklama özelliği olan donanımlar olduğu, bu nedenle de CMK 134. Madde kapsamına girdikleri ileri sürülmektedir[354]. Bu durumda yönetmeliğin Kanunda öngörülen hakka ilişkin daha geniş bir sınırlandırma yapılmasını öngörmesi, bu yönetmelik maddesinin uygulamasında kanunda öngörülen sınırların ötesine geçildiğini göstermektedir[355]. Bu sorunların giderilmesi açısından kanun maddesinin çağın gereklerine göre bilgisayar sistemlerinde kullanılabilen veya entegre edilebilen veri kaydetme özelliğine sahip donanım veya cihazların da CMK madde 134 kapsamına alınmasına yönelik bir güncellemenin, uygulamada hali hazırda yapılan bilgisayarlarla birlikte bu dijital veri kaynaklarına da el konulmasındaki hukuki sorunları giderebileceği söylenebilir.

Diğer yandan "Suç Eşyası Yönetmeliği"nin 8. Maddesine[356] göre de bilgisayar, bilgisayar kütükleri ve bu sisteme ilişkin verilerin asılları veya kopyalarının, ses ve görüntü kayıtlarının bulunduğu depolama aygıtlarının bozulmalarına neden olabilecek nem, ısı, manyetik alan ve darbelere karşı önlem alınmasını ve uygun ortamda muhafaza edilmesi gerekir. Bu durumda da CMK 134. Madde kapsamındaki bilgisayar, bilgisayar kütükleri ve programları ifadelerine Suç Eşyası Yönetmeliğinde ses ve görüntü kayıtları

[354] MV. Dülger, 2013, s.658
[355] S. Keskin Kiziroğlu v e diğerleri, 2013, s.94
[356] Suç Eşyası Yönetmeliği, Resmi gazete Sayı, 29662, Tarih 23 Mart 2016 http://www.resmigazete.gov.tr/eskiler/2016/03/20160323-2.htm, **Madde 8:***"(3) Bilgisayar, bilgisayar kütükleri ve bu sisteme ilişkin verilerin asıl ya da kopyaları, ses ve görüntü kayıtlarının bulunduğu depolama aygıtları gibi elektronik eşya, bozulmalarını engelleyecek, nem, ısı, manyetik alan ve darbelerden korunmalarını sağlayacak müstakil uygun alanlarda muhafaza edilir"*

gibi depolama aygıtları da yazılarak genişletilmiştir. Bu nedenlerle CMK 134. Maddenin günün gelişen koşullarına ve teknolojideki değişim hızına göre zaman zaman güncellenmesi gerektiği söylenebilir.

134. madde 2. Fıkra gereğince incelemeler kopya üzerinde yapılacağına göre el konulan bilgisayarın kopyası derhal alınmalı ve orjinali sahibine teslim edilmelidir. Önceden şüpheli veya vekilinin istemesi halinde el konulan bilgisayarın iadesi mümkün iken, "21.2.2014 tarihinde yürürlüğe giren ve hükümde değişiklik yapan 6526 sayılı "Kanun gereğince CMK 134. Madde 3. ve 4. Fıkraları gereğince el konulan bilgisayarın yedekleme yapılması, bu yedek tutanak ile birlikte şüpheliye ya da vekiline verilmesi zorunlu hale getirilmiştir[357]. Bu durum hem şüphelinin haklarının güvence altına almasına, hem de delillerin sıhhatinin korunmasına aracılık edecek bir uygulama olup ceza soruşturmasının doğru bbir şekilde gerçekleşmesi için olumlu bir değişiklik olmuştur. Bununla birlikte el konulan bilgisayarların adli bilişimin özellikleri çerçevesinde yedekleme işleminin çok uzun sürmesi ve görevlilerin bazen yanlarında yeterli yazılımları taşımamaları, kolluk kuvvetlerinin kopyalama işlemleri ile ilgili teknik bilgilerinin bulunmaması, el konulan malzemelerin adli bilişim incelemesinin yapılacağı laboratuvarlara götürülmesine neden olabilmektedir. Ancak kanun bilgisayarlara el konulma işlemi sırasında bir kopyasının alınmasını şart koşarak dijital delillerin güvenilirliğini sağlamak istemekte ve bunu bir zorunluluk olarak görmektedir.

5271 Sayılı CMK, Madde 134. Maddesi 5. Fıkrasına göre "*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."* Bu hüküm doğrultusunda

[357]5271 Sayılı CMK **134. Madde:***"(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."

bilgisayar delillerinin el konulmadan da kopyalanabileceği, kopyalananların da kağıda yazdırılarak ilgililere imzalatılacağı bildirilmiştir. Ancak, uygulamada arama işlemleri sırasında el koyma işlemi yapmadan bilgisayar verileri kopyalanabilse de bu verilerin kağıda dökülmesi pek mümkün gözükmemektedir. Bunun nedeni; verilerin sayfalarca tutabileceği, yazdırma işleminin çok uzun sürebileceği, yazdırma için arama alanında yazıcı ve kağıta ihtiyaç olabileceği gibi birtakım sorunlardır. Bu sorunların çözümü de mümkün görünmediğinden kanaatimizce el koyma işlemi yapılmayacaksa bilgisayar verilerinin dijital kopyasının CD üzerine alınması, CD üzerindeki alana çıkmayan yazı ile ilgililerin imzaları atılarak bir örneğinin şüpheliye verilmesidir. Bu uygulama ile verilerde sonradan oynama, değiştirme işleminin yapılıp yapılmadığı da kolaylıkla çözülebilecektir. Ancak yargılama işlemi çok uzun süren davalarda bu dijital veri kaynaklarının bozulmaması için "Suç Eşyası Yönetmeliği"nin 8. Maddesine göre özel koşullarda saklanması gerektiği de unutulmamalıdır.

Sonuç olarak ceza muhakemesinde, hukuka aykırı olamayacak şekilde elde edilen delillerin soruşturma ve yargılamada esas alınacağı, aksi taktirde kanunda öngörülen usullerden birine dahi uyulmamasının elde edilen delilin "kanuna aykırı delil" olmasına neden olacağı ve hukuki bir anlamı olmayacağı bilinmelidir. CMK'nın, birçok hükmü ceza yargılamasında isnadın ancak kanuna uygun elde edilmiş delillerle ispatlanabileceğinden bahsetmektedir. Bu nedenle kanuna aykırı bir delile dayanılarak verilen hükmün de mutlak bir biçimde bozulacağı CMK m. 206, 217, 289/j maddelerinden de anlaşılmaktadır.

b. AİHM'in Bilgisayar Aramalarına İlişkin Kararları

Bilgisayarların insan hayatına girmesi birçok işin kolaylaşmasını özellikle işyerlerinde hesapların tutulması, kayıtların alınması, ürün giriş çıkışlarının kontrol altına alınması ve personel bilgilerinin tutulmasını kolaylaştırmıştır. Ancak son 30 yılda

teknoloji ve internetteki hızlı gelişim bilgisayar ve akıllı cihazların kullanım alanını genişletmiştir. Teknolojideki bu gelişmeleri yakından takip eden suç örgütleri ya da suç işlemeye yatkın kişiler her gün yeni bir yöntem bularak suç işleyebilmektedir. Klasik suçlara göre daha rahat işlenen ve yakalanma riski daha az olan bu suçlara karşı tüm Dünya ülkeleri mücadele amacıyla kanunlarında güncellemeler veya özel birimler oluşturarak önlemlerini almaya başlamıştır. Ancak alınan tedbirlerin zaman zaman AİHS 8. maddesinde belirtilen "özel hayatın ve aile hayatının korunması" hakkını ihlal ettiği AİHM kararlarından anlaşılmaktadır.

AİHM'in dijital delillerle ilgili kararlarında en önemli hak ihlallerinin, AİHS'in "özel hayatın ve aile hayatının korunması" başlıklı 8. Maddesi[358] ile ek Protokol'ün[359] "mülkiyetin korunması" başlıklı 1. Maddesi ile ilgili olduğu görülmektedir. "AİHS 8. Madde" kapsamına özel yaşam, aile yaşamı ile konut dokunulmazlığı ve haberleşme hürriyeti girmektedir. Bu özgürlükler kişisel verilerin korunmasını da dolaylı olarak beraberinde getirmiştir.

"AİHM", kendisine yapılan hak ihlallerini değerlendirirken beş temel denetim aşamasından geçirmektedir. Bu sistemde ilk iki aşamada müdahalenin olup olmadığı tespit edilirken diğer üç aşamada müdahalenin hak ihlali oluşturup oluşturmadığı incelenmektedir[360]. Bu durumda bir hak ihlaline karar verirken;

---

[358]AİHM'in resmi internet sitesi http://www.echr.coe.int 8. maddesinin Türkçe tercümesi şu şekildedir:

> "*1. Herkes özel hayatına, aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.*
>
> *2. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç şplenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda zorunlu olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir.*"

[359] Avrupa Konseyi'nin Ek Protokol 1. Maddesi:*"Her gerçek ve tüzel kişinin mal ve mülk dokunulmazlığına saygı gösterilmesini isteme hakkı vardır. Bir kimse, ancak kamu yararı sebebiyle ve yasada öngörülen koşullara ve uluslararası hukukun genel ilkelerine uygun olarak mal ve mülkünden yoksun bırakılabilir."*

[360] Philip Leach, **Taking a Case to the European Court of Human Rights**, 3. Edition, Oxford University Press, 2011, s.310.

- *"Öncelikle başvurucunun iddiasının madde ile ilgili olup olmadığı,*
- *İlgiliyse maddede belirtilen özgürlüğe müdahale olup olmadığı*
- *Müdahale varsa bu müdahalenin kanun tarafından öngörülüp öngörülmediği,*
- *Müdahale kanunla öngörülmüşse, bu öngörünün maddede sayılan meşru amaçlardan birine veya birkaçına uyup uymadığı,*
- *Bu müdahalenin demokratik bir toplum açısından gerekli ya da genel olarak orantılı olup olmadığı değerlendirilmektedir."*[361]

Dijital delillerle ilgili hak ihlalleri AİHM kararlarına göre genellikle bilişim koruma tedbirlerinin uygulanmasında ortaya çıkmaktadır. Bu nedenle AİHM kararlarının göz önünde bulunması dijital delillerin elde edilmesine yönelik faaliyet sınırlarının belirlenmesi oldukça önem arz etmektedir.

Petri Sallinen ve Diğerleri- Finlandiya davasında, avukat Sallinen'in bir müvekkilinin sahtecilik suçuna suç ortağı olduğu iddiasına yönelik olarak bürosunda yapılan aramalarda tüm bilgisayar kayıtları incelenmiş ve bir bilgisayara elkonulurken diğer iki bilgisayardaki veriler kopyalanmıştır. Bu kapsamda inceleme ve denetimlerini yapan AİHM;

- Öncelikle bilgisayarlarda arama yapılmasını veelkonulması nedeniyle bilgisayar içerisinde bulunan e-postalara ulaşılabilecek olmasını özel hayatı ilgilendiren birmüdahale olarak görmüş,
- Bu müdahalenin hukuka uygunluğunun tespiti için iç hukukta var olan kurallar incelenmiş,
- Bu müdahale iç hukukta bulunmasına rağmen Kanunda yer alan ifadelerin açık olmaması öngörülebilirlik ilkesine uymadığını göstermiş,

[361] P. Leach, 2011, ss. 311-313.

- "avukat-müvekkil itimatilişkisine" kanunda yer verilmediği ve yeterli yasal garantilerin olmadığı belirlenerek AİHS'nin 8. maddesinin ihlaline karar vermiştir[362].

"Craxi-İtalya kararında", İtalya Eski Başbakanı olan Craxi hakkında "temiz eller" operasyonu düzenlenerek bilgisayarlardan elde edilen bir dosyaya el koymasını AİHM, 8. Maddenin ihlali olarak değerlendirmiştir. AİHM, gerekçesinde elde edilen özel ve dava ile ilgili olmayan bilişim verilerinin ve telefon konuşmalarının kovuşturma konusu olan duruşmada delil olarak okunmasının ve basına yayınlanmasının AİHS 8. Madde ihlaline yol açtığını ifade etmişlerdir[363].

Smirnov-Rusya kararında, örgütlü suç işlediği gerekçesiyle avukat olan Smirnov'un bilgisayarında arama yapılması ve bilgisayarına da elkonulmasını AİHM, hem AİHS 8. Madde hem de ek Protokolün 1. maddesini ihlal olarak değerlendirmiştir. Gerekçede, yeterli şüphe sebebi olmadan arama yapılması ve avukatların meslek sırlarının saklanmasıyla ilgili olarak kanunda yeterli bir garanti öngörülmemesi mesleki gizliliğe tecavüz olarak değerlendirilmiş ve 8. Maddenin ihlal edildiğini vurgulamışlardır. Bir avukatın bilgisayarının alınmasını ve üzerinde yapılan işlmeler sona ermesine rağmen uzun süre geri verilmemesini de ek Protokol'ün 1. maddesi açısından ihlal olarak görmüşlerdir[364]. GmbH-Avusturya kararında AİHM, avukat bürolarındayapılacak bilgisayar aramaları için gerekli şartların olması gerektiğine vurgu yapmıştır. Mahkeme, özellikle hakimin araştırma yapmak kararının olması gerektiğini ve yeterli suçşüphesinin bulunmasını öncelikli şart olarak vurgulamıştır. Ayrıca, avukatın bürosunda araştırma yapılırken kendisinin büroda olmaması halindebağımsız

[362] Petri Sallinen and others v. Finland, 50882/99, 27.09.2005.
[363] N. Kunter ve diğerleri, 2010, s.1113
[364] Smirnov/ Rusya, 71362/01, 07.06.2007

bir gözlemcinin o araştırmaya nezaret edip etmediği, materyallerine el konulup konulmadığı kriterler arasında sayılmıştır[365].

Bilgisayarlarda yapılan arama ve elkoymalara ilişkin, Prezhdarov Bulgaristan'a karşı davasında çiftin sahip olduğu beş bilgisayara polis el koymuştur. Çiftin müşterilerine kiraladıkları bu bilgisayarlarda bulunan oyunların, yasal yazılım lisanslarının olmaması şüphesi arama kararının esasını oluşturduğu anlaşılmıştır. "Prezhdarov bilgisayar programlarının", oyunların ve filmlerin hukuka uygun olmayacak şekilde dağıtımını yapmaktan ceza almış, dava bitene kadar da ilgili makamlar bilgisayarları iade etmemişlerdir. AİHM, elkoyulan bilgisayarların kişisel bilgiler içerdiğini ve yapılan elkoymaya karşı etkili bir itiraz yolunun ya da denetim yolunun bulunmadığını tespit etmiştir. Bundan başka uygulanan tedbirin orantısız olduğunu ve başvuruculların özel hayatına saygı gösterilmediği gerekçeleriyle ihlal kararı vermiştir[366].

Yuditskaya Rusya'ya karşı kararında bir rüşvet soruşturması kapsamında bir avukatlık ofisindeki tüm bilgisayarlara elkonulmuş ve veriler kopyalanmış, el konulduktan bir hafta sonra da bilgisayarlar iade edilmiştir. AİHM, yaptıkları inceleme sonunda özel hayatın gizliliğinin ihlal edildiğine karar vermiştir. Bu incelemede;

- "*Soruşturmayla ilgisi olmayan bilgilerin kopyalanması,*
- *Avukatların meslek sırlarının ortaya çıkması,*
- *Smirnov Rusya'ya karşı davasında olduğu gibi yeterli garantilerin alınmaması,*

[365] GmbH/ Avusturya, 74336/01, 16.10.2007.
[366] Prezhdarovi v. Bulgaria, 8429/05, 30.09.2014.

- *Uygulanan tedbirlerin kanun tarafından öngörülmüş olmasına rağmen demokratik bir toplum açısından gereklilik sınırlarının ötesine geçmesi ihlal gerekçesi olarak görülmüştür".*[367]

c. Bilgisayarlarda Yapılacak Aramalar Sonucu Elde Edilecek Tesadüfi Deliller

Tesadüfen elde edilen delil, yetkili makamların hukuka uygun olarak delil elde etme yöntemleri sırasında ilgili soruşturma ya da kovuşturma konusu dışında başka bir suç unsuruna ait delillerdir. Bu durumda kanuna aykırı delili tesadüfi delil ile karıştırmamak gerekir ki, tesadüfî delillerin hukuka aykırılığı ya da yok hükmünde sayılması mümkün değildir[368].

Bilgisayarlar, birçok insanın hem iş hem de özel hayatında sıklıkla kullandığı cihazlardır. Bu nedenle bilgisayarların kişisel veri barındırmama ihtimali yok gibidir. Bir suç soruşturması nedeniyle yapılan aramalarda bilgisayarlarda şüphelenilen suçun dışında başka bir suça ilişkin delillere ulaşılması da mümkündür. Tesadüfen ele geçirilen deliller ile ilgili CMK'nın 138. Maddesi şu düzenlemeyi içermektedir:

*"**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

[367] Yuditskaya v. Russia, 5678/06, 12.02.2015
[368] Bkz.Yargıtay CGK, E: 2007/5-101, K: 2008/3, 22.1.2008

uyandırabilecek bir delil elde edilirse; bu delil muhafaza altına alınır ve durum Cumhuriyet Savcılığına derhâl bildirilir."

Kanuna göre tesadüfi deliller ikiye ayrılmalıdır. Birincisi, arama veya elkoyma tedbiri sırasında konuyla ilgisi olmayan suçlarla ilgili tesadüfen ele geçirilen delil saklanır ve derhal durum savcılığa bildirilir, ikincisi ise telekomünikasyon yoluyla yapılan iletişimin kontrol edilmesi sırasında, tedbirin uygulandığı suç dışında bir başka suçun işlendiğine dair delilin ele geçirilmesi durumunda, bu delil ancak haberleşmenin kontrol edilmesi tedbiri uygulanacak katalog suçlardansa geçerli bir delil olarak görülecek ve Cumhuriyet savcılığına teslim edilecektir[369].

Göksoy'a göre "Adli ve Önleme Aramaları Yönetmeliği"nin 10/1-a maddesine göre "*Yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmakla birlikte, karar veya yazılı emirde konu edilmeyen"* bir delilin ele geçirilmesi de tesadüfi delil hükmünde ifade edilmiş ve bu haliyle yönetmelik kanuna aykırı olabileceği ileri sürülmüştür[370]. Ancak kanaatimizce de kanunda ilgili soruşturmayla bağlantısı olmayan deliller tesadüfi delil olarak nitelenmiş, ancak soruşturmayla ilgili olmasına rağmen arama ve el koyma emrinde yazılı olmayan delillerden bahsedilmemiştir. Yönetmelik kanundaki tesadüfi delil boyutunu genişletmiş görünmektedir. Yönetmeliğe göre her iki tesadüfi durum için derhal Cumhuriyet Savcısına bildirilmesi ve yeni bir arama ve el koyma kararı çıkartılması gerekir.

Özellikle ABD'de sık karşılaşılan bir durum olan belirli bir suç için failin bilgisayarında arama yapılması sırasında çocuk pornografisi gibi suçlara rastlanması halinde yeni bir soruşturma açılmaktadır. AİHM içtihatları da dikkate alındığında doğru olan yolun yeni suç unsuruna rastlanması halinde yeni bulunan suç bakımından arama

[369] M. Gödekli, 2016, ss.1886-1887
[370] Resul Göksoy, **Ceza Muhakemesinde Dijital Delillerin Elde Edilmesi Ve Güvenilirliğinin Sağlanması,** Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, İzmir, 2017,s.157

durdurulmalı ve yetkili makamdan bu yeni suç açısından bir arama kararının çıkartılması sağlanmalıdır. Aksi bir uygulama şekli aramayı ve elde edilen delilleri hukuka aykırı hale getirecektir (ABD- Carey, 1999; ABD- Walser, 2001 davalarındaki gibi)[371] Bu açıdan CMK 138/1. Fıkra AİHM içtihatlarıyla uyumlu hazırlandığı anlaşılmaktadır.

CMK'ya göre hukuka uygun bir arama ya da iletişimin tesbiti aşamasında elde edilen ve başkaca bir suçun ispat edilmesine yarayacak delilin ilgili suçun ispatında kullanılmasıyla ilgili hukuken bir sorun görünmemektedir. Konunun daha iyi anlaşılması açısından örnek verilecek olursa yağma suçu nedeniyle soruşturma yapılan bir şüphelinin bir failin evinde hukuka uygun olarak yapılan arama sırasında bulunan tabanca, yapılan incelemeler sonucunda o failin işlediği bir kasten adam öldürme suçu açısından delil olur. Benzer bir şekilde bir soruşturma ya da kovuşturmaya sırasında hukuka uygun yöntemler ile yapılan iletişimin dinlenmesinde failin başkaca bir suçu ya da suçları da işlediğine dair bilgi ve bulgular o suç ile ilgili delil değeri taşıyacaktır[372].

Kanun iletişimin denetlenmesi koruma tedbirinin uygulanması sırasında kuvvetli bir suç şüphesi olması durumunda katalog suçları belirleyerek somutlaştırmıştır. CMK 134. Maddeye göre tedbir kararının uygulanması sırasında tesadüfi delil elde edilmesi halinde CMK 138/1. Maddenin uygulanması gerekir[373]. Ancak bu tesadüfi suç unsurunun telekomünikasyon ile ilgilisinin bulunması halinde katalog suçlardansa CMK138/2. Madde uygulanırken katalog suçlardan olmaması durumunda özel hayatın gizliliği ve iletişim özgürlüğü ilişkisi dikkate alınmalıdır. Göksoy[374] bu durumu şu

[371] Nathan Judish, **Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations; Computer Crime and Intellectual Property Section Criminal Division**; Office of Legal Education Executive Office for United States Attorneys; https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009. pdf, s.5,90
[372] M. Kızılyar, 2014, s.78
[373] Osman Gazi Ünal, **Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma**, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2011, s. 125
[374] R. Göksoy, 2017, ss.157-158.

şekilde açıklamıştır; CMK md. 134 kapsamında bilgisayarlarda durağan halde bulunan verilerin bulunması kopyalanması veya el konulması durumunda bulunan edilen tesadüfi delillerin şahitlikten çekinme hakkı olanlara ait olması durumunda bile kanıtın saklanması ve Cumhuriyet Savcılığına bildirilmesi gerekir. Bunun nedeni tesadüfi delilin, iletişimin tespiti mahiyetinde akış halinde bulunan verilerden elde edilmemiş olmasıdır. Zira bu veriyi kaydeden kişinin bizzat şüpheli ya da şüphelinin kullandığı bilgisayar olup ayrıca iletişim geçmiş bir zamana ilişkin olması ve canlı bir iletişimin söz konusu olmamasıdır. Bu yüzden tanıklıktan çekinme hakkı olanlara ait olsalar bile bilgisayar aramalarında elde edilen bilgisayara kaydedilmiş, durağan haldeki elektronik postalarda suç unsuruna ait tesadüfi delillerin bulunması halinde deliller saklanmalıdır. Bilgisayarda durağan halde olmayan akış halinde verilerin toplanması sırasında elde edilen bir elektronik postada suç unsuruna rastlanması halinde bu suç unsuru katalog suçlardan biri değilse ya da tanıklıktan çekinme hakkı olanlara ait ise derhal yok edilmelidir. Bu nedenle kanunda açıkça ifade edilmeyen özel hayatın gizliliği ve iletişim özgürlüğü ilişkisi arasındaki bu ince ayrıma dikkat edilmesi gerekir.

d. CMK 134. Madde Kapsamında Getirilen Hukuki Düzenlemeye Aykırılık

Ceza Muhakemesi kapsamında bilgisayarlar için arama ve el koymaya yönelik düzenlenen tedbir CMK 134. Madde ile özel bir şekilde düzenlenmiştir. Bilgisayarların insan hayatına girişiyle birlikte birçok kullanım amacı ortaya çıkmış, o kişinin hem işi hem de özel hayatının bir parçası haline gelmiştir. Bu nedenle herhangi bir suç şüphesiyle arama yapılan bilgisayarlarda o suça ilişkin bilgilerin yanı sıra kişinin özel hayatına yönelik bilgilere de rastlanması yüksek olasılıklı bir durumdur. Yapılan aramaların kuralsızca bir şekilde gerçekleşmesi kişinin temel haklarından olan özel hayatın gizliliğinin ihlal edilmesine yol açabilir. Bundan başka bilgisayar aramalarında usulsüz bir yaklaşım sergilenmesi hem insanların temel haklarının zedelenmesine neden

olmakta hem de hukuka aykırı delillerin farklı amaçlar için kullanılmasına sebep olabilmektedir.

CMK 134. Madde kapsamında bilgisayarlarda, bilgisayar kütüklerinde ve bilgisayar programlarında yapılan arama, kopyalama ve elkoyma işlemlerinin nasıl yapılacağı ve gereken şartlar kanunun gerekçesinde de ana hatlarıyla ifade edilmiştir. Bu madde arama üzerine getirilen bir özel norm olup sadece "bilgisayarlarda, bilgisayar kütüklerinde ve bilgisayar programlarında yapılacak arama, kopyalama ve elkoyma işlemi"ni düzenlediğinden özel norm ve genel norm ilişkisi göz önünde bulundurulduğunda CMK 116. maddeye[375] göre yapılan bir arama kapsamında CMK 134. maddenin izni yoksa bu arama kapsamında araştırma yapılan yerlerdeki bilgisayarların aranması mümkün değildir[376]. Yani bu durumda CMK 116. Madde kapsamında yapılan bir aramada ele geçen bilgisayardaki verilerin kopyalanabilmesi, el konulabilmesi için CMK 134. Maddenin şartlarının yerine getirilmesi gerekir. Aksi takdirde yapılan arama usulsüz olacak, elde edilen deliller de hukuki bir niteliğe sahip olmayacaktır.

Ceza muhakemesinde delillerin temsil edici olabilmeleri ancak güvenilir olmalarıyla sağlanabilen bir özelliktir. Bu nedenle delil hukuka aykırı şekilde elde edilmemişse hukuki bakımdan çok önemlidir. Yani bilgisayar ve bilgisayar kütüklerinde ve programlarında CMK 134 çerçevesinde belirtilen usullere riayet edilmeden ele geçirilen delil kabul edilmeyecek, delil yasakları gereğince yok hükmünde sayılacaktır. Bu nedenle CMK 134. Madde kapsamında bir hukuki işlem yapabilmek için Cumhuriyet savcısının istemi ve hakim kararı alınması şarttır. Bununla birlikte CMK

[375]**CMK Madde 116** – *"(1) Yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe varsa; şüphelinin veya sanığın üstü, eşyası, konutu, işyeri veya ona ait diğer yerler aranabilir."*
[376]MV. Dülger, 2013, s.675

267. Madde[377] uyarınca hakim kararlarına itiraz edilmesi de mümkün hale getirilmiştir. 6526 sayılı kanun kapsamında bazı koruma tedbirleri için karar alınacak makam olarak ağır ceza mahkemesi belirlenmiş olsa da 134. Madde için bir değişiklik yapılmamıştır.

Bilgisayarların aranması ve verilere el konulmasına yönelik bir düzenleme hukuk sistemimizde bulunmasına rağmen dijital delillerin bütünlüğü ve güvenliği açısından özel bir düzenlemenin bulunmaması önemli bir eksikliktir. Bu tür deliller genel hükümlere tabidir ve bu durum gelişen teknoloji karşısında uygulanmanın sorun yaşamasına sebep olmakta, özellikle delil güvenliği açısından sorunlar yaratmaktadır. Hukuka uygun olmak şartıyla, maddi olayı ispata yarayacak her şeyin delil kabul edilmesi, bunlar arasında bir derecelendirmenin olmaması, yargılamada delil hiyerarşisinin dikkate alınmamasına neden olmaktadır. Mevzuatın teknolojinin çok gerisinde kalması uygulamada birçok sorunun çıkmasına, elde edilen delillerin güvenilirliklerin tartışılmasına neden olmuştur. Delillerin elde edilme aşamasında manipüle edilme ihtimalinin çok yüksek olması nedeniyle doktrin bu delillerin güvenilir deliller olarak kabul edilmemesi gerektiği düşüncesindedir. Türk Ceza muhakemesinde gelinen noktada dijital deliller "ikrar delili" niteliğine büründürülmüştür. Ancak bu deliller, "hukuka uygun süreçlerde olaya ilişkin maddi delillere ulaşmak için bir araç olarak kullanılmalı ve yalnızca onları destekleyici bir mahiyette olmadır".[378]

Bilgisayarlardan elde edilen delillerin bütünlüğü ve güvenliğinin ihlal edilmesi durumunda TCK'daki bazı suç tipleri oluşabilir. Konu bu açıdan ele alındığında, somut olaya göre, "haberleşmenin gizliliğini ihlal" (TCK m. 132), "özel hayatın gizliliğini ihlal" (TCK m. 134), "bilişim sistemine girme" (TCK m. 243), "bilişim sistemini engelleme, bozma", "verileri yok etme veya değiştirme" (TCK m. 244) suçları gündeme gelebilecektir. Bundan başka TCK'nın 281. maddesinde yer alan "suç delillerini yok

[377] CMK, **Madde 267 – "***(1) Hâkim kararları ile kanunun gösterdiği hâllerde, mahkeme kararlarına karşı itiraz yoluna gidilebilir."*
[378] S. Keskin Kiziroğlu ve diğerleri, 2013, ss.91-92

etme, gizleme veya değiştirme" suçunu işleme de gündeme gelebilir. Bununla birlikte sağlıklı bir delil güvenliği denetlenmesinin işlemediği bir sistemde yukarıda bahsedilen bir ihlalin varlığının tespiti de pek mümkün gözükmemektedir[379].

CMK 134. Maddede belirtilen usullere aykırı bir şekilde delil elde edilmesi ve şekle ilişkin usuli hataların basit hata olarak kabul edilmesi Anayasa'ya ve kanunlara aykırı bir durumdur. Sanığın evinde ya da iş yerinde yapılan aramalarda el konulan bilgisayar veya cep telefonları gibi dijital malzemeler üzerinde yapılacak incelemeler nihayetinde bilgi işlem merkezinde saatlerce ay da günlerce süren işlemden sonra bitmektedir. Bu verilerin güvenilirliği açısından hash değeri alınmış olsa bile bu aşamaların hiçbirinde sanığın ya da müvekkilinin katılmaması, yapılan incelemeler sırasında verilerin değiştirilmesine ya da yeni suç delilleri eklenmesine neden olabilmektedir. Bu nedenle bu cihazlardan elde edilen verilerin güvenliği ve kabul edilebilirliğinin sağlanması mümkün gözükmemektedir.

Adli bilişim bilgisayar incelemelerinde işletim sistemi, kullanıcı adı ve şifreye gerek olmamasına rağmen CMK 134. Maddede bilgisayarlara el konulabilmesinin şartlarından birinin şifrenin çözülememesi hali henüz kanundan kaldırılmış değildir. Bilgisayarlara el koyma şifrenin çözülememesinden dolayı değil, incelemenin uzun sürmesi durumunda gerekli olan bir uygulamadır. Bu nedenle kanundaki tezatlık giderilmelidir.

e. İletişimin Denetlenmesi Yoluyla Dijital Delil Elde Edilmesi

İletişimin Denetlenmesi tedbiri, pek çok temel hak ve özgürlüğe ciddi sınırlamalar getiren bir güvenlik tedbiridir. Özellikle de haberleşme hürriyeti ile özel hayatın gizliliği haklarıda doğrudan ciddi müdahale oluşturmaktadır. Bu tedbir, maddenin kapsamı bakımından üç ayrı tedbiri içermektedir. Bunlar (1) "şüpheli veya

[379] S. Keskin Kiziroğlu ve diğerleri, 2013, s.92

sanığın telekomünikasyon yoluyla iletişimi dinlenmesi, kayda alınması ve sinyal bilgilerinin değerlendirilmesi", (2) "şüpheli veya sanığın mobil telefonunun yerinin tespiti" ve (3) "Şüpheli ve sanığın telekomünikasyon yoluyla iletişiminin tespiti"dir.

İletişimin denetlenmesi tedbirine, ölçülülük ve son çare olma ilkeleri göz önünde bulundurularak, yalnızca "kanunda açıkça sayılan belli ağırlıktaki suçların işlendiğine dair kuvvetli şüphe varsa ve başka türlü delil elde etme imkanı yoksa başvurulmalıdır"[380]. Nitekim CMK m. 135/1'de de *"Bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir."* denilmektedir. Bu tedbir hem haberleşme hürriyetine hem de özel yaşamın gizliliğine çok ciddi müdahale oluşturacağından çok hassas bir biçimde uygulanmalı ve son çare olma niteliği gözden kaçırılmamalıdır.[381]

Dolayısıyla bu tedbir ancak (1) somut delillere dayanan kuvvetli suç şüphesinin bulunması halinde, (2) belli ağırlıktaki suçlarda, (3) ispatın neredeyse mümkün olmadığı istisnai hallerde uygulanabilir.

"Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi Ve Kayda Alınmasına Dair Usul Ve Esaslar İle Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev Ve Yetkileri Hakkında Yönetmeliğe" göre iletişim, *"Her türlü işaret, sembol, ses ve görüntünün ve elektrik sinyallerine dönüştürülebilen her türlü verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla*

[380] Devrim Aydın, **Ceza Muhakemesinde Deliller**, Yetkin Yayınları, Ankara 2014, s. 113.
[381] Erdener Yurtcan, **Ceza Yargılaması Hukuku,** Adalet Yayınevi, Ankara, 2018, s. 408.

iletilmesi, gönderilmesi ve alınması" anlamına gelir. Bu kapsamda sabit ya da mobil telefonlar üzerinden yapılan tüm görüşmeler, yazışmalar, görüntülü görüşmeler vb veri aktarımları iletişimin denetlenmesi yoluyla denetlenebilir.

Sinyal bilgilerinin değerlendirilmesi de, "İletişimin içeriğine müdahale niteliğinde olmayıp yetkili makamdan alınan karar kapsamında sinyal bilgilerinin iletişim sistemleri üzerinde bıraktığı izlerin tespit edilerek, bunlardan anlamlandırılan sonuçlar çıkarmak üzere gerçekleştirilen değerlendirme işlemleri"[382] olarak nitelendirilir.

Sanık/şüphelinin yerinin tespit edilmesi gereken durumlarda mobil telefonun yerinin tespiti yapılabilir. Sanık/şüphelinin yerinin tespiti kararı hakim ya da gecikmesinde sakınca bulunan hallerde cumhuriyet savcısı tarafından verilir. Mobil telefonun yerinin tespiti en fazla iki ay için uygulanabilir bir tedbirdir, en fazla 1 ay uzatılabilir. Her ne kadar CMK m.135/5 açıkça belirtmese de bu tedbir de, 135. Maddenin uygulama alan bulduğu katalog suçlar söz konusu ise uygulanabilir.[383] Yargıtay da aynı görüştedir:

"Somut olayda yakınan, evine girerek cep telefonunu evde unutan ve evin içini karıştırmış olan şüpheli ya da şüphelilerin belirlenerek, konut dokunulmazlığını bozma suçundan cezalandırılmaları istemiyle şikayette bulunmuştur. Cumhuriyet Başsavcılığı'nca konut dokunulmazlığını ihlal suçu ile ilgili olarak yapılan soruşturmada; yakınanın evinde bulduğunu iddia ettiği telefonun konut dokunulmazlığını bozma suçunu işleyen şüpheliye ait olabileceği düşüncesiyle, telefonu ve kartın sahibini belirlemek amacıyla Sulh Ceza Mahkemesinden bu telefonla yapılan son üç aylık görüşmelerin (arayan ve aranan dahil) HTS raporlarının tespitini istemiştir. Soruşturma konusu konut dokunulmazlığını bozma suçunu kimin işlediğinin

[382] Özbek ve arkadaşları, **Ceza Muhakemesi Hukuku**, Seçkin Yayınevi, Ankara, 2018, s. 389.
[383] Doğan Soyarslan, **Ceza Muhakemesi Hukuku**, Yetkin Yayınları, Ankara, 2018, s. 289.

belirlenmesi için, yakınanın evinde bulduğunu ileri sürdüğü ve eve giren kişiye alt olduğunu iddia ettiği cep telefonu ve sim kartının; abone adı, kimlik bilgileri, telefon numarası ve sim kart bilgilerinin işletmeci kurumlardan istenmesi için CYY'nin 135. maddesinin birinci fıkrasında yazılı bulunan 'iletişimin tespiti' kararına gereksinim bulunmamaktadır. Söz konusu bu bilgilerin, Cumhuriyet Savcısı'nın CYY'nin 160 ve 161. maddelerinde düzenlenen genel soruşturma yetkisi kapsamında, yargıç kararı olmadan, ilgili kurumdan istenmesi olanaklıdır."[384]

Yönetmeliğe göre mobil telefonun tespitinde süre, tedbir kararının Telekomünikasyon İletişim Başkanlığı'nda sisteme tanıtıldığı andan itibaren başlamıştır, bu süre kesintisiz bir biçimde devam eder.[385]

CMK m.135'te düzenlenen bir diğer tedbir de "İletişimin Tespiti" tedbiridir. 2014 yılında yeni bir fıkra olarak düzenlenerek kanuna eklenmiştir: *"(Ek: 2/12/2014-6572/42 md.) Şüpheli ve sanığın telekomünikasyon yoluyla iletişiminin tespiti, soruşturma aşamasında hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı, kovuşturma aşamasında mahkeme kararına istinaden yapılır. Kararda, yüklenen suçun türü, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, telefon numarası veya iletişim bağlantısını tespite imkân veren kodu ve tedbirin süresi belirtilir. (Ek cümleler: 24/11/2016-6763/26 md.) Cumhuriyet savcısı kararını yirmi dört saat içinde hâkimin onayına sunar ve hâkim, kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde kayıtlar derhâl imha edilir."*

İletişimin tespiti tedbirinde iletişimin içeriğine müdahale edilmez yalnızca iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişimdeki aramalar, aranmalar,

[384] Yargıtay 2. Ceza Dairesinin 25.06.2009 tarihli ve 2009/22575 Esas, 2009/31143 Karar sayılı kararı.
[385] 14 Şubat 2007 tarihli, 26434 sayılı "Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik", m. 12.

yer bilgileri ve kimlik bilgileri tespit edilir. Madde kapsamında düzenlenen diğer tedbirlerden farkı bu tedbirin geçmişe yönelik iletişimi (HTS raporu) tespit ediyor olmasıdır.

İletişimin denetlenmesi tedbirinin alındığı araçların iletişimi denetlenecek kişinin üzerine kayıtlı olup olmaması konusunda kanunda bir açıklık yoktur. Sanık ve şüphelilerin özellikle başka kişiler üzerine kayıtlı abonelikler oluşturduğu bilinmektedir. Bu tür durumlarda, abonelik sanık/şüpheli'den başka bir kişiye ait olsa dahi iletişimin denetlenmesi tedbirine başvurulması gerekir.[386] Sanık/Şüphelinin kullandığı aboneliğin sahibi de özel hayatına yönelen bu sınırlamaya katlanmak durumunda kalacaktır.

İspatın mümkün olmadığı istisnai halleri somutlaştırmak gerekirse, doktrinde soruşturma makamlarının suçun işlendiğine dair somut delil elde edebilmesi halinde iletişimin denetlenmesine başvuramayacağı ancak somut delil elde etmek mümkün değilse bu yola gidileceği savunulmaktadır.[387] Ancak, iletişimin denetlenmesi yoluna gidilmeden önce diğer tedbirlerin somut olarak denenip işe yaramadığının görülmesi şart değildir, bu diğer tedbirlere başvurulduğunda sonuç alınamayacağına ilişkin haklı bir beklenti olması ya da bu tedbirlere başvurulmasıyla ciddi tehlike altında kalınacağı fikri oluşmuşsa bu tedbirler hiç denenmeden de iletişimin denetlenmesi yoluna gidilebilir.[388]

Bununla birlikte elde birtakım somut delillerin bulunması durumunda da iletişimin denetlenmesi yoluna başvurulabilmektedir.[389] Örneğin Alman Federal Anayasa Mahkemesi, özel hayatın çekirdek alanına müdahale teşkil etmeyecekse izleme

[386] Yavuz, 2005, s. 249.
[387] Seydi Kaymaz, "Telekomünikasyon Yoluyla yapılan iletişimin denetlenmesinin bir koşulu olarak başka suretle delil elde etme imkanının bulunmaması", **Fasikül Hukuk Dergisi**, Yayın:2, Sayı: 3, Şubat 2010, s. 42. ; Hakan A. Yavuz, "Ceza Yargılamasında Bir Koruma Tedbiri Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi", **TBB Dergisi**, Sayı 60, 2005, s. 246.
[388] Yavuz, 2005, s. 247.
[389] Devrim Aydın, **Ceza Muhakemesinde Deliller**, Yetkin Yayınları, Ankara 2014, s. 114.

ve dinleme biçimindeki delil toplama yöntemlerine izin verilebileceğine karar vermiştir.[390]

İletişimin denetlenmesi kararı kural olarak ağır ceza mahkemesince oybirliğiyle alınır. Ancak gecikmesinde sakınca bulunan bir hal varsa Cumhuriyet savcısının kararıyla da iletişimin denetlenmesi kararı alınması mümkündür.

"İletişimin tespiti, dinlenmesi, kayda alınması" ve sinyal bilgilerinin değerlendirilmesi tedbirlerinin uygulanmasına ilişkin kararlarda Yönetmelik m.6/1 uygulanır: " *MADDE 6 – (1) İletişimin tespiti, dinlenmesi, kayda alınması veya sinyal bilgilerinin değerlendirilmesine ilişkin talepler ile hâkim ve Cumhuriyet savcısı kararlarında, aşağıda belirtilen hususlar yer alır:*

a) Soruşturma numarası veya kovuşturmaya geçilmişse mahkeme esas numarası,

b) Kararın hangi suçun soruşturulması için istendiği, bu suça ilişkin kuvvetli şüphe sebeplerinin neler olduğu,

c) Başka suretle delil elde edilmesi imkânının bulunmadığı hakkındaki açıklama, bilgi veya belgeler,

ç) Hakkında tedbir uygulanacak kişinin kimliği,

d) İletişim aracının türü ile numarası veya iletişim bağlantısının tespitine imkân veren kodu,

e) Tedbirin türü,

f) Tedbirin kapsamı,

[390] Björn Gercke, "Ceza Muhakemesine İlişkin Delil Elde Etme Önlemlerinin İçtimaı" (Çev. Y. Ünver), **Ceza Muhakemesi Önlemleri ve Özellikle Gizli Araştırma Önlemleri**, (ed. Yener Ünver), Seçkin Yayıncılık, Ankara, 2011, s. 278-279.

g) Tedbirin süresi."[391]

Bununla birlikte, mobil telefonun yerinin tespiti için verilecek kararda yalnızca mobil telefonun numarası ve tespit isteminin süresinin belirtilmesi yeterli olacaktır. Yargıtay'a göre de: *"...kolluk meciince belirtilen telefon hatları ile yapılan görüşmelerin hangi baz istasyonlarına ait olduğu ve tespit edilen baz istasyonlarından, 13.11.2008 günü 20.30 ile 21.15 saatleri arasında yapılan görüşmelerin bölgeli olarak arayan ve aranan olarak dökümlerine ait teknik bilgilerin ve görüşme yapan abonelerin kimlik bilgilerinin ve açık adreslerinin (nüfus cüzdanı fotokopisi, sürücü belgesi fotokopisi, abone sözleşmesi fotokopisi vb.) CD ortamında Telekomünikasyon İletişim Başkanlığı'ndan çıkarılmasına karar verildiği anlaşılmıştır. Anılan karar içeriğinde, belirtilen tarih ve saatler arasında sadece teknik bilgilerin, arayan ve aranan abonelerin kimliklerine ve adreslerine ilişkin bilgilerin ilgili kurumdan çıkartılmasına karar verilmiş; genel olarak belirtilen çevrede bulunan kişilerin ve kurumların, telefon görüşmelerinin dinlenmesine ya da iletişimlerinin tespitine ilişkin özel hayata müdahale oluşturacak ya da kişi hürriyetini kısıtlayıcı bir karar verilmemiştir".*[392]

CMK m. 135'te sayılan şartlara uygun olarak telekomünikasyon yoluyla yapılan iletişimin dinlenemesi ve kaydedilmesi suretiyle elde edilen deliller, hukuka uygun dijital delil niteliği taşıyacaktır. Bununla birlikte iletişim sürdürülürken, karşı tarafın iletişimi kaydetmesi durumunda bu delilin kabul edilip edilemeyeceğine ilişkin bir açık hüküm yoktur. Yargıtay ise bu durumda elde edilen dijital delillerin kabul edilebileceğine ilişkin kararlar vermiştir: *"Katılan sanıklar ile aynı ortamda ve telefonda yaptığı görüşmeleri cep telefonuna kayıt etmek suretiyle elde ettiği kayıtların, 5271 sayılı CYY'nın 135. Maddesi kapsamında değerlendirilmesi, bu bağlamda hakim*

[391] 14 Şubat 2007 tarihli, 26434 sayılı "Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik"
[392] Yargıtay 6. Ceza Dairesi, 04.10.2010 tarihli, 2009/11787 Esas, 2010/15266 Karar Sayılı Kararı.

kararı olmadığından bahisle hukuka aykırı kabul edilmesi olanaklı olmayıp, rüşvet istenmek suretiyle sanıklar tarafından kendisine karşı işlendiğini iddia ettiği suçla ilgili olarak, bir daha elde edilme olanağı bulunmayan kanıtların yetkili makamlara sunulmak amacıyla toplandığının, dolayısıyla hukuka uygun olduğunun kabulü gerekmektedir."[393]

Ayrıca şikayetçi/mağdurun durumun tespiti için kendi iletişim araçlarına ilişkin olmak kaydıyla iletişimin denetlenmesini talep etmesi de mümkündür. "Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı Ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik" m. 10/4 de, *"Bir soruşturma sırasında delil toplama kapsamında, somut olayın özelliğine göre maddî gerçekliğin araştırılması ve adil bir yargılamanın yapılabilmesi için zorunlu olduğu takdirde, açık rızasının bulunması ve iletişim aracının kendisine ait olması şartıyla şikâyetçinin iletişiminin tespiti Cumhuriyet savcısının yazılı kararıyla Başkanlıktan istenir"* demektedir. Bu tespit kararı, geçmişteki iletişimlerin tespitine ilişkin olarak da verilebilir.[394]

Diğer dijital delillerde olduğu gibi, iletişimin dinlenmesi yoluyla elde edilen kayıt biçimindeki deliller üzerinde bozulma ve değişiklik kolaylıkla gerçekleştirilebilecektir. Bu nedenle bu verilerin de tek başına delil olarak kullanılamayacağı ancak başka delillerle birlikte değerlendirilmesi gerektiği kabul edilmektedir.[395] Yargıtay da bu görüştedir: *"Sanıkların, iletişimin tespiti kararlarına dayanılarak dinlenen telefon görüşmelerinde bahsi geçen silah ve mermilerin ele geçmemesi nedeniyle niteliklerinin 6136 sayılı Yasa kapsamında ve atışa elveişli olup olmadıklarının saptanamadığı, üzerlerinde ve evlerinde yapılan aramalarda herhangi*

[393] Yargıtay Ceza Genel Kurulu, 21.06.2011 tarihli, 2010/5-187 Esas Sayılı, 2011/131 Karar Sayılı Kararı.
[394] Öztürk ve arkadaşları, **Nazari ve Uygulamalı Ceza Muhakemesi Hukuku**, Seçkin Yayıncılık, Ankara, 2020, s. 555.
[395] Aydın, 2014, s. 118.

bir suç unsuruna rastlanmadığı ve dolayısıyla savunmalarının aksine, içeriği maddi bulgularla desteklemeyen belirti delil niteliğindeki iletişim kayıtları dışında üzerlerine atılı suçu işlediklerine dair cezalandırılmalarına yeterli, kesin ve inandırıcı kanıt bulunmadığı gözetilmeden, atılı suçtan beraatları yerine yazılı şekilde mahkumiyet hükmü kurulması bozmayı gerektirmiştir".[396]

Yine diğer dijital deliller için belirtildiği gibi, iletişimin dinlenmesi yoluyla elde edilen haberleşme kayıtlarının bu konuda uzman görevliler tarafından toplanması ve bu hususta tutanak tutulması şarttır.[397] Bu tedbir uygulamada şu şekilde gerçekleşir: "Hakim ve savcı tarafından verilen dinleme kararının uygulanması için bu husus emniyete savcılıkça bildirilmekte ve emniyet ilgili biriminde 'üs' olarak nitelendirilen bir cihaz kurarak telekomünikasyon şirketinden, dinlenilmesi istenen telefonun üs ile irtibatlandırılmasını istemekte ve bu sağlandıktan sonra telefon polis tarafından dinlenmektedir."[398] Bu yolla elde edilen delillerin hem elde edilmesi hem saklanması hem de kayıtların tutanaklara geçirilmesi esnasında delillerin bozulmasına karşılık çok dikkatli olunmalıdır.

Sanık/şüpheli ile tanıklıktan çekilebilecek kişiler arasında gerçekleşen iletişim kayda alınamaz. Nitekim CMK m.135/3: "Şüpheli veya sanığın tanıklıktan çekinebilecek kişilerle arasındaki iletişimi kayda alınamaz. Kayda alma gerçekleştikten sonra bu durumun anlaşılması hâlinde, alınan kayıtlar derhâl yok edilir".

Yargıtay da *"Sanık hakkında mahkumiyet hükmü kurulurken delil olarak kabul edilen telefon dinleme kayıtları, dosya içindeki nüfus kayıtlarına göre sanık ile tanıklıktan çekinme hakkı bulunan kardeşleri sanık, tanık ve babası arasında yapılan görüşmelere ilişkin kayıtlar olup, kanun dışı elde edilmiş delil niteliğindedir.… Sanık*

[396] Yargıtay 8. Ceza Dairesi, 01.07.2009 tarihli 2009/4076 Esas ve 2009/10177 Karar sayılı kararı ve bu kararı onayan, Yargıtay Ceza Genel Kurulunun 09.11.2010 tarihli 2010/8-134 Esas ve 2010/217 Karar sayılı kararı.
[397] Aydın, 2014, s. 119.
[398] Yavuz, 2005, s. 254.

hakkında mahkumiyet hükmü kurulurken, delil olarak kabul edilen telefon dinleme kayıtları, dosya içindeki nüfus kayıtlarından da anlaşılacağı üzere, sanık İlhan ile 5271 sayılı CMK'nın 45. maddesi uyarınca tanıklıktan çekinme hakkı bulunan kardeşleri sanık Mükerrem, tanık Emrah ve babası sanık Karabey arasında yapılan görüşmelere ilişkin kayıtlar olup, kanun dışı elde edilmiş delil niteliğindedir. Kanun dışı elde edilmiş delillerle, T.C. Anayasası'nın 20, 38/6, AİHS'nin 6, 8 ve CMK'nın 217/2. maddesi uyarınca, ayrıca Yargıtay Ceza Genel Kurulu'nun 03.02.2006 gün, 2006/5MD-154 Esas-2007/145 Karar, 14.04.2006 gün, 2007/5MD-23 Esas-2007/167 Karar ve 22.01.2008 gün, 2007/5 MD-101 Esas-2008/3 Karar numaralı ilamı da dikkate alınarak, mahkumiyet yönünde hüküm kurulamadığı, dosya içeriğine ve oluşa göre, sanık hakkında elde edilen başka delillerin de maktulü öldürmesi için diğer sanık Mükerrem'i azmettirmediğini ya da fer'an katıldığını kabule ve mahkumiyete yeter nitelik ve derecede bulunmadığı gözetilmeden, sanığın beraati yerine yazılı şekilde mahkumiyetine karar verilmesi," demektedir.[399]

Son olarak, diğer tüm koruma tedbirleri gibi, iletişimin denetlenmesi tedbirinin de geçici ve orantılı olması gerekmektedir. Bu doğrultuda CMK m. 135/4: *"Birinci fıkra hükmüne göre verilen kararda, yüklenen suçun türü, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, telefon numarası veya iletişim bağlantısını tespite imkân veren kodu, tedbirin türü, kapsamı ve süresi belirtilir. Tedbir kararı en çok iki ay için verilebilir; bu süre, bir ay daha uzatılabilir. (Ek cümle: 25/5/2005 – 5353/17 md.) Ancak, örgütün faaliyeti çerçevesinde işlenen suçlarla ilgili olarak gerekli görülmesi halinde, hâkim yukarıdaki sürelere ek olarak her defasında bir aydan fazla olmamak ve toplam üç ayı geçmemek üzere uzatılmasına karar verebilir."* demektedir. Bu doğrultuda, iletişimin denetlenmesi tedbirine yalnızca bir süreliğine karar verilebildiğine göre bu süre sona erdiği anda tedbir de sona erer. Dolayısıyla tedbirin

[399] Yargıtay 1. Ceza Dairesi, 13.10.3009 tarihli, 2009/1721 Esas, 2009/5855 Karar sayılı kararı.

sona ermesinden sonra bu yolla elde edilecek dijital deliller de hukuka uygun delil olarak kullanılamayacaktır. Bu delillerin de CMK m. 137/3 kapsamında yok edilmesi gerekecektir: *"135 inci maddeye göre verilen kararın uygulanması sırasında şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da aynı maddenin birinci fıkrasına göre hâkim onayının alınamaması halinde, bunun uygulanmasına Cumhuriyet savcısı tarafından derhâl son verilir. Bu durumda, yapılan tespit veya dinlemeye ilişkin kayıtlar Cumhuriyet savcısının denetimi altında en geç on gün içinde yok edilerek, durum bir tutanakla tespit edilir."*

CMK m. 135/7, tedbir süresince dinlemenin iletişimin tarafları ve ilgililerinden gizli tutulması gerektiğini düzenlemektedir: "Bu madde hükümlerine göre alınan karar ve yapılan işlemler, tedbir süresince gizli tutulur." Bu doğrultuda tedbir sona erdiğinde taraflar ve ilgililer iletişimlerinin dinlendiğine ilişkin bilgilendirilmelidir. Bu bilgilendirme ancak soruşturma ve kovuşturmayı tehlikeye atmayacaksa yapılır.

Bu noktada, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma"yı düzenleyen CMK m.134 ile "İletişimin Tespiti, Dinlenmesi ve Kayda Alınması"nı düzenleyen CMK m.135 arasındaki farklara değinmekte de fayda vardır.

- CMK m. 134'te bilgisayarlara ilişkin olan bu tedbir bilgisayarların maddi varlığına yöneliktir. Ya doğrudan bu cihazlara el koyulur ya da içerisindeki veriler kopyaların ve dijital hallerine el koyulur. İletişimin tespiti tedbirinde ise uygulama genellikle başka bilgisayarlar üzerinden yapılır, suçun işlendiği cihazlara erişim çoğu zaman zorunlu değildir.

- CMK m. 135 yalnızca kanun maddesinde belirtilen katalog suçlarda uygulanabilen ikincil bir tedbirdir. CMK m. 134 için böyle bir sınırlama yoktur.

- İletişimin tespiti, denetlenmesi ve kayda alınması tedbirinde bir iletişimin varlığı zorunludur. Ancak bilgisayarlarda, bilgisayar programlarında ve kütüklerde arama, kopyalama ve el koymaya ilişkin tedbirde bilgisayarların bir iletişim için kullanılması zorunlu değildir.

- İletişimin tespiti denetlenmesi ve kayda alınması tedbiri bilgisayarların yanı sıra telefon faks vb iletişim araçları üzerinde de uygulanabilecektir. Bilgisayarlarda, bilgisayar programlarında ve kütüklerde arama, kopyalama ve el koyma tedbirinde bu uygulama yalnızca bilgisayar ortamında yapılabilir.

- İletişimin tespiti denetlenmesi ve kayda alınması bir süre için alınan bir tedbirdir, genellikle 1-2 ay gibi bir süreyle süreklilik gösterir. Ancak Bilgisayarlarda, bilgisayar programlarında ve kütüklerde arama, kopyalama ve el koyma tedbiri arama ve kopyalamanın kendisiyle sınırlıdır, belli bir sürede biter, süreklilik göstermez.[400]

Öğretide ve uygulamada iletişimin tespiti tedbirleri yoluyla elde edilen dijital delillerin delil olarak değeri bakımından bir görüş birliği yoktur. Bazı yazarlar yasaya uygun olarak elde edilmiş ve bozuma uğratılmamış dijital delillerin tek başına mahkumiyete esas olabileceğini savunurken[401], bazı görüşler de bu kayıtların bir belirti niteliği taşıdığını ve tek başına mahkumiyete esas olacak şekilde dayanmanın mümkün olmadığı savunmaktadır.[402] Şahbaz'a göre de, özellikle bu tedbir çerçevesinde ses kayıtlarının doğruluğu araştırılmalı, sanık/şüphelinin herhangi bir itirazında itiraz ciddiyetle ele alınmalı ve ancak bilimsel olarak doğruluğu kanıtlandıktan sonra bu

[400] Özbek ve arkadaşları, **Ceza Muhakemesi Hukuku**, Seçkin Yayınevi, Ankara, 2018.
[401] Şen, 2007, s. 122.
[402] Yasin Sezer, Ali İhsan İpek, Engin Parlak, **Adli ve Önleme Amaçlı İletişimin Denetlenmesi**, Seçkin Yayıncılık, Ankara, 2012, s. 166.

delillerden yararlanılmalıdır.[403] Yargıtay da bu ikinci görüşten yanadır: *"...sanığın suçsuz olduğuna ilişkin savunmasının aksine içerikleri tespit edilemeyen suça katılımını gösterir kanıt niteliğinde sayılamayan cep telefonu görüşme kayıtları dışında kuşkudan uzak kesin kanıt elde edilmediği gözetilmeden sanığın beraatına karar verilmesi gerekirken mahkumiyet hükmü kurulması yasaya aykırıdır."*[404]Bununla birlikte, bu delillerin tek başlarına kabul edilemeyecek olmalarını mutlak yorumlamak vicdani delil sistemiyle de bağdaşmayacaktır. Dolayısıyla hakim önüne gelen her olayda somut olaya bakarak bu dijital delillerin geçerliliğine karar verecektir.

f. Teknik Araçlarla İzleme Tedbiri Yoluyla Dijital Delil Elde Edilmesi

İletişimin denetlenmesi tedbirinin yanı sıra, teknik araçlarla izleme tedbiri de dijital delillerin elde edildiği bir koruma tedbiridir. CMK m. 140 bu tedbiri düzenlemektedir. 1. Fıkra *"Aşağıdaki suçların işlendiği hususunda somut delillere dayanan kuvvetli şüphe sebepleri bulunması ve başka suretle delil elde edilememesi hâlinde, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyeri teknik araçlarla izlenebilir, ses veya görüntü kaydı alınabilir"* demektedir. Bu kapsamda teknik araç ifadesi, "insanın görme ve işitme duyusunun algılama yeteneğinin sınırlarını aşmaya yardım eden her türlü teknik tertibatı" ifade eder.[405] Bu araçlar görüntü ve sesleri kaydetme, aktarma gibi özelliklere sahiptir. Bu araçlardan bir suçu aydınlatmak için dijital delil elde etmek için yararlanılmaktadır. Bununla birlikte haberleşme araçlarına vasıta niteliğinde araçlar sokarak dinleme tedbiri bu madde kapsamında değil, iletişimin denetlenmesi kapsamında değerlendirilecektir.[406]

Teknik araçlarla izleme tedbirinin uygulanması oldukça zor ve pahalıdır. Örneğin mikrofonla bir dinleme gerçekleştirilecekse konuşmanın yapılacağı yer

[403] İbrahim Şahbaz**, İletişimin Denetlenmesi ve Yasak Deliller**, Yetkin Yayınları, Ankara, 2009, s. 183.
[404] Yargıtay 8. Ceza Dairesinin 2.2.2009 tarihli, 2009/14950 Esas Sayılı, 2009/1140 Karar sayılı kararı.
[405] Öztürk ve arkadaşları, 2020, s. 580.
[406] Öztürk ve arkadaşları, 2020, s. 581.

belirlenecek ve daha sonra bu mekana dinlemeyi gerçekleştirecek bir mikrofon veya başka bir araç yerleştirilecektir. Bu işlemlerin gizli ve titizlikle yapılması gerektiği de göz önünde bulundurulduğunda pek çok kişinin yer aldığı iyi planlanmış bir organizasyon şart olmaktadır. Bu tedbir aynı zamanda ulaşım araçlarına takip cihazı yerleştirilmesi ve araçların bu yolla izlenmesi uygulamasını da içerir. Dolayısıyla kolluk görevlilerinin böyle bir uygulamaya gidebilmesi için CMK m.140 kapsamında bir karar alınması gerekir.[407]

Teknik araçlarla izleme tedbiri de iletişimin denetlenmesi tedbiri gibi "somut delillere dayanan şüphe" ve "başka yolla delil elde edilmememesi" şartlarına dayanır.[408] CMK m. 135/1 de, CMK m. 140 ile birlikte bu tedbir açısından da uygulanma imkanı bulacaktır. Ayrıca kanunda sayılan bu koşullar olmadan gerçekleştirilen izleme sonucunda özel hayatın gizliliği hakkı ihlal edilecek ve elde edilen deliller hukuka uygun delil niteliği taşımayacaktır.[409] Bu durumda CMK m. 140/4 uygulanacaktır: *"Elde edilen deliller, yukarıda sayılan suçlarla ilgili soruşturma ve kovuşturma dışında kullanılamaz; ceza kovuşturması bakımından gerekli olmadığı taktirde Cumhuriyet savcısının gözetiminde derhâl yok edilir."*

Yine bu tedbir, kanunda açıkça sayılan suçlar bakımından uygulama imkanı bulacaktır, aksi durumda bu suçlar dışında kalan bir suça ilişkin olarak toplanan dijital deliller CMK m. 140/4 kapsamında yok edilecektir. Teknik araçlarla izleme tedbiri açısından özellikli bir durum da CMK m. 140/5'te düzenlenmektedir: *"Bu madde hükümleri, kişinin konutunda uygulanamaz."* Dolayısıyla, bu tedbir hangi şartla olursa olsun kişinin konutunun izlenmesini içeremeyecektir.

[407] Özbek ve arkadaşları, 2018, s. 429.
[408] Öztürk ve arkadaşları, 2020, s. 580.
[409] Aydın, 2014, s. 125.

İlteişimin denetlenmesi tedbiri gibi, teknik araçlarla izleme tedbirinde de ağır ceza mahkemesinin oybirliğiyle alacağı bir karar aranmaktadır. CMK'nın ilk halinde iletişimin denetlenmesi tedbirinde öngürüldüğü gibi gecikmesinde sakınca bulunan hallerde bu teknik araçla izleme tedbirinin cumhuriyet savcısı tarafından alınabileceği öngörülmekteydi. 21.02.2014 tarih ve 6526 sayılı kanun 14. Maddeyle yapılan değişiklik bu tedbirin alınmasındaki koşulları ağırlaştırmış ve savcı kararıyla alınabilmesinin önüne geçmiştir. Yine bu değişiklikle teknik araçlarla izleme tedbirine bir süre sınırlaması getirilmiştir, CMK m. 140/3: *"Teknik araçlarla izleme kararı en çok üç haftalık süre için verilebilir. Bu süre gerektiğinde bir hafta daha uzatılabilir. Ancak, örgütün faaliyeti çerçevesinde işlenen suçlarla ilgili olarak gerekli görülmesi hâlinde, hâkim yukarıdaki sürelere ek olarak her defasında bir haftadan fazla olmamak ve toplam dört haftayı geçmemek üzere uzatılmasına karar verebilir."*

Ancak 140. Maddenin 2. Fıkrasında 2014 yılında yapılan değişiklik 2016 yılında 6763 sayılı kanunun 28. Maddesiyle geri alınmıştır. Yürürlükteki haliyle CMK m. 140/2: *"Teknik araçlarla izlemeye hâkim, gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından 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 kayıtlar derhâl imha edilir."* demektedir.

Son olarak, dijital delillerin değerlendirilmesinde açıklanmış bulunan "tesadüfen ele geçirilen delillerin değerlendirilmesi"'ne ilişkin esaslar hem iletişim denetlenmesi tedbiri hem de teknik araçlarla izleme tedbiri açısından da geçerli olacaktır.

g. Cumhuriyet Savcısının Genel Soruşturma Yetkisi Çerçevesinde Elde Edilen Dijital Deliller

Cumhuriyet savcısının CMK m.160 ve 161'e dayanan genel soruşturma yetkisi ve bu çerçevede yaptığı incelemeler ile de dijital delillerin elde edilmesi mümkündür. Yukarıda üzerinde durulmuş olan koruma tedbirlerinin dışında kalan durumlarda Cumhuriyet Savcısı bu yetkisine başvurabilecektir.[410] Özellikle de kişilerin mahremiyet alanında kalmayan, sosyal medyada alenen paylaştıkları veriler gibi alanlar temel hak ve özgürlüklere de dokunmadan dijital veri toplanmasını sağlayabilir. Bununla birlikte bankalardaki ve güvenlik kameralarındaki veriler de bu çerçevede toplanabilir.[411]

Bireysel nitelikte bir suçunun telekomünikasyon araçlarıyla işlenmesi söz konusu olduğunda, mesela tehdit suçunun telefon aramaları ve mesajlaşmaları yoluyla işlenmesi, bu iletişim hizmetini veren kurum ve kuruluşların yasalara uygun olarak kaydetmiş olduğu dijital kayıtlar da belirti delil olarak her zaman kullanılabilir. Bu deliller el koyma, bilgi ve belge isteme işlemine, bilirkişi veya keşif incelemelerine sebep oluşturabilir. Yargıtay da tehdit suçunun telekomünikasyon araçlarıyla işlenmiş olduğu bir somut olayda bu delillerin elde edilmesinde Cumhuriyet savcısının 160 ve 161. Maddelerinde düzenlenen genel soruşturma yetkisi olduğunu vurgulamıştır.[412] Ayrıca Yargıtay: *"CMK.nun 160. maddesinin 1. fıkrasında da Cumhuriyet Savcısı, ihbar veya başka bir suretle bir suçun işlendiği izlenimini veren bir hali öğrenir öğrenmez kamu davasını açmaya yer olup olmadığına karar vermek üzere hemen işin gereğini araştırmaya başlar. 2. fıkrasında 'Cumhuriyet Savcısı, maddi gerçeğin araştırılması ve adil yargılamanın yapılabilmesi için, emrindeki adli kolluk görevlileri marifetiyle, şüphelinin lehine ve aleyhine olan delilleri toplayarak muhafaza altına*

[410] Değirmenci, 2014, s. 387. ; Feridun Yenisey, Ayşe Nuhoğlu, **Açıklamalı Ceza Muhakemesi Kanunu**, Cilt1, Beta, İstanbul, 2013, s. 1353.
[411] Resul Göksoy, **Ceza Muhakemesinde Dijital Delillerin Elde Edilmesi ve Güvenilirliğinin Sağlanması**, Seçkin Yayıncılık, Ankara, 2019, s. 177.
[412] Yargıtay 8. Ceza Dairesi, T.29.11.2006, K.2006/17007.

almakla ve şüphelinin haklarını korumakla yükümlüdür'anılan yasanın 161. maddesinin 1. fıkrasında ise 'Cumhuriyet Savcısı, doğrudan veya emrindeki adli kolluk görevleri aracılığı ile her türlü araştırmayı yapabilir; yukarıdaki maddede yazılı sonuçlara varmak için bütün kamu görevlilerinden her türlü bilgiyi isteyebilir. Cumhuriyet Savcısı, adli görevi gereğince nezdinde görev yaptığı mahkemenin yargı çevresi dışında bir işlem yapmak ihtiyacı ortaya çıkınca, bu hususta o yer Cumhuriyet Savcısından söz konusu işlemi yapmasın: ister.' 2. fıkrasında da 'Adli kolluk görevlileri, el koydukları olayları, yakalanan kişiler ile uygulanan tedbirleri emrinde çalıştıkları Cumhuriyet Savcısına derhal bildirmek ve bu Cumhuriyet Savcısının adliyeye ilişkin bütün emirlerini gecikmeksizin yerine getirmekle yükümlüdür.' 3. fıkrasında 'Cumhuriyet Savcısı, adli kolluk görevlilerine emirleri yazılı; acele hallerde, sözlü olarak verir. (Ek cümle; 25.05.2005-5353/24 md) Sözlü emir, en kısa sürede yazılı olarak da bildirilir. 4. fıkrasında 'Diğer kamu görevlileri de, yürütülmekte olan soruşturma kapsamına ihtiyaç duyulan bilgi ve belgeleri, talep eden Cumhuriyet Savcısına vakit geçirmeksizin temin etmekle yükümlüdür.' Hükümleri yer almaktadır. Bu durumda dosya münderecatı ve yasal düzenlemeler karşısında C. Savcısının, iletişimin tespiti uygulamasını 5271 sayılı CMK.nun 160 ve 161. maddelerinde öngörülen genel soruşturma yetkisi çerçevesinde değerlendirerek çözüme kavuşturması olanaklıdır." demektedir.[413]

Yine Yargıtay'ın önüne gelen bir dosyada basit yaralama suçuna ilişkin olarak Cumhuriyet Savcısının CMK m.160 uyarınca dosyadaki diğer delillerle birlikte dijital delillerden yararlanması gerektiği ortaya koyulmaktadır: *"İncelenen somut olayda, müştekinin, aralarında boşanma davası devam eden ...'ın ile ortak çocukları olan mağdurlar ... ve ....'ın anneanneleri olan ... tarafından dövüldüğü, hakaret edildiği ve kötü muamelede bulunduğunu iddia ederek şikayetçi olduğu, dosyada bulunan dijital veri çözümleme raporunda mağdur ...'ın erkek kardeşi olan diğer mağdurun anneannesi*

[413] Yargıtay 8. Ceza Dairesi, E. 2007/8616, K. 2007/8160, T. 23.11.2007.

tarafından dövüldüğüne dair beyanının bulunması, boşanma davasında görev alan eğitim psikoloğu-bilirkişinin görüş yazısında da, anne ve anne yakınlarının çocuklara şiddet uygulamalarına son verilmesi amacıyla tedbirlerin alınması, çocukların babalarının yanında kalmasının uygun olacağına dair açıklamalara yer verilmesi, Adli Tıp Kurumu raporlarına göre mağdurlarda basit tıbbi müdahale ile giderilebilir nitelikte yaralanmaların bulunduğunun belirtilmesi karşısında, CMK'nın 170/2. maddesi uyarınca dosyadaki mevcut delillerin iddianame düzenlenebilmesi ve suçların işlendiği hususunda yeterli şüphe oluşturduğu açıktır."[414]

2. Yabancı Hukuk Sistemlerinde Dijital Delillere İlişkin Kurallar

Avrupa ülkelerinde dijital delillerin değerlendirilmesiyle ilgili kapsamlı ve özel bir yasa yer almamaktadır. Bununla birlikte konuyla ilgili sivil, ticari ve diğer ceza hukuku yasaları içerisinde birtakım düzenlemeler yapılmıştır. Dijital delillerle ilgili arama ve el koyma faaliyetlerine yönelik Birleşik Krallık'ta yürürlükte olan Polis ve Suç Delili Kodu (Police and Criminal Evidence Code), Belçika yasalarında bulunan Bilgisayar Suçları Yasası (Law on Computer Crimes), ABD'de Federal Delil Kuralları (Federal Rule of Evidence-FRE), İngiliz yargılamasında ACPO'nun yayınlamış olduğu Dijital Deliller için En İyi Uygulama Rehberi dikkate alınırken, Almanya ve Fransa gibi bazı ülke hukukunda dijital delillerle ilgili olarak delillerin serbest değerlendirilmesi ilkesi göz önüne alınmaktadır.

ABD'de FRE, genel olarak delillerin doğrulanması meselesinde sözkonusu delilin kabul edilebilmesi için gerekli bir aşamadır. Bu amaç doğrultusunda dokuz farklı doğrulama metodu öngörülen FRE'ye göre delili öne süren tarafın bu 9 farklı metottan

[414] Yargıtay 18. Ceza Dairesi, E. 2019/6269, K. 2019/12955, T. 24.9.2019.

biri ya da birden fazlasıyla delilinin doğruluğunu göstermesi yükümlülüğü bulunmaktadır[415].

FRE kapsamında ele alınan doğrulama metotları çerçevesinde bir tanığın teşhis edilmesi, bir kişinin fiziki özelliklerinin tarif edilmesi, uzman incelemesi olmaksızın bir el yazısının tanınması gibi bir delilin ilk bakışta ispat etmek istenen "şey" olup olmadığını belirleyecek örneklerdendir. FRE kurallarına göre doğrulama delilin ispat kuvvetini etkilememekte, bir tanığın doğrulanması tanığın söylediklerinin de doğru olacağı anlamına gelmemektedir. Dijital delillerin doğrulanması aslında basit ve yüzeysel bir doğrulamanın yerine verilerde herhangi bir değiştirmeye veya ekleme, verilerin kime ait olduğunun tespiti önem taşımaktadır. Bu nedenle FRE'nin getirdiği doğrulama kuralları dijital deliller konusunda yetersiz kalabilmektedir[416].

Anglosakson hukuk sisteminin etkisinde olan ABD'de ceza yargılaması genellikle çok sözlülüğe dayanır. Bu nedenle, FRE'nin pekçok kuralı da beyanlar ve yargılamadaki kişiler üzerinde yoğunlaşsa da az miktarda da olsa belge ve belirtilere ilişkin kurallar da mavcuttur. FRE'nin 1001. maddesidoğrultusunda bunlar yazı, kayıt ve fotoğraf olarak üçe ayrılmıştır. FRE'nin 1002. maddesi doğrultusunda federal kanunla aksi belirtilmediği müddetçe yazı, kayıt ya da fotoğrafların orijinal olduğu ispat edilebilmeli, 1003. kurala göre orijinallikle ilgili şüphe varsa ya da koşullar ikinci kopyanın kabulünü haksız hale getirmiyorsa, ikinci kopyanın da delil olarak kabul edilebileceği bildirilmektedir. Dublikasyon kanıtın yargılamada kabul edilebilmesi dijital delillerin kullanımını kolaylaştıran bir yaklaşım olmaktadır. FRE 1004. kuralına göre; "*orijinalinin, kötü niyetli haller dışında, kaybolması ya da yok olması, hiçbir adli yöntem ile elde edilememesi, taraflardan birinin kontrolünde olduğu için getirilmemesi*

[415] Steve Goode, "Admissibility of Electronic Evidence", **The Review of Litigation 2009,** 29(1), s. 8
[416] Leah Voigt Romano, "VI. Electronic Evidence and the Federal Rules", **Loyola Los Angles Law Review 2005,** 38, ss.1745 -1802

gibi hallerde delilin kabul edilebilirliği açısından eşyanın orijinal olması aranmayacaktır."[417]

ABD ceza muhakemesi hukuku, bilgisayar kayıtlarını delil olarak kabul eden bir hukuk sistemidir. Federal Delil Kanunun 802. maddesi, duyumun delil olamayacağını belirtmiş ancak istisnalarını da saymıştır. Federal Yüksek Mahkemenin 10. Dairesi, duyumun delil kabul edilebilmesi için öncelikle bilgisayar kayıtlarının özgünlüğünün sağlanması için oluşturulan rutin bir usul dâhilinde tutulmuş olması, ikincisi bu kayıtların doğruluklarının temin edilmesi gibi makul bir gayret gösterilmesi, üçüncüsü ise bu kayıtların sadece bir duyumdan ibaret olmaması gerektiğine karar vermiştir[418].

Federal Delil kanununun 803/6 fıkrasına göre düzenli yapılan faaliyetler ve iş nedeniyle tutulan kayıtlarla ilgili tutulan veriler delil olarak kullanılabilmektedir. Bu açıdan değerlendirildiğinde günlük iş akışı içinde kaydedilen, bir dava beklentisi ile oluşturulmamış bilgisayar kayıtlarının tanık ifadesi ile desteklenmesi verileri delil haline getirecektir. Ayrıca, 803/8.fıkrasına göre de resmi kurum kayıtları delil olarak kabul edilmektedir. Federal Yüksek Mahkemesinin 9. Dairesi, polis bilgisayarından çıktı alınarak sunulan sohbet içeriklerinin delil olarak sunulmasını kabul etmiştir[419].

ABD Federal Usul Kanunun 901/a fıkrasına göre bir delili sunan tarafın bu delilin özgünlüğünü ispat etmesi yükümlülüğü bulunmaktadır. Ancak burada kanun bilgisayar delillerinin hiçbir şekilde değişmezliğini ispat etmekten ziyade olaydaki kayıtların değiştirilmediğini ve doğru olduğunu ispat etmek gerekmektedir. ABD mahkemeleri, dijital delillerin değiştirilme ihtimalinin yüksekliği nedeniyle yapılan her itirazı kabul etmemekte dijital delilin karara esas alınmaması için daha özel bir sebep arama yolunu benimsemektedir. Bu nedenle ABD mahkemelerinde dijital delillerin

[417] Uğur Kaynakçıoğlu, **Ceza Muhakemesinde Dijital Deliller**, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, 2015, s.84
[418] N. Judish, 2009, ss.191-193
[419] N. Judish, 2009, s.197

değiştirilmiş olma ihtimali sadece delilin kabul edilebilirlik seviyesinde bir değişikliğe yol açacak, kabul edilebilirliğinde bir etki oluşturmayacaktır. ABD'de dijital delillerin özgünlüğü ispat edilirken genellikle bir uzmandan da faydalanılır. Ancak bu uzman her zaman bilişim alanında yetkili olması da gerekmez, burada özellikle delil olarak sunulan verilerin kayıt edilmesi, bu veri programını kullanabilen biri olabileceği gibi verilere el konulduğunda orada bulunan şahitlik yapacak bir kişi de olabilmektedir[420].

Almanya'da ceza muhakemesi açısından delil serbestisi esas alındığından mahkemeye her tür delil sunulabilir, dijital deliller de bu hükme dâhildir. Almanya'da dijital delillerle ilgili kararlar Almanya Ceza Usul Kanunu (Strafprozessordnung[StPO]) içindedir. Polis, şüpheliye ya da üçüncü kişilere yönelik üst, eşya, ev, işyeri ve onlara ait diğer yerleri hakim kararıyla acil durumda ise savcı kararıyla arayabilir ve eşyaya el koyabilir. StPO'da dijital delillerle ilgili özel bir arama ve el koymaya ilişkin hüküm bulunmadığından genel arama ve el koyma kuralları dijital deliller için de geçerlidir. Arama bittikten sonra, istenirse aramanın sebebi ve aramaya sebebiyet veren suçu gösteren yazılı bir belge verilebilmektedir. Elkonulan eşyanın iade edilmesiyle ilgili bir yükümlülük maddesi ve elkonulamayacak eşyanın listesi de bulunmaktadır. Katalog suçlar bakımdan hukuki makamlara bireysel verilerin birbiriylleriyle karşılaştırılması imkanı sunan uygulama da bulunmaktadır. Kişisel verilerin değerlendirmesi kararı mahkeme ya da acil hallerde savcı tarafından verilebilir[421].

Avustralya'da, doğrudan delillere yönelik olan "1995 tarihli Delil Kanunu (Evidence Act 1995)", dijital delillerin kullanımını kolaylaştırma adına da bazı maddelere sahiptir[422]. 1914 tarihli "Milletler Topluluğu Suçlar Kanunu" (The Commonwealth's Crimes Act 1914 [CCA]) ceza muhakemesine yönelik genel düzenlemelerin bulunduğu kanun olup dijital delil elde etmede kullanılan genel

[420] N. Judish, 2009, s.201-202
[421] U. Kaynakçıoğlu, 2015, ss.79-83
[422] Evidence Act 1995, http://www.austlii.edu.au/au/legis/cth/consol_act/ea199580/.

düzenlemeleri içermektedir[423]. Özellikle bu kanunun 3. maddesinde yer alan veri (data) ve veri depolama aygıtı (data storage device) ile "bilgisayarda tutulan veri" (data held in a computer) ile ilgili tanımlamalar dijital delillerin sınıflandırılmasında önemli kolaylıklar sağlamaktadır[424].

"Avustralya'da CCA 3E maddesine göre", makul sebeplerle bir mülkte arama yapılabilir. Bu aramada delil olabilecek materyal açısından bilgisayarlar ve veri depolama aygıtları da arama kararı kapsamına girebilir. CCA 3K ve 3L maddesine göre özellikle elektronik aygıtlar için aramaya esas olan eşya incelenme amacıyal gerekli cihazlar arama yerine getirilmelidir. Verilerden delil olabilecek materyal mülke getirilen elektronik aygıtların yanı sıra mülkün sahibinin yazılı izniyle mülkteki başka bir elektronik aygıt ile kopyalaması yapılabilir. Kopyalanmasının pratik olmaması ya da delil olabilecek materyalin CCA 3L/2-b hükmünde belirtilen şekilde belgeye dönüştürülememesi halinde materyale elkonulabilmekte, materyal kopyalandıktan sonra en kısa sürede iade edilmektedir[425].

Anglosakson hukuk sistemi uygulanan İngiltere'de ceza muhakemesi kanunu bulunmamaktadır. Dijital deliller, İngiliz ceza yargı sisteminde kabul edilen delillerdendir. Delillere ilişkin temel kurallarla dijital deliller arasında önemli bir farklılık yoktur. Bununla birlikte; dijital delil elde edilmesine yönelik İngiliz Polis Teşkilatı (Association of Chief Police Officers [ACPO]) "Bilgisayar Temelli Deliller için Uygulama Rehberi" (Good Practice Guide for Computer Based Evidence)'ni kullanmaktadırlar. Mahkemelerde olaylar incelenmesi sırasında bu rehberdeki ilkeler dijital delillerin sağlamlığının ve güvenilirliğinin denetiminde etkilidir. Öncelikli olarak ele geçirilen delillerin ele geçirildiği andan itibaren hakim önüne çıkana kadarki süreçte ne eksik ne de fazla olduğu yani hiçbir değişiklik olmadığı iddia makamınca

[423] The Commonwealth's Crimes Act 1914, http://www.austlii.edu.au/au/legis/cth/consol_ act/ca191482/.
[424] O.G. Ünal, 2011, s.73
[425] U. Kaynakçıoğlu, 2015, ss.90-91

ispatlanmalıdır. Bu nedenle araştırmalar kopyalar üzerinde yapılmalı, veriyi inceleyen üçüncü kişilerin de aynı sonuca ulaşması için verilerin orjinalliği bozulmamalıdır[426].

Hollanda ceza muhakemesi hukukuyla ilgili kurallar "Hollanda Ceza Muhakemesi Kanunu (Wetboek van Strafvordering [WS])"[427] içerisinde yer almaktadır. Bilgisayarlarda yapılan aramalar genel arama hükümleri çerçevesinde (WS 96b, 96c, 97, 110), arama sonucunda bulunan verilerin depolanmış bulunduğu aygıtlara elkonulması da genel elkoyma hükümleri uygulanarak (WS 95, 96, 96a, 104) yerine getirilmektedir. Veriler mal olarak kabul edilmediğinden elkonulamamaktadır. Bu sorun özellikle çocuk pornografisi veya virüs programı içeren verilerde Bilgisayar Suçları II Kanunu ile işlem yapılmakta öncelikle veriler kopyalanmakta ve aslı ya silinmekte (354. Madde hakim emriyle) ya da şifrelenerek erişimin engellenmesi sağlanmaktadır. Verilerin şifreli olması halinde veri sahibinin şifreyi kaldırması ya da şifreyi teslim etmesi (WS 125k) istenebilmektedir (WS 125o)[428].

"İsviçre'de ceza muhakemesi kuralları, "İsviçre Ceza Usul Kanunu (Schweizerische Strafprozessordnung [SStPO]/Code de procédure pénale suisse [CPPS]" ile federal düzeyde bir kurallar bütününden oluşmaktadır. İsviçre ceza muhakemesi sisteminde dijital delillere ilişkin temel kurallarda bulunmaktadır. İsviçre'de de her tür delil mahkemece kabul edildiğinden (SStPO/CPPS 139/1), dijital deliller de ceza yargılamasında kullanılmaktadır. Ancak delil serbestisi ile getirilen bu deliller hâkimin vicdani kanaati ile ölçülerek hükme konu edilebilmektedir. Arama (SStPO/CPPS 241/3) ya da elkoyma (SStPO/CPPS 263/3) savcı kararı ile birlikte acil hallerde polislerin de yetkisindedir Bu arama hem doğrudan belgelere de hem de kayıtlara yönelik olabilmektedir. İmkân olması halinde bilgisayara ilişkin verilerin

[426] ACPO Good Practice Guide for Computer Based Evidence, http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf.
[427] Wetboek van Strafvordering, http://www.wetboek-online.nl/wet/Wetboek%20van%20Strafvordering.html.
[428] Bert-Jaap Koops, "Cybercrime Legislation in the Netherlands", **Electronic Journal of Comparative Law 2010,** 14(3), s. 17, http://www.ejcl.org/143/art143-10.pdf. ss.18-20

kopyalanması yapılabilmektedir. Bu aramalara, ilgili kayıtların gizlilik hakları çerçevesinde itirazlar yapılabilmekte bu durumda kayıtların bulunduğu aygıt mühürlenmektedir (SStPO/CPPS 248). Mahkemenin bir ay içindeki karara göre materyalle ilgili işlem sürdürülebilmektedir[429].

3. Dijital Delillere İlişkin Uluslararası Kurallar

Dijital delillerin yargılamada kullanılması adına uluslararası alanda birtakım çalışmalar yapılmaya başlanmıştır. Özellikle elektronik delillerin toplanması aşamasında dikkat edilmesi gereken en önemli hususun kişisel verilerin korunması ilkesi ve özel hayatın gizliliği hakkına yönelik "Birleşmiş Milletler (BM) İnsan Hakları Evrensel Beyannamesi"nin 12. Maddesinin yanı sıra "BM Medeni ve Siyasi Haklara Dair Uluslar arası Misak"ın 17. maddesi, "BM'nin "Kişisel Verilerin Korunmasına Dair İlke Kararları", OECD'nin çeşitli tarihlerde çıkartmış olduğu ilke kararları, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi, Avrupa Konseyince çıkartılan "Kişisel Verilerin Korunmasına Dair Avrupa Konseyi Sözleşmesi" gibi birçok metinde özel hayatın gizliliği ve kişisel verilerin korunması güvence altına alınmıştır[430].

Devletlerin maddi ve usul hukuku açısından yeknesak bir ceza sistemine sahip olabilmesi içim etkili bir adli yardımlaşma sisteminin kurulmuş olması gerekir. Ulusal bir tehdit olmaktan çıkıp tamamen uluslararası suç haline gelen bilgisayar ve bilişim teknolojileri aracılığıyla işlenen suçlarda dijital delillerin ele de edilebilmesi ve etkin mücadele amacıyla "Avrupa Siber Suç Sözleşmesi" kaleme alınmış ve 1 Temmuz 2004 tarihinde yürürlüğe girmiştir. Ayrıca, bilişim sistemleri vasıtasıyla işlenen ırkçı ve yabancı düşmanı eylemlerin suç haline getirilmesine yönelik çalışmalar sonucunda

[429]Bertrand Perrin, Marc Rémy, Romain Roubaty, "Electronic Evidence in Swiss Criminal Procedure", **Digital Evidence and Electronic Signature Law Review2011**, 8, ss.72-74.
[430] M. Özen, G. Özocak, 2015, s.72

Avrupa Siber Suç Sözleşmesi'ne Ek Protokol 1 Mart 2006 tarihi itibariyle yürürlüğe girmiştir[431].

IOCE (International Organization on Computer Evidence) organizasyonu G8 Konferansında dijital delillere yönelik bir takım standartlar önermiştir. Bunlar:

- Dijital delillere el konulduğunda, yapılacak işlemler delili değiştirmemelidir.

- Bir kişinin dijital delilin orijinal haline ulaşması zorunlu ise o kişinin mutlaka adli yetkisinin olması gerekir.

- Dijital delillere elkoyulması, ulaşılması, depolanması ve aktarılmasına ilişkin tüm hareketler tamamen belgelenmeli, korunmalı ve incelemeye açık bulunmalıdır.

- Dijital delili elinde bulunduran kimse dijital delille ilgili yapılacak tüm işlemlerden sorumlu olmalı ve bu prensiplere uygun davranmakla mükellef olmalıdır[432].

IOCE'ya göre dijital delilin incelemesini yapacak kişi tüm sorumluluğu üstlenmeli ve delilin bütünlüğünün bozulmaması için özen göstermelidir. Dijital delillerin doğrulanabilmeleri ve güvenli bir şekilde hukuki süreçlere ışık tutabilmeleri için dijital delillerin tabii olduğu/olacağı süreçlerin hepsinin ayrıntılı olarak belgelenmesi ve bu belgelerin de aleni olarak incelemeye açılması gerekir. IOCE'nin belirtmiş olduğu bu standartlar 1999 yılında yapılan Uluslararası Yüksek Teknolojili Suçlar Konferansı'nda (International Hi-Tech Crime Conference) onaylanmıştır[433].

"Avrupa Konseyi Siber Suçlar Sözleşmesi (Council of Europe Cyber Crime Convention)" (Budapeşte Anlaşması) 2001 yılında çıkartılan dijital delillerle ilgili ilk

---

[431] Merve Erdem, Gürkan Özocak, "Sınıraşan Bir Suç Olarak Siber Suçlarla Mücadelede Uluslararası İşbirliği", **Akademik Bilişim 2017 (AB2017) Bildiriler Kitabı,** Şubat 2017, 1-7

[432] Peter Sommer, **Digital Evidence, Digital Investigation and E-Disclosure: A Guide to Forensic Readiness for Organizations**, Security Advisers and Lawyers, Information Assurance Advisory Council, 2012, http://www.iaac.org.uk/_media/DigitalInvestigations 2012.pdf.

[433] Forensic Science Communicatons, **Digital Evidence: Standart and Principles,** http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/,

bağlayıcı hukuki metindir. Bu sözleşme üye ülkelerle birlikte birçok ülkeden de destek görmüş ve imzalanmıştır. Siber Suçlar Sözleşmesi bilgisayar ve teknolojik cihazların kullanımı ile işlenen suçlara ilişkin uluslararası bir mücadele anlayışına yönelik yapılması gerekenleri ifade eden bir sözleşmedir. Avrupa Konseyinin 1995 yılında yayınladığı 95/13 sayılı tavsiye metni ve açıklayıcı genelgesine göre; dijital delillerle ilgilenmek için delilin birliğini ve doğruluğunu temin eden ve yansıtan özel usul ve teknik metotların geliştirilmesi gerekir. Belge delillerine ilişkin genel hukuki kurallar benzer olarak elektronik belgeler için de uygulanmalıdır. Açıklayıcı genelge ise elektronik belgelerin kağıt belgelerden farklı olduğunu vurgulamış ve bu tür belgelerin okunabilmeleri için özel donanım ve yazılımların olması gerektiğine ve bu sebeple gözle fark etmenin mümkün olmayacağı tahriflerin olabileceğini bildirmiştir[434].

Sözleşme, içerik bilgileri ve veri trafiği ilgili önemli düzenlemeler yaparak özellikle verilerin korunmasına yönelik düzenlemeler yapmıştır. Sözleşmenin 19. maddesi durağan veya saklı verilerin aranması, 20. Maddesi verilerin toplanması, 21. Maddesi de içerik verilerinin takibiyle ilgilidir. Sözleşmenin 19. Maddesi gereğince saklanmış bilgisayar verilerinin aranması ve bunlara el konulmasında sözleşmeyi imzalayan devletlerden her biri, bilgisayar sisteminin bir bölümü veya tümünde ve saklanmış bilgilerde ayrıca veri depolama birimlerinde arama ve bunlara erişme yetkisine sahip olmak için düzenlemeler yapması gerekir. Sınır ötesi sistemlerde arama ve elkoyma uluslararası işbirliği hükümlerine göre yürütülecektir. Sözleşmede elektronik posta sunucularındaki verilerin niteliğiyle lgili değerlendirme yapılmamış bu konu sözleşmeci devletlerin kendi hukuk sistemlerinde düzenlenmesi gerektiğini göstermiştir. Zira bazı ülkelerde bu tür veriler akış halinde veri olarak kabul edilirken bazı ülkelerde ise saklanan veri olarak kabul edilmektedir. Arama işleminde de ilgili kişinin bilgilendirilmesi de sözleşmede düzenlenmemiştir. Sözleşmeye göre verilere

[434] P. Sommer, 2012, s.43-44.

elkoyma yetkisi verilerin kopyalarının alınması mümkün olmadığında kullanılmalı veya bazı verilerin kurtarılması gereken durumlarda yerine getirilmelidir. Sonuç olarak Sözleşmeye göre, bu işlemelerin ancak bir suç soruşturması kapsamında yapılabileceği, alınacak tedbirlerin uluslararası insan hakları sözleşmelerinden kaynaklı yükümlülükler göz önünde bulundurularak uygulanabileceği, kamu yararı ve adaletin sağlıklı şekilde işletilmesi için üçüncü şahısların yetki, sorumluluk ve hakları da ihlal edilmemesi gerektiği anlaşılmaktadır[435].

III. TÜRK CEZA MUHAKEMESİ KAPSAMINDA DİJİTAL DELİLLERİN DEĞERLENDİRİLMESİ

Anayasa'nın 138. Maddesine göre "*Hâkimler, görevlerinde bağımsızdırlar; Anayasaya, kanuna ve hukuka uygun olarak vicdanî kanaatlerine göre hüküm verirler."* Diğer yandan CMK 217. Maddeye göre de *"Hâkim, kararını ancak duruşmaya getirilmiş ve huzurunda tartışılmış delillere dayandırabilir. Bu deliller hâkimin vicdanî kanaatiyle serbestçe takdir edilir."* Hükümleri gereğince, ceza yargılamalarında delillerin serbestliği ilkesi ve hâkimin vicdani kanaati esas alınmaktadır.

Hakimin vicdani kanaati, "maddi uyuşmazlığı çözmeye yetkili makam" olarak muhakeme faaliyetinin sonucunda, aklını rehber ederek hukukun koyduğu usul ve esaslar dahilinde, "maddi olayın oluş biçimine dair kendi açısından şüpheye yer vermeyen" bir kanaat şeklidir. Mutlak gerçeğin geçmişte kalması nedeniyle maddi gerçeğe ulaşmanın yolu o olayı temsil eden delillerin değerlendirilmesinden geçmektedir. Bu gerçekliğe ulaşmak için bilimsel yöntemlerle elde edilen delillerin, serbestçe değerlendirilmesi her ne kadar sınırları zorlayan bir sistem olsa da hâkimin vicdani kanaatinin oluşmasına aracılık eden bir unsurdur[436].

[435] Olgun Değirmenci, **Ceza Muhakemesinde Sayısal (Dijital) Delil**, 1. Baskı, Ankara, Seçkin Yayıncılık, 2014, ss.302-308.
[436] M. Koca, 2006, s.209.

Ceza muhakemesi sistemi delillerin elde edilmesi, ikamesi ve delillerin değerlendirilmesi açısından belli kurallar ve sınırlamalara sahiptir. Bu sınırlamalar vicdani delil sisteminin mutlak olmadığının da bir göstergesidir. Bu nedenle hakimin hukuka uygun delillere, kendi mantık kurallarına, tecrübelerine ve bilimsel verilere göre hareket etmesi uyuşmazlıklarda maddi gerçeğin ortaya çıkartılmasını sağlayacaktır.

Hukuken elde edilen delillerin geçerli sayılması için bazı gerekli prosedürlerin yerine getirilmesi ve bunların uluslararası standartlar taşıması büyük önem arz eder. Özellikle elektronik delil yapısı itibarıyla, diğer suçlarda elde edilebilecek fiziksel delilere nazaran daha hassas olup ve kolay bozulabilir nitelikte olduğu için birçok sorunu bünyesinde barındırmaktadır. Nitekim elektronik delilin elde edilmesi sırasında olay yerinde yapılacak en küçük bir hata, verilerin zarar görmesine veya yok olabilmesine neden olabilmektedir. Bu bakımdan elektronik delinin elde edilmesi sürecinde olaya ilk müdahele eden ekipten, incelemenin uzman birim ve laboratuvarlarda yapılmasını ve bundan sonra da elde edilen sonuçların mahkemeye sunulması aşamasına kadar devam eden her aşama büyük önem taşımaktadır [437].

A. Dijital Delillerin Hukuki Geçerliğinin İncelemesi

Elektronik delilin hukuki geçerliliğinin denetlenmesinde Öncelikle hukukun temel gerekleri olan ve diğer delillerde bulunması gereken özellikler olan gerçeklik, akıllıcılık, erişebilirlik, olayı temsil edicilik, müştereklik ve hukuka uygunluk özelliklerine sahip bulunması zorunludur.[438]

Delilin müştereklik özelliğinin gereği olarak, bir ceza yargılamasında öne sürülen elektronik delilinin, davanın bütün taraflarınca bilinir ve tartışılabilir olması gerekmektedir. Elektronik delil, delillerin müşterekliği ilkesi bakımından diğer deliller

[437] Çakır ve Sert, s. 148.
[438] Yusuf Başlar, **Ceza Yargılamasında Elektronik Delil**, Yetkin Yayınları, Ankara, 2016, s. 92.

nazaran daha avantajlı bir konumdadır. Zira henüz soruşturma aşamasında dahi elektronik delilleri içeren ve kopyası alınan elektronik verilerin bir kopyası şüpheliye verilmektedir. Bu durum çoğaltılabilme özelliğine sahip elektronik delil açısından bir avantaj niteliğindedir[439]. Gerçekten de, soruşturma veya kovuşturma makamlarında bulunan bir fiziksel delilin fail veya mağdur tarafından temin edilerek kendi istedikleri bir uzmana incelemeleri mümkün değilken elektronik delil açısından böyle bir imkan bulunmaktadır. Örneğin aleyhe delil niteliği arz eden bir bilgisayar diski, şüpheli tarafından başka bir uzmana inceletilebilir ve buradan elde edilen yeni bilgiler şüpheli lehine kullanılabilir [440].

Elektronik delil, akılcı, izah edilebilir ve rasyonel olmalıdır. Bu nedenle öngörüler ve zihin okuma araçlarıyla elde edilen elektronik veriler delil olarak kabul edilemezler. Delinin akıllıcılık özelliği, bilimsel açıdan kabul edilebilir biri nitelik taşımasına da beraberinde getirir [441]. Delilin bilimsel olması ise özellikle bilişim sistemlerinden elde edilen elektronik deliller bakımından ayrı bir özellik arz etmektedir. Adli bilişim uzmanı, bilişim sisteminde yer alan veriyi elde etmekte ve analiz etmek suretiyle suçla ilgisini ortaya koymaktadır. Bu bağlamda bilirkişi niteliği bulunduğundan şüphe duyulmayan adli bilişim uzmanı elektronik delil elde etme ve yorumlama yöntemi, mahkemeye etkilemekte kararın oluşmasına katkı sağlamaktadır. Her ne kadar adli bilişim uzmanının delil elde etme sürecine uyarak ilde ettiği delil, mahkeme açısından bağlayıcı olmasa da maddi gerçeğin ortaya çıkartılması açısından oldukça önemlidir [442].

Elektronik delilin bilimselliği, delinin elde edilmesi aşamasında genel kabul gören yöntemleri kullanılmasının yanı sıra elektronik delili elde eden soruşturma

[439] Hüseyin Akarslan, **Bilişim Suçları**, Ankara: Seçkin Yayıncılık, 2012, s. 132-133.
[440] Akarslan, s. 133.
[441] Bıçak, s. 429.
[442] Değirmenci, Ceza Yarhılamasında Sayısal (Dijital) Delil, s. 117.

personelinin ehliyetile de doğrudan ilgilidir. Elektronik delili elde edecek personel, kolluk kuvveti veya savcılık/mahkeme tarafından atanan bilirkişi, adli bilişim konusunda sertifikayla da desteklenen bilgi düzeyine sahip olmalıdır. Bununla birlikte, elektronik delilin bilimsel yöntemlere elde edilmesi, onun delil değerini taşıması için gerekli ve fakat yeterli olan bir özellikle değildir. Bilimsel yöntemlerle elde edilmeyen bir elektronik delil, geçerli bir delil olup olmadığı hususunda kuşku uyandıracaktır. Muhakeme makamları bu delilleri kabul ederken dikkatli davranmalı, varsa uzman raporlarının bilimselliği araştırılmalı, eldeki delile ulaşırken hangi teknik/bilimsel araçların kullanıldığı tespit edilmeli ve bu araçların bilimsel camiada güvenilir olarak kabul edilip edilmediği ortaya koyulabilmelidir.[443]

Ceza yargılaması bakımından delillerin en önemli özelliği olan "hukuka uygun elde edilmiş olma" hususu elektronik delil bakımından da büyük öneme sahiptir[444]. Nitekim elektronik delilin hassas yapısı, yığın halinde bulunabilme özelliği, sosyal hayatın elektronikleşmesi sonucunda ceza yargılamasında elektronik delile başvurma lüzumu hissedilmesine binaen hukuk kurallarına uyulmaksızın elde edilecek delil özel hayatın gizliliği, kişisel verilerin ifşası gibi bazı hak ihlallerine yol açacaktır.

Bu bakımdan, hukuk düzelince belirlenen koşullara uyulmaksızın veya sözkonusu koşulların sınırlarının aşılarak hareket edilmesi durumunda elde edilen elektronik delilin hukuka aykırılığı gündeme gelecektir [445]. Bu durumda ise elektronik delilin hukuken geçerliliğinden söz edilebilmeyecektir.

[443] Şenel Sarsıkoğlu, "Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil E Delil Kavramı", **Türkiye Adalet Akademisi Dergisi** , No.22, 2015, ss. 427-454.
[444] Akarslan, s. 133.
[445] Değirmenci, Ceza Yarhılamasında Sayısal (Dijital) Delil, s. 389.

B. Delil Değerlendirme İlkeleri

Çalışmamızın bu bölümünde delillerin değerlendirilmesinde hakimin re'sen inceleme, doğrudan doğruya inceleme, serbest inceleme, şüpheden sanık faydalanır ilkeleri hakkında bilgiler verilerek dijital delillerle ilişkisi ifade edilmeye çalışılmıştır.

1. Delillerin Re'sen İncelenmesi

Medeni hukukda dava malzemesinin taraflarca getirilmesi ilkesinin karşısında hakimin "re'sen araştırma yetkisi" (kendiliğinden araştırma ilkesi) bulunur. Hâkim, tarafların yargılama aşamasında getirdiği davayla ilgili malzemeler yanında, getirmedikleri dava malzemelerine de dikkat ederek gerekli gördüğünde uyuşmazlığın taraflarından bağımsız bir şekilde araştırma yapabilir. Re'sen araştırma ilkesinin uygulanma alanı tarafların dava konusu üzerinde serbestçe tasarruf etmelerinin mümkün olmadığı kişilik haklarını koruyan davalar, boşanma ve ayrılık davaları, babalık davaları, evlenmenin butlanı, nüfus kayıt düzeltme davaları gibi genellikle kamu düzeninin korunmasını gerektiren uyuşmazlık davalarıdır. Bununla birlikte "kendiliğinden araştırma ilkesi"nin uygulama alanı birçok uyuşmazlıklarda da geçerli bir ilkedir[446].

Ceza Muhakemesinde yargılamanın yapılabilmesi ancak hukukun suç saydığı bir eylemin meydana gelmesiyle mümkündür. Bu eylem ihbar, şikâyet, kolluğun ya da Cumhuriyet Savcısının re'sen tespiti ya da suç duyurusunda bulunma yöntemleriyle ortaya çıkmaktadır. CMK 134. Maddenin birinci fıkrası kapsamında uygulanacak tedbir kararı yalnızca soruşturma evresinde başvurulabilen bu tedbirdir. Bu nedenle hakim

[446] Seda Özmumcu, "Türk Hukukunda Yargıtay Kararları Işığında Re'sen Araştırma İlkesi", **S.D.Ü. Hukuk Fakültesi Dergisi MİHBİR Özel Sayısı 2014,** 4(2), ss.145-171,

veya mahkeme tarafından re'sen tedbirin uygulama alanı bulması mümkün olmayıp, Cumhuriyet savcısının istemi gerekir[447].

2.Delillerin Doğrudan Doğruya İncelenmesi

Delillerin doğrudanlığı ilkesi, "kendi kendine araştırma yapma ilkesi"'nin uygulandığı ceza hukuku kaynaklı bir ilke olarak görülmektedir. Bununla birlikte adil yargılamanın yapı taşını oluşturması nedeniyle bütün yargılama usullerinde uygulanabilecek bir ilkedir. Delillerin doğrudan doğruya incelenmesi doktrinde "yüzyüzelik", "vasıtasızlık", "doğrudan doğruyalık" gibi isimlendirmelerle anılmaktadır. Bu ilkeyi Arslan şu şekilde tanımlamıştır: *"...davanın açılmasından hüküm verilinceye kadar ki bütün delil toplama evrelerinin, kararı verecek olan hâkim veya hâkimlerin denetiminde ve gözetiminde gerçekleşmesinden sonra bu şekilde elde edilen delillerin araya fazla zaman girmeden değerlendirilerek, içlerinden adil bir hüküm tesisine doğrudan doğruya katkı sağlayacak olanların mahkeme tarafından seçilmesini konu alan bir usul hukuku ilkesidir."*[448]

Doğrudanlık ilkesi medeni hukukta adil ve doğru karar verilmesine hizmet eden bir ilkedir. Bu ilke doğrultusunda mahkeme tarafları ve delilleri huzurunda inceleyebilmekte ve onlarla ilgili kişisel izlenimlerde bulunarak kanaatinin oluşmasını sağlamaktadır. Doğrudanlık ilkesinin "şekli doğrudanlık", "maddi doğrudanlık" ve Alman hukukunda geçerli olan "zamansal doğrudanlık" olarak üç türü vardır. Şekli anlamda doğrudanlıkta "delillerin incelenmesi ve istinabe" başlığı altındaki HMK m.197'deye göre kanunda belirtilen haller dışında delillerin mahkemenin huzurunda ve mümkün olduğu kadar birlikte ve aynı duruşmada incelenmesi gerekir. Yani hâkimin şekli doğrudanlık gereğince delilleri bizzat görüp incelemesi ve karar vermesidir. Maddi

[447] Aykut, Özdemir, **Adli Bilişim Alanında Dijital Delil, Delil Karartma ve Delil Toplama**, Hacettepe Üniversitesi Fen Bilimleri Enstitüsü, 2015, Ankara, s.12
[448] Aziz Serkan Arslan, "Doğrudanlık İlkesi", S**.D.Ü. Hukuk Fakültesi Dergisi MİHBİR Özel Sayısı 2014,** 4(2), ss.133-144

doğrudanlıkta ise hakimin huzuruna getirilen deliller arasından ispatı gereken konuya en yakın delil aracını kullanma yönünde tercihte bulunması yani sonradan oluşturan dolaylı delilleri kullanmaktan kaçınması anlamına gelmektedir. Bu durumda mahkeme önüne konulan istinabe tutanakları üzerinden karar vermek yerine görgü tanıkları ve tarafların ifadelerini dinlemeyi tercih etmesi maddi doğrudanlık ilkesinin gereğidir. Zamansal doğrudanlık ise duruşma sırasında hâkimde oluşan kanaatin zaafa uğramamasının önüne geçmek amacıyla ilgililerin mümkün mertebe duruşmada hazır bulundurulması, duruşmanın aralıksız yapılması ve kararında en kısa sürede verilmesidir[449].

Elektronik delillerin içerisinde bulunan dijital verileri anlayabilmek için mutlaka bir uzmanın yardımını almak gerekir. Bu uzmanın alet ve cihazlar ile yaptığı nicel gözlemler verilerin delil özelliğini ortaya çıkartacaktır. Makine dili ile kodlanan bilgilerin bir makine tarafından yorumlanması ve uzman bir tarafından değerlendirilmesi kaçınılmaz bir gerçektir[450]. Bu açıdan değerlendirildiğinde CMK 134. Madde kapsamında hakimin dijital delilleri şekli doğrudanlık ilkesi uyarınca incelemesi delillerin sayfalarca tutması ve sayısal verilerden oluşması nedeniyle delilin mahkeme sırasında incelenmesini imkansız hale getirecektir. Bu nedenle kanaatimizce bilirkişi raporlarından faydalanmaktan başka çare bulunmamaktadır. Bununla birlikte elektronik delillerin yapısı gereği tahrif edilme veya yeniden oluşturma olasılığının göz önünde bulundurularak isnat edilen suç ile ilgili sanık ve tanık ifadelerine önem verilmesi maddi doğrudanlık ilkesinin yerine getirilmesini sağlayarak maddi gerçeklik hakkında doğrudan bir kanaate ulaşmasına aracılık edebilir. Bu açıdan kanaatimizce dijital deliller doğrudan doğruya inceleme açısından vicdani kanaati oluşturabilecek deliller olarak görülmemelidir.

[449] A.S. Arslan, 2014, ss.136-138.
[450] M. Özen, G. Özocak, 2015, s.59

3.Delillerin Serbestçe Değerlendirilmesi

Ceza muhakemesinin amacı maddi gerçeğe ulaşmaktır. Bu amaç ancak hakimin bir olay ile ilgili vicdani kanaate ulaşmasına aracılık eden delillerin ispatıyla mümkündür. Türk Ceza muhakemesinde vicdani delil sistemi kabul edildiğinden hakimi vicdani kanaate ulaştıracak her türlü delil ileri sürülebilmekte hakim de ileri sürülen bu delilleri serbestçe değerlendirebilmektedir. Hakimin bu yetkisi CMK'nın 217. Maddesinde şu şekilde ifade edilmiştir: "*Hâkim, kararını ancak duruşmaya getirilmiş ve huzurunda tartışılmış delillere dayandırabilir. Bu deliller hâkimin vicdanî kanaatiyle serbestçe takdir edilir."*

Hakim her ne kadar vicdani kanaatine göre karar verse de bu kanaatin oluşmasında delil olabilecek ve yargısal denetimden geçecek somut deliller etkili olmalıdır. Somut hiçbir veriye dayanmadan sadece kişilerin duruşmalardaki hal ve davranışlarından yola çıkarak karar vermek hukuki bir değerlendirme olmayacaktır. Bu nedenle alınan kararın delillerle desteklenebilir mahiyette olması gerekir[451]. Bununla birlikte hakimin tüm şüphelerden arınmasını beklemek imkansız bir durum olduğundan hakimin makul şüpheleri yenmesi gerekli ve yeterli sayılmaktadır[452].

Vicdani delil sistemi, hem delil serbestisi hem de delillerin değerlendirilmesi serbestisini içeren bir sistemdir. Ceza muhakemesinde duruşmalarda ortaya koyulup tartışılan her delil serbestçe ileri sürülebilmekte ve hakim de huzurunda tartışılan her türlü delili serbestçe değerlendirebilmektedir. Burada önemli olan delilin sağlam ve güvenilirliğini ispat etmektir[453].

---

[451] Ali Koyuncu, "Ceza Adaleti Usul Hukuku İlişkisi ve Vicdani Kanaat", **Ankara Barosu Dergisi 2011,** 4, ss.366-367.
[452] Mehmet Yayla, "Ceza Yargılamasında İspat İçin Yenilmesi Gereken Şüphe; Türkiye ve Amerika Birleşik Devletleri Sistemlerinin İncelenmesi", **Ankara Barosu Dergisi 2013**, 3, s.304.
[453] Cumhur Şahin, **Ceza Muhakemesinde İspat (Delillerin Doğrudan Doğruyalığı İlkesi),** Ankara, Yetkin, 2001, s. 46.

Delil serbestisi bağlamında karar verirken hâkimin keyfi hareket edeceği anlamını taşımamaktadır. Zira hâkim vermiş olduğu kararın ardında hangi delilin bu kararı vermesine neden olduğunu açık bir şekilde belirtme zorunluluğu bulunmaktadır. CMK, 223/5. Maddesine göre mahkemenin ancak sanığın yüklenen suçu işlediğinin sabit olması halinde mahkumiyet kararı verebileceğini bildirmesi de verilen kararın keyfilik içermesini engellemektedir. Ayrıca, CMK'nın 230. Maddesine göre de mahkûmiyet kararının iddia ve savunmada ileri sürülen görüşler, delillerin tartışılması ve değerlendirilmesi, hükme esas alınan ve reddedilen deliller, hukuka aykırı deliller, ulaşılan kanaat, sanığın suç oluşturduğu sabit görülen fiili ve nitelendirilmesinin açıkça yazılması gerektiği de bildirilmektedir[454].

CMK'ya göre kovuşturma evresinde delilleri hâkim tarafından değerlendirilirken, soruşturma evresinde bu yetki cumhuriyet savcısına aittir. Cumhuriyet savcısı delillerin kamu davası açılmasına yeterli olup olmadığını belirlemek için delilleri serbestçe değerlendirmekte, şüphelinin leh ve aleyhinde topladığı delillere dayanarak dava açma konusunda takdir hakkını kullanmaktadır (CMK md.170., 171/1., 171/2., 174.). Bu durumda Cumhuriyet savcısı mahkeme gibi, soruşturma evresinde elde edilen delilleri değerlendirebilmekte, delillerin değerlendirilmesine ilişkin kurallar ve kısıtlamalara da uyma yükümlülüğü bulunmaktadır[455].

Delil serbestisi ilkesine göre; *"(1) her şey kanıt olabilir, (2) ilgililer kanıt ileri sürebilir, (3) yargıç kendiliğinden kanıt araştırabilir, (4) kanıt ileri sürmede zaman sınırlaması yoktur, (5) ispat külfeti sanığa yüklenemez, (6) kanıt belirlemede yargıcı bağlayan üstün kanıt yoktur*"[456].

[454] M. Koca, 2006, ss. 208, 213, 221
[455] H.T. Gökcan, 2012, ss. 195-199.
[456] İsmail Ercan, **Ceza Muhakemesi Hukuku**, 6. Bası, İstanbul, 2013, s.117

Ceza muhakemesinde meydana gelen somut olayın ispatına yarayan her türlü vasıta delil olabileceğinden hâkimin bu vasıtalardan hangisini kabul edeceği kendi takdir yetkisine kalmıştır. Soruşturma ve kovuşturma aşamasında maddi gerçeğe ulaşmak için ispat vasıtası olabilecek tüm delillerin dikkate alınması gerektiği Yargıtay[457] kararlarından da anlaşılmaktadır.

9. Ceza Dairesi'nin 09.10.2013 tarihli (E. 2013/9110, K. 2013/12351) kararında şu ifadelere yer verilmiştir: *"... Dijital delillerinyapısı gereği manipülasyona açık olduğu bilinmektedir. Diğer delil türlerine göre özellik arz eden bazı yönleri olmakla birlikte dijital deliller de sonuçta, deliller hiyerarşisinin kabul edilmediği, delil serbestîsinin benimsendiği ceza muhakemesi sistemimizde bir ispat aracıdır. İspat aracı olan delilin değerlendirilmesinde, ceza muhakemesi hukukunda bir delil için öngörülen nitelikleri taşıyıp taşımadığı nazara alınıp, genel olarak; somut olayın özellikleri, yüklenen suçun işleniş biçimi, dosyadaki diğer deliller gibi 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. (...) Dijital deliller de, ... diğer tüm deliller gibi ... gizlenmeye, değiştirilmeye, bozulmaya elverişlidir. (...) Ancak, dijital delillerin değiştirilebilme kolaylığı ve sanal oluşundan hareketle hükme esas alınamayacak olduğunun ileri sürülmesi delil olgusuna aykırıdır. Kaldı ki, dijital deliller Türk ceza muhakemesi sisteminde ilk kez bu dava ile gündeme gelmiş olmayıp, geçmişte de pek çok davada tartışılmış ve hükme esas alınmıştır…".* Bu karar doğrultusunda dijital delillerin muhakeme sürecinde "delil serbestîsi ilkesi"nin bir gereği olarak kullanılabileceği açıktır. Klasik deliller gibi dijital delillerin de "olayı temsil edici, müşterek, akılcı ve gerçekçi" nitelikte ve "hukuka uygun yollardan elde

[457] Bkz. Yargıtay 11.Ceza Dairesi 05.02.2013 gün ve Esas Yargıtay 4.Ceza Dairesi 30.11.2011 gün ve Esas No: 2011/2606 Karar No: 2011/22901 sayılı kararı: *"...şüphelinin müşteki tarafından ibraz edilen mesaj kayıtlarını kabul etmemesi, mesaj kayıtlarının bu kapsamda usulüne uygun delil ve yazılı delil başlangıcı sayılamayacak olması ve müşteki tarafından yazılı bir belge ibraz edilememesi gerekçeleriyle kovuşturmaya yer olmadığına dair karar verilmiş ise de… mevcut delillerin kamu davası açılmasını gerektirir nitelikte bulunduğu ve bu delillerin mahkemesince değerlendirilmesi gerektiği gözetilmeksizin, itirazın kabulü yerine, yazılı şekilde reddine karar verilmesinde isabet görülmemiştir."*

edilmiş" olması zorunluluğu bulunmaktadır. Bu nedenle belgenin oluşturulduğu, değiştirildiği, yok edildiği ya da birtakım işlemlere tabi tutulduğu sistem ve araçların bir bütün olarak incelenmesi ve değerlendirilmesi ya da doğrulanması gerekir. Elektronik deliller bir olayın doğrudan ispatını sağlayabileceği gibi, soruşturma veya kovuşturma konusu fiilin fail tarafından işlenmediğine de delil olarak sunulabilmektedir. Bu nedenle dijital delillerle ilgili yapılan işlemler ve bu delillerle ilgili gözlem ve bulguların muhakeme sürecinde uzmanlarca raporlanması, belgelendirilmesi ve hakimin anlayacağı bir formata getirilmesi delilin kabul edilebilirlik derecesini değiştirecektir[458].

4.Delillerin Bütün Olarak Değerlendirilmesi

Dijital delil bakımından karşılaşılan en büyük sorunlardan birisi onun elde edilmesi ve yargılama sonuna kadar muhafazası süresinde bütünlüğünün korunması hususudur. Bu durum aynı zamanda elektronik delil ile fiziksel deliller arasındaki en temel farklarından birini teşkil etmektedir.

Cumhuriyet Savcısı, elektronik medyadan elde edilen verilerin ilk alındığı haliyle temsil edildiğini, elektronik medyanın tamamen kolluk güçleri ya da kısmen veya tamamen tanık veya sanık tarafından elde edildiği hususlarına bakmaksızın, mahkeme önünde doğru ve kesin olarak ortaya koymak zorundadır [459]. Elektronik delilin bütünlüğü ilkesi, elektronik delile ilk ulaşıldığı andan itibaren hem fiziken hem de Elif dönüş bakımdan koruma altına alınmak suretiyle delilin değişmediğinin tespit edilmesini ifade etmektedir. Elektronik delilin yapısı gereği kasten ya da yanlışlıkla silinmesi, değiştirilmesi veya bozulması kolay ve mümkündür. Bu durum elektronik

[458] Çetin Arslan, "Dijital Delil ve İletişimin Denetlenmesi", **CHKD 2015,** 3(2), s.257.
[459] John. D. Nilsson (Ed.),Digital Evidence in the Courtroom, New York: Nova Science Publishers, 1nc, 2010, s. 21.

delilin bütünlüğünü sağlamayı oldukça zorlaştırmaktadır. Bu nedenle elektronik delilin bütünlüğüne herhangi bir zarar gelmemesi son derece önemlidir [460].

"Bütünsellik" ilkesi yargılamada herhangi bir şeyin tek başına ve içinde bulunduğu bütünden ayrı olarak ele alınmamasıdır. Delillerin duruşmada ortaya konulması ve taraflarca hâkim huzurunda tartışılması yargılamanın kolektif bir mahiyet kazanarak adil bir hüküm çıkması sağlanabilir. Maddi gerçeğe ulaşmadaki mantık yolunun izlenmesinin önemini Yargıtay 19.04.1993 tarihli kararında şu şekilde ifade etmiştir: *"Ceza yargılamasının amacı hiçbir duraksamaya yer vermeden maddi gerçeğin ortaya çıkarılmasıdır. Bu araştırmada, yani gerçeğe ulaşmada mantık yolunun izlenmesi gerekir. Gerçek; akla uygun ve realist, olayın bütünü veya bir parçasını temsil eden kanıtlardan veya kanıtların bütün olarak değerlendirilmesinden ortaya çıkarılmalıdır. Yoksa birtakım varsayımlara dayanılarak sonuca ulaşılması, ceza yargılamasının amacına kesinlikle aykırıdır"*[461].

Ceza yargılamaları ve idari yargılamalarda deliller hâkim tarafından serbestçe belirlenebildiği için dijital delillerin ispat gücü ve uygulanma alanı özel hukuk yargılamalarına göre daha yüksektir. Özel hukukta güvenli elektronik imza ile imzalanan belgeler kesin delil niteliğinde olduğundan en yüksek ispat gücüne sahip iken güvenli elektronik imzayla oluşturulmayan dijital delilleri yalnızca delil başlangıcı olarak görmek gerekir. Bir dijital delilin dava aşamasındaki geçerliliği, verilerin bütünlüğüyle, doğruluğuyla ve doğrulanabilmesiyle ilgili olduğu kadar inkâr edilememesi ve sonradan dikkate alınabilirliğiyle de ilişkilidir. Bu nedenle hakim dijital

[460] Mustafa İlker Öztürk, s. 39.
[461] Bkz.Yargıtay CGK. 19.04.1993, 6-79/108

delilleri değerlendirirken delili bir bütün olarak ele almalı ve ona göre karar vermelidir[462].

Delil bütünlüğü, bir olayla ilgili olarak dijital adli delillerin toplanması sırasında sadece iddia makamının tespitlerine dayanarak kişinin suçlu olduğuna yönelik delillerle birlikte kişinin suçsuzluğunu gösterecek delillerin de toplanması demektir. Konuya örnek verilecek olursa bir bilgisayar sistemine saldırarak zarar verdiği şüphesiyle o kişi hakkında bilgi toplamak, kişinin suçluluğunu göstermeyebilir. Bunun yanı sıra, sisteme o anda bağlı olan bütün kullanıcıların IP, kullanıcı adı vb. bilgilerinin de tespit edilmesi ve saldırıyı yapanın başka kullanıcılar olabileceğinin de araştırılmasıdır[463].

Bu kapsamda düşünüldüğünde kanaatimizce dijital delillerin değerlendirilmesinde delilin ele geçirilmesinden, bilgisayar kullanıcısına, delilin kopyalanması sırasında ya da daha sonradan delilde meydana gelen değişikliklere varana kadar bir bütün olarak ele alınması ve iddia olunan suçun varlığını, var ise bu suçu kimin işlediğini belirlemek gerekir. Bu nedenle delillerin değiştirilmiş olabileceği, sonradan eklenmiş olabileceği ya da uzaktan erişim, virüs, solucan gibi faktörlerle kişinin bilgisayarına gönderilmiş olabileceği ihtimallerini düşünmeden ve bu şüpheden arınmadan bilgisayar sahibi veya kullanıcısını suçlamak, delillerin bütünsellik ilkesine aykırı olacaktır.

5.Şüpheden Sanığın Yararlanması

Ceza yargılaması hukukunda geçerli olan "şüpheden sanık yararlanır ilkesi" mevzuatımızda yazılı olarak hükme bağlanan bir ispat kuralıdır. Günümüz şartlarında bütün hukuk devletleri bu ilkeyi masumiyet karinesi ile de doğrudan ilişkilendirerek tartışmasız bir şekilde kabul etmiştir. Bu ilke gereğince suç işlediği iddia edilen kimse

[462] İlker Koç, Hüseyin Çakır, "Denetim Süreçlerinde Dijital Delillerin Elde Edilmesi Ve Korunması", **International Journal of Human Sciences 2015**, 12(2), s.1102.
[463] E. Çalışkan, 2013, s.100

hakkında mahkûmiyet kararı verilebilmesi için, bu durumun şüpheden mümkün olduğunca arındırılarak suçun ispatlanmış olması gerekir. Bu ilke Anayasanın 38. maddesinin 4. Fıkrası ve AİHS 6/2. Fıkrasında ifade edilen "suçsuzluk karinesi" ile doğrudan ilişkilidir.

Kişinin suçlu kabul edilmesi ancak kesin hüküm ile mahkûm edilmesine ve mahkûmiyetin de fiilen ispatlanmasıyla mümkündür. Bu sonuca ulaşabilmenin yolu failin leh ve aleyhindeki bütün delillerin toplanması, incelenmesi, mahkeme huzurunda tartışılması ve şüpheye yer vermeyecek bir şekilde fiilin fail tarafından gerçekleştirildiğinin ispatlanması gerekir. 5271 sayılı CMK'nın 223'üncü maddesi de "yüklenen suçun sanık tarafından işlendiğinin sabit olmaması" halinde beraat kararı verileceğini bildirerek şüpheden sanık yararlanır ilkesini gündeme getirmektedir[464].

Suçun ispat edilmemesi sanığa ceza verilmesine engel teşkil eder. Ceza muhakemesinde masumiyet karinesi ve susma hakkının olması "sanığın suçsuzluğunu ispat yükünün" bulunmadığı anlamına gelir. Bu nedenle sanığın mahkum edilebilmesi ancak hakim ve savcının maddi anlamda ispat yükümlülüğünü yerine getirmesiyle mümkündür. İspat faaliyeti sonucunda ortaya çıkan inanç ya da zan yeterli olmadığından hakimin tam bir vicdani kanaate ulaşması da beklenmemelidir. İspat konusunda şüphelerin yenilemiyor olması, kesin bir kanaat oluşturmaması şüpheden sanık yararlanır ilkesi gereğince sanık lehine bir değerlendirme yapılmasını zorunlu hale getirecektir. Dolayısıyla "*Beraat için suçsuzluğun sabit olması gerekmez; suçluluğun sabit olmaması yeterlidir.*"[465]

Dijital deliller açısından konuya yaklaşılacak olursa iddia ve savunmanın ileri sürdüğü deliller bir yandan bilişim cihazları üzerinden elde edilecek delillerle diğer yandan bilişim ağları üzerinden uzmanlarınca yapılacak bir çalışma ile elde edilen

[464] V. Bıçak, 2011, s.116
[465]Mehmet Yavuz, "Ceza Muhakemesinde İspat Sorunu", **TAAD 2012,** 3(9), ss.153-156.

bilgilerle örtüşüp örtüşmediği kontrol edilmelidir. Delillerin şüpheye yer bırakmaması için tanık ve sanık ifade beyanları ile karşılaştırması hem maddi gerçekliğin açığa çıkarılmasını hem de ispatlanamayan durumlarda şüpheden sanığın yararlanmasını sağlayacaktır[466].

Dijital delillerin güvenilirliğini sağlamak amacıyla bilgisayar verilerine elkonulmadan önce hash değerleri alınmakta daha sonra dijital delil kopyası üzerinde yapılan analizlerden sonra alınan hash değerleri ile karşılaştırılarak delil bütünlüğünün bozulup bozulmadığı belirlenebilmektedir. Çoğu davalarda bu hash değerinde meydana gelen ufak bir değişiklik bile sanığın delilin değiştirildiğine yönelik itirazlarına sebep olmaktadır. Bu durumda sanığın suçu işlediğine dair deliller bulunsa da delilerdeki şüpheler hakimin vicdani kanaatinin sanık lehine olmasına yol açacak, şüpheden sanığın faydalanması ilkesi gereğince sanığın beraati bile mümkün hale gelecektir[467].

Bazen bilgisayar verilerine ulaşmada problem yaşandığında veya şifreli verilere ulaşılması mümkün olmadığında da "şüpheden sanık yararlanır" ilkesi gereğince sanık lehine kararların alınması mümkündür[468].

6.Delillerin Doğrulanması İlkesi

Elektronik delil kullanımının yaygınlaşmasıyla birlikte ceza soruşturması yeni bır boyut kazanmıştır. Kolluk güçleri, daha önceden kullanılmayan birçok soruşturma yöntemini kullanma yolunu benimsemişlerdir. Bu kapsamda elektronik deliller, olay faillerinin arkalarında bıraktıkları dijital izler olarak takip edilmiş ve birçok soruşturma sonuçlandırlabilmiştir. Bununla birlikte, kovuşturma aşamasında ceza hakimi

[466] E. Casey, 2011, s.308.
[467] Yasin Başar, **Siber Suç Soruşturmalarında Adli Bilişim İncelemeleri**, Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 2015, ss.75-76.
[468] V. Bıçak, 2011, s.116; N. Kunter ve diğerleri, 2010, s.1336

tarafından elektronik delile ilgili göz önünde bulundurulması gereken temel ilke, elektronik delilin doğası gereği yeterince kişiselleştirilmemiş olmasıdır [469].

Elektronik delilin elde edilmesinden sonra adli soruşturma sürecinde gerçekten iddia olunan suçla veya şüpheliyle alakalı olup olmadığının ispatı gerekmektedir. Zira soruşturma sürecinde elde edilen elektronik verilerin aynısını herhangi bir kişi tarafından oluşturulması mümkündür. Hatta bu elektronik verilerin sonradan kolluk tarafından üretildiği de iddaa olunabilir. Bu bakımdan soruşturma sürecinde elektronik verilerin olay ve şüpheli ile ilişkisi teyit edilmelidir [470].

Elektronik delilin bulunduğu tiplerinde karşılaşılan en sorunlu konulardan birisi, bir olayda elde edilen elektronik delilin muhakeme esasında kabul edilebilirliği hususudur. Gerçekten de, elektronik delilin gerçek delil özelliği gösterebilmesi için ilk toplandığı andan itibaren hiçbir biçimde değiştirilmediğinin, kim veya kimler tarafından nerede ve ne zaman toplandığının doğrulanması gerekmektedir. Bu delillerin yargılama sırasında kabul edebileceğini sağlamak için yalnızca doğrulamada kullanılacak teknik yöntemleri yeterli değildir. Delilerin inceleme veya analiz işlemlerine tabi tutulduğu laboratuvar standartlarının bu işlemleri yerine getirmek için uygun olup olmadığı, kullanılan araç, gereç ve yöntemlerin yerindeliği gibi başka birçok konunun da değerlendirmeye alınması gerekmektedir. Bu bakımdan Adli Bilişim süreci için gerekli uluslararası standartların belirlenerek, Bu standartların uygulamaya konulması çok büyük öneme sahiptir.

7. Delillerin İnkar Edilmemesinin İncelenmesi

Elektronik delillendirme işlemindeki elektronik delilinin sahibi, bu delili elde eden kolluk birimi, deliln alındığı elektronik Medya, delilin içeriği gibi bütün

[469] Değirmenci, Ceza Yarhılamasında Sayısal (Dijital) Delil, s. 404.
[470] Mustafa İlker Öztürk, s. 39.

unsurların daha sonradan inkar edilmemesi gerekmektedir. Bu bakımdan, elektronik delilin elde edilmesi sırasındaki kullanılan bilgi ve tekniklerin doğruluğunu gerektirdiğinde adli sürecin tüm aşamalarında ispatı gereklidir [471].

CMK m. 169/2 her soruşturma işlemlerinin tutanağa bağlanmasını, tutanağın adli kolluk görevlisi, Cumhuriyet Savcısı veya Sulh Ceza Hakimi ile hazır bulunan zabit katibi tarafından imzalanmasını, CMK m. 134/3 İse bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında sistemdeki bütün velileri yedeklemesinin yapılmasını hükme bağlamıştır. Bu bakımdan Adli Bilişim sürecinde elde edilen elektronik verilerin tutanağa bağlanarak imza altına alınması elektronik delilin inkar edilmemesı açısından büyük önemi haizdir.

8. Delillerin Tekrar ele Alınabilirliği

Bilimsel bir yöntemin en önemli özelliği yapılan herhangi bir deney veya gözlemin doğruluğunu kanıtlamak için tekrar edilebilir niteliğe sahip olmasıdır. Bu bakımdan elektronik delilin elde edilmesi sürecinde bir uzman tarafından yapılan inceleme ve bulgular başka bir uzman tarafından daha sonra tekrar ele alınabilir olmalıdır. Nitekim bu durum elektronik delilin sonradan ele alınabilirliği ilkesini bir gereğidir.

Bu Bağlamda elektronik delilin sonradan ele alınabilirliği ilkesi, elde edilen ve mahkemeye delil olarak sunulan tüm bulgulara farklı kişiler tarafından, farklı yer ve zamanlarda da aynı yöntem ve metotlar kullanılarak ulaşılabilmesi ifade etmektedir. Sonuçların tekrar elde edilebilir olması, elektronik delile olan güvenilirliğin en önemli göstergesidir. Genel kabul gören teknikleri ön plana çıkmasındaki en önemli etken,

[471] Mustafa İlker Öztürk, s. 39-40.

farklı kişiler tarafından uygulanan bu tür yazılımların her defasında aynı sonuçu vermelidir [472].

9.Delillerin Doğruluğu İlkesi

Delillerin elde edilme sürecinde, elektronik delilin kişisel veya kurumsal sahibi, onu elde eden kolluk birimi, delilin elde edildiği elektronik ortam, elektronik delilin elde edildiği zaman, elektronik delilin içeriği gibi bütün unsurların doğruluğunun daha sonradan inkar edilmeyecek şekilde belgelenmesi gerekmektedir.

Gerçekten de elektronik delil ister insan müdahelesi ile oluşturulan bir delil niteliğinde olsun, ister sistem tarafından otomatik olarak oluşturulan bir delil olsun, doğruluğunun mutlaka kontrol edilmesi gerekmektedir. Bu bakımdan bilişim sistemlerinin girdi, süreç ve sonuç şeklinde çalışan sistemler olduğu göz önünde bulundurma malı ve elektronik Delil bakımından girdi, delilerin işlem görmesi durumunda işlemlerin doğruluğu ve çıktının girdi, işlem süreçleri ile uygunluğu kontrol edilmelidir[473].

Özellikle, belli orandaki bilginin kaydedilmeden önceki kayda hazırlık biçimleri, programdaki yapısal hatalar, veri girişim detayları, bilişim sistemine verilen komutlarda yapılan hatalar, kaydedilerek muhafaza edilen verideki hasar ve bozukluklar, bilişim sisteminin çalıştığı sırada elektrik kesintisinin olup olmadığı, bilişim sistemi hata verip vermediği, veri içerisinde kelime araması veya belli bölümlerin kesilmesi, verinin başka bir karaktere çevrilmesi gibi işlemler yapılırken sıradan, bireyin kendine özgü hatalar yapıp yapmadığını anlamk için kullanılan bilişim sisteminin standart tipte olup olmadığı, bilişim sisteminin hassas çalıştığına güvenilip güvenilmeyeceği gibi teknik hususların da bilirkişi tarafından incelenerek hazırlanan

[472] Henkoğlu, s. 2.
[473] Değirmenci, Ceza Yarhılamasında Sayısal (Dijital) Delil, s. 404.

bilginin bir kişi veya kişilerin kurgusu olup olmadığı teknik olarak bilirkişi tarafından oratya çıkarılacaktır[474].

Türk ceza hukukunda dijital delillerin nasıl değerlendirileceğine yönelik tartışmalar henüz bitmiş değildir. Özellikle 2008 yıllarından itibaren başlayan Balyoz, Ergenekon ve Askeri Casusluk gibi davalar dijital delillerle ilgili tartışmaların en yoğun yaşandığı dönem olmuştur. Dijitalleşmenin hayatın her alanına dahil olması ve bu dijital dünyada her türlü verinin kolay bir şekilde oluşturulması, transferi, değiştirilmesi gibi faktörler delillerin hukuki geçerliliğini de tartışılır hale getirmiştir. Bu kadar önemli bir konuda hukuki düzenlemelerin henüz istenilen düzeyde yapılmaması hem bir yandan hak yoksunluklarına neden olmakta hem de suç işleme niyetinde olan kişilerin daha rahat hareket etmesine yol açmaktadır. Türk hukuku açısından dijital delillerin doğrulanmasına yönelik kabul gören bir kurallar bütünü bulunmamaktadır. Ayrıca, dijital delillerin nasıl değerlendirileceğiyle ilgili de henüz tutarlı bir bakış açısı geliştirilmiş değildir.

C. CMK Kapsamında Dijital Delillerin Değerlendirilmesi

Türk Ceza Muhakemesi Hukuku kapsamında dijital deliller değerlendirilirken bilgisayar, bilgisayar kütükleri, bilgisayar programlarının yanı sıra dijital deliller kapsamına giren ses ve/veya görüntü tespit eden belgeler, bilgi depolayan cihazların da incelenmesi ve bu konudaki genel yaklaşımın belirlenmesi gerekir.

Ceza yargılamalarında ses ve görüntü içeren araçlar ile elektronik deliller belge delilleri olarak kabul edilmektedir. Video görüntüleri, yazı dosyaları, fotoğraflar, iletişim kayıtları, çeşitli bilgisayar programları, gizli ve şifreli dosyalar veya klasörler, internet ortamından indirilen dosyalar, son girilen ve sık kullanılan internet siteleri, silinmiş dosya veya klasörler elektronik delil hükmünde değerlendirilebilir. Bu

[474] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1104.

elektronik veriler bilgisayarlarda, internet, el bilgisayarı, cep telefonları, hafıza kartları, taşınır bellekler, CD ve DVD gibi teknolojik aletlerde bulunabilmektedir[475]. Bu delillerin mukahemede kullanılabilmesi için hukuka uygun yollardan elde edilmesi ve tahrifata uğramadığının ispatlanması gerekir. Yargıtay 16. Dairesi[476] de "…*CD, DVD, flash bellek, disket, harici ve dahili harddisk, bilgisayar özelliği içeren noktaları bakımından akıllı telefon ve benzerlerinden elde edilen ve tamamı 'dijital delil' olarak adlandırılan….",* ifadeleriyle bu materyallerin dijital delil olduklarını ancak suistimale müsait veriler olduğunu da vurgulamıştır.

Yargıtay ayrıca dijital delillerin ispat değeri üzerine de genel bir açıklama yapma ihtiyacı hissetmiştir: *"Dijital delillerin yapısı gereği manipülasyona açık olduğu bilinmektedir. Diğer delil türlerine göre özellik arz eden bazı yönleri olmakla birlikte dijital deliller de sonuçta, deliller hiyerarşisinin kabul edilmediği, delil serbestisinin benimsendiği ceza muhakemesi sistemimizde bir ispat aracıdır. İspat aracı olan delilin değerlendirilmesinde, ceza muhakemesi hukukunda bir delil için öngörülen nitelikleri taşıyıp taşımadığı nazara alınıp, genel olarak; somut olayın özellikleri, yüklenen suçun işleniş biçimi, dosyadaki diğer deliller gibi 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. Dijital deliller de, kimyasal, biyolojik ve benzeri diğer tüm deliller gibi sanıklar ya da başkaları tarafından çeşitli şekillerde gizlenmeye, değiştirilmeye, bozulmaya elverişlidir. Sanıklar veya başkalan tarafından delillerin yok edilme, silinme, gizlenme, değiştirilme veya bozulmak istenmesi o kadar olağandır ki; yasa koyucu maddi gerçeğin ortaya çıkarılabilmesi bakımından büyük bir tehlike oluşturan bu fiilleri ayrı bir suç olarak veya nitelikli hal olarak düzenlemiştir.Ancak, dijital delillerin değiştirilebilme kolaylığı*

[475] M. Özen, G. Özocak, 2015, ss.59-60
[476] Bkz.Yargıtay 16. Ceza Dairesi Esas No:2015/4672, Karar No:2016/2330

ve sanal oluşundan hareketle hükme esas alınamayacak olduğunun ileri sürülmesi delil olgusuna aykırıdır."[477]

Usulüne göre muhafaza edilen ve mahkemeye sunulan ses ve/veya görüntü bantların bir çeşit yazılı açıklama olarak kabul edilmesi ve yargılamaya esas deliller arasında sayılmaması yönünde bir yaklaşım bulunmaktadır. Yargıtay ve Anayasa Mahkemesi de ses ve/veya görüntü tespit eden kayıtların delil vasfını zayıf olarak nitelemiş, "Yargıtay 9. CD.'sinin 5.10.1985 tarihli kararında", *"teyp bantlarının tek başına delil vasfını haiz olamayacağı",* 22.2.2000 tarihli bir kararda ise "*teyp bantları, kaydedilen sözlerin kime ait olduğunun şüpheye yer bırakmayacak şekilde saptanmasının teknik olarak mümkün bulunmaması nedeniyle tek başlarına delil değeri taşımazlar*" kararıyla özellikle ses kaydını içeren belgelerin delil vasfının zayıflığını ancak söz konusu kayıttaki ifadelerin somut olaydaki diğer delillerle tam bir uyum içinde bulunmasının bu tür belgelerin mutlaka diğer delillerle desteklenmesi gerektiğini göstermiştir. Bu yargı kararlarına göre usulüne uygun olarak muhafaza altına alınan ve usulüne uygun bir şekilde mahkemeye delil olarak sunulan ses ve/veya görüntü bandları tek başlarına mahkumiyet kararı vermek için yeterli olamazlar. Bu nedenle başkaca delillerle de desteklenmesi şarttır. Bu kayıtlardaki en önemli problem değiştirilebilme riskinin yüksekliği, kişilerin seslerinin taklit edilebileceğidir[478].

Teknolojik yeniliklerin getirdiği avantajları kullanan kişilerin ses kayıtlarında oldukça ileriye giderek kişilerin her bir ses kaydındaki kelimeleri bir araya getirerek yeni cümleler oluşturabileceği ülkemizde yaşanan 17/25 Aralık 2013 olaylarında ileri sürülmüştür. Ses kayıtlarıyla ilgili her ne kadar çeşitli birimlerden raporlar alınabilse de özellikle önemli siyasi ve ideolojik olaylarda bu raporların güvenilirliğini her zaman tartışmalı hale getirmiştir. Bu açıdan değerlendirildiğinde ses kayıtlarıyla uyumlu diğer

[477] Yargıtay 9. Ceza Dairesinin 09.10.2013 tarihli, 2013/9110 Esas, 2013/12351 Karar sayılı kararı.
[478] E. Gökşen, 2014, s.113

deliller ve özellikle tanık beyanlarının aranması maddi gerçekliğin ortaya çıkartılması için zaruri olduğu kanaatindeyiz.

Şen'e göre, *"Hukuka aykırı delil, şüpheli/sanık aleyhine kesinlikle kullanılamaz, ancak bu delilin sanık lehine olduğu tespit edilmişse, masum bir kişinin cezalandırılmaması için istisnai olarak bu delilin soruşturma ve kovuşturmada değerlendirmeye alınması yerindedir".* Bu nedenle gizli kamera ile alına ses ve görüntü kayıtları sadece ve şartları uygun olduğunda savunma hakkına yönelik delil olabilir. Bununla birlikte belirtilen bu istisna dışında, hukuka aykırı delil vasfına sahip olduğundan suçun kanıtlanmasında kullanılamaz. Bu durumda kayıt yapan kişiye yönelik olarak işlenen bir suçun oluşması durumunda kayıt planlı olmaksızın kendiliğinden gerçekleşmişse suçun ispatı açısından sadece o kişi için kullanılması hukuka uygun görülebilirken, aynı kaydı kayıt sahibinden başka bir kişiye yönelik işlenen suçta kanıt olarak ileri sürmek mümkün değildir. Bununla birlikte doktrinin genel görüşü yasaya aykırı elde edilmiş bu delillerin hukuken yok hükmünde olduğudur. "AY m. 38/6 ve CMK'nın 206/2, 217/2 ve 289/1-i maddeleri" gereğince soruşturma ve kovuşturmaya yetkili organ ya da kişilerce hukuka uygun olmayan yollardan elde edilen veya delil toplama yetkisi bulunmayan özel kişiler tarafından usulsüz bir şekilde elde ettikleri deliller yargılamada kullanılamamalıdır[479].

Yargıtay 11. Ceza Dairesi bir kararında E-posta yoluyla virüs gönderilerek bir şirketteki bilgisayarlara zarar verildiği iddiasıyla açılan davada dijital delillerin incelenmesi usulünde dikkat edilmesi gereken kurallara dikkat çeken emsal niteliğinde bir karar vermiştir:

"- Virüs içeren bir e-posta veya e-postaların şikayetçinin bilgisayarlarına virüs bulaştırması sonucu doğacak zararın, şirketin gönderdiği e-postalar aracılığıyla başka

[479] M. Gödekli, 2016, ss.1852-1853.

adreslere virüs göndererek başka bilgisayarlara zarar vermesi ve kendi bilgisayarlarının sistem dosyalarını silerek çalışamaz duruma getirip iş ve zaman kaybına neden olması karşısında, virüslü veya virüssüz bir e-postayı gönderen bilgisayarı bulmanın mümkün olduğunu,

- E-postayı gönderen bilgisayarın IP numarası, e-postayı gönderen sunucu bilgisayarın IP numarası, gönderici ve alıcı adreslerinin, e-posta almayı ve göndermeyi sağlayan e-postanın sunucu bilgisayarlarının tuttuğu günlük kayıtlarında saklandığını, servis sağlayıcı firmaların bir süre sonra bu kayıtların olduğu dosyaları silebildiğini, bu bilgilerin servis sağlayıcı firmalardan resmi yollarla istenilerek öğrenilebileceğini,

- E-posta sağlayıcı şirketin günlük (log) kayıtları mevcutsa gönderici eposta adresini, e-postanın yazılıp yola çıkarıldığı ilk bilgisayarın IP numarasını ve IP numarasının sahibi servis sağlayıcı firmanın isminin bulanabileceğini, servis sağlayıcı firmadan da, günlük kayıtları mevcutsa verilen tarih ve saat için bu IP numarasının kullanıcısının öğrenilebileceğini,

- Şayet e-postanın yola çıkarıldığı sistemin IP numarası e-posta sağlayıcı şirketten öğrenilemezse ve e-postayı gönderen adres .....@yahoo.de olarak bulunursa Yahoo şirketinden; başka bir adres çıkarsa o e-posta adresini sağlayan servis sağlayıcıdan, bu adresi kullanan kişinin sistemde kayıtlı kimlik bilgileriyle, mevcutsa günlük kayıtlarından bu adres aracılığıyla e-posta gönderip almak için sisteme erişildiğindeki tarih ve saatler ile erişilen IP numaralarının öğrenilebileceğini,

- Bu kullanıcı telefonla bağlanan bir ev kullanıcısı ise bağlanılan telefon numarasından kimliğinin kolaylıkla bulunabileceğini,

- Gerçeğin kuşkuya yer vermeyecek şekilde belirlenmesi açısından; öncelikle e-posta yolu ile virüs göndererek sistemine zarar verilmiş bir bilgisayarda incelemenin,

olayın hemen akabinde yapılması ya da inceleme yapılacak bilgisayarın veya bilgisayara ait veri içeren ünitelerin, olaydan sonra inceleme yapılana kadar hiç kullanılmaması gerektiği,

- İncelenecek bilgisayarın diskine bazı bilgilerin yazılması, değişmesi veya silinebilmesini önlemek ve söz konusu diskin bütünlüğünü sağlamak için bilgisayarda virüslü dosya üzerinde inceleme yaparken ilk işlem olarak, söz konusu dosyanın birebir (sector-by-sector) yedeğinin alınması (yani incelemenin orijinal dosya üzerinde yapılmaması), daha sonra ikinci olarak alınan birebir yedeğin değiştirilip değiştirilmediğini tespite yarayacak zaman ve bütünlük kontrolü imkanı sağlayan değerin (hash) belirlenmesi,

- Bir e-postanın kimden geldiğinin tespiti için de, ilk olarak e-postayı gönderen IP adresinin bulunması (örneğin; şikayetçiye gelen e-postanın seçeneklerinden e-posta üst bilgisinin belirlenmesi ve bu üst bilginin uzman kişiler tarafından incelenmesi veya şikayetçiye gelen e-postanın göndericisinin ya da alıcısının e-posta sunucusunun sahibi şirkete belirtilen tarih ve saatte bahse konu e-postanın hangi IP adresinden gönderildiğinin sorulması,

- Daha sonra da bulunan IP adresinin belirtilen tarih ve saatte hangi abone tarafından kullanıldığının ve o abonenin açık adres ve kimlik bilgilerinin talep edilmesi ve bulunan IP adresini kullanan abonenin sanıkla bağlantısının araştırılması gerektiği"[480] ifade edilmiştir.

Bu konuya benzer bir şekil Yargıtay 8. Dairenin 2016 yılında aldığı kararlardan biri de şu şekilde ifade edilmiştir;*"Katılanın ....@hotmail.com adresine ait şifreyi kırarak ve hatırlatma sorusunu değiştirerek MSN sayfasına girilip ... adlı internet sitesindeki sayfasının kullanıldığı iddiasıyla açılan ve ilgili mail adresinin bağlı olduğu*

[480] E. Gökşen, 2014, s.115-117

Microsoft şirketine sorulmadan katılanın dosyaya sunduğu IP bilgileri üzerinden soruşturma yapılan olayda; öncelikle erişimi engellenen adresin ve e-mail adresinin sanığa ve katılana ait olup olmadığı saptanmalı, bu husus ilgili internet sağlayıcısından sorularak adreslerin oluşturulma tarihi, kim tarafından oluşturulduğu ve IP (internet Protokolu) numarası sorulmalıdır. ...'den de erişimin engellediği iddia olunan tarih/tarihler ve takip eden günlerde şikayetçinin e-mail adresine giriş yapılıp yapılmadığı, erişim sağlanmışsa IP bilgileri, bu tarihler itibariyle e-mail adresine ait şifrenin değiştirilip değiştirilmediği, değiştirilmiş ise ne zaman ve hangi IP numarası ile yapıldığı araştırılmalıdır. IP adresi kayıt bilgilerinden, ilgili... Müdürlüklerinden, sisteme giriş yapan veya başarısız olan IP numaraları kullanıcılarının adres ve telefon bilgileri istenmeli, aynı şekilde sanığa ait olduğu iddia olunan e-mail adresini kullanan IP numaraları saptanıp adres ve telefon bilgileri de istenmelidir.

Erişimin sağlanamaması halinde, giriş yapmak isteyenler arasında şikayetçinin de bulunup bulunmadığının IP numarasından tespit edilerek iddianın doğruluğu belirlenmelidir.

Suç tarihi de dikkate alınarak, sanıkla katılana ait bilgisayar ve cep telefonları getirtilip incelettirilerek tüm deliller toplandığında uzman bilirkişiden görüş alınmak suretiyle değerlendirme yapılıp sonucuna göre hukuki durumunun takdir ve tayini gerekirken, eksik incelemeye dayanarak yazılı şekilde hüküm kurulması,

SONUÇ : Yasaya aykırı, sanık müdafiinin temyiz itirazları bu itibarla yerinde görülmüş olduğundan hükmün bu sebepten dolayı 5320 Sayılı Kanun'un 8/1. maddesi uyarınca uygulanması gereken 1412 Sayılı CMUK.nun 321. maddesi gereğince (BOZULMASINA), 28.6.2016 tarihinde oybirliğiyle karar verildi."[481]

[481] Bkz. Yargıtay 8.Ceza Dairesi E.2016/5247 K.2016/8556 KT: 28.6.2016

Yargıtay 9. Ceza Dairesinin 10 Eylül 2012'de vermiş olduğu başka bir kararda da dijital delillerin delil olarak kabul edilebileceği ancak 11. Ceza Dairesinin vermiş olduğu karar kapsamında dijital delillerin kendilerine özgü özellikleri nedeniyle dikkatli bir şekilde incelenmesi gerektiği hukuka aykırı delillerin kabul edilemeyeceğini vurgulamıştır. Özellikle bilgisayar verilerinin örgütsel yapıdaki suçların aydınlatılması amacıyla kullanılabileceği ilk derece mahkemesinin kararını onayan 9. Dairenin dijital verileri delil olarak kabul ettiği ve mahkumiyet hükmü kurulabileceği bildirilmiştir. Yargıtay delillerde sahtecilik iddialarıyla ilgili iddialarda delillerin ele geçirilmesi aşamasından sonra herhangi bir değişikliğin yapılıp yapılmadığını önemsemektedir. Dijital deliller hakkındaki en önemli tartışma ne derece kuvvetli oldukları değil ne derece güvenilebilir oldukları yönündedir[482].

"CMK'nın 134. Maddesine göre", arama ve el koyma kararı, Cumhuriyet savcısının isteği doğrultusunda yargıç tarafından verilmektedir. Cumhuriyet Savcısının, suç üstü ya da gecikmesinde sakınca bulunan hallerde bile bu kararı alma yetkisi bulunmamaktadır. Cumhuriyet Savcısının bu kararı vermesi sonrasında edilen dijital delillerle ilgili el koymayı hakim onamış olsa dahi savcının emri doğrultusunda yapılacak aramada elde edilmiş deliller hukuksuzdur. Ceza muhakemesinde, ancak hukuka uygun yollarla elde edilen deliller soruşturmada ve yargılamada konu edilebileceğinden kanunda öngörülmüş olan usullerin herhangi birine uyulmaması hali elde edilen delilin "kanuna aykırı delil" olmasına neden olacaktır[483].

Ceza Muhakemesinde dijital delil olarak kullanılacak olan her verinin adli bilişim kurallarına uygun bir şekilde toplanması yine bu kurallara uygun bir şekilde saklanması ve ileri sürülmesi gerekmektedir. Bu gereklilikler dijital delilin hukuka uygunluğunu her zaman zedelemese de tek başına delil olarak kullanılmasını

[482] E. Gökşen, 2014, s.118-120.
[483] M. Özen, G. Özocak, 2015, s.63

engelleyecek bir şüphe oluşturacaktır. Yargıtay da bu görüştedir: *"Bu noktada mahkemece, katılanın konuşmalarının kaydedilmesi suretiyle oluşturulup, boşanma davasının görüldüğü dosyaya sunulan CD aslı temin edilip, kriminal inceleme yaptırılarak, görüşmedeki bayan sesinin sanığa ait olup olmadığının bilimsel olarak tespit edilmesi gerekirdi…. Görüldüğü üzere, mevcut deliller, iddiaya konu eylemi gerçekleştirenin sanık olduğunu, açık ve net olarak ortaya koymamaktadır."*[484]

Yargıtay 16. Dairesinin 2016 yılında aldığı bir kararda CMK'nın 134. Maddesinde yaşanan uygulama sorunlarına değinilmiştir. Bu madde hükümleri gereğince bilgisayarda yerinde inceleme yapılması gerekir. Ancak uygulamada bu çoğu kez mümkün ve sağlıklı olmadığından ya da teknik yetersizliklerden dolayı imajın da alınması mümkün olmamaktadır. Dijital delillerin, hukuka uygun yöntemlerle elde edilmiş olduğunun kabul edilebilmesi için delillerin kanuna uygun bir şekilde elde edilmesi, delillere harici müdahalenin olmaması gerekir. Bu konuda Yargıtay 16. Dairenin değerlendirmesi şu şekildedir; *"Adil yargılanmanın sağlanabilmesi, soruşturma ve kovuşturma aşamalarında toplanan bulguların delil değeri taşıyabilmesi için, şüpheli veya sanıktan elde edilen dijital verilerin, yasa ile sınırları belirlenmiş teknik gerekliliklere uygun olarak toplanması ve sonucunda yargılama makamlarına eksiksiz, bozulmamış halde sunulması gerekmektedir. Yasa koyucunun, CMK'nın 134. maddesini ayrıntılı olarak düzenlemesinin amacı da budur. Dijital delillere harici müdahalenin teknik olarak mümkün olması, çoğu zaman kim tarafından hangi tarihte müdahale yapıldığının da belirlenememesi karşısında, güvenli bir şekilde el konulup incelenebilmesi için mahallinde imaj alındıktan sonra orijinal medyanın şüpheliye bırakılması gerekmekte ise de bu şart soruşturma yapan kolluk personelinin teknik yetersizliği, ekipman yokluğu, ortamın incelemeye elverişli olmaması gibi nedenlerle yerine getirilememektedir.*

[484] Yargıtay 12. Ceza Dairesinin 17.06.2013 tarihli, 2012/32135 Esas, 2013/16483 Karar sayılı kararı.

Bu itibarla arama ve elkoymanın özel bir hali olarak CMK'nın 134. maddesinde düzenlenen ve özel hayatın gizliliğine daha fazla müdahale içermesi nedeniyle yasa koyucu tarafından genel arama ve elkoymadan daha sıkı koşullara tabi tutulan bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama ve elkoymanın bu özelliği gözardı edilmek suretiyle, aramayı gerçekleştiren kişilerce elkoyma işlemine geçildiği sırada sistemdeki verilerin yedeklemesi (imaj-adli kopya) yapılmadan ve yedekten bir kopya alınıp şüpheli veya vekiline verilmeden, ya da yukarıda yazılı nedenlerden dolayı mahalde yedekleme ve yedekten kopya verme olanağının bulunmadığının objektif olarak kabulünde zorunluluk bulunan hallerde, aramayı yapan kolluk birimince dijital delillere müdahaleyi önleyecek şekilde, seri numaraları tutanağa yazılmak suretiyle usulüne uygun olarak zapt edilip mühürlenmeden, şüpheli veya müdafiinin istemesi halinde nezaret etme ve denetleme imkanı sağlanarak inceleme mahalline kadar eşlik etmesi sağlanmadan ve bu yerde şüpheli veya müdafiinin hazır bulunmasına imkan verildikten sonra mümkün olan en kısa süre içinde mühür açılıp, dijital medyanın derhal imajının alınarak ilgilisine de imajlardan bir kopya ve orijinal medya teslim edilmeden, yine sanık veya müdafiinin mühür açma işlemi sırasında hazır bulunmasının mümkün olmadığı hallerde, mühür açma işleminin arama ve el koyma kararını veren hakimin huzurunda açılarak imaj alma işleminin bu sırada yapılması yoluna gidilmeden inceleme yapılması halinde arama ve elkoyma işleminin yasaya ve hukuka uygunluğundan bahsetmek mümkün olmadığı gibi bu yolla elde edilen delillerin de hukuka uygunluğu tartışılır hale gelecek ve yargılama makamınca hükme esas alınması mümkün olamayacaktır.''[485]

Yargıtay 16. Dairenin bu kararında da vurgulandığı gibi CMK 134. maddesinde belirtilen yedekleme işlemi ve incelemenin yedekleme üzerinden yapılması, ele geçirilen dijital verilere elkonulması sırasında hash değerinin alınarak delil

[485] Bkz. Yargıtay 16. Ceza Dairesi Esas No:2015/4672, Karar No:2016/2330; Aynı yönde: Yargıtay 16. Ceza Dairesi, E. 2015/2056, K. 2017/5023, T. 21.9.2017.

bütünlüğünün sağlanması ve ele geçirilen delillerden bir kopyasının imza karşılığı verilmesi gibi dijital deliller açısından hayati öneme sahip aşamalar genellikle yerine getirilmediğinden muhakeme sırasında hukuka aykırılık iddialarına sebebiyet vermektedir. Teknik yetersizlikler ve kolluk kuvvetlerinin bu konudaki bilgi ve beceri eksiklikleri karşısında ele geçirilen dijital delillerin mühürlenerek inceleme yapılacak birime sanıkla birlikte götürülmesi ya da yargılamayı yapacak olan hakimin gözetiminde delillerin açılması ve imajlarının o anda alınması bir kopyasının sanığa teslim edilmesi her ne kadar Yargıtay'ın önerdiği bir çıkış yolu olarak görülse de örgütlü suçlar ve gözaltına alınan kişi sayısının fazlalığında bunun uygulanmasında da önemli sorunlar yaşanacaktır. Ancak dijital delillerde sonradan bir oynamanın yapılmaması için kanuna uygun hareket edilmesi ve yüksek yargı organlarının içtihatlarına göre hareket edilmesi maddi gerçekliğin ortaya çıkması için en uygun seçenektir. İş yoğunluğu, personel yetersizliği, teknik imkansızlıklar, kolluk kuvvetlerinin yetenek eksikliği gibi bahanelerin hukukun üstünlüğünü akamete uğratacak sebeplerdir.

Güncel yargılamalardan biri olan FETÖ/PDY ile ilgili olarak birçok örgüt mensubu ByLock adı verilen mesajlaşma programını indirdiği ve aktif bir şekilde kullandığı gerekçeleri örgüt bağlantısı olarak görülerek haklarında mahkumiyet kararları verilmiştir. Bu karalardan bazılarının temyiz aşamasında yapılan incelemelerde mahkumiyete esas alınan delillerin hukuki niteliklerinin yetersiz olduğu birçok Yargıtay kararlarından anlaşılmıştır.

Yargıtay Ceza Genel Kurulu 26.09.2017 tarih, 2017/16.MD-956 E, 2017/370 sayılı kararıyla kesin olarak onanan "ByLock" iletişim sisteminin,"FETÖ/PDY" silahlı terör örgütü mensupları tarafından haberleşmek için kullandıkları tespit edilmiş ve örgüt talimatıyla bu ağa dahil olunduğu, "gizliliği sağlamak için haberleşme" amacıyla

kullanıldığı, "her türlü şüpheden uzak, kesin kanaate ulaştıracak teknik verilerle tespiti halinde", ***kişinin örgütle bağlantısını gösterendelil olduğu kabul*** edilmiştir.

16. Ceza Dairesi E: 2017/3394, K: 2018/453 22.02.2018 tarihli kararında, "kovuşturma aşamasından sonra dosyaya eklenen ByLock analiz raporunun CMK'nın 217. maddesi uyarınca mahkeme önünde tartışılmaması, sanık ve müdafinin diyecekleri sorulmadan karar oluşturulması" bozma kararına gerekçe olmuştur. Bununla birlikte Bazı Yargıtay kararlarında "…*sanığın ByLock kullanıcısı olduğunu bildiren ByLock HIS (CGNAT) sorgu sonuçlarının CMK'nın 217. maddesi uyarınca duruşmada sanık ve müdafiine okunarak diyeceklerinin sorulması, ByLock programı kullanıcı kimliği olan ID numarası ve varsa yazışma içeriklerinin tespiti için 'Tespit ve Değerlendirme Tutanağı' ile söz konusu GSM hattının ve cep telefonunun baz istasyonlarını gösterir HTS kaydı getirtilip karşılaştırılması ile tüm dosya kapsamının bir bütün halinde değerlendirilmesi suretiyle sanığın hukuki durumunun takdir ve tayini gerekirken sanığın ByLock kullanıcısı olduğuna dair Emniyet Genel Müdürlüğü Kaçakçılık veOrganize Suçlarla Mücadele Daire Başkanlığı tarafından düzenlenen eksik ve yetersiz olan yeni ByLock CBS sorgu sonucuna dayanılarak eksik araştırma ile yazılı şekilde karar verilmesi,*" bozma gerekçeleri olarak görülmüştür[486].

Ayrıca: "Yukarıdaki açıklamalar doğrultusunda somut olaydaki dosya kapsamına göre; şüpheli ... hakkında yapılan soruşturma evresi sonucunda, Balıkesir Cumhuriyet Başsavcılığınca düzenlenen 16.10.2017 tarihli ve 2017/9526 soruşturma, 2017/4347 esas, 2017/985 Sayılı iddianamenin iadesine dair Balıkesir 2. Ağır Ceza Mahkemesinin 18.10.2017 tarihli ve 2017/279 değişik iş sayılı kararına karşı yapılan itirazın reddine ilişkin mercii Balıkesir 3. Ağır Ceza Mahkemesinin 07.11.2017 tarihli ve 2017/702 değişik iş sayılı kararını kapsayan dosyasındaki dayanak delillerin

[486] Bkz.Yargıtay 16. Ceza Dairesi, Esas No: 2017/3652, Karar No: 2018/262; Yargıtay 16. Ceza Dairesi Esas No: 2017/3543,Karar No: 2018/256, Karar Tarihi: 06.02.2018

Dairemizin de kabul ve uygulamalarına göre terör örgütü üyeliği suçundan dava açılması için yeterli şüphe oluşturacak nitelikte olmadıkları, şüphelinin mensubu olduğu iddia edilen silahlı terör örgütü hakkında ülke genelinde kapsamlı biçimde soruşturma yapıldığı ve yeni delillerin ortaya çıktığı bu durum çerçevesinde şüphelinin hukuki durumunda değişiklik olabileceği nazara alınarak; Balıkesir 2. Ağır Ceza Mahkemesi tarafından CMK 174/1-b maddesi uyarınca 'suçun sübutuna mutlak etki eden delil' niteliğinde olduğu kabul edilerek iddianamenin iadesine sebep olarak gösterilen, 'teslim edilen dijital materyallere yönelik inceleme raporu' geldikten sonra rapor ve dosyada bulunan diğer tüm deliller birlikte değerlendirilerek sonucuna göre şüphelinin müsnet suçu işlediğine dair yeterli şüphe oluşuyor ise iddianame düzenlenmesi gerekirkenBalıkesir 2. Ağır Ceza Mahkemesinin iddianamenin iadesi kararına itiraz edilmesi yerinde görülmemiştir. ''[487]

Yargıtay'ın yukarıdaki kararlarından sonra "16. Ceza Dairesi Esas No: 2018/187, Karar No: 2018/1462, 27.03.2018 tarihli kararında" ByLock programı ile ilgili ayrıntılı bir analiz yaparak mahkumiyete esas alınacak şartları belirler nitelikte bilgi paylaşımında bulunmuştur. Bu karara göre: "…*ByLock uygulaması programını indirmek, mesajlaşmak/haberleşmek için yeterli değildir. Öncelikle kayıt esnasında kullanıcının bir kullanıcı adıyla parola üretmesi, mesajlaşma için ise kayıt olan kullanıcılara sistem tarafından otomatik olarak atanan ve kullanıcıya özel olan ID (kimlik) numarasının bilinmesi ve karşı tarafça onaylanması gerekmektedir. Karşılıklı ekleme olmaksızın iletişime geçme imkanı bulunmamaktadır.ByLock iletişim sisteminde bağlantı tarihi, bağlantıyı yapan IP adresi, hangi tarihler arasında kaç kez bağlantı yapıldığı, haberleşmelerin kimlerle gerçekleştirildiği ve içeriğinin ne olduğu tespit edilebilmektedir. Bağlantı tarihinin, bağlantıyı yapan IP adresinin tespit edilmesi ve hangi tarihler arasında kaç kez bağlanıldığının belirlenmesi, kişinin özel bir iletişim*

[487] Yargıtay 16. Ceza Dairesi, E. 2018/989, K. 2018/4981, T. 6.11.2018.

sisteminin bir parçası olduğunun tespiti için yeterlidir. Haberleşmelerin kimlerle yapıldığı ve içeriğinin ne olduğunun saptanması ise kişinin örgüt içindeki konumunu tespit etmeye yarayacak bilgilerdir.ByLock kullanıcı tespitleri ByLock sunucusunda kayıtlı IP adresleri üzerinden tespit edilebilmektedir. ByLock sunucusunda kaydı olan kullanıcıların User-ID (Kullanıcı No) tespiti yapılabilmekte ve mesaj içeriklerinin çözümü gerçekleştirilebilmektedir. Bu nedenle ByLock tespit değerlendirme tutanağında yer alan User-ID (Kullanıcı No), şifre ve gruba kayıtlı kişilerin tespiti bu kişilerin birbirleriyle olan ilişki ve irtibatlarının ortaya konulması sanığın hukuki durumunun belirlenmesi bakımından önemlidir.ByLock kullanıcılarının tespitleri açısından operatörler tarafından tutulan CGNAT (HIS) kayıtları bir çeşit üst veridir. CGNAT kayıtları özet veriler olması nedeniyle bir iz ve emare niteliğinde olduğundan tek başına kişinin gerçek ByLock kullanıcısı olduğunu göstermez. Kişiler iradeleri dışında ByLock sunucularına yönlendirilmiş olabilirler. Nitekim Ankara Cumhuriyet Başsavcılığı nezdinde yürütülen ve BTK tarafından yapılan teknik çalışmalar sonucunda iradeleri dışında ByLock sunucularına yönlendirildikleri saptanan 11.480 kişinin tamamının CGNAT kayıtlarının olduğu ve tespit edilen CGNAT kayıtlarına göre ByLock uygulamasının IP'lerine bağlantıya yönlendirildikleri belirtilmektedir."

Aynı şekilde, *"Kişinin User-ID ve şifrelerinin belirlenememesi ve fakat CGNAT kayıtlarıyla ByLock sunucusuna bağlantı yaptığının tespit edilmesi halinde, kişinin gerçek ByLock kullanıcısı olduğu ancak henüz User-ID ve şifresinin tespit edilemediği anlaşılabileceği gibi; ByLock sunucularına tuzak yöntemlerle (Morbeyin vb.) yönlendirilmiş olabileceği sonucuna da ulaşılabilir.Bu nedenle ancak operatör kayıtları ve User-ID eşleştirmesi doğru yapılabilen kişilerin gerçek ByLock kullanıcısı olduklarının kabulü gerekeceğinden, kişinin örgütsel gizliliği sağlamak ve haberleşmek amacıyla ByLock sistemine girdiğinin ve bu sistemi kullandığının, User-ID, şifre ve grup elemanlarını içerir ByLock tespit değerlendirme tutanağı ve CGNAT kayıtlarını*

içeren belgeler ile kesin olarak kanıtlanması zorunludur.Somut olayda; Erzincan İl Emniyet Müdürlüğü tarafından düzenlenen 21.06.2017 tarihli belgeye dayanılarak, ByLock kullanıcısı olduğu kabul edilerek mahkumiyetine karar verilen sanığın kimlik bilgilerinin istinaf aşamasından sonra Erzincan İl Emniyet Müdürlüğünün 28.12.2017 tarihli 'morbeyin' listesinde yer aldığının bildirilmiş olması karışışında hukuki durumunun yeniden değerlendirilerek tayin ve takdirinde zorunluluk bulunması,Bozmayı gerektirmiş, sanık müdafiinin temyiz itirazları bu itibarla yerinde görülmüş olduğundan hükmün bu sebeplerlen dolayı BOZULMASINA, 27.03.2018 tarihinde oybirliğiyle karar verildi."

Yine eldeki dijital verilerin ayrıntılı incelemesi yapılmadan verilen kararlar Yargıtay tarafından bozulmuştur : *"...yapılan arama sonucu el konulan dijital materyaller üzerinde yapılan inceleme neticesinde düzenlenen 09.12.2016 tarihli tutanakta imaj içinde yapılan kelime aramasında "..., ..., ..., ..." gibi sonuçlara ulaşıldığının bildirildiği nazara alınarak, ilgili birimlerden sanığın bylock kullanıcısı olup olmadığının etraflıca araştırılması istenip, el konulan dijital materyaller üzerinde yeniden detaylı bir inceleme yaptırıldıktan sonra, Tokat Gaziosmanpaşa Üniversitesindeki görevinden ihraç edilen sanığın idari tahkikat dosyasının da bir örneği dosya arasına getirtilip tüm deliller bir bütün halinde değerlendirilerek sonucuna göre hukuki durumun tayin ve takdir edilmesi gerektiği gözetilmeksizin eksik araştırma ile yazılı şekilde beraat kararı verilmesi"* [488].

Bu kararlardan da anlaşıldığı gibi kişinin işlediği iddia edilen suç ile ilişkili dijital verilerin delil olarak kabul edilebilmesi için sadece Emniyet Birimlerinin verdiği raporların kanıt teşkil etmediği bununla birlikte kişinin kullandığı telefon operatör kayıtları ve User-ID eşleştirmesinin doğrulanması, User-ID, şifre ve grup elemanlarını içeren ByLock tespit değerlendirme tutanağı ve CGNAT kayıtlarını içeren belgelerle

[488] Yargıtay 16. Ceza Dairesi, E. 2017/4111, K. 2018/5037, T. 11.12.2018.

kesin bir şekilde kanıtlanması zorunlu olarak görülmüş, kanuna aykırı deliller, eksik kanıtlar, eksik yargılama usulleri durumunda şüpheden sanık yararlanır ilkesi ile verilen mahkumiyet kararları bozulmuştur. Yargıtay, aynı zamanda dijital delillerin toplandığı materyallerin iadesine karar verilmemesini de hükmün bozulmasında bir sebep olarak ifade etmiştir: *"Sanığa ait dijital materyallerin inceleme sonucu geldikten sonra imajlarının dosyada delil olarak saklanmasına materyallerin ise sahibine iadesine karar verilmesi gerekirken, sanıktan ele geçirilen dijital materyaller hakkında karar verilmemesi(nden) dolayı CMK'nın 302/2. maddesi uyarınca BOZULMASINA…"*[489]

Ek olarak, Anasaya mahkemesinin de çeşitli kararlarında işaret ettiği üzere, dijital delillerin değerlendirilmesinde, bu delillerdeki hata payının ve değiştirilebilme kolaylığının da göz önünde bulundurulması ve delillerin içeriğine ilişkin itirazların ciddiye alınması gerekmektedir.[490] Anayasa Mahkemesi de şu şekilde ifade etmektedir:

"Kural olarak, bilirkişinin sunduğu rapor ve mütalaalar derece mahkemeleri açısından bağlayıcı olmamakla birlikte, İlk Derece Mahkemesi tarafından esasa ilişkin değerlendirmeler yapılırken Cumhuriyet Savcısı tarafından yaptırılan incelemelerin belirleyici bir etkisi olmuştur. Başka bir deyişle somut davada İlk Derece Mahkemesi, yalnızca dijital deliller üzerinde Cumhuriyet Savcısı tarafından yaptırılan çözümleme ve incelemeler ile kurumlardan gelen çizelgelere itibar etmiş, bu raporlara karşın başvuruculaın, mahkûmiyet kararının dayanağı olan dijital verilerin gerçeği yansıtmadığı iddialarını değerlendirmek üzere mahkemenin bilirkişi heyeti tayin etmesi ve rapor aldırması yönündeki talepleri ile bu belgelerin imajlarının verilmesi talebini reddetmiştir. Somut olayda, dijital deliller içindeki bilgi ve belgelere dayanılarak başvuruculaın mahkûmiyetine karar verilmiştir. Başvuruculaın dijital verilerin

[489] Yargıtay 16. Ceza Dairesi, E. 2019/10772, K. 2020/6583, T. 21.12.2020. ; Benzer Yönde: Yargıtay 16. Ceza Dairesi, E. 2019/5525, K. 2020/3147, T. 30.6.2020. ; Yargıtay 16. Ceza Dairesi, E. 2018/3123, K. 2020/77, T. 14.1.2020. ; Yargıtay 16. Ceza Dairesi, E. 2018/4397, K. 2018/5188, T. 17.12.2018.
[490] Fatih Birtek, **Ceza Muhakemesinde Delil ve İspat**, Adalet Yayınevi, Ankara, 2016, s. 208.

gerçeği yansıtmadığı yönündeki iddialarının araştırılması amacıyla bu deliller üzerinde bilirkişi incelemesi yaptırılması veya bunlara ilişkin imajların verilmesi taleplerinin, dijital belgelerin içeriklerinin devlet sırrı kapsamında kaldığından ve dijital delillerin usulüne uygun aramalar sonucu ele geçirildiğinden bahisle reddedilmesi yargılamanın bütünü yönünden adil yargılanma hakkını ihlal eder niteliktedir."[491]

[491] Yankı Bağcıoğlu ve diğerleri [GK], B. No: 2014/253, 9/1/2015, § 75.

SONUÇ

Kişisel bilgisayarların ve internetin Türkiyede yaygınlaşması bilgisayar, cep telefonu ve akıllı cihazların hem kurumsal hem de kişisel verilerin işlendiği birincil ortamlar haline gelmesini sağlamış, bu bilimsel gelişme bir yandan bilgiye erişimin hızlanmasını ve üretkenliği artırırken, diğer yandan yasadışı faaliyetlerin ve suç unsuru içeren her tür bilgi ve belgenin de sanal ortama taşınmasını sağlamıştır. Bundan başka sanal dünyanın kısa zamanda büyük bir güç haline gelmesi, devlet politikalarını siyasi ve ekonomik zaafa uğratması, pornografi ve zararlı madde satış alanları haline gelmesi, sosyal platformlardan insanların kişilik haklarına saldırılması, özel hayatın ihlal edilmesi gibi birçok suç unsurunun da bilgisayarlar ve akıllı telefonlarla işlenmesi bu cihazların ve diğer dijital delillerin hukuki geçerliliği hakkında ulusal ve uluslararası düzenlemelerin yapılmasını zaruri hale getirmiştir. Kimi devletler dijital delillerle ilgili özel yasalar çıkartırken kimi devletler de ceza muhakeme kanunlarına ekledikleri birkaç maddeyle sorunu çözmeye çalışmaktadır.

Dijital delillerin değerlendirmesiyle ilgili Türk Ceza Muhakemesi hukukunda önemli sorunların yaşandığı özellikle son 10 yılda yaşanan Ergenekon, Balyoz, Askeri Casusluk davalarında yaşanmıştır. Ergenekon ve Balyoz davalarında müebbetle yargılanan sanıkların dijital delil olarak ele geçirilen bilgisayar ve elektronik deliller üzerinde yapılması gereken işlemlerinin CMK 134. Maddeye aykırı bir şekilde işlem yapıldığı ve bazı delillerin değiştirildiği veya eklemelerin yapıldığına dair itirazlar geçte olsa sonuç vermiş 2015-2016 yılı itibariyle sanıklar isnat edilen suçlardan beraat ederek binlerce liralık tazminat kararları da çıkmıştır. Ayrıca devlete karşı darbe hazırlığı yapmakla suçlanan bazı üst düzey rütbeli askerlerin aklanarak önemli komutanlıkların başına getirildiği 2018 yılındaki Askeriyedeki atamalarda da görülmüştür.

17/25 Aralık 2013 olaylarıyla başlayan ve 15 Temmuz 2016 darbe girişimiyle devam eden yeni bir süreç Türk hukuk sisteminde de önemli değişikliklere yol açmıştır. Kanaatimize göre Ergenekon ve Balyoz sürecinde yaşandığı gibi bir örgüt ile mücadele edilirken Yüksek yargı kararlarının zaman zaman görmezden gelindiği, şüpheden sanık yararlanır ilkesinin çiğnendiği, dijital verilerin delil olması için uyulması gereken kanuni zorunlulukların yerine getirilmediği anlaşılmaktadır. Umarız ki ilerleyen süreçte Ergenekon ve Balyoz davalarında olduğu gibi kanunsuz yargılamalar yapıldığına dair kararlar ortaya çıkmasın ve ülke bütünlüğüne kasteden örgüt mensupları hak ettikleri cezalarla cezalandırılabilsin. Aksi halde, hukukun üstünlüğüne karşı olan inanç sarsılacak konjonktüre göre yargılamaların yapıldığı algısı oluşacak, siyasetin istediği şeyin yargı tarafından yerine getirildiği yönündeki ithamlar doğrulanmış olacaktır.

Bu sorunların yaşanmaması için her şeyden önce demokratik ve hukuk devletinde yasaların gelişen teknolojiye göre güncellenmesi gecikmemelidir. Hemen hemen her bireyin evinde ve işyerinde bulunan bilgisayarlar, hayatın bir parçası haline gelen akıllı cep telefonları, tabletler ve hafıza kartları günlük yapılan birçok faaliyetin izlerini üzerinde barındıran aletlerdir. Bu aletlerin sayısal verilerle çalışması karşılığında klasik delillerden farklı bir yapısının olduğu açık bir gerçektir. Bu nedenle de değerlendirmesinin de yine adli bilişim uzmanları tarafından yapılması bir zorunluluktur. Daha önce ifade edildiği gibi bu cihazların hayatımızın her alanında kullanılır hale gelmesi bu cihazların kişisel verileri içermesini de beraberinde getirdiğinden özel hayatın gizliliği ve iletişim özgürlüğü açısından arama ve elkoyma işlemini de klasik suçlara göre farklılaştırmıştır. Bu nedenlerle dijital delillerin değerlendirilmesi konusunda yapılması gerekenler ve sorunlara karşı alınması gerekenler şu şekilde sıralanabilir;

- Kişisel bilgisayarların ve internetin Türkiyede yaygınlaşması bilgisayar, cep telefonu ve akıllı cihazların hem kurumsal hem de kişisel verilerin işlendiği birincil

ortamlar haline gelmesini sağlamış, bu bilimsel gelişme bir yandan bilgiye erişimin hızlanmasını ve üretkenliği artırırken, diğer yandan yasadışı faaliyetlerin ve suç unsuru içeren her tür bilgi ve belgenin de sanal ortama taşınmasını sağlamıştır. Bundan başka sanal dünyanın kısa zamanda büyük bir güç haline gelmesi, devlet politikalarını siyasi ve ekonomik zaafa uğratması, pornografi ve zararlı madde satış alanları haline gelmesi, sosyal platformlardan insanların kişilik haklarına saldırılması, özel hayatın ihlal edilmesi gibi birçok suç unsurunun da bilgisayarlar ve akıllı telefonlarla işlenmesi bu cihazların ve diğer dijital delillerin hukuki geçerliliği hakkında ulusal ve uluslararası düzenlemelerin yapılmasını zaruri hale getirmiştir. Kimi devletler dijital delillerle ilgili özel yasalar çıkartırken kimi devletler de ceza muhakeme kanunlarına ekledikleri birkaç maddeyle sorunu çözmeye çalışmaktadır.

- CMK 134. Maddeye göre makul şüphe karşısında herhangi bir suç işlediği düşünülen kişiye ait bilgisayar, bilgisayar kütükleri ve programlarında arama yapabilmek ve başka şekilde incelenmesi mümkün değilse el koyabilmek için Cumhuriyet savcısının istemi hakimin de karar vermesi gerekir. Gecikmesinde sakınca olan acil durumlarda CMK 119. Maddeye göre savcının arama kararı yeterli iken CMK 134. madde hakim kararını zorunlu kılmıştır. Bu nedenle suçüstü ya da acil durumlarda bile bu cihazlara el koymak ve arama yapmak için kanun gereği hakim kararının çıkartılması zorunlu olduğundan suçlu olan kişilerin adalete teslim edilebilmesi için yasalara uygun hareket edilmesi delillerin de hukuki bir niteliğe kavuşmasının garantisidir.

- CMK 134. Maddeye ve Yargıtay kararına göre elkonulan malzemelerdeki dijital verilerin şüpheli şahsın yanında bir imaj kopyası alınmalı ve kendisine teslim edilmelidir. Bu işlem olay yerinde yapılamıyorsa elkonulan malzemeler mühürlenmeli

incelemenin yapılacağı yerde mühür şüpheli şahıs nezaretinde açılarak imajı alınmalıdır. Bu da yapılamıyorsa arama ve elkoyma kararı veren hakim nezaretinde imaj alınması gerçekleştirilmelidir. Kanaatimizce sanığı temsil eden müvekkilinin de bu işlem sırasında orda olması sonradan dijital verilerin değiştirildiğine yönelik itirazları önleyecektir. Bununla birlikte bazı davalarda bilgisayar imajlarının alınmasının saatlerce sürmesi bu uygulamanın da ihtiyaca cevap veremeyeceğini gösterecektir.

- Dijital delillerle ilgili itirazların en önemli kaynağı elkonulan dijital verilerle ilgili olarak şüpheli şahsın bu verilerin tamamını ya da bir kısmını kabul etmemesi, üzerinde oynanıldığı, değiştirildiği ve eklendiğini iddia etmesidir. Bu nedenle kanun koyucunun CMK 134. Maddede öngördüğü şartlara uygun arama ve elkoyma işleminin yapılması tüm sorunu çözecek kötü niyetli kişi ya da kişilerin delilleri karartma ya da masum insanları suçlu gösterme gayreti içinde olmasını engelleyecektir.

- Kolluk kuvvetlerinin hukuki kurallara uygun hareket etmesi verilerin değiştirilmesinin de önüne geçecek hak ve adaletten yana davranmaları hukukun üstünlüğünü ve adil yargılanmayı sağlayacaktır.

- Elde edilen dijital delilleri arama yapan kolluk kuvvetleri inceleyemez, bu verilerin incelenmesi ve hakkında rapor tutulması adli bilişim uzmanlarının işidir. Dijital adli analiz çalışmalarının her çalışmada aynı kalitede çıktı vermesi için dinamik dijital dünya ile sık sık güncellenen yasa, yönetmelik veya standartlara ihtiyaç vardır.

- Verilerin doğruluğu ve güvenilirliği adına her geçen gün yeni ürün, yazılım veya tekniklerin hayata geçirilmesi, personelin seçimi ve yetkilendirilmesi, adli bilişim disiplini içerisinde görev yapan personelin ihtisaslaşması, değerlendirmelerini bilimin aydınlatıcı ışığı altında yapmaları adli analizlerde belirli bir standardın oluşturulmasına ve daha kaliteli çıktıların üretilmesine yol açabilecektir.

- Dijital adli analiz konusunda çalışacak uzmanların hem bilgisayar teknoloji üzerine hem de "bilişim hukuku"nda eğitim almaları, hukukçuların vicdani kanaatlerinin oluşumuna önemli katkılar sunacak, hakimin dikkat etmesi gereken noktalara işaret edilerek adaletin tecelli etmesine yardımcı olacaklardır.

- Adli bilişim alanında meydana gelişmeler ve dijital delillerin doğal yapıları hakkında avukat, savcı ve hâkimin hatta kolluk kuvvetlerinin de bilgisinin olmaması, muhakemenin sadece salt "bilirkişi raporları" üzerinden yapılması önemli sorunlara yol açmaktadır. Her ne kadar hakim, teknoloji bilgisine dayanarak somut olay hakkında karar vermemesi gerekirse de bilirkişinin raporda sunduğu verileri anlaması ancak bilişim teknolojisi hakkında az da olsa bilgi sahibi olmasına bağlıdır. Bu nedenle Hâkimlerin yanı sıra tüm hukukçuların adli bilişimi kavraması bilimsel ve hakkaniyetli sonuçların elde edilmesine aracılık edecektir.

- Klasik suçların yerini bilişim suçlarının almaya başlaması ve giderek artan bir suç çeşitliliğinin olması bilişim alanında uzmanlaşmış mahkemelerin kurulmasını zorunlu hale getirecektir. Bu nedenle hukukçuların bu alanda kendilerini yetiştirmeleri, dijital adli delillerin yapısı, güvenilirliği ve hukuki niteliği hakkında hatalı yorumlar yapmalarına engel olacaktır.

-Adli bilişimin bilgisayar mühendisliği, hukuk ve kriminoloji disiplinleriyle yakından ilişkisi nedeniyle adli analizlerin "disiplinler arası" bir çalışma ile yapılması maddi gerçekliğe ulaşmayı daha da kolaylaştıracaktır. Dijital delillerin toplanması ve değerlendirilmesinin hukuki açıdan uygunluğunun yanı sıra delillerin incelenmesi sırasında bilgisayar mühendisliği bilimine ve dijital adli analiz prensiplerine riayet edilmesini de önemli kılmaktadır. Ayrıca, suçlunun psikolojisi değerlendirilerek bilgisayar kullanım alışkanlıkları hakkında kararların verilmesi kriminolojik bakış açısıyla milyonlarca veri arasından suç ve suçluyla ilgili olanı tespit etmeye

yarayacaktır. Bu nedenle hukukçuların dijital adli analiz uzmanını yönlendirmesi gibi kriminoloji ve bilgisayar uzmanlarının değerlendirmeleri de verilerin doğruluğu hakkındaki şüpheleri giderecektir.

-Dijital adli delillerin güvenilirliğiyle ilgili şüphelerde disiplinler arası çalışmanın önemli katkısı olacaktır. Bir dosyanın erişim tarihine yönelik araştırmalarda bir yandan dosyanın belirli bir tarihteki durumu sorgulanırken diğer taraftan ISP verileri toplanarak kişinin o tarihte internet üzerinde ne tür işlemler yaptığı sorgulanabilmektedir.Bu nedenleuzmanların ve avukatların dijital delillerle ilgili tecrübe, tahkikat ve incelemeye ait bilgileri, bağlamsal bilgisi, hukuk bilgisi ve iletişim yeteneği olması gerekir.

- Dijital delillerle ilgili değerlendirmelerde teknik personel yetersizliğinin giderilmesi, araştırma yöntemleri için gerekli materyalin sağlanması, dijital delillerin güvenilirliğini etkileyen zararlı yazılımlara karşı mücadele edebilecek teknik personelin yetişmesi oldukça önemlidir. Her ne kadar kanunlara uygun hareket edilse, el konulan verinin bir imajı şüpheli veya sanığa teslim edilse bile incelme yapılan imaj kopyasında bulunan özel zararlı yazılımların hareketi delillerin karartılmasına yol açabilir. Bu nedenle bu konuda uzman analistinin ilk yapması gereken işlemlerden biri eldeki imaj verinin bütünlüğünü bozacak program, virüs, solucan, truva atı gibi etkenlerden korumak olmalıdır.

Sonuç olarak dijital adli delilleri hakimin mahkemede kabul edebilmesi için delilin hukuki niteliklere sahip olması gerekir. Bu amaç doğrultusunda delil bütünlüğünün bozulmaması, ispat gücünün arttırılması için kanunlara uygun arama ve elkoyma işleminin yapılması, özel hayata saygı bağlamında kişisel verilerin korunması, adli bilişimin çağın gereklerine göre teknoloji ve personele sahip olmalıdır. Ayrıca, hukuk alanında hizmet eden her bir bireyin de tek amacının hukukun üstünlüğünü,

mahkemelerin bağımsızlığını, adil yargılanmayı, insan haklarını gözeten adil ve hakkaniyet ölçüsünde hareket eden bir kişiliğe sahip olması gerekir.

KAYNAKÇA

ACPO Good Practice Guide for Computer Based Evidence, http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf

AKALIN, Ş.H. (2002). Bilişim Türkçesi. Türk Dili Dil ve Edebiyat Dergisi, 551, 472-481.

AKHONDY, M. (1996). Ceza Muhakemesi Hukuku, Cilt 1, Kültür ve İslami Rehberlik Bakanlığı Yayınevi, Tahran.

AKYÜREK, G. (2012). Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu. Türkiye Barolar Birliği Dergisi, 101, 61-83.

ALTSCHAFFEL, R., KILTZ, S., DITTMANN, J. (2009). From the Computer Incident Taxonomy to a Computer Forensic Examination Taxonomy, 2009 Fifth International Conference on IT Security Incident Management and IT Forensics,

ANSAY, S.Ş. (1958). Hukuk Bilimine Başlangıç. 7. Baskı, Güzel Matbaası, Ankara.

ARSLAN, A.S. (2014). Doğrudanlık İlkesi. S.D.Ü. Hukuk Fakültesi Dergisi MİHBİR Özel Sayısı, 4(2), 133-144

ARSLAN, Ç. (2015). Dijital Delil ve İletişimin Denetlenmesi. CHKD, 3(2), 253-266

ASHCROFT, J., DANIELS, D.J., HART, S.V. (2004). Forensic Examination of Digital Evidence: A Guide for Law Enforcement. U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.

ASHOURI, M. (1980). Hamourabi Perspektifinden Ceza Adaleti Karşılaştırma. Hukuk Enstitü Dergisi, 7, 5.

ASHOURI, M. (1994). Ceza Muhakemesi Hukuku Cilt 1, Semt Yayınevi, Tahran,

ATAR, Y. (2000). Vergi Hukuku. Mimoza Yayınları, Konya,

AVCI, F. (2006). Ceza Yargılamasında Özel Hayatın Gizliliği Hak ve Hürriyetinin Hukuka Aykırı Olarak Elde Edilen Deliller Nedeniyle İhlal, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Konya.

AVŞAR, B. Z., ve ÖNGÖREN, G. (2010). Bilişim Hukuku, Yayın No: 270, Türkiye Bankalar Birliği, İstanbul.

AYDIN, Devrim, **Ceza Muhakemesinde Deliller**, Yetkin Yayınları, Ankara 2014.

AYERS, D. (2009). A Second Generation Computer Forensic Analysis System. Digital Investigation 6, 34-42

BAKICI, S. (2000). Olaydan Kesin Hükme Kadar Ceza Yargılaması ve Ceza Kanunu Genel Hükümler, Adalet Yayınevi, Ankara.

BALCIOĞLU, İ. (2014). İnternet Kullanımı ve Getirip Götürdükleri, Somuncubaba Dergisi, 64-67

BAŞAR, Y. (2015). Siber Suç Soruşturmalarında Adli Bilişim İncelemeleri. Yüksek Lisans Tezi,Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Afyon.

BAŞTÜRK, İ (2010). Bilgisayar Sistemleri ile Verilerinde Arama, Kopyalama ve El Koyma. Fasikül, 9, 25.

BIÇAK, V. (2011). Suç Muhakemesi Hukuku. İkinci Baskı, Seçkin Yayınevi, Ankara.

BİLGE, N., ÖNEN, E. (1978). Medeni Yargılama Hukuku Dersleri, 3. Baskı, Sevinç Matbaası, Ankara.

Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı, http://www.tbd.org.tr/bilisim-agi-hizmetlerinin-duzenlenmesi-ve-bilisim-suclari-hakkinda-kanun-tasarisi/

Bilişim Dergisi, ROM Bellek ve Çeşitleri, 2014, https://bilisimdergisi.wordpress.com/2014/01/27/rom-bellek-ve-cesitleri/#more-285

BİRTEK, F. (2013). Cumhuriyet Savcısı'nın Delilleri ve Fiili Takdir Yetkisi. Prof. Dr. Nur Centel'e Armağan, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 19 (2), 953-990

BİRTEK, Fatih, **Ceza Muhakemesinde Delil ve İspat**, Adalet Yayınevi, Ankara, 2016,

BLUM, B. (2018). Doctrines Without Borders: The 'New' Israeli Exclusinary Rule and the Dangers of Legal Transplantation. Stanford Law Review, 60(6), 2135-2136.

BURROWS, R. (2011). Judicial Confusion and The Digital Drug Dog Sniff: Pragmatic Solutions Permitting Warrantless Hashing of Known Illegal Files. George Manson Law Review, 19 (1), 255-261.

CANBEK, G., SAĞIROĞLU, Ş. (2006). Bilgi, Bilgi Güvenliği Ve Süreçleri Üzerine Bir İnceleme. Politeknik Dergisi, 9(3), 165-174

CANGEMI, D. (2004). Procedural Law Provisions Of The Council Of Europe Convention on Cybercrime. International Review of Law Computers &Technology,

CASEY, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computer and The Internet. Third Edition, Academic Press, London.

CASEY, E., and TURNBULL, B. (2011). Digital Evidence on Mobile Devices,CHAPTER 20. In: Casey, Eoghan, Digital Evidence and Computer Crime: Forensic Science, Computer and The Internet. Third Edition, Academic Press, London.

CENTEL, N., ve Zafer, H. (2011). Ceza Muhakemesi Hukuku. Beta Yayınevi, İstanbul.

CHISUM, J. (1999). Crime Reconstruction and Evidence Dynamics, Presented at the Academy of Behavioral Profiling Monterey.

CMK Madde Gerekçeleri, www.ceza-bb.adalet.gov.tr/mevzuat/cmkmaddegerekce.doc,

CMK, 5271 Sayılı Ceza Muhakemesi Kanunu, Kanun Kabul Tarihi: 04/12/2004, RG Tarihi:17/12/2004, RG Sayı: 25673http://www.ceza-bb.adalet.gov.tr/mevzuat/5271.htm

Computer Forensics World, http://www.computerforensicsworld.com/

ÇAKIR, H., KILIÇ, M.S. (2013). Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bir Bakış. Polis Bilimleri Dergisi, 15(3), 23-44

ÇAKIR, H., SERT, E. (2011). Bilişim Suçları ve Delillendirme Süreci. O. Ö. Demir ve M. Sever (Der.), Örgütlü Suçlar ve Yeni Trendler, Polis Akademisi Yayınları. Ankara,

ÇAKIR, Hüseyin, KILIÇ, Mehmet Serkan, **Adli Bilişim ve Elektronik Deliller**, Seçkin Yayıncılık, Ankara, 2020.

ÇALIŞKAN, E. (2013). Zararlı Yazılımların Etkisinde Dijital Adli Delillerin Güvenilirliği. İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezi, İstanbul.

DANİEL, L. 82011). Digital Forensic: The Subdisciplines. Digital Forensic for Legal Professions.

DEĞİRMENCİ, O. (2014). Ceza Muhakemesinde Sayısal (Dijital) Delil. 1. Baskı, Seçkin Yayıncılık, Ankara.

DEVELİOĞLU, F. (1978). Osmanlıca-Türkçe Ansiklopedik Lügat, 3. Baskı, Ankara.

DİNLER, V. (2009). Ceza Muhakemesinde Delillerin Toplanması, Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara

DOĞAN, Ramazan, **5237 Sayılı Türk Ceza Kanununda Bilişim Suçları**, Adalet Yayınevi, Ankara, 2014.

DONAY, S. (2010). Ceza Yargılama Hukuku, İstanbul, Beta Yayınları.

DOYLE, C. (1998). Computer Fraud And Abuse Laws: An Overview Of Federal Criminal Laws. Nova Science Publishers, Newyork.

DUMAN, E. (2012). Bilgisayarlarda ve Bilgisayar Ağlarında Delil Toplama ve Türkiye'deki Uygulama Sorunları, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi.

DÜLGER, M.V. (2004). Bilişim Suçları. Seçkin Yayıncılık, Ankara.

DÜLGER, M.V. (2013). Bilişim Suçları ve İnternet İletişim Hukuku. Seçkin Yayıncılık, Ankara.

EKİM, A. (2013). Bilişim Suçlarında Sayısal Delillerin Toplanması, Muhafaza Edilmesi, İncelenmesi Ve Raporlanması. Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

ERCAN, İ. (2013). Ceza Muhakemesi Hukuku (6. Bası). İstanbul.

ERDEM, M., ÖZOCAK, G. (2017). Sınıraşan Bir Suç Olarak Siber Suçlarla Mücadelede Uluslararası İşbirliği. Akademik Bilişim 2017 (AB2017) Bildiriler Kitabı,. Şubat 2017, 1-7

ERDOĞAN, Yavuz, **Türk Ceza Kanununda Bilişim Suçları**, Legal Yayıncılık, İstanbul, 2013.

EREM, F. (1964). Ceza Usülü Hukuku. Ankara Üniversitesi Hukuk Fakültesi Yayınları, Ankara.

EROĞLU, F. (2009). Beden Muayenesi ve Vücuttan Örnek Alma Suretiyle Elde Edilen Delillerin İspat Değeri. Yeditepe Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, İstanbul.

EUROPEAN COMMISSION. Justice, Data protection, Protection of personal data http://ec.europa.eu/justice/data-protection/. Erişim Tarihi: 14.11.2017

Evidence Act, (1995). http://www.austlii.edu.au/au/legis/cth/consol_act/ea199580/.

FEYZİOĞLU, M. (1996). Ceza Muhakemesi Hukukunda Tanıklık, Ankara.

FEYZİOĞLU, M. (2002). Ceza Muhakemesinde Vicdani Kanaat. Yetkin Yayınları, Ankara.

FLETCHER, G.P. (1978). Rethinking Criminal Law. Oxford University Press

FORENSIC SCIENCE COMMUNICATONS. Digital Evidence: Standart and Principles, http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/,

GARFINKEL, S.L. (2010). Digital Forensics Research: The Next 10 Years. Digital Investigation, 7, 64–73

GARZA, D. (2010). Investigating Hard Disks, File and Operating Systems. EC-Council Press ABD.

GEDİK, Doğan, **Ceza Muhakemesinde İspat**, Adalet Yayınevi, Ankara, 2018.

GERCKE, Björn, "Ceza Muhakemesine İlişkin Delil Elde Etme Önlemlerinin İçtiması" (Çev. Y. Ünver), C**eza Muhakemesi Önlemleri ve Özellikle Gizli Araştırma Önlemleri**, (ed. Yener Ünver), Seçkin Yayıncılık, Ankara, 2011,

GOODE, S. (2009). Admissibility of Electronic Evidence. The Review of Litigation, 29(1), 2-65.

GÖDEKLİ, M. (2013). Terörizmin Finansmanı Suçu. Atatürk Üniversitesi Yüksek Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi, Erzurum.

GÖDEKLİ, M. (2016). Türk Ceza Muhakemesinde Maddi Gerçeğe Ulaşmanın Ön Koşulu Olarak Hukuka Aykırı Delillerin Değerlendirilmesi Yasağı. Ankara Üni. Hukuk Fak. Dergisi, 65(4),1815-1924

GÖKCAN, H.T. (2012). Cumhuriyet Savcısının Delilleri Değerlendirme Yetkisi ve Yargıtay Uygulaması. Ankara Barosu Dergisi, 195 http://www.ankarabarosu.org.tr/siteler/ankarabarosu/tekmakale/2012-1/2012-1-9.pdf

GÖKSOY, R. (2017). Ceza Muhakemesinde Dijital Delillerin Elde Edilmesi Ve Güvenilirliğinin Sağlanması. Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir.

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

GÖKSU, M. (2011). Hukuk Yargılamasında Elektronik Delil (1086 Sayılı HUMK ve 6100 Sayılı HMK Çerçevesinde). Adalet Yayınevi, Ankara.

GÖKŞEN, E. (2014). Türk Ceza Muhakemesinde Dijital Verilerin Delil Değeri. Yüksek Lisans Tezi, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

GREGORY, J.D. (2002). Authentication Rules and Electronic Records. The Canadian Bar Review, 81(3), 529-562.

GÜNGÖR, M. (2015). Ulusal Bilgi Güvenliği: Strateji Ve Kurumsal Yapılanma. Uzmanlık Tezi, Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı, Ankara, Yayın No: 2919

HAFIZOĞLULLARI, Z., ÖZEN, M. (2012). Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar. Us-A Yayıncılık, Ankara.

HAKYEMEZ, Y.Ş. (2004). Mutlak Monarşilerden Günümüz Egemenlik Kavramı. Seçkin Yayınevi, Ankara.

HASH DEĞERİ. The Secure Hash Algorithm Directory MD5, SHA-1 and HMAC Resources, http://www.secure-hash-algorithm-md5-sha-1.co.uk/,

HEDAYATİ, M. (1963). Ceza Muhakemesi Hukuku, Tahran Üniversitesi Yayınevi, Tahran.

HEKİM, H. ve BAŞIBÜYÜK, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. Uluslararası Güvenlik ve Terörizm Dergisi, 4(2), 135-158.

HENKOĞLU, T. (2011). Adli Bilişim Dijital Delillerin Analizi. 1. Bası, Pusula Yayınları, İstanbul.

HENKOĞLU, T., YILMAZ, B. (2013). Avrupa Birliği (AB) Bilgi Güvenliği Politikaları, Türk Kütüphaneciliği, 27(3), 451-471

HIRŞT, E. (2005). Ernest Pratik Hukukta Metot. 4. Baskı, Banka ve Ticaret Hukuku Araştırma Enstitüsü Yayınları, Ankara.

HMK, Hukuk Muhakemeleri Kanunu, Kanun No. 6100, Kabul Tarihi: 12/1/2011, https://www.tbmm.gov.tr/kanunlar/k6100.html

HOSMER, C. (2002). Providing The Integrity of Digital Evidence With Time. International Journal of Digital Evidence, 1, 55.

http://pdfdergi.com. Ücretsiz Bilgisayar Dergisi, 2010, http://pdfdergi.com/4840/her-ele-bir-bilgisayar/

http://www.bilisimhukuk.com/2010/01/dijital-delillere-yargitaydan-ince-ayar/,

https://www.thinglink.com/scene/787328284789571584

Hüseyin Akarslan, Bilişim Suçlar, Ankara: Seçkin yayıncılık, 2012.

INFORMATION Q. (2016). https://www.informationq.com/central-processing-unit/

JESCHEK, H-H. (1989). 1989 Türk Ceza Kanunu Öntasarısının Genel Hükümleri Hakkında Karşılaştırmalı Bir İnceleme, Türk Ceza Kanunu Tasarısı İçin Müzakereler, Konya.

John. D. Nilsson (ED), (2010). Djital Evidence ın the Courtroom, New York: Nova Science Publishers.

JUDISH, N. (2009). Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations; Computer Crime and Intellectual Property. Section Criminal Division; Office of Legal Education Executive Office for United States Attorneys; https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf

KARAKEHYA, H. (2006). Ceza Muhakemesinde Maddi Gerçek. Eskişehir Barosu Dergisi, 10,

KARAKOÇ, Y. (1997). Türk Vergi Yargılaması Hukukunda Delil Sistemi, DEÜ Hukuk Fakültesi Döner Sermaye İşletmesi Yayınları.

KAYMAZ, Seydi, "Telekomünikasyon Yoluyla yapılan iletişimin denetlenmesinin bir koşulu olarak başka suretle delil elde etme imkanının bulunmaması", **Fasikül Hukuk Dergisi,** Yayın:2, Sayı: 3, Şubat 2010.

KAYNAKÇIOĞLU, U. (2015). Ceza Muhakemesinde Dijital Deliller. Yüksek Lisans Tezi, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

KEMP, S. (2017). Digital in 2017: Global Overview. Erişim Tarihi: 29.11.2017 https://wearesocial.com/blog/2017/01/digital-in-2017-global-overview.

KESKİN KİZİROĞLU, S. (2007). Ceza Muhakemesi Hukukunda Aykırı Deliller", Güncel Hukuk Dergisi, 32-35

KESKİN KİZİROĞLU, S., EROĞLU, F., Tepe, İ. (2013). Hazırlık Kolokyumu Bölüm III Ceza Muhakemesi Türkiye Ulusal Grup Raporu, AIDP XIX. Dünya

Kongresi, “Bilgi Toplumu ve Ceza Hukuku Hazırlık Kolokyumları”, Suç ve Ceza Ceza Hukuku Dergisi, Ocak Şubat Mart, 1, 75-100.

KESKİN, S. (1997). Ceza Muhakemesi Hukukunda Temyiz Nedeni Olarak Hukuka Aykırılık. Alfa Yayınları, İstanbul.

KIZILYAR, M. (2014). Ceza Yargılamasında Dijital Verilerin Delil Değeri, Adalet Dergisi, 50, 72-89.

KİM, Y-H., Kim, K.J. (2010). A Forensic Model on Deleted-File Verification for Securing Digital Evidence, 2010 International Conference, Information Science and Applications (ICISA); 978—1-4244-5493-8710 IEEE.

Kişisel Verilerin Korunması Kanunu 6698 Sayılı 24/3/2016. RG. Tarih: 7/4/2016 Sayı : 29677

KLOTTER, J.C. (1980). Criminal Evidence. Anderson Publishing Company, Cincinnati.

KOCA, M. (2000). Ceza Muhakemesinde Hukuka Aykırı Delilleri Değerlendirme Yasağı. Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi, 4(1-2), 105.

KOCA, M. (2006). Ceza Muhakemesi Hukukunda Deliller. Ceza Hukuku Dergisi, 1(2), Seçkin Yayınevi, Ankara

KOCAMUSTAFAOĞULLARI, M. (2013). Bilgi Güvenliği Farkındalığı Ve Uygulama Seviyesi Değerlendirmek İçin Bilgi Güvenliği Prototip Uygulaması, Yayımlanmamış Yüksek Lisans Tezi, Çankaya Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

KOÇ, İ., ÇAKIR, H. (2015). Denetim Süreçlerinde Dijital Delillerin Elde Edilmesi Ve Korunması. International Journal of Human Sciences, 12(2), 1092-1110

KOOPS, B-J. (2010). Cybercrime Legislation in the Netherlands, Electronic Journal of Comparative Law, 14(3), 17, http://www.ejcl.org/143/art143-10.pdf.

KOYUNCU, A. (2011). Ceza Adaleti Usul Hukuku İlişkisi Ve Vicdani Kanaat. Ankara Barosu Dergisi, 4, 366-367.

KUNTER, N. (1981). Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku. 7. Basım, Kazancı Matbaası, İstanbul.

KUNTER, N., YENİSEY, F. (1998). Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku. İstanbul.

KUNTER, N., YENİSEY, F., NUHOĞLU, A. (2010). Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, Beta Yayınevi, İstanbul.

KURT, L. (2005). Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması. Seçkin Yayınevi, Ankara.

KURU, B., ARSLAN, R., YILMAZ, E. (2003). Medeni Usul Hukuku. Genişletilmiş 12. Baskı, Yetkin Yayınları, Ankara.

LAST, D. (2012). Computer Analysts and Experts – Making the Most of GPS Evidence. http://articles. forensicfocus.com/2012/08/27/computer-analysts-and-experts-makingthe-most-of-gps-evidence/,

LAYKIN, E. (2013). Investigative Computer Forensics The Practical Guide for Lawyers, Accountants, Investigators, and Business Executives, USA.

LEACH, P. (2011). Taking a Case to the European Court of Human Rights. 3. Edition, Oxford University Press.

MALKOÇ, İ. (2006). Açıklamalı Yeni Türk Ceza Kanunu Özel Hükümler (170-345), II. Cilt. Malkoç Kitabevi, Ankara.

MOORE, M. (1994). The Independent Moral Significance of Wrongdoing, 5J. Contemp. Leg. Issues.

MUTLUER, M. K. (2006). Vergi Genel Hukuku, İstanbul Bilgi Üniversitesi Yayınları

ÖNGÖREN, G. (2006). İnternet Hukuku. Öngören Hukuk Yayınları, İstanbul.

ÖZBEK ve arkadaşları, **Ceza Muhakemesi Hukuku**, Seçkin Yayınevi, Ankara, 2018.

ÖZBEK, V.Ö. (2002). CMK İzmir Şerhi Ceza Muhakemesi Kanunun anlamı Açıklamalı Gerekçeli İçtihatlı. Pegem Yayınları.

ÖZBEK, V.Ö., KANBUR, M.N., KORAY, N.D., BACAKSIZ, P., TEPE İ. (2018). Ceza Muhakemesi Hukuku, Ankara.

ÖZDEMİR, A. (2015). Adli Bilişim Alanında Dijital Delil, Delil Karartma Ve Delil Toplama. Yüksek Lisans Tezi, Hacettepe Üniversitesi Fen Bilimleri Enstitüsü, Ankara

ÖZEN, M., ÖZOCAK, G. (2015). Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134), Ankara Barosu Dergisi, 1, 42-77

ÖZENÇ, K. (2007). Bilgi ve iletişim teknolojilerinde kişisel ve kurumsal bilgi güvenliğinin sağlanması. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, 13-14 Aralık 2007, Ankara.

ÖZGEN, E. (1968). Ceza Muhakemesinin Yenilenmesi. Ankara Üniversitesi Hukuk Fakültesi Yayınları, Ankara.

ÖZKAN, H. (2014). Ceza Muhakemesinde Ekran Görüntüsü Çıktılarının Delil Niteliği, Karşılaştırmalı Güncel Ceza Hukuku Serisi:15, Ceza Muhakemesi Hukukunda Delil ve İspat, Ankara.

ÖZMUMCU, S. (2014). Türk Hukukunda Yargıtay Kararları Işığında Re'sen Araştırma İlkesi. S.D.Ü. Hukuk Fakültesi Dergisi MİHBİR Özel Sayısı, 4(2), 145-171.

ÖZTÜRK ve arkadaşları, **Nazari ve Uygulamalı Ceza Muhakemesi Hukuku**, Seçkin Yayıncılık, Ankara, 2020.

ÖZTÜRK, B. (1995). Yeni Yargıtay Kararları Işığında Delil Yasakları. Ankara Üniversitesi Siyasal Bilimler Fakültesi İnsan Hakları Merkezi Yayınları, Ankara.

ÖZTÜRK, B. (2000). Ses veya Görüntü Kaydeden Araçlarla Yapılan Tespitlerin Ceza Muhakemesi Hukukunda Değeri. Prof. Dr. Seyiullalı Edis'e Armağan.

ÖZTÜRK, B. (2005). Yeni Ceza Muhakemesi Kanunu'nda Delil Yasakları. Hukuki Perspektifler Dergisi, 135

ÖZTÜRK, B., Erdem, M.R. (2006). Uygulamalı Ceza Mahkemesi. 10. Baskı, Seçkin Yayıncılık, Ankara.

ÖZTÜRK, B., TEZCAN, D., ERDEM, M.R., SIRMA, Ö., SAYGILAR, Y., ALAN, E. (2010). Nazari ve Uygulamalı Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, Ankara.

PALLI, H. (2008). Türk Hukukunda Ve Mukayeseli Hukukta Bilişim Suçları. Yüksek Lisans Tezi, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü.

PDA ne demek? 2007, http://mobilyazilar.blogspot.com.tr/2007/01/pda-ne-demek.html

PEKCANITEZ, H., ATALAY, O., ÖZEKES, M. (2005). Medeni Usül Hukuku. Yetkin Yayınları, Ankara.

PERRIN, B., RÉMY, M., ROUBATY, R. (2011). Electronic Evidence in Swiss Criminal Procedure. Digital Evidence and Electronic Signature Law Review, 8, 72-74

PETERSON, L.L., DAVIE, B.S. (2012). Computer Networks a System Approach. 5th Edition, USA.

ROGERS, M.K., GOLDMAN, J.M., RICK, W., TIMOTHY, D.S. (2006). Computer Forensics Field Triage Process Model, Conference of Digital Forensics, Security and Law, Nevada, Las Vegas.

ROMANO, L.V. (2015). VI. Electronic Evidence and the Federal Rules. Loyola Los Angles Law Review, 38,1745 -1802.

SABAN, N. (2006). Vergi Hukuku. Beta Yayınevi, İstanbul.

SAĞIROĞLU, Ş., KARAMAN, M. (2012). Adli Bilişim. Telepati Dergisi, 203, 62.

SANCAR, M. (1989). Vergi Yargısında Dava Malzemesinin Toplanması ve İspat yükü. Mali Hukuk, 24

SARSIKOĞLU, Ş. (2013). Türk Ceza Muhakemesi Hukuku'nda Beden Muayenesi ve Vücuttan Örnek Alınması. Erciyeş Üniversitesi Hukuk Fakültesi Dergisi, VIII(2)

SARSIKOĞLU, Ş. (2015). Ceza Muhakemesinde Delil Ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı. TAAD, 6(22), 427-454

SARSIKOĞLU, ŞENEL. "Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil E Delil Kavramı." **Türkiye Adalet Akademisi Dergisi** , no.22, ss. 427-454, 2015

SCHMIDT, A. H. (2004). Building a Mosaic Of Security For A Better World, Security Matters. USA, Aspatore Books.

SEZER, Yasin, Ali İhsan İpek, Engin Parlak, **Adli ve Önleme Amaçlı İletişimin Denetlenmesi**, Seçkin Yayıncılık, Ankara, 2012,

SIEBER, U. (1998). Legal Aspects of Computer Related Crimes. http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf

SINAR, H. (2001). İnternet ve Ceza Hukuku. Beta Yayınları, İstanbul.

SOMMER, P. (2012). Digital Evidence, Digital Investigation and E-Disclosure: A Guide to Forensic Readiness for Organizations. Security Advisers and Lawyers, Information Assurance Advisory Council, http://www.iaac.org.uk/_media/DigitalInvestigations2012.pdf ,

SOMMER, P., BROWN, I. (2011). Reducing Systemic Cybersecurity Risk, OECD Multi-Diciplinary. Issues International Futures Program, January www.oecd.org/dataoecd/57/44/46889922.pdf

SOYARSLAN, Doğan, **Ceza Muhakemesi Hukuku**, Yetkin Yayınları, Ankara, 2018.

SOYASLAN, D. (2010). Ceza Muhakemesi Hukuku. Yetkin Yayınları, Ankara.

SOYGÜT, A., BUKET, M. (2009). Avrupa İnsan Hakları Mahkemesi'nin Miailhe/Fransa Kararı. İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, 8(16), 159-171.

Suç Eşyası Yönetmeliği, Resmi gazete Sayı ,29662, Tarih 23 Mart 2016 http://www.resmigazete.gov.tr/eskiler/2016/03/20160323-2.htm

SYMANTEC. Internet Security Threat Report. http://www.symantec.com/content /en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf (25.09.2017).

ŞAFAK, A., BICAK, V. (2005). Ceza Muhakemesi Hukuku ve Polis. Roma Yayınevi.

ŞAHBAZ, İbrahim, **İletişimin Denetlenmesi ve Yasak Deliller**, Yetkin Yayınları, Ankara, 2009.

ŞAHİN, C. (2001). Ceza Muhakemesinde İspat (Delillerin Doğrudan Doğruyalığı İlkesi), Yetkin, Ankara.

ŞAHİN, C. (2011). Ceza Muhakemesi Hukuku I. Seçkin Yayınları, Ankara.

ŞANVER, S. (1983). Vergi Hukukunda İspat. Vergi Dünyası,

ŞENER, Y.S. (2013). Fikri Mülkiyet Hukukunda Dijital Veri Tabanlarının Korunması. Doktora Tezi, İstanbul Kültür Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

ŞENGÜL, S. (1987). Özel Hukukta ve Vergi Hukukunda Delil Sistemi. Maliye Dergisi

ŞENLEN SUNAY, S. (1997). İdari Yargılama Usulüne Hakim Olan İlkeler Karşısında İspat ve Delil Hususları. Kazancı Matbaacılık, İstanbul.

ŞİMŞEK, Y., DURMAZ, M., KARATAŞ, N. (2012). Dijital Delil Yöntemi. Polis Akademisi Yayınları, Ankara.

TANRIKULU, C. (2014). Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama Ve Elkoyma. Doktora Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü.

TAŞKIN, Ş.C. (2008). Bilişim Suçları. Beta Yayıncılık, İstanbul.

TDK. BSTS / Bilişim Terimleri Sözlüğü 1981, Veri, Erişim Tarihi: 14. 11.2017 http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5a0aee1d5bd5d8.31054914

TDK. Güncel Sözlük, belge kavramı, http://www.tdk.org.tr,

TDK. Türk Dil Kurumu, Genel Türkçe Sözlük, Bilişim. Erişim Tarihi: 13.11.2017. http://www.tdk.gov.tr/index.php?option=com_gts&kelime=B%C4%B0L%C4%B0%C5%9E%C4%B0M

TEKEREK, M. (2008). Bilgi Güvenliği Yönetimi, KSÜ Fen ve Mühendislik Dergisi, 11(1), 132

TEZCAN, D. ve ERDEM, M.R. (2002). Teorik ve Pratik Ceza Hukuku. Şafak Matbaacılık, İzmir.

TEZEL, A. (1997). Türk Vergi Hukukunda İspat ve Delil Sistemi. Yaklaşım, 56, 12.

The Commonwealth's Crimes Act 1914, http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/

TOPALOĞLU, M. (2005). Bilişim Hukuku. Karahan Kitabevi, Adana.

TOROSLU, N. (2008). Ceza Hukuku Özel Kısım. Savaş Yayınları, Ankara.

TOROSLU, N., FEYZİOĞLU, M. (2009). Ceza Muhakemesi Hukuku. Savaş Yayınları, Ankara.

TOSUN, Ö. (1976). Türk Suç Muhakemesi Hukuku Dersleri, C.II, Muhakemenin Yürüyüşü. İstanbul.

TOSUN, Ö. (1984). Türk Suç Muhakemesi Hukuku Dersleri Cilt I Genel Kısım, 4. Bası, Acar Matbaacılık, İstanbul.

TPC. (2002). Texas Penal Codes Section,

TURHAN, O. (2006). Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar). Planlama Uzmanlığı Tezi, Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Ankara.

TUTUMLU, M.A. (2007). Medeni Muhakeme Hukukunda Delillerin İleri Sürülmesi. 4. Baskı, Seçkin Yayınevi, Ankara.

TÜİK. 2017. Hanehalkı Bilişim Teknolojileri Kullanım Araştırması, Sayı: 24862, 18 Ağustos 2017. http://www.tuik.gov.tr/HbPrint.do?id=24862

Türk Ceza Kanunu Madde Gerekçeleri, www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc.

Türk Ceza Kanunu, RG: Kanun No. 5237, 26.9.2004. Bilişim Alanında Suçlar. Onuncu Bölüm, http://www.resmigazete.gov.tr/eskiler/2004/10/20041012.htm.

TÜRK HUKUK LÜGATI. (1991). Türk Hukuk Kurumu Yayını, Ankara.

UMAR, B., YILMAZ, E. (1980). İspat Yükü. Kazancı Matbaacılık, İstanbul.

USC (2002). Title 18 of the US Code, in Chapter 47, Section 1030.

USDOJ. (2004). U.S. Department of Justice, FBI LAw Enforcement Bulletin, August.

UZUNAY, Yusuf. "Dijital Delil Araştırma Süreci", **2. Polis Bilişim Sempozyumu**. Ankara, 14-15 Nisan 2005,

ÜNAL, O.G. (2011). Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma. Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Ünver Yener. "Ceza Muhakemesinde İspat, CMK ve Uygulamamız". Ceza Hukuku Dergisi (CHD). Sayı. 2, Aralık 2006, ss. 103-205.

ÜNVER, M., CANBAY, C., MİRZAOĞLU, A.G. (2011). Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum Ve Alınması Gereken Tedbirler, Ankara.

ÜNVER, Y., HAKERİ, H. (2012). Ceza Muhakemesi Hukuku, Adalet Yayınevi, Ankara.

WAGNER, A.E., BROOKE, C. (2007). Wasting Time: The Mission İmpossible With Respect To Technologyoriented Security Approaches Electronic. Journal of Business Research Methods, 5(2), 117-124.

WALDEN, I. (2007). Computer Crimes and Digital Investigations. Oxford University Press, Oxford.

Wetboek van Strafvordering, http://www.wetboek-online.nl/wet/Wetboek%20van%20Strafvordering.html.

YAVUZ, Hakan A., "Ceza Yargılamasında Bir Koruma Tedbiri Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi", **TBB Dergisi**, Sayı 60, 2005.

YAVUZ, M. (2012). Ceza Muhakemesinde İspat Sorunu. TAAD, 3(9), 151-176

YAYLA, M. (2013). Ceza Yargılamasında İspat İçin Yenilmesi Gereken Şüphe; Türkiye ve Amerika Birleşik Devletleri Sistemlerinin İncelenmesi. Ankara Barosu Dergisi, 3, 291-313

YAZICIOĞLU, R.Y. (2004). Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi. Hukuk ve Adalet: Eleştirel Hukuk Dergisi, 1 (1), 172-185.

YAZICIOĞLU, Y. (2004). Bilişim Suçları. Hukuki Perspektifler Dergisi, 2, 142-146.

YENİDÜNYA, A.C., DEĞİRMENCİ, O. (2003). Mukayeseli Hukuk ve Türk Hukukunda Bilişim Suçları, Legal Yayıncılık, İstanbul.

YENİSEY, F. (2007). Ceza Muhakemesi Hukukunda (Hukuka Uygun Bir Şekilde Elde Edilmiş) Delil. Ceza Hukuku Dergisi, 2(4), 19.

YENİSEY, Feridun, NUHOĞLU, Ayşe, **Açıklamalı Ceza Muhakemesi Kanunu**, Cilt1, Beta, İstanbul, 2013.

YETİM, S. (2014). Siber Suçlar, Yargılama Yetkisi ve Yeni Bir Model Önerisi. TAAD, 5(17), 183

YILDIRIM, M.K. (1990). Medeni Usül Hukukunda Delillerin Değerlendirilmesi. Kazancı Hukuk Yayınları, İstanbul.

YILDIZ, A.K. (2002). Ceza Muhakemesinde İspat ve Delillerin Değerlendirilmesi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Doktora Tezi, İstanbul.

YILDIZ, S. (2007). Suçta Araç Olarak İnternetin Teknik Ve Hukuki Yönden İncelenmesi. Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 17, 609-623.

YILMAZ, E. (1996). Hukuk Sözlüğü. Yetkin Yayınları, Ankara.

YILMAZ, S. (2011). 5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar. TBB Dergisi, (92), 62-100.

YURTCAN, E. (1998). Yargıtay Kararları Işığında Hukuka Aykırı Delillere Dayanma Yasağı. İstanbul Üniversitesi Hukuk Fakültesi.

YURTCAN, E. (2005). **Ceza Yargılaması Hukuku**. 11. Baskı, Vedat Kitapçılık, İstanbul.

YURTCAN, Erdener, **Ceza Yargılaması Hukuku**, Adalet Yayınevi, Ankara, 2018,

ZİYAADDİN, (1979). **Peymani Devrimi'nin Hukukunda Adli Deliller**, Cilt 1. Horremi Yayınevi, Tahran.

ZUCKERMAN, A. (1989). **The Principle of Criminal Evidence**. Oxford University Press, Oxford.

Yargıtay Ceza Genel Kurulu'nun 19.04.1993 tarih, E.1993/6-79, K.1993/108

Yargıtay 4. Ceza Dairesi'nin 06.11.2007 tarih, E.2007/8601, K.2007/8929

Yargıtay Ceza Genel Kurulu'nun 19.04.1993 tarih, E.1993/6-79, K.1993/108

Yargıtay 4. Ceza Dairesi'nin 06.11.2007 tarih, E.2007/8601, K.2007/8929

Yargıtay CGK. 19.04.1993, 6-79/108, YKD Ekim 1993.

Yargıtay CGK, E. 1993/6-79, K.1993/108, T. 19.04.1993 (YKD C.19, S.10, Ekim 1993, s.1565).

Yargıtay İçtihadı Birleştirme Kurulu, 09.10.1940 gün ve 1938/38-1940/79

Yargıtay 6. CD. 4.7.1983, 2707/3846,

Yargıtay 14. CD., 14/4/2014 T., 2012/7985 E, 2014/5302 K

Yargıtay Sekizinci Ceza Dairesinin 24/10/2013 tarih ve E.2012/21817, K.2013/25428

Yargıtay Kararı, 9. C.D.'nin 10.09.2012 tarihli ve 3282/ 8981

Yargıtay 7. Ceza Dairesi'nin 03.07.2013 tarih, E.2013/5127, K.2013/17549

Yargıtay CGK, E: 2007/5-101, K: 2008/3, 22.1.2008

Yargıtay 11.Ceza Dairesi 05.02.2013 gün ve Esas Yargıtay 4.Ceza Dairesi 30.11.2011 gün ve Esas No: 2011/2606 Karar No: 2011/22901

Yargıtay CGK. 19.04.1993, 6-79/108

Yargıtay 16. Ceza Dairesi Esas No:2015/4672, Karar No:2016/2330

Yargıtay 8.Ceza Dairesi E.2016/5247 K.2016/8556 KT: 28.6.2016

Yargıtay 16. Ceza Dairesi Esas No:2015/4672, Karar No:2016/2330

Yargıtay 16. Ceza Dairesi, Esas No: 2017/3652, Karar No: 2018/262

Yargıtay 16. Ceza Dairesi Esas No: 2017/3543,Karar No: 2018/256

ÖZET

CMK 134. Madde, bilgisayarlarda arama ve el koymanın hukuki rejimini düzenleyen bir maddedir. Hangi şartlar altında bilgisayar incelemesine başvurulacağı, incelemenin hangi kapsamda yapılacağı ifade edilmiştir. Bu madde gerekçesine göre iki yıl veya daha fazla hürriyeti bağlayıcı cezayı gerektiren cürümlerde, "başka suretle delil elde etme" imkanının bulunmaması halinde Cumhuriyet Savcısının istemi hakimin yazılı emri ile bu malzemelerde arama yapılabilecek ve şifreleme, teknik imkansızlıklar gibi nedenlerle yerinde inceleme imkanı yok ise zorunlu olarak geçici bir şekilde elkonulabilecektir. Yargıtay, CD, DVD, flash bellek, disket, harici ve dahili harddisk, bilgisayar özelliği içeren noktaları bakımından akıllı telefon ve benzerlerinden elde edilenlerin tamamını 'dijital delil' olarak adlandırmıştır. Dijital verilerin delil olarak mahkeme huzurunda tartışılabilmesi için bu verilerin ele geçirilmesi, saklanması, incelenmesi ve raporlaştırılmasında kanuni zorunluluklarının yerine getirilmesi, kanuna aykırı delil niteliğinde olmaması, elde edilen delilin bütünlüğü ve güvenilirliğini gösteren has değeri ve imaj kopyalarının sanığın yanında veya arama kararı veren hakimin yanında mührünün açılarak alınması, incelemelerin imaj dosyalar üzerinde yapılmış olması, delil üzerinde her hangi bir oynama, ekleme ya da silme işleminin olmaması, işlenen suç ile dosya oluşturma hareketlerinin tarih ve zamansal açıdan uyuşması, verinin şüpheliye ait olduğu gibi kriterlerin bilimsel ve adli bilişim yöntemleriyle ispatlanması gerekir.

Anahtar Kelimeler: Dijital deliller, Bilgisayar, Ceza Muhakemesi, Veriler,Ispat

ABSTRACT

Criminal Procedure Code (CPC) Article 134 is an article regulating the legal regime of search and seizure of computers. The conditions under which the computer examination will be applied and the scope of the examination are stated. According to the justification of this article, in crimes that require a penalty of two years or more, if there is no possibility of "obtaining evidence by other means", by the request of the Public Prosecutor and the written order of the judge these devices can be searched and if there is no possibility to examine on site due to encryption, technical impossibilities, etc. they may necessarily need to be temporarily seized. The Supreme Court has named all of the information obtained from CD, DVD, flash memory, floppy disk, external and internal hard disk, smart phones and the like in terms of characteristics containing computer features, as "digital evidence". In order for digital data to be discussed before the court as evidence they should meet the below mentioned requirments. It is necessary to fulfill the legal obligations in the acquisition, storage, examination and reporting of these data. It is not to be unlawful evidence.The unique value indicating the integrity and the reliability of the evidence obtained and image copies should be taken by opening the seal in the presence of the defendant or the judge who made the search decision. Criteria such as investigations on image files, absence of any manipulation, addition or deletion on the evidence, date and temporal agreement of the crime committed and file creationprocess, data belonging to the suspect must be proven by scientific and forensic methods.

Keywords: Digital evidence, Computer, Criminal Procedure, Data, Proof