T.C.
ATILIM ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANA BİLİM DALI
KAMU HUKUKU YÜKSEK LİSANS PROGRAMI

CEZA MUHAKEMESİ HUKUKUNDA DİJİTAL DELİLLER

Yüksek Lisans Tezi

Zeynel Abidin AYHAN

Ankara-2022

T.C.
ATILIM ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANA BİLİM DALI
KAMU HUKUKU YÜKSEK LİSANS PROGRAMI

CEZA MUHAKEMESİ HUKUKUNDA DİJİTAL DELİLLER

Yüksek Lisans Tezi

Zeynel Abidin AYHAN

Tez Danışmanı

Dr. Öğr. Üyesi Özgür TAŞDEMİR

Ankara-2022

KABUL VE ONAY

Zeynel Abidin AYHAN tarafından hazırlanan "Ceza Muhakemesi Hukukunda Dijital Deliller" başlıklı bu çalışma 02/06/2022 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından Kamu Hukuku Ana Bilim Dalı, Kamu Hukuku Programında Yüksek Lisans Tezi olarak oy birliği/oy çokluğu ile kabul edilmiştir.

Doç. Dr. Ali Rıza TÖNGÜR (Başkan)

Dr. Öğr. Üyesi Özgür TAŞDEMİR (Danışman)

Dr. Öğr. Üyesi Timuçin KÖPRÜLÜ (Üye)

Doç. Dr. Şule TUZLUKAYA

Enstitü Müdürü

ETİK BEYAN

Atılım Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Kılavuzuna uygun olarak hazırladığım bu tez çalışmasını;

- Akademik ve etik kurallar çerçevesinde hazırladığımı,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne atıfta bulunarak kaynak gösterdiğimi,
- Bu tezde sunduğum çalışmanın özgün olduğunu bildirir,

Aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

02.06.2022

Zeynel Abidin AYHAN

ÖZ

AYHAN, Zeynel Abidin. Ceza Muhakemesi Hukukunda Dijital Deliller, Yüksek Lisans Tezi, Ankara, 2022.

Teknolojinin gelişimi ile birlikte suçun da dijitalleşmesi kaçınılmaz olmuştur. Günümüzde ise teknolojinin gelişme hızı, küresel boyuta ulaşan suçların, olağan suçlar haline gelmesine yol açmaya başlamıştır. Söz konusu suçların aydınlatılması bakımından büyük önem arz eden dijital delillerin ele alınması ise günümüzde bir zorunluluk halini almıştır.

Nitel araştırma yönteminin kullanıldığı bu çalışmada; dijital- elektronik delil kavramları arasındaki farklara değinilerek dijital delil kavramının kullanımının daha doğru olduğu, dijital delillerin bir delil türünü temsil etmediği fakat delilin bulunduğu yapıyı ifade ettiği, dijital delillerin elde edilmesinin teknik boyutunu oluşturan adli bilişim bilimi hakkında eksik olan düzenlemelerin uygulamada sıkıntılara yol açtığı, yine dijital delillerin elde edilmesinin temel kaynağı olan Ceza Muhakemesi Kanunu'nun 134. maddesinin kapsamı başta olmak üzere çeşitli boşlukları barındırdığı ve bu bağlamda yeniden düzenlenmesi gerektiği, dijital delillerin hükme esas alınabilmeleri bakımından taşıması gereken teknik özelliklere mevzuatımızda yer verilmediği ve buradan doğan sıkıntıların çözümlenmesinin uygulamaya bırakıldığı gibi sonuçlara ulaşılmıştır.

Gerçekleştirilen araştırma, teknolojinin gelişim hızının geometrik bir şekilde artması karşılığında hukuk düzenlemelerinin aritmetik ve hatta sabit bir hızda ilerleyiş gösterdiğini ve bu durumun, günümüzde yarattığı sıkıntılar bir yana, ileride daha da büyük sıkıntıların doğmasına neden olacağını göstermiştir. Bu bağlamda en azından gelişen teknolojiye uyum sağlayabilecek kapsayıcı düzenlemeler yapılmasının önemi ortaya çıkmıştır.

Anahtar Sözcükler: Dijital Delil, Adli Bilişim, Ceza Muhakemesi Hukuku, Bilişim Sistemi, Kabul Edilebilirlik

ABSTRACT

AYHAN, Zeynel Abidin. Digital Evidence in Criminal Procedure Law, Master Thesis, Ankara, 2022.

With the development of technology, the digitalization of crime has become inevitable. Today, the speed of development of technology has started to cause crimes that have reached a global dimension to become ordinary crimes. The handling of digital evidence, which is important in terms of illuminating these crimes, has become a necessity today.

In this study, in which the qualitative research method was used, some results were obtained. In this context, it has been determined that the use of the concept of digital evidence is more accurate by mentioning the differences between the concepts of digital and electronic evidence. Digital evidence does not represent a type of evidence, but expresses the structure in which the evidence is found. Incomplete regulations on forensic science, which constitutes the technical dimension of obtaining digital evidence, cause difficulties in practice. Again, article 134 of the Criminal Procedure Code, which is the main source of obtaining digital evidence, contains various gaps, especially its scope, and therefore needs to be rearranged. The technical features that digital evidence must have in order to be taken as a basis for judgment are not included in our legislation and the solution of the problems arising from this is left to practice.

The research carried out has shown that legal regulations progress at an arithmetic speed and even at a constant speed in return for the geometrical increase in the development speed of technology, and this situation will cause even greater problems in the future, let alone the problems it creates today. In this context, the importance of making inclusive regulations that can at least adapt to the developing technology has emerged.

Key words: Digital Evidence, Computer (Digital) Forensics, Criminal Procedure Law, IT System, Admissibility

İÇİNDEKİLER

SİMGELER VE KISALTMALAR DİZİNİ

ABD : **Ankara Barosu Dergisi**

AİHM : **Avrupa İnsan Hakları Mahkemesi**

AİHS : **Avrupa İnsan Hakları Sözleşmesi**

AÜHFD : **Ankara Üniversitesi Hukuk Fakültesi Dergisi**

AYM : **Anayasa Mahkemesi**

Bkz. : **Bakınız**

C. : **Cilt**

CD. : **Ceza Dairesi**

CGK : **Ceza Genel Kurulu**

CMK : **5271 Sayılı Ceza Muhakemeleri Kanunu**

E. : **Esas Numarası**

Hk. : **Hakkında**

HukDer : **Hukuk Dergisi**

K. : **Karar Numarası**

KVKK : **Kişisel Verilerin Korunması Kanunu**

m. : **Madde**

PVSK : **Polis Vazife ve Salâhiyet Kanunu**

S. : **Sayı**

SSS : **Sanal Ortamda İşlenen Suçlar Sözleşmesi (Siber Suçlar Sözleşmesi)**

s. : **Sayfa**

T. : **Karar Tarihi**

TAAD : **Türkiye Adalet Akademisi Dergisi**

TCK : **5237 Sayılı Türk Ceza Kanunu**

Vb. : **Ve benzeri**

V.d. **: Ve diğerleri**

Yar. **: Yargıtay**

YCGK **: Yargıtay Ceza Genel Kurulu**

Yuk. **: Yukarıda**

GİRİŞ

Ceza muhakemesi, günümüzde şüpheli ve sanığın haklarına saygılı bir biçimde maddi gerçeğe ulaşmayı amaçlamaktadır.[1] Maddi gerçeğe ise yargılamaya konu suçun gerçekten işlenip işlenmediğinin tespit edilmesi, failinin gerçekten kim olduğunun belirlenmesi ve sonuç olarak görünüşteki gerçeğin değil asıl gerçeğin araştırılması suretiyle ulaşılabilecektir.[2] Ancak ceza muhakemesinde bu amaca ulaşılmasından önce iki farklı aşamadan geçildiğini belirtmemiz gerekir. Bunlar *suçlunun cezalandırılması aşaması* ve *sanığın korunması aşamasıdır*.[3] Aydınlanma dönemine kadarki süreçte geçerli olan suçlunun cezalandırılması aşamasında sanığın suçlu olduğu baştan kabul edilmiş ve bu sebeple başka bir delil aranmamış, sanığın suçunu kabul etmesi yeterli görülmüştür. Buna karşılık aydınlanma dönemine geçiş sonucu sanığın korunması aşamasına geçilmesi ile birlikte masumiyet karinesi[4] kabul edilmeye başlanmış ve böylece de ceza muhakemesinin amacı, suçluluğu peşinen kabul edilmiş olan sanığı cezalandıracak delillere ulaşmak yerine gerçeğin araştırılıp ortaya konulması şekline dönüşmüştür.[5]

Gerçek araştırılmaya çalışılırken de karar mercilerinin en büyük aracı deliller olacaktır. Çünkü yargıç, kararını bizzat temasa geçtiği delillerle dayanarak verecektir.[6]

> *"Gölgesi altında bulunduğumuz yeni çağ, hayatımızın sayısallaşacağını (dijitalleşeceğini) ve sanallaşacağını, sayısallaşamayan bölümünün dahi verilerle temsil edilebilir duruma geleceğini bize söylüyor."*[7]

Günümüzde teknolojinin gündelik hayatımızda yarattığı olağanüstü değişimin elbette ki suç dünyasına da yansımaları olmuş ve dijital suçlar gündeme gelmiştir. Öyle

---

[1] Nur Centel ve Hamide Zafer, *Ceza Muhakemesi Hukuku*, Yenilenmiş ve Gözden Geçirilmiş Yirminci Bası (İstanbul: Beta Yayıncılık, Eylül 2021) 6; Bahri Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku* (Ankara: Seçkin Yayınevi, Güncellenmiş 15. Baskı, 2021), 31; Durmuş Tezcan, v.d., *Dijital Ceza Muhakemesi Hukuku*, ed., Bahri Öztürk, Durmuş Tezcan, Mustafa Ruhan Erdem (Ankara: Seçkin Yayıncılık, Güncellenmiş ve Genişletilmiş 2. Baskı, 2022), 37; Nevzat Toroslu ve Metin Feyzioğlu, *Ceza Muhakemesi Hukuku* (Ankara: Savaş Yayınevi, 18. Baskı, Ekim 2018), 8.

[2] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 8.

[3] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 6-7.

[4] Masumiyet karinesi, kişinin suçluluğu hükmen sabit oluncaya kadar masum sayılmasını öngörmektedir. Buna göre; Avrupa İnsan Haklar Sözleşmesi (AİHS) m. 6/2: *"Bir suç ile itham edilen herkes, suçluluğu yasal olarak sabit oluncaya kadar masum sayılır."*, 2709 sayılı Türkiye Cumhuriyeti Anayasası (RG, 17844) m. 38/4: *"Suçluluğu hükmen sabit oluncaya kadar, kimse suçlu sayılamaz."*

[5] Devrim Aydın, *Ceza Muhakemesinde Deliller*, (Ankara: Yetkin Yayınları, 2014), 15-16.

[6] Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* 295.

[7] Özgür Taşdemir, "Ceza Adaletini Dijitalleştirmek, Büyük Veri Vicdani Kanaate Karşı," ed., Bilge Y, *Sağlık Alanında Büyük Veri Analitiği ve Uygulamaları*, 1. Baskı, Ankara: Türkiye Klinikleri (2021): 38.

ki bu değişimle birlikte geleneksel suçlar da artık dijital bir biçimde işlenebilir hale gelmişlerdir.[8] Tüm bu gelişmeler, karşımıza "Dijital Delil" kavramını çıkarmıştır. Zira *"teknolojinin çıktıları, toplumu ve toplumdan kaynaklanan suçu, dolayısıyla da suç delillerini fizikselden sayısala doğru hareketlendirmektedir."*[9]

1990'larda, İnternet'in ticarileşmesi ve World Wide Web'in (WWW) gelişmesi İnternet'i popüler hale getirmiş ve milyonlarca kişi tarafından erişilebilir kılmıştır. Zamanla küresel ağdaki suçlar çeşitlenmiş ve suçlar bilişim sistemlerine izinsiz girişlerin ötesine geçmiştir.[10] Dijital deliller, suçun artık küresel hale geldiği gerçeği göz önüne alındığında daha da önemli hale gelmektedir. Bu konuda teröristlerin sosyal ağlar aracılığıyla iletişim kurarak veya anlık mesajlaşma sistemlerini kullanarak çevrimiçi bir şekilde sohbet ederek saldırılarını organize ettiğini söylemek yeterli olacaktır.[11]

Günümüz dijital toplumunda, her tür soruşturmanın potansiyel olarak dijital bir boyutu vardır. Bir başka ifadeyle incelenen vakayla ilgili bilgilerin tamamı değilse de önemli bir kısmı, ilgili taraflara ait olan bilişim sistemlerine kadar takip edilebilmekte ve buralardan çeşitli çıktılar alınabilmektedir.[12]

Öyle ki dijital deliller, yalnızca bilişim suçları bakımından değil, bilişim suçları dışında kalan suçlar bakımından da stratejik önem taşımaktadır.[13] Dijital delillere dayanmayan cezai soruşturmalar gün geçtikçe istisna haline gelmeye başlamış ve hatta

[8] Çetin Arslan, "Hukuk Öğretiminde Adlî Bilişim Türkiye Örneği Bağlamında Bir Değerlendirme," *2nd International Symposium on Digital Forensics and Security (ISDFS'14),* Houston, TX (2014): 83.
[9] Olgun Değirmenci, "Bilgi Toplumunun Delil Türü: Sayısal Deliller ve Bilimselliği," *Terazi Hukuk Dergisi,* Cilt: 9, Sayı: 97 (Eylül 2014): 20- 21.
[10] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, Third Edition* (USA California: Academic Press, Published by Elsevier Inc., 2011), 36.
[11] Maria Angela Biasiotti, "Present and Future of the Exchange of Electronic Evidence in Europe", *Law, Governance and Technology Series*, ed. Maria Angela Biasiotti, v.d., vol. 39, Cham, Switzerland: Springer, (2018): 14.
[12] Maria Angela Biasiotti, v.d., "Introduction: Opportunities and Challenges for Electronic Evidence Handling and Exchanging Electronic Evidence Across Europe," *Law, Governance and Technology Series*, ed. Maria Angela Biasiotti, v.d., vol. 39, Cham, Switzerland: Springer, (2018): 4.
[13] Biasiotti, v.d., "Introduction: Opportunities," 5; Delia Magherescu, "Enhancing Procedure of Using New Means of Technologies in Criminal Proceedings," *IUS ET SCIENTIA*, Vol. 6, No. 1 (2020): 9; Olgun Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj) Yönteminin Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi," *Bilişim Hukuku Dergisi*, C. 2, S. 1 (2020) 57- 58; Yusuf Başlar, "Elektronik Delil ve Ceza Yargılamasında Kabul Edilebilirliğine İlişkin Bir İnceleme," *Legal Hukuk Dergisi,* Cilt: 16, Sayı: 184 (2018): 1655; Murat Kızılyar, "Ceza Yargılamasında Dijital Verilerin Delil Değeri," *Adalet Dergisi*, Sayı: 50 (2014): 79.

dijital delillerin önemi, "geleceğin tek delil türü" şeklinde ifade edilerek belirtilmiştir.[14]

Bu modern çağda, dijital boyutu olmayan bir suçu hayal etmek zordur.[15] Gerçekten de artık büyük miktarda kişisel verinin toplanması ve işlenmesi günümüzde günlük bir faaliyete dönüşmüştür.[16] Bu sebeple de herhangi bir bilişim cihazı, yürütülen bir soruşturmanın ya doğrudan bir aracı ya da soruşturma konusu suçla ilgili bir bilgi kaynağı haline gelmiştir.[17]

Konuyla bağlantısı bakımından güncel bir gelişmeden de söz etmek yerinde olacaktır. Hâkimler ve Savcılar Kurulu Birinci Dairesinin, 25.11.2021 tarihli ve 1229 sayılı kararı[18] uyarınca bilişim ile ilgili düzenlenen suçlara ilişkin açılacak davalara bakacak mahkemeler nezdinde ihtisas mahkemelerinin belirlenmesi hususunda bir karar verilmiştir. Bu karar uyarınca asliye ve ağır ceza mahkemelerinin görev alanına giren bazı doğrudan bilişim suçları ve bazı dolaylı bilişim suçları (bilişim sistemlerinin suçun işlenmesinde araç olarak kullanıldığı suçlar), bilişim suçları mahkemesinin görev alanına geçirilmiştir. Bu suçlar;

I) *"26.09.2004 tarihli ve 5237 sayılı Türk Ceza Kanunu'nun; 1) Bilişim sistemlerinin kullanılması suretiyle nitelikli hırsızlık (madde 142/2-e), 2) Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle nitelikli dolandırıcılık (madde 158/1-f), 3) Kişinin, kendisini kamu görevlisi veya banka, sigorta ya da kredi kurumlarının çalışanı olarak tanıtması veya bu kurum ve kuruluşlarla ilişkili olduğunu söylemesi suretiyle nitelikli dolandırıcılık (madde 158/1-l), 4) Bilişim sistemine girme (madde 243), 5) Sistemi engelleme, bozma, verileri yok etme veya değiştirme (madde 244), 6) Banka veya kredi kartlarının kötüye kullanılması (madde 245), 7) Yasak cihaz veya programlar (madde 245/A), 8) Bilişim alanında yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbiri uygulanması (madde 246)"*

[14] Alexander Seger, "e-Evidence and Access to Data in the Cloud Results of the Cloud Evidence Group of the Cybercrime Convention Committee," *Law, Governance and Technology Series*, ed. Maria Angela Biasiotti, v.d., vol. 39, Cham, Switzerland: Springer, (2018): 35; Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj)," 56; Şenel Sarsikoğlu, "Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı," *Türkiye Adalet Akademisi Dergisi*, Yıl:6, Sayı:22 (Temmuz 2015): 527- 528.

[15] Casey, *Digital Evidence*, 3; Ann D. Zeigler and Ernesto F. Rojas, *Preserving Electronic Evidence for Trial* (USA: Elsevier Science, 2016), 55.

[16] Daniel Drewer and Jan Ellermann, "The Online Environment as a Challenge for Privacy and the Suppression of Crime," *Law, Governance and Technology Series*, ed. Maria Angela Biasiotti, v.d., vol. 39, Cham, Switzerland: Springer, (2018): 141.

[17] Zeigler and Rojas, *Preserving Electronic Evidence for Trial*, 55.

[18] Resmî Gazete Tarihi: 30 Kasım 2021, Sayı: 31675.

II) *"29.04.1959 tarihli ve 7258 sayılı Futbol ve Diğer Spor Müsabakalarında Bahis ve Şans Oyunları Düzenlenmesi Hakkında Kanun'da düzenlenen suçlardan kaynaklanan dava ve işler."*

Bilişim suçları alanında ihtisaslaşan mahkemelerin kurulması, dijital delillerle ilgili yaşanan belli bazı sıkıntıların önüne geçilebilmesi bakımından olumlu bir adım olarak değerlendirilebilir. Gerçekten de alana özgü mahkemelerin bilişim suçlarına yaklaşımının, diğer mahkemelere oranla daha doğru ve uluslararası düzenlemelerle daha paralel olacağı düşünülebilir. Bununla birlikte bilişim mahkemelerinin görevine giren suçlar incelendiğinde ilgili düzenlemenin olumlu fakat yine de eksik olduğunu söylemek yanlış olmayacaktır. Yukarıda da belirtildiği üzere günümüzde bilişim suçları dışında birçok suçun da dijital bir boyut içerdiği kaçınılmaz bir gerçektir. Adli bilişimin öneminin ortaya çıktığı bu tarz suçların ise bir kısmının bilişim suçları mahkemesinin görev alanına, kalanların ise yine asliye ceza ve ağır ceza mahkemelerinde görülmeye devam edecek oluşu, görüş ayrılıklarına sebebiyet verebilecek potansiyeldedir. Özellikle mevzuattaki boşluklar ve bu boşlukların mahkemeler aracılığıyla doldurulması gerekliliği düşünüldüğünde belirli kavramların tanımlanması ve çeşitli başlıkların sınırlarının belirlenmesi konusunda farklı tanımlamalar gündeme gelebilecek ve günümüzde yaşanan kargaşa katlanabilecektir.

Bu gelişmelerin, ceza muhakemesi hukukuna yansımalarını ele almak amacıyla çalışmamızda öncelikle birinci kısımda dijital deliller tanımlamaya çalışılmış, geleneksel deliller ile arasındaki farklar tespit edilmeye çalışılmış ve uluslararası hukukta dijital delillerin nasıl ele alındığı açıklanmaya çalışılmıştır. İkinci kısımda öncelikle dijital delillerin elde edilişinin teknik ve hukuki olmak üzere iki boyutuna değinilmiş ve dijital delillerin elde edilişi, adli bilişim ve ceza muhakemesi hukuku perspektifinde ele alınmış, devamında Türkiye'nin de taraf olduğu siber suçlar sözleşmesi uyarınca dijital delillerin nasıl ele alınmaları gerektiği değerlendirilmeye çalışılmış ve önleyici kolluk tedbirleri çerçevesinde elde edilen dijital delillerin delil değerleri belirlenmeye çalışılmıştır. Son olarak üçüncü bölümde dijital delillerin ispat değerleri belirlenmeye çalışılmış ve bu bağlamda dijital delillerin delil olarak kabul edilebilmeleri için taşımaları gereken teknik özelliklerine değinilmiştir. Ek olarak dijital delillerin güvenilirliklerinin nasıl sağlanabileceği ve uygulamada bunun için hangi işlemlerin gerçekleştirildiğine değinilmiş ve delil yasakları kavramı çerçevesinde dijital delillerin konumları belirlenmeye çalışılmıştır.

Çalışmamız sürecinde dijital delillerle ilgili olarak birçok açından çeşitli sorunlar tespit edilmiş ve bu sorunlara cevap aranmaya çalışılmıştır. Bu sorunlara kısaca değinecek olursak ilk olarak "dijital delil" kavramının kullanımı bakımından uygulamada ve doktrinde terminoloji bakımından bir kargaşa olduğu; ikinci olarak teknolojinin gelişme hızı karşısında yavaş kalan hukuk sistemlerinin, dijital ortamda işlenen suçlar bakımından suçun işlendiği yerin tespit edilebilmesi bakımından yetersiz kaldığı ve bu bağlamda uluslararası boyut kazanabilen dijital suçlar bakımından adli yardımlaşma kurallarının yeterince etkin olmadığı; üçüncü olarak dijital deliller bakımından delil ile fail arasında her zaman kolay bir şekilde bağlantı kurulamadığı ve bu sebeple dijital delillerin belirti delili olarak sayılması eğilimi gösterildiği tespit edilmiştir. Fakat kanımızca günümüz teknolojisinin gelişimi karşısında bu eğilimin gerçekçilikten uzak olduğu ve dijital delillerin de doğrudan delil sayılabilmeleri önünde bir engel olmadığı ileri sürülmüştür. Dördüncü ve son olarak dijital suç soruşturmaları sırasında gerçekleştirilen arama ve elkoyma işlemlerinin, başta özel hayatın gizliliği ve bu doğrultuda kişisel verilerin korunması gibi pek çok hakka büyük ölçüde müdahalede bulunduğu ve bu doğrultuda orantılılık konusunda bir belirsizliğin olduğu tespit edilmiştir.

BÖLÜM 1: CEZA MUHAKEMESİ HUKUKUNDA DİJİTAL (SAYISAL/ELEKTRONİK) DELİLLER VE KAYNAKLARI

1.1. Ceza Muhakemesi Hukukunda Dijital Deliller

1.1.1. Ceza muhakemesi hukukunda delil kavramı

Ceza muhakemesinin amacı, şüpheli ve sanığın haklarına saygılı bir biçimde maddi gerçeğe ulaşılmasıdır.[19] Maddi gerçek her ne pahasına olursa olsun araştırılıp bulunmalıdır diye bir kural hiçbir hukuk devletinde söz konusu değildir. Bu bağlamda ceza muhakemesi, insan hakları ihlallerine yol açmadan maddi gerçeğin araştırılıp bulunması, adaletin gerçekleştirilmesi ve hukuki barışın sağlanması amaçlarını hedeflemektedir.[20]

Görülmekte olan bir ceza uyuşmazlığına konu olan maddi olay, kronolojik olarak muhakemenin duruşma safhasından önce gerçekleşmiştir. Bu sebeple o olaydan günümüze kalanlar ile olay hakkında bir sonuca ulaşmak gerekecektir. Geçmişte yaşanan olay ile ilgili olan ve günümüze devrolunan her şey delil kavramı altında incelenmektedir. Elde edilen deliller ile maddi olay, mahkeme önünde yeniden oluşturulacak ve suça konu olan olay yeniden yapılandırılacaktır.[21]

Ceza muhakemesinde hukuk düzenince kabul edilen araçlarla maddi gerçeğe ulaşma çabası, *"ispat"* olarak anılacaktır. Fiilin, fail tarafından işlendiği veya işlenmediği konusunda tam bir kanaate ulaştıran şeyler ise delil olarak anılacaktır.[22] İspat çabası, sabit oluşu gerektirir.[23] Bu bakımdandır ki kişinin suç işlediğinin sabit olup olmadığı konusunda tam bir kanaate ulaşılmadığı müddetçe kişi hakkında mahkûmiyet kararı verilemeyecektir.

Ceza muhakemesinde ispat bakımından belirli delillere başvurulması zorunluluğu söz konusu değildir. Aksine ceza muhakemesinde bir olay, her türlü

[19] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 6.
[20] Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* 31; Tezcan, v.d., *Dijital Ceza Muhakemesi Hukuku,* 37.
[21] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 255; Olgun Değirmenci, *Ceza Muhakemesinde Sayısal (Dijital) Delil* (Ankara: Seçkin Yayınevi, Mart 2014), 112.
[22] Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku*, 296; Bu anlamda deliller, olayın dilsiz tanıkları olarak tasvir edilmiştir. Yusuf Başlar, "Adli Bilişim Sürecinde Karşılaşılan Sorunlar ve Çözüm Önerileri," *Türkiye Barolar Birliği Dergisi*, Cilt: 33, Sayı: 148 (2020): 48.
[23] Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku*, 296.

delille ispat edilebilecektir.[24] Öyle ki herhangi bir şey, kabul edilebilirlik sınırları içerisinde kaldığı sürece, delil olarak kabul edilebilecektir.[25] Belirli bazı delillere öncelik tanımak ve diğerlerini kabul etmemek düşüncesi yahut delilleri, ispat gücü bakımından bir derecelendirmeye tabi tutmak düşüncesi maddi gerçeğe ulaşma amacı ile uyuşmamaktadır ve neticesinde ceza muhakemesini işlemez kılacaktır.[26] Bu bakımdandır ki ceza muhakemesinde *"delil serbestisi"* esastır.[27]

Anayasa'nın 138. maddesi 1. fıkrası uyarınca *"Hakimler... vicdanı kanaatlerine göre hüküm verirler."* Ek olarak Ceza Muhakemesi Kanunu'nun (CMK) 217. maddesinin 1. fıkrası uyarınca *"... deliller hâkimin vicdanî kanaatiyle serbestçe takdir edilir."* Bu açıklamalar sonrasında diyebiliriz ki hukukumuzda *"delil serbestisi"* ve bunun neticesinde *"vicdani ispat"*[28] sistemi kabul edilmiştir ve sonuç olarak bir nesne veya açıklamanın delil olarak kabul edilmesi, yargıçta vicdani kanaat oluşturmasına bağlı kılınmıştır.[29]

Şu husus belirtilmelidir ki *"delil serbestisi"* ne kadar maddi gerçeğe ulaşmak için her yolun mübah olduğu anlamına gelmiyorsa, *"vicdani delil sistemi"* de o kadar hâkimin keyfi olarak delilleri takdir edeceği anlamına gelmemektedir.[30] Zira yukarıda bahsi geçen maddeler incelendiğinde Anayasa m. 138/1 hükmüne göre hâkimlerin *"... Anayasaya, kanuna ve hukuka uygun..."* olarak karar verebileceklerini ve CMK m. 217/1 hükmüne göre hâkimlerin, kararlarını *"ancak duruşmaya getirilmiş ve huzurunda tartışılmış delillere"* dayandırabileceklerini görmekteyiz.

İlgili maddeler ışığında diyebiliriz ki hâkim, bilime, maddi gerçeğe ve hukuka uygun şekilde elde edilen delilleri[31], keyfi bir biçimde değil, akla ve mantığa uygun

[24] Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku*, 295.
[25] Charles R. Swanson, v.d., *Criminal Investigation*, 11th Edition (Boston, McGraw-Hill, 2012), 636-637; Benzer şekilde, "Polisin Adli Görevlerinin Yerine Getirilmesinde Delillerin Toplanması, Muhafazası ve İlgili Yerlere Gönderilmesi Hakkında Yönetmelik" (RG: 17/02/1983, S: 17962) m. 3 uyarınca deliller; *"Meydana gelen bir suçun aydınlatılması ve suç sanıklarının tesbitine yarayan her türlü ispat vasıtalarını"* ifade etmektedir.
[26] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 256.
[27] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 256; Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* 295; Toroslu ve Feyzioğlu, *Ceza Muhakemesi Hukuku,* 199; Aydın, *Ceza Muhakemesinde Deliller,* 35.
[28] İspat ve delil sistemleri hakkında detaylı bilgi için bkz. Aydın, *Ceza Muhakemesinde Deliller,* 28-37.
[29] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 256.
[30] Muharrem Özen ve Gürkan Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)," *Ankara Barosu Dergisi,* 1 (2015): 57.
[31] Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku*, 297.

olarak serbestçe değerlendirmeli[32], akıl yürütme faaliyeti yoluyla değerlendirdiği deliller aracılığıyla maddi meseleye ilişkin sonuca ulaşmalıdır.[33]

Aynı şekilde Yargıtay da çeşitli kararlarında, ceza yargılamasının amacının:

> *"hiçbir duraksamaya yer bırakmadan maddi gerçeğin ortaya çıkarılması"*[34] olduğunu, *"gerçeğe ulaşmada mantık yolunun izlenmesi ve delillerin gerçekçi ve akılcı"*[35] olması gerektiğini belirtmiştir.

1.1.2. Ceza muhakemesi hukukunda delillerin özellikleri ve dijital deliller

Delil serbestisi ilkesi, delillerin hiçbir özelliğe sahip olmaksızın kabul göreceği anlamına gelmemektedir. Delillerin sahip olması gereken bu özellikler, söz konusu ispat aracının delil olarak nitelendirilebilmesi bakımından gereklidir ve bu bağlamda belirlenen niteliklere sahip olmayan bir ispat aracına, ceza muhakemesinde delil işlemi yapılamayacaktır.[36]

1.1.2.1. Akılcılık

Deliller, akılcı ve bilimsel olmalıdır.[37] Nitekim yukarıda Yargıtay kararlarında da bu husus defaatle belirtilmiştir. Başka bir ifadeyle deliller, bilimsel açıdan kabul edilebilir yöntemle elde edilmiş ve bilimsel olarak kabul edilebilir[38] olmakla birlikte akla uygun olarak ifade edilebilmelidir.[39]

Konumuzla bağlantısı çerçevesinde burada dijital delillerin bilimselliği konusuna da kısaca değinmek gerekir. Bilimsel delil kavramından farklı olarak dijital delilin bilimsel oluşu, delilin elde edilmesi anından hükme esas teşkil ettiği ana kadar geçen süreçte bilimsel yöntemlerin uygulanması anlamına gelmektedir.[40] Bu bağlamda

---

[32] Toroslu ve Feyzioğlu, *Ceza Muhakemesi Hukuku,* 200; Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 256.
[33] Aydın, *Ceza Muhakemesinde Deliller,* 33.
[34] CGK., E. 1996/138 K. 1996/145 T. 18.06.1996; CGK., E. 2006/341 K. 2007/118 T. 29.5.2007; CGK., E. 1998/268 K. 1998/320 T. 20.10.1998; CGK., E. 1996/217 K. 1996/224 T. 19.11.1996; CGK., E. 1977/282 K. 1997/296 T. 09.12.1997; CGK., E. 1997/131 K. 1997/152 T. 10.06.1997; CGK., E. 2000/166 K. 2000/175 T. 03.10.2000; CGK., E. 2013/124 K. 2013/585 T. 3.12.2013; CGK., E. 2017/282 K. 2018/287 T. 19.6.2018.
[35] CGK., E. 1993/79 K. 1993/108 T. 19.04.1993; CGK., E. 2007/239 K. 2008/86 T. 15.04.2008; CGK., E. 2017/1087 K. 2018/211 T. 15.5.2018; CGK., E. 2013/59 K. 2013/302 T. 18.6.2013; CGK., E. 2006/137 K. 2006/142 T. 16.5.2006.
[36] Değirmenci, *Sayısal Delil,* 114.
[37] Toroslu ve Feyzioğlu, *Ceza Muhakemesi Hukuku,* 201; Aydın, *Ceza Muhakemesinde Deliller,* 48; Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 259; Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* 297.
[38] Değirmenci, *Sayısal Delil,* 116.
[39] Toroslu ve Feyzioğlu, *Ceza Muhakemesi Hukuku,* 201.
[40] Değirmenci, *Sayısal Delil,* 5.

ileride daha ayrıntılı değinilecek olmakla birlikte dijital delillerin elde edilmeleri bakımından hukuki gerekliliklerin yanında bazı teknik gerekliliklerin de sağlanması gerektiğini ve bu çerçevede adli bilişim biliminin karşımıza çıktığını söyleyebiliriz.

1.1.2.2. Temsil edicilik/ gerçekçilik

Deliller öncelikle ilgili ceza uyuşmazlığının bir parçasını ispat edebilecek nitelikte[41] bir başka anlatımla olayı temsil edici nitelikte[42] ve beş duyu organıyla algılanabilecek maddi ve gerçekçi bir yapıda olmalıdırlar.[43] Bununla birlikte birazdan ele alacağımız dijital deliller, klasik delillerden farklı olarak soyut bir yapıya sahiptirler ve varlıklarının anlaşılması için çeşitli alet veya teçhizatlara ihtiyaç duyulmaktadır.[44]

Delillerin kabul edilebilirliğini düzenleyen kurallardan biri, delilin konuyla ilgili olması gerekliliğidir. Delillerin, yargılanan davadaki konularla ilgili olması[45] bir başka anlatımla olayı temsil etmesi gerekir.

Delillerin olayı temsi edici olmaları ve bu bağlamda beş duyu organıyla algılanabilecek maddi bir yapıda olmaları gerekliliği konusunda, dijital delillerin soyut yapısı bazı sorunları gündeme getirebilecektir. Bu konu hakkında dijital delillerin mahkemeye sunulması açısından yazıcıdan çıktı alınması durumunda hukuki niteliğinin ne olacağı tartışılmıştır.[46] Ancak genel olarak dijital verilerin çıktısının mahkemeye sunulması hususu bazı sakıncalar doğurabilecektir. Çünkü dijital verilerin yazdırılmasıyla suçun işlendiği koşullara ilişkin çok önemli bilgilerin kaybolma ihtimali bulunmaktadır.

Bu noktada bilgi hakkında bilgi olarak tanımlanan meta data (üst veri) kavramına da değinmek yerinde olacaktır. Meta data, dijital olarak depolanan, verileri karakterize eden ve dijital bir depolama aygıtında belgelenen verilerin, kim tarafından, ne zaman, nerede, neden ve nasıl oluşturulduğu, değiştirildiği, kimler tarafından gözden geçirildiği yahut herhangi başka bir işlemin gerçekleştirilip

[41] Toroslu ve Feyzioğlu, *Ceza Muhakemesi Hukuku,* 201.
[42] Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku*, 297; Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 57.
[43] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 258.
[44] Değirmenci, *Sayısal Delil,* 132.
[45] Swanson, *Criminal Investigation,* 637.
[46] Değirmenci, *Sayısal Delil,* 116.

gerçekleştirilmediği gibi o veriyle ilgili sorulara yanıt veren bilgilerdir.[47] Özellikle klasörden görüntülenebilecek olan üst veriler (meta-data), yazdırılma işlemi sonucu elde edilen çıktıda görülemeyecektir.[48] Bu sebeple bir bilişim sistemi aracılığıyla görüntülenebilen, elde edilebilen bir dijital delil, soyut yapıda olsa dahi, doğruluğu tespit edildiği sürece olayı temsil edebilecek nitelikte kabul edilmelidir. Zira dijital delil, çıktısı alınarak maddi yapıya büründürülmüş veri değil, bizzat bilişim sistemi bünyesinde oluşturulan, iletilen, tutulan, değiştirilen ve nihayet soyut yapıda olan veridir. Bu bağlamda temsil edicilik kavramı, dijital deliller bakımından daha farklı değerlendirilmelidir. Bunlara karşılık dijital ortamda saklanan veri ile aynı verinin çıktısının, birebir aynı olması durumunda; çıktının, yine dijital delil niteliğinde olacağını ve hukuki niteliği bakımından gerçekçiliğini ve olayı temsil ediciliğini yitirmemiş sayılacağını belirten Değirmenci'nin görüşüne katılmaktayız.[49]

1.1.2.3. Hukuka uygunluk

Vicdani delil sistemin sınırını oluşturan hukuka aykırı deliller, ceza muhakemesinde hiçbir aşamada kullanılamayacaklar ve dolayısıyla vicdani kanaate ve hükme de esas alınamayacaklardır.[50]

Öncelikle delilin hukuka uygun bir delil olması gerekir. İkinci olarak delillerin hukuka uygun yollardan elde edilmiş olmalıdır.[51] Deliller, ilgili usul kurallarına uygun olarak elde edilmezlerse hükme esas alınamayacaklardır. Ek olarak *"İfade alma ve sorguda yasak usuller"*i düzenleyen CMK m. 148 hükmüne aykırı olarak elde edilen deliller de hukuka aykırı sayılacak ve hükme esas alınmayacaklardır.[52]

Bu çerçevede dijital deliller bakımından, ileride ayrıntılı bir şekilde değinilecek olmakla birlikte, hukuki gerekliliklerin yanı sıra bazı teknik gerekliliklerin de

[47] Lily R. Robinton, "Courting Chaos: Conflicting Guidance from Courts Highlights and the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence," *Yale Journal of Law and Technology*, vol. 12, no. 2 (2009-2010): 322; Philip J. Favro, "A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata," *Boston University Journal of Science & Technology Law*, Vol. 13, Issue 1 (2007): 7. Aktaran, Değirmenci, "Bilgi Toplumunun Delil Türü," 21.
[48] Magherescu, "Enhancing Procedure of Using New Means of Technologies," 18.
[49] Değirmenci, *Sayısal Delil,* 116; Sarsikoğlu, "Elektronik Delil (E-Delil) Kavramı," 517; Değirmenci, "Bilgi Toplumunun Delil Türü," 18.
[50] Khalil Afandak, "Ceza Muhakemesinde Dijital Deliller" (Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuk Anabilim Dalı, Ankara-202), 24.
[51] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 259; Aydın, *Ceza Muhakemesinde Deliller,* 52; Toroslu ve Feyzioğlu, *Ceza Muhakemesi Hukuku,* 201; Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* 297.
[52] Delilin hukuka uygunluğu ile ilgili ilerde daha ayrıntılı bilgiler verilecektir.

sağlanması, delilin hukuka uygunluğu konusunda şüpheleri ortadan kaldırıcı nitelikte olacaktır. Özellikle dijital delil elde edilmesi bakımından CMK m. 134 "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" koruma tedbirinin şartlarına uyulmaması veya bu çerçevede delil elde edilmesi sırasında uluslararası adli bilişim yöntemlerinin uygulanmıyor oluşu elde edilenleri, hukuka aykırı delil haline getirebilecektir.

1.1.2.4. Önemlilik

Delillerin kabul edilebilirliği ayrıca önemlilik testine tabi tutulur. Belirli bir delilin konuyla ilgili olduğu varsayıldığında bile, önemi davanın sonucunu etkilemeyecek kadar önemsiz ise kabul edilemez olabilir. Başka bir ifadeyle önemlilik, söz konusu delil öğesinin yargılamaya bir etkisi olup olamayacağı ile ilgilenir.[53]

1.1.2.5. Müştereklik

Deliller müşterek olmalıdır.[54] Bir başka ifadeyle delilin içeriği sadece hâkim tarafından değil, taraflar tarafından da bilinmeli ve tartışmaya açılmalı ve hüküm yalnızca hâkimin kişisel bilgisine göre tesis edilmemelidir.[55] Nitekim CMK m. 216/1 uyarınca deliller *ortaya konmalı* ve *tartışma*ya konu olmalıdır. Ek olarak CMK m. 217/1 uyarınca *"hâkim, kararını… huzurunda tartışılmış delillere…"* dayandırabilecektir.

Dijital delillerin müşterekliği ise şüpheli veya sanık tarafından kullanılan bilişim sistemine el konulması ve el konulan bilişim sisteminin, adli bilişim uzmanları tarafından incelenmesi neticesinde hazırlanan adli bilişim raporunun, mahkemeye sunulması ile sağlanacaktır. Bu çerçevede hazırlanacak raporun, raporu okuyan kişiler tarafından da anlaşılabilmesi adına, sade bir dille hazırlanması, teknik kavramlarla dolu olmaması önem arz edecektir.

---

[53] Swanson, *Criminal Investigation,* 637.
[54] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 259; Aydın, *Ceza Muhakemesinde Deliller,* 50; Toroslu ve Feyzioğlu, *Ceza Muhakemesi Hukuku,* 202.
[55] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 259; Toroslu ve Feyzioğlu, *Ceza Muhakemesi Hukuku,* 202; Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 58.

1.1.2.6. Güvenilirlik

Deliller sağlam ve güvenilir olmalıdır.[56] Bir başka ifadeyle delil değiştirilmemiş yahut taklit edilmemiş olmalı ve muhakemede delilin aslı kullanılmalıdır.[57]

Bu özellik bakımından da dijital deliller farklılık arz etmektedirler. Şöyle ki dijital ortamda bulunan dijital delillerin, aslının aranması, delilin hiçbir zaman kullanılamamasına neden olabilecektir.[58] Çünkü soyut bir yapıda olan ve bu sebeple gözle görülmeleri mümkün olmayan dijital deliller, gerekli araç ve teçhizatlar yardımıyla görünür kılınabilmektedir. Bu sebeple dijital delille teması sağlayan araç ve teçhizatlar üzerindeki haller, delilin asıl hali olarak kabul edilmelidir.[59] Ek olarak dijital deliller tamamen kopyalanabilme özelliğine sahiptir. Bu sebeple delilin bozulma ihtimalinin ihtimal dışı bırakılması adına incelemeler, bu kopyalar üzerinden gerçekleştirilebilecektir.[60] Tamamen kopyalanabilme özellikleri sayesinde bazı durumlarda hangi belgenin asıl olduğunun tespiti dahi imkânsız hale gelebilmektedir. Bu bakımdan sayısal delillerin orijinalliğinin belirlenmesinde delil niteliğini haiz asıl belgeden ziyade bu delili bulunduran sistemin tam ve doğru çalışıyor oluşunun tespiti, ilgili belgenin orijinalliğini sağlayacaktır.[61]

Dijital delillerin bazı özellikleri, delillerin taşıması gereken genel özelliklere, yapısı gereği uyum sağlayamamaktadır. Bu bakımdan dijital delillerin doğası gereği ortaya çıkan bu uyumsuzlukların irdelenmesi ve bunun neticesinde delillerde bulunması gereken özelliklerin, dijital delillerde de aranması gereklidir.[62] Örneğin dijital delillerin hassas yapısı bir başka ifadeyle kolayca değiştirilebilir, tahrif edilebilir, yok edilebilir ve soyut yapısı, yani dijital delili fiziksel bir nesneyle ilişkilendirmenin zorluğu dikkate alındığında, güvenilirlik bakımından çeşitli endişeler ortaya çıkabilmektedir.[63] Bu endişelerin önüne geçilebilmesi için dijital

---

[56] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 258.
[57] Değirmenci, *Sayısal Delil,* 115.
[58] Değirmenci, *Sayısal Delil,* 116.
[59] Değirmenci, *Sayısal Delil,* 116.
[60] Hatta birazdan açıklanacağı üzere adli bilişim uzmanının incelemelerini bu kopyalar üzerinden gerçekleştirmesi zorunludur.
[61] Değirmenci, *Sayısal Delil,* 140.
[62] Değirmenci, "Bilgi Toplumunun Delil Türü," 19.
[63] Nigel Jones, v.d., *Bilişim Suçları Eğitim Modülü, Türk Ceza Adalet Sisteminin Etkinliğinin Geliştirilmesi, Avrupa Birliği- Avrupa Konseyi Ortak Projesi* (Ankara: MATBAM Ajans & Reklam & Tanıtım, 2014), 144. Ek olarak dijital deliller genelde onu içeren cihazla karıştırılır. Başka bir ifadeyle bazı durumlarda dijital delili barındıran bilişim sisteminin bizzat kendisi dijital delil olarak kabul

delillerin, veri olarak ilk elde edildiği ilk andan delil kategorisine alındığı ve en sonunda mahkemeye sunulduğu ana kadar belgelenmesi, delil zincirinin bu belgelere dayandırılması, dijital delillerin kim tarafından elde edildiği ve kabul edilebilirliğinin kim tarafından nasıl korunduğu gibi detayların belirtilmesi büyük önem arz etmektedir.[64,65]

1.1.2.7. Elde edilebilirlik

Delillerin olayı temsil edebilmeleri için onlara ulaşılması, elde edilebilmeleri[66] ve nihayetinde ortaya konulabilmeleri gereklidir.[67] Sonuç olarak ulaşılması mümkün olmayan bir ispat aracı duruşmaya getirilemeyecek ve tartışmaya açılamayacaktır.[68,69]

Dijital delillerin elde edilişi ise bunları barındıran bilişim sistemlerinin aranması yahut belli bazı koşulların oluşması halinde istisnai olarak dijital delilleri barındıran bilişim sistemlerinin fiziksel varlığına elkonulması ve aramanın adli bilişim laboratuvarlarında gerçekleştirilmesi neticesinde gerçekleşmektedir.

1.1.3. Ceza muhakemesi hukukunda delil türleri ve dijital delillerin yeri

Deliller birçok farklı açıdan ayrımlara tabi tutulmuştur. Maddi olayı temsil etmesi yönünden yapılan bir ayrıma göre deliller doğrudan ve dolaylı deliller (belirtiler) olarak ayrılmıştır. Buna göre doğrudan deliller, asıl olayı ispatlarlarken dolaylı deliller, esas olaya bağlı yan olayları açıklamaktadırlar. Örneğin olay yerinde şüpheliye ait DNA bulunması, şüphelinin olay mahallinde olduğunu ispat eder ancak, asıl olayı işleyip işlemediğini ispat etmez.[70]

Bir başka ayrım uyarınca ise deliller, kaynağı kişi olan deliller (beyan delilleri, şüpheli, sanık, tanık, mağdur, bilirkişi) ve kaynağı nesne olan deliller (belge delilleri

---

edilebilmektedir. Bu durum da dijital delile yaklaşım açısından bazı sıkıntılara vücut verebilmektedir. Biasiotti, v.d., "Introduction: Opportunities," 3.

[64] Biasiotti, v.d., "Introduction: Opportunities," 3; Yusuf Başlar, "Elektronik Delilin Toplanması ve Muhafazası," *Hacettepe Hukuk Fakültesi Dergisi*, C.10 (2020): 98.

[65] Ek olarak dijital delillerin hassas yapısı ve zamanla bozulabilmeleri ihtimali ve dava sürecinin uzunluğu dikkate alındığında dijital delillerin süreç boyunca adli olarak eğitilmiş personel tarafından periyodik bir şekilde kontrol edilmesi önem arz edecektir. Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 59.

[66] Toroslu ve Feyzioğlu, *Ceza Muhakemesi Hukuku,* 201.

[67] Aydın, *Ceza Muhakemesinde Deliller,* 49; Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 57.

[68] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 259.

[69] Örneğin ölmüş bir kişinin tanık olarak beyanına başvurulamaması.

[70] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 259- 260; Toroslu ve Feyzioğlu, *Ceza Muhakemesi Hukuku,* 205.

ve belirtiler) olarak ikiye ayrılmaktadır.[71] Ancak çoğunlukla kullanılan ayrım, doğrudan deliller ve belirti delilleri şeklinde olduğu için, burada bu ayrımı yalnızca değinmekle yetineceğiz.

1.1.3.1. Doğrudan deliller

Doğrudan delil genellikle, sanığın suçu işlediğini olumlu bir şekilde ifade edebilen bir görgü tanığının ifadesi gibi, sanığı doğrudan suçun işlenmesine bağlayan delillerdir.[72] Bir tanıma göre dolaylı deliller şüpheli veya sanığı suça mantıksal olarak bağlaması koşuluyla, doğrudan delil dışındaki tüm delilleri ifade etmektedir.[73] Dolaylı deliller bir suçun ispatına yarayacak delillerden oluşan zincirin bir halkasına benzetilebilir. Öyle ki suçun ispatında tek başına yeterli olmasa da diğer delillerle desteklendiklerinde hükme esas alınabileceklerdir.

1.1.3.1.1. Beyan

Uyuşmazlık konusu maddi olaya ilişkin açıklamalar, beyan delilini oluşturur. Beyanlar şüpheli veya sanığa, mağdura ya da mağdur dışındaki üçüncü kişilere (tanık gibi) ait olabilir.[74]

1.1.3.1.2. Belge

Olay anında olayın bire bir şekilde, bir nesne üzerine aktarılması durumunda belge delili gündeme gelecektir. Belge delilleri, somut olayı bire bir temsil eden delilleridir bu bağlamda olayın taşıyıcısı bir insan olduğunda tanıktan, bir nesne olduğunda ise belgeden söz edebiliriz. Olay yazıya döküldüğünde, olayın taşıyıcısı yazılı bir belge; olay ses olarak tespit edilmişse bir ses bandı; olay hem şekil hem de ses olarak taşınmışsa taşıyıcı dar anlamda bir film şeridi veya CD vb. olacaktır.[75]

CMK'da bir belgenin *okunmasından (CMK m. 214-215)* söz edildiği gerekçesiyle dar yorum faaliyeti ile okuma dışında görme ve dinleme suretiyle içeriği öğrenilen teknik aletlerin, belge delili değil fakat keşfe konu belirti delilleri olabileceği

[71] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 260; Toroslu ve Feyzioğlu, *Ceza Muhakemesi Hukuku,* 206.
[72] Swanson, *Criminal Investigation,* 640.
[73] Swanson, *Criminal Investigation,* 641- 642.
[74] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 261; Toroslu ve Feyzioğlu, *Ceza Muhakemesi Hukuku,* 206.
[75] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 312. Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* 331; Toroslu ve Feyzioğlu, *Ceza Muhakemesi Hukuku,* 228.

ve bu sebeple başka delillerle desteklenmeleri gerektiği ileri sürülmüştür.[76] Bununla birlikte hukuki yoldan elde edilmeleri ve teknik açıdan doğrulanmaları neticesinde görüntü ve ses tespit eden aletlerden elde edilenlerin, diğer delil türlerinden bir farkı olmadığı; bir şeyin delil olarak kabul edilmesi ile o delilin vicdani kanaati oluşturabilmesi bakımından başka delillerle de doğrulanması gerekliliğinin farklı şeyler olduğu belirtilmiştir.[77]

Dijital delillerin de görüntü veya ses şekline dönüştüğünde belirti delili oldukları ancak okunabilir hale getirildiklerinde belge delili özelliği gösterecekleri belirtilmiştir.[78]

1.1.3.2. Belirtiler

Belirti delilleri, olaydan geriye kalan iz ve eserlerdir. Belirti delilleri, maddi olayı tek başlarına ispat edebilme gücüne sahip olmamakla birlikte, beyan ve belge delilleri gibi doğrudan deliller aracılığıyla elde edilen kanaati destekleyici niteliktedirler.[79]

Belirti deliller kendi içerisinde doğal ve yapay belirtiler olmak üzere ikiye ayrılırlar. Failin iradesi dışında olaydan geriye kalan iz ve eserler (ör. ayak izi, tükürük), *doğal (tabii)* belirti olarak anılırken failin iradesiyle veya başka bir insan tarafından belirli amaçlar doğrultusunda hazırlanmış olan nesneler (ör. tabanca, bıçak) *yapay (suni)* belirtiler olarak anılacaktır.[80]

Belirtiler, çoğu zaman esas uyuşmazlığı doğrudan ispatlama konusunda yetersiz kalırlar. Bu bağlamda çoğunlukla somut olaya ilişkin diğer delil araçlarının değerlendirilmesine yararlar ve çoğu zaman başka delillerle desteklenmeleri gerekir. Ancak bu desteklenme gerekliliği yalnızca belirtiler bakımından değil kural olarak bütün deliller bakımından geçerlidir. [81] Zira delil serbestisinin kabul edildiği ceza muhakemesi hukukunda hâkim, vicdani kanaatini oluştururken bir belirtide olabileceği

---

[76] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 313; Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* 332.
[77] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 313.
[78] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 314.
[79] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 260; Toroslu ve Feyzioğlu, *Ceza Muhakemesi Hukuku,* 230.
[80] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 316; Toroslu ve Feyzioğlu, *Ceza Muhakemesi Hukuku,* 230- 231.
[81] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 316- 317; Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* 335.

gibi bir belge veya beyan delilinin de başka delillerle desteklenmesini arayabilecektir. Ek olarak hiçbir delil türünün olayı kesin olarak ispat edebileceğini söylemek mümkün olmayacaktır. Gerek doğrudan ve gerekse dolaylı delillerin hepsinde mutlaka bir yanılma payı bulunmaktadır.[82] Fakat hükme esas alınabilmesi bakımından bir delilin belirti niteliğinde olduğu tespit edilirse yalnızca o delile dayanılarak kişi hakkında hüküm tesis edilemeyecektir.

Bilimsel deliller olarak da anılan belirtiler, bilimsel yöntemlerle kriminalistik biliminin verilerine göre elde edilirler ve elde edilmeleri neticesinde hazırlanan raporlar, bilimsel delil olarak anılır.[83] Bu bağlamda bir belirti delilinin yanılma payının, bir tanıktan daha az olabileceği ifade edilmiştir.[84]

Dijital deliller açısından bir değerlendirme yapacak olursak dijital delillerin, genellikle bazı dijital nesne veya olayların bir soyutlaması olduğunu söyleyebiliriz. Örneğin bir kişi bir bilgisayara e-posta göndermek gibi bir görevi gerçekleştirmesi talimatını verdiğinde, bu işlem neticesinde gerçekleşen hareketler, gerçekte ne olduğuna dair yalnızca kısmi bir görünüm veren veri kalıntılarıdır. Bu sebeple dijital deliller genellikle belirti delili olarak kabul edilmektedir. Çünkü yalnızca dijital delile dayanarak bir bilgisayar etkinliğinin bir bireye atfedilmesi her zaman kolay değildir. Bu nedenle, dijital deliller çoğunlukla soruşturmaların bir bileşeni niteliğinde kabul edilirler. Gerçekten de suç fiilinin gerçekleşmesi esnasında bilgisayarı başka birinin kullanmış olma ihtimali vardır. Bu bağlamda dijital delillerin delil gücünün artması için bilişim sisteminin bir bütün olarak incelenmesi gereklidir. Dijital delillerin, fiziksel delillerden farklı olarak bütünden ayrı bir şekilde incelenmesi, dijital delilin olayı temsil edici niteliğini yitirmesine veya büyük ölçüde kaybetmesine neden olabilecektir. Sonuç olarak dijital delillerin doğrulanması ve delil değeri kazanması bakımından, veriyi barındıran bilişim sisteminin bütün olarak incelenmesi veya elde edilenlerin başka delillerle desteklenmesi katkı sağlayacaktır.[85]

---

[82] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 260.
[83] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 317.
[84] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 260; Öztürk, "Bilişim Cihazlarındaki Sayısal Delillerin Tespiti," 335.
[85] Casey, *Digital Evidence*, 25- 26; Eoghan Casey, "Error, Uncertainty and Loss in Digital Evidence," *International Journal of Digital Evidence*, Vol. 1, Issue 2 (2002): 42; Değirmenci, *Sayısal Delil,* 135; Değirmenci, "Bilgi Toplumunun Delil Türü," 22; Afandak, "Ceza Muhakemesinde Dijital Deliller," 42.

1.1.3.3. Dijital delillerin, diğer delil türlerinden farkları ve delil türleri arasındaki yeri

Ceza muhakemesinde delil değeri bakımından dijital deliller ile fiziksel deliller arasında bir fark bulunmamaktadır. Her iki delil türü bakımından ayrım çoğunlukla dijital delillerin kendi doğasından kaynaklanmaktadır.[86] Bu bakımdan dijital delil kavramının, bir delil türünü değil, delilin vücut bulduğu yapıyı ifade ettiğini belirtmek gerekecektir. Bu sebeple dijital deliller karşımıza, temsil ediciliği bakımından genel nitelikte veya özel nitelikte, değerleri bakımından doğrudan doğruya veya dolaylı, içerikleri bakımından belge veya belirti delilleri şeklinde çıkabilmektedirler.[87]

Bu bağlamda dijital deliller, bazen bir saldırı olayını kaydeden elektronik kameradaki bilgiler gibi doğrudan delil bazen de bilişim sistemine hukuka aykırı erişim suçunda erişilen bilişim sisteminde bulunan dijital izlerde olduğu gibi dolaylı delil niteliği taşıyabileceklerdir.[88] Bu bakımdan dijital deliller bir vakanın doğrudan ispatını sağlayabileceği gibi, tam aksini, başka bir ifadeyle soruşturma- kovuşturma konusu fiilin fail tarafından işlenmediğini de ortaya koyabilir.[89]

Bu bağlamda hukuka uygun bir şekilde elde edilen ve içeriklerinin gerçeği yansıttığı, bozulup değişikliğe uğramadığı başka bir ifadeyle teknolojik olarak geçerli oldukları tespit edilen dijital delillerin, diğer delillerde olabildiği gibi, tek başlarına hükme esas alınmalarında bir problem olmadığı görüşündeyiz. Nitekim bu şartları taşımayan veriler, belirti delili olarak dahi kullanılamayacaklardır.[90] Bu bağlamda dijital delillerin bir delil türünden ziyade, delil elde etme yöntemi olarak kabul edilmesi gerektiği ileri sürülmüş ve bu şekilde hukuki ve bilimsel bir şekilde elde edilen dijital delilin yalnızca sanal ortamda bulunması sebebiyle kabul edilmemesinin önüne geçilmiş olacağı belirtilmiştir.[91]

Bilgisayardaki verilerin kolaylıkla değiştirilebilir olduğu kabul edilmekle birlikte verilerin değiştirilip değiştirilmediği de gelişen yazılımlar sayesinde

---

[86] Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj)," 56; Çetin Arslan, "Dijital Delil ve İletişimin Denetlenmesi", *Ceza Hukuku ve Kriminoloji Dergisi,* Cilt: 3, Sayı: 2 (2015): 193.

[87] Değirmenci, *Sayısal Delil,* 130; Yazar ek olarak dijital delillerin, geleneksel delillerin ayrımında kullanılan ölçütler bakımından yerinin tespit edilmesi yerine; bizim de ileride bahsedeceğimiz güvenilirlik, özgünlük, inanılırlık ve bütünlük konularına öncelik verilmesi gerektiğini belirtmiştir. Bkz. Sarsikoğlu, "Elektronik Delil (E-Delil) Kavramı," 523- 524.

[88] Sarsikoğlu, "Elektronik Delil (E-Delil) Kavramı," 520- 521.

[89] Arslan, "Dijital Delil ve İletişimin Denetlenmesi," 195.

[90] Sarsikoğlu, "Elektronik Delil (E-Delil) Kavramı," 524; Başlar, "Elektronik Delil," 1680.

[91] Sarsikoğlu, "Elektronik Delil (E-Delil) Kavramı," 529.

anlaşılabilmektedir. Bu sebeple elde edilen verilerin, adli bilişim sürecinin uygulanması sonucunda veya bu süreç uygulanmaksızın, bütünlüğünün ve güvenliğinin teknik bir inceleme sonucunda ispat edilmesi durumunda, söz konusu veriler delil olarak kabul edilebileceklerdir. Bu hususta gerçekleştirilen teknik inceleme sırasında dijital veriler üzerinde hangi işlemlerin yapıldığı ayrıntılı bir şekilde kaydedilmelidir.[92] Öyle ki adli bilişim süreci tamamlanmaksızın veya teknik incelemesi gerçekleşmeksizin mahkemeye sunulan verilerin, ancak belirti hükmünde kalacakları da ileri sürülmüştür.[93]

Buna karşılık bir başka görüşte ise dijital deliller, "ispat edilecek olayın kanıtlanmasına dolaylı olarak yardımcı olan ve vakıa ve iz şeklinde tanımlanan bir belirti" şeklinde tanımlanmıştır. Buna göre dijital delillerin ne zaman, ne şekilde oluşturulduğu veya içeriğine müdahale edilip edilmediğinin çoğu zaman tespit edilemediği bu sebeple bu delillerin tek başlarına delil olarak kullanılmasının genellikle mümkün olmadığı bu sebeple de dijital delillerin diğer delillerle birlikte değerlendirilmesi ve teyit edilmesi gerektiği belirtilmiştir.[94] Benzer şekilde dijital delillerin diğer delillerle desteklenmesi ihtiyacının, dijital delilin niteliğine göre belirlenmesi gerektiği ve dijital delilin, insan tarafından oluşturulan ve bilişim sisteminde muhafaza edilen bir delil niteliğinde olması durumunda doğruluğunun diğer delillerle desteklenmesi gerekeceği; ancak dijital delilin, bilişim sistemi tarafından insan müdahalesi olmaksızın oluşturulan bir delil olması durumunda ise sistemin uygun şekilde işleyip işlemediğinin göz önüne alınması gerekeceği belirtilmiştir.[95] Bu görüşün, teknik standartlara ve kurallara uyulmadan elde edilen dijital deliller bakımından yerinde olduğunu söyleyebiliriz. Özellikle bilişim bağlantılı suçlarda çok daha önemli olan adli bilişim sürecinin, iyi eğitim almış deneyimli teknik uzmanlar tarafından yürütülmesi gerekmektedir.[96] Ancak yine de zaten teknik standartlara ve kurallara uyulmaksızın elde edilen verilerin, dijital delil niteliğini taşıyamayacaklarını ve bu bağlamda belirti delili olarak dahi ele alınamayacaklarını tekrardan belirtmek yerinde olacaktır.

---

[92] Osman Gazi Ünal, "Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma" (Yayınlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, 2011), 20.
[93] Ünal, "Bilgisayarlarda Bilgisayar Programlarında," 20; Başlar, "Elektronik Delil," 1677.
[94] Arslan, "Dijital Delil ve İletişimin Denetlenmesi," 201; Dülger, *Bilişim Suçları,* 600.
[95] Başlar, "Elektronik Delil," 1676.
[96] Başlar, "Elektronik Delil," 1675- 1676.

Genel anlamda dijital delillerin tek başına hükme esas alınıp alınamayacağı konusundaki tartışmalar, delilin olayı temsil ediciliği, sahihliği ve tahrif edilebilirliği noktasında toplanmaktadır. Bununla birlikte, bu sıkıntıların diğer deliller bakımından da geçerli olduğunu ve olayı temsil edici niteliği bulunmayan, sahih olmayan veya tahrif edilmiş durumda bulunan diğer delillerin de ceza yargılamasında delil olarak kullanılamayacaklarını söylemek yanlış olmayacaktır. Bu sebeple bilişim sistemlerinden elde edilen dijital delillerin de her ihtimalde güvenilir olmadıkları iddia edilemeyecektir. Buradan yola çıkarak usule uygun şekilde elde edilmiş ve elde edildiği andan hükme esas teşkil edeceği ana kadar bilimsel kurallara riayet edilmiş olan dijital delillerin de en az fiziksel deliller kadar güvenilir olduğunu düşünmekteyiz.[97]

Zira Yargıtay da bu konuda hukuka uygun olmak kaydıyla, her türlü delilin ispat aracı olarak kullanılabileceğini ve bu bakımdan maddi gerçeğe ulaştıracak delilin fiziki ya da elektronik olmasının önem arz etmemekte olduğunu belirtmiştir.[98]

Hukuki ve teknik gereklilikleri sağlanarak elde edilen bir dijital delil ile yine hukuka uygun şekilde elde edilen bir fiziksel delilin arasında delil olma ve ispat gücü bakımından bir fark olmayacağına dair düşüncemize yukarıda yer vermekle birlikte yine de dijital delillerin soyut yapıda oluşu ve geleneksel delillerin fiziksel yapıda oluşu sebebiyle farklı özellikleri olduğu ve bu delillerin gerek elde edilişleri ve gerekse değerlendirilmeleri bakımından farklı işlemlere tabi tutulmaları gerektiği gerçeğini kabul etmek gerekir.

1.1.4. Dijital delil- elektronik delil kavramlarının ayrımı ve kişisel veriler

Dijital delil, birden fazla disiplini ilgilendiren bir delil türüdür. Delilin elde edilme sürecinde, adli bilişim, hukuk, elektrik elektronik gibi birçok alana temasta bulunulmaktadır. Bu bağlamda, disiplinler arası bir konu olduğundan, farklı disiplinlerde aynı kavramı ifade eden dijital (sayısal) delil, elektronik delil, bilgisayar delili gibi farklı ifadelerin kullanıldığı görülmektedir.[99]

[97] Başlar, "Elektronik Delil," 1678.
[98] Yargıtay CGK., E. 2017/956 K. 2017/370 T. 26.9.2017.
[99] Değirmenci, *Sayısal Delil,* 453; Başlar, "Elektronik Delil," 1660; Değirmenci, "Bilgi Toplumunun Delil Türü," 17.

"Dijital" kelimesi, Fransızca "Digital" kelimesinden Türkçeye geçmiş olup, "Sayısal" anlamına gelmektedir.[100] Dijital (sayısal) delil ve elektronik delil kavramları genellikle birbirlerinin yerine kullanılmaktadır. Ancak aralarında farklar vardır. Dijital deliller, sayıları esas alan yöntemlerle çalışan, elektronik cihazlarda muhafaza edilen ve bu cihazlar kullanılarak oluşturulan delillerdir. "Elektronik" alanı ise temelinde elektronların hareketlerini esas alan ve bu hareketlere uygun devreler yapılmasıyla ilgilenen bir bilim dalıdır. Elektronik alanında yer alan cihazlar "analog[101] (örneksel) elektronik" ve "dijital (sayısal) elektronik" cihazlar olmak üzere ikili bir gruplandırma ile ele alınmaktadır. Bu bağlamda elektronik delil kavramı, elektronik cihazlardan, başka bir ifadeyle hem dijital hem de analog cihazlardan elde edilen ve bu sebeple dijital (sayısal) delilleri de kapsayan üst bir kavram olarak karşımıza çıkmaktadır.[102]

Bu açıklamaya karşılık çalışmamızda, elektronik delil kavramının daha kapsayıcı bir kavram olduğunu kabul etmekle birlikte dijital delil kavramını tercih edeceğiz. Gerekçelerini şu şekilde sıralayabiliriz.

Öncelikle, günümüzde analog cihazların neredeyse hiç kullanım alanı kalmamıştır. Öyle ki teknolojinin gelişimi neticesinde analog cihazların kullanımının bulunduğu alanlar ya giderek dijitalleşmiş ya da zamanla kullanımı azalarak ortadan kalkmıştır.[103,104] Bu sebeple de elektronik üst başlığı anlamını zamanla yitirmeye başlamıştır. Ek olarak doktrinde yer alan çalışmalarda bahsi geçen "elektronik delil" kavramıyla çoğunlukla kastedilen yine dijital deliller olmuştur.[105]

İkinci olarak analog delillerin kullanım alanın azalması ile birlikte bu iki delil türünün, elde edilmesinde farklı işlemler ve usuli gerekliliklerin söz konusu olduğunu söyleyebiliriz. Açıklanacak olursa analog cihazlar ile oluşturulan deliller kalıcı bir şekilde meydana getirilmektedir. Örneğin analog bir fotoğraf makinesi ile elde edilen görüntü, negatife yansıtılır ve bu negatifin çeşitli işlemlerden geçirilmesi suretiyle

---

[100] https://sozluk.gov.tr/ , son erişim: 15.01.2022.
[101] Analog kavramı ile ilgili bilgi için bkz. Uğur Kaynakçıoğlu, "Ceza Muhakemesinde Dijital Deliller" (Yayınlanmamış Yüksek Lisans Tezi, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Haziran 2015), 25.
[102] Sarsikoğlu, "Elektronik Delil (E-Delil) Kavramı," 519- 520; Başlar, "Elektronik Delil," 1660- 1661; Kaynakçıoğlu, "Dijital Deliller," 27; Afandak, "Ceza Muhakemesinde Dijital Deliller," 61- 62.
[103] Değirmenci, *Sayısal Delil,* 127; Değirmenci, "Bilgi Toplumunun Delil Türü," 17.
[104] Analog teknolojiden dijitale evrilen teknolojilere birkaç örnek vermek gerekirse, "plakların CD ve MP3'e, daktilonun yazıcıya, analog fotoğrafların (negatif filmden oluşturulan) dijital fotoğraflara, analog televizyon yayınının (doğrudan anten ile alınan) dijital televizyon yayınına, ankesörlü ve sabit hatlı telefonların cep telefonlarına" dönüşmesi vs. Aktaran: Kaynakçıoğlu, "Dijital Deliller," 26.
[105] Değirmenci, *Sayısal Delil,* 127; Kaynakçıoğlu, "Dijital Deliller," 26.

neticede asıl görüntünün bir kopyası oluşturulur. Dijital fotoğraf makinesi ile farklı olarak, analog fotoğraf makinesi ile elde edilen negatifin değiştirilmesi büyük bir beceri gerektirir ve yine de bu değişikliklerin büyük çoğunluğu tespit edilebilir. Dijital fotoğraf makinesi ile elde edilen fotoğrafların üzerinde ise değişim kolaylıkla gerçekleştirilebilir ve bunların tespit edilmesi ayrı bir beceri gerektirir. Bu sebeple aslında dijital ve analog cihazlardan elde edilen delillerin farklılıkları sebebiyle birbirleriyle karıştırılmamaları gerektiği, bunların ortak bir başlıkta ele alınmalarının farklı sıkıntılara yol açabileceği ve bu sebeple farklı düzenlemelere tabii tutulması gerektiği belirtilmiştir.[106]

Üçüncü olarak, dijital delillerin elde edilmesinin temel kaynağını oluşturan CMK m. 134'ün başlığı "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" şeklindedir. Maddenin içerik itibariyle yalnızca bilgisayarları, bilgisayar programlarını ve kütüklerini ele alması hususunun, dijital delillerin elde edilebileceği diğer kaynakları göz ardı edişi sebebiyle getireceğimiz eleştirilere ileride değinmekle birlikte; temel anlamda bilgisayarların çalışma prensibinin, bilgisayarın donanım ve yazılımları arasında gerçekleştirilen komut alışverişi ile gerçekleştiğini, bu alışveriş ile birlikte dijital verilerin üretildiğini ya da var olan verilerin çeşitli başka formatlara dönüştürüldüğünü ve bu alışverişte kullanılan mevcut metodolojinin, *ikili değer (binary)* olarak adlandırıldığını söyleyebiliriz. Bilgi işlem teknolojisinin temelini oluşturan bu ikili değer metodolojisi neticesinde dijital verilerin hareketi, bu iki durum ile, başka bir ifadeyle 1 ve 0'ların uygun dizilimi ile dijital (sayısal) bir şekilde temsil edilir.[107] Bu bakımdan söyleyebiliriz ki bilgisayarlardan elde edilebilecek deliller, zaten dijital yapıda olacaklardır. Bu sebeple bir dijital delil elde etme yöntemi olarak CMK m. 134 değerlendirildiğinde "elektronik delil" diyerek analog delilleri de kapsama alma düşüncesinin görünürde bir faydası olmayacaktır.

Son olarak günümüzde analog veriler dijitale ve dijital veriler de kolaylıkla analoğa kolaylıkla çevrilebilmektedir.[108] Ancak somut olayın temsili bakımından değerlendirildiğinde gerçekliğin dijital ve analog temsilleri arasındaki kritik fark, delilin dijital alana bir kez girdiğinde, benzersiz atomlara sahip üç boyutlu nesnelerin

[106] Kaynakçıoğlu, "Dijital Deliller," 27; *Ankara Barosu Uluslararası Hukuk Kurultayı: Bilişim ve Hukuk,* Cilt- 2 (8 Ocak- 11 Ocak, 2008): 172- 173.
[107] Kızılyar, "Ceza Yargılaması," 79- 81; Marcella and Guillossou, *Cyber Forensics,* 2- 3.
[108] Kaynakçıoğlu, "Dijital Deliller," 26.

dünyasından, depolanmış bilgi dünyasına geçiyor oluşudur. Bu bağlamda da dijital deliller temel düzeyde, *birler ve sıfırlardan* başka bir şey değildir.[109]

Yukarıda açıklananlar neticesinde çalışmamızda "dijital delil" kavramının kullanımını tercih etmiş bulunmaktayız.

1.1.4.1. Veri kavramı

Veriler, günümüzün petrolüne benzetilmiştir.[110] Gündelik hayatlarımızın, internet gezintilerimizin, alışkanlıklarımızın ve daha birçok bilgimizin kaydedilerek veri haline getirilmesi ve hatta bizzat insanların da birer veri oldukları gerçeği düşünüldüğünde bu benzetme hiç de yanlış değildir.

Verilerin artan önemi, hangi bilgilerin veri olarak kabul edileceği konusundaki soru işaretlerini de arttırmıştır. Bu bağlamda veri kavramı, farklı açılardan ve farklı özellikleri vurgulanmak suretiyle çeşitli şekillerde tanımlanmıştır. Yargıtay, veri kavramını, *bilişim suçlarının konusu* olarak tanımlanmıştır.[111] İngilizce *"data"* kelimesinin karşılığı olan veri kavramı, TDK tarafından; *"Olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi."* Şeklinde tanımlanmıştır.[112]

5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"[113] m 2/1-k uyarınca veri; *"Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri…"* ifade etmektedir.

5070 sayılı "Elektronik İmza Kanunu"[114] m 3/1-a uyarınca ise elektronik veri; *"Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları…"*

---

[109] David Chaikin, "Network investigations of cyber attacks: the limits of digital evidence," *Crime Law Soc Change*, vol. 46 (2006) 241-242; Orin S. Kerr, "Digital Evidence And The New Criminal Procedure," *Columbia Law Review*, Vol. 105:279 (2005): 284; Charles Leacock, "Search and Seizure of Digital Evidence in Criminal Proceedings," *Digital Evidence and Electronic Signature Law Review*, vol. 5 (2008): 221; Afandak, "Ceza Muhakemesinde Dijital Deliller," 81.
[110] Drewer and Ellermann, "The Online Environment as a Challenge," 141
[111] Yargıtay CGK, E. 2007/6-136, K. 2007/150, T. 19.06.2007.
[112] https://sozluk.gov.tr/ son erişim: 21.12.2021.
[113] İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Resmî Gazete Tarihi: 23/5/2007, Sayı: 26530.
[114] Elektronik İmza Kanunu, Resmî Gazete Tarihi :23/1/2004, Sayı: 25355.

ifade etmektedir. Buna göre elektronik ortamda var olan ve nerede, nasıl ve kim tarafından oluşturulduğunun önemi olmayan her veri, elektronik veridir.[115]

İleride ayrıntılı olarak bahsi geçecek Avrupa Konseyi Siber Suç Sözleşmesi[116] m. 1 uyarınca bilgisayar verisi olarak başlıklandırılan dijital veriler; *"bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlar da dâhil olmak üzere, bir bilgisayar sisteminde işlenmeye uygun nitelikteki her türlü bilgi ve konsept"* şeklinde tanımlanmıştır.[117]

> *"Tüm dijital veriler temel olarak birler ve sıfırların kombinasyonudur. Genellikle bit olarak adlandırılır."*[118]

Dijital veriler, kişiler tarafından kaydedilen, biriktirilen veya transfer edilen çeşitli bilgilerden oluşabileceği gibi, aynı zamanda yine bu kişilerin bu sistem ve aygıtları kullanmaları sonucunda bıraktıkları dijital izlerden de oluşabilmektedir. Bilişim sistemlerinin donanım ve yazılımları arasında gerçekleştirilen komut alışverişi, dijital veri üretir ya da var olan verileri çeşitli başka formatlara dönüştürür. Verilerin geçiş yollarına veya barındığı ortamlara dijital ortam denir ve her dijital veri de ilgili bilişim sisteminde bir iz bırakır.[119] Elektronik bitler olarak başlayan verinin yaşam döngüsü, baytlara ve karakterlere, sonra kelimelere evrilmesi ile bir bilgiye ve en sonunda gerekli koşulların da sağlanması ile birlikte bir delile vücut verir.[120]

Dijital veri aktarımı için mevcut metodoloji, *ikili değer (binary)* şeklinde isimlendirilmektedir ve ikili değer, tüm bilgi işlem teknolojisinin temelini oluşturmaktadır.[121] *Binary*, iki tabanlı numaralandırma sistemine veya kodlama şemasına verilen isimdir ki bu sistemde yalnızca iki olası durum söz konusudur. Bilgisayarlarda, dijital verilerin hareketi bu iki durum ile kısaca 1 ve 0'ların uygun dizilimi ile kolayca temsil edilir.[122] Tek başına bir (1) ve sıfır (0), bir biti temsil eder.

---

[115] Başlar, "Elektronik Delil," 1661.
[116] Avrupa Konseyi Siber Suç Sözleşmesi, 23 Kasım 2001 tarihinde Budapeşte'de imzaya açılmıştır ve Türkiye tarafından da 2010 yılında imzalanıp 2014 yılında yürürlüğe girmiştir. Merve Erdem ve Gürkan Özocak, "Avrupa Konseyi Siber Suç Sözleşmesi ve Türk Hukukuna Etkileri," *4. UBHK Bildiriler Kitabı*, İzmir, (Mayıs 2016) 1. http://ozocak.com/Dosyalar/27669f.pdf , son erişim: 10.01.2022.
[117] Başlar, "Elektronik Delil," 1661.
[118] Casey, *Digital Evidence*, 442.
[119] Kızılyar, "Ceza Yargılaması," 79- 81.
[120] Albert J. Marcella and Frederic Guillossou, *Cyber Forensics: From Data to Digital Evidence* (Hoboken New Jersey: John Wiley & Sons, 2012), 1- 2.
[121] Marcella and Guillossou, *Cyber Forensics*, 2.
[122] Marcella and Guillossou, *Cyber Forensics*, 3- 4; Robinton, "Courting Chaos," 323.

Bu şekilde temsil edilen bir bit, bilgisayar tarafından tanınan veya işlenen en küçük veri birimi olmaktadır.[123] Sekiz adet bit ise bayt olarak adlandırılmaktadır.[124]

Bir dijital soruşturmada bu bir ve sıfırlardan oluşan belki binlerce sayfa gündeme gelmektedir. Adli bilişim uzmanlarının da bu binlerce sayfa bir ve sıfırları anlamlandırması ve *dijital ekmek kırıntılarını*[125] bir araya getirerek anlamlı bir sonuca ulaşması gerekmektedir. Bu sebeple bilgisayarlar için kolayca anlaşılan bu dilin bizler için de okunulabilir kılınması amacıyla birler ve sıfırlar, *onaltılık (Hexadecimal- HEX)* şekilde yahut belirli bir ve sıfır kombinasyonlarının belirli harf ve sayıları temsil ettiği ASCII değerinin kullanılması suretiyle anlamlandırılır.[126]

Belirli bayt kombinasyonları için dijital delil araması yapılırken bir bayt sırası farkındalığı gereklidir.[127] Birçok dosya türü, yazılım geliştiriciler veya standartlar tarafından tasarlanan ve veri parçalarını sınıflandırmak ve kurtarmak için faydalı olabilecek ayırt edici bir yapıya sahiptir. Bir JPEG görüntüsündeki, Word belgesindeki veya diğer dosya türlerindeki ortak başlıklara genellikle dosya imzaları (*file signatures*) denir ve bunlar, silinen dosyaların bölümlerini bulmak ve kurtarmak için kullanılabilir. Belirli bir dosya imzasını arama ve ilişkili verileri çıkarmaya çalışma süreci, kavramsal olarak daha büyük bir veri kümesinden belirli bir veri parçasını kesmeyi içerdiğinden "oyma" (*carving*) olarak adlandırılır. Adli bilişim bağlamında oyma işlemi ile sabit sürücüdeki belirli bir dosya sınıfının özellikleri kullanılır.[128]

1.1.4.1.1. Kişisel veriler

Yukarıda genel anlamda veri kavramına değindikten sonra yine veri kavramının altında bulunan fakat önemi itibariyle kendisine Anayasanın *"Özel Hayatın Gizliliği"* başlıklı 20. maddesinin 3. fıkrasında yer bulan ve günümüzde artık yalnızca özel hayatın gizliliği hakkıyla değil fakat haberleşme özgürlüğü, düşünceyi açıklama ve yayma özgürlüğü ve hatta basın özgürlüğü gibi birçok temel hak ve

[123] Marcella and Guillossou, *Cyber Forensics,* 4.
[124] Marcella and Guillossou, *Cyber Forensics,* 18; Angus M. Marshall, *Digital Forensics: Digital Evidence in Criminal Investigation* (Chichester: Wiley-Blackwell, 2008), 69.
[125] Kerr, "Digital Evidence And The New Criminal Procedure," 285.
[126] Casey, *Digital Evidence,* 442; İkili değerin, *"ondalık (decimal)"* değere dönüştürülmesi ve sonrasın elde edilen ASCII değeri aracılığıyla harflerin temsil edilmesi ya da ikili değerin *"onaltılık (Hexadecimal- HEX)"* değere dönüştürülmesi aracılığıyla harflerle temsil edilmesi hakkında detaylı bilgi için bkz. Marcella and Guillossou, *Cyber Forensics,* 18- 39.
[127] Casey, *Digital Evidence,* 444.
[128] Oyma işlemi ile ilgili detaylı bilgi için bkz., Casey, *Digital Evidence,* 445.

özgürlükle de bağlantılı olan *"kişisel veri"* kavramına da kısaca değinmek yerinde olacaktır.

6698 sayılı Kişisel Verilerin Korunması Kanunu'nun (KVKK)[129] 3. maddesi, 1. fıkrası d bendi uyarınca kişisel veri; *"Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi"* ifade etmektedir. Günümüzde bilişim sistemlerinin kullanım alanlarının giderek genişlediği ve depolama alanlarının kapasitesi düşünüldüğünde elbette kişisel verilerin de bu sistemlerde yer alacağı kaçınılmaz bir gerçektir. Gerçekten benzer şekilde Anayasa Mahkemesi (AYM) kararları[130] da incelendiğinde, kişisel verilerin;

> *"belirli veya kimliği belirlenebilir olmak şartıyla bir kişiye ilişkin bütün bilgileri ifade ettiği kabul edilmekte olup bu bağlamda adı, soyadı, doğum tarihi ve doğum yeri gibi bireyin sadece kimliğini ortaya koyan bilgilerin değil telefon numarası, motorlu taşıt plakası, sosyal güvenlik numarası, pasaport numarası, öz geçmiş, resim, görüntü ve ses kayıtları, parmak izleri, genetik bilgiler, IP adresi, e-posta adresi, hobiler, tercihler, etkileşimde bulunulan kişiler, grup üyelikleri, aile bilgileri gibi kişiyi doğrudan veya dolaylı olarak belirlenebilir kılan tüm verilerin…"* kişisel veri kavramı çerçevesinde değerlendirildiği belirtilmektedir.

Bu bağlamda bir verinin, kişisel veri olarak kabul edilebilmesi için bazı şartların gerektiğini söyleyebiliriz. Buna göre ilgili verinin öncelikle bir kişiye ait olması gerekmektedir. Başka bir ifadeyle söz konusu veri ile ilgili kişi arasında bir bağlantı kurulabiliyor ve o veriden ilgili kişinin kimliğine ulaşılabiliyorsa, söz konusu veri kişisel veri olarak anılabilecektir.[131] Bu bağlamda doğrudan kişiden elde edilmeyen fakat kişilerin ilişkili oldukları nesnelerden elde edilen verilerin de somut olayın özelliğine göre kişisel veri olarak kabul edilebilecekleri belirtilmiştir.[132] Örnek olarak bir firmanın nakliye araçları üzerine yerleştirdiği ve çalışanlarının verimliliğini

---

[129] Resmî Gazete Tarihi: 07.04.2016, Sayı: 29677.

[130] AYM, E.Ç.A. başvurusu, Başvuru no. 2014/5671, T. 7/6/2018, R.G. Tarih ve Sayı: 24/7/2018-30488; AYM, Kemal Karanfil başvurusu, Başvuru no. 2017/24776, T. 24/5/2018, https://kararlarbilgibankasi.anayasa.gov.tr/ , son erişim: 08.05.2022.

[131] Bahri Öztürk, Elif Altınok Çalışkan ve Serkan Seyhan, *Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı* (Ankara: Seçkin Yayıncılık, Güncellenmiş 2. Baskı, 2022), 17-18; Serdar Çelikel, *Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri* (Ankara: Seçkin Yayıncılık, 2022), 68; Şeyma Sert, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması* (Ankara: Seçkin Yayıncılık, 2019), 31; Onur Baskın, *Türk Hukuku Bakımından Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması,* (Ankara: Seçkin Yayıncılık, 2021), 22.

[132] Öztürk, Altınok Çalışkan ve Seyhan, *Kişisel Verilerin Korunması Hukuku*, 18; Çelikel, *Kişisel Verilerin Korunması Hukuku*, 68.

tespit etmek amacıyla kullandığı araç takip sistemlerinden elde edilen verilerin, çalışan bakımından kişisel veri olarak kabul edilebileceği söylenebilecektir.[133]

Bir verinin, kişisel veri olarak kabul edilebilmesi için gereken ikinci şart ise, veri sahibi kişinin, kimliği belirli ya da belirlenebilir bir kişi olmasıdır. KVKK m. 3/1-d'de yer alan açık hüküm çerçevesinde, kişisel veri sahibi olan kişi ancak gerçek kişi olabilecektir. Bu çerçevede ilgili veri, gerçek bir kişinin kimliğini belirli veya belirlenebilir kılma gücüne sahipse, kişisel veri olarak kabul edilebilecektir.[134] Bu bağlamda IP adreslerinin[135] bilgisayarın birden fazla kullanıcısı olması durumunda, gerçek bir kişinin tespit edilmesini sağlayamayacağı ve bu sebeple belirlenebilir kişiye ait bir veri olarak edilemeyeceği ancak buna karşılık tek bir kullanıcı tarafından kullanılan bilgisayardan elde edilen IP adresinin, kişisel veri olarak kabul edilmesi gerektiği ileri sürülmüştür.[136] Benzer şekilde kişilerin bilişim ağlarında bıraktığı elektronik izler ve internette gezinme geçmişi gibi hususlar da bazı hallerde gerçek kişiyi belirlenebilir kılabilecektir. Bu bilgilerin toplanması, işlenmesi ve aktarılması durumlarında ise kişisel verilerin korunması hakkının ihlali gündeme gelebilecektir. Ek olarak gündelik hayatın giderek dijitalleştiği ve hayatın neredeyse her anının bilişim sistemlerine kaydedildiği gerçeği göz önünde bulundurulduğunda kişiye ait bilişim sistemine müdahale ile birlikte, kişisel verilere de müdahale edilmiş olacağını söylemek yanlış olmayacaktır.[137]

Kısaca kişisel veri kavramını tanımladıktan sonra bir suçun aydınlatılması amacıyla bilişim sistemlerinden verilerin (ve bu bağlamda kişisel verilerin) elde edilmesi kavramını düşündüğümüzde, bunun KVKK anlamında karşılığının, *"Kişisel verilerin işlenmesi"* olduğunu görmekteyiz. Gerçekten de KVKK m. 3/1-e uyarınca kişisel verilerin işlenmesi; *"Kişisel verilerin… elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi… gibi veriler üzerinde gerçekleştirilen her türlü işlemi"* ifade etmektedir. Bununla birlikte kişisel veriler, her zaman ve her koşulda

---

[133] Öztürk, Altınok Çalışkan ve Seyhan, *Kişisel Verilerin Korunması Hukuku*, 18.
[134] Çelikel, *Kişisel Verilerin Korunması Hukuku,* 69; Sert, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması,* 31.
[135] IP adresi, "Belirli bir ağa bağlı cihazların birbirini tanımak, birbirleri ile iletişim kurmak ve birbirlerine veri yollamak için kullandıkları, internet protokolü standartlarına göre verilen adresi ifade eder. İnternete bağlanan her bilgisayara internet servis sağlayıcı tarafından bir IP adresi atanır ve internetteki bilgisayarlar birbirlerine bu IP adresi ile ulaşırlar." Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 55.
[136] Ayözger, A. Çiğdem, *Kişisel Verilerin Korunması* (İstanbul: Beta Yayıncılık, 2016), 11. Aktaran: Sert, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, 32.
[137] Değirmenci, Sayısal Delil, s. 107.

değil ancak belli bazı hallerde işlenebilecektir. Anayasanın "Özel hayatın gizliliği" başlığını taşıyan 20. maddesinin 3. fıkrası incelendiğinde kişisel verilerin, "*ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla*" işlenebileceğini görmekteyiz.

KVKK m. 4/2 incelendiğinde kişisel verilerin işlenmesi sırasında belli bazı ilkelere uyulmasının zorunlu olduğunu görmekteyiz. Buna göre öncelikle kişisel veriler, *"ancak bu Kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak"* işlenebilecektir.[138] İkinci olarak kişisel veriler işlenirken *"hukuka ve dürüstlük kurallarına uygun olunması"* gerekecektir. Hukuka uygun olma ile veri işlemenin usul ve esas bakımından mevzuata, içtihatlara ve hukukun evrensel ilkelerine uygun olması kastedilirken; dürüstlük kuralına uygun olma ile veri denetçilerinin, verileri işlerken kişisel veri sahiplerinin çıkarlarını ve makul beklentilerini göz önünde bulundurmaları gerekliliğinin ifade edildiği söylenebilir.[139] Üçüncü olarak kişisel verilerin, *"doğru ve gerektiğinde güncel olması"* gerekmektedir. Bu doğrultuda işlenen verinin doğruluğunun veri işleme sürecinin sonuna kadar devam etmesi gerekmekte ve bu sebeple de veri sahiplerinin, kişisel verilerinde ortaya çıkan değişikliklerin, güncellenmesini isteyebilmeleri gerekmektedir.[140] Dördüncü olarak kişisel verilerin, *"belirli, açık ve meşru amaçlar için işlenmesi"* gerekmektedir. KVKK'nın gerekçesi uyarınca söz konusu ilke ile veri sorumluları, veri işleme amaçlarını açık ve net olarak belirlemeli ve söz konusu amaç meşru bir amaç olmalıdır. Amacın meşru olması ise veri sorumlusu tarafından işlenen kişisel verilerin, sunmuş olduğu hizmet yahut yapmış olduğu iş ile bağlantılı ve bunlar için gerekli olmasıdır.[141] Beşinci olarak ise kişisel verilerin işlenmesinde *"amaçla bağlantılı, sınırlı ve ölçülü"* olunmalıdır. Bu bağlamda veri, sunulan hizmet ile ilgili yahut bağlantılı amaçlar için ve bu alanlarla sınırlı bir şekilde işlenebilecektir.[142] Altıncı ve son olarak kişisel veriler *"ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza"* edilebileceklerdir. Bu bağlamda örneğin CMK m. 134 kapsamında kişilerin bilişim sistemlerinden elde edilen kişisel veriler (her ne kadar ilgili maddede

[138] Öztürk, Altınok Çalışkan ve Seyhan, *Kişisel Verilerin Korunması Hukuku*, 58.
[139] Öztürk, Altınok Çalışkan ve Seyhan, *Kişisel Verilerin Korunması Hukuku*,59; Sert, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması,* 77.
[140] Sert, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, 82.
[141] Sert, Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması, 79.
[142] Öztürk, Altınok Çalışkan ve Seyhan, *Kişisel Verilerin Korunması Hukuku,* 61.

bir süre öngörülmemişse de), kişi hakkında verilen kararın kesinleşmesiyle birlikte artık muhafaza edilmeyecektir.

Kişisel verilerin işlenmesiyle ilgili genel ilkelere değindikten sonra kişisel verilerin işlenmesi şartlarını düzenleyen KVKK m. 4 vd. hükümleri incelendiğinde kanunun, kişisel verileri kendi içerisinde bir ayrıma tabi tuttuğu görülmektedir. Bu doğrultuda kişisel veriler, genel nitelikli kişisel veriler ve özel nitelikli kişisel veriler olarak iki başlıkta incelenmektedir. Özel nitelikli kişisel veriler, kanunda sınırlı sayıda sayma yöntemiyle belirtildiği ve bunlar dışında kalan kişisel veriler, genel nitelikli kişisel veriler olarak kabul edildiği için öncelikle özel nitelikli kişisel veriler incelenecek olup devamında genel nitelikli kişisel verilere yer verilecektir.

İlk olarak KVKK m. 6/1, kimi bazı verilerin, *"hassas veri"* niteliğinde olmaları ve bunların hukuka aykırı işlenmeleri neticesinde kişilerin doğrudan ayrımcılığa uğrayabilmeleri ihtimali sebebiyle bu verilerin işlenebilmesi bakımından farklı koşullar getirmiştir.[143] Bu bağlamda özel nitelikte kişisel veriler, *"Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri"* şeklinde sınırlı sayma yöntemiyle belirtmiştir. Aynı maddenin ikinci fıkrası uyarınca da *"özel nitelikli kişisel verilerin, ilgilinin açık rızası[144] olmaksızın işlenmesi"*nin yasak olduğu belirtilmiştir. Buna karşılık, üçüncü fıkra incelendiğinde, bu sayılan özel nitelikli kişisel verilerden, "sağlık ve cinsel hayat" dışındaki verilerin, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebileceği; buna karşılık sağlık ve cinsel hayat verilerinin ise *"kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi"* amaçlarıyla ve yalnızca *"sır saklama yükümlülüğü altında*

[143] Öztürk, Altınok Çalışkan ve Seyhan, *Kişisel Verilerin Korunması Hukuku*, 82-83.

[144] Bu doğrultuda "açık rıza" kavramına kısaca değinmek yerinde olacaktır. KVKK m. 3/1-a uyarınca açık rıza; *"Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rızayı"* ifade etmektedir. Bu doğrultuda açık rıza öncelikle *"belirli bir konuya ilişkin"* olmalıdır. başka bir ifadeyle genel bir irade açıklaması yapılarak "kişisel verilerimin işlenmesini kabul ediyorum" şeklinde açık uçlu ve belirsiz bir ifade tek başına Kanun bağlamında "açık rıza" olarak kabul edilemeyecektir. İkinci olarak açık rıza *"bilgilendirmeye dayanma"*lıdır. Başka bir ifadeyle kişinin neye rıza gösterdiğini bilmesi ve sadece konu üzerinde değil, aynı zamanda rızasının sonuçları üzerinde de tam bir bilgi sahibi olması gerekmektedir. Üçüncü ve son olarak açık rızanın *"özgür iradeyle açıklanması"* gerekmektedir. Başka bir ifadeyle kişinin iradesini sakatlayacak her tür fiil, kişisel verilerinin işlenmesi için verdiği rızayı da sakatlayacak ve bu doğrultuda rızanın özgür iradeyle verildiği söylenemeyecektir. Detaylı bilgi için bkz. KVKK, Açık Rıza Rehberi, https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf , son erişim: 14.05.2022.

bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından" ilgilinin açık rızası aranmaksızın işlenebileceği belirtilmiştir. Özel nitelikli kişisel verilerin işlenmesi konusunda dikkat çeken bir diğer husus ise KVKK m. 6/4 hükmüdür. Buna göre *"özel nitelikli kişisel verilerin işlenmesinde, ayrıca Kurul tarafından belirlenen yeterli önlemlerin alınması şarttır."* Bu önlemlerin neler olduğu, Kişisel Verileri Koruma Kurulu'nun, 31/01/2018 Tarihli ve 2018/10 Sayılı Kararında sayılmıştır. Buna göre;

1- Özel nitelikli kişisel verilerin güvenliğine yönelik sistemli, kuralları net bir şekilde belli, yönetilebilir ve sürdürülebilir ayrı bir politika ve prosedürün belirlenmesi,
2- Özel nitelikli kişisel verilerin işlenmesi süreçlerinde yer alan çalışanlara yönelik, özel nitelikli kişisel veri güvenliği konularında düzenli olarak eğitimler verilmesi, gizlilik sözleşmelerinin yapılması, verilere erişim yetkisine sahip kullanıcıların, yetki kapsamlarının ve sürelerinin net olarak tanımlanması, periyodik olarak yetki kontrollerinin gerçekleştirilmesi ve görevden ayrılanların bu alandaki yetkilerinin derhal kaldırılması ve envanterin geri alınması,
3- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortam ise bu ortama özgü tedbirlerin alınması,
4- Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, fiziksel ortam ise yeterli güvenlik önlemlerinin alındığından emin olunması ve fiziksel güvenliğin sağlanması,
5- Özel nitelikli kişisel veriler aktarılacaksa aktarım yöntemine uygun tedbirlerin alınması,
6- Kişisel Verileri Koruma Kurumunun internet sitesinde yayımlanan Kişisel Veri Güvenliği Rehberinde belirtilen uygun güvenlik düzeyini temin etmeye yönelik teknik ve idari tedbirler de dikkate alınması.[145]

İkinci olarak genel nitelikli kişisel verilerin işlenmesini inceleyecek olursak öncelikle karşımıza KVKK m. 5 çıkmaktadır. Madde incelendiğinde ilk olarak özel nitelikli kişisel verilerden farklı bir şekilde, genel nitelikli kişisel verilerin sınırlı sayıda belirtilmediği görülmektedir. Buna göre yukarıda sayılan özel nitelikli kişisel

[145] Öztürk, Altınok Çalışkan ve Seyhan, *Kişisel Verilerin Korunması Hukuku*, 86.

verilerden sayılmayan kişisel veriler, genel nitelikli kişisel veri olarak kabul edilecektir.[146]

Özel nitelikli kişisel verilerde olduğu gibi genel nitelikli kişisel verilerin de ilgili kişinin *açık rızası* olmaksızın işlenemeyeceğini görmekteyiz. Buna karşılık, genel nitelikli kişisel veriler de belli bazı şartların gerçekleşmesi halinde ilgili kişinin açık rızası aranmaksızın işlenebilecektir. Bu şartlar ise;

> *"Kanunlarda açıkça öngörülme; fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması; bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması; veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması; ilgili kişinin kendisi tarafından alenileştirilmiş olması; bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması; ilgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması." şeklindedir.*

Son olarak KVKK'nın "İstisnalar" başlığını taşıyan 28. maddesini de incelemek yerinde olacaktır. Söz konusu madde, Kişisel Verilerin Korunması Kanunu'nun uygulanmayacağı ve bu bağlamda kişisel verilerin işlenmesinin hukuka aykırı sayılmayacağı halleri, sınırlı sayma yöntemiyle belirtmiştir.[147] Bu istisnalardan konumuzla bağlantısı çerçevesinde KVKK m. 28/1-d hükmü önem arz etmektedir. Buna göre: *"Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi…"* halinde KVKK hükümleri uygulanmayacaktır.[148] Buna göre KVKK m. 4'te belirtilen kişisel verilerin işlenirken uyulması gereken ilkelerin de bu istisna hükmü karşısında, *"yargı makamları veya infaz mercileri tarafından yürütülen*

---

[146] Çelikel, *Kişisel Verilerin Korunması Hukuku,* 77; Baskın, *Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması,* 42-43.

[147] Öztürk, Altınok Çalışkan ve Seyhan, *Kişisel Verilerin Korunması Hukuku*, 36; Sert, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, 125; Murat Volkan Dülger, *Kişisel Verilerin Korunması Hukuku* (İstanbul: Hukuk Akademisi Yayınevi, 3. Baskı, 2020), 349.

[148] Diğer istisnai haller için bkz. KVKK m. 28/1: *"a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi. b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi. c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi. ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi."*

soruşturma, kovuşturma, yargılama veya infaz işlemleri" sırasında geçerli olmayacağını belirtmek yanlış olmayacaktır.[149]

Buna karşılık KVKK m. 28/2 hükmü, bir istisna hükmü olarak düzenlenen birinci fıkra hükmünün de bir istisnasını getirmiştir.[150] Konumuzla bağlantısı bakımından KVKK m. 28/2-a maddesi incelenecek olursa: *"Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması…"* durumunda, kişisel verilerin korunması amacına ve temel ilkelerine uygun ve orantılı olmak kaydıyla KVKK'nın veri sorumlusunun aydınlatma yükümlülüğünü düzenleyen 10 uncu, zararın giderilmesini talep etme hakkı hariç, ilgili kişinin haklarını düzenleyen 11 inci ve Veri Sorumluları Siciline kayıt yükümlülüğünü düzenleyen 16 ncı maddeleri uygulanmayacaktır.[151] Buna göre, belirtilen istisnanın istisnası halleri gerçekleşmişse KVKK'nın yukarıda bahsedilen maddeleri uygulanmayacak olup kalan maddeler uygulanmaya devam edilecektir. KVKK m. 28/2- a bendinin, önceki fıkranın d bendinden farklı olarak, kolluk görevlilerine hitap ettiğini belirtmemiz gerekecektir. Buna göre kolluk görevlileri kişisel verileri yalnızca "suç işlenmesinin önlenmesi" amacıyla idari kolluk görevi esnasında veya bir "suç soruşturması" sırasında adli kolluk görevi esnasında işlerlerse, KVKK m. 28/2 de belirtilen istisnanın istisnası hükümlerinden yararlanabileceklerdir. İlk fıkrada belirtilen "yargı makamları" ve "infaz mercileri"nden farklı olarak kolluk görevlilerinin, suç soruşturması ve suç işlenmesinin önlenmesi dışında da farklı görevlerinin olması sebebiyle onlara, ilk fıkradaki gibi tam bir muaflığın verilmediğini söyleyebiliriz. Gerçekten de kolluk görevlileri, trafiği düzenleme görevi esnasında kişisel veri işlerlerse, hiçbir istisna hükmü uygulanmaksızın, KVKK'ya tamamen tabi olacaklardır.[152]

[149] Tezcan, v.d., *Dijital Ceza Muhakemesi Hukuku*, 178.
[150] Öztürk, Altınok Çalışkan ve Seyhan, *Kişisel Verilerin Korunması Hukuku*, 37.
[151] Diğer istisnanın istisnası halleri için bkz. KVKK m. 28/2: *"b) İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi. c) Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması. ç) Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması."*
[152] Dülger, *Kişisel Verilerin Korunması Hukuku*, 359.

Bu kapsamda, KVKK m. 28'de öngörülen istisna ve istisnanın istisnası hükümlerinin, aynı zamanda kişisel verilerin işlenmesiyle ilgili olarak hukuka uygunluk nedenleri şeklinde de değerlendirilebileceği belirtilmiştir.[153]

Sonuç itibariyle, KVKK ve diğer kanunlara uygun olarak işlenen ancak işlenmesini gerektiren sebeplerin ortadan kalktığı, başka bir ifadeyle, bir cezai soruşturma veya kovuşturma çerçevesinde elde edilen fakat sonrasında hakkında verilen kararın kesinleştiği kişinin kişisel verilerinin; KVKK m. 7 uyarınca silinmesi, yok edilmesi yahut anonim hale getirilmesi gerekecektir. Söz konusu silme, yok etme veya anonim hale getirme işlemi ise, *"Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik"*[154] hükümleri çerçevesinde gerçekleştirilecektir. Buna göre yönetmeliğin yedinci maddesi uyarınca işlenen kişisel verilerin, *"işlenme şartlarının tamamının ortadan kalkması halinde, veri sorumlusu*[155] *tarafından resen veya ilgili kişinin talebi üzerine silinmesi, yok edilmesi veya anonim hâle getirilmesi"* gerekecektir.

Bununla birlikte kişisel verileri silme, yok etme yahut anonim hale getirme işlemlerinin, KVKK'nın birinci ve ikinci fıkrası çerçevesinde farklılık gösterebileceğini söyleyebiliriz. Yukarıda da belirtildiği üzere, KVKK m. 28/1, kanunun kapsamı dışında kalan halleri düzenlerken; KVKK m. 28/2, belirli maddeler hariç kanunun kalanının uygulanmaya devam edeceği halleri belirtmiştir. Buna göre konumuzla bağlantısı açısından KVKK m. 28/1-d uyarınca kişisel veriler, *"soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından"* işlenmişlerse bu verilerin, KVKK anlamında silinmesi, yok edilmesi yahut anonim hale getirilmeleri söz konusu olmayacaktır. Buna karşılık yine konumuzla bağlantısı açısından KVKK m. 28/2-a uyarınca kişisel veriler *"suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması"* gibi amaçlarla işlenmişlerse bu verilerin, KVKK m. 7 anlamında silinmesi, yok edilmesi yahut anonim hale getirilmeleri gerekecektir.

---

[153] Tezcan, v.d., *Dijital Ceza Muhakemesi Hukuku*, 178; Sert, *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*, 126.
[154] Resmî Gazete Tarihi: 28.10.2017, Sayı: 30224.
[155] KVKK m. 3/1-a: *"Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi"* ifade eder.

1.1.4.2. Dijital delil

Bilişim sistemlerinde delil aramanın amacı yargılamaya konu maddi olayı herhangi bir şekilde tespit eden verilere ulaşmak ve dijital delilleri elde edebilmektir.[156] Bu bağlamda, veri ile dijital delil arasındaki ilişkinin bir fonksiyon ilişkisi olduğunu, dijital delilin mutlaka dijital veri niteliğinde bulunması gerektiğini ve buna karşın sadece maddi olayla irtibatlı olan dijital verinin dijital delil olarak nitelendirilebileceğini söyleyebiliriz.[157]

Veri ile bilgi, bilgi ile de delil arasında fark vardır. İlk olarak karşımıza veriler çıkar. Verilerin anlamlı bir şekilde sıralanması neticesinde ise bilgi elde edilir. Sonrasında soruşturmayı yürüten kişiler veya mahkeme tarafından yapılan inceleme ve değerlendirme ile delil kavramı ortaya çıkar.[158] Bu bağlamda dijital delillerin, soruşturma veya kovuşturma konusu suçla ilgisi olan ve suçun aydınlatılmasında kullanılan bilgiler olduğunu söyleyebiliriz. Dijital deliller çeşitli açılardan ele alınarak tanımlanmaya çalışılmıştır.

Bir tanıma göre dijital delil, bir suçun nasıl meydana geldiğine dair bir teoriyi destekleyen veya çürüten veya kast veya mazeret gibi suçun kritik unsurlarını ele alan bir bilgisayar kullanılarak saklanan veya aktarılan herhangi bir veri olarak tanımlanır.[159]

Bir başka tanım, elektronik delili, herhangi bir elektronik cihaz aracılığıyla manipüle edilen, üretilen, depolanan veya iletilen potansiyel ispat değeri olarak tanımlamıştır.[160]

Bir diğer tanım uyarınca dijital delil, ikili değer (binary) biçiminde saklanan, iletilen veya elde edilen delil niteliğindeki herhangi bir bilgidir.[161]

Yargıtay'ın yapmış olduğu tanıma göre dijital deliller; "CD, DVD, flash bellek, disket, harici ve dahili harddisk, bilgisayar özelliği içeren noktaları bakımından akıllı

---

[156] Değirmenci, *Sayısal Delil,* 348.
[157] Değirmenci, *Sayısal Delil,* 60; Başlar, "Elektronik Delil," 1662.
[158] Sergey Zuev, "Traditional Values of Criminal Procedure in Terms of IT Development," *Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT*, (2019): 420.
[159] Casey, *Digital Evidence,* 7.
[160] Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 143- 144; Jeanne Pia Mifsud Bonnici, Melania Tudorica and Joseph A. Cannataci, "The European Legal Framework on Electronic Evidence: Complex and in Need of Reform," *Law, Governance and Technology Series*, ed. Maria Angela Biasiotti, v.d., vol. 39, Cham, Switzerland: Springer, (2018): 189; Leyla Keser Berber, *Adli Bilişim* (Ankara: Yetkin Yayınları, 2004), 46. Aktaran: Kaynakçıoğlu, "Dijital Deliller," 23.
[161] Leacock, "Search and Seizure of Digital Evidence," 221.

telefon ve benzerlerinden elde edilen ve tamamı "dijital delil" olarak adlandırılan, suistimale müsait olan veriler…" şeklinde tanımlanmıştır.[162]

Bir başka tanım uyarınca dijital delil;

> *"iddia edilen bir fiilin ispatında kullanılmak istenen veya kullanılan; elektronik ortamda oluşan/ oluşturulan, değiştirilen, iletilen veya saklanan veri, kayıt ve belgeleri"* ifade etmektedir.[163]

Bir diğer tanım dijital delili;

> *"suç konusu fiille ilgili olarak yürütülen bir adli bilişim çalışması esnasında, bilişim sistemleri (bilgisayar, mobil telefon, dijital fotoğraf makineleri, dijital videolar, dijital faks makineleri vb.) ve bu kapsamdaki depolama aygıtları üzerinden elde edilen adli deliller"* olarak ifade edilmiştir.[164]

Bir başka tanım uyarınca dijital deliller, dijital ortamda tutulan, oluşturulan, depolanan ve iletilen verilerdir. Söz konusu veriye delil değeri kazandıran şey, cezai uyuşmazlığa konu olan suç fiili ile olan ilgisidir.[165] Eelektronik ortamda muhafaza edilen bilgiler muhakeme konusu maddi olayla ilgili ve güvenilir olduğu hallerde delil olarak kabul edilecektir.[166]

Bir diğer tanıma göre ise dijital deliller;

> *"bilişim teknolojisi içeren her türlü donanım, bu donanım üzerinde çalışan her türlü yazılım/yazılımlar tarafından kullanılan/üretilen her türlü veri ile bilişim teknolojisi tarafından kullanılan her türlü elektronik sinyali"* ifade etmektedir.[167]

Avrupa birliğine ait bir proje olan ve 7. Çerçeve Programının bir parçası olarak Avrupa Komisyonu tarafından finanse edilen bir proje olan *"Evidence"*[168] projesinde elektronik delil ve dijital delil tanımına yer verilmiştir. Buna göre

> *"elektronik delil herhangi bir elektronik cihaz kullanılarak oluşturulan, işlenen, saklanan veya iletilen, analog bir cihazın ve/veya potansiyel değere sahip dijital bir cihazın çıktısından kaynaklanan herhangi bir veridir. Üretilmiş veya sayısal bir formata dönüştürülmüş elektronik delil ise dijital delildir."*[169]

---

[162] 16. Ceza Dairesi., E. 2015/4672 K. 2016/2330 T. 21.4.2016.
[163] Arslan, "Dijital Delil ve İletişimin Denetlenmesi," 191.
[164] Türkay Henkoğlu, *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi* (İstanbul: Pusula Yayıncılık, 2. Baskı, 2014), 5.
[165] Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj)," 56- 57.
[166] Sarsikoğlu, "Elektronik Delil (E-Delil) Kavramı," 519.
[167] Mustafa İlker Öztürk, "Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri" (Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Fizik İncelemeler ve Kriminalistik Programı, Ankara 2007), 38.
[168] "EVIDENCE; European Data Informatics Exchange Framework for Courts and Evidence".
[169] https://cordis.europa.eu/project/id/608185/reporting , son erişim; 07.01.2022.

Dijital Delil Hakkında Bilimsel Çalışma Grubu *(The Scientific Working Group on Digital Evidence- SWGDE)*[170] dijital kanıtı, *ikili değer (binary)* biçiminde depolanan veya iletilen, delil değeri olan bilgi olarak tanımlamaktadır.[171] Ancak bu tanım, dijital delillerin ikili değer biçiminde depolandığını yani yalnızca bilgisayarlardan elde edilebildiğini halbuki dijital delillerin diğer başka cihazlardan da elde edilebilmelerinin mümkün oluşu sebebiyle eleştirilmiştir.[172]

Ulusal Polis Şefleri Konseyi *"(National Police Chiefs' Council- NPCC)"*[173] yapılan bir tanıma göre dijital delil, bir bilgisayarda depolanan veya bir bilgisayar tarafından iletilen ve araştırma değeri olan bilgi ve verilerdir.[174]

Görüldüğü üzere ulusal ve yabancı kaynaklı olmak üzere dijital deliller çeşitli kişiler ve kurumlarca, çeşitli özelliklerine göre ve farklı açılardan birçok şekilde tanımlanmıştır. Tüm bu tanımlamalardan yola çıkarak bir tanım ortaya koyacak olursak dijital deliller; bir suçla bağlantısı olan, bilişim sistemleri bünyesinde ikili değer (binary) biçiminde üretilen, depolanan veya iletilen, uzman kişiler tarafından yürütülen bir adli bilişim faaliyeti neticesinde elde edilebilen, verilerdir.

1.1.5. Dijital delillerin nitelik ve özellikleri

Dijital delillerin geçerli olabilmeleri için öncelikle bir delilde hukuken olması gereken özellikleri barındırması ve buna ek olarak teknolojik anlamda da bazı özelliklere sahip olması gerekmektedir. Bu özellikler, dijital delillerin bilişim alanı açısından sahip olduğu teknik özelliklerinin getirdiği sonuçlar neticesinde ortaya çıkmaktadırlar.[175] Öyle ki dijital deliller, hukuken doğru bir şekilde elde edilmiş olsa bile elde edilme sırasında teknik anlamda hatalar gerçekleştirildiyse, o delilin geçerliliği tartışmalı hale geleceği gibi teknik anlamda bir kusur olmaksızın elde edilen delil, hukuk kurallarına aykırı bir şekilde elde edilmişse hükme esas alınamayacaktır.

---

[170] 1992 yılında bir grup devlet temsilcisinin ortak çabası olarak oluşturulan kolluk kuvvetleri üyelerinden oluşan bir ABD örgütüdür ve ABD Gizli Servisi (USSS) ve Federal Soruşturma Bürosu'nun (FBI) ortak çabasıdır. Bkz. https://www.swgde.org/home , son erişim, 14.01.2022.
[171] Gordana Buzarovska Lazetik and Olga Koshevaliska, "Digital Evidence in Criminal Procedures -A Comparative Approach-," *Balkan Social Science Review*, Vol. 2 (December 2013): 65.
[172] Chaikin, "Network investigations," 241.
[173] Ulusal Polis Şefleri Konseyi, 2015 yılında, kendisinden önce var olan Polis Şefleri Birliği *(Association of Chief Police Officers- ACPO),* yerine kurulmuş bir İngiliz kurumudur. Ancak böyle bir değişiklikle birlikte günümüzde de hala ACPO tarafından getirilen kurallar ve tanımlamalar geçerliliğini büyük ölçüde korumaktadır. Bkz. Graeme Horsman, "ACPO principles for digital evidence: Time for an update?," *Forensic Science International: Reports*, Volume 2 (2020): 1.
[174] Buzarovska Lazetik and Koshevaliska, "Digital Evidence in Criminal Procedures," 66.
[175] Kaynakçıoğlu, "Dijital Deliller," 37.

Bu bağlamda hukuken ve teknolojik bakımdan geçerliliği denetlenen bir dijital delilin ceza yargılamasında kullanılmasında haliyle bir sakınca olmayacaktır.[176]

Dijital deliller öncelikle gözle görülemez ve gizli niteliktedirler. Bu sebeple daha önce de belirttiğimiz gibi dijital delillerin varlığının anlaşılabilmesi, fiziksel delillerden farklı olarak yardımcı alet veya teçhizat ile mümkün olabilmektedir. Çünkü verilerden elde edilen bilgiler yalnızca insanın duyu organları ile algılanamaz. Söz konusu teçhizat ise çeşitli donanım ve yazılımlardan oluşmaktadır.[177] Bu konu ile ilgili olarak denmiştir ki,

> *"makine dili ile kodlanmış olan bilgiler yine bir makine tarafından yorumlanmalıdır".*[178]

Dijital deliller, değerlendirilmesi çok zor olabilen dağınık, kaygan bir delil türüdür. Örneğin, bir sabit disk, üst üste katmanlanan büyük bilgi parçalarından oluşur. Ancak çoğunlukla bu büyük bilgi yığının sadece küçük bir kısmı suç konusu fiille ilgilidir. Dijital deliller, bulunduğu ortamda olayla ilgili olmayan verilerle karışık bir halde bulunmaktadır. Bu durum ise suçla bağlantılı bilgilerin çıkarılmasını, bir araya getirilmesini ve yorumlanabilecek bir forma dönüştürülmesini gerekli kılar. Olayla ilgili olan sayısal verilerin bulunması, çıkarılması ve anlaşılabilir hale getirilmesi ise oldukça vakit alıcı bir faaliyettir.[179]

Dijital delillerin aksine fiziksel deliller, gözle görülebilen, üzerinde el koyma, muhafaza altına alma kararı verilerek kolayca götürülebilen deliller iken dijital deliller, böyle bir somut yapıya sahip değildir. Elbette ki dijital deliller var olabilmeleri bakımından bir donanıma ihtiyaç duyarlar ve dolayısıyla bir dijital delilin içerisinde bulunduğu bir donanım aygıtı mutlaka vardır. Ancak dikkat edilmesi gereken husus,

---

[176] Başlar, "Elektronik Delil," 1655; Furkan Yılmaz ve Hüseyin Çakır, "Karar Destek Sistemlerinin Mobil Cihaz Adli Bilişimi Süreçlerine Uygulanmasına Yönelik Bir Öneri Çalışması," *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 7 (2021): 26; Değirmenci, "Bilgi Toplumunun Delil Türü," 15; Afandak, "Ceza Muhakemesinde Dijital Deliller," 65- 66.

[177] Değirmenci, *Sayısal Delil,* 132; Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 59; Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj)," 58- 59; Sarsikoğlu, "Elektronik Delil (E-Delil) Kavramı," 516- 517; Başlar, "Elektronik Delilin Toplanması," 80; Değirmenci, "Bilgi Toplumunun Delil Türü," 21; Öztürk, "Bilişim Cihazlarındaki Sayısal Delillerin Tespiti," 39; Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku* (Ankara: Seçkin Yayınevi, 8. Baskı, 2020), 617; Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 144.

[178] Kubilay Say, "Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi" (Disiplinlerarası Adli Tıp Anabilim Dalı Fizik İncelemeler ve Kriminalistik Bilim Dalı Yüksek Lisans Tezi, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, Ankara, 2006), 29.

[179] Casey, *Digital Evidence,* 25; Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj)," 60- 61; Başlar, "Elektronik Delil," 1666; Değirmenci, "Bilgi Toplumunun Delil Türü," 21- 22.

burada delil niteliği taşıyan şeyin, dijital delili içerisinde barındıran donanım veya dijital delilin ekran çıktısı değil bizzat bilişim sisteminde yer alan veri olduğudur.[180] Öyle ki birazdan bahsi geçecek olan ve bilginin kaynağını gösteren bilgi olarak tanımlanabilecek olan üst veriler (meta-data); dijital delil, elektronik ortamda bulunan delilin çıktısı değil ancak bizzat kendisi olarak kabul edilebilirse, dijital delil kapsamında değerlendirilebileceklerdir.[181] Aksi durumda bu veriler belki delil olarak bile ele alınamayacaklardır. Çünkü bu veriler dijital delilin çıktı alınması halinde görülememektedirler.

Dijital deliller, genellikle bazı dijital nesne veya olayların bir soyutlamasıdır. Örneğin bir kişi bir bilgisayara e-posta göndermek gibi bir görevi gerçekleştirmesi talimatını verdiğinde, bu işlem neticesinde gerçekleşen hareketler, gerçekte ne olduğuna dair yalnızca kısmi bir görünüm veren veri kalıntılarıdır. Bu sebeple dijital deliller genellikle belirti delili olarak kabul edilmektedir. Çünkü yalnızca dijital delile dayanarak bir bilgisayar etkinliğinin bir bireye atfedilmesi her zaman kolay değildir. Bu nedenle, dijital deliller çoğunlukla soruşturmaların bir bileşeni niteliğinde kabul edilirler. Gerçekten de suç fiilinin gerçekleşmesi esnasında bilgisayarı başka birinin kullanmış olma ihtimali vardır. Bu bağlamda dijital delillerin delil gücünün artması için bilişim sisteminin bir bütün olarak incelenmesi gereklidir. Dijital delillerin, fiziksel delillerden farklı olarak bütünden ayrı bir şekilde incelenmesi, dijital delilin olayı temsil edici niteliğini yitirmesine veya büyük ölçüde kaybetmesine neden olabilecektir. Sonuç olarak dijital delillerin doğrulanması ve delil değeri kazanması bakımından, veriyi barındıran bilişim sisteminin bütün olarak incelenmesi veya elde edilenlerin başka delillerle desteklenmesi katkı sağlayacaktır.[182]

Dijital deliller, hassas bir yapıya sahiptirler. Dijital delillerin kolayca manipüle edilebilmesi veya yok edilebilmesi, adli bilişim uzmanları bakımından yeni zorluklar doğurmaktadır. Öyle ki dijital deliller, suçlular tarafından kötü niyetli bir şekilde veya

---

[180] Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 144; Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 59; Dülger, *Bilişim Suçları,* 603; Çağrı Börekçi, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde; Arama, Kopyalama ve Elkoyma" (Yayınlanmamış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul 2020), 27.

[181] Sarsikoğlu, "Elektronik Delil (E-Delil) Kavramı," 520; Başlar, "Elektronik Delil," 1659; Değirmenci, "Bilgi Toplumunun Delil Türü," 21.

[182] Casey, *Digital Evidence,* 25- 26; Casey, "Error, Uncertainty and Loss," 42; Değirmenci, *Sayısal Delil,* 135; Değirmenci, "Bilgi Toplumunun Delil Türü," 22; Afandak, "Ceza Muhakemesinde Dijital Deliller," 42.

adli bilişim uzmanları tarafından elde edilmeleri sırasında herhangi bir belirgin bozulma işareti bırakmadan yanlışlıkla değiştirilebilir veya yok edilebilirler.[183]

Fiziksel delillerin, delilin incelenmesi ile birlikte tükenebilme ihtimali söz konusudur. Öyle ki olay yeri dondurulamayacağı için bütün delillerin aranması sürecinde olay yerinde yer alan izler de zamanla kaybolma eğiliminde olacaktır. Buna karşılık dijital deliller kolaylıkla birebir kopyalanabilmektedirler ve çıkarılan kopya üzerinden gerçekmiş gibi işlem yapılabilmektedir. Bu işlem ile delil kaybı ihtimali neredeyse sıfıra indirilir ve incelemeler, kopya üzerinden gerçekleşir.[184]

Dijital delillerin, fiziksel delillerden farklı olarak tamamen yok edilmesi ancak onu barındıran fiziksel ortamın geriye döndürülemeyecek şekilde tahrip edilmesi ile mümkündür. Bu sebeple dijital delil niteliğinde olan bir veri silinse yahut sabit disk sürücüsü formatlansa dahi veriler, adli bilişim uzmanları tarafından geri getirilebilmektedir.[185]

Bir diğer özellik olarak dijital deliller yaygın ve uluslararası nitelikte olabilmektedirler. Özellikle bilişim sistemleri arasında kurulabilen bağlantılar düşünülünce, dijital delillerin bulunabileceği alanın da ne kadar geniş bir yaygınlığa sahip olabileceği öngörülebilmektedir. Nitekim delilin kaynağının yeri, farklı bir ülkenin yetki alanına girmekteyse, delillerin elde edilmesi meselesi de uluslararası bir mesele haline gelecektir ki bu gibi durumlar, ülkeleri zorunlu bir şekilde adli yardımlaşmaya yönlendirecektir. Adli yardımlaşma konusundaki yetersiz düzenlemeler ise delillerin alışverişi konusunda olumsuz sonuçlar doğuracaktır.[186] Dijital delillerin uluslararası niteliği ve geniş bir alana yayılmış olabileceği gerçeği, bu

[183] Casey, *Digital Evidence,* 26; Chaikin, "Network investigations," 242; Zuev, "Traditional Values of Criminal Procedure," 421; Değirmenci, *Sayısal Delil,* 133; Sarsikoğlu, "Elektronik Delil (E-Delil) Kavramı," 521; Arslan, "Dijital Delil ve İletişimin Denetlenmesi," 194; Taşdemir, "Ceza Adaletini Dijitalleştirmek," 49- 50; Başlar, "Elektronik Delil," 1656- 1657; Değirmenci, "Bilgi Toplumunun Delil Türü," 21; Afandak, "Ceza Muhakemesinde Dijital Deliller," 1.

[184] Nikolaus Forgó, v.d., "Privacy Protection in Exchanging Electronic Evidence in Europe," *Law, Governance and Technology Series,* ed. Maria Angela Biasiotti, v.d., vol. 39, Cham, Switzerland: Springer, (2018): 258; Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj)," 61. Değirmenci, "Bilgi Toplumunun Delil Türü," 21- 22.

[185] Casey, *Digital Evidence,* 26; Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj)," 61; Değirmenci, "Bilgi Toplumunun Delil Türü," 21- 22; Afandak, "Ceza Muhakemesinde Dijital Deliller," 43.

[186] Kaynakçıoğlu, "Dijital Deliller," 40.

tür delillere yönelik gerçekleştirilen hukuki düzenlemelerin, uluslararası düzeyde ve yeknesak bir şekilde kaleme alınması gerekliliğini bizlere göstermektedir.[187]

Ek olarak dijital delilin, özelliklerinden birisi de bilimselliğidir. Dijital delil, bilimsel yöntemlerle elde edilmiş olmalıdır. Bilimsel yöntemi, fark edilir ve kabul edilebilir kılan özellik ise kullanmış olduğu yöntembilim veya metodolojidir. Dijital delilin elde edildiği metodolojinin doğru ve ilgili bilim topluluğu tarafından ortak kabul gören geçerli bir yöntem olması, delilin bilimselliği bakımından şarttır. Bu bağlamda bilimsel yöntemin gözlem, nesnellik, eleştiriye açıklık, tekrarlanabilirlik ve yenileme gibi özelliklere sahip olması gerektiği söylenebilecektir.[188]

Bilimselliğin önemli bir yönü, delil elde etmede kullanılan yöntemin, bağımsız bir şekilde doğrulanabilmesi adına herhangi bir deney veya gözlem aracılığıyla tekrarlanabilmesidir. Bu bakımdan dijital delillerin elde edilmesinde kullanılan bilimsel yöntemlerin doğruluğunun kanıtlanması bakımından elde edilen sonuçlar, başka uzmanlar tarafından da doğrulanabilmeli ve sonuçlar aynı bilimsel yöntem kullanılarak tekrardan elde edilebilmelidir. Bu bakımdan delilin elde edilmesi sırasında atılan adımların ayrıntılı bir şekilde belgelenmesi önem arz etmektedir.[189]

Delilin taşıması gereken özelliklerden olan akılcılık ile delilin bilimsel yöntemle elde edilişi arasında da sıkı bir ilişki bulunmaktadır. Öyle ki hakimler, hükmünü varsayımlar veya ilmi değeri olmayan raporlar üzerine inşa edemeyeceklerdir.[190]

İleride daha ayrıntılı bir şekilde değinmekle birlikte yine de kısaca bahsedecek olursak dijital delillerin bilimselliği konusunda ABD eyaletlerinin çoğunda, bilimsel deliller, *Daubert v. Merrell Dow Pharmaceuticals, Inc.*'kararında (1993)[191] geliştirilen dört kriter kullanılarak değerlendirilmektedir. Bu kriterler aşağıdaki gibidir:[192]

---

[187] Kaynakçıoğlu, "Dijital Deliller," 61.
[188] Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj)," 62- 63; Sarsikoğlu, "Elektronik Delil (E-Delil) Kavramı," 507
[189] Casey, *Digital Evidence,* 25.
[190] CGK., E. 1993/79 K. 1993/108 T. 19.04.1993.
[191] Daubert v. Merrell Dow Pharm., Inc., 43 F.3d 1311 (9th Cir. 1995).
[192] Casey, *Digital Evidence,* 73; Eric Van Buskirk and Vincent T. Liu, "Digital Evidence: Challenging the Presumption of Reliability," *Journal of Digital Forensic Practice*, vol. 1 (2006): 23; Erin E. Kenneally, "Gatekeeping out of the Box: Open Source Software as a Mechanism to Assess Reliability for Digital Evidence," *Virginia Journal of Law & Technology*, vol. 6, no. 3 (2001): 8; Ryan and Shpantzer, "Legal aspects of digital forensics," 2; Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj)," 65.

- Delilin elde edilmesinde kullanılan teori veya tekniğin test edilip edilemeyeceği (ve test edilip edilmediği).

- Bu teorinin bilinen veya potansiyel hata oranının yüksek olup olmadığı ve tekniğin işleyişini kontrol eden standartların varlığı ve bakımı.

- Bu teori veya tekniğin hakem incelemesine veya yayına tabi tutulup tutulmadığı.

- Bu teori veya tekniğin ilgili bilim camiasında "genel kabul" görüp görmediği.

Bu bağlamda *Daubert* kararı kapsamında, yukarıdaki koşulları sağlamayan bir yöntem ile elde edilen deliller bilimsel delil sayılmayacaklar ve hükme esas alınmayacaklardır.

Son olarak dijital deliller, onları bünyesinde barındıran bilişim sistemlerine fiziksel olarak gerçekleştirilecek müdahaleler neticesinde de bozulup, değişikliğe uğrayabileceklerdir. Dijital delil içeren cihazlar zamanla veya ateşe, suya, jet yakıtına ve zehirli kimyasallara maruz kaldığında bozulabilmektedir.[193] Özellikle birazdan bahsi geçecek, USB bellekler ve artık günümüzde bulut bilişimin gelişmesiyle beraber kullanımları yavaş yavaş sonlanan DVD bellekler gibi depolama birimleri, hassasiyetleri nedeniyle paketleme, taşıma veya muhafaza edilme aşamalarında yapılan yanlışlar sonucu dış etkenlerden gelebilecek manyetik etkiye maruz kalma sonucu veya ortam sıcaklığındaki keskin değişimler sebebiyle zarar görebilir ve bünyelerinde barındırdıkları verileri kaybedebilirler. Bu gibi etkilerin ortadan kaldırılması veya en aza indirgenebilmesi adına; faraday çantası, antistatik baloncuklu delil zarfları ve kâğıt kaplı antistatik delil zarfları gibi bazı ekipmanların kullanılması suretiyle özel önlemler alınması gerekecektir.[194]

1.2. Dijital Delillerin Türleri ve Kaynakları

Dijital deliller, ilgili bilişim sisteminin kullanıcısı tarafından, bizzat bilişim sistemi tarafından yahut hem kullanıcı hem de bilişim sistemi tarafından oluşturulabilirler. Bunun dışında adli bilişim uzmanlarınca incelenecekleri aşamada şifrelenmiş, gizlenmiş yahut silinmiş durumda bulunabilirler.

---

[193] Casey, *Digital Evidence,* 27.

[194] Önel ve Irmak, "Dijital delillerin windows işletim sistemi üzerinde incelenmesi," 1190; Başlar, "Elektronik Delilin Toplanması," 100.

1.2.1. Oluşturulma şekilleri bakımından dijital deliller

Oluşturulma şekli bakımından bir dijital delil, ilgili bilişim sisteminin kullanıcısı tarafından, bizzat bilişim sistemi tarafından yahut hem kullanıcı hem de bilişim sistemi tarafından oluşturulabilir. Kısacan incelenecek olursa;

Bilişim sistemi kullanıcısı tarafından oluşturulan deliller, iki insan arasındaki etkileşim neticesinde oluşabileceği gibi, bilişim sistemi kullanıcısının, bilişim sistemine verdiği bir komut neticesinde de oluşabilir. İkinci olarak bizzat bilişim sistemi tarafından oluşturulan dijital deliller, bir yazılımın çıktısı niteliğindedir. Öyle ki bu çıktının oluşturulmasında bir insanın verdiği bir komut veya herhangi başka bir müdahale söz konusu değildir. Üçüncü ve son olarak hem kullanıcı hem de bilişim sistemi tarafından oluşturulan deliller, kullanıcının bilişim sistemi üzerinde gerçekleştirdiği bir girdinin, çeşitli süreçlerden geçmesi neticesinde oluşturulur ve sonrasında dijital olarak ilgili bilişim sisteminde saklanır. Son aşamada saklanan bu veri hem kullanıcı hem de bilişim sistemi tarafından oluşturulan delil niteliğinde olacaktır.[195]

1.2.2. Bulundukları durum bakımından dijital deliller

1.2.2.1. Şifrelenmiş dijital deliller

Güçlü şifrelemenin e-ticaret ve benzeri faaliyetler bakımından son derece önemli olduğunu ve gizliliği korumak için önemli bir araç olduğunu kabul etmek gerekir.[196] Ancak anonim kalma ve şifreleme hizmetlerinin ve araçlarının yasa dışı amaçlarla kötüye kullanımı, dijital delil ve suç istihbaratı toplama bağlamında kolluk kuvvetleri açısından suçun tespiti, soruşturulması ve kovuşturulması bakımından ciddi bir engel teşkil etmektedir.[197]

Dijital deliller aranırken karşılaşılan en büyük engellerden ikisi parola koruması ve kriptografidir.[198] Güçlü şifreleme sistemleri mevcuttur ve bunları satın almak veya indirmek isteyen herkes tarafından ücretsiz olarak kullanılabilmektedir.

---

[195] Değirmenci, *Sayısal Delil,* 141.
[196] Jasmin Ćosić, Miroslav Bača, "(Im)proving chain of custody and digital evidence integrity with time stamp," *The 33rd International Convention MIPRO* (2010) 1227; Leacock, "Search and Seizure of Digital Evidence," 224.
[197] Drewer and Ellermann, "The Online Environment as a Challenge," 144.
[198] Casey, *Digital Evidence,* 458.

Sonuç olarak, bazı suçlular faaliyetlerini gizlemek için şifreleme kullanmayı tercih etmektedirler.[199]

Parola koruması, genellikle üstesinden gelinmesi daha kolay olan bir zorluktur. Bir adli bilişim uzmanının, analiz ettiği bir bilgisayarda bulunan dosyalar üzerindeki parola korumasının tek tek üstesinden gelmesi genel olarak kabul edilebilir olmakla birlikte farklı dosya türlerinde bulunan parolaları elde etmek, çözmek veya tahmin etmek için çeşitli araçlar mevcuttur.[200]

Kriptografi orijinal verilerin veya mesajın, yetkisiz hiç kimsenin orijinal içeriği görememesi adına çözülemeyecek veya çözümünü zorlaştıracak şekilde karıştırılmasıdır.[201,202] Başka bir ifadeyle kriptografi, okunabilir bir dijital nesnenin (düz metin) matematiksel bir işlev kullanılarak okunamaz bir dijital nesneye (şifreli metin) dönüştürülmesi işlemidir.[203]

Kriptografi, bilgi kodlamanın çeşitli yöntemleri için genel bir terimdir. Kavramsal olarak, kriptografi verileri bir anahtarla kilitler ve yalnızca uygun anahtara sahip kişiler bu verilerin kilidini açabilir.[204] Bu anahtar pek çok biçimde olabilir. Örneğin kriptografi bilgisi gerektiren ve ancak öyle bulunabilen bir şifre veya verilerin kodunu çözmek için gereken gizli bir kelime, cümle veya sayı veya şifreleyen kişinin fiziksel özellikleri (parmak izi gibi) bir anahtar olabilir.[205]

Anahtarlar güçlü şifreleme şemaları söz konusu olduğunda karşımıza çıkmaktadır. Buna karşılık basit, anahtarsız kodlama sistemleri de vardır. Örneğin, ROT13, düz metin mesajındaki her bir harfi, alfabede 13 harf daha uzakta olan harfle değiştiren basit bir koddur. Böylece a n olur, b o olur, vb.[206,207]

---

[199] Marshall, *Digital Forensics,* 79.
[200] Casey, *Digital Evidence,* 458.
[201] Marshall, *Digital Forensics,* 79; Daniel J. Ryan and Gal Shpantzer, "Legal aspects of digital forensics," *Proceedings: Forensics Workshop,* (2002): 5.
[202] Bazı ülkelerde, şüphelilerin şifrelerini açıklamaya zorlanabilecekleri "anahtar ifşa düzenlemeleri" vardır. Şifresini vermeyi reddeden kişi, sırf şifresini açıklamadığı için suçlanabilmektedir. İngiltere ve Avustralya bu uygulamanın en belirgin örneklerindendir. Bkz. Drewer and Ellermann, "The Online Environment as a Challenge," 144.
[203] Casey, *Digital Evidence,* 458.
[204] Ćosić and Bača, "Chain of Custody," 1227.
[205] Marshall, *Digital Forensics,* 79- 80.
[206] Casey, *Digital Evidence,* 458.
[207] Örneğin, bir uyuşturucu satıcısı, uyuşturucuyu satacağı kişiye, "Mallar hazır. Ne kadar istiyorsun?" cümlesini, ROT 13 koduyla şifreleyerek gönderirse ulaştıracağı mesaj "Znyyne unmıe. Ar xnqne vfgvlbefha?" şeklinde olacaktır. Ek olarak ROT 13 kodu ve benzer kodlarla ilgili olarak internetten kolaylıkla erişilebilen mesaj dönüştürücü sitelerin bulunduğunu belirtmemiz gerekir.

Kısaca bir mesajı şifrelemek için kullanılan anahtarın aynısı, aynı zamanda şifresini çözmek için de kullanılır. Şifrelemeyi bir kilit olarak düşünürsek, verileri kilitleyen anahtarın aynısı onu açmak için kullanılır ve anahtar olmadan verilerin kilidini açmak çok zordur.

1.2.2.2. Gizlenmiş dijital deliller

Bir dosyayı gizlemeye yönelik en basit yaklaşım, adını adli bilişim uzmanlarını yanıltacak şekilde değiştirmektir. Örneğin, hukuka aykırı içerik barındıran ve jpg formatında olan bir fotoğrafın adının ve formatının "hukukaaykırıfotoğraf.jpg" den "sysup32.exe"ye çevrilmesi, adli bilişim konusunda bilgisiz olan bir kişiyi, o dosyanın sıradan bir sistem dosyası olduğu düşüncesine yönlendirebilir. Bu gizleme tekniğinin üstesinden gelmek için adli bilişim uzmanları, bir dosyanın ne içerebileceğini belirlerken yalnızca dosya adlarına güvenmezler, dosya başlığını (diğer adıyla dosya imzası) kontrol etmek için daha fazla araştırma yaparlar.[208]

Dosyanın adının değiştirilmesinden farklı olarak bir diğer gizleme tekniği, dijital fotoğrafları Microsoft Powerpoint dosyasına gömmek gibi suç teşkil eden verileri zararsız bir dosyada gizlemeyi içerir. Bir bilgisayarda depolanan fotoğrafları arayan bir adli bilişim uzmanı, Powerpoint dosyalarını gözden kaçırabilir. Bunlar gibi bir dosya içindeki verileri gizlemek için daha karmaşık yöntemler mevcuttur ve bu yöntemler genel olarak steganografi (steganography) olarak adlandırılır. Steganografinin şifrelemeye göre en büyük avantajı, incelemeyi yapan kişinin, önündeki dosyanın içinde önemli bilgiler saklandığını bilmiyor oluşu sebebiyle fark edememesi ve es geçebilmesidir.[209] Steganografi şöyle bir örnekle açıklanabilir. Bir insanın saçı kazıtılır ve kafasının üzerine bir harita dövmesi yapılır. Sonrasında saç uzayınca harita gizlenmiş olur. Bu yöntemle gizlenen bilgiyi, yalnızca nereye bakması gerektiğini bilen kişiler bulabilecektir.[210]

Bir dosyayı diğerinin içine gizlemek için kullanılan "Invisible Secrets"[211] gibi bazı yazılımlar, sabit diskte yer alan düzinelerce görünüşte zararsız video ve fotoğrafı

[208] Casey, *Digital Evidence,* 456.
[209] Casey, *Digital Evidence,* 456; Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 147.
[210] Marshall, *Digital Forensics,* 81.
[211] Invisible Secrets, kullanıcısına; dosya şifreleme yazılımı, hassas verilerin ve doya içeriklerinin güvenli bir şekilde gizlenmesi, herhangi bir uygulamanın güvenli bir şekilde parola ile korunması, askeri güçte şifreleme algoritmaları sunulması ve e-posta şifreleme çeşitli hizmetleri sunan ve günümüzde

gizlemek için kullanılabilirler. Bu tür gömülü verileri bulmak, kurtarmak ve inceleyebilmek, adli bilişimde günümüzde hala devam eden zorluklardandır. Her ne kadar bazı steganografik teknikleri tespit etmek için çeşitli araçlar mevcut olsa da bunlar bilinen yöntemlerle sınırlıdır. Bu sebeple yeni ve yaratıcı veri saklama tekniklerinin kullanımı konusunda adli bilişim uzmanları tetikte olmalılardır.[212]

Verileri gizlemede kullanılan bir diğer yöntem, *"soğan yönlendirmesi (onion routing/ onion skin routing)"* yöntemidir. Onion Routing, internette gezinme, güvenli kabuk[213] ve anında mesajlaşma gibi uygulamaları anonim hale getirmek için tasarlanmış bir ağdır.[214] Bu yöntemde her biri kendi şifreleme ve şifre çözme anahtarına sahip olan düğümlerin bulunduğu katmanlar vardır (soğan katmanları gibi).[215] Başlangıç ve hedef katman arasında yer alan bu aktarım düğümleri yalnızca kendisine mesaj gönderen ve kendisinin mesaj gönderdiği düğümlerin farkındadır. Bu sebeple aktarma düğümleri, kendisine gelen mesajı, o mesaj bir başka düğümün anahtarıyla şifrelendiği için okuyamaz ancak kendisinden sonra gelen düğüme gönderebilir. Başka bir ifadeyle yalnızca hedef düğüm, ilgili mesajın şifresini çözebilecek anahtara sahiptir.[216] Sonuç olarak kendilerine gelen şifre anahtarına sahip aktarım düğümleri, mesajı diğer katmana yeni şifresiyle ve anahtarı ile birlikte gönderir. Her katmanda çözülen düğümler sonucunda gönderilmek istenen mesaj, en son hedefine ulaşır ve hedefte bulunan anahtar sayesinde şifre çözülür ve gizlenen veriye ulaşılır.[217]

1.2.2.3. Silinmiş veriler

Sabit disklerde gerçekleştirilen silme işlemleri farklı boyutlarda gerçekleşir. Kullanıcı tarafından gerçekleştirilen basit silme (delete) işleminde dosyaların sadece dosya sistemindeki adres ve uzunluk bilgileri silinmektedir. Kalıcı silme (wipe) işleminde ise verilerin sabit disk üzerinde bulunan tüm değerleri 0 yapılmaktadır.

---

kolayca erişilebilen bir yazılımdır. İlgili yazılım hakkında daha detaylı bilgi için bkz. https://www.east-tec.com/invisiblesecrets/ , son erişim. 25.04.2022.

[212] Casey, *Digital Evidence*, 457.

[213] "Güvenli Kabuk (*Secure Shell)"*, ağ hizmetlerinin kullanımı sırasında, güvenli olmayan bir ağ üzerinde, güvenli bir şekilde uzaktan oturum açmak için kullanılan, şifreli katmanlardan oluşan bir protokoldür., bkz., Tatu Ylönen and Chris Lonvick, "The Secure Shell (SSH) Protocol Architecture," *RFC* 4251 (2006): 3.

[214] Roger Dingledine, Nick Mathewson and Paul Syverson, "Tor: The Second-Generation Onion Router," *Naval Research Lab*, Washington DC (2004): 1.

[215] Marshall, *Digital Forensics*, 106.

[216] Marshall, *Digital Forensics*, 106.

[217] Dingledine, Mathewson and Syverson, "Tor: The Second-Generation," 1.

Başka bir ifadeyle basit silme işlemi neticesinde işletim sistemi, sabit disk üzerinde herhangi bir dosya olmadığını gösterir. Oysa dosyalar yerinde durmaktadır. Buna karşılık kalıcı silme işleminde sabit disk üzerindeki ger sektör 0 bilgisi ile işaretleneceği için sabit disk adli bilişim anlamında steril hale getirilmiş olacaktır.[218] İşte silinen verilerin elde edilmesi hususu, üzerinde basit silme işlemi gerçekleştirilen veriler bakımından gündeme gelmektedir.

Bir depolama biriminde üzerine veri yazılmamış ve veri yazılmış fakat sonradan silinmiş ancak hala eski veriden kalıntılar barındıran alanlar, boş alan olarak adlandırılır. Bir dosya silindiğinde, o dosyanın işletim sistemi üzerindeki durumu, "silinmiş" şeklinde güncellenir ve bu şekilde güncellenen alan üzerine yeni bir dosya yazılmadığı müddetçe eski veriler barınmaya devam eder. Eski verilerin bulunduğu alan, olası bir yeniden kullanım durumu için işaretlenir.[219] Devamında ilgili diske yeni bir dosya yüklenir ancak yüklenen dosya tüm sektörü kaplamazsa, eski dosyanın bir kısmı boş alanda kalmaya devam edebilir.[220] Bu durumda dosyanın bir kısmı silindikten ve kısmen üzerine yazıldıktan çok daha sonra bile veriler tekrardan elde edilebileceklerdir.[221] Buna karşılık tekrardan elde edilen veriler önceden "silinmiş" olarak işaretlendikleri için ilgili dosyanın önceden barındırdığı üst verilere (zaman-tarih damgası gibi) artık ulaşılamayacaktır.[222]

1.2.3. Dijital delillerin kaynakları

Dijital deliller, gelişen teknoloji ve küreselleşme nedeniyle, doğası gereği dünyanın herhangi bir yerinde bulunabilir, işlenebilir veya saklanabilirler.[223]

Bu başlıkta bünyesinde dijital delil barındırabilecek ve adli bilişim incelemesine konu olabilecek çeşitli cihazlar, bunların çalışma prensipleri ve yaratabilecekleri zorluklar ele alınmaya çalışılmıştır. Ancak şu husus da belirtilmelidir ki dijital delil barındıran cihazlar aşağıda sayılanlarla sınırlı değildir. Sayıları

---

[218] Değirmenci, *Sayısal Delil,* 258; Say, "Bilişim Suçlarında Elde Edilen Deliller," 76.
[219] Marshall, *Digital Forensics,* 51.
[220] Burada kesinlikte ziyade ihtimalden bahsedilmesinin sebebi, depolama cihazına yüklenen bir verinin, depolama cihazının hangi birimlerine yükleneceği konusunda kullanıcının bir yetkisinin olmaması; işlemin tamamen dosya sistemi tarafından gerçekleştirilmesi sebebiyledir. Bu sebeple yeni yüklenen veri, eski verinin tamamen üzerine yazılabileceği gibi, yalnızca bir kısmı da eski verinin üzerine yazılabilecektir. Bu konu hakkında detaylı bilgi ve çeşitli görseller için bkz. Değirmenci, *Sayısal Delil,* 259.
[221] Casey, *Digital Evidence,* 455.
[222] Marshall, *Digital Forensics,* 51.
[223] Mifsud Bonnici, Tudorica and Cannataci, "The European Legal Framework," 190.

teknolojik gelişime bağlı olarak her geçen gün artmakta ve çeşitlenmektedir.[224] Biz burada gündelik hayatta daha çok karşımıza çıkan cihazları değerlendirmeye çalıştık.

1.2.3.1. Bilgisayarlar

Veriler bilgisayarlarda dijital olarak saklanır ve dijital deliller; video görüntüleri, belgeler, resimler, müzik, silinen dosyalar, gizli ve şifreli dosyalar, indirilen öğeler, internet geçmişi, iletişim kayıtları, çeşitli bilgisayar programları, işletim sistemleri şeklinde karşımıza çıkabilirler.[225] Bu deliller bilgisayarların çeşitli bileşenlerinden elde edilebilir. Örneğin, bizzat ekrandan, işletim sisteminden, sabit disk ve bilgisayara bağlı herhangi bir çıkarılabilir depolama aygıtından (USB, harici sabit sürücüler, eski sistemlerde olan diskler vb.) ve bunun gibi birazdan bahsedeceğimiz diğer bileşenlerden dijital deliller elde edilebilecektir.[226]

Bilgisayarların çalışma prensiplerine kısaca değinecek olursak bilgisayarlar, üzerine yüklenen programlar vasıtasıyla çalışabilme, veri girişini sağlayan mekanizmalar vasıtasıyla söz konusu verileri depolama, verileri işleme tabi tutma, verileri bir yere nakletme, söz konusu verilerden bazı sonuçlar çıkarma, aritmetik ve mantık işlem dizileriyle çalışabilme gibi özelliklere sahiplerdir. Bu özellikleri, bilgisayarları diğer makinelerden ayırır. Bilgisayar terimi ile masaüstü, dizüstü bilgisayarlar, cep telefonu ve benzeri özelliklere sahip tüm elektronik araçların ifade edilebileceğini söyleyebiliriz.[227]

Tüm bilgisayarların mimarisi, bir araya getirildiğinde çalışan temel donanım (hardware) ve yazılım (software) bileşenlerinden oluşur ve bu bileşenlerin bir araya gelmesi neticesinde karşımıza çıkan bütün, bir "bilgisayar" olarak anılır. Bu bileşenler şunları içerir: işlemci (programları eylemlere dönüştürür), bellek (bilgi aktif olarak işlenirken bilgileri gerçek zamanlı olarak depolar), kalıcı depolama (bilgileri, programları ve uzun süreli kullanım için diğer talimatları depolar) ve mantık kartları (makinenin iletişimini, girişini ve çıkışını yönetir). Ayrıca klavye gibi bir giriş cihazı

[224] Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 144.
[225] Chaikin, "Network investigations," 243; Arslan, "Hukuk Öğretiminde Adlî Bilişim" 83; Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 144.
[226] Zeigler and Rojas, *Preserving Electronic Evidence for Trial*, 58.
[227] Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 55; Değirmenci, *Sayısal Delil,* 34- 35; Afandak, "Ceza Muhakemesinde Dijital Deliller," 88.

ve monitör veya başka bir ekran gibi görsel bir arayüz aracı ayrıca bilgi çıkışını sağlayan çeşitli donanımlar da bir bilgisayarı oluşturan bileşenlerdendir.[228]

Dijital delillerin elde edilmesi bakımından söz konusu bileşenler önem kazanmaktadır. Zira dijital deliller, bilgisayarın her bileşeninde bulunabilirler. Bununla birlikte her bir bileşende bulunan dijital delillerin ispat bakımından işlevi ve delilin elde edilmesi bakımından söz konusu delile yaklaşım farklı olacaktır.[229]

Şüpheli veya sanığın, mağdurun veya üçüncü bir kişinin kullandığı bilgisayarlar, bir bilişim suçu veya diğer suçlarla ilgili olarak çok çeşitli bilgiyi içerebilirler. Bununla birlikte yürütülen soruşturma kapsamında yapılan incelemelerde çoğu kez şüphelinin bilgisayarı öncelikledirilmektedir ve istatistiksel olarak bakıldığında, bu incelemelerin büyük bir kısmı incelemeye konu suç fiiline yönelik delillerin tespitiyle sonuçlanmaktadır.[230]

Öncelikle, suçlular kurbanlarını internet üzerinden bulduğunda veya hedef aldığında, başka bir ifadeyle bilgisayarlar etkin bir şekilde suçun bir aracı haline getirildiğinde, önemli bilgilere bu bilgisayarlar aracılığıyla ulaşılabilmektedir. Bu gibi durumlarda bilgisayarlar, suçun planlanması ve işlenmesiyle doğrudan ilgili delilleri barındırabilirler. Ek olarak mağdur veya şüpheli tarafından kullanılan İnternet servis sağlayıcılarından alınan veriler, bu kişilerin suç anındaki faaliyetlerini, nerede olduklarını ve kimliklerini belirlemeye de yardımcı olabilirler.[231]

İkinci olarak bir siber saldırı neticesinde güvenliği ihlal edilen bilgisayarlar, genellikle bu saldırının delillerini içeren günlük dosyaları biçiminde kayıtlara sahip olacaktır. Mağdurun bilgisayarında veya suçla bağlantılı diğer bilgisayarlarda, saldırının gerçekleştirildiği bilgisayarın izleri olabilir ve bu izler suçun aydınlatılması adına kullanılacak dijital delillere dönüşebilir. Buna karşılık bilişim sistemine girme (TCK m. 243) suçunun failleri, tespit edilmemek veya sonraki herhangi bir soruşturmayı engellemek için sık sık fiillerinin dijital izlerini değiştirir veya kaldırırlar. Tipik olarak, ağın çeşitli bölümlerine günlük girişleri ekler, değiştirir veya yok ederler. Daha ileri seviye siber suçlular, adli bilişim uzmanlarının yanlışlıkla delilleri

[228] Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 56- 57; Afandak, "Ceza Muhakemesinde Dijital Deliller," 88.
[229] Değirmenci, *Sayısal Delil,* 46.
[230] Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 47.
[231] Casey, *Digital Evidence,* 309.

değiştirmesini veya yok etmesini sağlamak adına çeşitli tuzaklar bile kurabilirler.[232] Bu bağlamda adli bilişim uzmanlarının çok dikkatli olmaları gerekmektedir.

Üçüncü olarak bilgisayarlar, suç ile doğrudan bağlantılı olmasalar bile yahut işlenen suç doğrudan bir bilişim suçu olmasa bile, yararlı bilgiler içerebileceklerdir. Bu bağlamda bilgisayarlar olay yerinin bir uzantısı olarak düşünülebilirler. Bu nedenle bilişim suçları dışındaki suçlarda da hem fiziksel hem de dijital olay yerinin, fiziksel ve dijital potansiyel delil bütünlüğünün sağlanması adına gerçekleştirilecek metodolojik bir çalışma, suçun aydınlatılması konusunda işleri oldukça kolaylaştıracaktır.[233]

Dijital delillerin elde edilmesi bakımından özellikle bilgisayar işletim sistemleri üzerinde yapılacak inceleme sonucunda, delil niteliği taşıyabilecek verilere ulaşılabilecektir. İşletim sistemleri aracılığıyla tüm arama ve dosya işlemlerine, sistem kayıtlarına, çalışan uygulamalara, internet geçmişi ve e-posta dosyaları gibi birçok farklı yapıda bulunan verilere ulaşılabilmektedir. Bu nedenle işletim sistemleri üzerinde adli bilişim incelemeleri ile dijital delil elde edebilme olanağı çok fazladır.[234]

Bunlara ek olarak bilgisayarların kullanımının günümüzde devlet kurumları ve iş hayatında da oldukça yaygın olduğunu söylemek yanlış olmayacaktır. Söz konusu bilgisayarlar, bünyesinde bulunduğu kurum veya şirket ile ilgili önemli bilgileri içerebilmekle birlikte, o şirket veya kurum aleyhine işlenen suçlarda yahut o şirket veya kurumdan bağımsız olarak üçüncü kişilere karşı işlenen suçlarda da araç olarak kullanılabilmekte ve suçun konusunu oluşturabilmektedirler. Bu bağlamda kurum veya şirket bilgisayarlarında yer alan verilerin de birçok suça ilişkin dijital delilleri barındırabileceğini söyleyebiliriz.

1.2.3.1.1. Depolama birimleri

Depolama ortamları birçok biçimde ortaya çıkabilse de sabit disklerin bilgisayarlardaki en zengin dijital delil kaynakları olduklarını söylemek yanlış

[232] Chaikin, "Network investigations," 244.
[233] Casey, *Digital Evidence,* 227.
[234] Bünyamin Önel ve Erdal Irmak, "Adli bilişim ve dijital delillerin windows işletim sistemi üzerinde incelenmesi," *Politeknik Dergisi,* C. 24, S. 3 (2021): 1188.

olmayacaktır.[235] Bir sabit disk, bir kütüphane dolusu bilgiyi saklayabilir ve örneğin dijital kameralar binlerce yüksek çözünürlüklü fotoğrafı saklayabilirler.[236]

Sabit disklerden silinen verilerin tekrardan elde edilebilmesi konusuna yukarıda[237] değinmiştik. Bu bağlamda suç materyallerinin yahut suçla ilgili bilgiler içeren fakat silinen materyallerin, geri getirilmesi aracılığıyla delil olarak elde edilebilmeleri ve muhakeme sürecinde kullanılabilmeleri gündeme gelebilecektir.

Farklı olarak depolama birimleri içerisinde veri bulunabilecek yerlerden birisi de takas alanıdır (*swap space*). İşletim sisteminin ön belleği (RAM) işlenecek verilere yetmediği zaman takas alanı, ram yerine geçer ve bu sayede veri akışı kesintisiz bir şekilde devam eder. Sonradan takas alanında bulunan veriler, ana belleğe geri yüklenir. Kullanıcının bu işlem üzerinde de hiçbir kontrolü olmadığı için, başka herhangi bir nedenle depolama cihazlarına hiç yazılmamış verilerin takas alanında bulunması mümkündür. Bu bağlamda takas alanının, genellikle şifrelenmiş dosyalar ve diğer hassas veriler hakkında iyi bir bilgi kaynağı olduğu belirtilmiştir.[238]

Depolama aygıtlarından veri toplanırken bunların uçuculuklarına ve bilgi kaybı potansiyellerine göre toplanacağı sıra için bazı önceliklendirmeler söz konusudur. Örneğin, bilgisayar korsanlığı (hacking) olasılığından şüphelenilen durumlarda, kötü amaçlı yazılımın (bilgisayar operatörünün bilgisi olmadan kötü niyetli hareket etmesi amaçlanan yazılımlar) olası varlığı için önce bilgisayarın son işlevsel etkinliklerinin bellek bilgilerinin toplanması gerekir. Buna karşılık örneğin E-posta aracılığıyla taciz yahut çocuk pornografisi gibi ihtimallerde, bu bilgilerin toplanması o kadar önemli değildir.[239]

Sabit disklerden farklı olarak bilgisayar ve diğer bilişim sistemleri arasında veri transferi ya da depolama gibi amaçlarla; hafıza kartı, CD-ROM, DVD-ROM ve USB bellek gibi çeşitli taşınabilir aygıtlar da kullanılmaktadır. Bunlar dışında kullanım amaçları farklı olmakla birlikte yine belli bazı dijital verilerin depolanabildiği; fotoğraf

---

[235] Sabit diskler, silindir, baş ve sektör olarak adlandırılan birimlerden oluşur ve bu birimler sabit diskin boyutunu ölçmeye ve içinde yer alan bölümlerin konumlarının belirlenmesine yardımcı olur. Diskler tipik olarak ortak bir eksen üzerinde yer alan birkaç fiziksel plakadan oluşmaktadır. Her plakanın iki tarafında iz adı verilen halkalar bulunmaktadır. Her bir iz de sektör adı verilen bölümlerden oluşmaktadır. Bir sektör diskte yer alan en küçük fiziksel depolama birimidir ve neredeyse 512 bayt boyutundadır. Marcella and Guillossou, *Cyber Forensics,* 130.
[236] Casey, *Digital Evidence,* 32.
[237] Bkz. "1.2.3.3. Silinmiş veriler" başlığı.
[238] Marshall, *Digital Forensics,* 52.
[239] Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 58.

makineleri, video kameralar, taşınabilir müzik çalarlar, tarayıcılar, fotokopi makineleri, faks, yazıcı ve cep telefonları da dijital delillerin elde edilmesi bakımından önem arz etmektedirler.[240]

1.2.3.2. E- postalar

E- postaların temelinde "Basit Posta Aktarım Protokolü" (Simple Mail Transfer Protocol- SMTP) yer alır ve e- mailler, gönderilme ve elde edilme olmak üzere iki şekilde hareket ederler.[241]

E- posta, belirli iki nokta arasında doğrusal bir şekilde hareket etmez. Çeşitli aktarım noktalarından geçerek hedefine ulaşır. Her aktarım noktasında da mesajın en üstüne fazladan bir bilgi satırı eklenir ve bu satırda e- postanın nereden alındığı, alındığı zamanı ve nereye gittiğiyle ilgili bilgiler yer alır. Bu şekilde "Basit Posta Aktarım Protokolü" üzerinden iletilen her e-posta, İnternet'teki yolculuğunun tüm ayrıntılarını içeren bir dizi "başlık" alır.[242]

E- posta aracılığıyla işlenen suçlar bakımından yahut e- postalar aracılığıyla taşınan suç materyallerinin elde edilmesi bakımından, e- postaların gönderildiği ve elde edildiği noktaların ve bunlar arasında yer alan aktarım noktalarının takip edilmesi büyük önem arz etmektedir.

1.2.3.3. Mobil cihazlar

Günümüzde cep telefonları gibi mobil cihazların, kişilerce sürekli yanlarında taşınması ve kişilerin en mahrem anlarına dahi tanıklık ediyor oluşu diğer dijital materyallere göre suça konu bulguları taşıma ihtimalini daha da artırmaktadır.[243]

Günümüzün mobil odaklı bilgi işlem ve iletişim dünyasında, akıllı telefonlar, ile bilgisayarlar arasında neredeyse hiç fark kalmamıştır. Akıllı telefonlar ve tabletlerde depolama bakımından yerleşik bellekler ve ek depolama birimleri olarak SD (secure digital) kartlar veya USB (universal serial bus) flash sürücü aygıtları kullanılabilmektedir. Bu depolama seviyesi ile, kişilerin cebindeki küçük mobil cihazların hafızasında önemli bilgiler saklanabilir.[244]

---

[240] Afandak, "Ceza Muhakemesinde Dijital Deliller," 97.
[241] Marshall, *Digital Forensics,* 101.
[242] Marshall, *Digital Forensics,* 101.
[243] Yılmaz ve Çakır, "Mobil Cihaz Adli Bilişimi Süreçleri," 25.
[244] Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 69- 70.

Bu cihazlardaki işletim sistemleri ve uygulamalar genellikle son derece gelişmiştir ve veri çıkarma ve yorumlama genel olarak bilgisayarlardan biraz daha zorludur.[245] Bu bağlamda mobil cihazlarda şifreleme ve cihaz anahtarının olması gibi durumlar, dijital veriye normal yöntemlerle ulaşılamama sorununu gündeme getirmektedir. Bu sebeple bazı ileri düzey ek tekniklerin uygulanmasını gerekebilmektedir.[246]

Çoğu cep telefonu ve tablet işletim sistemi (Android ve Apple'ın iOS'u pazarda en önde gelen iki işletim sistemidir), cihaz işlemlerini optimize etmek için bellek alanının veri bölümünü yeniden düzenleyen veya silen yerleşik rutinlere sahiptir. Bu rutinler aracılığıyla, yeni veriler için boş alan sağlamak adına veriler gerektiği anda kendiliğinden yeniden düzenlenir veya silinir. Cihazın kullanıcısı ne kadar meşgulse, veriler o kadar hızlı yeniden düzenlenir veya silinir. Bu işlevsellik nedeniyle cihazda olabilecek ilgili verilerin derhal toplanabilmesi için cihaz elde edilirken adım adım fakat hızlı bir şekilde hareket edilmesi gerekmektedir.[247]

Ek olarak, mobil cihazlardan veri toplama süreci, geleneksel bir bilgisayar sabit diskinden veri toplama süreci gibi değildir. Mobil cihazdaki veriler canlı, gerçek zamanlı olarak toplanır. Bir başka deyişle geleneksel adli bilişim yöntemlerinde olduğu gibi bilgisayarın sabit diskinin, delil toplama cihazından izole edilmesi amacıyla bir yazma engelleyiciye (write blocker) bağlanması ve sonrasında birebir kopyalanması[248] gibi bir işlem yerine dijital olarak depolanan bilgiler, telefonun işletim sistemine komutlar gönderilerek veri toplama cihaz çalışırken elde edilir.[249]

Farklı olarak mobil cihazlardan servis sağlayıcılara ait fatura bilgileri ya da arama detay bilgilerinin de elde edilmesi mümkündür. Arama detay bilgilerinin çözümlenmesi ile kişinin hangi zamanda kimleri aradığı, bu kimselerle ne kadar süre iletişimde bulunduğu gibi, incelemeye konu suç fiilinin tespiti bakımından çok önemli ve delil niteliği taşıyabilecek bilgiler de elde edilebilmektedir.[250]

---

[245] Marshall, *Digital Forensics,* 109.
[246] Bu ileri düzey tekniklerden biri olan chip-off rooting, yöntemi, sim kart üzerindeki kalıcı veri tutan hafıza çipinin sökülerek ikili değer (binary) düzeyinde veriye ulaşılmasıdır. Barındırdığı tehlikeler sebebiyle yalnızca gerekli olduğu zamanlarda ve işin uzmanı kişilerce uygulanması gerekir. Başlar, "Adli Bilişim," 58; Yılmaz ve Çakır, "Mobil Cihaz Adli Bilişimi Süreçleri," 30.
[247] Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 70.
[248] Bu yöntem hakkında detaylı bilgiye ileride yer verilecektir. Bkz. "Üçüncü Bölüm, 3.3.1.1. Birebir Kopya" başlığı.
[249] Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 70.
[250] Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 48.

Mobil cihazlar, bir suçla ilgili iletişim bilgilerinin yanı sıra ses veya video kayıtları da içerebilirler. Mobil cihazlar ayrıca önemli zamanlarda mağdurların ve şüphelilerin konumlarının tespit edilebilmesi bakımından da bilgi da sağlayabilirler.[251]

Ek olarak mobil cihazlardan, arama günlükleri, mesaj günlükleri, yerleşik GPS çiplerinden gelen konum bilgileri, harita yazılımından gelen navigasyon verileri ve mobil uygulamalardan toplanan veriler toplanabilir ve bu veriler suçla bağlantıları noktasında dijital delil olarak elde edilebilirler.[252]

Bu bağlamda mobil cihazı oluşturan bileşenlerden elde edilebilecek dijital delillere kısaca değinmek yerinde olacaktır.

1.2.3.3.1. Çıkarılabilir bellek

Çıkarılabilir bellekler mobil cihazlar arasında taşınacak şekilde tasarlandığından için güç kesildiğinde veri kaybetmezler ve inceleme bakımından sabit diskler gibi düşünülebilirler.[253]

1.2.3.3.2. Dahili bellek

Bir mobil cihazın dahili belleğinin iki işlevi vardır. Hem programın yürütülmesi için aygıtın birincil belleği olarak çalışır hem de verilerin depolanabilmesi için bir dosya sistemi olarak çalışır. Dahili belleğin nasıl programlandığına bağlı olarak, hafızada bu işlemler için ayrılmış farklı alanlar olabilir.[254]

Birçok mobil cihaz, bir bilgisayara bağlandığında iki farklı çalışma modu sağlar: biri kişisel verilerin (örneğin günlükler, e-posta, notlar vb.) senkronizasyonu ve diğeri veri dosyalarının aktarımıdır. Bu modlardan hiçbiri dahili bellek içeriğini tam olarak göstermez ve bu sebeple cihazı sökmek ve özel tanılama ekipmanına bağlamak veya cihaza bir veri kurtarma programı yüklemek gerekebilir. Ancak cihaza bir program yükleme, cihazın durumunu değiştirebilecektir. Bu sebeple bu işlem yapacak kişinin, cihaza program yükleme ve program üzerinden inceleme yapma hususunu ve bu işlemlerin cihazı nasıl etkilediğini açıklayabilecek kalifiyede olması gerekecektir.[255]

---

[251] Casey, *Digital Evidence,* 310.
[252] Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 70.
[253] Marshall, *Digital Forensics,* 111.
[254] Marshall, *Digital Forensics,* 111.
[255] Marshall, *Digital Forensics,* 112.

1.2.3.3.3. SIM kartlar

Bu kartlar, küçük miktarlarda bellek ve/veya işleme kapasitesi bulunan ve "akıllı" kart ailesinin parçası olan kartlardır.[256] SIM kart, cep telefonu şebekesine erişime izin vermek için bir telefon ile bir aboneyi ilişkilendirir. Şebekenin çağrı verilerinin nereye yönlendirileceğini bilmesi için, SIM'e özgü ve üretim sırasında programlanmış hem mantıksal hem de fiziksel bir adres gerekir. Mantıksal adres, telefon numarasını, "Uluslararası Mobil Abone Kimliği" (International mobile subscriber identity- IMSI) ile eşleştiren ve bir veri tabanı aracılığıyla SIM ile ilişkilendirilen telefon numarasıdır. Sonuç olarak bir aramayı bağlamak için şebeke, çevrilen telefon numarasını Uluslararası Mobil Abone Kimliği ile eşleştirir ve arama, Uluslararası Mobil Abone Kimliğinin geçerli konumuna yönlendirilir.[257]

Son olarak SIM kartlarda, SIM kart abonesi için hangi ağ hizmetlerinin ve kısıtlamaların yürürlükte olduğunu belirlemek için ağ sağlayıcısına ayrılmış olan operatör verisi alanı; telefon rehberi, kısa kodlu arama numaraları, yapılan ve alınan aramalar ve gönderilen ve alınan SMS (metin) mesajları gibi SIM kartı abonesi tarafından yaratılan kişisel verileri tutan küçük depolama alanları bulunmaktadır.[258]

1.2.3.3.4. Hücre bölgesi analizi

Cep telefonlarını içeren bir başka verimli araştırma alanı, hücre bölgesi analizidir. Hücre bölgesi analizi, cep telefonu şebekesinin özelliklerine dayalı olarak bir telefonun bulunduğu veya kullanıldığı konumu belirlemede kullanılır.[259]

1.2.3.3.5. Küresel konumlandırma sistemi

Küresel konumlandırma sistemi (Global Positioning System- GPS) dünyanın etrafındaki yörüngede bulunan bir uydu ağını kullanır. Her uydunun benzersiz bir kimliği ve doğru bir saatle birleştirilmiş iyi tanımlanmış bir yörüngede izlediği bir yol vardır. Bu uydular, geçerli saat ve yörüngeleri hakkında bilgi yayınlarlar. Bir GPS alıcısı, dünyanın herhangi bir noktasından, görünür uyduları belirler ve uydular

[256] Marshall, *Digital Forensics,* 113.
[257] Marshall, *Digital Forensics,* 114.
[258] Marshall, *Digital Forensics,* 114.
[259] Marshall, *Digital Forensics,* 115.

tarafından gönderilen verilere dayalı bir hesaplama yaparak, dünyanın yüzeyinin tam olarak neresinde olduğunu hesaplar.[260]

1.2.3.3.6. Mobil ağlar

Mobil ağlar, özellikle GSM ağları, ilk zamanlarda sabit ağlarla aynı güvenlik protokollerine sahip olacak şekilde geliştirilmiştir. Bu husus ise bu tür ağları, üçüncü kişilerin erişimine karşı savunmasız bırakmıştır. Ancak bu zayıflık, elde edilmesi zor olabilecek delillere daha rahat ulaşabilme konusunda kolluk kuvvetlerine kolaylık sağlamıştır.[261]

Uluslararası mobil abone kimlik yakalayıcı (IMSI Catchers) araçlar aracılığıyla kolluk kuvvetleri, aracın menzili içerisinde bulunan şüpheliler hakkında bilgi toplayabilmekte, trafik bilgilerini inceleyebilmektedirler. Hatta bazı gelişmiş kimlik yakalayıcılar, telefon görüşmelerini, kısa mesaj servislerini ve veri servislerini gizlice dinleyebilmektedirler.[262]

Konu ile ilgili detaylı bilgiye ileride yer verilecektir.[263]

1.2.3.4. İnternet ve ağlar

İnternet, dünyayı çevreleyen bilgisayar ağlarını ve kurumsal bilgisayar sistemlerini birbirlerine bağlayan elektronik iletişim ağını ifade etmek için kullanılan bir terimdir.[264]

İnternet ağlarının dinamik ve dağıtılmış doğası, soruşturmaya konu suçla ilgili tüm dijital delilleri bulmayı ve toplamayı zorlaştırır. Veriler bir grup bitişik binaya, birkaç şehre, eyalete ve hatta ülkeye yayılabilir. Bulut hizmetleriyle (örneğin Google Drive bulut hizmeti) uğraşırken, verilerin konumu daha da belirsiz olabilir. En küçük ağlar dışında, belirli bir anda tüm ağın anlık görüntüsünü almak mümkün değildir. Ağ trafiği geçicidir ve aktarım sırasında yakalanması gerekir. Ağ trafiği yakalandıktan sonra yalnızca kopyalar kalır ve orijinal veriler karşılaştırma için kullanılamaz.

---

[260] Marshall, *Digital Forensics,* 116.
[261] Neil Redmond, v.d., "Long Term Evolution Network Security and Real-Time Data Extraction," *Cyber And Digital Forensic Investigations*, Springer International Publishing, New York, USA, (2020): 204.
[262] Redmond, v.d., "Network Security and Real-Time Data Extraction," 205.
[263] Bkz. Bölüm 2, "2.1.2.2. İletişimin Tespiti, Dinlenmesi ve Kayda Alınması (Cmk M. 135)" başlığı.
[264] Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 57.

Toplama işlemi sırasında kaybedilen veri miktarı belgelenebilir ancak kaybolan deliller geri alınamaz.[265]

Bilgisayar sistemleri internetin ortaya çıkmasıyla birlikte farklı bir boyut kazanmıştır. Başlangıçta sadece veri depolama ve bazı günlük işlerin yapılması gibi işlerde kullanılan bilgisayarlar, internetin tüm dünya üzerinde önemli bir ağ kurması ile dünyanın her tarafındaki insanlarla iletişim kurulmasına olanak sağlamakla birlikte ihtiyaç duyulan bilgiye daha hızlı ve çok fazla çaba sarf etmeden ulaşılması imkanını doğurmuştur. [266]

Siber suçlular, İnternet ve uluslararası kapsamı olan ağ iletişimlerinden oldukça yararlanmaktadırlar. Bu bağlamda farklı ülkelerden siber saldırılar düzenlerler, suçlarının delillerini farklı ülkelerde saklarlar ve uluslararası kanunlarda yer alan iş birliğine yönelik düzenlemelerdeki zayıflıklardan yararlanırlar.[267]

Ağlar, birlikte çalışmak üzere birbirine bağlı olan bilgisayar gruplarını kapsamaktadır. Büyük organizasyonların karmaşık ağlarından evlerde bulunan tüm çok birimli sistemlere kadar ağ tanımı genişletilebilir. Bu bilgisayar ortamlarının, coğrafi olarak uzak olabilecek cihazlar arasında kolayca bilgi aktarabilme ve kullanıcıların kolaylığı için birden fazla yerde bilgileri çoğaltabilme yeteneğine sahip olduğunu anlamak önemlidir.[268] Öyle ki belirli bir sistem içerisinde kurulu olan Local, Wan ya da İnternet ağ trafiklerinin izlenmesi, analiz edilmesi ve analiz neticeleri doğrultusunda adli makamlar tarafından soruşturma konusu suça yönelik gerekli bulgular elde edilebilmektedir.[269]

Ek olarak ağlar, ağdaki dosyalar hakkında da bilgi üretir. Yukarıda dosya sistemi tarafından otomatik olarak üretildiği belirtilen ve *"Üst veri (meta-data)"* olarak adlandırılan bu veriler, bir dosyanın depolanan bir konumda ne, ne zaman ve kim tarafından oluşturulup değiştirildiğini belirlemek için kullanılabilirler. Üst veriler aynı zamanda bir kişinin, ağda yer alan bir bilgi hakkında bilgisinin olup olmadığı ya da kullanıcılar tarafından uygulanan bir eylem sonucu hangi değişikliğin meydana geldiğinin tespit edilmesi bakımından da oldukça önemlidir. Bu tür bilgiler, bir

[265] Casey, *Digital Evidence,* 31.
[266] Afandak, "Ceza Muhakemesinde Dijital Deliller," 104.
[267] Chaikin, "Network investigations," 240.
[268] Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 60.
[269] Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 48.

sistemde meydana gelen olayların zaman çizelgelerini de oluşturabilir. Her dosya, dosyayı oluşturan yazılıma bağlı olarak, kendisiyle ilişkilendirilmiş belirli miktarda dosya üst verisine sahiptir.[270] Ağlar çeşitli açılardan farklı şekillerde ele alınabilmektedir.

1.2.3.4.1. Yerel alan ağları- geniş alan ağları

Yerel alan ağlarında, makineler bir anahtar veya anahtarlar (makinelerin sayısına bağlı olarak) aracılığıyla birbirine bağlanır ve sırayla bir tür elektronik ağ geçidi aracılığıyla İnternet'e bağlanır.[271]

Geniş alan ağları ise özel devreler veya bir organizasyonun birden çok konumu arasında, internet üzerinden onları birbirine bağlamak için şifreli dijital tüneller kullanır ve bu şekilde aralarında bağlantı kurar.[272]

1.2.3.4.2. Özel ağlar- kurumsal ağlar

Özel ağlar, genellikle onları kullanan kişiler hakkında daha yüksek konsantrasyonda dijital bilgi içerir ve bu da ilgili dijital verileri bulmayı ve toplamayı küresel İnternete kıyasla daha kolay hale getirir.[273]

Farklı olarak bir suç ile ilgili yürütülen soruşturmalarda mağdurlar ve şüpheliler hakkında önemli miktarda bilgi, işyerlerindeki bilgisayar sistemlerinde bulunabilir. Modern işyerinde, çalışanlar belge oluşturmak, e-posta göndermek ve Web'e erişmek amaçlarıyla bilgisayarlarını kullanarak önemli miktarda zaman harcarlar. Bu bağlamda çalışanlar, şirket veya kurum bilgisayarlarını veya akıllı telefonlarını daha çok kullandıkça ve işyerlerinin dışarısına taşıdıkça, giderek artan miktarda bilgi üretmektedirler ki bu bilgiler de kurumsal ağlar tarafından tutulmaktadırlar. Ek olarak, kurumsal ağlarda kullanıcıların günlük kayıtları da tutulmaktadır. Hatta bazı kuruluşlar, ağ etkinliklerinin ve telefon görüşmelerinin içeriğini toplama yeteneğine bile sahiptir. Tüm bu bilişim teknolojisi sistemleri, ilgili kişilerin belirli bir zamanda ne yaptığını, kiminle iletişim kurduklarını ve hatta ne söylendiğini belirlemek için yararlı olan dijital deliller içerebilmektedir.[274]

---

[270] Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 62.
[271] Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 60.
[272] Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 61.
[273] Casey, *Digital Evidence,* 311.
[274] Casey, *Digital Evidence,* 315- 316.

1.2.3.4.3. Günlük kayıtları- trafik bilgisi

Bilgisayar günlük kayıtları (log[275] files), bir sistemde meydana gelen faaliyetler hakkında elektronik olarak oluşturulan ve saklanan bir bilgi dosyasıdır. Genellikle her biri geçmiş bir olay hakkında açıklayıcı nitelikler içeren bir dizi girdi şeklindedir.[276] Öyle ki bu kayıtlar bizlere, kişilerin internet ortamında gerçekleştirdiği her türlü erişimi, bu erişimin zamanı ve geçirilen süresini, erişim sırasında yararlanılan hizmetin türü ve aktarılan veri miktarı gibi değerleri gösterirler.[277]

Birçok farklı günlük türü vardır. Örneğin, denetim ve işlem günlükleri, bir bilgisayar sisteminin yakalamaya programlandığı her türlü veriyi içerebilir. Ayrıca e-posta günlükleri, web sunucusu günlükleri, yönlendirici günlükleri, İnternet servis sağlayıcısı günlükleri ve diğer ağ tabanlı günlükler, siber saldırılarla ilgili önemli bilgileri barındırırlar.[278]

Günlükler insanlar tarafından değil, bilgisayarlar tarafından otomatik olarak oluşturuldukları[279] için önyargı gibi insani yargıları içermezler. Bu sebeple bilgisayar günlüklerinin, içerikleri bakımından, diğer dijital delillere oranla daha doğru sonuçlar verebileceği belirtilmiştir.[280]

1.2.3.4.3.1. Ağ tabanlı olarak elde edilebilecek delillerin kaynakları

Ağ tabanlı olarak elde edilebilecek deliller, İnternet Servis Sağlayıcıları, yönlendiriciler, sunucular (server) ve İzinsiz Giriş Tespit Sistemlerinden gelen delilleri içermektedir.[281]

İnternet Servis Sağlayıcıları (ISS)- İnternet Servis Sağlayıcıları, kullanıcılara İnternet bağlantısı, e-posta ve web sitesi barındırma dahil olmak üzere bir dizi hizmeti sunar ve bu hizmetlerin her biriyle ilgili günlük dosyaları oluşturur. Ayrıca İnternet'e ISS aracılığıyla erişirken belirli bir IP adresini kullanan kişinin tanımlanmasını

[275] "log" kelimesi bazı yazarlar tarafından CMK m. 134'te yer alan "kütük" kelimesinin karşılığı olarak kullanılmakla birlikte (Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 56.) bilişim terminolojisinde "günlük" anlamında kullanılmaktadır. Bkz. Değirmenci, *Sayısal Delil,* 52.
[276] Chaikin, "Network investigations," 249.
[277] Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 58.
[278] Chaikin, "Network investigations," 249.
[279] Bilgisayarlar tarafından üretilen deliller (evidence computer generated) ve bilgisayarlar tarafından saklanan deliller (evidence computer stored) ayrımını yapan Değirmenci, günlük kayıtları ve kütükler arasındaki farkı bu ayrım ile belirtmiştir. Bkz. Değirmenci, *Sayısal Delil,* 53.
[280] Chaikin, "Network investigations," 249.
[281] Chaikin, "Network investigations," 244.

sağlayan "Kullanıcı Hizmetinde Uzaktan Kimlik Doğrulama Araması" kayıtları da ISS tarafından tutulmaktadır.[282] ISS yöneticileri, özel e-postaları okuyabilir, depolanmış dosyaları okuyabilir ve bireylerin İnternette gezinmelerini kaydeden erişim günlüklerini inceleyebilirler.[283]

Yönlendiriciler- Yönlendiriciler, iki ağı birbirine bağlamak için kullanılan ve genellikle özel bir bilgisayar olan cihazlardır. İnternette yönlendirici görevi gören bu bilgisayarlara *ağ geçidi* adı verilir. Yönlendiricilerin işlevi, çeşitli kaynaklardan veri paketleri almak, hedeflerini belirlemek ve bunları amaçlanan ağa iletmektir. Bu yönlendirme araçları değerli bilgiler içerirler.[284]

Sunucular- Sunucular, özel hizmetler sağlayan, bilgisayar ve yazılımın birleşiminden oluşan sistemlerdir. Bir web sitesindeki her ziyaret veya dosya talebi sunucu günlük dosyaları biçiminde kaydedilebilmekte ve bilgisayar ağlarında diğer kullanıcıların erişebileceği, kullanımına veya paylaşımına açık kaynakları barındırabilmektedir.[285]

İzinsiz Giriş Tespit Sistemleri- İzinsiz Giriş Tespit Sistemleri yazılımı, bir ağdaki yetkisiz erişimi veya izinsiz girişleri algılar. Kurumsal güvenlik ağlarındaki çoğu izinsiz giriş tespit sistemi, yasal işlemlerde delil olarak kullanılabilecek şekilde bilgilerin bütünlüğünü toplamak ve korumak amacıyla tasarlanmamıştır.[286]

1.2.3.4.4. Sosyal medya paylaşımları

Günümüzde sosyal medya paylaşımları da delil olarak ceza soruşturmalarının konusunu oluşturabilmektedir. Örneğin facebook, twitter gibi uygulamalar üzerinden yapılan paylaşımlar aracılığıyla hakaret, tehdit gibi suçlar işlenebilmekte ve bu paylaşımlar, yargılamalarda delil değeri taşıyabilmektedir. Ancak bu durumlarda da akla belli bazı sorular gelmektedir. Örneğin kişiler, başkaları adına açtıkları hesapları kullanarak bu suçları işleyebilmektedirler. Hatta bizzat bir başkasının hesabına erişim sağlamak suretiyle de bu ve benzeri suçlar işlenebilmektedir.[287]

---

[282] Chaikin, "Network investigations," 244.
[283] Leacock, "Search and Seizure of Digital Evidence," 223.
[284] Chaikin, "Network investigations," 245.
[285] Chaikin, "Network investigations," 245; Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 67
[286] Chaikin, "Network investigations," 245.
[287] Paul W. Grimm, Daniel J. Capra and Joseph P. Gregory, "Authenticating Digital Evidence," *Baylor Law Review*, vol. 69, no. 1 (2017): 31.

Sosyal medyadan elde edilen delillerin kabul edilebilir olup olmadıkları konusunda bazı ABD mahkemeleri; suç içeriği içeren sayfa ve hesapların, gönderiyi yaptığı iddia edilen kişiyle ilişkili İnternet protokol adresleri aracılığıyla izlenebiliyor oluşunu yeterli görmüştür.[288]

Bu hususa ek olarak, sosyal medya paylaşımlarının delil olarak kabul edilebilmesi bakımından bazı önerilerde de bulunulmuştur. Buna göre örneğin, ilgili paylaşımın sosyal medya hesabı sahibinin bilgisayar sabit diskinde yapılan arama sonucunda elde edilen bulguların uyuşup uyuşmadığının tespit edilmesi; ilgili sosyal medya uygulamasından söz konusu suçla ve yargılanan kişiyle ilgili olan bilgilerin talep edilmesi ve bunlarla suç konusu fiil arasında bağlantı kurulup kurulamaması veya ilgili sosyal medya hesabına yalnızca yargılanan kişiye ait cihazlardan mı girilebildiği yoksa başka kişilerin erişimine de açık olup olmadığı gibi bazı hususların tespit edilmesi, elde edilen verilerin mahkemede delil olarak kabul edilebilme ihtimalini arttıracaktır.[289]

Sosyal medya paylaşımlarının delil olabilmeleri konusu ülkemizde de sıkıntılı bir durumdur. Bu çerçevede Yargıtay'ın sosyal medya üzerinden gerçekleştirilen iletişime ve sosyal medya paylaşımlarına yönelik yaklaşımını da irdelemek yerinde olacaktır. Öncelikle sosyal medya aracılığıyla işlenmiş suçlarda (hakaret gibi) suçun dayanağı olan paylaşımların gerçekten var olup olmadığı ve eğer varlarsa suçu işlediği iddia edilen kişiye ilişkin bilgilerin *"sosyal paylaşım sitesinin yer sağlayıcısı olan şirketten, tespit edilen mesajın ne zaman ve hangi IP numarasından geldiğinin öğrenilmesi…"* suretiyle elde edilmesi gerekliliği vurgulanmış[290] fakat yer sağlayıcı şirketin bu bilgileri paylaşmaması halinde de diğer teknik araştırma yöntemleriyle bu bilgilerin elde edilmesi gerektiği belirtilerek suçu işlediği iddia edilen kişi ile suçun dayanağını oluşturan materyaller arasında kuvvetli bir bağlantı kurulması gerekliliği vurgulanmıştır.[291] Görüldüğü üzere Yargıtay, sosyal medya hesabı ile fail arasındaki

[288] United States v. Hassan, 742 F.3d 104, 133 (4th Cir. 2014); United States v. Brinson, 772 F.3d 1314, 1321 (10th Cir. 2014). Aktaran: Grimm, Capra and Gregory, "Authenticating Digital Evidence," 32.
[289] Diğer öneriler hakkında bkz. Grimm, Capra and Gregory, "Authenticating Digital Evidence," 32-33.
[290] Yar. 17. CD., E. 2015/27517, K. 2017/1716, T. 15.02.2017 https://www.lexpera.com.tr/ , son erişim, 20.03.2022
Yar. 18. CD., E. 2015/42049, K. 2018/371, T. 17.01.2018; benzer olarak bkz. Yar. 4. CD., E. 2018/8211, K. 2019/1552, T. 07.02.2019 https://www.lexpera.com.tr/ , son erişim, 07.06.2022.
[291] Yar. 18. CD., E. 2015/33358, K. 2016/663, T. 18.01.2016; Yar. 18. CD., E. 2016/219, K. 2016/8540, T. 25.04.2016; Yar. 16. CD., E. 2017/634, K. 2017/4806, T. 19.07.2017; Yar. 18. CD., E. 2016/202, K. 2016/7884, T. 18.04.2016 https://www.lexpera.com.tr/ , son erişim, 07.06.2022.

bağlantının kurulmasında, elde edilecek teknik bilgiler neticesinde IP adreslerinin eşleşmesi gibi çeşitli unsurları aramaktadır. Bunun da ötesinde bir kararında[292] Yargıtay,

> *"ilgili hesabın 8431 tweet attığı, 11.362 takipçisi olduğu, bu şartlarda sanığın iddia ettiği gibi hesabın sahte olmasının ve sanığın fotoğrafının diğer sosyal medya adreslerinden kopyalanarak alınmasının söz konusu olamayacağı…"*

Gibi bir kabulle sanık ile kovuşturmaya konu suç arasında bir bağlantı olduğu sonucuna ulaşmıştır. Sosyal medya paylaşımlarının ve bu doğrultuda dijital delillerin yukarıda da belirtilen özellikleri değerlendirildiğinde, bu şekilde gerçekleştirilen kabullerin, muhakeme sürecini hızlandıracağı şüphesiz olmakla birlikte suçun sübutuna ilişkin şüpheleri gidermeyeceğini belirtmemiz gerekir. Gerçekten de günümüzde teknolojinin geldiği yer ve suça ilişkin delillerin gizlenmesi teknikleri düşünüldüğünde bu kabuller bizleri maddi gerçeğin ortaya çıkarılabilmesi amacından uzaklaştıracaktır. Bu sebeple bu delillerin diğer delillerle de desteklenmesi gerektiğini düşünmekteyiz.

1.2.3.5. Bulut bilişim

Önceleri sabit diskler gibi bilgisayarda bulunan veri saklama birimlerinde tutulan bilgiler, taşınabilir bilişim sistemlerinin hayatımıza girmesi akıllı telefonlar ve taşınabilir bilgisayarlar gibi taşınabilir aletlerde tutulmaya başlamıştır. Gelinen noktada taşınabilir sistemlerin de kapasitelerindeki yetersizlikler nedeniyle ve kişilerin taşımak istediği bilginin çoğalması sonrasında bir ağa ulaşmak koşulu ile bu bilgilerin depolanmasında bulut bilişim sistemleri kullanılmaya başlanmıştır.[293]

Dijital deliller, günümüzde soruşturmayı yürüten yargı makamının sahasından ziyade, giderek artan bir şekilde yabancı, çoklu veya bilinmeyen yargı alanlarında, yani "bulutta" bir yerde bulunmaktadır.[294] *Bulut* kavramı, fiziksel olarak bir binada, büyük bir ofisin veya deponun, bir parçasına veya bütününe yayılmış, genellikle sunucu çiftliği olarak adlandırılan geniş bir bağlantılı sunucular dizisi olarak tanımlanabilecektir. Bulut hizmeti servis sağlayıcıları, ülke genelinde ve belki de birkaç ülkede dağılmış sunucu çiftliklerine sahip olabilirler.[295]

---

[292] Yar. 18. CD., E. 2018/4381, K. 2019/1853, T. 22.01.2019 https://www.lexpera.com.tr/ , son erişim, 07.06.2022.
[293] Sarsikoğlu, "Elektronik Delil (E-Delil) Kavramı," 524- 525.
[294] Seger, "e-Evidence and Access to Data in the Cloud," 35.
[295] Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 110.

Bulut bilişim, *"bilişim aygıtları arasında ortak bilgi paylaşımı sağlayan hizmetlere verilen genel ismi"* ifade etmektedir.[296]

Bulut bilişim kavramı, Türk Standartları Enstitüsü tarafından hazırlanan "Bulut Bilişim Güvenlik ve Kullanım Standardı"nda şu şekilde tanımlanmıştır:

> *"İşlemci gücü ve depolama alanı gibi bilişim kaynaklarının ihtiyaç duyulan anda, ihtiyaç duyulduğu kadar kullanılması esasına dayanan, uygulamalar ile altyapının birbirinden bağımsız olduğu ve veriye izin verilen her yerden kontrollü erişimin mümkün olduğu, gerektiğinde kapasitenin hızlı bir şekilde arttırılıp azaltılabildiği, kaynakların kullanımının kolaylıkla kontrol altında tutulabildiği ve raporlanabildiği bir bilişim türüdür".*[297]

Belirtildiği üzere teknolojinin gelişimi, suçun da evrilmesine yol açmıştır. Sonuç olarak yakın geçmişte bilgisayar ve hard disk odaklı karşılaşılan bilişim suçları, giderek bulut bilişime doğru yönelmektedir. Öyle ki bulut bilişim teknolojileri sayesinde, artık her işlem sadece internete bağlanma uzaklığındadır. Bu durum ise adli bilişim uzmanları bakımından sorunu daha da zor hale getirmektedir.[298]

Sorunların birincil nedeni, geleneksel adli bilişim uygulamalarının, belirli fiziksel konumlardaki bellek, sabit diskler, sunucular vb. gibi fiziksel cihazlardan veri toplanmasına dayanmasıdır. Adli bilişim uzmanı, çok sayıda müşteriye sanal hizmetler sağlayan "bulut" ortamıyla karşı karşıya kaldığında, verileri yalnızca bir müşterinin verilerini içeren fiziksel bir ortamda kullanılan geleneksel bir adli yöntemlerle görüntüleyememektedir. Öyle ki bir bulutta geleneksel adli bilişim yöntemleri kullanılsaydı, verileri toplanan kişinin verileri, birçok *"sunucu çiftliği"*nde yer alacağı için alınacak birebir kopyanın bir parçası diğer birçok kullanıcının verilerini bir başka ifadeyle muhakeme konusu maddi olaya ilişkin olmayan bilgilerin de açık hale gelmesine yol açardı. Bulut bilişim ortamında yoğun olarak sanallaştırma uygulamaları kullanılmaktadır ve bu sebeple erişim çoğu zaman imkân dahilinde olmadığı için elektronik cihazların toplanması da pratikte mümkün olmamaktadır. Bu

---

[296] Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 57.

[297] TSE, *Bulut Bilişim Güvenlik ve Kullanım Standardı*, 5. (https://statik.tse.org.tr/upload/tr/dosya/icerikyonetimi/1202/17032015093613-3.pdf erişim tarihi: 01.12.2021).

[298] Sebastian Schlepphorst, Kim-Kwang Raymond Choo and Nhien-An Le-Khac, "Digital Forensic Approaches for Cloud Service Models: A Survey," *Cyber And Digital Forensic Investigations*, Springer International Publishing, New York, USA, (2020): 175; Adem Emekci, Emin Kuğu ve Murtaza Temiztürk, "Adli Bilişim Ezberlerini Bozan Bir Düzlem: Bulut Bilişim," *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, Cilt. 2, No. 1 (2016): 8.

bağlamda bir bulutta yer alan dijital delillerin elde edilmesi, çeşitli sanal uygulamalar ve sanal diskler üzerinden gerçekleştirilebilmektedir.[299]

Bir diğer sorun ise Bulut depolamada verilerin bir dizi depolama sunucusu konumuna yayılıyor oluşu ve binlerce bulut kullanıcısına hizmet veriyor oluşu nedeniyle kişinin verilerinin bulunduğu sunucunun bir bölümü bir başka kıtadaki bir kişi veya bir kuruluşun verilerini de barındırıyor olabilir ki bu husus ülkesellik bağlamında bazı sorunları gündeme getirebilir. Nitekim ilgili verilerin bulunduğu yere göre soruşturulan suç fiilinin ilgili yerde suç olup olmadığı veya yapılacak adli bilişim işlemlerinin hangi ülke yasaları çerçevesinde gerçekleştirileceği gibi durumlar, sıkıntılara yol açabilmektedir.[300]

Bulut bilişimle ilgili sorunlar[301] bu sayılanlarla son bulmamakla birlikte bu sorunları ele almak adına birazdan bahsi geçecek olan Avrupa Konseyi Siber Suç Sözleşmesi Komitesi tarafından, 2014 Aralık ayında ortak uluslararası çözümlerin ve seçeneklerin belirlenmesi için *"Bulut Delili Çalışma Grubu (Cloud Evidence Working Group- CEG)"* kurulmuştur.[302]

Bir buluttan delil elde edilmesi konusunda karşılaşılan engeller ve bu engellerin aşılması konusunda öneriler, farklı açılardan ele alınmış olmasına karşılık Avrupa ve küresel düzeyde ülkelerin sadece küçük bir azınlığı, sınır ötesi verilere uzaktan erişime ve buluttan veri alınmasına izin veren özel yasal hükümlere sahiptir. Bu hükümlere göre uzaktan erişime yalnızca, arama sırasında şüphelinin cihazında bulunan verilere doğrudan erişilebiliyorsa izin verilmektedir. Bununla birlikte, bu tür düzenlemelerin olmadığı bazı ülkelerin uygulamalarında ve yargı kararlarında, bu tür

[299] Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 112; Emekci, Kuğu ve Temiztürk, "Bulut Bilişim," 12- 13; Sarsikoğlu, "Elektronik Delil (E-Delil) Kavramı," 526- 527.
[300] Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 112; Emekci, Kuğu ve Temiztürk, "Bulut Bilişim," 12; Önel ve Irmak, "Dijital delillerin windows işletim sistemi üzerinde incelenmesi," 1188.
[301] Sorunların organizasyonel, yasal ve teknik boyutlarının ele alındığı daha detaylı bilgi için bkz. Emekci, Kuğu ve Temiztürk, "Bulut Bilişim," 11- 13.
[302] Dijital delillerin elde edilmesi bakımından, "Bulut Delili Çalışma Grubu", bir bulut üzerinde çalışılırken karşılaşılan sorunlar ve bunların çözüm önerileri hakkında çeşitli tespit ve önermelerde bulunmuştur. Bu sorunlar temel olarak hukuki ve teknik sorunlar olarak belirlenmiştir. Söz konusu sorunlara ve bunların çözümü için önerilen çözümlere burada yer vermemekle birlikte bu konu hakkında detaylı bilgi edinmek için bkz. Seger, "e-Evidence and Access to Data in the Cloud," 35- 39.

uzaktan erişimlere, verilerin konumunun belirlenememesi gibi ihtimallerde izin verildiğini söyleyebiliriz.[303]

Ek olarak bulut bilişim ile ilgili düzenlemelerin eksikliğinin, kişilerin temel hak ve özgürlükleri konusunda da çeşitli ihlalleri gündeme getirebileceğini söyleyebiliriz. Bilgisayarların, ağların ve bulutların sınır ötesi aranmaları hususu, çeşitli hak ihlallerine vücut verebileceği gerekçesiyle, gerekli ve yeterli olan düzenlemelerin ve önlemlerin alınması bakımından önem arz etmektedir. Hangi güvencelerin ve korumaların uygulanması gerektiği konusu ise Devletlerin farklı hakları farklı açılardan ele alışları sebebiyle aralarında fikir ayrılıklarına yol açmaktadır. Bu bağlamda, verilere sınır ötesi erişim konusunda adli yardımlaşma hükümleri düzenlenirken, veri sahiplerinin de yeterli korumayla donatılması konusunda tartışmaların devam etmesi ve olması gerekene yakın bir düzenleme yapılması büyük önem arz etmektedir.[304]

Bulut bilişim hizmetleri kendi içerisinde üç gruba ayrılmaktadır. Bunlar; Altyapı hizmeti (Infrastructure as a Service- IaaS), Platform hizmeti (Platform as a Service- PaaS) ve Yazılım hizmeti(Software as a Service- SaaS) şeklindedir.[305,306] Bunlara değinmeden önce, genel, özel, hibrit ve topluluk bulutu şeklinde görülen bulut bilişim dağıtım (deployment) modellerinden kısaca bahsetmek yerinde olacaktır. Bu modeller az önce bahsi geçen hizmetlerin alındığı bulutlara erişim sağlayacak kişiler bakımından gündeme gelmektedir. Örneğin, genel dağıtım modeli, isteyen herkese açık bir bulut iken, özel dağıtım modeli genellikle güvenlik gereksiniminin ön planda olduğu organizasyonlarca tercih edilmektedir. Bu bakımdan bulut hizmeti sağlayıcılarının, müşterilerince talep edilen bulut hizmeti ve bulut bilişim dağıtım modeline göre farklı erişim imkanları tanıdığını söyleyebiliriz.[307]

---

[303] Sabine Berghs, Geoffrey Stewart Morrison and Caroline Goemans-Dorny, "Electronic Evidence: Challenges and Opportunities for Law Enforcement," *Law, Governance and Technology Series,* ed. Maria Angela Biasiotti, v.d., vol. 39, Cham, Switzerland: Springer, (2018): 97.
[304] Berghs, Morrison and Goemans-Dorny, "Electronic Evidence," 97.
[305] Schlepphorst, Choo, Le-Khac, "Digital Forensic Approaches," 175; Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 109; Emekci, Kuğu ve Temiztürk, "Bulut Bilişim," 9- 10; Sarsikoğlu, "Elektronik Delil (E-Delil) Kavramı," 526.
[306] Bununla birlikte kullanıcıların ihtiyaçları çerçevesinde ortaya çıkabilen, bulut güvenlik hizmeti (Security as a Service), bulut adli bilişim hizmeti (Forensics as a Service), bulut veritabanı hizmeti (Database as a Service) gibi hizmetler de gündeme gelebilmektedir. Emekci, Kuğu ve Temiztürk, "Bulut Bilişim," 10.
[307] Schlepphorst, Choo, Le-Khac, "Digital Forensic Approaches," 176; Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 109; Emekci, Kuğu ve Temiztürk, "Bulut Bilişim," 10.

Bulut bilişim hizmetlerinin neler olduğuna burada ayrıca yer verilmesinin sebebi, bulut hizmetlerinin, her geçen gün artan oranda yeni kişilere ulaşması ve bu kişiler tarafından (satın alınan hizmete bağlı olarak) farklı şekillerde kullanılıyor oluşudur. Buna bağlı olarak gündelik hayat giderek bulut ortamına taşınmaktadır ve bunun sonucunda suç da giderek bulut ortamında kendine yer edinmektedir. Bu sebeplerle bulut bilişimin ne olduğu, bulut hizmetlerinin neler olduğu ve bu hizmetler aracılığıyla ile nelerin yapılıp yapılamayacağının bilinmesinin önem arz ettiği düşüncesindeyiz.

1.2.3.5.1. Altyapı (infrastructure as a service- iaas) hizmeti

Altyapı hizmeti kişilere, bulut bilişimde kişilere en fazla erişim kontrolü sağlayan hizmettir. Genel olarak, sunucularda ve masaüstü sistemlerinde dosya sistemlerinin ve ham veri depolarının yedeklenmesi ve kurtarılması, büyük ölçeklerde depolama kapasitesi gibi işlevleri vardır. Bu hizmet, fiziksel bir bilgisayar ile aynı mantıkla çalışır ve kullanıcılara bulut altyapısı temelinde; işlemci gücü, veri depolama ortamları, bilgisayar ağları ve işletim sistemleri gibi diğer temel bilişim kaynaklarını kullanabildikleri ve bahsedilen ortamlar üzerinde kontrol ve denetim yapabildikleri ortamı sağlar.[308] Altyapı hizmeti ortamında faaliyet gösteren bazı kuruluşlara örnek olarak Amazon.com©, Facebook© ve Windows Live© verilebilir.[309]

1.2.3.5.2. Platform (platform as a service- paas) hizmeti

Platform hizmeti kişilere, bulut ortamındaki uygulama katmanı üzerinde kullanıcı tarafından tasarlanan bir uygulamayı çalıştırabilmeleri, bulut altyapısı üzerinden sunulan yazılım geliştirme ortamlarında kendi yazılımlarını geliştirebilmeleri ve geliştirilen yazılımlar üzerinde kontrol ve denetim yapabilmeleri için mantıksal bir sunucuda alan sağlar.[310] Genel olarak, veri analizi, rapor sistemleri gibi uygulamaların oluşturulması imkânı sağlanmaktadır.[311]

---

[308] Schlepphorst, Choo, Le-Khac, "Digital Forensic Approaches," 180; Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 110; Emekci, Kuğu ve Temiztürk, "Bulut Bilişim," 9-10; Sarsikoğlu, "Elektronik Delil (E-Delil) Kavramı," 526.
[309] Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 111.
[310] Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 111; Emekci, Kuğu ve Temiztürk, "Bulut Bilişim," 9; Sarsikoğlu, "Elektronik Delil (E-Delil) Kavramı," 526.
[311] Schlepphorst, Choo, Le-Khac, "Digital Forensic Approaches," 189.

1.2.3.5.3. Yazılım (software as a service- saas) hizmeti

Yazılım hizmeti kişilere sadece bulut ortamında sunulan kaynaklara erişim izni verir. Genel olarak kullanıma ve ürün ve hizmetlere yönelik aboneliklere dayalı olarak müşteri faturalandırmasını yöneten faturalama uygulamaları, çağrı merkezi uygulamalarından satış gücü otomasyonuna kadar uzanan "Müşteri İlişkileri Yönetimi" (CRM) uygulamaları, web tabanlı uygulamalar için içerik üretimi ve içeriğe erişim için içerik yönetimi gibi işlevleri vardır.[312] Yazılım hizmeti ile oluşturulan birçok örnek vardır: MS Office©, Salesforce.com©, GoToMeeting©, Google Mail©, VoIP© telefon hizmetleri, Photoshop © ve daha fazlası.[313]

1.3. Uluslararası ve Karşılaştırmalı Hukukta Dijital Deliller

Bilişim suçları anlamında Kanada, 1983 yılında Ceza Kanununda değişiklik yaparak bilgisayar suçlarını ele alan bir federal yasa çıkaran ilk ülke olmuştur. Sonrasında ABD 1984 yılında, "Federal Bilgisayar Dolandırıcılığı ve Kötüye Kullanımı" kanunu kabul etmiş ve bu kanun da 1986, 1988, 1989 ve 1990'da değişikliklere uğramıştır. Sonrasında 1989 yılında Avustralya ceza kanununda bir değişikliğe gidilmiş "Bilgisayarlara İlişkin Suçlar" (Bölüm 76) eklenmiştir. İngiltere'de de 1990 yılında, bilişim sistemlerine izinsiz girişler, "Bilgisayarın Kötüye Kullanımı Kanunu"nun kabul edilmesiyle birlikte suç sayılmıştır.[314]

Karşılaştırmalı hukuk değerlendirildiğinde dijital deliller ile diğer deliller arasında bunları birbirine eşdeğer sayma yönünde yaygın bir eğilim olduğu görülmektedir. Bu eşdeğerlik özellikle üç alanda karşımıza çıkmaktadır. Öncelikle ve en yaygın olarak, elektronik belgenin, kâğıt bazlı belgeye eşdeğer sayılması yönündedir. İkinci olarak yine bir elektronik delil olarak kabul edilen elektronik imzanın, el ile atılan imzaya eşdeğerliği düzenlenmektedir. Üçüncü olarak ise elektronik postaların, klasik posta usullerine eşdeğer sayılmasına sıklıkla rastlanmaktadır.[315]

Bu başlıkta öncelikle Türkiye'nin de taraf olduğu ve ceza muhakemesi bakımından dijital delillerin ele alındığı uluslararası sözleşmeler irdelenmeye

[312] Schlepphorst, Choo, Le-Khac, "Digital Forensic Approaches," 190- 191; Emekci, Kuğu ve Temiztürk, "Bulut Bilişim," 9.
[313] Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 112.
[314] Casey, *Digital Evidence,* 36.
[315] Değirmenci, *Sayısal Delil,* 129.

çalışılacaktır. Devamında İçtihat Hukukunun geçerli olduğu ABD ve İngiltere'de dijital delillerin nasıl ele alındığı ve değerlendirildikleri hususu incelenmeye çalışılacaktır. Bu ülkeler, bilişim teknolojilerinin öncüleri olmaları ve adli bilişim teknolojileri konusunda kaynak ülke konumunda olmaları sebebiyle seçilmiştir. Son olarak öncelikle genel olarak Avrupa'da ve sonrasında Kıta Avrupası Hukukunun geçerli olduğu Almanya ve İtalya'da dijital delillerin nasıl ele alındığı ve değerlendirildikleri hususu incelenmeye çalışılacaktır. Bu ülkeler ise, ceza hukuku sistemleri bakımından Türkiye'ye benzerlikleri sebebiyle seçilmiştir.

1.3.1. Türkiye'nin taraf olduğu ilgili uluslararası sözleşmeler

1.3.1.1. "Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi"[316]

"Ceza İşlerinde Karşılıklı Adli Yardım Avrupa Sözleşmesi" 1959 yılında imzalanmış ve 1969 yılında Türkiye, bu sözleşmeye taraf olmuştur. İmzalanma tarihi göz önüne alındığında özellikle dijital deliller ve verilerin gizliliği konularında değinilmediği görülmektedir. Ek olarak sözleşme, delillerin elde edilmesine yönelik değil fakat değiş tokuşuna yöneliktir.

Sözleşmenin amacı, Üye Devletlerin kolluk kuvvetlerinin diplomatik kanalları kullanmak yerine doğrudan birbirlerine yaklaşmalarına olanak sağlamaktır. Bu nedenle, dijital delillerin elde edilmesi bakımından için yenilikçi yöntemler ve teknolojilerden kaynaklanan belirli veri koruma konularını kapsamadığı bir gerçektir.

Bu bağlamda dijital delillerin elde edilmeleri ve uluslararası ortamda değiş tokuşunun sağlanması adına güncel ve dijital delillerin teknik yönlerini irdeleyen yeni uluslararası adli yardımlaşma düzenlemelerinin kaleme alınması bu konudaki olumsuzlukları minimum düzeye indirecektir. Dijital delillerin dünya geneline yayılmış olabilecekleri gerçeği, bu konuda gerçekleştirilecek hukuki düzenlemelerin, uluslararası düzeyde ve yeknesak bir şekilde kaleme alınması gerekliliğini bizlere göstermektedir.[317]

---

[316] *"Ceza İşlerinde Karşılıklı Adlî Yardım Avrupa Sözleşmesi'nin onaylanmasının uygun bulunduğu hakkında Kanun"*: Resmî Gazete Tarihi: 23.3.1968, Sayı: 12856.
[317] Kaynakçıoğlu, "Dijital Deliller," 61.

1.3.1.2. "Sanal Ortamda İşlenen Suçlar Sözleşmesi" (siber suçlar sözleşmesi)[318]

Devletlerin maddi ve usul hukuku açısından yeknesak bir ceza sistemine sahip olabilmeleri için etkili bir adli yardımlaşma sisteminin oluşturulması ve uluslararası bir suç haline gelen bilgisayar ve bilişim teknolojileri aracılığıyla işlenen suçlarda dijital delillerin elde edilebilmesi, değişimi ve siber suçlarla etkin mücadele amacıyla "Avrupa Siber Suç Sözleşmesi" kaleme alınmış ve 1 Temmuz 2004 tarihinde yürürlüğe girmiştir. Ek olarak bilişim sistemleri vasıtasıyla işlenen ırkçı ve yabancı düşmanı eylemlerin suç haline getirilmesine yönelik çalışmalar sonucunda Avrupa Siber Suç Sözleşmesi'ne Ek Protokol 1 Mart 2006 tarihi itibariyle yürürlüğe girmiştir.[319]

Siber Suçlar Sözleşmesi, dijital delillerle ilgili olarak çıkarılan ilk bağlayıcı hukuki metindir. 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.[320]

Sözleşmede ileride ayrıntılarına yer vereceğimiz çeşitli koruma tedbirleri yer almaktadır. Bu tedbirler, dijital delillerin elde edilmesi bakımından usule ilişkin kurallardan bahsederken, sözleşmenin tarafı ülkelerin iç hukuk ilkelerinin gerektirmesi halinde başka önlemler yoluyla hedeflerine ulaşmalarına izin vermektedir. Ek olarak bu tedbirlerin uygulanması sırasında verilerin gizliliği konusunda çeşitli güvencelere de yer verilmiştir.[321]

Bahsi geçen güvencelere, dijital delillerin elde edilmesi için kullanılan koruma tedbirlerinden önce, m. 15'te yer verilmiştir. Bu güvenlik önlemleri nispeten genel niteliktedirler ve belirli önlemlerle ilgili belirli riskleri dikkate almamaktadırlar. Buna karşılık bu önlemler, Avrupa düzeyinde dijital delil toplamayla ilgili verilerin gizliliğini kaleme alan tek önlemlerdir.[322]

Siber suçlar sözleşmesi, taraf devletlere oldukça fazla hareket alanı bırakmakla birlikte, detaylarına ileride değineceğimiz şu üç zorunlu güvenlik önlemine tarafların

---

[318] *"Sanal Ortamda İşlenen Suçlar Sözleşmesi"*, Resmî Gazete Tarihi: 09.08.2014, Sayı: 29083.
[319] Afandak, "Ceza Muhakemesinde Dijital Deliller," 169- 170.
[320] Afandak, "Ceza Muhakemesinde Dijital Deliller," 170- 171.
[321] Forgó, v.d., "Privacy Protection," 273.
[322] Forgó, v.d., "Privacy Protection," 274.

uymalarını beklemiştir. Bu önlemler; "Adli veya diğer bağımsız denetim", "Başvuruyu haklı çıkaran gerekçeler" ve "Kapsamın ve sürenin sınırlandırılması"dır.

1.3.2. Karşılaştırmalı hukukta dijital deliller

1.3.2.1. İçtihat hukuku

Avustralya, İngiltere ve Amerika Birleşik Devletleri gibi içtihat hukuku yetki alanlarında, elektronik olarak tutulan tüm kayıtlar da dahil olmak üzere ticari kayıtların, delil olarak kabul edilebilir olduğu kabul edilmektedir. Burada dikkat edilen, mahkemeye sunulan kaydın, orijinal kaydın doğru bir temsili olup olmadığının tespiti bakımındandır. Sunulan kaydın orijinalliği tespiti bakımından odaklanılan husus ise kaydın oluşturulduğu andan mahkemeye verildiği ana kadar, üzerinde değişiklik yapılmadığı veya başka bir şekilde tahrif edilmediğinin güvenle tespit edilebilmesi için kaydın muhafaza edilmesine yönelik prosedürlerin kalitesi olması ile ilgilidir.[323]

Genel anlamda bilişim sistemlerine yönelik olarak gerçekleştirilen aramalar ayrı bir düzenlemesi bulunmaya içtihat hukukunun geçerli olduğu ülkelerde genel aramaya ilişkin olan kurallar, bilişim sistemlerinin aranması bakımından da uygulanmaktadır. Bu çerçevede İngiltere ve Galler gibi örf ve içtihat yetki alanlarında, polisin bir kişinin evini genel olarak onun aleyhine delil aramak için aramaması kural haline getirilmiştir. Arama ve el koyma amacıyla binaya yasal olarak giriş, her zaman belirli bir amaçla ilgili olmalı ve arama belirtilen amaçla tutarlı olmalıdır. Benzer şekilde ABD'de de aramalarla ilgili olarak gerçekleştirilen Dördüncü Değişiklik, makul olmayan aramaları yasaklar ve tüm aramaların yürütülmesinde makul bir mahremiyet beklentisi oluşturur.[324]

Bilişim sistemleri de dahil olmak üzere gelen olarak arama izninin alınabilmesi için savcılar, arama sebeplerini göstermeli ve aranacak yer ile ele geçirilecek kişi veya şeyleri detaylandırmalılardır. Arama izni alabilmek için savcıların bir hakimi veya sulh hakimini, her ihtimalde bir suç işlendiğine, suç delillerinin mevcut olduğuna ve

[323] Chaikin, "Network investigations," 247; Rand Europe and Lawfort, "Update to the Handbook of Legal Procedures of Computer and Network Misuse In Eu Countries For Assisting CSIRTs, D15: Final Report", 2005, ftp://ftp.cordis.europa.eu/pub/ist/docs/directorate_d/trust-security/ec-csirtd15.pdf , (29 Mayıs 2016): 268. Aktaran: Başlar, "Elektronik Delil," 1672.
[324] Leacock, "Search and Seizure of Digital Evidence," 222.

aranacak yer (veya bilişim sisteminde) suça ilişkin delillerin bulunmasının muhtemel olduğuna ikna etmesi gerekir.[325]

Mahkemeler dijital deliller bakımından öncelikle kabul edilebilirliklerini ve bu bağlamda delilin orijinal delil olup olmadığını değerlendirirler. Bu bağlamda ilk ele alınan konu, orijinal delil ile bu delilin birebir kopyalanması suretiyle elde edilen ve üzerinde inceleme gerçekleştirilen birebir kopyanın aynı olup olmadığıdır. Bunun tespiti ise ileride daha ayrıntılı bir şekilde ele alınacak olan özet değer işleminin gerçekleştirilmesi ile sağlanmaktadır.[326,327] düzgün bir delil zincirinin takip edilmesi ve belgelemenin bir bütün halinde olması da dijital delillerin kabul edilebilmesi bakımından önem arz edecektir.[328]

Dijital kanıtların doğrulanması için güvenilirliklerinin de değerlendirilmesi gerekir. Mahkemede dijital delillere güvenilip güvenilemeyeceğinin değerlendirilmesinde iki genel yaklaşım vardır. İlk yaklaşım, delili oluşturan bilişim sisteminin normal şekilde çalışıp çalışmadığına odaklanmaktır. Diğer yaklaşım ise dijital delilleri, yalnızca bilişim sistemlerine yönelik olarak gerçekleştirilen müdahaleleri veya bilişim sistemine zarar veren diğer davranışları tespit edebilmek amacıyla incelemektir.[329]

Geçmişte, Amerika Birleşik Devletleri ve Birleşik Krallık'taki mevzuatın çoğu, 1993 yılına kadar mahkemelere bilgisayar tarafından oluşturulan kayıtları, kayıtları oluşturan sistem ve sürecin güvenilirliği temelinde değerlendirmeleri talimatını vererek ilk yaklaşımı izlemiştir.[330]

1993 yılında ise adeta bir dönüm noktası yaşanmış ve dijital delillerin elde edilmesi konusunda, *bilimsel delil* kriterini ortaya koyan bir karar verilmiştir. Buna bağlı olarak *bilimsel delil* olarak kabul edilen dijital deliller, hükme esas alınabilecektir. *Daubert v. Merrell Dow Pharmaceuticals, Inc.'kararında* (1993)[331]

---

[325] Casey, *Digital Evidence,* 57.
[326] Casey, *Digital Evidence,* 59.
[327] Birazdan bahsedecek olmakla birlikte kısaca birebir kopya ve özet değer alma işlemlerini özetleyecek olursak; birebir kopya işlemi, elde edilen bilişim sisteminin, içerdiği her şey ile birlikte tam ve eksiksiz bir kopyasını oluşturma işlemini ifade ederken özet değer işlemi ise, çıkarılan birebir kopya ile orijinal bilişim sisteminin aynı olduğunu, üzerinde bir değişiklik yapılmadığını ispat etmeye yarayan matematiksel bir fonksiyonu ifade etmektedir. Bkz. Üçüncü Bölüm, *"3.3.1.1. Birebir kopya"* ve *"3.3.1.2. Özet değer"* başlıkları.
[328] Casey, *Digital Evidence,* 60.
[329] Casey, *Digital Evidence,* 61.
[330] Casey, *Digital Evidence,* 61-62.
[331] Daubert v. Merrell Dow Pharm., Inc., 43 F.3d 1311 (9th Cir. 1995).

geliştirilen dört kriteri sağlayan deliller *bilimsel delil* olarak kabul edilecektir. Bu kriterler aşağıdaki gibidir:[332]

1. Delilin elde edilmesinde kullanılan teori veya tekniğin test edilip edilemeyeceği (ve test edilip edilmediği).

2. Bu teorinin bilinen veya potansiyel hata oranının yüksek olup olmadığı ve tekniğin işleyişini kontrol eden standartların varlığı ve bakımı.

3. Bu teori veya tekniğin hakem incelemesine ve yayına tabi tutulup tutulmadığı.

4. Bu teori veya tekniğin ilgili bilim camiasında "genel kabul" görüp görmediği.

Daubert ölçütleri incelendiğinde, adli bilişim yöntemlerinin, cezai uyuşmazlıklarda kullanılabilecek bilimsel bir disiplin olarak kabul edilebilmesi için diğer bilimsel disiplinler için geçerli olan standartları karşılaması gerektiği açık olarak ortaya çıkmaktadır. Bu standartlara ise *Daubert* ölçütleri çerçevesinde formel test edilebilir teoriler, önceden gözden geçirilmiş metodoloji ve araçlar, tekrar edilebilir ampirik çalışmalar dahildir.[333]

Daubert kararı uyarınca delil elde etmede ve incelemede kullanılan yazılımların bağımsız kaynak kodlarının incelenmesi, kusurları ortaya çıkarmak için belki de en açıklayıcı yöntemdir. Ancak çoğu durumda, kaynak kodun özel niteliği, bu tür bir incelemeyi mümkün kılmamaktadır.[334]

Dijital delillerin bilimselliğinin sağlanması amacıyla bazı yöntemler önerilmiştir. Öncelikle dijital delillerin elde edilmesini ve incelenmesini sağlayan yazılımların doğru çalışıp çalışmadıkları konusunda uzmanların, uygulamanın dahili mantığı hakkında önceden bilgi sahibi olmadan yazılımdaki kusurları belirlemeye çalıştığı bir yazılım testi metodolojisi olan *Kara Kutu Testi*[335] adı verilen bir metodolojinin uygulanması önerilmiştir.[336]

---

[332] Casey, *Digital Evidence,* 73; Buskirk and Liu, "Digital Evidence," 23; Kenneally, "Gatekeeping out of the Box," 8; Ryan and Shpantzer, "Legal aspects of digital forensics," 2; Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj)," 65.
[333] Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj)," 65.
[334] Buskirk and Liu, "Digital Evidence," 23.
[335] Kara kutu testi, bulanıklaştırma ve mantık geçişi olarak adlandırılan ve iki aşamadan oluşan bir yöntemdir. Detaylı bilgi için bkz. Buskirk and Liu, "Digital Evidence," 23.
[336] Buskirk and Liu, "Digital Evidence," 23; Kenneally, "Gatekeeping out of the Box," 24.

İkinci olarak dijital delilleri elde etmede kullanılan yazılımlarda ortaya çıkan hataları azaltmak için önerilen bir yaklaşım, insanların yazılımın kritik bileşenleri için kaynak kodunu görmelerini sağlamayı önermektedir. Dünyanın her yerindeki programcılara kaynak kodu sağlamak, bu yazılı inceleyenlerin programı daha iyi anlamasını sağlayacak ve hataların bulunma olasılığını arttıracaktır.[337] Ancak ticari amaçla bu yazılımları geliştirenlerin, rekabet avantajlarını korumak için programlarının bazı bölümlerini gizli tutmak isteyecekleri aşikardır.[338]

Dijital delilleri işlemek için kullanılan araç ve tekniklerin bilimsel geçerliliğini değerlendirmeye yönelik bir diğer yaklaşım, uzmanların bir ön inceleme yapmalarını önermektedir. Bu bağlamda ABD'deki bazı yargı bölgeleri ve uluslararası mahkemeler, farklı uzmanlar tarafından hazırlanan ve olay hakkındaki bulguları özetleyen açıklayan ortak bir rapor sunmalarını şart koşmaktadırlar.[339]

Son olarak adli bilişim araçlarının "çapraz doğrulanması" adı verilen bir başka yaklaşım uyarınca bir araçtan elde edilen bulgular ile bir başka araçtan elde edilecek bulgular karşılaştırılmalı ve çıkan sonuca göre o araçtan elde edilecek delilin bilimsel olup olmayacağı belirlenmelidir.[340]

Muhakemenin sonraki aşamalarında adli bilişim uzmanlarından genellikle ifade vermeleri veya bulgularının yazılı bir özetini bir yeminli beyan ile veya bilirkişi raporu şeklinde mahkemeye sunmaları istenir. Beyanda bulunmak veya bir rapor hazırlamak, soruşturma sürecinin en önemli aşamalarından biridir. Çünkü elde edilen bulgular yazılı olarak açık bir şekilde iletilmedikçe, başkalarının bunları anlaması veya kullanması, adli bilişim terminolojisinin herkesçe bilinemiyor oluşu sebebiyle olası değildir.[341]

Devam edecek olursak ABD'de geçerli olan ve olay yerinin incelenmesi ve delillerin elde edilmesi sırasında geçerli olan "aşikâr biçimde belli olma öğretisi"ne[342] de değinmek yerinde olacaktır. Aşikâr biçimde belli olma öğretisi uyarınca olay

[337] Buskirk and Liu, "Digital Evidence," 24.
[338] Brian Carrier, "Open Source Digital Forensics Tools: The Legal Argument," *Research Report* (October, 2002): 8.
[339] Casey, *Digital Evidence,* 75.
[340] Buskirk and Liu, "Digital Evidence," 24.
[341] Casey, *Digital Evidence,* 75.
[342] Değirmenci tarafından "asikâr biçimde belli olma öğretisi" olarak anılan *the plain view doctrine* kavramına değinirken içeriğini doğru yansıtıyor oluşu sebebiyle aynı terimi kullanmayı tercih etmekteyiz.

yerinin incelenmesi sırasında aşikâr biçimde belli olan başka suçlarla ilgili delillerle karşılaşılırsa bu deliller, ayrı bir arama kararı gerekmeksizin elde edilebilecektir.[343]

Horton v. California[344]kararı, incelemede bulunan görevliler bakımından bir delilin aşikâr biçimde belli olmasına dayanılarak ele geçirilmesi konusunda üç temel kural getirmiştir. İlk olarak incelemeyi yapan kolluk personeli bu incelemeyi yaparken yasal yetkiye dayanmak zorundadır. Başka bir ifadeyle gerçekleştirilen inceleme, usulüne uygun olarak alınmış bir arama kararı çerçevesinde gerçekleştirilmelidir. İkinci olarak soruşturma konusu suçla bağlantısı olmayan ancak bir başka suça ilişkin olduğu iddia edilen delil, yapılan inceleme sırasında aşikâr bir biçimde görülebilmeli, başka bir deyişle bu delile ulaşmak için özel bir çaba sarf edilmemelidir. Üçüncü olarak soruşturma konusu suçla ilgisi olmayan bu delil, bir başka suçun işlendiği hususunu aşikâr bir biçimde belli etmelidir. Çünkü aşikâr biçimde belli olma öğretisi, elde edilen bu delil eğer kesin nitelikte değilse, bu delilin işaret ettiği suça yönelik araştırma yapılmasına izin vermemektedir.[345]

Aşikâr biçimde belli olma öğretisi, Türk hukukunda yer alan "tesadüfen elde edilen delil" kavramına karşılık gelen ve içtihat hukukunun yaratmış olduğu, arama kararı olmaksızın delil elde etmeye yarayan bir istisnadır.[346] Tesadüfen elde edilen deliller ve aşikâr biçimde belli olma öğretisi hakkında ileride detaylı bilgiler verilecektir.

Son olarak, ABD Adalet Bakanlığına bağlı olan *"ABD Ulusal Adalet Enstitüsü (National Institute of Justice- NIJ)"* tarafından hazırlanan ve dijital delillerin toplanması, elde edilmesi, değerlendirilmesi gibi konular hakkında kurallar getiren kılavuzlara da değinmek yerinde olacaktır. Bu bağlamda dijital delile ilk müdahalede bulunan ekibin,[347] dijital olay yerinde inceleme yapan ve delilleri toplayan ekibin[348]

[343] Değirmenci, *Sayısal Delil,* 282; Robinton, "Courting Chaos," 331.
[344] Horton v. California (496 U.S. 128 (1990).
[345] Robinton, "Courting Chaos," 331.
[346] Değirmenci, *Sayısal Delil,* 282.
[347] U.S. Department of Justice Office of Justice Programs, "Electronic Crime Scene Investigation: A Guide for First Responders", US National Institute of Justice, Washington, USA, July 2001, https://www.ojp.gov/pdffiles1/nij/219941.pdf son erişim: 03.12.2021.
[348] U.S. Department of Justice Office of Justice Programs, "Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders", US National Institute of Justice, Washington, USA, November 2009, https://www.ojp.gov/pdffiles1/nij/227050.pdf son erişim: 03.12.2021.

ve sonrasında kolluk birimlerinin ve savcıların uyması gereken kurallar,[349] kesin bir şekilde belirtilmiştir. Ek olarak ABD'deki adli bilişim birimleri bu kriterleri her zaman gözden geçirerek gelişen teknoloji ve yeni suç tiplerine göre güncellemekte ve bu kriterlerin belirlendiği sempozyum ve konferanslara ev sahipliği yapmaktadır.[350]

Bunlara karşılık olarak içtihat hukukunda dijital delillerle ilgili net yasal kuralların olmamasının bu alandaki belirsizliği arttırdığı, ceza muhakemesi kurallarının genellikle dijital incelemeler konusunda sessiz olduğu ve içtihat hukukunun bu konuda yetersiz olduğu çünkü kuralların bir mahkemeden diğerine büyük ölçüde değişiklik gösterebildiği ve bu durumun da uygulayıcıları, resmi olmayan geçici çözümleri tercih etmelerine yönlendirdiği ileri sürülmüş ve çözüm adına etkili adımlar atılması gerektiği belirtilmiştir.[351]

1.3.2.2. Kıta Avrupası hukuku

Avrupa düzeyinde, dijital delillerin elde edilişi ve Üye Devletler arasında tek tip bir şekilde değişimini mümkün kılan birleşik bir yasal çerçeve yahut ortak kurallar bulunmamaktadır. Avrupa düzeyinde, dijital delillerin toplanması, saklanması, işlenmesi ve değişimi ile doğrudan veya dolaylı bir şekilde ilgili olan sınırlı sayıda yasal kural bulunmaktadır. Bu kuralların çoğu, Üye Devletler tarafından genellikle kendi yasal sistemlerine ve geleneklerine göre farklı şekillerde uygulanmaktadır.[352]

Dijital delillerin elde edilmesi ve değişimi, terörle mücadele operasyonlarında ve küresel suçlarla mücadelede oldukça önem arz etmektedir.[353] Buna karşılık bölgesellik ilkesinin getirdiği sınırlamalar, özellikle siber suçların kapsamı ve giderek artan uluslararası boyutuyla çatışma halindedir.[354]

Dijital delillerin, toplanması, saklanması ve değiş tokuşu ile ilgili olarak AB ülkeleri arasında tek tip bir yasal çerçeve bulunmamaktadır. Bu durum, polis ve adli makamları belirsiz bir ortamda görev yapmaya ve zaman zaman hem hukuki hem de

[349] U.S. Department of Justice Office of Justice Programs, "Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors", US National Institute of Justice, Washington, USA, January 2007, https://www.ojp.gov/pdffiles1/nij/211314.pdf son erişim: 03.12.2021.
[350] Başlar, "Adli Bilişim," 65.
[351] Jenia I. Turner, "Managing Digital Discovery in Criminal Cases," *Journal of Criminal Law and Criminology*, vol. 109, no. 2 (2019): 240- 241.
[352] Biasiotti, v.d., "Introduction: Opportunities," 8.
[353] Biasiotti, v.d., "Introduction: Opportunities," 13.
[354] Biasiotti, v.d., "Introduction: Opportunities," 14.

teknolojik açıdan tutarsız veya kafa karıştıran çözümler benimsemeye zorlamaktadır.[355]

Yukarıda bahsi geçen *"EVIDENCE"* projesi, dijital delillerin toplanması (ve değiş tokuş edilmesi) için Avrupa'da ortak bir yasal çerçevenin olmadığı ve böyle bir çerçevenin oluşturulması gerekliliği düşüncesiyle hayata geçirilmiştir.[356]

AB ülkeleri çerçevesinde bu konuyla ilgili özellikle delillerin toplanması ve değişimi için, günümüzde giderek bir "karşılıklı tanıma" ilkesine dönüşen "karşılıklı yardım" ilkesi tasarlanmıştır. Karşılıklı tanıma ilkesi, bir Üye Devletin makamları tarafından yasal olarak toplanan delillerin, orada geçerli olan standartlar da dikkate alınmak suretiyle, diğer Üye Devletlerin mahkemelerinde de kabul edilebilir olduğu anlamına gelmektedir. Ek olarak, birlik içinde farklı hukuk sistemleri içerisinde elde edilmiş olsa bile deliller, üye ülkelerin her birinin adli makamlarınca kabul edilir ve kullanılırlar.[357]

Bununla birlikte, karşılıklı güven oluşturma çabalarına rağmen, "karşılıklı tanıma" prosedürleri, giderek daha küresel ve karmaşık hale gelen mevcut suçların önlenmesi için dijital delillerin hızlı ve verimli aktarımı gerekliliğini hala tam olarak karşılayamamaktadır. Buna ek olarak "karşılıklı tanıma" prosedürlerinin sınırlı bir kapsamı olduğu gerçeğinin yanı sıra, ulusların karşılıklı tanıma ilkesini uygulama konusundaki isteksizliklerinin olduğu hipotezi de ileri sürülmüştür.[358]

Bu bağlamda Avrupa Komisyonu'nun, mümkün olan en kısa sürede dijital delil değişimi için çevrimiçi bir sistem benimsemenin olası yolları hakkında Üye Devletlerle ilgili bir karar vermesi gerektiği ve bu sistemin; ya Avrupa Komisyonu tarafından yönetilen ve tüm Üye Devletlerin ulusal veri tabanlarını bağlaması gereken merkezi bir sistem ya da Avrupa Komisyonu'nun iletim ve talepler konusunda yönetim yetkisi bulunmadığı ve Üye Devletlerin ulusal veri tabanlarını bağlamadığı fakat doğrudan kendilerinin bağlantıya geçtiği merkezi olmayan bir sistem olması gerektiği önerilmiştir.[359]

[355] Biasiotti, v.d., "Introduction: Opportunities," 14
[356] Forgó, v.d., "Privacy Protection," 263.
[357] Biasiotti, v.d., "Introduction: Opportunities," 15- 16.
[358] Biasiotti, v.d., "Introduction: Opportunities," 16- 17.
[359] Biasiotti, v.d., "Introduction: Opportunities," 20.

1.3.2.2.1. Almanya

Alman Ceza Muhakemesi Kanunu m. 244/2 uyarınca, yetkili soruşturma makamı kabul edilebilir olmak koşuluyla, delilleri dikkate almakta ve delillerin ağırlığını belirlemekte özgürdür. Ancak mahkemeye sunulan video veya fotoğraf gibi dijital delillerin oluşturulma tarihi ve kaynağı ile ilgili belirli gereksinimleri karşılamaları gerekmektedir.[360]

Alman hukukunda dijital Delillerin ceza yargılamasında delil olarak kullanılıp kullanılmadığı konusuna bakıldığında delil serbestisi ilkesinin geçerli olduğunu ve mahkemeye her türlü delilin sunulabildiği görülmektedir. Buna göre dijital delilin de yaygın bir delil türü olarak kabul edildiği görülmektedir. Nitekim dijital delilin, daha gerçekçi yapısı nedeniyle hâkimi yargılama sürecinde daha kolay ikna etme özelliğine sahip olduğu da değerlendirilmektedir.[361]

Öncelikle Alman Ceza Muhakemesi Kanunu'nda özel olarak bilişim sistemlerinde veri arama, kopyalama ve elkoyma tedbirinin düzenlenmediğini söyleyebiliriz. Bu bağlamda Siber Suçlar Sözleşmesi m. 19'da yer alan "Saklanan Bilgisayar Verilerinin Aranması ve Bunlara Elkonulması" tedbirinin dahil edilmediği Alman Ceza Muhakemesi Kanununa göre bilişim sistemlerinde veri aranması, kopyalanması ve bunlara elkonulması; Alman Ceza Muhakemesi Yasası'nın elkoymayı düzenleyen 94. maddesi, süpheli kişiler için aramayı düzenleyen 102. maddesi, diğer kişiler bakımından aramayı düzenleyen 103. maddesi, arama emri ve icrasını düzenleyen 105. maddesi, bilgi toplama ve soruşturmayı düzenleyen 161. maddesi, adli kolluk görevlerini düzenleyen 163. maddesi ve belgelerin incelenmesini düzenleyen 110. Maddesi hükümlerine göre gerçekleştirilecektir. Ek olarak Alman hukukunda trafik verilerin gerçek zamanlı olarak toplanması m. 100a, 100b ve 100g maddelerine; içerik verilerinin elde edilmesi ise 100a ve 100b maddelerine göre yapılmaktadır.[362]

---

[360] Karolina Aksamitowska, "Digital Evidence in Domestic Core International Crimes Prosecutions: Lessons Learned from Germany, Sweden, Finland and The Netherlands", *Journal of International Criminal Justice,* Volume 19, Issue 1 (March 2021): 198.

[361] Rand Europe and Lawfort, "Update to the Handbook" 115, Aktaran: Başlar, "Elektronik Delil," 1672.

[362] Değirmenci, *Sayısal Delil,* 290- 291.

Bu düzenlemelerden farklı olarak Alman Ceza Muhakemesi Kanununa m. 100b ile getirilen yeni bir düzenleme ise *uzaktan arama*dır.

Almanya'da açıklanan resmi rakamlara göre bir günde on binlerce sanal saldırı olmakta ve bu konuda siber suçlulukla mücadelede devletin yetersiz kaldığı eleştirileri yapılmaktadır. Alman İç İşleri Bakanlığı bu saldırılarla mücadele etmek amacıyla "Uzaktan Adli Yazılım" (Remote Forensic Software) adı verilen bir Trojan virüsü tasarlayarak, siber suç faili olduğundan şüphelenilen kişilerin bilgisayarlarına girme bunlar üzerinde uzaktan arama yapma konusunda çalışmalar yapmaya başlamıştır.[363]

"Online arama", "uzaktan arama" ve "federal trojan" olarak da isimlendirilen bu yöntem ile özellikle aşırılık yanlısı ve terörist gruplar olmak üzere, suçluların iletişimi, suçlarını planlamada ve işlemede interneti kullanmaları durumunda soruşturmalarda ortaya çıkan zorlukların giderilmesi hedeflenmiştir.[364]

Özel olarak tasarlanmış bir bilgisayar programı olan, "uzaktan adli yazılım" (Remote Forensic Software- RFS) aracı, şüphelinin bilgisi dışında bilgisayarına yerleştirilir. Bu program ile bilgisayarda depolanan tüm veriler kopyalanabilmekte ve ardından değerlendirme için soruşturma makamına geri aktarılabilmektedir. Uzaktan arama yöntemiyle soruşturma birimleri, bilgisayarın sabit diskinde ve çalışan belleğinde depolanan verileri arayabilmekte; şüphelinin, e-posta trafiğini, web'de gezinme alışkanlıklarını ve anlık mesajlaşmalarını izleyebilmektedir.[365]

1.3.2.2.2. İtalya

İtalyan ceza muhakemesi hukuku açısından doktrinde dijital unsurlar içeren soruşturmalara özel önem verilmesi gerektiği ileri sürülmüştür. Öyle ki gelişen teknoloji neticesinde her geçen gün bu tür soruşturmaların sayısı giderek artmaktadır ve bu soruşturmalar, bünyelerinde kendine has, üzerinde uzmanlaşma gerektiren konuları barındırmaktadır. Bu bağlamda öncelikle "dijital soruşturma" kavramının tanımlanması ve sınırlarının belirlenmesi gerektiği belirtilmiştir. Buna göre dijital soruşturmalar; *"işlenen suça bakılmaksızın, bilgi teknolojisi kullanan veya bilgisayar ve bilgi teknolojisi aracılığıyla dijital delil unsurlarının elde edilmesi"* şeklinde

[363] Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 73.
[364] Burkhard Schafer and Wiebke Abel, "The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822," *Scriptorium*, Volume 6, Issue 1 (April 2009): 108- 109.
[365] Schafer and Abel, "The German Constitutional Court," 109.

tanımlanabileceklerdir. Ancak İtalyan hukuk sisteminde henüz iyi tanımlanmış bir "dijital soruşturma" kavramının görülmediği belirtilmiştir.[366]

1993 yılında İtalyan yasa koyucu, İtalyan Ceza Muhakemesi Kanununda dijital delillerle ilgili ilk düzenlemeyi getirmiştir. Bu düzenleme ile İtalyan CMK m. 266 uyarınca telekomünikasyon ve bilgisayar sistemleriyle ilgili iletişim akışının dinlenmesi ve aranması hususu kanunlaştırılmıştır.[367]

İtalyan Ceza muhakemesi hukukunda, dijital soruşturma faaliyetleri, yeni tür soruşturma faaliyetleri olarak kabul edilmemiştir. Bunun yerine, dijital soruşturma faaliyetleri, normal soruşturmaların yürütülmesi sırasında alınması gereken teknik önlemler gibi ele alınmıştır. Bu bakımdan kanun koyucu özellikle şu hususlara önem vermiştir; İncelemeler, orijinal materyale dokunulmadan yürütülmelidir; araştırmanın yürütüldüğü orijinal materyalin kopyası ile orijinal materyalin aynı oldukları ispat edilmelidir; veriler kesinlikle değiştirilemeyecek şekilde saklanmalıdır.[368]

Bunlarla birlikte bu düzenlemede, bahsi geçen sonuçlara nasıl ulaşılacağı somut bir şekilde belirtilmemiştir. Bu sebeple kabul edilen görüş, uluslararası düzeyde onaylanan adli bilişimin "en iyi uygulamalarının" dijital soruşturmalarda kullanılması gerektiği şeklindedir.[369]

[366] Silvia Signorato, "Electronic Investigations in Italian Criminal Proceedings," *Law Series of the Annals of the West University of Timisoara*, vol. 2014, no. 1 (2014): 12.
[367] Signorato, "Electronic Investigations in Italian Criminal Proceedings," 18.
[368] Signorato, "Electronic Investigations in Italian Criminal Proceedings," 18- 19.
[369] Signorato, "Electronic Investigations in Italian Criminal Proceedings," 19.

BÖLÜM 2: CEZA MUHAKEMESİNDE DİJİTAL DELİLLERİN ELDE EDİLMESİ VE MUHAFAZASI

Dijital dünyaya özgü suçlar haricinde, dijital boyutu bulunan suçlar ile fiziksel dünyada gerçekleşen suçlar arasında, suçun gerçekleştiği ortam dışında büyük bir fark bulunmamaktadır. Elbette dijital suçların aydınlatılabilmesi için daha farklı yaklaşımlar gerekiyor olsa da temel itibariyle delil elde etme kuralları ve delillere ilişkin kurallar büyük farklılıklar göstermemektedir. Locard'ın "Değişim İlkesi"ne göre, iki öğe arasındaki temas, bir değişim ile sonuçlanacaktır. Bu ilke suç mahallindeki herhangi bir temas için de geçerlidir. Buna göre fail, mağdur, olay yeri ve başka insanlar arasında her zaman bir etkileşim olacaktır ve olay yerini terk eden bir kimsenin orada bulunduğuna dair iz bırakmaması ya da üstünde o ortamdan bir şeyler alıp götürmemesi mümkün olmayacaktır. Ancak elbette bu etkileşim her zaman kolayca tespit edilemeyecektir. Yine de unutulmamalıdır ki "delilin yokluğu, yokluğun delili değildir"[370]. Bu etkileşim hem fiziksel hem de dijital dünyalarda gerçekleşir ve bunun neticesinde bu dünyalar arasında bağlantılar kurulur. Nasıl ki fiziksel ortamda gerçekleştirilen her temas iz bırakmakta ise bilişim sistemleri üzerinde de dijital izler bırakmadan işlem yapmak imkânsıza yakındır.[371]

2.1. Genel Olarak Dijital Delillerin Elde Edilmesi ve Muhafazası

Dijital delillerin elde edilmesi sırasında kişisel verilerin korunması, düşünce açıklama ve yayma özgürlüğü, haberleşme özgürlüğü ve özel hayatın gizliliği gibi bazı temel insan hak ve özgürlüklerine müdahale edilmektedir. Bu bakımdan maddi olaya ilişkin dijital delillerin bütünüyle ve doğru bir şekilde olarak ve ayrıca elde edilen bilgilerin hukuka ve usullere uygun olarak elde edilmesinin sağlanması amacıyla özellikle Ceza Muhakemesi Kanunu olmak üzere bütün kanuni düzenlemeler, sürekli değişen ve gelişen teknolojinin ihtiyaçlarını irdeleyerek düzenlenmelidir.[372]

Elde edilen dijital delillerin incelenmesi ve yorumlanması sırasında bazı hatalar ortaya çıkabilmektedir. Örneğin dijital delillerin incelenmesi amacıyla kullanılan

---

[370] *"absence of evidence is not evidence of absence"* cümlesi, bir suç mahallinde mutlaka suçun nasıl, kim, ne zaman, nerede işlendiği gibi soruların cevabının bulunduğunu, iyi bir araştırmanın bu cevapların bulunmasını sağlayacağını vurgulamak amacıyla kullanılmıştır. Casey, *Digital Evidence,* 16; Casey, "Error, Uncertainty and Loss," 15.

[371] Casey, *Digital Evidence,* 16; Başlar, "Adli Bilişim," 48.

[372] Sarsikoğlu, "Elektronik Delil (E-Delil) Kavramı," 528.

araçlar, verileri yanlış temsil etmelerine neden olan hatalar içerebilir ve adli bilişim uzmanı bu sebeple verileri yanlış yorumlayabilir. Yahut bir adli bilişim uzmanın kanıtların nasıl değiştirildiğini bilmeden gerçekleştirdiği incelemeler neticesinde yanlış sonuçlara varabilir ve mahkemeyi hatalı sonuçlara yönlendirebilir.[373] Bu bağlamda dijital delillerle ilgilenen adli bilişim uzmanının çok dikkatli hareket etmesi gerekir.

Dijital delillerin elde edilmesi, onların toplanması, işlenmesi ve anlamlandırılması neticesinde bir bütün olarak delile dönüştürülmesi anlamına gelir. Bu bağlamda bilişim sistemlerinden delil elde edilmesinin beş farklı şekilde icra edilebileceği ifade edilmiştir.[374] Bunlar;

- Bilişim sisteminde arama yapılması ve gerekli dosyaların çıktılarının alınması.
- Bilişim sisteminde arama yapılması ve gerekli dosyaların dijital bir şekilde kopyalanması.
- Bilişim sisteminin, laboratuvara götürülmeksizin bulunduğu yerde kopyalanmasının sağlanması. (on- site)
- Bilişim sistemine el konulması ve adli bilişim laboratuvarlarında analiz yapılması. (off- site)
- Bilişim sistemlerine uzaktan erişilmesi suretiyle arama yapılması. (remote search)

Özetleyecek olursak, dijital delillerin elde edilmesi kavramını, birazdan bahsi geçecek olan ve uluslararası düzeyde kabul görmüş olan adli bilişim evrelerinin, adli bilişim uzmanı denetiminde, dijital delil üzerinde uygulanması şeklinde tanımlayabiliriz.[375]

İleride bahsi geçecek olan dijital delil elde etme yöntemlerine değinmeden önce burada kısaca Cumhuriyet Savcısının, genel soruşturma yetkisi çerçevesinde elde edebileceği dijital delillere de değinmek yerinde olacaktır. Buna göre Cumhuriyet savcısı CMK m.160 ve 161'e dayanan genel soruşturma yetkisi çerçevesinde yaptığı incelemeler ile dijital delillerin elde edebilecektir. Ancak bu yetki çerçevesinde dijital

[373] Casey, *Digital Evidence,* 28.
[374] Değirmenci, *Sayısal Delil,* 221- 222.
[375] Kaynakçıoğlu, "Dijital Deliller," 52.

deliller, ancak aşağıda bahsedeceğimiz koruma tedbirlerinin dışında kalan durumlarda Cumhuriyet Savcısı tarafından elde edilebilecektir.[376]

Son olarak bu bölümde dijital delillerin elde edilmesi konusunun iki açıdan ele alınacağını belirtmemiz gerekir. Bu bağlamda ilk olarak dijital delillerin elde edilmesinin teknik boyutunu oluşturan ve dijital delillere ilk müdahale anından, elde edilen delillerle ilgili hazırlanan teknik raporun mahkemeye sunulması anına kadar geçen süreci kapsayan adli bilişim ve teknikleri ele alınacaktır. İkinci olarak ise dijital delillerin elde edilmesinin hukuki boyutunu oluşturan ve adli bilişim teknikleri uygulanırken ve elde edilen deliller mahkeme tarafından değerlendirilirken uyulması gereken kuralların ceza muhakemesi hukuku boyutu ele alınmaya çalışılacaktır.

2.1.1. Dijital delillerin elde edilmesi ve adli bilişim

Dijital ortamda işlenen suçların veya dijital cihazların suçta araç olarak kullanılmasının artışı neticesinde dijital ortamlarda bulunan delillerin değeri artmış ve dijital deliller önem kazanmaya başlamıştır. Bilgisayar bağlantılı suçların artması sonucu adli bilişim bilimi bir uzmanlık ve bilim dalı olarak gelişmeye başlamıştır.[377] Dijital cihazlar aracılığıyla işlenen suçların tespiti amacıyla yapılan araştırmalar ve çalışmalar ise bilişim sistemleri ve elektronik cihazların dâhil olduğu adli olaylarda adli bilişim disiplinin oluşmasını sağlamıştır.[378] Bu bağlamda adli bilişim bilimi bir ispat vasıtası haline gelmiş ve ceza muhakemesi hukukunun bir parçasını oluşturmaya başlamıştır. Öyle ki adli bilişim, dijital deliller ile ceza muhakemesi hukukunun ortak paydasını oluşturmuş[379] ve sonuçta dijital delillerin, muhakeme sürecine dahil edilebilmesi, adli bilişim bilimi sayesinde mümkün olabilmiştir.[380]

Soruşturma veya kovuşturma konusu suç fiilinin, bünyesinde dijital verileri barındırdığı durumlarda, adli bilişim biliminin karşımıza çıkacağını belirtmiştik. Çünkü dijital materyallerden veri elde edilmesi ve bu verilerin anlamlandırılarak delil haline getirilmesi süreci, teknik bilgi gerektiren ve teknolojik cihazlar kullanılması suretiyle gerçekleştirilebilen bir süreçtir. Bu noktada adli bilişim süreci ne kadar sağlıklı gerçekleştirilirse o kadar sağlıklı dijital deliller elde edileceğini söyleyebiliriz.

---

[376] Değirmenci, *Sayısal Delil,* 387.
[377] Casey, *Digital Evidence,* 9- 10.
[378] Önel ve Irmak, "Dijital delillerin windows işletim sistemi üzerinde incelenmesi," 1187.
[379] Arslan, "Hukuk Öğretiminde Adlî Bilişim" 83.
[380] Börekçi, "Bilgisayarlarda, Bilgisayar Programlarında," 31; Emekci, Kuğu ve Temiztürk, "Bulut Bilişim," 10.

Dijital delillerin elde edilişi konusuna ileride değinilmekle birlikte hukuka aykırı bir şekilde elde edilen delillerin, hükme esas alınamayacağını belirtmek yanlış olmayacaktır. Bu bakımdan dijital delillerin elde edilişi sürecinin de hukuka uygun olması gerektiğini söylememiz gerekir. İşte bu noktada karşımıza adli bilişimin önemi çıkmaktadır. Sonuç itibariyle sağlıklı ve düzgün yürütülmeyen bir adli bilişim sürecinden elde edilen çıktılar, delil niteliğini haiz olamayacaklardır.

Önceleri delillerin incelenmesi sırasında kâğıt dokümanlar talep edilmekteydi ve muhakeme sürecinde soruşturma ve kovuşturma görevi yapan hâkim ve savcılar da bu geleneği devam ettirerek "kâğıt sistemi"ni uygulamaktaydılar. Ancak, teknolojik gelişmeler ve suç işlenirken bilişim sistemlerinin yoğun bir biçimde kullanılması, kâğıdın dışında, bilişim sistemlerinde ve bunların parçalarında yapılacak incelemeleri zorunlu hale getirmiştir. İşte suç delillerinin bir kısmının bilgisayar ve diğer elektronik cihazlar üzerinde bulunması ve bunların keşfedilme ihtiyacı neticesinde, en yaygın delil bulma yöntemlerinden biri olarak adli bilişim bilim dalı ortaya çıkmıştır.[381]

Adli bilişim terimi İngilizce "computer forensics" kelimesinin karşılığı olarak kullanılmaktadır. Bilgisayar anlamına gelen "computer" ile "mahkemeye ait, adli" anlamlarına gelen "forensics" kelimelerinin bir araya gelmesinden türetilen bu terim Türkçeye birebir çevrildiğinde "bilgisayar adli bilimi" anlamına gelmektedir. Geçmişte, dijital delillerin birincil kaynakları bilgisayarlar olarak görüldüğü için *computer forensics* kelimesi tercih edilmiştir. Bununla birlikte bu kavramın karşılığı olarak genellikle "adli bilişim" ifadesi kullanılmaktadır.[382]

Buna karşılık günümüzde özellikle son yirmi yılda teknolojik evrim yavaş yavaş mobil cihazlara doğru kaymış ve iletişim küresel bir boyut kazanmıştır. Bu sebeple giderek daha yeni ve daha karmaşık cihazların ve sistemlerin kullanımı yaygınlaşmaya başlamıştır. Yalnızca *Nesnelerin İnterneti (IoT- Internet of Things)*nin gelişimini göz önünde bulundurulduğunda bile, akıllı saat, televizyon gibi cihazların yaygınlaşması, bulut depolama sistemlerinin artan kullanımı ve sanal para birimlerinin (Bitcoin gibi) kullanımı oldukça popüler hale gelmiştir.[383] Elbette adli bilişimin de bu değişime ayak uydurması gerekliliği ortaya çıkmıştır.

[381] Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 44.
[382] Arslan, "Hukuk Öğretiminde Adlî Bilişim" 83; Başlar, "Adli Bilişim," 49.
[383] Biasiotti, v.d., "Introduction: Opportunities," 7.

Computer forensics, cyber forensics, forensic computing gibi adli bilişime işaret eden ifadelerin, yukarıda da belirtildiği üzere günümüzde dijital verilerin birçok ortamda üretilebildiği, işlenebildiği, tutulabildiği ve elde edilebildiği düşünüldüğünde yetersiz kaldıkları belirtilmiş ve daha kapsayıcı bir kavram olarak "digital forensics" ifadesinin kullanılması gerektiği ileri sürülmüştür.[384]

Tüm bu tanımlardan yola çıkarak adli bilişim biliminin, muhakemeye konu olan maddi olayın ne şekilde gerçekleştiğini, dijital delillerden istifade ederek ve bilimsel esaslara uygun olarak, ortaya koyan bir bilim dalı olarak karşımıza çıktığını söyleyebiliriz.[385]

2.1.1.1. Adli bilişimin tanımı

Adli bilişim, yürütülen yasal soruşturmayla ilgili adli sorunları ele almak amacıyla dijital bilgilerin teşhis edilmesi, korunması, elde edilmesi ve analizi ile ilgilenen bir disiplindir.[386] Bu bağlamda oldukça teknik bir alandır ve bu nedenle bünyesinde bilgisayar, matematik fizik ve benzeri bilimleri barındırır. Ayrıca özellikle elektrik, makine ve sistem mühendisliği bilgisi gerektiren bir disiplindir.[387]

Adli bilişim geçmişten günümüze çeşitli özelliklerine göre farklı açılardan birçok defa tanımlanmıştır. Bu tanımların incelenmesi, adli bilişim uzmanlarının görevlerinin sınırının çizilmesi bakımından önem arz etmektedir. Çizilen bu sınır aynı zamanda delilin hukuka uygunluğunun sınırlarını da belirleyecektir.

İlk yapılan tanımlardan birine göre adli bilişim, dijital delillerin hukuki olarak kabul edilebilir bir şekilde tanımlanması, korunması, analiz edilmesi ve sunulması sürecini ifade etmektedir.[388] Yine benzer tarihli bir diğer tanıma göre adli bilişim, potansiyel delillerin belirlenmesi adına bilgisayar araştırma ve analiz tekniklerinin uygulandığı bir disiplini ifade etmektedir.[389] Yapılan bu ilk tanımlamalar incelendiğinde öncelikle adli bilişim süreçlerinde (tanımlama, inceleme, analiz,

---

[384] Rohit Tamma, v.d., *Practical Mobile Forensics: Forensically investigate and analyze iOS, Android, and Windows 10 devices* (UK: Packt Publishing Ltd, Fourth Edition, 2020), 7; Emekci, Kuğu ve Temiztürk, "Bulut Bilişim," 10; Başlar, "Adli Bilişim," 49.
[385] Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj)," 50.
[386] Biasiotti, v.d., "Introduction: Opportunities," 6.
[387] Ryan and Shpantzer, "Legal aspects of digital forensics," 2.
[388] Rodney McKemmish, "What is forensic computing?," *Australian Institute of Criminology Trends & issues in crime and criminal justice*, Vol. 118 (1999) 1.
[389] Scott M. Giordano, "Electronic Evidence and the Law," *Information Systems Frontiers*, vol. 6:2 (2004): 162.

raporlama gibi) uygulanan tekniklerin bilimselliği belirtilmiş ve devamında bu tekniklerin üzerinde uygulanacağı verilerin öncelikle hukuka uygun bir şekilde elde edilmiş olmaları gerekliliği vurgulanmıştır.

Başka bir tanıma göre 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 belgeleme süreçlerinin bütünü…"* şeklinde tanımlanmıştır.[390]

Bu tanım incelendiğinde toplanan verilerin hukuka uygun bir şekilde elde edilmeleri gerekliliği benzer ifade edilmiş olmakla birlikte, dijital verilerin, bulunabilecekleri ortamlar sayma yöntemiyle belirtilerek, adli bilişim yöntemlerinin üzerinde uygulanacağı cihazlar vurgulanmaya çalışılmıştır. Adli bilişim uzmanlarının görev alanlarının sınırlarının çizilmesi bakımından cihazların sayılması kanımızca doğru olmakla birlikte eksik bir düşüncedir. Öyle ki muhakemeye konu suç fiilinin aydınlatılmasında kullanılabilecek dijital verilerin bulunabilecekleri ortamlar, özellikle günümüzde sayma yöntemiyle ele alınamayacak kadar artmıştır. Bu bağlamda adli bilişim yöntemlerinin üzerinde uygulanacağı cihazların tek tek sayılması yerine, genel anlamda *elektronik veri barındıran* cihazlar şeklinde kapsayıcı bir şekilde belirtilmesinin daha doğru olacağını düşünmekteyiz.

Son olarak ise bir başka tanıma göre adli bilişim, bir yargılama sırasında kullanılabilecek potansiyel delillerin belirlenmesi için bilişim sistemlerinin kullanıldığı ve aranan bilişim sistemindeki delillere ilk temas edildiği andan yargı makamlarının önüne getirilmesi anına kadar geçen sürecin bütünüdür.[391] Bu tanımda ise adli bilişim sürecinin zamansal olarak başlangıcı ve sonu belirtilmiştir. Buna göre adli bilişim süreci, ilgili cihazdaki veriye ilk temas anından itibaren başlamakta ve incelemeler sonucu hazırlanan raporun yargı makamlarının önüne getirilmesi anında bitmektedir. Bu bağlamda elde edilen verilerin sağlamlığının ve bütünlüğünün korunması gereken sürenin, başka bir ifadeyle muhafaza altında tutulması gereken sürenin de sınırları belirtilmiştir. Ancak bir ekleme yapacak olursak, adli bilişim süreci, ilgili delillere dayanılarak hazırlanan raporun mahkemeye sunulması anına

[390] Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 44- 45.
[391] Başlar, "Adli Bilişim," 50-51.

kadar değil fakat sanık veya şüpheli hakkında mahkeme tarafından kesin bir hüküm tesis edilinceye kadar devam etmelidir. Öyle ki masumiyet karinesi gereğince kişi hakkında bir kesin hüküm tesis edilinceye kadar, o kişinin lehine veya aleyhine elde edilen dijital deliller ve bunları barındıran cihazlar saklanmalı, korunmalı ve talep halinde tekrardan incelemeye konu edilebilmelidir. Çünkü sanık hakkında elde edilen dijital delillerle ilgili mahkemeye bir rapor sunulmuş olsa dahi hâkim kovuşturmanın sonuna kadar aynı cihazların tekrar aynı şekilde yahut farklı açılardan incelenmesini isteyebilecektir.

Kısaca bilim ve hukukun bir sentezi olan ve bilim ve mühendisliğin dijital delillere uygulanması sonucu elde edilenler[392] şeklinde tanımlayabileceğimiz adli bilişimi yukarıda anılanlar çerçevesinde biz de tanımlayacak olursak: Adli bilişim, bir suç fiili ile bağlantısı olan, her tür elektronik ortamda yer alabilen verilere ilk temas anından şüpheli veya sanık hakkında kesin bir hüküm tesis edilinceye kadar süren, ele geçirilen verilerin, alanında uzman kişilerce uygulanan bilimsel teknikler neticesinde hukuka uygun bir şekilde elde edilmesi, anlamlandırılması, analiz edilmesi ve raporlanması neticesinde bir delile dönüştürülmesi süreçlerinin bütününü ifade etmektedir. Sonuç olarak adli bilişimin, *"hukukun, delil elde etme konusunda bilişimle ilgili meseleler konusunda yardım alacağı bir uygulamalar bütünü"* olduğu sonucuna varabiliriz.[393]

2.1.1.2. Adli bilişimin alt disiplinleri

Hızlı ve sürekli olarak evrimleşen teknoloji, adli bilişimin alt disiplinlerinin oluşmasına ve bunların da aynı hızla gelişmesine neden olmuştur. Birkaç öne çıkan alt disiplin şu şekilde sayılabilir;[394]

Bilgisayar Adli Bilişimi (Computer forensics)- dosya sistemlerinin, işletim sistemlerinin ve uygulamaların adli analizi için yazılım araçlarını içeren disiplindir.

---

[392] Tony Sammes and Brian Jenkinsen, *Forensic Computing: A Practitioners Guide* (London: Springer-Verlag, Second Edition, 2007), 1. Aktaran: Jasmin Ćosić, Zoran Ćosić, Miroslav Bača, "An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence," *Journal Of Information And Organizational Sciences*, vol. 35, no. 1 (2011) 3.
[393] Kaynakçıoğlu, "Dijital Deliller," 53.
[394] Casey, *Digital Evidence,* 38; Biasiotti, v.d., "Introduction: Opportunities," 7; Emekci, Kuğu ve Temiztürk, "Bulut Bilişim," 11; Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 45- 46.

Ağ Adli Bilişimi (Network forensics)- ağ trafiğinin analiz edilmesi ve dijital verilerin gerçek zamanlı olarak incelenmesi ile ilgilenen disiplindir.[395,396] Bu bakımdan, ağda gerçekleşen olayların yakalanması, kaydedilmesi ve analiz edilmesi işlemi, ağ adli bilişiminin alanına girmektedir.[397]

Mobil Cihaz Adli Bilişimi (Mobile device forensics)- mobil cihazların analiz edilmesi ve mobil cihazlardan delil elde edilmesi ile ilgilenen disiplindir.[398]

Zararlı Yazılım Adli Bilişimi (Malware forensics)- zararlı yazılımları (ör; fidye yazılımı[399], truva atı yazılımı[400], casus yazılım gibi[401]) inceleyen disiplindir. Bu bağlamda zararlı yazılım adli bilişimi, bünyesinde bir zararlı yazılım bulunduran

[395] Chaikin, "Network investigations," 243.
[396] Bulutta yer alan delillerin analiz edilmesi ile ilgilenen *"Bulut Adli Bilişimi (Cloud Forensics)",* bulutların ağlardan ve ağa bağlı cihaz ve sistemlerden oluşan yapısı nedeniyle ağ adli bilişiminin (network forensics) bir alt disiplini olarak kabul edilmektedir. Emekci, Kuğu ve Temiztürk, "Bulut Bilişim," 11.
[397] Ahmad Almulhem and Issa Traore, "Experience with Engineering a Network Forensics System," *Lecture Notes in Computer Science*, vol. 3391 (2005): 2.
[398] Tamma, v.d., *Practical Mobile Forensics,* 8.
[399] Fidye yazılımı (Ransomware), örneğin tehlikeli bir internet sitesi adresine tıklanılarak aktif hale getirilen ve bilgisayarı kilitleyen zararlı bir yazılımdır. Bu yazılım ile bilişim sisteminde yer alan tüm kişisel veriler kullanıcı tarafından kullanılamaz hale gelir. Kriptografik şekilde tüm verileri şifreleyen bu yazılımın ortadan kaldırılması ise, elinde şifrelerin anahtarı bulunan siber suçlu aracılığıyla yapılabilmektedir. Siber suçlular da takip edilebilirliği çok zor olması bakımından bu şifre çözme işlemini ortalama 1 bitcoin yapmaktadırlar ki çoğunlukla yalnızca parayı alıp ortadan kaybolmaktadırlar. Avrupa Polis Teşkilatı (EUROPOL) ve bazı endüstri ortaklarından oluşan bir çalışma grubu fidye yazılımlarına tepki olarak https://www.nomoreransom.org/tu/index.html (son erişim; 11.01.2022) internet sitesini oluşturmuştur. Bu site, fidye yazılımlarına karşı bir farkındalık oluşturma çabası ile birlikte kurbanların fidye ödemeden bilişim sistemlerinin şifresini çözmelerine yardımcı olmak amacıyla kurulmuştur. Ayrıca bu zamana kadar şifreleri çözülmüş bazı fidye yazılımları hakkında bilgiler de sitede yer almaktadır. Drewer and Ellermann, "The Online Environment as a Challenge," 142- 143.
[400] Truva Atı yazılımı, virüslü bir bilgisayarın uzaktan kontrol edilmesini sağlar. Kötü niyetli üçüncü taraf bilgisayar korsanları (hacker), sahibinin bilgisi dışında bir bilgisayara önceden yüklenmiş olan casus yazılımları veya reklam yazılımlarını rutin olarak tarar ve ardından yasa dışı görüntüler içeren dosyaları yükler. Ek olarak bilgisayar üzerinde yapılan inceleme sonucunda Truva Atı programının izine rastlanmaması gerçekçi olmayabilir çünkü yetenekli bir bilgisayar korsanı bir Truva Atı'nın kanıtlarını kaldırma yeteneğine de sahiptir. Chaikin, "Network investigations," 250.
[401] Casus yazılım (Spyware) Kullanıcının haberi olmadan birinin internet geçmişi veya şifreleri gibi kişisel bilgilerini toplayan zararlı bir yazılımdır. (https://dictionary.cambridge.org/dictionary/english/spyware son erişim: 11.01.2022.). Fidye yazılımları gibi aktif edilmesi için yine bir internet sitesi adresine tıklanılmasının yeterli olduğu casus yazılımlar; izinsiz bir şekilde uzaktan eriştiği bilişim sisteminin kullanıcısının, şifrelerine, fotoğraflarına vs. erişebilmekle birlikte bilişim cihazının mikrofonunu ve kamerasını da açıp kapatabilir hale gelmektedir. Dahası önceleri yalnızca masaüstü bilgisayarlar için bir tehdit olan casus yazılımlar, günümüzde akıllı telefonlar için de giderek artan bir sorun haline gelmektedir. Drewer and Ellermann, "The Online Environment as a Challenge," 143.

bilişim sistemlerinden nasıl veri toplanacağı ve uçucu verilerin nasıl korunacağı konusu ile ilgilenmektedir.[402]

Bellek Adli Bilişimi (Memory Forensics)- RAM belleği ve hazırda bekletilen dosyalarının analizi ile ilgilenen disiplindir. Bu bağlamda bellek adli bilişimi, bellek dökümlerinde ve işletim sistemlerinde depolanan verilerin elde edilmesi ile konusu ile ilgilenmektedir.[403]

2.1.1.3. Adli bilişimin amacı

Adli analizin temel taşı nesnelliktir. [404] Delillerin yorumlanması ve sunulması, karar vericilere gerçekler hakkında mümkün olan en açık görüşü sağlamak için önyargıdan uzak olmalıdır. Objektif kalabilmek için yapılabilecek en iyi yaklaşım, delillerin mümkün olduğunca kendisi için konuşmasına izin vermektir. Adli bilişim incelemesi ile herhangi bir kişinin suçlu ya da masum gösterilmesi hedeflenmez. Aksine inceleme neticesinde elde edilen tüm dijital deliller, adli birimlere eksiksiz ve tarafsız bir biçimde sunulmalıdır.[405]

Adli bilişimin temel amacı, elde edilen veriler ile muhakeme konusu olay arasındaki veya muhakeme konusu suç fiili ile işlenen veriler ve kullanıcı arasındaki bağlantıyı ortaya koymaktır.[406]

Bu amaç doğrultusunda araç olarak birçok disiplinden faydalanılmaktadır. Dijital deliller, fiziksel deliller gibi doğrudan elde edilip değerlendirilememektedirler. Bunun için birtakım teknik donanım ve yazılımlara ihtiyaç duyulmaktadır. Bu ihtiyaçlar da adli bilişimin gelişmesini teşvik etmektedir. Zira uyuşmazlığı ortaya koymaya yarayacak deliller, çoğunlukla elektronik araçlar üzerinde yer almaktadır ve bilişim teknolojisi kullanılarak elde edilmektedir.[407]

Adli bilişim süreci genellikle olay yerinde kolluk birimleri tarafından ve sonrasında da bilirkişiler tarafından (çoğu zaman laboratuvar ortamında) yerine getirilmektedir.[408] Adli bilişim süreci sonunda görünmez nitelikte olan dijital delil,

---

[402] Cameron H. Malin, Eoghan Casey and James M. Aquilina. *Malware Forensics: Investigating and Analyzing Malicious Code* (USA: Elsevier Inc., 2008), 2.
[403] Malin, Casey and Aquilina, *Malware Forensics,* 122.
[404] Casey, *Digital Evidence,* 24.
[405] Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 45.
[406] Başlar, "Adli Bilişim," 52; Henkoğlu, *Adli Bilişim,* 1.
[407] Arslan, "Hukuk Öğretiminde Adlî Bilişim" 83.
[408] Henkoğlu, *Adli Bilişim,* 22.

görünür ve anlaşılır hale getirilir ve bu süreç içerisinde bir dijital delilin sonradan değiştirilip değiştirilmediği veya tahribata uğrayıp uğramadığı da saptanır.[409] Bu bağlamda adli bilişim uzmanlarının, tüm bu görevlerini düzgün bir şekilde yerine getirmelerine, bilimsel gerçeği bulmalarına ve nihayetinde elde ettiklerinin mahkemede delil olarak kabul edilmesine yardımcı olması amacıyla bilimsel bir metodolojiye ihtiyaçları olacaktır.

2.1.1.4. Adli bilişimin yöntemleri (metodoloji)

Adli bilişim süreci, kısaca, yargı makamları tarafından suç ve suçlunun tespitinde gerekli olabilecek dijital deliller ile ilgili kolluk kuvvetleri veya diğer uzman görevliler tarafından yürütülen adli bilişim çalışmalarının bütünü şeklinde açıklanmıştır. Bu süreçte temel olarak hedeflenen soruşturma sürecinin başından kovuşturma sürecinin sonuna kadar geçen süreçte, hukuka uygun bir şekilde dijital delillerin elde edilmesi, bütünlüğünün korunması ve doğru şekilde muhafaza edilmesi suretiyle yargı makamlarına bir rapor eşliğinde sunulmasıdır.[410] Elbette gerçekleştirilen bu adımlar, rastgele bir şekilde değil fakat uluslararası alanda kabul edilen ve teknolojik gelişmelere uygunluk açısından en güncel olan kuralların takip edilmesi suretiyle atılmalıdır. Bu noktada da karşımıza süreç modelleri çıkmaktadır.

Süreç modelleri ya da başka bir deyimle metodolojiler, eğitim ve araştırmaları yönlendirmek için bir çerçeve oluşturur ve genel kabul görmüş uygulamaların performanslarını ve güncelliklerini kıyaslamak için alanın durumu ve doğası üzerine düşünmek için faydalı referans noktaları sağlarlar.[411] Formüle edilen bir metodoloji kullanmak, eksiksiz ve titiz bir soruşturmayı teşvik eder, elde edilen verilerin uygun şekilde işlenmesini sağlar ve önyargılı teoriler, zaman baskısı ve diğer potansiyel tuzaklar tarafından yaratılan hata olasılığını azaltır. Etkili bir metodoloji, hedeflere ulaşmak için gerekli adımları tanımlar ve gelecekte dijital delil kaynağı haline gelebilecek yeni teknolojilere de uygulanabilir.[412]

---

[409] Ünal, "Bilgisayarlarda Bilgisayar Programlarında," 21.
[410] Yazar adli bilişim sürecini; delile ilk müdahale aşaması, delillerin toplanması ve güvenirliği, delillerin muhafaza edilmesi ve taşınması ve delillerin raporlanması şeklinde dört adıma ayırmış ve detaylandırmıştır. Bkz. Önel ve Irmak, "Dijital delillerin windows işletim sistemi üzerinde incelenmesi," 1189.
[411] Ülkemizde metodoloji ile ilgili sayı itibariyle fazla çalışmaya rastlanmasa da belli bazı çalışmalar göze çarpmaktadır. Bu konuda bkz. Yılmaz ve Çakır, "Mobil Cihaz Adli Bilişimi Süreçleri," 24-45.
[412] Casey, *Digital Evidence,* 188.

Yeni ve farklı metodoloji geliştirme motivasyonları çoktur. Öncelikle bilişim teknolojilerindeki yaşanan gelişmeler, her bir donanım ve yazılım için farklı yaklaşımların sergilenmesini gerektirmektedir. Bu noktada her bir donanım ve yazılım bakımından farklı metodolojiler geliştirilmektedir. İkinci olarak bilişim suçu faillerinin, suç delillerinin tespitini ve ortaya çıkarılmasını önleme amacıyla geliştirdikleri yöntemlerin etkisiz kılınması amacıyla gösterilen gayretler de çeşitli metodolojilerin geliştirilmesine vesile olmuştur.[413]

Ek olarak dijital delillerin hükme esas alınabilmesi bakımından bilimsel esaslara uygun olarak elde edilmesi gerekliliği de değerlendirildiğinde, metodolojilerin, adli bilişim uzmanının delil elde etme sürecinde uyması gereken adımları belirlemesi ve ayrıca, adli bilişim uzmanları tarafından tartışılarak, eleştirilerek oluşturulmaları, delilin bilimselliğinin tespitine katkı sağlayacaktır.[414]

Sonuç olarak, bu süreç modelleri dikte etmek için değil, dijital araştırmalara hizmet etmek içindir. Her araştırma benzersizdir ve öngörülemeyen zorluklar getirebilir, bu nedenle süreç modelleri ve diğer metodolojiler bir son nokta olarak değil, üzerine inşa edilecek bir çerçeve veya temel olarak görülmelidir.[415]

Hazırlanan ilk metodolojilerden biri uyarınca dijital delil incelemesi şu dört aşamayı içermelidir; dijital delilin tanımlanması, dijital delilin korunması, dijital delilin analizi, dijital delilin sunumu. (The identification of digital evidence, The preservation of digital evidence, The analysis of digital evidence, The presentation of digital evidence.)[416] Yapılan bu metodolojinin, terminoloji ve ayrıntılardaki farklılıkları dikkate alınmaksızın, dijital araştırmalarda bir temel olabileceği ileri sürülmüştür.[417]

İlgili aşamaları tanımlayacak olursak;[418]

Dijital delilin tanımlanması- Hangi delilin mevcut olduğunu, nerede saklandığını ve nasıl saklandığını bilmek, geri kazanımını kolaylaştırmak için hangi süreçlerin kullanılacağını belirlemek için hayati önem taşır.

---

[413] Değirmenci, *Sayısal Delil,* 162.
[414] Değirmenci, *Sayısal Delil,* 164.
[415] Casey, *Digital Evidence,* 188; Değirmenci, *Sayısal Delil,* 163.
[416] McKemmish, "What is forensic computing," 1-2.
[417] Casey, *Digital Evidence,* 188- 189.
[418] Casey, *Digital Evidence,* 189- 190.

Dijital delilin korunması- Sistemin ağ üzerinden yalıtılması, ilgili günlük dosyalarının güvence altına alınması ve sistem kapatıldığında kaybolacak uçucu verilerin toplanması dahil olmak üzere dijital delilin yaşayabileceği değişikliklerin yerinde önlenmesi yahut veri değişikliklerinin kaçınılmaz olduğu durumlarda en az miktarda değişikliğin meydana gelmesinin sağlanması önem arz eder. Değişimin kaçınılmaz olduğu durumlarda, değişimin doğasının ve nedeninin açıklanabilmesi esastır.

Dijital delilin analizi- Dijital verilerin çıkarılması, işlenmesi ve yorumlanması, aşamalarından oluşan analiz aşaması genel olarak adli bilişimin ana unsuru olarak kabul edilir. Elde edilen dijital delillerin okunabilir hale getirilmesi işlenme ve dolayısıyla analiz aşamasıyla gerçekleşir.

Dijital delilin sunumu- analiz aşamasın sonrası elde edilen bulguların, yargı makamlarınca anlaşılır hale getirilmesi aşamasıdır.

Bir başka metodoloji önerisi ise dijital soruşturma sürecini, fiziksel suç mahalli ile ilişkili daha yerleşik soruşturma süreciyle ilişkilendirerek, bilgisayarı veya dijital aygıtın kendisini bir olay yeri olarak kavramsallaştırarak kendini farklı kılmıştır.[419] Carrier tarafından ele alınan *"Entegre Dijital Soruşturma Süreci modeli",* Hazırlık, Dağıtım, Fiziksel Olay Yeri İnceleme, Dijital Olay Yeri İnceleme ve Değerlendirme olmak üzere beş gruptan ve on yedi aşamadan oluşmaktadır.[420]

Söz konusu metodoloji, fiziksel olay yeri ile dijital olay yeri arasında farklar bulunduğu ve bu sebeple dijital olay yerlerine, fiziksel olay yeri gibi bakılmaması gerektiği gerekçesiyle eleştirilmiştir. Buna göre fiziksel olay yerinin aksine dijital olay yeri ancak çeşitli işletim sistemi ve adli araçlar da dahil olmak üzere çeşitli soyutlama katmanları aracılığıyla görülebilmektedir. Bununla birlikte dijital olay yerleri, fiziksel olanlardan daha yüksek derecede titizlik ve özgünlükle aranabilmektedir. Öyle ki fiziksel olay yeri ekiplerinin tüm suç mahallini moleküler düzeyde kopyalayıp araştırmaları mümkün değildir. Ancak bir dijital olay yeri, özellikleri daha sonra incelenmek ve analiz edilmek üzere birebir ve tam bir şekilde kopyalanabilir ve incelemeler bu kopyalar üzerinden gerçekleştirilebilir.[421]

---

[419] Brian Carrier and Eugene H. Spafford "Getting Physical with the Digital Investigation Process," *International Journal of Digital Evidence,* Volume 2, Issue 2 (Fall 2003): 1.
[420] Carrier and Spafford, "Getting Physical," 6.
[421] Casey, *Digital Evidence,* 191- 192.

Üçüncü olarak bir metodoloji önerisi, dijital soruşturma sürecini, hazırlık, alanı inceleme, belgeleme, koruma, inceleme ve analiz, yeniden inşa, raporlama olmak üzere yedi bölüme ayırmaktadır. Burada önceki metodolojilerden farklı olarak yeniden inşa aşaması da sürece eklenmiştir. Bu aşamanın; ne oldu, olaya kim sebep oldu, olay nerede, nasıl ve ne şekilde gerçekleşti gibi sorulara cevap verilmesi bakımından önem arz ettiği ve bu aşamanın sonunda, gerçekleşen vakanın daha da eksiksiz bir resminin ortaya çıkarılabileceği ileri sürülmüştür. [422]

Dördüncü ve son olarak Amerika Birleşik Devletleri örneğini verebiliriz. Yukarıda belirtildiği üzere ABD, dijital delillerin elde edilmesi ve değerlendirilmesi konusunda uygulamacılara öncülük etmesi açısından çeşitli kılavuzlar yayınlamıştır. Bunlardan "Elektronik Olay Yeri İncelemesi: İlk Müdahaleciler İçin Bir Kılavuz"[423] içerisinde dijital delillerin; toplanması, incelenmesi, analizi ve raporlanması aşamalarını içeren dört aşamadan oluşan bir süreç tanımlanmıştır. Buna göre dijital delillerin, toplanması: dijital delillerin arandığı, tanındığı, toplandığı ve belgelendiği; incelenmesi: delilin görünür hale getirildiği, kökeninin ve öneminin açıklandığı, bilgilerin arandığı ve gereksiz verilerin azaltıldığı; analiz edilmesi: inceleme sonrasında çıkan ürüne vaka için önemi ve delil değeri açısından bakıldığı ve son olarak raporlanması: inceleme sürecini ve kurtarılan ilgili verilerin özetlendiği aşama olarak tanımlanmaktadır. [424]

Söz konusu metodolojiler bunlarla sınırlı kalmamakla birlikte[425] pratikte, çoğu dijital soruşturmanın doğrusal bir şekilde ilerlemediği ve bahsi geçen adımların birbirinden düzgün bir şekilde ayrılmamış olduğu unutulmamalıdır. Soruşturma sürecinin tüm adımları genellikle iç içedir ve dijital bir araştırmacı, vakanın daha rafine bir şekilde anlaşılması ışığında adımları tekrar gözden geçirme ihtiyacı duyabilecektir.[426] Örneğin hazırlık aşaması yalnızca başlangıçta ayrı bir adım

[422] Casey, *Digital Evidence,* 466- 499.
[423] U.S. Department of Justice Office of Justice Programs, "Electronic Crime Scene Investigation: A Guide for First Responders", US National Institute of Justice, Washington, USA, July 2001, https://www.ojp.gov/pdffiles1/nij/219941.pdf son erişim: 03.12.2021.
[424] Toplama: dijital delillerin arandığı, tanındığı, toplandığı ve belgelendiği; İnceleme: delilin görünür hale getirildiği, kökeninin ve öneminin açıklandığı, bilgilerin arandığı ve gereksiz verilerin azaltıldığı; Analiz: inceleme sonrasında çıkan ürüne vaka için önemi ve delil değeri açısından bakıldığı ve son olarak Raporlama: inceleme sürecini ve kurtarılan ilgili verilerin özetlendiği aşama olarak tanımlanabilir. Buzarovska Lazetik and Koshevaliska, "Digital Evidence in Criminal Procedures," 74-75.
[425] Daha detaylı bilgi için bkz. Casey, *Digital Evidence,* 187-197.
[426] Casey, *Digital Evidence,* 201-202.

olmaktan ziyade, araştırmanın her adımında yinelenmelidir. Yahut raporlama aşaması analiz aşaması sonrasında değil fakat inceleme ve analiz aşamalarında senkronize bir şekilde yerine getirilmelidir.

Burada önemli olan bir metodoloji belirlenmesi ve bu metodolojinin, bilimsel yöntemlerle ortaya çıkartılmasıdır[427] ki bu husus da ilgili metodolojilerin, gelişen teknolojiye uyum sağlamasını kolaylaştıracaktır.

2.1.1.4.1. Adli bilişim yöntemlerinin standart hale getirilmesi

Yukarıdaki araştırmalar neticesinde dijital delillerin soruşturma ve kovuşturma makamlarınca kullanılması sürecinin, tam bir standardizasyona sahip olmadığını söyleyebiliriz. Bu konuda ISO tarafından geliştirilen standartların, standardizasyonu sağlama kapasitesine sahip olabileceği belirtilmiştir.[428]

Dijital delillerin, hukuki ve cezai davalarda kullanılması konusunda güvenilirliğinin ve delil olarak kabul edilebilirliğinin sağlanması adına Uluslararası Standardizasyon Örgütü (ISO- International Organization for Standardization) ve Uluslararası Elektroteknik Komisyonu (IEC- International Electro-technical Commission); çeşitli standartlar ortaya koymuştur. Bunlardan ISO/IEC 27041 ve 27043 standartları, dijital delillerin elde edilmesinin planlanmasından, delillerin raporlanması ve vakanın kapatılmasına kadar tüm sürecin kontrolü ve yeterliliği için tavsiyeler sunmakla birlikte, sürecin alt adımları, 27035-2, 27037 ve 27042 standartlarında kılavuz ve tavsiyeler sunmaktadır.[429]

Buna göre ISO/IEC 27035-2 standardı, olaya ilk müdahale için planlama ve hazırlık ilkelerini; ISO/IEC 27042 standardı dijital delillerin, analizi ve yorumlanması için tavsiyeleri; ISO/IEC 27037standardı ise dijital delillerin belirlenmesi, edinimi, bir araya getirilmesi ve korunması hakkında ilkeleri içermektedir.[430]

ISO/IEC 27037, dijital delillerin bütünlüğünü ve özgünlüğünü korumak için uyumlu ve küresel olarak kabul görmüş bir metodoloji sağlamakla birlikte yargı alanları arasında dijital delillerin değiş tokuşunu kolaylaştırmayı ve potansiyel dijital

---

[427] Casey, *Digital Evidence,* 202.
[428] Nursel Yalçın ve Berker Kılıç, "ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042 ve ISO/IEC 27043 Standartlarına Göre Sayısal Kanıtlar", *4th International Symposium on Innovative Approaches in Engineering and Natural Sciences Proceedings,* ISAS (WINTER-2019): 445.
[429] Yalçın ve Kılıç, "ISO/IEC 27037," 445.
[430] Yalçın ve Kılıç, "ISO/IEC 27037," 445; Başlar, "Adli Bilişim," 60.

delillerin tanımlanması, toplanması, elde edilmesi ve korunmasından sorumlu kişilere rehberlik sağlamayı amaçlamaktadır.[431]

Söz konusu standart uyarınca dijital delilin tanımlanması, toplanması, elde edilmesi ve korunmasından sorumlu kişiler; ilk müdahale görevlileri, dijital delil uzmanları, olay müdahale uzmanları ve adli laboratuvar yöneticileridir. Ek olarak bu standart delile müdahalede bulunan kişilerin, potansiyel dijital delilleri dünya çapında kabul edilebilir uygulamalı yollarla yönetmesini ve elde etmesini sağlamaktadır.[432,433]

Adli bilişim yöntemlerinin uygulanmasında bir standart getirilmesinin birçok açıdan faydası olacaktır. Gerçekten de uluslararası anlamda kabul gören bir standart, hem dijital delillerin elde edilmesi görevini üstlenen adli bilişim uzmanlarına bir harita çizmesi sebebiyle adli bilişim süreçlerinin daha hızlı ve pratik bir biçimde uygulanmasını sağlayacak, hem de elde edilen delilleri inceleyen mahkemeleri, uygulanan yöntemin doğru bir yöntem olup olmadığı yönünde bir araştırma yapma gereksiniminden uzaklaştırarak yalnızca yöntemin doğru bir şekilde uygulanıp uygulanmadığını değerlendirmeye yönlendirecektir. Ek olarak böyle bir standartın varlığı, bu standart uygulanarak elde edilen bulguların, delil değeri taşıyacakları yönünde bir karine oluşmasına dahi vücut verebilir. Gerçekten de dijital delililler, uluslararası alanda kabul edilen bir standart çerçevesinde elde edilirlerse, bunların delil değeri taşımamaları ancak haklarında bir hukuka aykırılık iddiası varsa ve bu iddia ispatlanabilirse mümkün olacaktır. Bu durum da mahkemeleri, elde edilen dijital delilin, güvenilir olup olmadığı konusunda bir değerlendirme yapma külfetinden kurtaracak ve ispat sürecine katkı sağlayacaktır.

2.1.1.5. Adli bilişim uzmanı

Adli bilişimdeki genel kabul görmüş uygulama ve eğitim standartlarının önemi göz ardı edilemez çünkü bunlar yanlış kullanılan analiz ve yorumlamadaki hata riskini azaltır. Gerçekten de yanlış bir şekilde gerçekleştirilen analiz ve delil işleme faaliyetleri sonucunda masum kişiler suçlanabilir yahut suçlu kişiler aklanabilirler.[434]

[431] Buzarovska Lazetik and Koshevaliska, "Digital Evidence in Criminal Procedures," 70- 71.
[432] Buzarovska Lazetik and Koshevaliska, "Digital Evidence in Criminal Procedures," 71.
[433] Söz konusu standartlar ile ilgili ayrıntılı bilgiler için bkz. Yalçın ve Kılıç, "ISO/IEC 27037," 445-449.
[434] Casey, *Digital Evidence,* 11.

Bu bakımdan adli bilişim uzmanlarının ilgili alanda yeterli bilgi düzeyine sahip ve bunu belgelendirebilir kişiler arasından seçilmesi önem taşımaktadır.[435]

Yorumlama ve analiz aşamalarındaki hatalar, bilimsel yöntemin titiz bir şekilde uygulanmasıyla, kapsamlı inceleme ve araştırma yapılmasıyla, tüm varsayımların sorgulanmasıyla ve gerçekleri açıklayan bir teori geliştirilmesiyle azaltılabilir. Adli bilişim uzmanı varsayımlarına yüksek derecede güvense bile, olası hatalar ve alternatif açıklamalar araştırılmalı ve ortadan kaldırmalı veya en azından olası olmadığını belgelemelidir.[436]

Dijital delillerin analizinde adli bilişim uzmanı tarafından ulaşılan herhangi bir sonucun, muhakemeye konu olan maddi olayla bağlantısının kurulması gerekmektedir. Bu sebeple adli bilişim uzmanı, elde ettiği bulguları yorumlayıp, maddi olayla bağlantısını ortaya koymalıdır. Adli bilişim uzmanları, yargı makamlarının hareket edecekleri yönü belirlemelerine yardımcı olmak için vardıkları sonuçların altında yatan kesinlik düzeyini tahmin edebilmeli ve tanımlayabilmelidir.[437] Mahkemelerin amacı adaleti yönetmektir ve adli bilişim uzmanlarının da bu bağlamdaki rolü destekleyici gerçekleri ve olasılıkları sunmaktır.[438]

Adli bilişim uzmanları, mümkün olduğunca tek bir dijital delil kaynağındaki herhangi bir potansiyel zayıflığın, net bir sonuca zarar vermesini önlemek için raporlarındaki iddiaları birden fazla bağımsız delil kaynağıyla desteklemelidirler. Adli bilişim uzmanları, karar organlarının raporu yorumlamalarına yardımcı olmak ve başka bir yetkin adli bilişim uzmanının sonuçları doğrulamasını sağlamak için tüm delillerin nasıl ve nerede bulunduğunu açıkça belirtmelidirler. Rapordaki bulguları açıklarken destekleyici kanıtlara başvurmak gerekebileceğinden, önemli dijital delil öğelerini şekil veya ek olarak eklemek yararlı olacaktır. Alternatif senaryolar sunmak ve bunların neden daha az makul ve kanıtlarla daha az uyumlu olduklarını göstermek, temel sonuçların güçlendirilmesine yardımcı olabilir. Diğer açıklamaların neden olası veya imkânsız olduğunu açıklamak, bilimsel yöntemin uygulandığını, verilen sonucu çürütmek için çaba sarf edildiğini ve eleştirel incelemeden geçtiğini gösterir.[439] Alternatif bir senaryoyu destekleyecek herhangi bir delil yoksa, adli bilişim uzmanları

[435] Sarsikoğlu, "Elektronik Delil (E-Delil) Kavramı," 528- 529.
[436] Casey, "Error, Uncertainty and Loss," 35.
[437] Casey, *Digital Evidence,* 68.
[438] Casey, *Digital Evidence,* 49.
[439] Casey, *Digital Evidence,* 75.

ilgili delilin gözden kaçırılmış veya mevcut olmamasının daha olası olup olmadığını açıkça belirtmelidir. Dijital deliller toplandıktan sonra değiştirildiyse adli bilişim uzmanları, değişikliklerin nedenini açıklayarak ve dava üzerindeki etkilerini tartarak raporlarında bundan bahsetmelidirler. Masumiyet veya suçluluk hakkında açıklama yapılmaması önem arz etmektedir. Sonuçlar objektif olmalı ve gerçeklere dayanmalıdır. Kanıtın kendisi için konuşmasına izin verilmeli ve yargılayıcı olmaktan kaçınılmalıdır.[440] Kısacası, adli bulgularının resmi bir raporu, okuyuculara delilleri ve ilgili sonuçları değerlendirmek için ihtiyaç duydukları tüm bilgileri vermelidir.[441,442]

Ek olarak adli bilişim uzmanı ve diğer görevliler tarafından dijital delilin kolaylıkla değiştirilebilir olduğu bilinmeli ve delillerin toplanması, incelenmesi ve analizi süreci boyunca alınan prensip ve prosedürlere uyulmalıdır. Zira delillerin karartılmasına, bozulmasına, tahrif edilmesine veya değişmesine neden olabilecek yanlış uygulamalar sebebiyle mahkemeler delilleri reddedebileceklerdir.[443] Bu bağlamda adli bilişim uzmanı, olay yerinde el konulan bilişim araçları içerisindeki verilerin, mahkemede hükme esas teşkil edene kadar değiştirilmeden muhafaza edilmesini sağlamalıdır.[444]

Özetlenecek olursa adli bilişim uzmanları, büyük veri yığınlarından değerli bitleri çıkarır ve bunları yargı makamlarının anlayabileceği şekillerde sunar. Temel malzemedeki veya işlenme şeklindeki kusurlar, nihai ürünün değerini düşürür. Adli bilişim uzmanları genellikle dijital delillerin toplanmasından, belgelenmesinden ve korunmasından; faydalı verilerin çıkarılmasına ve bir bütün olarak suçun giderek daha net bir resmini oluşturmak için birleştirilmesine kadar gerekli tüm görevleri yerine getirir.[445] Genel anlamda adli bilişim uzmanlarının, konunun nesnel, tarafsız gerçeğini mahkeme huzuruna sunma görevi vardır.[446]

---

[440] Casey, *Digital Evidence,* 78.
[441] Casey, *Digital Evidence,* 76.
[442] Bir bilirkişi raporu, giriş, delil özeti, inceleme özeti, dosya sistemi incelemesi, adli analiz ve bulgular ve son olarak sonuçlar olmak üzere çeşitli başlıkları bulundurmalıdır. Bu bağlamda, raporda değinilmesi gereken hususlar, başlıkların ayrıntıları ve bir bilirkişi raporu örneği için bkz. Casey, *Digital Evidence,* 76-77.
[443] Başlar, "Adli Bilişim," 56.
[444] Değirmenci, *Sayısal Delil,* 248.
[445] Casey, *Digital Evidence,* 465.
[446] Casey, *Digital Evidence,* 51.

2.1.1.6. Türkiye'de adli bilişim alanında görülen sorunlar ve ceza yargılamasına etkileri

İlk olarak Adli bilişim ilke ve standartlarının belirlenememiş olması, başka bir ifadeyle adli bilişim alanı ile ilgili olarak mevzuatta net bir düzenleme bulunmaması; adli bilişim sürecini, bu alanda çalışan kişileri ve dijital delillerle ilgilenen yargı makamlarını oldukça zora sokmaktadır.

"Adli bilişim" kavramının mevzuatta yer aldığı tek düzenleme, Adlî Tıp Kurumu Kanunu Uygulama Yönetmeliği'ne[447] 2016 yılında eklenen 14/A maddesidir.[448] Bu madde uyarınca adli bilişim ihtisas dairesinin kuruluşu ve teşkilatlanması belirtilmiş ve adli bilişim ihtisas dairesinin görevleri ve çalışma usulleri sayılmıştır. Bu düzenleme dışında adli bilişim uygulaması ve adli bilişim uzmanları hakkında herhangi bir düzenlemeye yer verilmeyerek işleyişin uygulamaya bırakılması büyük bir eksikliktir. Ek olarak bir "Adli Bilişim Kurumu"nun kurulmasının da son derece gerekli olduğu belirtilmiştir.[449]

Uluslararası alanda kabul edilen adli bilişim ilkelerine ülkemizde de önem veriliyor olmakla birlikte dijital delilin elde ediliş sürecine ilişkin işlemlerin ve bu bağlamda izlenmesi gereken adımların neler olduğu, uyulması gereken standartların ve sorumlulukların belirsizliği, kısaca net bir iş akış modelinin olmaması ve buna ek olarak bilirkişi olarak atanan kişilerin bilimsel ehliyetlerini ön şart olarak ortaya koyan ve bu hususu takip eden net yasal düzenlemelerin bulunmaması gibi eksiklikler uygulamada birçok dijital delilin daha elde edilmeleri sırasında geri dönülemeyecek şekilde kaybolmasına veya kullanılamaz hale gelmesine zemin hazırlamaktadır.[450] Bu bakımdan söz konusu standartların, kuramların ve yöntemlerin, belirlenmesi ve yazılı şekilde kural haline getirilmesi gerekmektedir. Fiilen kurallara riayet ediliyor oluşu, gelecekte de bu kurallara riayet edileceği anlamına gelmez.[451]

İkinci olarak günümüzde adli bilişim alanında çalışanların tamamı tarafından ifade edilen bir sorun, elde edilen delillerin incelenmesi için harcanan sürenin her geçen gün artıyor oluşudur. Bunun temel sebepleri;

---

[447] Resmî Gazete Tarihi: 31.07.2004, Sayı: 25539.
[448] Resmi Gzete Tarihi: 25.11.2016, Sayı:29899.
[449] Arslan, "Dijital Delil ve İletişimin Denetlenmesi," 191.
[450] Değirmenci, *Sayısal Delil,* 121; Başlar, "Adli Bilişim," 59; Yılmaz ve Çakır, "Mobil Cihaz Adli Bilişimi Süreçleri," 25.
[451] Say, "Bilişim Suçlarında Elde Edilen Deliller," 98.

> *"dijital verilerin depolandığı cihazların maliyetlerindeki düşüş ve bununla ters orantılı olarak cihazların veri saklama kapasitelerinin artması, veri taşıma araçlarının çeşitliliği, ağa her yerden ulaşılabilmesinin sonucu olarak verinin birden fazla yerde ancak kopya veri olarak tutulması, bilişim teknolojilerinin hayatı kolaylaştırmasının sonucu olarak toplumsal hayatın her noktasında gerek insan gerekse de makine kaynaklı veri kaydının sürekli yapılması"* olarak gösterilebilir. [452]

Bunun sonucu olarak da adli bilişim incelemelerinde vaka başına düşen verinin miktarı artmakta ve bu verileri incelemek için geçirilen süre de uzamaktadır.[453] Bu sorunun elbette yalnızca Türkiye'ye özgü olmayıp, dünya çapında gerçekleşen bir sorundur. Öyle ki globalleşen dünyada gelişen teknoloji neticesinde adli bilişim alanı, veri depolama cihazlarının kapasitelerindeki artışa ve bu cihazların insanlar arasındaki yayılma hızına yetişememektedir.

Türk hukuku bakımından bu gecikmelerin sadece adli bilişim açısından sakıncaları bulunmamaktadır. Öyle ki söz konusu gecikmeler, yeterli delile dayanarak iddianameyi hazırlama yükümlülüğü altında bulunan Cumhuriyet savcılığı bakımından (CMK m. 170/2) soruşturmanın ve delile dayanan vicdani kanaatini oluşturacak mahkeme bakımından ise hükmün, geç bir şekilde açıklanması anlamına gelecektir.[454] Bu durumun ise Avrupa İnsan Hakları Sözleşmesi m. 6'da yer alan ve "Adil Yargılanma Hakkı" kapsamında korunan, makul sürede yargılanma hakkı bakımından ihlallere vücut verebilecektir.

Bir nevi dijital bir samanlıkta iğne aramaya benzetilen bu sürecin çözümü yahut en azından kolaylaştırılması için çeşitli adımlar atılabilir. Bu kapsamda delil elde etmede kullanılan yazılımların geliştirilmesi ve hızlandırılması önerilebileceği gibi farklı olarak adli tıp alanında uygulanan ve *"sınırlı kaynakların etkinliklerinin azami seviyede kullanılması için geliştirilmiş bir süreç"* olan *Önceliklendirme (Triyaj)* metodunun, adli bilişim alanında da uygulanması ve geliştirilmesi önerilmiştir.[455]

---

[452] Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj)," 50- 51.
[453] Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj)," 50- 51.
[454] Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj)," 52.
[455] Adli bilişimde önceliklendirme temel olarak olay yerinde önceliklendirme ve laboratuvar ortamında önceliklendirme şeklinde ikiye ayrılmaktadır. Bu yöntem ile hedeflenen, deliller üzerinde gerçekleştirilen delil elde etme sürecinin, soruşturma veya kovuşturma konusu suç çerçevesinde yürütülmesi ve buna göre delillerin aranması sırasında incelenen bilişim sistemi içerisindeki verilerin uyuşmazlık konusu suç fiili çerçevesinde önceliklendirilmesidir. Önceliklendirme yöntemi ve bu yöntem kapsamında geliştirilen metodolojiler hakkında detaylı bilgi için bkz. Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj)," 47- 79.

Bu sebeplerle öncelikle dijital delil elde etme sürecinde çalışacak bilirkişilerin görevlendirilmesi konusunda ve devamında adli bilişim ilke ve standartlarına ilişkin uluslararası alanda kabul edilen adli bilişim standartlarına[456] önem verilmesi ve bunların yasal bir zemine oturtulması gerekmektedir.[457]

Bir başka sorun, adli bilişim laboratuvarlarının yeterli seviyede olmayışıdır. Uluslararası alanda kabul edilen adli bilişim ilke ve standartlarına önem verilmesi ve bunların yasal bir zemine oturtulması tek başına yeterli değildir. Aynı zamanda bu ilkelere uygun teknolojik alt yapının kurulması da gereklidir.[458]

Uygulayıcıların eğitimi hususu ise ayrıca önem arz etmektedir. Ortalama bir polis memuru yeni teknolojiler hakkında bilgi sahibi olmayabilir ve yine ortalama bir polis birimi dijital delilleri işlemek için doğru kaynaklara sahip olmayabilir. Suçlular bıraktıkları dijital izlerin çoğunlukla farkındadırlar ve bu izlerden kurtulmak için çeşitli yollar izlerler. Bu bağlamda bilişim sistemleri tahrif edilebilmekte, izler gizlenebilmekte ve hatta izleri arayan kolluk görevlilerine tuzaklar kurulmak suretiyle izlerin ortadan kaldırılması sağlanabilmektedir. Bu nedenle adli bilişim sürecinde görev alan uygulayıcıların, her bir dijital delilin farklılıklarını bilmeleri ve adli bilişim süreciyle ilgili o zamana kadar yapılan çalışmalara her soruşturma bakımından kolayca güvenmemeleri gerekmekte olup yeni oluşacak koşullara ilişkin çalışmaları ve bunların sonuçlarını da yakından takip etmeleri gerekmektedir.[459,460]

2.1.2. Ceza muhakemesi hukukunda dijital delillerin elde edilmesi ve muhafazası

2.1.2.1. Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma (CMK m. 134)

CMK m. 134'ün, genel olarak arama ve elkoyma hükümlerini düzenleyen CMK m. 116 ve devamının, özel bir hali olduğu görüşüne katılmaktayız.[461] Genel

---

[456] ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042 ve ISO/IEC 27043 gibi standartlar.
[457] Başlar, "Adli Bilişim," 60.
[458] Başlar, "Adli Bilişim," 61.
[459] Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 145; Mifsud Bonnici, Tudorica and Cannataci, "The European Legal Framework," 203; Başlar, "Adli Bilişim," 63; Yılmaz ve Çakır, "Mobil Cihaz Adli Bilişimi Süreçleri," 26.
[460] Türkiye'de dijital delillerle ilgili olarak kolluk görevlilerine Siber Suçlarla Mücadele Daire Başkanlığı, Bilişim Suçları Akademisi Şube Müdürlüğü tarafından çok çeşitli eğitimler verilmektedir. Bu eğitimler hakkında bkz. https://www.egm.gov.tr/siber/egitimler son erişim: 18.12.2021.
[461] Değirmenci, *Sayısal Delil,* 315; Dülger, *Bilişim Suçları,* 589.

arama ile bilişim sistemleri üzerinde gerçekleştirilen arama arasındaki fark aramanın konusu yönündendir. Gerçekten de genel arama tedbirinde aramanın konusu maddi varlığı bulunan bir mal iken bilişim sistemlerinde aramanın konusu gayri maddi niteliği bulunan verilerdir. Benzer şekilde genel elkoyma tedbiri de maddi varlığı bulunan mallar üzerinde gerçekleştirilirken, bilişim sistemlerinde elkoyma ise, bilişim sistemlerinin donanımları üzerinde gerçekleştirilir. Bu bakımdan CMK m. 134'ün genel olarak arama ve elkoyma hükümlerinin özel bir hali olduğunu söylemek yanlış olmayacaktır. Bu sebeple koruma tedbirleri için geçerli olan ve yine bir koruma tedbiri olan arama ve elkoyma tedbirlerine ilişkin genel düzenlemeler, CMK m. 134 bakımından da geçerli olacaktır.[462]

Herhangi bir suç bilişim sistemleriyle ilgili olabileceğinden, bilişim sistemi kullanılarak işlenebilen suçlar ile bilişim sistemlerinin suçun işlenmesinde bir unsur değil fakat bir araç olarak kullanıldığı suçlar arasındaki çizginin nereye çekileceği önem arz etmektedir. Bu ayrımın önemi ise, adli bilişim uzmanlarının, bilişim sistemi üzerinde arayacakları verilerin, nitelikleri bakımından karşımıza çıkacaktır. Örneğin bilişim sistemi, suçun hedefi veya aracı olduğunda olay yeri inceleme, bilişim sisteminde ilgili suça ilişkin delil niteliğinde olan verileri arayacaktır. Başka bir ifadeyle suçun varlığına veya faile yönelik veriler aranacaktır. Buna karşılık bilişim sistemi herhangi bir suçun delillerini barındırıyorsa, arama sırasında, o suça ilişkin delillere ulaşılmaya çalışılacaktır.[463]

Bilişim suçlarının tanımlanmasındaki ana zorluklardan biri, bir bilgisayarın veya ağın doğrudan bir suça karışmadığı ancak yine de suçla ilgili dijital delilleri içerdiği durumların ortaya çıkmasıdır. Bu tarz durumlarda *bilgisayarla bağlantılı (computer-related) suçlar* terimi kullanılmaktadır. ABD Adalet Bakanlığı (USDOJ) ve Avrupa Konseyi, bilgisayarları ve ağları içeren çok çeşitli suçlara atıfta bulunmak için siber suç terimini kullanır.[464]

[462] Değirmenci, *Sayısal Delil,* 74- 77; Dülger, *Bilişim Suçları,* 589; Feridun Yenisey ve Ayşe Nuhoğlu, *Ceza Muhakemesi Hukuku* (Ankara: Seçkin Yayıncılık, Güncellenmiş 9. Baskı, 2021), 443.
[463] Değirmenci, *Sayısal Delil,* 63.
[464] Casey, *Digital Evidence,* 37.

Bilgisayar bağlantılı suçlar *Parker* ve *Nycum* tarafından 4 kategoriye ayrılmıştır.[465]

1. Bilişim sistemleri suçun konusu (the object of a crime) olabilecektir. Bilişim sistemin, suç olan hareketten etkilendiği durumlarda, suçun konusu olacaktır. Örneğin bilgisayarların tahrip edilmesi veya çalınmasında bilgisayar, suç olan hareketten etkilenen konumundadır.

2. Bilişim sistemi suçun süjesi (the subject of a crime) olabilecektir. Bilişim sisteminin suçun işlenmesinde uygun ortamı sağladığı durumlarda, bilişim sisteminin süje olma rolünden bahsedilecektir. Bilgisayarın, çeşitli programlamalar ve otomatik mekanizmalar aracılığıyla yanlış bilgiler üretmesi sonucu piyasayı manipüle etmek için kullanılması, suçun süjesi olmasına örnek olarak verilebilecektir.

3. Bilişim sistemi suçun islenmesinde veya planlanmasında araç (tool) olarak kullanılabilecektir. Bilgisayarların kullanılması suretiyle sahte bir belgenin oluşturulması veya bilgisayarın, diğer bir bilgisayara hukuka aykırı şekilde erişilmesi için kullanılması, araç olarak kullanılmasına örnek olarak verilebilir.

4. Bilişim sistemi tehdit veya hile fiillerinde sembol olarak kullanılabilir. Parker'ın söz konusu durum için verdiği örnek, bir borsa simsarının müşterilerini bir bilgisayar programı kullanmak suretiyle büyük karlar elde edecekleri konusunda aldatmasıdır. Örneğe göre ortada böyle bir program bulunmamaktadır ancak simsar bilgisayarı sembol olarak kullanmak suretiyle dolandırıcılık eylemini gerçekleştirmektedir. Ancak *Parker* ve *Nycum* tarafından yapılan bu tanım dijital delil kaynağı olarak sadece bilgisayarları kabul etmesi sebebiyle eleştirilmiştir.[466]

Buna karşın Siber Suçlar Sözleşmesi de suçları benzer bir çizgide kategorilere ayırmıştır. Buna göre suçlar, bilgisayar bütünlüğü suçları (bilgisayarın suçun nesnesi olduğu durumlarda), bilgisayar destekli suçlar (bilgisayarın bir araç olduğu

[465] Donn B. Parker and Susan H. Nycum, "Computer Crime," *Communications of the ACM*, Volume 27, Issue 4 (April 1984): 313. Aktaran: Değirmenci, *Sayısal Delil,* 62; Başlar, "Elektronik Delil," 1669; Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* 38.
[466] Casey, *Digital Evidence,* 41.

durumlarda) ve içerikle ilgili suçlar (bilgisayar ağının suç ortamını oluşturur) olmak üzere üçe ayrılmıştır.[467]

Tedbiri incelemeye geçmeden önce şu hususun belirtilmesi gerekir; "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" tedbiri, birazdan bahsi geçecek olan, "İletişimin Tespiti, Dinlenmesi ve Kayda Alınması" tedbirinden farklılık arz etmektedir. Öyle ki CMK m. 134 gerekçesi incelendiğinde, bu tedbir, durağan haldeki aygıtta araştırılma yapılmasını ve durağan verilerin elde edilmesi hususunu düzenlerken; İletişimin Denetlenmesi tedbiri, akışkan haldeki verilerin elde edilmesini düzenlemektedir.[468] Akışkan ve durağan haldeki veri ayrımı ise geçmişte gerçekleşen bir fiile yönelik mi yoksa gelecekte gerçekleşebilecek bir fiile yönelik mi arama yapılacağı ve bu doğrultuda hangi koruma tedbirine başvurulacağı konusunda önem arz etmektedir. Yargıtay'ın da çeşitli kararlarında belirttiği üzere,

> *"CMK'nın 135. maddesine göre yapılan iletişimin dinlenmesi ve kaydı… geleceğe dönük olarak yapılabilir.… geçmişte… internet ortamında gerçekleştirilen iletişime ilişkin kayıtlar, bilgisayar kütüğünde kayıt altına alındığından bu iletişim kayıtları hakkında CMK'nın 134. Maddesinde yer alan koruma tedbiri uygulanacaktır."*[469]

Bu doğrultuda bir e- posta eğer gönderen ile alıcı arasında aktarım noktalarında hareket halindeyse CMK m. 135 çerçevesinde inceleme gerçekleştirilebilecektir. Ancak ilgili e- posta hareketini tamamlamış ve alıcıya ulaşmışsa artık bilişim cihazına kayıtlı bilgi ve belgeye dönüşecektir ve o andan itibaren CMK m. 134 çerçevesinde bir inceleme gerçekleştirilebilecektir.

Asıl olarak inceleme konumuz "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" tedbiri olmakla birlikte, dijital delillerin elde edilmesi noktasında "İletişimin Tespiti, Dinlenmesi ve Kayda Alınması" tedbiri ile "Teknik Araçlarla İzleme" tedbirlerine de kısaca yer verilecektir.

---

[467] Casey, *Digital Evidence,* 41.
[468] Dülger, *Bilişim Suçları,* 581; Börekçi, "Bilgisayarlarda, Bilgisayar Programlarında," 54.
[469] Yar. CGK, E. 2020/67, K. 2021/372, T. 07.09.2021; Yar. CGK, E. 2020/61, K. 2021/546, T. 11.11.2021; Yar. CGK, E. 2019/, K. 2022/11, T. 13.01.2022 https://www.lexpera.com.tr/ , son erişim, 09.06.2022.

2.1.2.1.1. Tedbirin amacı

"Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" tedbirinin amacı bilişim sistemleri üzerinde bulunan delillerin elde edilmesidir.[470] Ancak hem dijital verilerin özel ve hassas yapısının, elde edilmesinde farklı yöntemlerin kullanılmasını zorunlu kılması ve hem de bilişim sistemlerinin, suçla ilişkili veri barındırma ihtimalleri yanında bir çok özel nitelikte kişisel veriyi barındırması ve gün geçtikçe kullanımları artan bilişim sistemlerinin çoğunluğunun aynı zamanda iletişim ve haberleşmede de kullanılıyor oluşları sebebiyle, bu sistemlerin aranması ve bunlara el konulmasının normal arama ve elkoymaya oranla başka birçok hakka da müdahale teşkil edebilecek oluşu; bu tedbirin genel arama hükümlerinden ayrılarak, özel bir şekilde ve daha kapsamlı korumalarla donatılarak düzenlenmesine vesile olmuştur.

CMK m. 134, Türkiye'de adli bilişimle ilgili temel düzenleme olmakla birlikte, bünyesinde birçok boşluk barındırması sebebiyle, uygulayıcıları inisiyatif almaya ittiği ancak uygulayıcıların da bu konuda yeterli bilgiye sahip olmadıkları gerekçesiyle eleştirilmiştir.[471,472]

2.1.2.1.2. Tedbirin konusu

Tedbirinden konusu, tedbirin üzerinde uygulanacağı şeylerdir. Bu bağlamda madde başlığında ve içerisinde bahsi geçen, tedbirin uygulanacağı şeyler; bilgisayarlar, bilgisayar programları ve bilgisayar kütükleridir.

2.1.2.1.2.1. Bilgisayarlar

Bilgisayarlar, bilgisayar verileri ve bilişim sistemleri farklı anlamlarda kullanılmaktadır. Kısaca bu kavramları tanımlayacak olursak;

Bilgisayar sistemi, "bir veya birden fazlası, belirli bir yazılım çerçevesinde otomatik olarak veri işleyebilen bir cihazı veya birbirine bağlı veya birbiriyle ilişkili

[470] Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 62; Kaynakçıoğlu, "Dijital Deliller," 109.
[471] Yılmaz ve Çakır, "Mobil Cihaz Adli Bilişimi Süreçleri," 26.
[472] Bilişim sistemlerinde gerçekleştirilecek arama, kopyalama ve elkoymalarla ilgili olarak, olay yerine ilk temas anından, inceleme neticesinde hazırlanan raporun mahkemeye sunulması anına kadar geçen süreçte yapılması ve yapılmaması gereken şeyler konusunda bkz. Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 145- 148; Casey, *Digital Evidence,* 479- 480.

bir dizi cihazı" ifade ederken[473], bilgisayar verisi ise "bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlar da dahil olmak üzere, bir bilgisayar sisteminde işlenmeye uygun nitelikteki her türlü bilgi ve konsepti" ifade etmektedir.[474]

Bununla birlikte bilişim sistemi ise bilgisayar, çevre birimleri (bir bilgisayarın çalışması için zorunlu olmayan ancak kullanımını kolaylaştıran hoparlör, CD ROM, mouse, klavye, kulaklık, yazıcı vb), iletişim altyapısı (elektronik haberleşme, internet, intranet gibi) ve programlardan oluşan veri işleme saklama ve iletmeye yönelik sistemi ifade etmektedir.[475] Bu bağlamda bilgisayar ise en temel bilişim sistemidir.[476]

Görüldüğü üzere bilişim sistemi kavramı, bilgisayarları da içine alan daha geniş bir kavrama işaret etmektedir. Bu bağlamda biz de Değirmenci tarafından kullanılan "Bilişim Sistemi" teriminin içerik ve anlam bakımından daha doğru sonuç vereceği kanaatindeyiz.[477] Öyle ki CMK m. 134'te yer alan terimin bilişim sistemlerine işaret etmediğini kabul etmek, bilgisayar olarak nitelendirilmeyen teknolojik aygıtlarda yer alan verilerin, söz konusu maddenin sağladığı korumadan yararlanamaması anlamına gelecektir.[478]

Ek olarak yasada geçen "bilgisayar" teriminin yorumlanması hususu bazen uygulamada da sorunlara yol açabilmektedir. Kavramın dar yorumlanması sonucunda maddenin üzerinde uygulanacağı cihazların yalnızca "bilgisayarlar" olabileceği gibi bir anlam çıkarılabilir.[479] Fakat günümüz teknolojik gelişmeleri düşünüldüğünde artık yalnızca geleneksel bilgisayarlar değil, taşınabilir mobil bilgisayarlar ve hatta cep telefonları dahi bilgisayar görevini üstlenebilmektedir. Öyle ki günümüz mobil cihazları, "*Telefon, tablet, gps cihazları gibi elde kullanılması mümkün olan son kullanıcı düzeyindeki bilgisayar sistemleri"* şeklinde tanımlanmaktadır.[480]

Özellikle mobil cihazlara da el konulması düşünüldüğünde veri barındıran bilişim sistemlerine bakış değişmelidir. Böyle bir dijital veri taşıyıcısı (akıllı telefon

[473] Değirmenci, *Sayısal Delil,* 36.
[474] Casey, *Digital Evidence,* 130.
[475] Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 55.
[476] Tezcan, v.d., *Dijital Ceza Muhakemesi Hukuku,* 34.
[477] Değirmenci, *Sayısal Delil,* 310.
[478] Değirmenci, *Sayısal Delil,* 41.
[479] Kaynakçıoğlu, "Dijital Deliller," 110; Nitekim madde metninde geçen "bilgisayar" ifadesinin dar yorumlanarak cep telefonlarının bu kategoriye sokulmaması ve genel arama hükümleri ile elde ediliyor oluşu eleştirilmiştir. Bkz. Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 69; Afandak, "Ceza Muhakemesinde Dijital Deliller," 77.
[480] Yılmaz ve Çakır, "Mobil Cihaz Adli Bilişimi Süreçleri," 27.

veya kişisel bilgisayar), ele geçirilirse, yalnızca sahibinin değil, aynı zamanda iletişim içinde olduğu kişilerin de çok büyük miktarda kişisel verisini içerecektir. Bu durumda, yalnızca mülkiyet hakkı değil, aynı zamanda özel hayatın gizliliği ve büyük olasılıkla iletişim hakkı da etkilenecektir. Bu tür bir cihazda depolanan verilerin analiz edilmesi, sahibinin (ve iletişime geçtiği kişilerin) hem profesyonel hem de özel hayatının çeşitli alanlarında kapsamlı bilgiler sağlarken, elde edilen ve dolayısıyla yargı makamlarının erişimine açık hale gelen büyük miktardaki verinin çoğunluğu durumla muhtemelen alakasız olacaktır.[481]

Nitekim Yargıtay'a konu olan bir davada, cumhuriyet savcısının talimatıyla sanığın cep telefonu üzerinde arama yapılmış ancak *"işlevi itibarıyla bilgisayar niteliğinde olan cep telefonu üzerinde inceleme yapılabilmesi için CMK'nın 134. maddesi uyarınca hâkim kararı alınması gerektiği"* hususu belirtilerek elde edilenler delil olarak kabul edilmemiştir.[482] Yine bir başka davada dijital delili tanımlayan Yargıtay bu delillerin, *"CD, DVD, flash bellek, disket, harici ve dahili harddisk, bilgisayar özelliği içeren noktaları bakımından akıllı telefon ve benzerlerinden elde edilen…veriler"* olduklarını belirtmiş ve *"bilgisayar özelliği içeren noktaları bakımından akıllı telefon ve benzerlerini"* de kapsama almıştır. Buna karşılık yine aynı kararda Yargıtay, elektronik (dijital) delilleri; *"bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen, soruşturma açısından değeri olan bilgi ve veriler…"* şeklinde kapsayıcı olarak tanımlayan Keser Berber'e[483] de atıfta bulunmuştur.[484] Yargıtay'ın bu iki dairesinin cep telefonlarına olan yaklaşımı, cep telefonların tamamen bilgisayar özelliği gösterip göstermediği noktasında ortaya çıkmaktadır. Zira 17. Ceza Dairesi, cep telefonlarının, bilgisayar gibi üzerine yüklenen programlar vasıtasıyla çalışabilme, veri girişini sağlayan mekanizmalar vasıtasıyla söz konusu verileri depolama, verileri işleme tabi tutma, verileri bir yere nakletme, söz konusu verilerden bazı sonuçlar çıkarma, aritmetik ve mantık işlem dizileriyle çalışabilme gibi özellikleri[485] barındırdığını kabul etmiş ve cep telefonlarının CMK m.

---

[481] Forgó, v.d., "Privacy Protection," 256; Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 66; Börekçi, "Bilgisayarlarda, Bilgisayar Programlarında," 10.
[482] Yar. 17. CD., E. 2015/27517, K. 2017/1716, T. 15.02.2017 https://www.lexpera.com.tr/ , son erişim, 20.03.2022; Başlar, "Adli Bilişim," 68.
[483] Keser Berber, *Adli bilişim,* 46.
[484] Yar. 16. CD., E. 2015/4672 K. 2016/2330 T. 21.4.2016 https://www.lexpera.com.tr/ , son erişim, 20.03.2022.
[485] Bilgisayarların özellikleri ve çalışma prensipleri hakkında yukarda bkz. Bölüm 1., "1.2.3.1. Bilgisayarlar" başlığı.

134 kapsamına girdiklerini kabul etmiştir. Buna karşılık 16. Ceza Dairesi cep telefonlarının yalnızca bilgisayar özellikleri taşımadığını fakat bunun dışında arama, sms gönderme gibi telefonlara has özellikleri de bulunduğuna vurgu yapmış ve cep telefonlarını, bilgisayar özelliği içerdiği müddetçe CMK m. 134 kapsamına almıştır.

Öncelikle bahsi geçen bu iki kararın birbirlerine tezat içerisinde olduklarını düşünmekteyiz. Öyle ki 17. Ceza Dairesi, akıllı telefonların işlevi itibariyle bilgisayar niteliğinde olduğu ön kabulü ile hareket ederken; 16. Ceza Dairesi, akıllı telefonlarda, "bilgisayar özelliği içeren kısımlar" ve "bilgisayar özelliği içermeyen kısımlar" şeklinde bir ayrıma giderek, CMK m. 134'ün zaten kafa karıştırıcı olan içeriğini, daha da anlaşılmaz hale getirmiştir. Dahası aynı kararda, amacı dijital delillerin elde edilmesi olan CMK m. 134'ün kapsamına akıllı telefonlar yalnızca bilgisayar özelliği taşıdığı ölçüde dahil edilmiş ancak devamında dijital deliller, *"elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen, soruşturma açısından değeri olan bilgi ve verilerdir"* şeklinde tanımlanmıştır. Bu tanım ise, soruşturmayla ilgisi olması koşuluyla bütün elektronik cihazlarda bulunan verilerin, dijital delil olarak kabul edilmesi anlamına gelmektedir. Aynı kararda yer alan bu tezatlık ise hali hazırda karmaşık olan CMK 134'ün içeriği bakımından daha büyük soru işaretlerinin habercisi olmaktadır.

Bu bağlamda Yargıtay 16. Ceza Dairesinin yapmış olduğu bilgisayar özelliği içeren- içermeyen kısımlar ayrımının, yalnızca "bilgisayar" kavramının kapsamının belirlenmesi açısından doğru olduğunu kabul etmekle birlikte maddenin uygulanışı bakımından tüm bilişim sistemlerinin kapsama alınmasının daha doğru olacağı düşüncesindeyiz. Öyle ki ceza muhakemesi kurallarının temel hak ve özgürlüklere müdahale etmedikleri sürece kıyas yoluyla genişletilebileceği ve CMK m. 134'ün temel hak ve özgürlükler bakımından, genel arama hükümleri ile karşılaştırıldığında daha fazla koruma sağladığı gerçeği karşısında, CMK m. 134'ün, tüm bilişim sistemleri bakımından uygulanması daha doğru bir çözüm olacaktır.[486] Yine de birazdan bahsi geçecek "delilin yapısı, dijital delil, veri" odaklı yaklaşımın, bu tarz karmaşıklıkların önüne daha rahat bir şekilde geçeceğini ve temel hak ve özgürlükler bakımından daha korumacı bir bakışa sahip olduğunu düşünmekteyiz.[487]

[486] Değirmenci, *Sayısal Delil,* 329.

[487] Bu konuda benzer şekilde Değirmenci de "veri" odaklı bir yaklaşımın daha yerinde olacağını belirtmiştir. Gerekçe olarak ise, delillerin aranacağı yerlerin, bilgisayar, bilgisayar programı, kütükler

Yargıtay 17. Ceza Dairesi'nin CMK m. 134'te yer alan "bilgisayar" kavramını geniş yorumlayarak *"işlevi itibarıyla bilgisayar niteliğinde olma"* unsurunu araması, olumlu bir adım olsa da yine de dijital deliller bakımından yeterince kapsayıcı değildir. Öyle ki günümüzde bilgisayar niteliğinde olmamakla birlikte bünyesinde dijital veriler barındırabilen sayısız cihaz bulunmaktadır. Örneğin yazıcılar, fotokopi makinaları, mp3 çalar gibi birçok cihaz bünyesinde dijital delil olmaz özelliği sağlayabilecek veriler barındırabilmektedir.[488] Elbette ki bu veriler, cumhuriyet savcısının genel delil toplama yetkisi (CMK m. 161) çerçevesinde elde edilebilecektir. Bununla birlikte CMK m. 134'te yer alan "kütük" kavramının geniş yorumlanarak, içinde veri barındıran cihazlar şeklinde anlaşılması ve bahsi geçen verilerin de CMK m. 134 korunmasından faydalanılarak elde edilmesinin daha doğru bir yaklaşım olacağını düşünmekteyiz.

Tüm bu yorum faaliyetlerinden farklı olarak dijital delillerin elde edilmesi konusunda CMK m. 134 gibi "delilin elde edildiği cihaz, sistem" yaklaşımından ziyade "delilin yapısı" gibi bir yaklaşımın, daha doğru ve insan haklarına daha az müdahale edecek bir yaklaşım olacağını düşünmekteyiz. Ek olarak böyle bir yaklaşımın, madde gerekçesinde işaret edilen "*Bireye ait kişisel bilgiler üzerindeki hak, temel insan haklarından olduğundan hakkın kısıtlanabilmesi için yasal düzenleme gerekliliği"* ve *"hem gerçeğin açığa çıkarılması ve hem de bireysel yararların saklı tutulması"* amaçlarına daha iyi hizmet edeceği de aşikardır. Öyle ki CMK m. 134, kişinin bilgisayarında hassas ve kişisel verilerinin diğer ortamlara nazaran daha yoğunlukta olduğunu öngörmüş ve genel arama hükümlerinden (CMK m. 116 v.d.) farklı olarak daha kısıtlayıcı ve zor koşulların gerçekleşmesi gerektiğini belirtmiştir.

Günümüzün depolama kapasitelerinin yoğunluğu ve teknolojik gelişim düşünüldüğünde, dijital delil çoğu zaman kişilerin isnat edilen suç ile hiçbir ilgisi olmayan kişisel verilerinin de saklandığı bilişim sistemlerinde bulunmaktadır. Öyle ki bünyesinde dijital veri barındıran bir yazıcı dahi, onu kullanan kişi hakkında kişisel veriler içerebilecektir. Bu nedenle söz konusu bilişim sistemi içerisinde çok küçük bir

şeklinde belirtilmesinin, diğer delil içeren aygıtları kapsama alamama ihtimalinin bulunduğu halbuki CMK m. 134'ün bir delil elde etme aracı olarak öncelikle dijital delil elde edilmesi ve dolayısıyla veri elde edilmesi amacıyla uygulanan bir tedbir olduğu belirtilmiş ve bağımsız olarak verinin aranması ve veriye el koyma tedbirinin düzenlenmesinin daha yerinde olacağı belirtilmiştir. Değirmenci, *Sayısal Delil,* 310- 311.

[488] Değirmenci, *Sayısal Delil,* 23.

alanda saklı bulunan soruşturmaya konu dijital verinin tespiti ve elde edilmesi sürecinde de kişilerin kişisel verileri ifşa olmakta ve dolayısıyla özel hayatlarının gizliliğine müdahalede bulunularak çok çeşitli mağduriyetlere neden olunmaktadır ki dijital delile ulaşılamayan arama faaliyetlerinde bu mağduriyet katlanarak artmaktadır.[489] Bu sebeplerle belirttiğimiz üzere CMK m. 134'te olduğu gibi delilin elde edildiği kaynağın, bilgisayar veya bilgisayar işlevi gören bir cihaz olması hususu yerine bizzat elde edilecek delilin yapısının dijital olması, CMK m. 134'te yer alan korumalardan faydalanabilmesi için yeterli olmalıdır.[490] Bu bağlamda güncel CMK m. 134'ün, barındırdığı korumalar ve sınırlamalar baki olmak koşuluyla, "delilin yapısı" gibi bir yaklaşımla yeniden düzenlenmesinin, kişisel verilerin gizliliği, özel hayatın gizliliği ve iletişim özgürlüğü gibi insan hakları temelli bir bakışa daha uygun olacağı görüşündeyiz.[491,492]

2.1.2.1.2.2. Bilgisayar programları

Bilgisayar programları, verileri topladıktan sonra otomatik işlemelere tabi tutan manyetik sistemler olarak tanımlanabilir.[493] Farkı olarak 5846 sayılı "Fikir ve Sanat Eserleri Kanunu" (FSEK)[494] m. 1/B-g uyarınca ise bilgisayar programları:

> *"Bir bilgisayar sisteminin özel bir işlem veya görev yapmasını sağlayacak bir şekilde düzene konulmuş bilgisayar emir dizgesini ve bu emir dizgesinin oluşum ve gelişimini sağlayacak hazırlık çalışmaları…"* şeklinde tanımlanmıştır.

Bilgisayar programları, sistem programları (yazılımları) ve uygulama programları olarak iki grupta incelenmektedir. Bilgisayar programları da birer veridir ve kendi içerisinde de ayrıca veri barındırırlar. Bu bakımdan dijital deliller, bilgisayar programlarının içerisinde de aranabilecektir.[495]

---

[489] Başlar, "Elektronik Delil," 1669.
[490] Dijital delillerin, delil türleri arasındaki yeri hakkında yukarda bkz. Bölüm 1, "1.1.3.3. Dijital delillerin, diğer delil türlerinden farkları ve delil türleri arasındaki yeri" başlığı.
[491] Bu konuda CMK. m. 134'ün uygulama alanının bilişim sistemleri ve bunlara bağlı donanımları da kapsayacak ve de gelişen teknolojinin gerisinde kalmayacak genel bir çerçevede belirlenmesi ve hatta *"dijital delil, bilişim suçları, adli bilişim, bilişim sistemlerinde uygulanacak koruma tedbirleri gibi bilişim hukukuna ilişkin hususların ayrı bir kanunda ve tereddütlere mahal bırakmayacak biçimde yeniden düzenlenmesi gerektiği"* görüşü hakkında bkz. Başlar, "Adli Bilişim," 68.
[492] Benzer şekilde, içeriğinde bilişim teknolojisi bulunan veri taşıyıcılarının, CMK m. 134 kapsamında değerlendirilmesi gerektiği hakkında bkz. Tezcan, v.d., *Dijital Ceza Muhakemesi Hukuku,* 564.
[493] Veli Özer Özbek, Koray Doğan ve Pınar Bacaksız, *Ceza Muhakemesi Hukuku* (Ankara: Seçkin Yayıncılık, Genişletilmiş ve Güncellenmiş 14. Baskı, 2021), 362.
[494] Resmî Gazete Tarihi: 13.12.1951, Sayı: 7981.
[495] Değirmenci, *Sayısal Delil,* 51.

2.1.2.1.2.3. Bilgisayar kütükleri

Bilgisayar kütükleri teriminden ne anlaşılması gerektiği konusu tartışmalıdır ve bu sebeple kütük kavramı farklı şekillerde tanımlanmıştır.

Bir tanıma göre kütükler, *"sabit, taşınabilir ya da bulut formunda her türlü veri taşımaya ve depolamaya yarayan araçlar ya da sistemlerdir."*[496] Benzer şekilde kütükler, oluşturucusunun belirlediği ilişkili bilgiler yığını olarak tanımlanmıştır. *"Mantıksal depolama birimini anlamlandırmak için uygun araçların sahip oldukları sektör, track vb. gibi nitelikleri ölçülür. Bu şekilde boyutlanan mantıksal depolama birimi kütük adını alır."*[497] Yine benzer bir şekilde kütüklerin; bilgisayarın ve bilgisayarda yer alan dosyaların, geçirdiği aşamalara dair kayıtların ve verilerin tutulduğu yeri ifade ettiği belirtilmiştir.[498]

Yukarıda bir *"depolama birimi"*, *"depolama sistemi"* yahut *"verilerin tutulduğu yer"* olarak tanımlanmış olmasına karşılık başka bir tanıma göre kütüklerin, İngilizce *"log (günlük dosyaları)"* kelimesinin karşılığı olduğu ve *"internet servis sağlayıcılarının, internet erişimi sağladıkları kullanıcılara ait IP numaralarını ve diğer erişim bilgilerini depoladıkları veri tabanlarını"* ifade ettiği belirtilmiştir.[499]

Buna karşılık "kütük" ve "log" kavramlarının farklı iki şeyi ifade ettiği ve buna göre kütüklerin, insan müdahalesi ile bilişim sistemi tarafından oluşturulan ve saklanan dosyaları ifade ederken log kaydının ise insan müdahalesi olmaksızın oluşturulan ve saklanan dosyaları ifade ettiği belirtilmiştir. Buna göre örneğin Word programında yazılan bir metin "kütük" olarak isimlendirilebilirken; internet bağlantı bilgilerinin sistem tarafından otomatik olarak tutulması neticesinde elde edilenler, "log" olarak adlandırılacaktır. Bunun da neticesinde dijital deliller, sistem tarafından oluşturulan ve sistem tarafından saklanan deliller şeklinde ikiye ayrılacaktır.[500]

Benzer şekilde kütükler, *"Bir arada işlenen ve birbirleriyle ilgili olan kayıtların tümü."* şeklinde tanımlanmıştır.[501] Bu tanımdan yola çıkarak "kütük"

---

[496] Dülger, *Bilişim Suçları,* 585.
[497] Resul Göksoy, "Ceza muhakemesinde dijital delillerin elde edilmesi ve güvenilirliğinin sağlanması" (Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, Kamu Hukuku Programı, İzmir 2017), 48.
[498] Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 56.
[499] Özbek, Doğan ve Bacaksız, *Ceza Muhakemesi Hukuku,* 362; Tezcan, v.d., *Dijital Ceza Muhakemesi Hukuku*, 563- 564.
[500] Değirmenci, *Sayısal Delil,* 53.
[501] https://sozluk.gov.tr/ , son erişim: 07.03.2022.

teriminden bilgisayarın ana belleğinin dışında, fiziki olarak var olan depolama biriminin kendisi veya bu birimin içinde sadece mevcut olan herhangi bir verinin değil, birbirleriyle ilişkili verilerin oluşturduğu anlamlı bütünlük, yani dosyaların anlaşılması gerektiği belirtilmiştir.[502] Buna göre bilgisayar kütüklerinin bir depolama birimi içine kaydedildiği ve kütüklerin, bazen sabit diskte veya CD'de, bazen flash bellekte, bazen de bilgisayardan uzakta bulunan bir başka donanım üzerinde, mesela internet sunucusu (web server) üzerinde bulunabileceği belirtilmiştir. Buradan yola çıkarak CMK m. 134/2 de yer alan "*bu araç ve gereçlere elkonulabilir"* ifadesinin yanlış anlaşılabileceği, çünkü araç ve gereçlerin bizzat kendisinin kütük olmadığı ancak kütüğü bulunduran birimler olarak nitelendirilmesi gerektiği ifade edilmiştir.[503]

2.1.2.1.3. Tedbirin kapsamı

Tedbirin kapsamı, tedbir kapsamında elde edilen bilişim sistemleri üzerinde uygulanabilecek işlemlerdir. Bu bağlamda madde başlığı ve içerisinde bahsi geçen ve elde edilen bilişim sistemlerine uygulanabilecek olan işlemler; arama, kopyalama ve elkoymadır.

2.1.2.1.3.1. Arama

CMK m. 134'ün, genel olarak arama hükümlerini düzenleyen CMK m. 116'nın, özel bir hali olduğu görüşüne katıldığımızı belirtmiştik. Buna göre CMK m. 116 uyarınca çıkarılan bir arama kararı kapsamında gerçekleştirilen bir arama sırasında ele geçirilen bilişim sistemlerindeki verilerin aranabilmesi, kopyalanabilmesi ve bunlara elkonulabilmesi mümkün olmayacaktır. Bu bağlamda CMK m. 134 uyarınca bir arama kararı çıkartılması ve bilişim sistemlerinin bu şekilde aranması gerekecektir. Aksi durumda yapılan arama hukuka aykırı olacak ve elde edilenler, delil değeri taşıyamayacaklardır.[504]

CMK m. 134 bağlamında "arama"dan anlaşılması gereken veri aramasıdır. Veri araması ile amaçlanan şey ise, şüpheli tarafından kullanılan bilişim sistemlerinde,

---

[502] Yargıtay da çeşitli kararlarında, kütük kavramının *"bilgisayar dosyaları (computer files)"*na işaret ettiğini belirtmiştir. Bu konuda bkz. Yar. CGK, E. 2020/67, K. 2021/372, T. 07.09.2021; Yar. CGK, E. 2020/61, K. 2021/546, T. 11.11.2021; Yar. CGK, E. 2019/, K. 2022/11, T. 13.01.2022 https://www.lexpera.com.tr/ , son erişim, 09.06.2022.

[503] Göksoy, "Ceza muhakemesinde dijital delillerin elde edilmesi," 48- 50.

[504] Börekçi, "Bilgisayarlarda, Bilgisayar Programlarında," 54; Afandak, "Ceza Muhakemesinde Dijital Deliller," 144.

işlendiği konusunda şüphe bulunan bir suça ait delil, emare ve izlerin ele geçirilmesidir.[505]

Birçok hukuk sisteminde olduğu gibi CMK m. 134 de öncelikle yerinde arama (on- site) arama yapılmasını tercih etmiştir. Ancak belli bazı koşulların gerçekleşmesi halinde bilişim sistemine elkonulması suretiyle adli bilişim laboratuvarlarında (off-site) arama yapılmasına izin verilmiştir. Bununla birlikte yerinde aramanın kural haline getirilmesi; arama işleminin uzun sürmesi, arama sırasında nitelikli personelin çoğu zaman arama bölgesinde bulunmaması, ihtiyaç duyulan teknik aletlerin her zaman erişilebilir olmaması gibi sıkıntılar sebebiyle çoğunlukla ikinci planda kalmıştır ve bu sebeple istisnai nitelikte olan elkoyma tedbiri neredeyse kural haline gelmiştir.[506]

Günümüzün dijital medyasının gelişmiş depolama kapasitesi, dijital aramaların kapsamını karmaşıklaştırmaktadır. Bu bağlamda bir bilişim sisteminde bir suça dair delil aranması hususu samanlıkta iğne aramaya benzetilmiştir.[507] Bu dijital yığın içerisinde ise delil olarak kullanılabilecek veri, sistemde yer alan verinin yüzde, binde ve hatta on binde biri seviyelerindedir.[508]

Bilgisayarlarda delilin yeri mutlaka delilin kendi karakterine bağlı değildir. Bir bilgisayarda depolanan bilgiler, "sıfırlar ve birler" ile temsil edilir, bu da depolanan bilgilerin biçimini ve konumunu esnek ve tahmin edilmesi zor hale getirir.[509]

Bununla birlikte bu bilgilerin biçim ve konumları bakımından gerçekleştirilecek bir önceliklendirme çalışması, samanlıkta aranan iğneyi bulma sürecini hızlandırabilecektir.[510]

Bu bakımdan ilk olarak arama kararı çıkartılması aşamasında, genel aramayı düzenleyen CMK m. 119/2-b hükmünde de olduğu gibi, hangi sayısal delilin hangi veri taşıma aracında olabileceğinin, soruşturma veya kovuşturmanın verdiği bilgiler

[505] Değirmenci, *Sayısal Delil,* 74.
[506] Değirmenci, *Sayısal Delil,* 222.
[507] Chaikin, "Network investigations," 242; Robinton, "Courting Chaos," 323; Kerr, "Digital Evidence And The New Criminal Procedure," 301.
[508] Değirmenci, *Sayısal Delil,* 61; Başlar, "Adli Bilişim," 62; Yılmaz ve Çakır, "Mobil Cihaz Adli Bilişimi Süreçleri," 25- 26.
[509] Robinton, "Courting Chaos," 323.
[510] Samanlıkta iğne aramaya benzetilen süreç, inceleme aşamasında gözle görülür hale getirilen verilerin, analiz edilmesi aşamasıdır. Bir tür ayıklama aşaması olarak da kabul edilen bu aşamada, elde edilen verilerin hangilerinin ne ölçüde adli makamlara sunulmak üzere raporlanacağının tespiti yapılır. Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 148.

ışığında belirlenebileceği ve arama kararında bir önceliklendirmeye yer verilebileceği belirtilmiştir.[511]

Ek olarak böyle bir önceliklendirme ile getirilen sınırlamaların, dosya türleri bakımından değil ancak arama yapılacak bilişim sistemi ile aramaya neden olan suç fiili arasında bir bağlantı kurulması suretiyle getirilmesi gerektiği belirtilmiştir. Gerçekten bu şekilde bir sınırlandırma getirilmesinin önemi, bilişim sistemleri üzerinde gerçekleştirilen aramaların, genel aramalara oranla temel hak ve hürriyetleri ihlal potansiyelinin daha fazla olduğu düşünüldüğünde daha iyi anlaşılacaktır. Öyle ki bilişim sistemleri üzerinde herhangi bir sınırlama olmaksızın gerçekleştirilen arama ve elkoyma tedbirleri, özel hayatın gizliliğini tamamen göz ardı etmek anlamına gelecektir.[512]

Bununla birlikte bilişim sistemi üzerinde gerçekleştirilecek arama sırasında bir önceliklendirme işlemi uygulanması suretiyle sınırlama getirilmesi konusunda gizlenmiş verilerin gözden kaçırılmamasına da dikkat edilmelidir. Yukarıda da belirtildiği üzere çeşitli gizleme teknikleri aracılığıyla örneğin .jpg formatına sahip bir suç materyali barındıran resimlerin formatı değiştirilebilmekte yahut bu tarz dosyalar, dikkat çekmemesi adına powerpoint veya excel formatındaki dosyaların içinde gizlenebilmektedir. Gerçekten de delil niteliğini taşıyan verilerin, bilişim sisteminin neresinde olacağı, nerden çıkarılacağı veya hangi formatlarda elde edileceğini önceden tahmin etmek neredeyse imkansızdır. Bu sebeple bilişim sistemi aramalarında önceden aranacak yerlerin belirlenmesi gibi bir sınırlama getirmenin oldukça zorlayıcı olacağı ileri sürülmüştür.[513]

Ek olarak dijital verilerin yapısının da bu tarz bir önceliklendirme çabasına fazla uygun olmadığı ileri sürülmüştür. Fiziksel dünyada gerçekleştirilen aramalar, bir ev veya apartman düzenine göre bir yer aramasının kapsamını sınırlamaktadır. Fiziksel dünyada aranacak alanı sınırlamak, aramanın kapsamı üzerinde önemli bir sınırlama işlevi görür. Ancak böyle bir sınırlama bir bilişim sisteminin aranması sırasında gündeme gelebilmesi neredeyse imkansızdır.[514]

---

[511] Değirmenci, *Sayısal Delil,* 197; Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj)," 67- 68; Yılmaz ve Çakır, "Mobil Cihaz Adli Bilişimi Süreçleri," 25.
[512] Değirmenci, *Sayısal Delil,* 199- 200.
[513] Kerr, "Digital Evidence And The New Criminal Procedure," 304; Turner, "Managing Digital Discovery," 254.
[514] Kerr, "Digital Evidence And The New Criminal Procedure," 302.

Bu gibi sebeplerle getirilebilecek bir sınırlama, bilişim sistemi üzerinde aranacak yerlerin sayılması ve bunların dışına çıkılmaması suretiyle değil fakat aranacak yerlerin hangi sıra izlenerek aranması gerektiği yönünde olabilir. Bu şekilde aramaya neden olan suç fiiline yönelik delillere, daha hızlı ve bilişim sistemi aranan kişi bakımından haklarına daha az müdahale edici şekilde ulaşılabilecektir. Gerçekten de kişilerin, bilişim sistemlerinde gerçekleştirdikleri gizleme çabalarının, bir adli bilişim uzmanının gözünden kaçma olasılığının, kişinin de en az adli bilişim uzmanı kadar bilgili olması gerektiği gerçeği karşısında; bu şekilde adım adım ilerleyen bir önceliklendirme işlemi neticesinde, delil niteliği taşıyan verilerin çoğunluğuna ilk birkaç adımda ulaşılabilecektir.

Ancak tüm bu açıklamaların aksine uygulamada önceliklendirme konusuna dikkat edilmemekte ve bu şekilde hem adli kolluğun işi zorlaşmakta hem de kişilerin özel hayatlarına daha fazla müdahale edilmektedir. Ek olarak böyle bir önceliklendirme olmayışı, gerçekleştirilen aramayı adeta bir keşif aramasına dönüştürdüğü gerekçesiyle de eleştirilmektedir.[515]

Farklı olarak bilişim cihazlarına uzaktan erişmek suretiyle yapılan aramanın (remote search) hukuka uygun olup olmadığı sorununa da değinmek yerinde olacaktır. Uygulamada yalnızca Almanya'da görülen ve ülkemizde hakkında bir düzenleme bulunmayan uzaktan arama yöntemi, teknolojideki akıl almaz ilerleme sonucunda internet veya diğer bilişim ağları üzerinden, bilişim sistem aracına bağlanmak suretiyle ya da kişinin bilişim sistemine uzaktan bir yazılım (trojan horse – truva atı virüsü) yüklenmesi suretiyle kullanıcının bilgisi olmaksızın erişim mümkün olabilmekte ve bu yolla dijital verilere ulaşılabilmektedir.[516]

Uzaktan arama yoluyla kolluk kuvvetleri bir ağa bağlı bilgisayarın sabit diskini veya çalışan diğer belleklerini arayabildiği gibi elektronik posta trafiğinin denetlenmesi, ağ tarayıcısının faaliyetlerinin izlemesi veya internette gerçekleştirilen arama alışkanlıkları ve hatta anlık mesajlaşmaların görüntülenmesi gibi imkanlardan da faydalanabilmektedir.[517] Siber suçlar sözleşmesi m. 32 uyarınca eğer ki kişinin

[515] Değirmenci, *Sayısal Delil,* 197.
[516] Değirmenci, *Sayısal Delil,* 364; Başlar, "Adli Bilişim," 71- 72.
[517] Wiebke Abel, "Agents, Trojans and Tags: The next Generation of Investigators", *International Review of Law, Computers & Technology,* Vol. 23, Nos. 1-2 (March-July 2009): 100.

bilgisayar verileri halka açık bir durumdaysa, o kişinin haberi olmaksızın verilerine ulaşabilmek mümkündür.

Ne var ki Türk hukuku bakımından ise uzaktan aramanın mümkün olmadığını düşünmekteyiz. CMK m. 134'e dayanılarak bu şekilde bir arama hukuken mümkün değildir. Bu sebeple bu şekilde yapılan bir arama sonucu elde edilenler hukuka aykırı delil olmaları sebebiyle hükme esas alınamamakla birlikte zaten böyle bir arama da temel hak ve özgürlüklere ağır müdahale anlamını taşıyacaktır.[518] Öyle ki uzaktan arama ile şüphelinin kendine ait bilişim sistemlerinde arama yapıldığını ve delil toplandığını bilme gibi bir durumu yoktur. Bu nedenle, elde edilecek deliller üzerinde kişinin gözetleme, haklarının korunmasını isteme gibi hakları ortadan kaldırılmakta ve dahası bu delillere kolluk veya üçüncü kişiler tarafından yapılacak hukuka aykırı müdahalelerin de önü açılmaktadır.[519]

Ek olarak uzaktan arama suretiyle delil elde edilmesi işleminde, delillerin güvenilirliği konusunda birazdan bahsi geçecek olan birebir kopya alma işlemi ve bunu takiben özet değer alınması işlemini gerçekleştirmek mümkün olmayacaktır.[520] Bu husus ise delilin gerçekliği, güvenilirliği ve elbette ki hükme esas alınabilmesi konularında şüphelere yol açacaktır. [521]

2.1.2.1.3.2. Kopyalama

Madde uyarınca gerçekleştirilecek inceleme, orijinal sistemin, bir kopyası üzerinden gerçekleştirilecektir. Yapılan arama sonucunda tespit edilen dijital deliller, bunların kopyalanması sonucunda elde edilmiş olacaktır.[522]

CMK m. 134 anlamında "kopyalama"dan anlaşılması gereken şey, verinin kopyalanmasıdır. Verinin kopyalanmasının amacı ise, incelenmesi sonucu delil elde edilecek verilerin, bütünlüğünün ve güvenilirliğinin sağlanmasıdır.[523]

---

[518] Değirmenci, *Sayısal Delil,* 364- 365; Başlar, "Adli Bilişim," 72- 73.
[519] Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 50.
[520] Birazdan bahsedecek olmakla birlikte kısaca birebir kopya ve özet değer alma işlemlerini özetleyecek olursak; birebir kopya işlemi, elde edilen bilişim sisteminin, içerdiği her şey ile birlikte tam ve eksiksiz bir kopyasını oluşturma işlemini ifade ederken özet değer işlemi ise, çıkarılan birebir kopya ile orijinal bilişim sisteminin aynı olduğunu, üzerinde bir değişiklik yapılmadığını ispat etmeye yarayan matematiksel bir fonksiyonu ifade etmektedir. Bkz. Üçüncü Bölüm, *"3.3.1.1. Birebir kopya"* ve *"3.3.1.2. Özet değer"* başlıkları.
[521] Değirmenci, *Sayısal Delil,* 236.
[522] Börekçi, "Bilgisayarlarda, Bilgisayar Programlarında," 94.
[523] Değirmenci, *Sayısal Delil,* 76.

Adli bilişimde, elektronik donanımların içerisinden yapılan birebir kopyalama işlemine birebir kopya, imaj (*forensic image*) adı verilmektedir. Bu kopyalama işlemi, sistemdeki tüm verilerin özel yazılımlar kullanılmak suretiyle ve düşük seviye bit bazında başka bir ortamda bir örneğinin (*imajının yahut görüntüsünün*) oluşturulması ile yapılmaktadır.[524]

"...elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır." ifadesi uyarınca yedeklemenin, elkoymadan sonra değil, el koyma işlemi esnasında yapılması gerekeceğini belirtmemiz gerekir.

Bu konuda Adli ve Önleme Aramaları Yönetmeliği incelenecek olursa m. 17/3 uyarınca elkonulan sistemde yer alan bütün verilerin yedeklemesinin yapılacağı belirtilmekle birlikte cümlenin devamında yedekleme işleminin, *"bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da"* uygulanacağı belirtilmiştir. Bu düzenleme uyarınca çıkarılabilir donanımlardan olan CD, DVD, Flash Bellek ve cep telefonları gibi veri saklama özelliği olan donanımlar da kapsama dahil edilmiştir. İlk bakışta yönetmelik maddesinin, kanunun içeriğini genişlettiği düşünülse de dijital veri odaklı bir bakış açısıyla bakıldığında, CMK m. 134'ün lafzına göre kanuna dahil edilmeyen ve bu sebeple aslında genel arama hükümlerine göre elde edilebilecek olan bu veri saklama özellikli çıkarılabilir donanımların, bir nevi CMK m. 134 korumasına dahil edildiğini görmekteyiz. Bu sebeple biz de bu yönetmelik düzenlemesini yasanın genişletilmesi olarak değil fakat daha gerçekçi ve doğru bir düzenleme olarak görmekteyiz.[525]

Devam edecek olursak, 21/2/2014 tarihli ve 6526 sayılı Kanun m. 11 ile getirilen düzenleme ile *"Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi"* yapılacaktır ve bu yedekten alınan bir kopya şüpheliye veya vekiline (müdafiine) verilerek bu husus tutanağa geçirilerek imzalancaktır. Değişiklikten önce bu kopya, *"istenmesi halinde"* şüpheli veya müdafiine verilmekteydi. Bu bağlamda bu değişikliğin, sonradan delilin üzerinde oynandığı, tahrif edildiği gibi iddiaların önüne geçilmesi adına ve gerek şüphelinin haklarını güvence altına alması gerekse delillerin sıhhatini koruyarak ceza soruşturmasının sağlıklı bir biçimde yürümesini sağlaması bakımından, olumlu bir

[524] Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 66.
[525] Değirmenci, *Sayısal Delil,* 331.

değişiklik olduğunu düşünmekteyiz.[526] Ancak yine de uygulamada elkoyma işlemi sırasında sistemdeki bütün verilerin yedeklemesinin yapılması ve bu yedekten bir kopyanın şüpheli ya da vekiline verilmesi kurallarına halen riayet edilmediği ve bu durumun da itirazlara neden olduğu belirtilmiştir.[527]

Devamında bilgisayardaki verilerin mevcut hâli ile yedeği alındıktan sonra ya da daha doğru bir ifadeyle dijital deliller elde edildikten sonra bilişim sistemi iade edilecektir. Bu bakımından dijital delili ihtiva eden araçlara elkoyma süresinin uzaması durumunda mülkiyet hakkının ihlalinin söz konusu olabileceği ifade edilmiştir.[528]

CMK m. 134/5 uyarınca *"Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası"*nın alınabileceğine yer verilmiştir. Söz konusu fıkra incelendiğinde, sanki önceki fıkraların aksine, elkoyma tedbirinin kural, arama ve kopyalama tedbirinin ise istisna olduğu gibi bir anlam çıkarılabilmektedir. Bu düzenlemenin asıl hedefinin, mümkün olduğu durumlarda el koyma tedbirine başvurmaksızın direkt kopyalama tedbirini gerçekleştirmeleri yönünde uygulayıcıları yönlendirmek olduğunu düşünsek de anlam karmaşasının önüne geçilmesi adına bu fıkranın gözden geçirilmesi yerinde olacaktır.[529]

Yasada düzenlenmemekle birlikte konusu suç teşkil eden delilleri barındıran cihazların iadesi konusuna da değinmek gereklidir. Örneğin, çalınan kredi kartı şifreleri, çocuk pornografisi vb. suç unsuru barındıran bilişim sistemlerinin durumu ne olacaktır? Bu bağlamda uygulamada suç unsuru barındıran bilişim sistemlerinin iade edilmedikleri görülmektedir.[530] Gerçekten de TCK m. 54 "Eşya Müsaderesi" hükümlerinin işletilmesi suretiyle suç eşyası niteliğindeki verilerin ve bunların saklı bulunduğu fiziksel ortamların birlikte eşya müsaderesinin konusunu oluşturabileceğini söyleyebiliriz.[531] Bu doğrultuda elkonulan bilişim sistemlerinde yer alan verilerin, suç konusu veya suçtan kaynaklanan veri olmaları durumunda bunların iadesi söz konusu olmayacaktır. Ancak burada yine TCK m. 54/1 uyarınca veri saklama aracının üçüncü

[526] Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 63; Arslan, "Dijital Delil ve İletişimin Denetlenmesi," 197.
[527] Başlar, "Adli Bilişim," 67-68.
[528] AYM Özgür Güleç Bireysel Başvuru Kararı, BN.2014/1150, T. 31.2.2017, aktaran: Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj)," 71.
[529] Aynı yönde bkz. Dülger, *Bilişim Suçları,* 588.
[530] Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 148.
[531] Değirmenci, *Sayısal Delil*, 376.

bir kişiye ait olması yahut TCK m. 54/3 uyarınca veri saklama aracının *"müsadere edilmesinin işlenen suça nazaran daha ağır sonuçlar doğuracağı ve bu nedenle hakkaniyete aykırı olacağı…"* gibi durumlarda verinin nasıl müsadere edileceği bir sorun olmaya devam etmektedir.[532] Bu gibi durumların önüne geçilmesi adına tarafı bulunduğumuz Siber Suçlar Sözleşmesi m. 19'da yer alan *"bilgisayar sistemindeki bilgisayar verilerinin erişilemez hale getirilmesi veya silinmesi."* gibi bir tedbirin, mevzuatımıza eklenmesinin ve verilerin müsaderesi konusundaki eksikliğin giderilmesinin önemli bir husus olduğunu düşünmekteyiz.[533]

2.1.2.1.3.3. Elkoyma

CMK m. 134 kapsamında "elkoyma"dan anlaşılması gereken veriye el koymadır ve veriye el koymanın amacı ise, bilişim sisteminde yer alan delil niteliğindeki verilere ulaşılması ve söz konusu verilerin muhafaza altına alınmasının sağlanmasıdır.[534] Bir bilişim sistemi yalnızca birkaç dijital delil içerdiğinde, araştırmacıların tüm bilgisayarı toplama yetkisi olmayabilir. Bununla birlikte, bir bilgisayar bir soruşturmada en önemli delil parçasıysa ve büyük miktarda dijital delil içeriyorsa, genellikle bilgisayarın tamamını ve içeriğini toplamak gerekir.[535]

Madde yukarda bahsi geçtiği üzere öncelikle yerinde aramayı (on- site) öngörmüştür. Ancak *"şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması"* gibi ihtimaller gündeme gelirse *"çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere"* elkonulabileceği hüküm altına alınmıştır.

Görüldüğü üzere CMK 134, öncelikle delillerin tespit edilmesini amaçlamaktadır. Bu sebeple yer alan elkoyma tedbiri, geleneksel elkoymadan farklılık arz etmektedir. Öyle ki burada asıl hedeflenen, bilişim sisteminin aranması ve kopyalanmasıdır. Elkoyma yolu ise ancak belli bazı şartların gerçekleşmesi koşuluyla, istisnai bir nitelikte düzenlenmiştir.[536] Buna göre "elkoyma" işlemine ancak

[532] Değirmenci, *Sayısal Delil,* 376.
[533] Kaynakçıoğlu, "Dijital Deliller," 27; Değirmenci, *Sayısal Delil,* 377.
[534] Değirmenci, *Sayısal Delil,* 76.
[535] Casey, *Digital Evidence,* 39.
[536] Börekçi, "Bilgisayarlarda, Bilgisayar Programlarında," 101.

"kopyalama" bakımından ihtiyaç duyulan hallerde başvurulabileceği açıkça anlaşılmaktadır.[537]

Öncelikle 25/7/2018 tarihli ve 7145 sayılı Kanun m. 16 ile getirilen *"işlemin uzun sürecek olması"* koşulu, uygulamada hali hazırda bu sebeple elkonulan ancak diğer koşulların gerekçe olarak gösterilmesi durumunun önüne geçerek bir nevi malumun ilanı niteliğinde bir düzenleme olmuştur. Bu sebeple bu değişiklik ile usule aykırı elkoymaların önüne biraz da olsa geçilebildiğini söylemek yanlış olmayacaktır.[538]

Ancak yine de bu maddenin teknik olarak hatalı olduğunu söylemek gerekir. Gerçekten de bilgisayarlarda yerinde inceleme yapılması çoğunlukla mümkün değildir ve bu bağlamda en basitinden kolluk kuvvetlerinin kopyalama işlemi için kullanacakları cihazların ihtiyaç duyduğu elektriğin nereden sağlanacağı gibi birçok teknik sıkıntı, elkoyma işlemini biraz da mecburen kural haline getirmiştir.[539]

Bu sebeple bizim de katıldığımız görüş uyarınca olması gereken bir düzenleme, delilleri koruyucu ve şüphelinin mağduriyetini önleyici tüm önlemlerin alınması suretiyle, bilgisayara el konulması ve teknik uzmanlar tarafından laboratuvar ortamında incelenmesi olacaktır.[540] Aksi şekilde bir kabul, insan haklarına dayalı bir bakışı kabul etse de mevcut koşullar düşünüldüğünde, hukuka aykırı şekilde gerçekleştirilen elkoyma işlemlerinin devamını sağlamaktan başka bir işe yaramayacaktır.

Devam edecek olursak şifreli verilerde, şifre çözme anahtarlarının cihaz sahibinden ya da üçüncü kişilerden istenip istenemeyeceği hususu üzerinde durmak gereklidir. Anayasa m. 38/5'te yer alan *"kişinin kendini suçlayan beyanda bulunmaya zorlanamaması"* (nemo tenetur se ipsum accusare) ilkesi uyarınca *"Hiç kimse kendisini… suçlayan bir beyanda bulunmaya veya bu yolda delil göstermeye"* zorlanamayacaktır. Görüldüğü üzere madde, beyanla sınırlı kalmayıp, kişinin kendi aleyhine delil göstermeye zorlanmasını da yasaklamıştır. Bu bakımdan kişinin bilişim

[537] Arslan, "Dijital Delil ve İletişimin Denetlenmesi," 197.
[538] Başlar, "Adli Bilişim," 67.
[539] Benzer şekilde *Jones* da bir bilgisayar içindeki delillere ulaşma, verileri kurtarma gibi işlemlerin yapılabilmesinin, doğal olarak o anda ve olay yerinde mümkün olamayacağı ve bunun için bilgisayarın muhafaza altına alınması ve götürülmesi gerektiğini belirtilmiştir. Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 145.
[540] Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 63.

sisteminde yer alan verilerini korumak için kullanmış olduğu şifre anahtarını teslim etmeye zorlanması ve zorlanarak elde edilen anahtarın kullanılması suretiyle elde edilecek verilerin, kişinin aleyhine kullanılması; kişinin kendi aleyhine delil göstermeye zorlandığı anlamına gelecektir.[541] Nitekim benzer şekilde şüphelinin şifre anahtarını teslim etmemesi de suçu işlediğine yönelik aleyhine bir delil olarak değerlendirilemeyecektir.[542]

Devamında ise ispat bakımından yararlı görülen ancak olay yerinde incelemesi yapılamadığı için elkonulan eşyanın mühür altına alınması gerekecektir. El konulan bilişim sisteminin saklanması konusunda ise karşımıza, Suç Eşyası Yönetmeliği[543] çıkmaktadır. Buna göre "Suç eşyasının muhafazası" başlığını taşıyan m. 8/3 uyarınca;

> *"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."*

İleride mührün kaldırılması ve eşyanın incelenmesine karar verildiği takdirde, bu işlemin yapılmasında hazır bulunmak üzere eşyanın sahibi veya müdafi/vekilinin de çağrılması gereklidir.[544] Son olarak elkonulan bilgisayar, bilgisayar programları ve bilgisayar kütükleri, *"şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde… gecikme olmaksızın iade"* edilecektir. Konusu suç oluşturan veri taşıma araçlarının iadesi ile ilgili yukarıdaki[545] görüşlerimizi burada da yinelemekle yetiniyoruz.

2.1.2.1.4. Tedbirin şartları

2.1.2.1.4.1. Bir suç dolayısıyla yapılan soruşturma

Burada ilk olarak karşımıza *"bir suç dolayısıyla"* ibaresi çıkmaktadır. Buradan anlaşılacağı üzere söz konusu tedbire, mahiyeti ve cezası ne olursa olsun her suç tipi

---

[541] Değirmenci, *Sayısal Delil,* 265- 266; Başlar, "Adli Bilişim," 71.
[542] Buna karşılık, yukarıda da belirttiğimiz üzere, bazı ülkelerde, şüphelilerin şifrelerini açıklamaya zorlanabilecekleri "anahtar ifşa düzenlemeleri"nin bulunduğunu yinelememiz gerekir. Buna göre şifresini vermeyi reddeden kişi, sırf şifresini açıklamadığı için suçlanabilmektedir. İngiltere ve Avustralya bu uygulamanın en belirgin örneklerindendir. Bkz. Drewer and Ellermann, "The Online Environment as a Challenge," 144.
[543] Resmî Gazete Tarihi: 23 Mart 2016 Çarşamba, Sayı: 29662.
[544] Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj)," 70.
[545] Bölüm 2., "2.1.2.1.3.2. Kopyalama" başlığı.

için başvurulabilecektir.[546] Bu bağlamda yalnızca siber suçların soruşturmalarında değil, aynı zamanda nitelikleri itibariyle ceza muhakemesinde dijital delile ihtiyaç duyulan her suçun soruşturulmasında bu tedbire başvurulabilecektir[547]. Ancak bu durum, tedbirin, CMK m. 135 "İletişimin Tespiti, Dinlenmesi ve Kayda Alınması" koruma tedbirinde olduğu gibi katalog suçlara değil, fakat bütün suçlara uygulanabiliyor oluşu nedeniyle çeşitli insan hak ve özgürlükleri ihlali kaygıları gerekçesiyle eleştirilmiştir.[548]

İkinci olarak *"bir suç dolayısıyla yapılan soruşturma"*nın varlığı gerekmektedir. Buna göre bir idari soruşturma, önleme araması yahut önalan araştırması sırasında bu tedbire başvurulamayacaktır.[549] Ancak, bu şartı dar anlamda yorumlamamak gerekir. Zira, kovuşturma aşamasında eksik deliller söz konusu ise, elbette bu aşamada da CMK m. 134 uyarınca koruma tedbiri kararı verilebilecektir.[550] Ek olarak CMK m. 192/1 *"Mahkeme başkanı veya hâkim… delillerin ikame edilmesini sağlar."* hükmü uyarınca delillerin toplanması aşamasının, soruşturma aşaması ile sınırlı olmadığını ve gerektiğinde kovuşturma aşamasında da delillerin elde edilebileceğini söyleyebiliriz.

Buna karşılık tedbire kovuşturma aşamasında başvurulmasının, sanığın hakkında uygulanacak tedbiri, aleni duruşmada öğrenmesi neticesinde ilgili bilişim sisteminde yer alan verileri silebileceği ve bu sebeple de bilişim sistemine elkonulsa dahi muhakeme süreci açısından faydalı bir bilgi elde edilemeyeceği gerekçesiyle anlamını yitireceği ve bu sebeple tedbire kovuşturma aşamasında başvurulmaması gerektiği belirtilmiştir.[551] Benzer şekilde, kanunda açıkça tedbire soruşturma aşamasında başvurulabileceğinin belirtilmesi sebebiyle, tedbire kovuşturma aşamasında başvurulamayacağı, aksi durumun kanuna aykırılık sonucunu doğuracağı belirtilmiştir.[552] Ancak biz de daha önce tespit edilemeyen, fakat sanık tarafından kullanılan ve delil niteliği taşıyan bilişim sistemlerinin, kovuşturma aşamasında ortaya

[546] Arslan, "Dijital Delil ve İletişimin Denetlenmesi," 196.
[547] Değirmenci, *Sayısal Delil,* 310.
[548] Arslan, "Dijital Delil ve İletişimin Denetlenmesi," 196.
[549] Değirmenci, *Sayısal Delil,* 333; Börekçi, "Bilgisayarlarda, Bilgisayar Programlarında," 79.
[550] Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 62.
[551] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 491.
[552] Yenisey ve Nuhoğlu, *Ceza Muhakemesi Hukuku,* 449.

çıkabileceği gibi ihtimaller sebebiyle tedbire kovuşturma aşamasında da başvurulabileceğini düşünmekteyiz.[553]

Yine birazdan daha ayrıntılı bahsedeceğimiz *"başka surette delil elde etme imkanının bulunmaması"* koşulu düşünüldüğünde, hakkında yeterli şüphe derecesine ulaşılan ve bu vesileyle iddianame hazırlanabilecek düzeyde delil elde edilen bir maddi olayda, bilişim sistemlerinin aranması, kopyalanması ve elkonulması tedbirine gerek olmaksızın delil elde edildiği ve zaten iddianamenin de bu delillerle hazırlandığı, bu sebeple de artık bu tedbire başvurulamayacağı çünkü başka surette delillerin elde edilebildiği düşünülebilir. Bu konuyla ilgili olarak ise, *"başka surette delil elde etme imkanının bulunmaması"* koşulunun, soruşturma ve kovuşturma aşamalarında ayrı ayrı değerlendirilmesi gerekeceğini, öyle ki soruşturma aşamasında elde edilen delillerin, iddianamenin hazırlanabilmesi bakımından yeterli olabileceği, fakat kovuşturma aşamasında vicdani kanaati oluşturmak bakımından yeterli olmayabileceğini; bu bakımdan da kovuşturma aşamasında bu tedbire başvurulamayacağının söylenmesinin, soruşturma aşamasında olası tüm delillerin toplandığı kabulü anlamına geleceğini ancak böyle bir kabulün, hayatın olağan akışına aykırı bir kabul olacağını söylemek gerekecektir.[554]

2.1.2.1.4.2. Somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı

Tedbire başvurulabilmesi için gerçekleşmesi gereken bir diğer şart "*somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı*"dır. Bu düzenlemeyle, kanun koyucunun CMK m. 134'ün uygulanmasını isabetli bir biçimde zorlaştırdığı ve ancak kuvvetli şüphe doğuracak somut nitelikte olan emarelerin varlığı halinde bu tedbirin uygulanması yönünde kesin bir irade ortaya koyduğu anlaşılmaktadır.[555] Buradaki kuvvetli şüphe, hem şüphelinin soruşturma konusu suçu işlediği yönünde olmalıdır (ki bu durum, şüphenin belli bir yoğunluğa ulaşmaksızın kişilerin haklarına müdahale teşkil edecek olan koruma tedbirlerine başvurulamamasının bir sonucudur), hem de arama tedbirinin üzerinde gerçekleştirileceği bilişim sisteminde suç delillerinin bulunabileceği yönünde olmalıdır. Öyle ki soruşturma konusu suçun ilgili kişi tarafından işlediğine yönelik kuvvetli şüphe bulunsa bile kişinin kullandığı bilişim sisteminde, soruşturulan suça ilişkin bir delil olabileceği yönünde bir beklenti yoksa

[553] Değirmenci, *Sayısal Delil,* 335.
[554] Değirmenci, *Sayısal Delil,* 335.
[555] Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 62.

söz konusu bilişim sisteminde veri elde edilmesi amacıyla arama gerçekleştirilmesi de mantıklı olmayacaktır.[556]

2.1.2.1.4.3. Başka surette delil elde etme imkanının bulunmaması

Tedbire başvurulabilmesi için başka surette delil elde etme imkanının bulunmaması gerekmektedir. Bir başka deyişle, bilgisayarlarda arama ve el koyma işleminin yapılması delil elde etme açısından *son çare* olmalıdır.[557] Bununla birlikte son çare olma ilkesi, tedbir ile elde edilebilecek faydanın, bu tedbire son çare olarak başvurulması durumunda azalacağı ve hatta ortadan kalkabileceği gerekçesiyle eleştirilmiştir.[558]

Gerçekten de tedbire son çare olarak başvurulması ilkesi, diğer tüm yolların denenmesi ve neticesinde delil elde edilememesi, sonrasında bu tedbire başvurulması şeklinde anlaşılırsa bu kaygılar gündeme gelebilecektir. Öyle ki şüphelinin hakkında diğer koruma tedbirleri uygulanmak suretiyle delil elde edilmeye çalışılması ancak bunlardan delil elde edilememesi halinde bilişim sisteminin aranması gibi bir durum, şüphelinin kullandığı bilişim sisteminde yer alan delilleri tahrif etmesi, gizlemesi veya yok etmesi gibi sonuçlara vücut verebilecektir.

Bu sebeple başka surette delil elde edilememesi koşulu, hiçbir yoldan sonuç alınamaması neticesinde ancak bu tedbire başvurulabilir şeklinde anlaşılmamalıdır. Burada kabul edilmesi gereken, başka yollara başvurulsa dahi hiçbir surette delil elde edilemeyeceği şeklinde oluşan ve mümkünse desteklenen bir kanaattir.[559] Gerçekten de Cumhuriyet savcısı veya hâkim, diğer delil elde etme yöntemlerinin fayda etmeyeceği konusunda bir kanaat oluşturur ve bunu gerekçelendirebilirse, bilişim sistemlerinde arama kopyalama ve elkoyma tedbiri yoluna gidebilmelidir. Bu sayede tedbir ile elde edilmesi beklenen fayda minimum düzeyde etkilenmiş olacaktır.

2.1.2.1.5. Tedbir kararını verecek mercii

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama veya elkoyma kararına hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından karar verilecektir. Cumhuriyet savcısı tarafından verilen kararlar ise

[556] Değirmenci, *Sayısal Delil,* 352- 353.
[557] Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 562.
[558] Dülger, *Bilişim Suçları,* 585.
[559] Değirmenci, *Sayısal Delil,* 342- 343.

yirmi dört saat içinde hâkim onayına sunulacaktır. Hâkim de kararını en geç yirmi dört saat içinde verecektir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde çıkarılan kopyalar ve çözümü yapılan metinler derhâl imha edilecektir.[560]

2.1.2.1.6. Tedbirin hakkında uygulanacağı kişi

CMK m. 134/1 *"şüphelinin kullandığı"* bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama, kopyalama ve elkoymadan söz etmiştir. Buradan yola çıkarak aranacak bilişim sisteminin, şüpheliye ait olması gibi bir zorunluluğun bulunmadığını, yalnızca şüpheli tarafından kullanılmış olmasının[561] yeterli göründüğünü söyleyebiliriz.[562]

"Şüphelinin kullandığı" ifadesi de yine yukarıda değindiğimiz şekilde tedbirin yalnızca şüpheli hakkında uygulanabileceği ve dolayısıyla bu tedbire yalnızca soruşturma aşamasında başvurulabileceği şeklinde anlaşılmalara vücut verebilecektir. Gerçekten lafzi yorumlama metodu ile düşünüldüğünde bu tedbire kovuşturma aşamasında başvurulamayacağı sonucuna ulaşılabilir.[563] Buna karşılık ceza muhakemesinin kendisine yüklenen işlevi yerine getirebilmesi amacıyla gerekildiği hallerde bu tedbire kovuşturma aşamasında da başvurulabileceğini ve yukarıda belirttiğimiz gerekçelerle birlikte yineliyoruz.

2.1.2.1.7. Üçüncü kişilerde bulunan dijital deliller

Türk hukukunda bazı dijital deliller Cumhuriyet savcısının genel delil toplama yetkisi kapsamında elde edilebilecektir. Özellikle diğer koruma tedbirlerinin alanına girmeyen, daha çok üçüncü kişilerde bulunan dijital ortamdaki veriler Cumhuriyet savcısı tarafından elde edilebilecektir. Bu kapsamdaki verilere örnek olarak sosyal paylaşım sitelerindeki bazı veriler, dijital kameralardaki veriler, bankalar gibi üçüncü kişilerde bulunan veriler gösterilebilir.[564]

---

[560] 25/7/2018 tarihli ve 7145 sayılı Kanun m. 16 ile "Cumhuriyet savcısının istemi üzerine" ibaresi "hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından" şeklinde değiştirilmiştir.

[561] Bilişim sisteminin *"kullanılmış olması"* kavramının belirlenmesi önem arz etmektedir. Öyle ki bir bilişim sistemine fiili ve sanal olmak şekilde iki şekilde erişilerek bu sistemler kullanılabilecektir. Burada kabul edilmesi gerekenin "fiziksel" olarak kullanma olduğunu belirtmekle birlikte bilişim sistemlerinin fiili ve sanal kullanım ile ilgili detaylı bilgi için bkz. Değirmenci, *Sayısal Delil,* 321.

[562] Değirmenci, *Sayısal Delil,* 318; Dülger, *Bilişim Suçları,* 582.

[563] Yenisey ve Nuhoğlu, *Ceza Muhakemesi Hukuku,* 449.

[564] Değirmenci, *Sayısal Delil,* 387.

Bunun dışında şüpheli veya sanık dışındaki kişilerin, bilişim sistemlerinde CMK m. 134 kapsamında bir arama, kopyalama ve elkoyma kararı verilip verilemeyeceği hususuna da değinmek yerinde olacaktır.

Öncelikle tedbirin yazım şekli incelendiğinde, hitap ettiği kişinin şüpheli (veya sanık) olduğu görülmektedir. İkinci bir açıdan bakılacak olursa yukarıda da belirtildiği üzere CMK m. 134, genel aramayı düzenleyen CMK m. 116 ve devamı hükümlerinin özel bir halini oluşturmaktadır. CMK m. 116, şüpheli ve sanık hakkında gerçekleştirilecek arama tedbirini düzenlerken, CMK m. 117, diğer kişilerle ilgili arama tedbirini düzenlemektedir. Bu bağlamda biz de kişilerin bilişim sistemlerinde gerçekleştirilen aramanın, temel hak ve özgürlüklere, genel aramaya oranla daha fazla müdahale edeceğini öngören yasa koyucunun, diğer kişilerin bilişim sistemlerinde de arama yapılmasını isteseydi, genel aramada olduğu gibi ayrı bir şekilde düzenleme getireceğini düşünmekteyiz.[565]

Sonuç olarak diğer kişilerin bilişim sistemlerinde CMK m. 134 anlamında gerçekleştirilecek bir aramanın, ancak ilgili bilişim sisteminin şüpheli (veya sanık) tarafından kullanılan bir bilişim sistemiyse gerçekleştirilebileceğini söyleyebiliriz.

2.1.2.1.8. Tesadüfen elde edilen deliller

Tesadüfen elde edilen delil kavramı, soruşturma makamlarının, hukuka uygun olarak delil elde etme yöntemlerini uygulamaları sırasında ilgili soruşturma ya da kovuşturma konusu suç dışında bir başka suç unsuruna ait olan delillere rastlanmasına işaret etmektedir.[566]

Bilişim sistemlerinde arama sırasında tesadüfen delil elde edilmesi konusunda karşımıza CMK m. 138/1 çıkmaktadır. Buna göre;

> *"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."*

Görüldüğü üzere kanun, yürütülmekte olan soruşturma veya kovuşturmayla ilgisi olmamakla birlikte diğer bir suçun işlendiği şüphesini uyandıracak delilleri kapsama almıştır. Buna karşılık Adli ve Önleme Aramaları Yönetmeliği m. 10/a ise

[565] Değirmenci, *Sayısal Delil,* 319.
[566] Afandak, "Ceza Muhakemesinde Dijital Deliller," 140.

kanunda olmayan yeni bir şart getirmiştir. Buna göre *"Yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmakla birlikte, karar veya yazılı emirde konu edilmeyen bir delil elde edilirse"* de bu deliller, tesadüfen elde edilen delil kavramı altında değerlendirilebilecek ve bunlara el konulabilecektir. Yönetmelikte yer alan bu ek madde, CMK m. 138/1'de yer alan tesadüfen elde edilen delil kavramını genişlettiği gerekçesiyle eleştirilmiştir.[567]

Geri dönecek olursak tesadüfen elde edilen delil kavramının, yukarıda bahsi geçen içtihat hukukunun yaratmış olduğu aşikâr bir biçimde belli olma (plain view doctrine) öğretisinin karşılığı olduğunu belirtmiştik.[568] Yineleyecek olursak aşikâr bir biçimde belli olma öğretisi uyarınca başka bir suça aşikâr bir biçimde işaret etmediği sürece elde edilen delil ile ilgili ayrıca bir araştırma yapılması yasaklanmıştır. Geleneksel deliller bakımından uygulanması büyük sıkıntılar doğurmayan bu öğreti, zamanla teknolojinin gelişmesi ve dijital verilerin de suçların aydınlatılmasında delil değeri taşımaya başlamasıyla birlikte çeşitli sıkıntılara vücut vermeye başlamıştır. Söz konusu sıkıntılar ise başka bir suça işaret eden bulguların, tesadüfen elde edilen delil olarak kabul edilebilmesindeki sınırlarda karşımıza çıkmaktadır. Gerçekten de yürütülen soruşturma veya kovuşturmanın konusunu oluşturan suç sebebiyle yürütülen bir arama kararı esnasında, farklı bir suça ilişkin delillere ulaşma amacıyla hareket edilmişse yahut, söz konusu arama kararı, diğer bir suça ilişkin delillerin bulunabilmesi amacıyla bir araç olarak kullanılmışsa ulaşılan deliller, tesadüfen elde edilen delil olarak kabul görmeyecekler ve bu sebeple hükme esas alınmayacaklardır.[569] Öyle ki gerçekleştirilen eylem artık *tesadüf etme* fiilinden ziyade yeni ve farklı bir arama eylemine dönüşmüştür.

Açıklamalar neticesinde bir delilin tesadüfen elde edilmiş sayılabilmesi için başka suçlara ilişkin delillerin elde edilmesi saikiyle hareket edilmemesi gerektiği ve gerçekleştirilen aramanın, yalnızca arama konusu suç fiiline yönelik delillerin elde edilmesi amacıyla gerçekleştirilmesi gerektiğini söyleyebiliriz. Bunlara rağmen yine de başka bir suça ilişkin delillere tesadüf ediliyorsa söz konusu deliller, tesadüfen elde edilen deliller olarak değerlendirilebileceklerdir.

---

[567] Değirmenci, *Sayısal Delil,* 448.
[568] Bölüm 1, *"1.3.2.1. İçtihat hukuku"* başlığı.
[569] Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* 519; Tezcan, v.d., *Dijital Ceza Muhakemesi Hukuku,* 561.

Gelinen nokta itibariyle tesadüfen elde edilen delillerle ilgili çizilen sınırlar, geleneksel arama tedbirinde anlam bulabilmektedir. Gerçekten de örneğin silahla yaralama fiili neticesinde suç eşyasının aranması sırasında şüphelinin evinde bulunan belgeler arama kararının kapsamı dışında incelenirse ve bu belgelerde de şüphelinin dolandırıcılık suçunu işlediği ve dolandırdığı kişilerin finansal bilgilerinin yer aldığı anlaşılırsa; söz konusu bulgular tesadüfen elde edilen delil kavramı altında değerlendirilemeyecek fakat hukuka aykırı delil olarak değerlendirilecektir. Çünkü söz konusu belgelerin incelenmesi anıyla birlikte artık silahla yaralama fiiline ilişkin delillerin elde edilmesi amacıyla gerçekleştirilen arama kararının sınırları dışına çıkılmaya başlanmıştır. Gerçekten de suç eşyası niteliğinde olabilecek araç, belgelerin arasında olamayacaktır. Bir şekilde belgelerin arasına saklansa dahi söz konusu belgelerde yazan satırlar, arama eyleminin sınırları dışında kalacaktır. Gerçekleştirilen arama eyleminin, silahla yaralama eylemi neticesinde alınan arama kararının sınırları dışına çıkması sebebiyle de söz konusu belgelerin incelenmesi bir hukuka aykırı aramaya vücut verecektir. Elbette hukuka aykırı arama çerçevesinde elde edilen şeyler de hukuka aykırı olacağı için delil niteliğinden yoksun olacaklardır.

Buna karşılık tesadüfen elde edilen delil kavramı ile ilgili çizilen bu sınırlar, bilişim sistemlerinin aranması tedbirinde oldukça belirsiz ve silik kalmaktadır. Açıklamak gerekirse ilk başta bir suçun aydınlatılması için şüpheli veya sanığın bilişim sisteminde araştırılma yapılırken şüphelinin bilişim sisteminin kopyası, adli bilişim uzmanları tarafından incelenir. Adli bilişim laboratuvarında gerçekleştirilen bu inceleme elbette orada bulunan bilgisayarlar üzerinden gerçekleştirilir. Bu adımda karşımıza çıkan ilk sıkıntı, "*Aramanın yapılacağı eşya"* (CMK m. 119/2-b) olarak nitelendirilebilecek şüpheli veya sanığın kullandığı bilişim siteminin, bütün detayları ve suçla ilgili veya ilgisiz tüm bulguları ile birlikte adli bilişim uzmanının, arama fiilini gerçekleştirdiği bilgisayarın ekranında görünüyor olmasıdır.[570] Bu durum ise incelemede bulunan kişilerin delil incelemesi yaptıkları ekranlardan her zaman her şeyi görebildikleri düşünüldüğünde; dijital delillerin elde edilmesi hususunda çıkartılan arama kararlarını, "genel arama" kararlarına dönüştürdüğü gerekçesiyle eleştirilmiştir. Bu sebeple de fiziksel delillerin elde edilmesi sırasında bir şekilde anlamlı olan tesadüfen elde edilen delil (aşikâr biçimde belli olma öğretisi)

[570] United States v. Gray, 78 F. Supp. 2d 524, 531 n.11. Aktaran: Robinton, "Courting Chaos," 333.

kavramının, dijital delillerin elde edilmesi bakımından anlamını yitirdiği belirtilmiştir.[571]

Bu sıkıntıyla ilgili olarak özellikle ABD'de hem akademisyenler hem de mahkemeler, dijital aramaların fiziksel olay yeri aramalarıyla karşılaştırılamayacağı ve karşılaştırılmaması gerektiğini ileri sürmüş ve dijital medyanın muazzam depolama kapasitelerine atıfta bulunmuşlardır.[572] Dijital aramalarla ilgili olarak bilgisayar aramaları sırasında bilgisayarlarda bulunan her dosyanın incelenmesi gerekliliği düşüncesi yerine, kolluk kuvvetlerinin veri aramalarını dosya türüne göre sınırlamaları veya ilgili dosyaları bulmak için anahtar kelime aramaları kullanmaları önerilmiştir ve ek olarak başka bir suçun işlenmiş olabileceğine işaret eden delilleri de barındıran dosyaların incelenmemesi, o noktada durulması ve incelemeye devam edilmesi için bir onay mekanizması getirilmesi ve bu onayın da hâkim kararına dayanması gerektiği önerilmiştir.[573] Bu görüş, ilk defa *United States v. Carey*[574] davasında kabul edilmiş ve *carey- winick* görüşü olarak anılmaya başlanmıştır. Ancak bazı mahkemelerce bu görüş kabul edilmekle[575] beraber diğerleri, bu görüşün kusurlarına atıfta bulunarak incelemeyi çok kısıtladığı gerekçesiyle kabul etmemişlerdir.[576]

Gerçekten de günümüzde suçlular, dijital delilleri onları inceleyenlerin tahmin edemeyecekleri şekillerde gizleyebilmektedirler. Bu bağlamda *carey- winick* görüşü

---

[571] Robinton, "Courting Chaos," 333; Kerr, "Digital Evidence And The New Criminal Procedure," 305.
[572] United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999), aktaran: Robinton, "Courting Chaos," 339.
[573] Raphael Winick, "Searches and Seizures of Computers and Computer Data," *Harvard Journal of Law & Technology*, vol. 8, no. 1 (1994): 105. Aktaran; Robinton, "Courting Chaos," 339.
[574] United States v. Carey, 172 F.3d 1268 (10th Cir. 1999), Söz konusu davada ele geçirilen bir sabit diskte kokainle ilgili kanıt arayan bir memur, çocuk pornografisi görüntülerine rastlamıştır. Sonrasında memur narkotikle ilgili kanıt aramayı bırakmış ve sonraki birkaç saati çocuk pornografisi görüntülerini arayarak geçirmiştir. Mahkeme bu olayda aşikâr biçimde belli olma öğretisine aykırı olarak memurun, sübjektif düşünceyle hareket ettiğine ve bu sebeple araştırmasının odağını bir kanıt türünden diğerine değiştirdiği için, arama kapsamı dışındaki kanıtların keşfedilmesine izin vermemiş ve çocuk pornografisine ilişkin delillerin gizlenmesine karar vermiştir. Aktaran: Robinton, "Courting Chaos," 340; Kerr, "Digital Evidence And The New Criminal Procedure," 316- 317.
[575] Örneğin önceki olaya benzer bir davada bilgisayar korsanlığı kanıtı için bir arama emri uyarınca ele geçirilen bir sabit diski inceleyen bir memur, bir çocuk pornografisi görüntüsüne rastlamıştır. Ancak müfettiş, bilgisayar korsanlığı kanıtı aramaya devam etmiştir. Fakat yol boyunca keşfettiği ek çocuk pornografisi görüntülerini de kaydetmiştir. Mahkeme, memurun gerçekleştirdiği aramayı izin kapsamında tuttuğuna hükmederek çocuk pornografisine ilişkin delillerin kabul edilebilirliğini onaylamıştır. Bkz. United States v. Gray, 78 F. Supp. 2d 524- 544. (E.D. Va. 1999). Aktaran: Kerr, "Digital Evidence And The New Criminal Procedure," 317; Leacock, "Search and Seizure of Digital Evidence," 222.
[576] Robinton, "Courting Chaos," 340.

çerçevesinde veri aramaları, dosya türüne göre sınırlandırılırsa birçok suça ilişkin delil, gizli kalacak ve suçlar aydınlatılamayacaktır.[577]

İkinci bir eleştiri farklı bir suça ışık tutan bir delile erişildiğinde o aşamada durulması ve delilin işaret ettiği suç bakımından ikinci bir arama kararı çıkartılması önerisine getirilmiştir. Söz konusu eleştiri, ilk olarak bu önerinin öncelikle aşikâr biçimde belli olma öğretisinin korumayı hedeflediği amaçlardan biri olan özel hayatın gizliliği gibi hakları ihlal edebileceği yönündedir. İkinci olarak, ikinci bir arama kararının çıkartılmasının, aynı öğretinin "aşikâr bir biçimde başka bir suça işaret etme" kuralının da anlamını yitirmesine neden olacağı yönündedir. Gerçekten de dijital delil araştırması sırasında ikinci bir suça ilişkin deliller zaten somut bir şekilde elde edilmiştir ve adli bilişim uzmanının ekranındadır. Bu sebeple o aşamada ikinci bir arama kararı çıkartılması oldukça basitleşecek ve adeta malumun ilanı haline gelecektir.[578]

Söz konusu eleştirilere bir çözüm olarak getirilen bir öneri, bilişim sistemi aramalarında aşikâr biçimde belli olma öğretisinin kaldırılması yönünde olmuştur. Bu bağlamda bir arama emri kapsamı dışında keşfedilen dijital delillerin kabul edilemez olduğuna dair bir kuralın, hedeflenen bir aramanın bir genel aramaya dönüşmesini engelleyeceği belirtilmiştir.[579]

Farklı olarak ve bizce de daha adaletli bir görüş olarak, bahsedilen sıkıntıların çözümü adına var olan aşikâr biçimde belli olma öğretisinin yorumlanması bakımından bazı kurallar getirmekten ziyade gizlilik ve adalet arasında ölçülü bir şekilde yeni bir düzenleme getirilmesi önerilmiştir. Bu düzenlemenin ise şu üç hususu barındırması gerekliliği belirtilmiştir. Öncelikle aramaların kapsamları daraltılmalı ancak belli bazı koşullarda tüm dosyalara erişime izin verilmelidir. İkinci olarak soruşturma konusu suçla ilgisi olmayan başka bir suça işaret eden deliller bakımından ikinci bir arama kararı çıkartılmalı ancak aşikâr biçimde belli olma öğretisi kapsamında değerlendirilebilen deliller bakımından doğrudan el koymaya izin verilmelidir. Üçüncü ve son olarak ise kişisel nitelikte veriler içeren dosyaların veya

[577] Thomas K. Clancy, "The Fourth Amendment Aspects of Computer Searches and Seizure: A Perspective and a Primer," *Mississippi Law Journal*, vol. 75, (2005): 206-207.
[578] Robinton, "Courting Chaos," 341.
[579] Kerr, "Digital Evidence And The New Criminal Procedure," 314.

üçüncü kişilere işaret eden delillerin, başka bir objektif kişi veya kurum tarafından yapılacak değerlendirmeye tabii tutulması gereklidir.[580]

2.1.2.1.9. Dijital olay yeri incelemesi

Dijital delilin elde edilmesi aşamalarının ilk olan dijital delilin toplanması aşamasında karşımıza *olay yeri* kavramı çıkmaktadır. Adli Arama Önleme Aramaları Yönetmeliği[581] çerçevesinde yapılan bir tanım uyarınca olay yeri incelemesi;

> *"suçun aydınlatılması amacıyla olay yerlerinde her türlü iz, eser, emare ve delil niteliği taşıyabilecek bulguların uzmanlaşmış personelce, çeşitli bilimsel, teknik yöntem ve metot kullanarak araştırılması, elde edilen bulguların tespit edilmesi ve kayıt altına alınması (belgelenmesi), toplanması, muhafazası ve incelenmek üzere ilgili yerlere gönderilmesini sağlayan özel amaçlı bir araştırma işlemi"* şeklinde tanımlanmıştır.[582]

Elbette delillerin dijitalleşmesi, beraberinde olay yerinin de dijitalleşmesi sonucunu getirmiştir. Bilişim sistemlerinin gündelik hayatta yaygın kullanımı, bilişim sistemlerini suçun hedefi haline getirdiği gibi olay yerinin de fiziksellikten sıyrılıp bilişim sistemlerinin oluşturduğu sanal bir alana kaymasına neden olmuştur.[583] Dijital delillerin elde edildiği suçlarda da olay yeri artık bilgisayar sistemleri yahut dijital bilgi saklama ortamları, bilgisayar ağları ve internetin sanal sonsuzluğu haline dönüşmüştür.[584]

Delillerin sağlıklı bir şekilde toplanabilmesi, olay yerine yapılan ilk müdahalenin ne kadar sağlıklı olduğuna bağlıdır. Bu bağlamda adli bilişim uzmanının, delil kaybını en aza ve hatta sıfıra indirgeyebilmesi için gerekli olan bilgiye ve deneyime sahip olması, ek olarak suçlular tarafından düzenlenmiş ve verilerin kaybına yol açabilecek tuzaklara karşı dikkatli olmaları gereklidir.[585]

Elde edilen delillerin, toplandıkları aşamadan sonra mahkemeye sunulana kadar ve devamında mahkemenin söz konusu maddi olay hakkına bir hüküm tesis etmesi aşamasına kadar korunması gerekir. Bu süreç, potansiyel dijital delilin bütünlüğünün ve orijinal durumunun korunması sürecidir. Başka bir ifadeyle dijital delilin, değişikliklere karşı korunmak için güvenli bir şekilde saklanması, delil

---

[580] Robinton, "Courting Chaos," 347.
[581] Resmî Gazete Tarihi: 01.06.2005, Sayı: 25832
[582] Say, "Bilişim Suçlarında Elde Edilen Deliller," 22.
[583] Değirmenci, *Sayısal Delil,* 125.
[584] Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku*, 38- 39.
[585] Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 145; Dülger, *Bilişim Suçları,* 613.

zincirinin kaydedilmesi ve delile erişimine izin verilen kişilerin delilleri işlemeye yetkili kişilerle sınırlandırılması gerektiği anlamına gelmektedir.[586]

Bilişim sistemi laboratuvara taşınırken donanımın hassas yapısı gereği, dikkatlice paketlenmesi ve yine aynı dikkatle taşınması gerekir. Sarsıntı, elektrik akımları, elektromanyetik ortamlar, aşırı sıcak ya da sıvı maddelerle teması, bu aygıtların işlevini yitirmesine neden olacaktır ki bu da potansiyel delillerin kaybı ile sonuçlanacaktır. Ayrıca paketlemenin, statik elektrikten ve manyetik alanlardan etkilenmeyecek biçimde yapılması da gerekmektedir.[587] Öyle ki olay yerinden elde edilen delillerin laboratuvara getirilmesine kadar geçen süreçte delillerin bozulmadan saklanması, olay yeri inceleme süreci kapsamında bulunmaktadır.[588]

2.1.2.2. İletişimin tespiti, dinlenmesi ve kayda alınması (CMK m. 135)

Dijital verilere ilişkin olarak yasada yer verilen koruma tedbirlerinden bir diğeri İletişimin Tespiti, Dinlenmesi ve Kayda Alınması tedbiridir.[589] Bilişim sistemleri aracılığıyla işlenen ve saklanan veri, aynı zamanda sistemler arasında da transfer edilebilmektedir. Bu transfer esnasında elde edilen verilerin de dijital delil niteliği bulunabilecektir.[590] Öyle ki transfer sırasında veriler, bilgisayar ağı içerisinde bir akış izi bırakırlar. Bu ize ise iletişimin denetlenmesi bakımından sinyal bilgisi adı verilir. Bu sinyal bilgilerinin ise daha sonradan analiz edilmesi adına elde edilmeleri ve saklanmaları, söz konusu tedbire vücut vermektedir.[591]

İletişimin tespiti, dinlenmesi ve kayda alınması tedbiri; bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirinden farklı olarak, akışkan haldeki verilerin incelenmesi için getirilen bir düzenlemedir. Başka bir ifadeyle şüphelinin kullandığı bilişim sistemi ile diğer bilişim sistemleri arasındaki verilerin iletişimi halinde bu tedbire başvurulabilecektir.[592]

---

[586] Mifsud Bonnici, Tudorica and Cannataci, "The European Legal Framework," 191; Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 64- 65.
[587] Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 145- 146. Ek olarak bilişim sistemleri laboratuvara taşınırken dikkat edilmesi gereken hususlar hakkında daha detaylı bilgi için bkz. Say, "Bilişim Suçlarında Elde Edilen Deliller," 39- 41.
[588] Dülger, *Bilişim Suçları,* 613.
[589] Arslan, "Dijital Delil ve İletişimin Denetlenmesi," 197.
[590] Değirmenci, *Sayısal Delil,* 382.
[591] Yenisey ve Nuhoğlu, *Ceza Muhakemesi Hukuku,* 449.
[592] Değirmenci, *Sayısal Delil,* 309- 310.

İletişimin Tespiti, Dinlenmesi ve Kayda Alınması tedbiri, pek çok temel hak ve özgürlüğe ciddi sınırlamalar getiren bir koruma tedbiridir. Özellikle de haberleşme hürriyeti ile özel hayatın gizliliği haklarına doğrudan ciddi müdahale oluşturmaktadır. İletişimin denetlenmesi tedbiri incelendiğinde bünyesinde dört ayrı tedbiri barındırdığı görülmektedir. Bunlar; "şüpheli veya sanığın telekomünikasyon yoluyla iletişiminin dinlenmesi, kayda alınması", "sinyal bilgilerinin değerlendirilmesi", "şüpheli veya sanığın mobil telefonunun yerinin tespiti" ve "şüpheli ve sanığın telekomünikasyon yoluyla iletişiminin tespiti"dir.[593]

"Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmelik (İletişimin Denetlenmesi Yönetmeliği)"[594] m. 3-r uyarınca telekomünikasyon;

> *"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 iletilmesi, gönderilmesi ve alınmasını"* ifade etmektedir.

Bu bağlamda sabit ya da mobil telefonlar üzerinden yapılan tüm aramalar, yazışmalar, görüntülü aramalar vb. her türlü veri aktarımları, bu tedbir kapsamında denetlenebilecektir.[595]

İletişimin denetlenmesi tedbirlerinden ilki olan iletişimin dinlenmesi ve kayda alınması tedbiri, teknik araçlar vasıtasıyla konuşma ile dinlemenin eş zamanlı olarak gerçekleştirilmesi ve neticesinde ele geçirilen bilgilerin kaydedilmesi olarak tanımlanabilir.[596]

İkinci olarak sinyal bilgilerinin değerlendirilmesi tedbiri incelenecek olursa öncelikle sinyal bilgisi kavramı, İletişimin Denetlenmesi Yönetmeliği m. 3-p uyarınca "Bir şebekede haberleşmenin iletimi veya faturalama amacıyla işlenen her türlü veri" olarak tanımlanmıştır. Sinyal bilgileri ile iletişimin içeriğine girilmeksizin kişinin

---

[593] Afandak, "Ceza Muhakemesinde Dijital Deliller," 146- 147.
[594] Resmî Gazete Tarihi: 07/08/2009, Sayı: 27312.
[595] Afandak, "Ceza Muhakemesinde Dijital Deliller," 147- 148.
[596] Özbek, Doğan ve Bacaksız, *Ceza Muhakemesi Hukuku,* 369; Yenisey ve Nuhoğlu, *Ceza Muhakemesi Hukuku,* 468; Tezcan, v.d., *Dijital Ceza Muhakemesi Hukuku,* 612; Muzaffer Enes Cirit, "İletişimin Tespiti, Dinlenmesi ve Kayda Alınması (CMK mad. 135)" (Yayınlanmamış Yüksek Lisans Tezi, İstanbul Medipol Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuk Anabilim Dalı, İstanbul, 2018), 34.

telefon numarası, telefonun seri numarası ve görüşmenin gerçekleştiği yer gibi bilgiler değerlendirilerek iletişimin tespiti sağlanır.[597]

Üçüncü olarak iletişimin tespiti tedbiri, sadece sanık veya şüphelinin telekomünikasyon vasıtasıyla kimler ile iletişim kurduğunun belirlenmesini ifade etmektedir.[598] iletişimin içeriğine müdahale edilmemekte yalnızca iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişimdeki aramalar, aranmalar, yer bilgileri ve kimlik bilgileri tespit edilmektedir. Madde kapsamında düzenlenen diğer tedbirlerden farkı bu tedbirin geçmişe yönelik iletişimi (HTS raporu) tespit ediyor oluşudur.[599]

Son olarak mobil telefonun yerinin tespitine bakacak olursak, bu tedbire CMK m. 135/5 uyarınca yalnızca Şüpheli veya sanığın yakalanabilmesi amacıyla başvurulabilecektir. Söz konusu tedbirin, bir tür teknik izleme olduğu ileri sürülmüş ve bu bağlamda şüpheli veya sanık tarafından kullanılan mobil telefonun yerinin tespit edilmesi suretiyle bu kişilere ulaşılmasının hedeflendiği belirtilmiştir.[600]

Bu tedbirlere, 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 imkânı yoksa başvurulmalıdır."[601] CMK m. 135/1'e göre bu tedbirin uygulanabilmesi için öncelikle somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı gerekecektir.

Değişiklikten önce, iletişimin denetlenmesi kararını alma yetkisinin "ağır ceza mahkemeleri"ne verilmiş olması hususu, bu kararın, ağır ceza mahkemesi heyetince oybirliğiyle alınması gerekeceği ve yasa koyucunun iletişimin denetlenmesi noktasında yaşanan keyfi uygulamaları bertaraf edebilmeyi hedeflediği belirtilmekle birlikte; bir sanığın müebbet hapsine karar verilebilmesi için iki hakimin oyunun yeterli oluşu ancak söz konusu koruma tedbirine başvurulması bakımından oybirliğinin aranıyor oluşunun bünyesinde bir tezat barındırdığı gerekçesiyle eleştirilmiştir.[602] Ancak 24/11/2016 tarihli ve 6763 sayılı Kanun m. 26 ile madde

[597] Özbek, Doğan ve Bacaksız, *Ceza Muhakemesi Hukuku,* 370; Tezcan, v.d., *Dijital Ceza Muhakemesi Hukuku,* 616.
[598] Cirit, "İletişimin Tespiti," 31; Özbek, Doğan ve Bacaksız, *Ceza Muhakemesi Hukuku,* 369; Yenisey ve Nuhoğlu, *Ceza Muhakemesi Hukuku,* 469- 470.
[599] Afandak, "Ceza Muhakemesinde Dijital Deliller," 149- 150.
[600] Yenisey ve Nuhoğlu, *Ceza Muhakemesi Hukuku*, 471
[601] Aydın, *Ceza Muhakemesinde Deliller,* 113.
[602] Arslan, "Dijital Delil ve İletişimin Denetlenmesi," 197- 198.

metninde yer alan "ağır ceza mahkemesi" ibaresi "hâkim" şeklinde değiştirilmiş ve bu görev, sulh ceza hakimliklerine devredilmiştir.

Devam edecek olursak ilgili maddeye 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 süresinin belirtilmesi gerekecektir.

CMK m. 135'te sayılan şartlara uygun bir şekilde telekomünikasyon yoluyla yapılan iletişimin dinlenmesi ve kaydedilmesi suretiyle elde edilen deliller, hukuka uygun dijital delil niteliği taşıyacaktır.[603] Diğer dijital delillerde olduğu gibi, iletişimin dinlenmesi yoluyla elde edilen kayıt biçimindeki dijital delillerin de bozulma ve değişikliğe uğramaları kolaylıkla gerçekleşebileceği için bu verilerin de tek başına delil olarak kullanılamayacağı ancak başka delillerle birlikte desteklenmesi gerektiği ileri sürülmektedir.[604] Benzer şekilde Yargıtay da bu görüş bağlamında karar vermektedir.[605]

2.1.2.2.1. Tesadüfen elde edilen deliller

> CMK m. 138/2 uyarınca; *"Telekomünikasyon yoluyla yapılan iletişimin denetlenmesi sırasında, yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan ve ancak, 135 inci maddenin altıncı (sekizinci) fıkrasında sayılan suçlardan birinin işlendiği şüphesini uyandırabilecek bir delil elde edilirse; bu delil muhafaza altına alınır ve durum Cumhuriyet Savcılığına derhâl bildirilir."*

Görüldüğü üzere CMK m. 138/2, yukarıda bahsi geçen arama koruma tedbiri neticesinde tesadüfen elde edilen deliller bakımından farklılık arz etmektedir. Bu bağlamda CMK m. 138/1'den farklı olarak telekomünikasyon yoluyla yapılan iletişimin denetlenmesi sırasında, herhangi başka bir suçun işlendiği şüphesini uyandırabilecek deliller değil; ancak CMK m. 135/6'da yer alan suçlardan birinin işlendiği şüphesini uyandırabilecek bir delil elde edilirse bu delil tesadüfen elde edilen delil kapsamında değerlendirilebilecektir.

İletişimin tespiti, dinlenmesi ve kayda alınması tedbirinin, yalnızca belli bazı suçlarla ilgili olarak uygulanabildiği düşünüldüğünde (CMK m. 135/8), bu tedbir

---

[603] Afandak, "Ceza Muhakemesinde Dijital Deliller," 152.
[604] Aydın, *Ceza Muhakemesinde Deliller,* 118.
[605] Yar. CGK, E. 2010/8-134, K. 2010/217, T. 09.11.2010. Aktaran: Afandak, "Ceza Muhakemesinde Dijital Deliller," 153.

uygulanırken başka herhangi bir suç yerine yine aynı katalogda yer alan fakat farklı suçlara işaret eden delillerin, tesadüfen elde edilen delil kapsamında değerlendirilmesi doğru bir adım olmuştur. Gerçekten de bu tedbirin uygulanması sırasında tedbir kararına konu olan suç dışında herhangi başka bir suça ilişkin bulguların delil olarak değerlendirilebilmesine olanak verilirse, hakkında söz konusu tedbirin uygulanmasına olanak bulunmayan suçların incelenmesi amacıyla tedbirin uygulanabilmesine olanak sağlanmış olur ve bu sebeple de tedbirin ancak CMK m. 135/8'de yer alan katalogda tek tek sayılmak suretiyle gösterilen belirli ağırlıktaki suçlar bakımından uygulanabileceği yönündeki güvence işlevini yitirir.[606]

CMK m. 135/8'de yer alan katalogda bulunmayan bir suç ile ilgili olarak elde edilen bulguların durumu hakkında bir düzenlemeye yer verilmemekle birlikte, var olan düzenlemenin aksi yorumundan bu bulguların, suçun aydınlatılması bakımından kullanılamayacağı söylenebilir.[607] Gerçekten de CMK m. 135/8'de yer alan suçlar haricinde söz konusu tedbire başvurulamayacağı açıktır. Bu sebeple katalog dışında yer alan suçlar dışında başka bir suça işaret eden delillerin, tesadüfen elde edilen delil olarak kabul edilmesi; iletişimin tespiti, dinlenmesi ve kayda alınması tedbirinin, CMK m. 135/8'de yer alan suçlar dışındaki suçlar bakımından da uygulanabileceği anlamına gelir. Elbette böyle bir durum söz konusu olamayacağı ve katalogda yer almayan bir suç bakımından bu tedbirin uygulanması hukuka aykırılığa vücut vereceği için hukuka aykırı bir iletişimin tespiti, dinlenmesi ve kayda alınması tedbiri neticesinde elde edilenler de hukuka aykırı delil olarak kabul edilecekler ve başlangıç şüphesine dahi esas alınamayacaklardır.

2.1.2.3. Teknik araçlarla izleme (CMK m. 140)

Teknik araçlarla izleme tedbiri, şüpheli veya sanığın kamuya açık yerlerdeki faaliyetleri ve işyeri teknik araçlarla izlenmesine ve ses veya görüntü kaydının alınabilmesine olanak sağlayan bir tedbirdir. Söz konusu tedbir neticesinde elde edilen ses ve görüntü kayıtları da nitelikleri itibariyle dijital delil olarak değerlendirilebilecektir.

---

[606] Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* 569; Tezcan, v.d., *Dijital Ceza Muhakemesi Hukuku,* 640.
[607] Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* 570; Tezcan, v.d., *Dijital Ceza Muhakemesi Hukuku,* 641.

Teknik araçlarla izleme tedbirinin uygulanması oldukça zor ve pahalıdır. Örneğin mikrofonla bir dinleme gerçekleştirilecekse konuşmanın yapılacağı yer belirlenecek ve daha sonra bu yere dinlemeyi gerçekleştirecek bir mikrofon veya başka bir araç yerleştirilecektir. Bu işlemlerin gizli ve titizlikle yapılması gerektiği de düşünüldüğünde pek çok kişinin yer aldığı iyi planlanmış bir organizasyon gerçekleştirilmesi şart olmaktadır.[608]

Teknik araçlarla izleme tedbiri de İletişimin Tespiti, Dinlenmesi ve Kayda Alınması tedbiri gibi "somut delillere dayanan şüphe" ve "başka yolla delil elde edilememesi" şartlarına dayanmaktadır.

Yine benzer şekilde Teknik Araçlarla İzleme Tedbiri, kanunda açıkça sayılan suçlar bakımından uygulama imkânı bulacaktır (CMK m. 140/1). Öyle ki bu suçlar dışında kalan bir suça ilişkin olarak toplanan dijital deliller CMK m. 140/4 kapsamında yok edilecektir.

2.2. Önleme Araması Sırasında Elde Edilen Dijital Veriler ve Delil Niteliğinin Değerlendirilmesi

Önleme araması, suç işleneceğine ilişkin şüphe üzerine, suç işlenmeden evvel önleme veya caydırma amacıyla yahut suç işleneceğine ilişkin şüphe mevcut olmadığı halde sadece düzenleme, olası failleri caydırma ve önleme amacıyla yapılmaktadır.[609] Bu bağlamda kamu düzenini tehlikeye atan eşya veya kişiler bulunur ve kolluğun korumasına alınır. Bu doğrultuda önleme amacıyla gerçekleştirilen aramanın, tehlike yaratan bir eşyanın ele geçirilmesi için; ceza muhakemesi amacıyla gerçekleştirilen bir aramanın ise saklanan şüpheli veya sanığın ve delillerin elde edilmesi amacıyla yapıldığı ifade edilmiştir.[610]

> 2559 sayılı "Polis Vazife ve Salahiyet Kanunu" (PVSK) m. 9 uyarınca *"Polis, tehlikenin veya suç islenmesinin önlenmesi amacıyla usulüne göre verilmiş sulh ceza hâkiminin kararı veya bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hâllerde mülkî âmirin vereceği yazılı emirle; kişilerin üstlerini, araçlarını, özel kâğıtlarını ve eşyasını arar; alınması gereken tedbirleri alır, suç delillerini koruma altına alarak 5271 sayılı Ceza Muhakemesi Kanunu hükümlerine göre gerekli işlemleri yapar."*

[608] Afandak, "Ceza Muhakemesinde Dijital Deliller," 158- 159.
[609] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 473; Kadir Can Özel, "Bir Koruma Tedbiri Olarak Arama," *D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan,* C.21, Özel S., (2019) 1226.
[610] Yenisey ve Nuhoğlu, *Ceza Muhakemesi Hukuku,* 301.

Belirtildiği üzere bir idari işlem olarak tesis edilen önleme araması kararı, sulh ceza hakiminin kararı ile yahut gecikmesinde sakınca bulunan bir hal varsa il sınırları içerisinde vali, ilçe sınırları içerisinde kaymakam tarafından "yazılı" bir şekilde verilebilecektir.[611] Yasada mülki amirin vereceği yazılı emrin hâkim onayına sunulması hususu düzenlenmemiştir. Bununla birlikte Anayasa m. 20/2 uyarınca yetkili mercii tarafından verilen arama kararları yirmi dört saat içinde görevli hâkimin onayına sunulacak ve olası bir elkoyma durumunda da hâkim kararını el koymadan itibaren kırk sekiz saat içinde açıklayacaktır. Aksi durumda elkoyma kararı kendiliğinden hükümsüz kalacaktır.[612]

Arama talep yazısında arama için makul sebeplerin oluştuğunun gerekçeleriyle birlikte gösterilmesi gerekecektir ve önleme araması ancak kanunda sayılan belli bazı yerlerde gerçekleştirilebilecektir (PVSK m. 9/4). Bu bağlamda somut tehlikenin baş gösterdiği her yerde önleme araması yapılamayacaktır.[613] Ancak yinelemek gerekirse, kararın verilebilmesi bakımından aranan ön şart, "yakın tehlike" ihtimalinin bulunmasıdır.[614]

Önleme aramasının eşya üzerinde gerçekleştirilmesi, ilk olarak üzeri aranabilecek kişilerin yanlarında bulundurdukları eşya bakımından geçerli olacaktır. Bununla birlikte kişinin örneğin bir konteyner içerisinde yardıma ihtiyaç duyduğu anlaşılıyorsa yahut arabasında oturan kişinin gözaltına alınması gibi bir durum söz konusuysa kolluk, suçun önlenmesi adına ilgili eşyalar üzerinde kendiliğinden arama yapabilir.[615]

Dijital delillerin elde edilmesi bakımından değerlendirecek olursak önleme araması kapsamında kişilerin üstleri, araçları ve eşyasının aranabildiğini belirtmiştik. Bu arama işlemi sırasında kişilerin yanlarında bulundurduğu tabletler, akıllı cep telefonları, akıllı saatler ve taşınabilir diğer bilişim sistemleri gibi çeşitli cihazların içeriklerinde, kolluk kuvvetleri tarafından suç işlenmesinin önlenmesi amacıyla arama yapılıp yapılamayacağı sorusu sorulabilir.

[611] Yenisey ve Nuhoğlu, *Ceza Muhakemesi Hukuku,* 301.
[612] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 475.
[613] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 474.
[614] Yenisey ve Nuhoğlu, *Ceza Muhakemesi Hukuku,* 302.
[615] Yenisey ve Nuhoğlu, *Ceza Muhakemesi Hukuku,* 304.

Öncelikle yukarıda da belirtildiği üzere bilişim sistemlerinin aranması tedbiri, özel bir adli arama tedbiridir. Kişilerin üzerlerinde yahut araçlarında taşıdıkları bilişim cihazlarının günümüzde büyük verileri barındırabildiğini ve bu verilerin çoğunlukla kişisel veriler yahut kişilerin özel hayatlarının dokunulmaz alanına ilişkin veriler olduğunu öngören kanun koyucu, adli aramalar bu cihazların aranabilmesi bakımından özel bir düzenleme getirmişken önleme aramaları bakımından sessiz kalmıştır. Bu bağlamda ilk olarak PVSK m. 9 kapsamında kişilerin bilişim sistem araçlarında önleme araması yapılabileceğini söylemek temel hak ve hürriyetlere orantısız bir müdahale teşkil etmekle birlikte hukuka da aykırı olacaktır.[616]

İkinci olarak, CMK m. 134'te yer alan tedbirlere başvurulabilmesi için aranan ilk koşul bir suç dolayısıyla yürütülen bir soruşturmanın (veya kovuşturmanın) varlığıdır. İkinci olarak ise somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı gerekmektedir. Ortada henüz CMK m. 160 kapsamında Cumhuriyet savcısının kamu davasını açmaya yer olup olmadığına karar verebilmesi adına işin gerçeğini araştırmaya başlamasını gerektiren ve suçun işlendiği izlenimini veren bir hal bile yokken, başka bir ifadeyle Cumhuriyet savcısının hazırlık işlemleri çerçevesinde delil toplama yetkisini kullanabileceği bir durum dahi kısaca herhangi bir delil söz konusu değilken CMK m. 134'te yer alan tedbirlere başvurulması mümkün olamayacaktır.

Üçüncü ve son olarak CMK m. 134' te yer alan tedbirlere başvurulmasına, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından karar verilebilecektir. PVSK m. 9 uyarınca önleme aramasının gecikmesinde sakınca bulunan hallerde mülkî âmirin vereceği yazılı emirle de gerçekleştirilebileceği düşünüldüğünde; önleme araması ile bilişim sistemlerinin aranabileceğini kabul edilmesi, CMK m. 134 hükmünün dolanılması anlamına gelecektir. Ek olarak böyle bir kabul, CMK m. 134 ile getirilen güvencelerin anlamını yitirmesine sebep olacaktır.

Sonuç olarak yukarıda açıklanan sebepler neticesinde bir önleme araması neticesinde bilişim sistemlerinde arama gerçekleştirilemeyeceği açıktır. Buna karşılık tehlikenin veya suç işlenmesinin önlenmesi amacıyla usulüne uygun bir şekilde önleme araması gerçekleştiren kolluk kuvvetlerinin, kişilerin üstlerinde yahut araçlarında buldukları bilişim sistemleri araçlarında işlenen bir suçun delillerinin bulunduğu veya bizzat ilgili aracın suçun işlenmesinde kullanıldığı konusunda bir

[616] Değirmenci, *Sayısal Delil,* 336.

şüpheye sahip olmaları durumunda ilgili araca el koyabilecekleri ve CMK m. 134'teki diğer koşulların sağlanması durumunda alınacak karar üzerine ilgili bilişim sistemi araçlarında aramanın gerçekleştirilebileceği ileri sürülmüştür.[617]

Gerçekten de CMK m. 134 kapsamında aranması ve elde edilmesi hedeflenen şeyin, bilişim sistemi aracı değil fakat ilgili bilişim sistemi aracının içerisinde bulunan veriler olduğu düşünüldüğünde; kolluk kuvvetlerinin el koyacakları şeyin, bilişim sistemi aracının içerisinde yer alan veriler değil fakat bilişim sistemi aracının fiziksel varlığı (donanım- hardware) olacağı ve bu bağlamda fiziksel varlığına el konulan bu aracın, Cumhuriyet savcılığına intikal ettirilebileceği düşünülebilecektir.

Buna karşılık CMK m. 134/2'de yer alan ve genel elkoyma tedbirinin de özel bir halini oluşturduğunu düşündüğümüz bilişim sistemlerine elkoyma tedbiri uyarınca bilişim sistemlerine yalnızca, şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması hallerinde elkonulabilecektir. Bu sebeple maddede belirtilen hallerin dışına çıkılarak tehlikenin veya suç işlenmesinin önlenmesi gibi amaçlarla gerçekleştirilen bir önleme araması çerçevesinde bu cihazlara elkonulmasının, CMK m. 134/2 hükmünün dolanılması anlamına geleceğini ve kanunun sağladığı korumaların anlamını yitireceğini düşünmekteyiz.

2.3. Siber Suçlar Sözleşmesi Uyarınca Sayısal Delillerin Elde Edilmesi

Siber Suçlar Sözleşmesi, bazı siber faaliyetlerin suç olarak sınıflandırılmasına yol açan maddi unsurları tanımlayan ve bu faaliyetlerin önlenmesine, tespit edilmesine ve kovuşturulmasına izin veren usul hükümlerine sahip ana (ve tek) uluslararası anlaşmadır.[618,619]

Siber Suçlar Sözleşmesinin amacı, siber suçlar alanındaki suçların maddi ceza hukuku unsurlarını ve bağlantılı hükümlerini uyumlu hale getirmek, bu tür suçların ve diğer suçların soruşturulması ve kovuşturulması için gerekli ulusal ceza muhakemesi hukuku yetkilerini sağlamak ve aynı zamanda siber suç olmamakla birlikte bilişim

[617] Değirmenci, *Sayısal Delil,* 336.
[618] Mifsud Bonnici, Tudorica and Cannataci, "The European Legal Framework," 198.
[619] Sözleşmenin orijinal metni için bkz. https://rm.coe.int/1680081561 . Sözleşmenin Türkçe çevirisi için bkz. https://www.resmigazete.gov.tr/eskiler/2014/08/20140809-5-1.pdf , son erişim: 08.06.2022.

sistemleri vasıtasıyla işlenen suçlarda hızlı ve etkili bir uluslararası iş birliği rejimi oluşturmaktır.[620]

Siber Suçlar Sözleşmesi, Sözleşmeye taraf devletlerin, sözleşmede atıfta bulunulan suçlara, bir bilgisayar sistemi aracılığıyla işlenen diğer suçlara uygulanacak soruşturma ve kovuşturmalara ve dijital delillerin toplanmasına ilişkin yetki ve usulleri tesis etmek için mevzuat ve tedbirler kabul etmelerini sağlamaktadır.[621]

Siber Suçlar Sözleşmesi, yargı yetkisini tesis etmek için ülkesellik ve vatandaşlık ilkelerine dayanmaktadır.[622] Siber Suçlar Sözleşmesi'nin 22. maddesi uyarınca, Sözleşmeye taraf devletler; Siber Suçlar Sözleşmesi'nde belirtilen suçlar kendi topraklarında, kendi bayrağını taşıyan bir gemide, kendi kanunlarına göre kayıtlı bir uçakta veya suçun kendi vatandaşlarından biri tarafından işlenmesi halinde ve söz konusu suçun işlendiği yerde ceza kanununa göre veya suçun herhangi bir devletin yargı yetkisi dışında işlenmesi halinde, yargı yetkisini tesis etmek için gerekli yasal ve diğer önlemleri almaları gerekmektedir.

Suçu araştıran bir devletin başka bir ülkede saklanan veya bulunan delilleri toplama yetkisi yoksa uluslararası iş birliği (adli yardım) devreye girer. Siber Suçlar Sözleşmesinin 3. Bölümü uluslararası iş birliğini düzenler. Karşılıklı yardımlaşma, uluslararası iş birliğinin en önemli aracıdır ve siber suçların sınır ötesi niteliği dikkate alınarak Siber Suçlar Sözleşmesi tarafından düzenlenen en önemli unsurlardan biridir. Karşılıklı yardımın temel amaçlarından biri, ceza davalarında ve yargılamalarda kullanılmak üzere delil elde etmektir. Tabii talepte bulunulan devlet tarafından ve kendi usulleri çerçevesinde yurtdışında toplanan delillerin, talep eden devletin delil kurallarına uyması gerekecektir.[623]

Siber Suçlar Sözleşmesi, Parker'ın klasik tipolojisine kabaca benzeyen üç suç kategorisi arasında ayrım yapmaktadır.[624] Buna göre bilgisayar suçları; bilgisayarla bütünleşen suçlar (computer-integrity crimes- bilgisayarın suçun nesnesi olduğu durumlar), bilgisayar destekli suçlar (computer assisted crimes- bilgisayarın araç

[620] Mifsud Bonnici, Tudorica and Cannataci, "The European Legal Framework," 199.
[621] Mifsud Bonnici, Tudorica and Cannataci, "The European Legal Framework," 200.
[622] Mifsud Bonnici, Tudorica and Cannataci, "The European Legal Framework," 201.
[623] Mifsud Bonnici, Tudorica and Cannataci, "The European Legal Framework," 201-202.
[624] Parker and Nycum, "Computer Crime," 313.

olduğu durumlar) ve içerikle ilgili suçlar (content-related crimes- bilgisayar ağının suç ortamını oluşturduğu durumlar) şeklinde üçe ayrılmaktadır.[625]

Birinci suç kategorisi, bilgisayar verilerinin veya bilgisayar sistemlerinin gizliliğine, bütünlüğüne veya kullanılabilirliğine yönelik suçları cezalandıran "hard-core" siber suçlarla ilgilidir. Siber Suçlar Sözleşmesi, bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı aşağıdaki beş suçu bu başlık altında değerlendirmektedir.[626]

1. Yasadışı erişim. Başka bir ifadeyle bir bilgisayar sisteminin tamamına veya herhangi bir kısmına kasıtlı olarak haksız[627] erişim (Madde 2).

2. Yasadışı müdahale. Bilgisayar verilerinin üzerinde bulunduğu bir bilgisayar sisteminden elektromanyetik dalgalar yayılması da dahil olmak üzere, kamuya açık olmayan bilgisayar verilerinin iletimi sırasında, teknik yöntemler kullanarak başka bir bilgisayar sistemi veya verilerin bulunduğu bilgisayar sistemi üzerinden veri iletimine haksız surette dahil olma (Madde 3).

3. Verilere müdahale. Başka bir ifadeyle bilgisayar verilerinin kasıtlı olarak zarar görmesi, silinmesi, bozulması, değiştirilmesi veya baskı altına alınması (Madde 4).

4. Sistemlere müdahale. Bilgisayar verilerine yeni veriler ilave etmek, bilgisayar verilerini başka yerlere iletmek, tahrip etmek, silmek, bozmak, değiştirmek veya erişilemez kılmak suretiyle bir bilgisayar sisteminin işleyişini ciddi ölçüde ve haksız şekilde engellemek (Madde 5).

5. Cihazların kötüye kullanımı. Başka bir ifadeyle bir cihazın veya parolanın veya erişim kodunun suçlardan herhangi birinin işlenmesi amacıyla kullanılması amacıyla üretimi, satışı, kullanım için tedarik edilmesi, ithal edilmesi, dağıtılması veya başka bir şekilde kullanıma sunulması (Madde 6).

---

[625] Casey, *Digital Evidence,* 129-130.
[626] Casey, *Digital Evidence,* 130.
[627] "Haksız" ifadesi, Avrupa Konseyi tarafından hazırlanan Siber Suçlar Sözleşmesi Açıklayıcı Raporunda (paragraf 38) şu şekilde değerlendirilmektedir: Tanımlanan suçların ortak özelliği, gerçekleştirilen fiillerin "haksız olarak" gerçekleştiriliyor oluşudur. Bu bağlamda tanımlanan fiiller her zaman kendi başına cezalandırılabilir değildir. Rıza, kendini savunma veya zorunluluk gibi klasik yasal savunmaların geçerli olduğu durumlarda ve diğer ilkelerin veya çıkarların cezai sorumluluğun hariç tutulmasına yol açtığı durumlarda gerçekleştirilen fiil haksız olmayacaktır. Detaylı bilgi için bkz. Casey, *Digital Evidence,* 130.

Siber Suçlar Sözleşmesi'nin ele aldığı ikinci suç kategorisi bilgisayarlarla ilişkili (bilgisayar destekli) suçlardır. Bilgisayarların veya bilgisayar ağlarının yokluğunda işlenemeyen ve genellikle bilgisayarın suçun hedefi olduğu bu bağlamda yeni suç türlerine vücut veren bilgisayarla bütünleşen suçlarının aksine, bilgisayar destekli suçlar, bilgisayarın sadece araç olarak kullanıldığı geleneksel suçlardır.[628]

Siber Suçlar Sözleşmesi'ndeki üçüncü suç kategorisi içerikle ilgili suçlarla ilgilidir. Geleneksel suçlarla ilgili olmaları ve bilgisayarların hedeften ziyade yine bir araç olarak kullanılmaları sebebiyle bilgisayar destekli suçlara benzerler. Bilgisayar destekli suçlarla en büyük farkı ise, bilgisayar destekli suçlarda geleneksel suçların kullanımında bilgisayar bir araç olarak kullanılırken; içerikle ilgili suçlarda, içeriği itibariyle suç konusu oluşturan materyaller erişilebilir kılınmakta ve dağıtılmaktadır (SSS m. 9).[629,630]

Son olarak Siber Suçlar Sözleşmesi m. 15'te, *"Tedbirler ve Şartlar"* başlığı altında dijital deliller toplanırken uyulması gereken şartlar belirtilmiştir. Buna göre dijital deliller elde edilirken taraf devletler, başta Avrupa Konseyi İnsan Hakları ve Temel Özgürlükler Sözleşmesi, BM Siyasal ve Medeni Haklar Sözleşmesi gibi uluslararası insan hakları belgeleri çerçevesinde üstlenilen yükümlülüklerden doğan hakların gerekli ölçüde korunmasını temin edecek ve hakkaniyet ilkesinin tesis edilmesini sağlayacak şekilde uygulayacaklardır. Bu uygulamalar yapılırken, kamu yararının ve adaletin sağlıklı şekilde yürütülmesi için üçüncü şahısların yetki, sorumluluk ve yasal hakları üzerindeki etkileri de göz önünde bulundurulacaktır.[631]

2.3.1. Siber suçlar sözleşmesinde yer alan tedbirler

Siber Suçlar Sözleşmesi, *"Bölüm II— Usul Hukuku"* başlığı altında dijital delil toplamaya ilişkin çeşitli hükümler yer almaktadır.[632] Bununla birlikte yazının devamında dijital delillerin elde edilmesi anlamında konumuzla ilgisi bakımından yalnızca "Depolanmış bilgisayar verilerinin aranması ve bunlara elkonulması",

[628] Casey, *Digital Evidence,* 132.
[629] Casey, *Digital Evidence,* 132.
[630] SSS'de yer alan suç tipleri hakkında bkz. Casey, *Digital Evidence,* 134-172.
[631] Değirmenci, *Sayısal Delil,* 308; Afandak, "Ceza Muhakemesinde Dijital Deliller," 172.
[632] Forgó, v.d., "Privacy Protection," 273.

"Trafik verilerinin gerçek zamanlı toplanması" ve "İçerik verilerinin takibi" tedbirlerine yer verilecektir. [633]

2.3.1.1. Depolanmış bilgisayar verilerinin aranması ve bunlara elkonulması

CMK m. 134 "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" koruma tedbiri; Siber Suçlar Sözleşmesi m. 19 "Depolanmış Bilgisayar Verilerinin Aranması ve Bunlara Elkonulması" tedbirinin iç hukuka uyarlanmış halidir.[634]

SSS m. 19/1 uyarınca sözleşmeye taraf Devletler,

a) Bir bilgisayar sisteminin tamamını veya bir kısmını ve bilgisayar sistemleri içerisinde depolanmış bilgisayar verilerini,

b) Yahut bilgisayar verilerinin depolanmış olabileceği bir depolama aygıtını,

Arama ya da bunlara erişme yetkisi sağlayacak benzer şekillerde gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.

Maddede ilk olarak görüldüğü üzere Siber Suçlar Sözleşmesi, terim olarak "bilgisayar sistemi", ve "bilgisayar verisi" terimlerini tercih etmiş ve taraflardan, bunların elde edilmesi konusunda düzenleme yapmalarını beklemiştir.

Sözleşmenin tanımlar başlıklı birinci maddesi uyarınca bilgisayar sistemi; *"bir veya birden fazlası, belirli bir yazılım çerçevesinde otomatik olarak veri işleyebilen bir cihazı veya birbirine bağlı veya birbiriyle ilişkili bir dizi cihazı"* ifade etmektedir.

Aynı madde uyarınca bilgisayar verisi ise *"bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlar da dahil olmak üzere, bir bilgisayar sisteminde işlenmeye uygun nitelikteki her türlü bilgi ve konsepti"* ifade etmektedir.

CMK m. 134'ten farklı olarak Siber Suçlar Sözleşmesi, kapsamı bilgisayarlarla sınırlı tutmak yerine "bilgisayar sistemlerinin" kapsama alınması gerektiğini belirtmiştir. Buna karşılık sözleşmede bilgisayar sistemlerinin, "*belirli bir yazılım çerçevesinde otomatik olarak veri işleyebilen bir cihazı veya birbirine bağlı veya birbiriyle ilişkili bir dizi cihaz"* şeklinde tanımlanması, sınırlamayı farklı bir açıdan getirmiştir.

[633] Siber Suçlar Sözleşmesinde yer alan diğer tedbirler hakkında detaylı bilgi için bkz. Değirmenci, *Sayısal Delil,* 301- 308.
[634] Börekçi, "Bilgisayarlarda, Bilgisayar Programlarında," 37.

Devamında ise SSS m. 19/3 tarafların, erişilen bilgisayar verilerine el konulması ya da bunların başka şekillerde koruma altına alınabilmesi için gerekli yasama işlemlerini ve diğer işlemleri gerçekleştirmeleri gerektiğini belirtmiştir. Söz konusu koruma yöntemleri ise şu şekilde olacaktır;

a) Bir bilgisayar sisteminin tamamına veya bir kısmına veya bilgisayar verileri depolama aygıtına el koyma veya benzer şekilde koruma altına alma,

b) Söz konusu bilgisayar verilerinin bir kopyasını oluşturma ve bunu muhafaza etme,

c) İlgili depolanan verilerin bütünlüğünün korunması,

d) Erişilen bilgisayar sistemindeki bilgisayar verilerinin erişilemez hale getirilmesi veya silinmesi.

CMK m. 134, Siber Suçlar Sözleşmesinden farklı olarak bilgisayar verilerinin erişilemez hale getirilmesi veya silinmesi konusunda bir düzenleme getirmemiştir. Bu durum ise el konulan bütün bilgisayar verilerinin, muhafaza edilmesinin zorunlu olduğu şeklinde yorumlanabileceği gerekçesiyle eleştirilmiştir.[635]

2.3.1.2. Trafik bilgilerinin gerçek zamanlı olarak toplanması ve içerik verilerinin takibi

Sözleşmenin 20. ve 21. maddelerinde, trafik verilerinin gerçek zamanlı olarak toplanması ve iletişim kayıtlarına yönelik içerik verilerinin hem zamanlı bir biçimde, başka bir ifadeyle iletişim anında kesilerek toplanması ve kaydedilmesi tedbirleri öngörülmüştür.[636]

SSS m. 20 uyarınca taraf devletler, ulusal sınırları içerisinde bulunan teknik imkanların kullanılması suretiyle bilgisayar sistemleri aracıyla iletilen trafik verilerinin gerçek zamanlı olarak toplanması veya kaydedilmesi konusunda yahut herhangi bir hizmet sağlayıcısının söz konusu eylemleri gerçekleştirebilmesi adına gerekli düzenlemeleri gerçekleştirecektir.

SSS m. 21 uyarınca ise taraf devletler ulusal yasalarca belirlenecek ciddi nitelikteki suçlara ilişkin olarak, ülke sınırları içerisinde bulunan teknik imkanların kullanılması suretiyle bilgisayar sistemleri aracılığıyla gerçekleştirilen iletişimlerin

[635] Rezan Epözdemir, "Bilişim Sistemlerinde Arama ve Elkoyma Tedbirleri," *Terazi Hukuk Dergisi,* C. 13, S. 142 (2018): 95. Aktaran Börekçi, "Bilgisayarlarda, Bilgisayar Programlarında," 38.
[636] Erdem ve Özocak, "Avrupa Konseyi Siber Suç Sözleşmesi ve Türk Hukukuna Etkileri," 20.

içeriklerinin gerçek zamanlı olarak toplanması veya kaydedilmesi konusunda yahut herhangi bir hizmet sağlayıcısının söz konusu eylemleri gerçekleştirebilmesi adına gerekli düzenlemeleri gerçekleştirecektir.

İlgili tedbirler incelendiğinde mevzuatımızda bunlarla ilgili doğrudan bir düzenleme olmadığı görülmektedir.[637] Her ne kadar CMK m. 135'te düzenlenen iletişimin tespiti, dinlenmesi ve kayda alınması tedbiri ile benzerlik gösterdiği düşünülse de söz konusu tedbirin, SSS m. 20 ve 21'de aranan koşulları tam olarak karşılamadığını belirtmemiz gerekir. Öncelikle CMK m. 135 hükmü yalnızca kişiler arası iletişimin bulunması halinde uygulanan bir tedbirken sözleşmenin 20 ve 21. maddelerinde düzenlenen ve taraf devletlerin bu yönde düzenleme yapmasını öngören tedbirler, bilişim sistemleri arasındaki her türlü veri iletişimini kapsamaktadır.[638] İkinci olarak CMK m. 135 yalnızca 8. fıkrasında yer alan sınırlı sayıdaki (katalog) suçlar için başvurulabilecek bir tedbir olmakla birlikte burada sayılan suçların arasında Sözleşmede sayılan suçların hiçbiri yer almamaktadır.[639]

Bu sebeplerle sözleşmeyle paralelliğin sağlanması adına sözleşmede yer alan bu tedbirlerin de CMK'da ayrıca düzenlenmesi gerektiğini yahut bir değişiklik yapılması suretiyle paralelliğin sağlanması gerektiğini söyleyebiliriz.[640]

2.3.2. Uluslararası işbirliği ve adli yardımlaşma

Teknolojinin gelişimi ve bilişim cihazlarının hayatımızın her yerine nüfuz etmesi neticesinde suç da giderek küresel bir boyut kazanmaya başlamıştır. Bu bağlamda örneğin bir suç, x şehrindeki bir bilişim sistemi kullanılarak, fakat y şehrinde yer alan bir ağa bağlı olarak, z şehrinde sonuç doğuracak şekilde işlenebilmektedir. Yahut yine x şehrinde işlenen bir suça ilişkin deliler y şehrinde yer alan bir bulut sisteminde ve hatta bütün dünyaya yayılmış bir sistemde depolanıyor olabilir. Böyle durumlarda karşılaşılan bu gibi çıkmazlar ise ancak hızlı ve pratik bir şekilde gerçekleştirilecek işbirliği ve adli yardımlaşma düzenlemeleri aracılığıyla

[637] Erdem ve Özocak, "Avrupa Konseyi Siber Suç Sözleşmesi ve Türk Hukukuna Etkileri," 20.
[638] Mücahid Özbek, "Avrupa Siber Suçlar Sözleşmesinin Türk Ceza Hukukuna Etkileri" *GSI,* (2015): 86. https://docplayer.biz.tr/4315393-Avrupa-siber-suclar-sozlesmesinin-turk-ceza-hukukuna-etkileri.html , son erişim: 15.04.2022; Erdem ve Özocak, "Avrupa Konseyi Siber Suç Sözleşmesi ve Türk Hukukuna Etkileri," 20.
[639] Erdem ve Özocak, "Avrupa Konseyi Siber Suç Sözleşmesi ve Türk Hukukuna Etkileri," 20.
[640] Özbek, "Avrupa Siber Suçlar Sözleşmesi," 86; Erdem ve Özocak, "Avrupa Konseyi Siber Suç Sözleşmesi ve Türk Hukukuna Etkileri," 20.

aşılabilecektir. Siber suçlar sözleşmesi de uluslararası işbirliği ve adli yardımlaşma konusunda çeşitli adımlar atmıştır.

İlk olarak Siber Suçlar Sözleşmesi'nin uluslararası işbirliği başlığını taşıyan üçüncü bölümü, uluslararası işbirliğine ve adli yardımlaşmaya ilişkin temel ilke ve kuralları belirlemiştir. Siber suçlar sözleşmesi m. 23 uyarınca sözleşmeye taraf olan devletler, bilgisayar sistemleri ve verileri ile ilgili olarak yürütülen soruşturma ve kovuşturmalarda yahut yine yürütülen bir soruşturma veya kovuşturmayla ilgili olarak elektronik ortamda delillerin toplanması amacıyla birbirleriyle mümkün olan en geniş ölçüde işbirliği yapacaklardır.

İşbirliğine ilişkin getirilen sözleşmenin anılan 23. maddesi, çerçeve niteliğinde bir kural getirmiştir. Bu bağlamda işbirliği konusunda somut kurallar getirmeyen siber suçlar sözleşmesi, sonraki hükümlerle bu çerçevenin sınırlarını çizmeye ve daha belirgin kılmaya çalışmıştır.[641]

Sonrasında adli yardımlaşmaya ilişkin genel ilkelere 25. maddede verilmiştir. Buna göre sözleşmeye taraf olan devletler, bilgisayar sistemleri ve verileriyle ilgili yürütülen soruşturma ve kovuşturmalarda veya yürütülen bir soruşturma veya kovuşturma kapsamında bir suç fiiline ilişkin olarak elektronik ortamda delil toplanması hususunda mümkün olan en geniş ölçüde birbirlerine yardım sağlayacaklardır. Maddenin devamında tarafların birbirlerine sağlayacağı yardımların çerçevesi çizilmeye çalışılmıştır. Buna göre taraf devletler, sözleşmenin 27. ve 35. maddelerinde belirtilen yasal yükümlülüklerin yerine getirilebilmesi adına gerekli olacak yasama tedbirlerini ve diğer tedbirleri kabul edeceklerdir.[642]

Son olarak Siber Suçlar Sözleşmesi m. 27 ve devamı hükümleri yine devletler arası karşılıklı adli yardımlaşma hükümlerini düzenlemektedir. Ancak bu hükümler, öncelikle devletler arasında halihazırda var olan adli yardımlaşma hükümlerinin yerini almayı değil, fakat onları tamamlamayı hedeflemektedir. Bununla birlikte 27. madde ve devamındaki maddeler, aralarında bir adli yardımlaşma anlaşması olmayan devletler bakımından uyulması gereken adli yardımlaşma hükümlerine de yer

[641] Murat Önok, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği," *Prof Dr. Nur Centel'e Armağan, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,* C. 19, S. 2 (2013): 1249.
[642] Söz konusu tedbirler hakkında detaylı bilgi için bkz. Önok, "Siber Suçlarla Mücadelede Uluslararası İşbirliği," 1251- 1252.

vermektedir. Bu bağlamda söz konusu bu düzenlemenin ilgili ilke ve kuralları belirlemesi, önemli bir adım olarak değerlendirilmiştir.[643]

Anlatılanlara ek olarak sözleşmede, diğer devletlerin ulusal sınırları içinde bulunan verilerin aranması ve bunlara el konulmasına olanak sağlayan "sınır ötesi arama ve elkoyma" yetkisinin düzenlenmemiş olduğunu belirtmemiz gerekir. Bu bağlamda sınır ötesi arama ve elkoyma işlemlerinin, uluslararası iş birliği esaslarına göre yürütülebileceğini söyleyebiliriz.[644]

[643] Önok, "Siber Suçlarla Mücadelede Uluslararası İşbirliği," 1244; Erdem ve Özocak, "Avrupa Konseyi Siber Suç Sözleşmesi ve Türk Hukukuna Etkileri," 6.
[644] Değirmenci, *Sayısal Delil,* 306.

BÖLÜM 3: CEZA MUHAKAMESİNDE DİJİTAL DELİLLERİN DEĞERLENDİRİLMESİ VE İSPAT GÜCÜ

3.1. Ceza Yargılamasında İspat

3.1.1. Dijital delillerin vicdani delil sistemi açısından değerlendirilmesi

Ceza muhakemesi hukukunda belirli hususların, belirli bazı delillerle ispat edilmesi gibi bir zorunluluk bulunmamaktadır. Benzer şekilde delillerin ispat gücü bakımından da bir derecelendirme söz konusu olmamakla birlikte tüm deliller, delil değeri bakımından eşittir.[645] Bu bağlamda bir nesnenin yahut açıklamanın delil olabilmesi bakımından, delil kurallarını sağlamasının yanında belirli bir hususu ispat bakımından hâkimde vicdani kanaat oluşturabilecek düzeyde olması önem arz etmektedir.[646]

Bu bakımdan öncelikli hedefin, maddi gerçeğin ortaya çıkarılması olduğu ceza muhakemesi hukukunda hâkim, taraflarca ileri sürülen delillerle bağlı olmayacak ve delil olarak kabul edilebilme kurallarını taşımaları koşuluyla her şeyi delil olarak kabul edilebilecek ve bu şekilde her şeyin, her şeyle ispatı mümkün olabilecektir. Elbette ki her şeyin delil olabileceği gerçeği, her şeyin muhakeme sürecinde ileri sürülebileceği, incelemeye sunulabileceği ve tartışılabileceği anlamlarına da gelecektir.[647]

Bu bağlamda ispat edilecek hususun, geçmişteki olaylara ilişkin olması ve bu olayların da ortaya çıkacağı zamanın ve şartların önceden bilinememesi, sonuç olarak da delillerin önceden hazırlanamayacak oluşu nedeniyle ceza muhakemesinde *delil serbestisi* ilkesi benimsenmiştir.[648]

Her olayın her delille ispatlanabilmesi olanağını sağlayan "vicdani delil sistemi"nden önce "kanuni delil sistemi"nin geçerli olduğu zamanlarda kişiler, yargılama konusu suçla ilgili kanunun aradığı delillerin bulunması durumunda, suçsuzluklarına inanılsa dahi mahkûm edilebiliyor yahut suçu işledikleri farklı delillerle ortaya konulmasına karşın kanunun aradığı delillerin elde edilemeyişi

[645] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 255.
[646] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 255- 256.
[647] Toroslu ve Feyzioğlu, *Ceza Muhakemesi Hukuku,* 199.
[648] Toroslu ve Feyzioğlu, *Ceza Muhakemesi Hukuku,* 199.

sebebiyle beraat edebiliyorlardı.[649] Örneğin zina ancak ikrar yahut belirli sayıda tanık beyanı ile ispat edilebilmekteydi. Bu sebeple zinaya yönelik ikrar yahut yeterli sayıda tanık beyanı elde edildiğinde hâkimin bunlara dayanarak karar verme ve sanığı mahkûm etme zorunluluğu bulunmaktaydı.[650]

Günümüzde, henüz tam olarak bilimsel delil sistemine geçilmemekle birlikte kanuni delil sisteminin olumsuz sonuçlarını gidermek amacıyla ortaya çıkmış olan vicdani delil sistemi geçerlidir.[651] Delillerin serbestliği ve delillerin serbest değerlendirilmesi ilkeleri, vicdani delil sistemi ile açıklanabilmektedir.[652]

Bununla birlikte delillerin serbestçe değerlendirilebilmesi hususu hâkimin keyfi bir şekilde hüküm tesis edebileceği anlamına gelmeyecektir. Söz konusu değerlendirme akla ve mantığa dayalı bir değerlendirme olarak gerçekleştirilmelidir.[653] Ek olarak yukarıda bahsedilen ve bir şeyin delil olarak kabul edilebilmesi için gereken koşulların da taşınması gerekecektir.

Gerçekleştirilen ceza muhakemesinin sonunda, yargılamaya konu fiilin sanık tarafından işlendiğinin veya işlenmediğinin sabit olduğu sonucuna varılamazsa sanık ilgili fiil sebebiyle mahkûm edilemeyecektir. Bu durum ise *şüpheden sanık yararlanır* ilkesi olarak anılmaktadır.[654] Nitekim Yargıtay da şüpheden sanık yararlanır ilkesini şu ifadelerle açıklamaktadır;

> *"sanığın bir suçtan cezalandırılmasının temel koşulu, suçun kuşkuya yer vermeyen bir kesinlikle ispat edilmesine bağlıdır. Şüpheli ve aydınlatılamamış olaylar ve iddialar sanığın aleyhine yorumlanarak hüküm tesis edilemez. Ceza mahkûmiyeti bir ihtimale değil, kesin ve açık bir ispata dayanmalıdır."*[655]

---

[649] Doğan Gedik, "Ceza Muhakemesinde Hakimin Delilleri Değerlendirme Serbestliği (Cmk M.217)," *D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan,* C.21, Özel S., (2019): 915; Mehmet Yavuz, "Ceza Muhakemesinde İspat Sorunu," *TAAD*, Yıl 3, S. 9 (20 Nisan 2012): 152-153.
[650] Aydın, *Ceza Muhakemesinde Deliller,* 32.
[651] Gedik, "Ceza Muhakemesinde Hakimin Delilleri Değerlendirme Serbestliği" 915.
[652] Tezcan, v.d., *Dijital Ceza Muhakemesi Hukuku,* 367; Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* 297.
[653] Centel ve Zafer, *Ceza Muhakemesi Hukuku,* 256; Tezcan, v.d., *Dijital Ceza Muhakemesi Hukuku,* 367; Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* 297; Toroslu ve Feyzioğlu, *Ceza Muhakemesi Hukuku,* 200.
[654] Tezcan, v.d., *Dijital Ceza Muhakemesi Hukuku,* 366; Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* 296.
[655] Yar. CGK., E. 2005/90, K. 2005/112, T. 11.10.2005. (https://www.lexpera.com.tr/ictihat/Arama , son erişim: 21.03.2022)

3.2. Dijital Delillerin Kabul Edilebilirliği ve Ortaya Konulması

Dijital veriler, ancak bunların doğru oldukları, başka bir ifadeyle kim tarafından ve ne zaman oluşturuldukları ve üzerlerinde herhangi bir değişiklik yapılmadığı ispatlanabilirse delil olarak kabul edilebilirler.[656]

Kabul edilebilirlik, delil kurallarının temelinde yer almaktadır.[657] Bu bağlamda öncelikle dijital delillerin mahkemeye sunulabilmeleri ve delil olarak kabul edilebilmeleri için genel anlamda delillerin taşıması gereken özellikleri barındırmaları gerekecektir.[658] Ancak yalnızca bunların sağlanması yeterli değildir. Gerçekten de dijital delillerin hassas ve kolayca değiştirilebilir yapısı, bunların delil olarak değerlendirilebilmesi bakımından bazı ek güvencelerin varlığını zorunlu kılmaktadır.

Bu aşamada karşımıza kabul edilebilirlik kuralları çıkmaktadır. Gerçekten de bir dijital verinin, delil olarak kabul edilebilmesi için bu verinin elde ediliş anından mahkemeye sunulduğu ana kadar geçen süreçte kabul edilebilirlik kuralları da dahil olmak üzere gerekli tüm kurallara uyulması ve yasal şartların sağlanması gerekmektedir.[659] Söz konusu kabul edilebilirlik kurallarını şu şekilde sıralayabiliriz; delilin özgün/sahih olması, delilin bütün olması, delilin güvenilir bir delil olması ve ispat bakımından inanılır olması.[660] Bu bağlamda elde edilen bir dijital veri, yukarda bahsedilen delil olma kurallarını ve birazdan bahsi geçecek olan kabul edilebilirlik kurallarını bünyesinde barındırırsa; dijital delil olarak kabul edilebilecektir.

3.2.1. Özgünlük- sahihlik

Bir dijital verinin delil olarak kabul edilebilmesi bakımından öncelikle o delilin özgün bir delil olup olmadığı ve hükme esas alınabilmesi bakımından olayı doğru bir şekilde yansıtıp yansıtmadığı değerlendirilmelidir.[661,662]

Dijital delillerin olayı doğrudan temsil etmeleri konusunda özgün bir delil olarak değerlendirilip değerlendirilemeyeceğinin nasıl tespit edileceği konusuyla ilgili

---

[656] Ćosić, Ćosić and Bača, "An Ontological Approach," 3.
[657] Swanson, *Criminal Investigation,* 637; Leacock, "Search and Seizure of Digital Evidence," 221.
[658] Kenneally, "Gatekeeping out of the Box," 8
[659] Mifsud Bonnici, Tudorica and Cannataci, "The European Legal Framework," 191; Giordano, "Electronic Evidence and the Law," 162.
[660] Casey, *Digital Evidence,* 57
[661] Casey, *Digital Evidence,* 56.
[662] Bu bakımdan özgünlüğün belirlenmesi adına kullanılabilecek standartlar geliştirilmesinin, delilin iddia edildiği gibi olduğundan emin olunması için önemli olduğu belirtilmiştir. Kenneally, "Gatekeeping out of the Box," 11.

olarak bilgisayar tarafından oluşturulan kayıtların, kayıtları oluşturan sistemin ve sürecin güvenilirliğinin tespit edilmesi gerektiği ve güvenilirlik incelemesinin, bunlara dayanması gerektiği; çünkü bu tür kayıtların bir insan beyanının karşılığı olmadığı, bilgisayar tarafından üretildiği ileri sürülmüştür.[663]

Bununla birlikte belirli bir bilgisayar sisteminin veya işleminin güvenilirliğini değerlendirmek her zaman bu kadar basit olmamaktadır. Dijital delillerin kabul edilebilirliği bakımından önemli bir yere sahip olan özgünlük konusunda karşılaşılan en önemli problemlerden biri, daha önce de sözünü ettiğimiz gibi dijital delillerin değiştirilmeye müsait hassas yapılarıdır. Gerçekten bilişim sistemlerinde bulunan dijital deliller bazen bilinçli olarak bazense istemsiz bir şekilde değişikliğe uğrayabilmektedir. Bu gibi durumlarda da verilerin bozulması yahut tamamen ortadan kalkmaları gibi sonuçlar gündeme gelebilmektedir. Bazen de bilişim sisteminin hatalı bir şekilde çalışıyor oluşu, o sistem tarafından işlenen verinin de hatalı bir şekilde oluşturulmasına sebebiyet verebilmektedir.[664] Bu gibi durumlarda, hatalı bir şekilde oluşturulan veriyi esas alarak oluşturulan dijital delilin, özgün bir delil olarak ve dolayısıyla delil olarak kabul edilemeyeceğini söyleyebiliriz.[665]

Delilin özgünlüğü ile ilgili problemlerin çözümlenebilmesi ve elde edilen verilerin güvenilir olduğunun belirlenebilmesi adına konu ile ilgili olarak bilirkişi incelemelerinin önemi vurgulanmıştır. Gerçekten de tüm dijital deliller bir dereceye kadar belirsizliğe sahiptir. Bu sebeple bir adli bilişim uzmanı, mahkemeye fikir vermek adına, incelediği verilerden çıkarttığı delillere bir kesinlik seviyesi ön görebilir ve bu sayede elde edilen delilin olayı hangi derecede temsil ettiği ve söz konusu fiilin hangi derecede sanığa atfedilebileceği konusunda mahkemeye yardımcı olunmuş olur.[666]

Özgünlük konusundaki bir başka sorun ise dijital delili barındıran bilişim sistemi ile o sistemin sahibi arasında her zaman bir ilişki kurulamayacağı gerçeğidir. Gerçekten de özellikle kötücül veya casus amaçlı yazılımlar kullanılarak herhangi bir bilişim sistemi suçun islenmesinde araç olarak kullanılabilmektedir. Bu gibi

[663] Casey, "Error, Uncertainty and Loss," 2.
[664] Söz konusu karmaşıklıklar sebebiyle mahkemelerin, bilişim sistemlerinin güvenilirliği ve elde edilen delillerin özgünlükleri bakımından derinlemesine inceleme yapmaktan kaçındıkları ve hata oranlarını veya belirsizlikleri dikkate almadan dijital delillerin özgünlüklerini tespit ettikleri ileri sürülmüş ve bu husus eleştirilmiştir. Bkz. Kenneally, "Gatekeeping out of the Box," 4.
[665] Değirmenci, *Sayısal Delil,* 138; Kenneally, "Gatekeeping out of the Box," 4.
[666] Casey, "Error, Uncertainty and Loss," 4.

durumlarda suçun gerçek fail veya faillerine ancak bilişim sisteminde yer alan veri ile fail/failler arasındaki bağlantının ispatlanması yoluyla ulaşmak mümkün olacaktır.[667] Nitekim Yargıtay da önüne gelen bir davada;

> *"sanığa ait bilgisayar cep telefonu veya diğer dijital aygıtlarda suça ilişkin bir delilin bulunmaması ve sanığın atılı suçları inkar etmesi karşısında, e-postaların gerçekten gönderilip gönderilmediğinin, içeriklerinde herhangi bir tahrifat yapılıp yapılmadığının, başka bir şahsın bu hesaplara erişip mail atması veya dışarıdan e-posta yerleştirilmesi ihtimalinin, internet erişiminin şifresiz olduğunun beyan edilmesi karşısında sunucunun uzaktan izinsiz erişime ne kadar açık olduğunun araştırılarak, maillerin ulaştığı hesapla ilgili de bir inceleme yapıldığına dair teknik bir rapor alınmadan eksik inceleme ile yazılı şekilde mahkumiyet hükmü kurulması"*nı hukuka aykırı bulmuştur.[668]

Gelinen noktada dijital delillerin tek başlarına kabul edilip edilmeyeceklerine yönelik yapılan tartışmaların çoğunlukla özgünlük ve tahrif edilebilirlik etrafında döndüğünü söyleyebiliriz. Bu noktada dijital delillerin, olayı temsil eden diğer delillerle desteklenerek hükme esas alınabilecek olmaları yanında, yine dijital delillerin özgünlüklerinin ve tahrif edilmedikleri hususunun da diğer delillerle desteklenebileceği söylenebilir. Gerçekten de dijital delillerin elde edildikleri sistemin düzgün bir şekilde çalıştığı, elde edilen delillerin tahrife maruz kalmaksızın tamamen olayı temsil ettiği ve yargılamaya konu fiil ile sanık arasında da bağlantı kurulabildiği müddetçe; dijital delillerin tek başlarına hükme esas alınabileceklerini ve bu sebeple özgün olarak kabul edilebileceklerini söylemek yanlış olmayacaktır.[669]

3.2.2. Bütünlük

Deliller sadece belirli bir bakış açısını değil, tüm hikâyeyi anlatabilmeli ve suç fiili ile delil arasında bir bağlantı bulunmalıdır.[670] Bu bakımdan dijital delillerin ceza yargılamasında kullanılabilmesi ve hükme esas alınabilmesi, veri bütünlüğünün korunmuş olmasına olacaktır.[671] Veri bütünlüğünün sağlam olması ise delillerin, olay yerinde elde edildiği ilk andan mahkemenin hükmüne esas alınacağı son ana kadar, belgelenmesine ve bu sürecin delil zinciri[672] ile garanti altına alınmasına bağlıdır.[673]

---

[667] Değirmenci, *Sayısal Delil,* 176; Değirmenci, "Bilgi Toplumunun Delil Türü," 21- 22.
[668] Yar. 4. CD., E. 2016/13150 K. 2016/13202 T. 7.10.2016. Aktaran: Başlar, "Elektronik Delil," 1668.
[669] Değirmenci, *Sayısal Delil,* 396.
[670] Giordano, "Electronic Evidence and the Law," 162.
[671] Başlar, "Elektronik Delilin Toplanması," 78.
[672] Delil zinciri, bir delilin fiziki veya dijital olarak toplanması, muhafaza edilmesi, başka bir yere aktarılması ve analiz ve incelenmesini gösteren kronolojik belgelendirme süreci olarak tanımlanmıştır. Başlar, "Elektronik Delilin Toplanması," 98.
[673] Olgun Değirmenci, "Yargılama Makamı İçin Şüphe, Müdafi İçin Savunma Nedeni: Adli Bilişimde Özet Değer (Hash Value) Kavramı ve Özet Değer Çakışmasının Ceza Muhakemesine Etkileri," *Terazi*

Dijital delillerin veri bütünlüğünün korunması, elektronik ve fiziksel koruma şeklinde iki biçimde ortaya çıkmaktadır. Elektronik koruma, dijital delillerin elde edildikleri ilk andan itibaren, bütünlüğünün bozulmadığını ve değiştirilmediğini, çeşitli mekanizmalar[674] aracılığıyla ispatlamayı içerirken fiziksel koruma ise dijital delillerin, bunlar üzerinde incelemenin gerçekleştirileceği laboratuvara bozulmadan getirilmesi ve mahkemeye sunulacağı ana kadar bütünlüğünün bozulmayacağı ortamlarda saklanmasını içerir.[675]

Olay yerinden elde edilen dijital verilerin, mahkemeye sunulana kadar muhafaza edilmesi ve değişikliklere ya da herhangi bir tahribata karşı korunması, hâkimin vicdani kanaatinin tam ve doğru delillere dayanarak oluşturulması açısından önemlidir. Bu bakımdan, dijital delillerin bütünlüğünün sağlanabilmesi ve korunabilmesi, hükme esas alınabilmesi bakımından önemli bir adımdır.[676]

Delillerin doğruluğunun kanıtlanmasındaki en önemli ölçütlerinden bir tanesi de delil zincirini sürdürmek ve belgelemektir.[677] Sağlam bir delil zinciri olmadan, delilin uygunsuz bir şekilde ele alındığı ve değiştirildiği veya suçlayıcı delillerle değiştirildiği iddia edilebilir.[678] Bu durum da elbette delilin kabul edilebilirliğini etkileyecektir.

Düzgün bir şekilde gerçekleştirilen raporlama neticesinde tutulan bir delil zinciri, dijital delilin belirli bir sistemden veya konumdan elde edildiğini ve toplandığı andan itibaren sürekli kontrol edildiğini gösterir. Bu nedenle düzgün şekilde hazırlanan delil zinciri belgeleri, mahkemenin dijital delilleri suçla ilişkilendirmesini kolaylaştırır. Eksik belgelendirme, dijital delilin nereden, nasıl, ne şekilde ve ne zaman

Hukuk Dergisi, C. 13, S. 137 (2018): 123; Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku*, 39- 40.

[674] Söz konusu mekanizmalar, ileride "dijital delillerin güvenilirliği" başlığı altında inceleyeceğimiz, birebir kopya alma ve özet değer çıkartılması işlemleridir. Ayrıntılarına ve delilin korunması konusunda sağladıkları katkıya daha ayrıntılı bir şekilde değinecek olmakla birlikte kısaca, elde edilen materyallerin birebir kopyalarının alınması ve sonrasında gerçekleştirilecek incelemenin bu kopyalar üzerinde yapılması, orijinal materyal üzerinde gündeme gelebilecek olası bozulmaların önüne geçerken, özet değer çıkartılması işlemi ise orijinal materyal ile elde edilen birebir kopya arasında bir fark olmadığını ispat etmeye yarayacaktır.

[675] Başlar, "Adli Bilişim," 51.

[676] Casey, *Digital Evidence,* 22; Değirmenci, *Sayısal Delil,* 189; Başlar, "Elektronik Delil," 1666; Afandak, "Ceza Muhakemesinde Dijital Deliller," 80.

[677] Casey, *Digital Evidence,* 21; Ćosić, Ćosić and Bača, "An Ontological Approach," 1.

[678] Casey, *Digital Evidence,* 22; Mifsud Bonnici, Tudorica and Cannataci, "The European Legal Framework," 191; Başlar, "Elektronik Delilin Toplanması," 81.

elde edildiği gibi sorulara cevap verme konusunda kafa karışıklığına neden olabilir ve dijital delilin güvenilirliği konusunda şüphelere yol açabilir.[679]

Bu bakımdan yukarıda bahsedilen ve dijital delillerin "toplanması", "incelenmesi", "analiz edilmesi" ve "raporlanması" aşamalarından oluşan adli bilişim safhalarının, doğru ve eksiksiz bir şekilde yönetilmesi ve delil zincirinin eksiksiz bir şekilde oluşturulması suretiyle veri bütünlüğünün sağlanması; elde edilecek dijital delilin, adli makamlar tarafından kabul görmesi bakımından oldukça önem arz etmektedir.[680]

3.2.3. Güvenilirlik

Delillerin kabul edilebilirliği tespit edilirken, mahkemeye sunulan delilin olayı doğrudan mı yoksa dolaylı bir şekilde mi temsil ettiği veya bizzat en başta şüpheli veya sanığın bilişim sistemlerinin incelenmesinde kullanılan adli yazılımların güvenli olup olmadığı gibi hususlar tartışılabilir.[681]

Delilin kaynağının sorgulanmadığı diğer delil biçimlerinin aksine, dijital delillerin güvenilirliği, kaynağının da güvenilir olmasına bağlıdır. Bu kaynak, verileri üreten, işleyen ve depolayan adli yazılımlardır.[682,683]

Gerçekten de dijital delillerin özgünlükleri ve veri bütünlüklerinin korunmasının yanı sıra bunların nasıl elde edildikleri ve daha sonra işlendikleri, gerçeklikleri ve doğrulukları hakkında da şüphe uyandıran hiçbir şey olmamalıdır.[684]

Yukarda bahsi geçen *Daubert* kararı uyarınca getirilen kriterler, bilimsel delillerin, bilimin yöntem ve prosedürlerinden elde edilen bilgilere dayanmasını sağlayarak *delillerin güvenilirlik standardı*nı karşılama girişimi olarak tasvir edilmiştir. Bu bağlamda bilginin geçerliliği, onu elde etmede kullanılan bilimsel metodolojiye bağlanmış ve güvenilirlik, sübjektif inançlar veya desteklenmeyen

[679] Casey, *Digital Evidence,* 60; Ćosić, Ćosić and Bača, "An Ontological Approach," 3.
[680] Önel ve Irmak, "Dijital delillerin windows işletim sistemi üzerinde incelenmesi," 1189.
[681] Giordano, "Electronic Evidence and the Law," 163; Değirmenci, *Sayısal Delil,* 396.
[682] Kenneally, "Gatekeeping out of the Box," 3.
[683] Ülkemizde kolluk tarafından da kullanılan EnCase, X-Ways ve FTK bu yazılımlara örnek olarak verilebilir. Detaylı bilgi için bkz. Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 147- 148.
[684] Giordano, "Electronic Evidence and the Law," 162; Afandak, "Ceza Muhakemesinde Dijital Deliller," 81.

spekülasyonlardan daha fazlası tarafından test edilerek doğrulanabilen ve desteklenen bir kavram olarak tanımlanmıştır.[685]

Bu bağlamda dijital delillerin güvenilirliği, onu elde etmede kullanılan metodolojinin güvenilirliği ve bilimselliğinin yanı sıra delili oluşturmak için kullanılan araçların doğruluğuna veya güvenilirliğine göre de değişebilecektir.[686] Bu sebeple dijital delillerin elde edilmeleri esnasında kullanılan tekniklerin ve kullanılan araçların doğruluğunun, gerektiğinde tüm adli süreç boyunca ispat edilebilmesi gerekmektedir.[687]

Dijital delillerin elde edilmeleri ve incelenmeleri esnasında kullanılan araçlar dendiğinde ise karşımıza adli yazılımlar çıkmaktadır. Bu yazılımlar ise açık ve kapalı kaynak kodlu olmak üzere iki şekilde oluşturulmaktadırlar.[688] Dijital delilin güvenilirliğinin tespit edilmesinde, onun elde edildiği yazılımların doğru çalışıp çalışmadığının kontrol edilmesinin önemli bir unsur olduğuna yukarıda değinmiştik. Buna karşılık kapalı kaynaklı kodla hazırlanan adli yazılımlarda böyle bir kontrol mekanizmasının söz konusu olamayacağını söyleyebiliriz. Gerçekten de kapalı kaynak kodlu yazılımlarda kaynak koduna, yalnızca o yazılımı geliştiren kişi tarafından erişilebildiği düşünüldüğünde, bu yazılımın doğru çalışıp çalışmadığının üçüncü kişilerce teyit edilmesi mümkün olmayacaktır. Bu husus da özellikle mahkemeleri, delillerin elde edildiği ve incelendiği kapalı kaynaklı kodla hazırlanan adli yazılımları *"güvenilir olarak varsayma"*[689] düşüncesine itmektedir. Sonuç olarak kapalı kaynak kodlu adli yazılımların bünyesinde hata bulundurduğuna ve yanlış sonuçlar verdiğine yönelik itirazlar, ispat şansı olmadığı için dikkate alınmamakta ve bu sebeple kendi içinde bir kısır döngü yaratmaktadır.[690]

---

[685] Kenneally, "Gatekeeping out of the Box," 8.
[686] Giordano, "Electronic Evidence and the Law," 167.
[687] Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* 40.
[688] Açık kaynak, bilgisayarlar tarafından kullanılan yazılım kaynak kodunun geliştirici dışındaki diğer kişilerin kullanımına sunulduğu koşulları tanımlamak için kullanılır. Kapalı kaynak ise tersi şekilde kaynak kodunun yalnızca geliştiricisi tarafından kullanılabildiği durumu tanımlar. Kenneally, "Gatekeeping out of the Box," 4.
[689] "The Presumption Of Reliability" kuralı, Amerikan Hukukunda uygulanan ve mahkemeye sunulan delilin elde edildiği kaynağın, sıkıntılı olduğunun ya da bozuk olduğunun ispat edilmediği sürece güvenilir sayıldığını kabul eden kuraldır. Buskirk and Liu, "Digital Evidence," 21; Chaikin, "Network investigations," 242; Kenneally, "Gatekeeping out of the Box," 16.
[690] Buskirk and Liu, "Digital Evidence," 21; yazar bu hususu şu soruyu sorarak eleştirmektedir. "Kişi, ilgili adli yazılımın kaynak kodunun hatalı olduğunu, elinde bir delil olmadan ispat edemiyorsa, ancak bu konuyla ilgili delili de kaynak koduna eriştiğinde bulabiliyorsa, güvenilir varsayma kuralının aksini nasıl ispat edebilecektir?".

Bu bağlamda dijital delilleri elde etmede kullanılan adli yazılımlarda ortaya çıkan hataların önlenmesi yahut en aza indirgenmesi ve bu sayede adli yazılımların ve bunlardan elde edilen delillerin güvenilirliklerinin sağlanması bakımından çeşitli önerilerde bulunulmuştur. İlk olarak adli yazılımlardan açık kaynaklı olanların kullanılması yahut kapalı kaynak kodlu olanların da açık hale getirilmesi ve bunların üçüncü kişiler tarafından da görülmelerinin sağlanması önerilmiştir.[691] Gerçekten de dünyanın her yerindeki programcılara kaynak kodu sağlamak, bu yazılımı inceleyenlerin programı daha iyi anlamasını sağlar ve hataların bulunma olasılığını artırır. Ancak ticari amaçla bu yazılımları geliştiren kişilerin, rekabet avantajlarını korumak için programlarının bazı bölümlerini ve hatta tamamını gizli tutmak isteyecekleri aşikardır.[692]

İkinci olarak kaynak kodunun tamamının veya bir kısmının mevcut olmayışı gibi durumlarda güvenilirliğin başka şekillerde de sağlanabileceği önerilmiştir.[693] Buna göre aynı bulguların elde edildiğinden emin olunması adına başka bir yazılım veya donanım kullanılarak incelenen delillerin güvenilir olup olmadıklarının tespit edilebileceği belirtilmiştir.[694] Buna ek olarak elde edilen sonuçların doğrulanması ve hata oranlarının belirlenmesi adına en etkili yaklaşımın, elde edilen sonuçların bir başka adli bilişim uzmanı tarafından da incelenmesi olduğu, başka bir ifadeyle başka bir adli bilişim uzmanının, sonuçların güvenilir ve tekrarlanabilir olduğundan emin olmak için birden fazla araç kullanarak bulguları iki kez kontrol etmesi olacağı belirtilmiştir.[695]

3.2.4. İnanılırlık

Elde edilen ve delili inceleyen yargı makamlarına sunulan deliller kolayca inanılır ve anlaşılır olmalıdır.[696] Bu bağlamda adli bilişim aşamalarında incelenen dijital delillerle ilgili bir rapor hazırlanması sırasında söz konusu raporun, dijital delilin inanılır bir dijital delil olmasındaki etkisi büyük olacaktır.

---

[691] Carrier, "Open Source Digital Forensics Tools" 8.
[692] Carrier, "Open Source Digital Forensics Tools" 8; Kenneally, "Gatekeeping out of the Box," 22- 23.
[693] Casey, *Digital Evidence,* 74.
[694] Casey, *Digital Evidence,* 74.
[695] Casey, *Digital Evidence,* 74.
[696] Giordano, "Electronic Evidence and the Law," 162; Afandak, "Ceza Muhakemesinde Dijital Deliller," 81.

Gerçekten de adli bilişim uzmanının, bu alanda sahip olduğu teknik bilgiler çoğunlukla yargılama makamları tarafından bilinmiyor olacaktır. Bu sebeple de teknik detaylarla dolu olan bir rapor, her ne kadar doğru sonuçlara işaret etse de hakimler tarafından anlaşılamayacağı için hükme esas alınamayabilecek yahut savunma ve iddia makamlarınca anlaşılamayacağı için rapora dayanılarak gerçekleştirilmesi beklenen iddia ve savunma eylemleri, doğru bir şekilde gerçekleştirilemeyebilecektir. Bu gibi sebeplerle hazırlanacak olan delil inceleme raporunun, özellikle delillerle ilgili ifadelerinin, alan hakkında hiçbir bilgisi olmayan bir kişinin dahi anlayabileceği bir dilde hazırlanması gerekmektedir. Bu doğrultuda teknik bilgisi, bir adli bilişim uzmanı kadar olması beklenmeyen yargılama makamlarının, raporda bahsedilenleri anlayabileceğini ve bunun da delilin inanılırlığını olumlu yönde etkileyeceğini söyleyebiliriz.[697]

3.3. Dijital Delillerin Güvenilirliği ve İspat Gücü

Dijital verilerin delil olarak kabul edilebilmeleri için diğer unsurlarla birlikte aynı zamanda güvenilir olmaları gerektiğine de yukarıda değinmiştik. Bu başlıkta dijital delillerin güvenilirliklerinin sağlanması adına uygulamada hangi işlemlerin gerçekleştirildiği ve bilişim sistemlerinin hangi özelliklerinin kullanıldığı anlatılacak olup, aynı zamanda dijital delillerin ispat gücü ve hangi durumlarda hükme esas alınıp alınamayacakları konusu değerlendirilmeye çalışılacaktır.

3.3.1. Dijital delillerin güvenilirliği

Dijital delillerin güvenilirliklerinin değerlendirilmesinde öncelikle delili oluşturan bilişim sisteminin normal şekilde çalışıp çalışmadığının tespit edilmesi ve bunun sonucunda elde edilen delillerin güvenilir olup olmadıklarının belirlenebileceği ileri sürülmüştür.[698] Buna karşılık bilişim sistemlerinin güvenilirliğinin bu şekilde değerlendirilmesinin zor olacağı çünkü uygulamada her bilişim sisteminin güvenilirliğinin değerlendirilmesi için yeterli donanım kaynağına sahip olunmadığı ve bilişim sistemlerinin artan çeşitliliği ve karmaşıklığı sebebiyle bu tarz bir değerlendirme yapılmasının, zaman geçtikçe pratik olmayan bir hal alacağı belirtilmiştir.[699]

---

[697] Casey, *Digital Evidence,* 391.
[698] Casey, *Digital Evidence,* 61.
[699] Casey, *Digital Evidence,* 61.

Bu bağlamda dijital delillerin güvenilirliği değerlendirilirken, delili oluşturan sürecin ve delili barındıran bilişim sisteminin güvenilirliğinden ziyade delilin kendisine odaklanılması gerektiği ileri sürülmüştür.[700] Gerçekten de belirli bir bilişim sisteminin genel olarak güvenilir olduğunu ispatlamaya çalışmak yerine, belirli bir dijital delil öğesinin değiştirilmediğini yahut müdahaleye uğramadığını uğradıysa dahi tahrif edilmediğini ispatlamaya çalışmak daha etkili ve pratik olacaktır.

Dijital deliller elde edilmesi ve güvenliklerinin sağlanması için gerçekleştirilen ve birazdan bahsedeceğimiz işlemler, çeşitli yazılım ve donanımlar aracılığıyla gerçekleştirilmektedir. Bununla birlikte denebilir ki dijital delili elde eden kişiler ve sonrasında elde edilenleri inceleyen mahkemeler büyük ölçüde bu adli araçlara ve onlardan çıkan sonuçlara güvenmektedirler. Ancak adli bir aracın düzgün çalışmaması gibi ihtimallerin gerçekleşmesi durumunda, bu güven ölümcül bir zayıflık haline gelebilmektedir. Bu nedenle, tamamen adli araçların sonuçlarına güvenmemek ve aynı zamanda önemli sonuçları da doğrulamak gerekli ve önemlidir.[701]

Bu konuyla ilgili olarak birazdan incelenecek tarih- zaman damgaları ile ilgili yapılan bir araştırma, bilgisayarda yapılan çeşitli kodlamalar aracılığıyla, dosya sistemi tarafından tutulan tarih- zaman damgalarının, adli yazılımlar tarafından takip edilemeyecek şekilde değiştirilebildiğini; ek olarak yine bazı kodlamalar aracılığıyla, dosya sistemi tarafından *ikili değer(bir ve sıfırlar)* sisteminde tutulan ve adli yazılımlar aracılığıyla bizler tarafından okunabilir hale getirilen zaman damgalarının, okunamaz halde tutulmasının sağlandığını ortaya koymuştur.[702,703]

Bu gibi ihtimaller, elde edilen delillerin güvenilirliğini etkileyecek niteliktedir. Gerçekten delil niteliğinde olabilecek dosyaların, gerek adli bilişim yazılımlarından kaynaklanan hatalar sebebiyle, gerekse bizzat adli bilişim yazılımlarının erişemeyecekleri veya gözden kaçırabilecekleri şekilde gerçekleştirilen gizleme

---

[700] Casey, *Digital Evidence,* 64.
[701] Casey, *Digital Evidence,* 457; Buskirk and Liu, "Digital Evidence," 19.
[702] Bu konu hakkında detaylı bilgi için ve bahsi geçen "kodlamalar" hakkında bkz. Buskirk and Liu, "Digital Evidence," 22.
[703] Bir örnek ile somutlaştırmaya çalışacak olursak, örneğin 01.01.2022 tarihinin ikili değer sistemindeki karşılığı, 110000 110001 101110 110000 110001 101110 110010 110000 110010 110010 dir. Bilgisayarların dosya sistemlerinde veriler, bu örnekte olduğu gibi ikili değer sisteminde tutulur ve bunların okunabilir hale getirilişi, adli bilişim yazılımlarıyla gerçekleştirilir. Bu bağlamda soruşturma veya kovuşturma konusu suçun işlendiği tarihle ilgili bir bilgi sağlayabilecek olan tarih- zaman damgası, bahsi geçen kodlamalarla *okunamaz* kılınırsa, 01.01.2022 tarihi, ikili değer formatında gözükmeye devam edecektir. (İkili değer sisteminden yazıya çeviri yapmak konusunda yardımcı bir kaynak olarak bkz. https://charactercalculator.com/tr/binary-translator/ , son erişim: 27.04.2022)

tekniklerinin sonucu olarak elde edilememe ihtimalleri bulunmaktadır. Bu sebeple adli bilişim yazılımlarının elbette araç olarak kullanımı devam etmelidir, ancak bu yazılımların yüzde yüz doğru sonuç vermeme ihtimallerinin bulunduğu da unutulmamalıdır.

3.3.1.1. Birebir kopya (imaj- forensic image- mirror image- ghosting- bitstream copy) alma

Birebir kopya alma, *"delilin üzerindeki bütün verilerin kopyasının alınması anlamına gelir."*[704] Öyle ki bu işlem ile, dijital delil niteliğindeki bir veri depolama birimi ve dosya içerikleri, adli bilişim yöntemleriyle veri bütünlüğüne bir zarar verilmeksizin birebir (bit-to-bit) şekilde kopyalanır.[705]

Bu anlamda birebir kopyalama, kullanıcı tarafından gerçekleştirilen dosya düzeyinde kopyalama ile farklılık arz etmektedir. Dosya düzeyinde gerçekleştirilen kopyalama, herhangi bir dosyanın çoğaltılması amacıyla kullanılırken[706] birebir kopyalama ile silinmiş, değiştirilmiş, deforme edilmiş verilere de ulaşılması olanağı vardır. Gerçekten de birebir kopya alma ile bir dijital depolama cihazının, kullanılmayan tüm alanı, silinen verileri, üst verileri ve hatta hasarlı alanları da dahil olmak üzere cihazın tam bir kopyasını üretilir.[707] Bu bakımdan birebir kopyanın doğru bir şekilde alınması, delil bütünlüğü açısından da büyük önem arz etmektedir.[708]

Yürütülen bir soruşturma çerçevesinde ele geçirilen bir bilişim sisteminin incelenmesi, *"dijital kirlilik"*[709] olasılığının en aza indirgendiği şekilde yapılmalıdır. Bu bağlamda ele geçirilen bilişim sistemlerinin birebir kopyasının üretilmesinin önemi, gerçekleştirilecek incelemenin bu kopya veya kopyalar üzerinden gerçekleştirilmesi ve bu bağlamda orijinal verilerin en az şekilde değişikliğe maruz bırakılması noktasında karşımıza çıkmaktadır.[710] Bununla birlikte dijital teknolojinin

---

[704] Ahmet Serhat Şirikçi ve Nergis Cantürk, "Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi," *Bilişim Teknolojileri Dergisi*, Cilt 5, Sayı 3 (2013): 29.
[705] Yılmaz ve Çakır, "Mobil Cihaz Adli Bilişimi Süreçleri," 28.
[706] Değirmenci, *Sayısal Delil,* 245.
[707] Marshall, *Digital Forensics,* 43; Robinton, "Courting Chaos," 326; Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 56; Şirikçi ve Cantürk, "Birebir Kopya Alınmasının (İmaj Almak) Önemi," 30.
[708] Dülger, *Bilişim Suçları,* 618.
[709] Kullanılan "dijital kirlilik" kavramı, orijinal cihaz üzerinde yapılan inceleme sırasında ilgili cihazı bilinçli veya bilinçsiz bir şekilde değişime uğratma anlamında kullanılmıştır. Marshall, *Digital Forensics,* 43.
[710] Marshall, *Digital Forensics,* 43; Chaikin, "Network investigations," 243; Kerr, "Digital Evidence And The New Criminal Procedure," 288; Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 146; Zeigler and Rojas, *Preserving Electronic Evidence for Trial,* 59.

kullanımının, bireyler ve işletmeler bakımından giderek yaygın bir hale gelişi, gigabaytlarca ve hatta terabaytlarca veri içeren bilişim sistemlerinin incelendiği vakaları artık olağan hale getirmeye başlamıştır.[711] Bu bağlamda gerek dijital delillerin birebir kopyasının alındığı depolama cihazlarının (ve bunları elde etmede kullanılan yazılım ve diğer donanımların) maliyetlerinin kamu üzerinde yarattığı olumsuz etki, gerekse de artan veri yığınlarının birebir kopyasının alınması için gereken sürenin zamanla artıyor oluşu; uygulayıcıları bu konuda, olay yerinde inceleme yapmaksızın direkt olarak el koyma tedbirini gerçekleştirmeye yahut dijital sterilize[712] işlemi gerçekleşmemiş hard diskleri, birebir kopya işleminde kullanmaya yönlendirebilmektedir.

Birebir kopya alınması işleminde karşılaşılabilecek bir sorun, kopyası alınacak bilişim sisteminin bir ortak bilgisayar veya ağ olması durumunda ne yapılacağıdır. Gerçekten de bu gibi durumlarda eksiksiz bir kopya üretilememe ihtimali bulunmaktadır.[713] Çünkü belirli ve sabit bir bilgisayar sisteminin olmadığı ağlarda veriler akışkan halde bulunmaktadır ve akışkan haldeki verilerin anlık görüntüleri alınabilse dahi bu veriler düzenli aralıklarla değiştiklerinden alınan görüntünün bir süre sonra anlamı kalmayacaktır.[714]

Bu gibi durumlarda "ön izleme" adı verilen ve ilgili bilişim sistemi üzerinde direkt inceleme yapma anlamına gelen yöntem[715] uygulanabilmektedir.[716] Ancak bu yöntemin, delilleri değişikliğe uğratabileceği, bozabileceği ve hatta ortadan kaldırabileceği için son derece tehlikeli olduğu ve yalnızca işin uzmanları tarafından uygulanması gerektiği belirtilmiştir. Ek olarak bu yöntemle dahi ağ trafiğini görüntülerken, trafiği oluşturan etkinlik ile verilerin monitörde görüntülenmesi arasında yine anlık bir gecikme olacağı ve bu sebeple de sonuçların tam olarak doğru olmayacakları belirtilmiştir.[717]

---

[711] Turner, "Managing Digital Discovery," 250.
[712] *Digital sanitation (dijital temizlik)* işlemi, birebir kopya almalarda kullanılan sabit disklerin, bir başka işlemde kullanmadan önce bit boyutunda temizlenmesini içeren işlemedir. Casey, Digital Evidence, 467.
[713] Marshall, *Digital Forensics,* 43.
[714] Chaikin, "Network investigations," 243.
[715] *Sniffer* adı verilen program aracılığıyla ağ trafiği canlı bir şekilde görüntülenebilmektedir. Chaikin, "Network investigations," 243; Casey, "Error, Uncertainty and Loss," 5.
[716] Detaylı bilgi için bkz. Marshall, *Digital Forensics,* 43- 47.
[717] Casey, "Error, Uncertainty and Loss," 5.

Yapısı gereği hassas olan dijital veriler ile ilgili olarak elde edildikleri ilk andan itibaren delil zincirinin oluşturulmasının, delillerin bütünlüğü ve dolayısıyla kabul edilebilirlikleri bakımından önem arz ettiğini yukarıda belirtmiştik. Bu bağlamda dijital delillerin elde edildiklerinde üzerlerinde gerçekleştirilecek ilk işlemin birebir kopya alma işlemi olduğunu ve birebir kopya alma işlemindeki bir eksiklik veya hatanın, inceleme ve raporlama aşamasında ortaya konan diğer delilleri de gölgeleyebileceğini söyleyebiliriz. Gerçekten de dijital delil incelemesi yapılan orijinal bilişim sisteminin kopyasının, düzgün bir şekilde kopyalanmadığı gibi bir ihtimal söz konusu olursa bu kopyadan elde edilen delillerin de doğrulanmadıkları müddetçe delil olarak kabul edilmeleri mümkün olmayacaktır.[718]

Son olarak birebir kopya alma işleminin, bu işlem için geliştirilmiş donanım veya yazılımlarla[719,720]; çevrimiçi (online imaging) ve çevrimdışı (offline imaging) olmak üzere iki şekilde gerçekleştirilebileceğini söyleyebiliriz. Bunları kısaca inceleyecek olursak;

Çevrimdışı birebir kopya, en basit yöntemdir, ancak kopyası alınacak bilişim sisteminin boyutuna bağlı olarak, gerçekleştirilecek bu işlem uzun bir zaman alabilir. Bu yöntemle, ilgili bilişim sistemi, yazılım engelleyici[721] kullanılarak bir birebir kopya alma cihazına bağlanır. Daha sonra birebir kopya alma yazılımı, ilgili bilişim sistemindeki verileri okumaya başlar ve ayrı bir dosyaya veya cihaza depolar. Birebir kopyalama tamamlandıktan sonra, ilk kopya genellikle ana kopya olarak kabul edilir ve gerektiğinde daha fazla çalışma kopyası oluşturulabilir.[722]

Elde edilecek kopyalarla ilgili şu hususun da belirtilmesi gerekir; bir donanım yazma engelleyici kullanılırken dahi orijinal depolama biriminin durumu değişikliğe uğrayabilir. Bu bağlamda *"her şeyi koru ama hiçbir şeyi değiştirme"* gibi bir kuralı mutlak bir standart olarak belirlemek, sadece diğer adli disiplinlerle tutarsız olmakla

---

[718] Yılmaz ve Çakır, "Mobil Cihaz Adli Bilişimi Süreçleri," 25.
[719] Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 146; Başlar, "Elektronik Delilin Toplanması," 91.
[720] Yazılımsal olarak birebir kopya alınması sırasında adli amaçlı olarak kullanılan yazılımlar, bağlanılan cihazın işletim sistemini kullanmaksızın, medya ile bağlantı kurar ve medyaya istenen işlemleri yaptırarak birebir kopyaların alınmasını sağlarlar. Detaylı bilgi için bkz. Şirikçi ve Cantürk, "Birebir Kopya Alınmasının (İmaj Almak) Önemi," 30.
[721] Yazılım engelleme aygıtları, incelenecek bilişim sisteminin belleğinde veya diğer veri depolama alanlarında yer alan verilerin değiştirilmesini engellemektedirler. Sonuç olarak yazılım engelleme aygıtının çalıştırılmasından sonra yapılan hiçbir işlem, bellekteki verileri değiştirmeyecektir. Değirmenci, *Sayısal Delil,* 361.
[722] Marshall, *Digital Forensics,* 47.

kalmaz, aynı zamanda yasal bağlamda da tehlikelidir. Çünkü böyle bir kabul söz konusu olursa bilişim sisteminin incelenmesi esnasında gerçekleşen önemsiz yanlışlıklar, delilin tamamen işlevsiz hale gelmesine yol açabilecek ve bu durum da suçların aydınlatılmasını geciktirebilecek ve hatta tamamen engelleyebilecektir. Böyle bir standarda uymak bazı durumlarda imkânsız bile olabilecektir.[723] Bu nedenle, *her şeyi koru ama hiçbir şeyi değiştirme* gibi bir kural yerine gerçekleşen değişikliklerin nedeninin açıklanması ve bunların dava üzerinde varsa etkilerinin, hazırlanacak raporlarda belirtilmesinin daha doğru olacağı ve bu sayede gereksiz tartışmaların da önüne geçileceği belirtilmiştir.[724]

Çevrimiçi birebir kopya, ilgili bilişim sisteminin kapatılmasının veya sisteme elkonulmasının mümkün olmadığı ya da birebir kopya alma aygıtının, ilgili bilişim sistemine bağlanmasının zor veya imkânsız olduğu durumlarda uygulanan bir yöntemdir. Bu yöntemle, ilgili bilişim sistemi yerinde bırakılır ve veriler, canlı birebir kopya alma araçları aracılığıyla toplanır. Bu yöntem, "ön izleme" yöntemine benzer sorunları barındırmakla birlikte benzer şekilde güvenilir araçların kullanılmasının ve işlemin uzman kişilerce gerçekleştirilmesinin, bu sorunların oluşmamasını veya en aza indirgenmesini sağlayacağı belirtilmiştir.[725]

3.3.1.2. Özet değer (hash value- hashing)

Bir bilişim sisteminin birebir kopyası oluşturulduktan sonra, delillerin korunması için ve değiştirilmesi veya bozulmasının önlenmesi için kopyası alınan bilişim sistemi ve kopyası, bir suç mahalliymiş gibi ele alınmalıdır.[726] Bu bağlamda dijital verilerin güvenilirliğinin sağlanmasında uygulanan yöntemlerden bir diğeri olan dijital delilin özet değerinin alınması kavramı karşımıza çıkmaktadır.[727] Özet değer;

> *"Bir bilgi dizgesi olan bilgisayar dosyasının (veya herhangi sabit olmayan boyuttaki bir veri dizgesinin) matematiksel işlemlere tabi tutulmak suretiyle, başka bir karakter veya sembole çevrilmesi işlemidir."*[728,729]

---

[723] Casey, *Digital Evidence,* 19-20.
[724] Casey, *Digital Evidence,* 76.
[725] Marshall, *Digital Forensics,* 47-48.
[726] Marshall, *Digital Forensics,* 48.
[727] Değirmenci, "Özet Değer (Hash Value) Kavramı," 120.
[728] Değirmenci, "Özet Değer (Hash Value) Kavramı," 123.
[729] Adli bilişimde, özet değerin hesaplanmasında kullanılan en yaygın algoritmalar, MD5 ve SHA-1'dir. SHA-1, MD5 e çok benzerdir ve ABD'nin özet değer almada kullanmayı tercih ettiği bir algoritmadır. Temel olarak, MD5 algoritması, 32 sayı ve harf kombinasyonundan oluşur ve bu kombinasyonu oluşturmak için bir bilişim sisteminde yer alan verileri kullanır. Ek olarak ülkemizde de özet değer

Özet değer, girilen verilere dayalı olarak sayısal bir değer üreten matematiksel bir hesaplamadır. Tekrar edilmesinin çok zor oluşu bakımından parmak izine de benzetilen hash değeri, dosyaların çeşitli karmaşık algoritmalar ile taranması ve dosyanın benzersiz bir özetinin oluşturulması suretiyle elde edilir.[730] Bu bakımdan özet değer, matematik işlemlerinde yapılan sağlama işlemlerine benzetilebilir.[731] Öyle ki elde edilen özet değer ile incelenen bilişim sistemi ve bu sistemden elde edilen kopya üzerinde herhangi bir değişiklik yapılmadığı ortaya konmaktadır. Bu bakımdan özet değeri alınan bir dosyanın bir nevi mühürlendiği söylenebilir.[732]

Orijinal bilişim sisteminin bir veya daha fazla özet değeri üretilmesi gerektiği belirtilmiştir.[733] Çünkü birebir kopya, orijinal bilişim sisteminden üretilmiştir ve elde edilen kopya, orijinal bilişim sisteminde bulunan verilerin birebir aynısını içermektedir. Bu sebeple birebir kopyanın özet değeri ile orijinal bilişim sisteminin özet değerinin birbiriyle eşleşmesi gerekmektedir.[734] Nitekim bu eşleşme, dijital delilin bütünlüğünün sağlanması bakımından da önem arz etmektedir.[735] Aksi durum, delilin değiştirildiği şüphesini doğurur ve bahsi geçen "mühürlenme" işleminin yanlış yapıldığı sonucunu ortaya çıkarır.

Buna karşılık örneğin, bozuk sektörler sonucu, alınan birebir kopyalarda ilk özet değer çıkarılması işleminden sonra "bad sektör" oluşması halinde ikinci özet değer alma işleminde özet değer doğal olarak farklı çıkacaktır. Ayrıca el konulan donanımların bozulması veya arızalı olmaları veya elektriksel sorunlar sebebiyle de özet değerin farklı çıkabilme ihtimali bulunmaktadır. Aynı şekilde birebir kopya almaya yarayan yazılım ve donanımlar üzerinde gerçekleşen teknik sıkıntılar sonucu orijinal bilişim sistemi ile alınan birebir kopya da aynı olmayabilir ve sonucunda

alınmasında en çok tercih edilen algoritmadır. Casey, *Digital Evidence,* 22- 23; Say, "Bilişim Suçlarında Elde Edilen Deliller," 78.

[730] Casey, *Digital Evidence,* 22; Ćosić and Bača, "Chain of Custody," 1227; Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 57; Philip Turner, "Unification of Digital Evidence from Disparate Sources (Digital Evidence Bags)," *Digital Investigation,* vol. 2 (2005) 225; Değirmenci, "Özet Değer (Hash Value) Kavramı," 120.

[731] Marshall, *Digital Forensics,* 49.

[732] Dülger, *Bilişim Suçları,* 588.

[733] Marshall, *Digital Forensics,* 49; Değirmenci, "Özet Değer (Hash Value) Kavramı," 123.

[734] Marshall, *Digital Forensics,* 49; Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 57; Değirmenci, "Özet Değer (Hash Value) Kavramı," 123.

[735] Başlar, "Elektronik Delilin Toplanması," 92; Göksoy, "Ceza muhakemesinde dijital delillerin elde edilmesi," 87.

çıkarılan özet değerler de farklı olabilir.[736] Bu sebeple kolluk kuvvetleri uygulamada özet değerin farklı çıkmasını ve delilin değiştirildiği şüphelerini önlemek adına bilişim sistemlerine doğrudan elkoyarak birebir kopyalarını kendi birimlerinde almayı tercih etmektedirler.[737]

Bu açıklamalardan sonra aynı özet değerine sahip iki özet değerin üretilmesinin mümkün olup olmadığı sorusu sorulabilecektir. Bu konu hakkında özet değerlerin çakışmasının, başka bir ifadeyle bir sistemden alınan ilk özet değer ile o sisteme sonradan başka şeyler eklenmesi ve sonrasında yeniden özet değer alınması sonucu oluşturulan özet değerin aynı olması ihtimalinin imkansıza yakın olduğu fakat yine de mümkün olabileceği belirtilmiştir.[738] Ancak bu olasılığın oldukça düşük olduğu ve delil üzerinde şüphe oluşturacak düzeyde olmadığı, bu sebeple de verilerin bütünlüğünün sağlanmasında özet değerlerin kullanılabileceği belirtilmiştir.[739]

Tüm bunlara karşılık özet değerler, elde edilen delillerin tam anlamıyla güvenilir olduğunu yine de göstermezler.[740] Çünkü özet değer, bilişim sisteminin o anki durumu göz önünde bulundurularak hesaplanır. Bu sebeple de özet değerin hesaplanmasından önce gerçekleştirilen değişiklikler ortaya konamaz. Bir örnek verecek olursak, şüpheli veya sanığın bilişim sistemini inceleyen fakat bu kişinin düşmanı olan adli bilişim uzmanı, özet değeri hesaplamadan önce delilleri değiştirmiş ve özet değeri sonrasında hesaplamışsa, elde edilen özet değerin değerlendirilmesi neticesinde gerçekleştirilen bu değişiklik tespit edilmeyecektir. Bu bakımdan birebir kopya ile orijinal bilişim sisteminin özet değerinin aynı olması, tek başına güvenilirliği sağlama konusunda her zaman yeterli olmayabilecektir. Bu sebeple özet değerin, bilişim sistemlerinde arama sırasında ilk müdahale esnasında eş zamanlı olarak alındığının da ispatlanması, dijital delilin güvenilir kabul edilebilmesi bakımından bir artı olacaktır.[741]

Son olarak özet değer işleminin bazı durumlarda suçların aydınlatılması amacıyla da kullanılabildiği görülmektedir. Özellikle çocuk pornografisi gibi suçlarda

---

[736] Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 57; Değirmenci, "Özet Değer (Hash Value) Kavramı," 125.
[737] Jones, v.d., *Bilişim Suçları Eğitim Modülü,* 57.
[738] Casey, *Digital Evidence,* 22- 23; Robinton, "Courting Chaos," 326.
[739] Değirmenci, "Özet Değer (Hash Value) Kavramı," 125.
[740] Casey, *Digital Evidence,* 24; Değirmenci, "Özet Değer (Hash Value) Kavramı," 124.
[741] Casey, *Digital Evidence,* 24; Başlar, "Elektronik Delilin Toplanması," 95; Değirmenci, "Özet Değer (Hash Value) Kavramı," 124; Değirmenci, *Sayısal Delil,* 250.

önceden yürütülen soruşturmalardan elde edilen materyallerin özet değerleri çıkarılarak bir veri tabanına kaydedilmektedir. Sonrasında yürütülen benzer soruşturmalarda, ele geçirilen ve üzerinde arama yapılan bilişim sisteminin özet değerleri ile önceden veri tabanına kaydedilen özet değerler karşılaştırılarak bir eşleşme olup olmadığı tespit edilebilmekte ve bu sayede de suça ilişkin deliller elde edilebilmektedir.[742]

3.3.1.3. Tarih- zaman damgası

Özet değer alınmasına ek olarak elde edilen dijital delile ilk ulaşılma zamanının (zaman damgasının) belirlenmesi de büyük önem arz etmektedir. Zaman damgası ve özet değer üretimi ile veriler üzerinde ikili kontrol noktası oluşturulmak suretiyle dijital delilin güvenilirliği artırılmış olacaktır.[743]

Başlarda bilgisayar işletim sistemi tarafından çeşitli hesaplamalarda kullanılmak amacıyla tasarlanan tarih- zaman damgaları, zamanla önemli bir araştırma aracı olarak da benimsenmiştir.[744] Gerçekten de muhakemeye konu olayın yeniden inşa edilmesinde özellikle yararlı bir teknik "zaman çizelgesi" oluşturulmasıdır. Bu yöntemde, kendileriyle ilişkilendirilmiş bir zaman damgası olan ayrı olaylar, bir zaman çizelgesinde sıralanırlar. Zaman damgaları, dosya sistemi üst verilerinden (meta-data), sistem günlüklerinden veya uygulama verilerinden elde edilebilen ve işletim sistemi tarafından oluşturulup yönetilen verilerdir.[745] Olayların kaynağına bağlı olarak zaman damgaları, bir sistemde (veya birden fazla sistemde) meydana gelen olayları ayrıntılı bir şekilde sıralar ve bu sayede adli bilişim uzmanları meydana gelen olayları sıralayarak muhakemeye konu olan fiili yeniden yapılandırabilirler.[746] Ancak bilgisayar sistemi tarafından kaydedilen zaman damgaları değerlendirilirken, birkaç faktörün dikkate alınması gereklidir.

Bir bilişim sistemindeki zaman, sistemin donanım saati tarafından veya bazı durumlarda ek bir yazılım sistemi tarafından tutulur. Bu saatlerin doğruluğuna, nasıl başlatıldıklarına ve senkronize olup olmadıklarına bağlı olarak, gösterilen saat, *gerçek*

---

[742] Casey, *Digital Evidence,* 24; Değirmenci, *Sayısal Delil,* 363.
[743] Önel ve Irmak, "Dijital delillerin windows işletim sistemi üzerinde incelenmesi," 1189; Başlar, "Elektronik Delilin Toplanması," 95.
[744] Buskirk and Liu, "Digital Evidence," 21; Ćosić and Bača, "Chain of Custody," 1227.
[745] Marshall, *Digital Forensics,* 50; Buskirk and Liu, "Digital Evidence," 21; Ćosić and Bača, "Chain of Custody," 1227.
[746] Marcella and Guillossou, *Cyber Forensics,* 242.

zamandan oldukça farklı olabilir.[747] Ayrıca, saatler yanlış zaman diliminde olacak şekilde yanlış yapılandırılabilir veya yanlış zamana ayarlanmış olabilir, keyfi olarak manipüle edilebilir ya da hızlı veya yavaş çalıştırılabilir (*clock skew*).[748] Bu sebeple bilişim sistemleri incelenirken, ilgili bilişim sisteminin tarih ve saatini not etmek ve onu güvenilir bir saat kaynağıyla karşılaştırmak çok önemlidir.[749]

Bunlara karşılık bu tarz izole ağların saatlerindeki yanlışlıklar, internete bağlanıldığı anda görünür olacaktır.[750]Ağ Zaman Protokolü (Network Time Protocol-NTP)[751], bilgisayarların saatlerini belirli bir zaman referansına senkronize etmek için kullanılan bir İnternet protokolüdür.[752] Yerel saat dilimi farklılıkları, kafa karışıklıklarına neden olabilmekle birlikte Web sunucuları, greenwich ortalama saatine göre tarih-zaman damgalı günlükler oluşturur. Bu bakımdan da zamansal hataların bir miktar da olsa önüne geçilmesi sağlanır.[753] Ek olarak ağ trafiği analizi sırasında bahsi geçen birebir kopya alınması ve özet değerinin çıkarılması hususu, verinin akış halinde oluşu sebebiyle anlamını yitirecektir. Bu sebeple akış halindeki bu verilerin doğruluğunun ve gerçekliğinin bir başka ifadeyle güvenilirliklerinin sağlanması bakımından ağ trafiğinin zaman damgasının alınmış olması hayati önem arz etmektedir.[754]

Zaman damgaları belirtildiği üzere dosya sistemi kayıtlarında saklanan üst verilerdir (meta-data). Ek olarak zaman damgası verileri, sistem günlükleri ve uygulama verileri gibi diğer konumlarda da bulunabilir. Örneğin Microsoft Office ürünleri gibi çeşitli programlar, dosya içeriğine veya üst veri etiketlerine kendi tarih ve saat kayıtlarını koyar. Ancak dosya sistemi düzeyinde tutulan tarih ve saat damgası, dosyanın kendisinde depolanan saat ve tarih damgalarını değiştirmez.[755]

---

[747] Önel ve Irmak, "Dijital delillerin windows işletim sistemi üzerinde incelenmesi," 1189- 1190.
[748] Marcella and Guillossou, *Cyber Forensics,* 242; Casey, "Error, Uncertainty and Loss," 6; Başlar, "Elektronik Delilin Toplanması," 96.
[749] Casey, *Digital Evidence,* 20.
[750] Marcella and Guillossou, *Cyber Forensics,* 242.
[751] Ağ zaman protokolü, ulusal standart zamanın, İnternet ve bağlı özel ve kurumsal ağlar aracılığıyla sistematik olarak yayılmasını sağlayan entegre bir teknolojidir. Ağ zaman protokolünün nihai amacı, bu protokole dahil olan tüm bilgisayarlardaki saatleri evrensel zamana göre bir veya iki milisaniyeden daha kısa bir düzende senkronize etmektir. Ağ zaman protokolü ve çalışma prensibi hakkında daha detaylı bilgi için bkz. David L. Mills, *Computer Network Time Synchronization; The Network Time Protocol* (USA: CRC Press, 1st edition, 2006), 2- 3.
[752] Marcella and Guillossou, *Cyber Forensics,* 243.
[753] Casey, "Error, Uncertainty and Loss," 8.
[754] Başlar, "Adli Bilişim," 57.
[755] Marcella and Guillossou, *Cyber Forensics,* 244.

Bilişim sistemlerinde tutulan üç çeşit tarih- zaman damgası bulunmaktadır.

3.3.1.3.1. Oluşturulma tarihi ve zamanı

Oluşturma tarihi ve zamanı, bir dosyanın veya klasörün orijinal oluşturulma tarihini ve zamanını belirtir.[756] Dosya veya klasör oluşturulduğunda veya bir konuma ilk kez kaydedildiğinde, oluşturma tarihi ve zamanı dosya sistemine kaydedilir. Asıl amacı orijinal dosya oluşturulma tarihini ve saatini belirtmek olduğundan, bu tarih ve saat özelliği daha sonra asla değişmez.[757]

3.3.1.3.2. Son değiştirilme tarihi ve zamanı

Son değiştirilme tarihi ve zamanı, dosya veya klasörün en son ne zaman değiştirildiğini dosya sistemleri düzeyinde gösterir. Dosyanın içeriği değiştirildiğinde ve kaydedildiğinde, son değiştirilme tarihi ve zaman damgası, değişikliklerin yapıldığı zamana karşılık gelecek şekilde düzenlenir.[758]

3.3.1.3.3. Erişim tarihi

Erişim tarihi dosya sistemleri düzeyinde bir dosyaya en son ne zaman erişildiğini gösterir. Son erişim tarihi özelliği, değiştirilme tarihinden farklıdır. Değişiklik tarihi ve zamanı, bir dosyanın içeriğinde son değişikliklerin ne zaman yapıldığını gösterirken, son erişim tarihi mutlaka içerik değişikliklerini gerektirmez. Bir dosya değiştirildiğinde, değişiklik ve son erişim tarihleri aynı değere ayarlanır. Ancak dosya yalnızca görüntülenmek, kopyalanmak, taşınmak için açılırsa yalnızca son erişim tarihi güncel tarih olarak değiştirilir. Ek olarak bazen, bazı programların dosya veya klasörlerle çalışması nedeniyle son erişim tarihi değişebilir. Örneğin virüs tarama amacıyla dosyalara erişen bir anti-virus yazılımı, eriştiği dosyanın tarih damgasını değiştirecektir.[759] Son olarak birçok işletim sisteminde, erişim tarihi damgasında yalnızca son erişilen tarihin kaydedildiğini belirtmemiz gerekir.[760]

---

[756] Marshall, *Digital Forensics,* 50.
[757] Marcella and Guillossou, *Cyber Forensics,* 244.
[758] Marcella and Guillossou, *Cyber Forensics,* 244; Marshall, *Digital Forensics,* 50.
[759] Marcella and Guillossou, *Cyber Forensics,* 245.
[760] Marshall, *Digital Forensics,* 50.

3.3.1.3.4. Giriş değişikliği zamanı

Giriş değişikliği zaman damgası önceki üç zaman damgasından farklı olmak üzere yalnızca NTFS[761] dosya sistemlerinde bulunan bir zaman damgasıdır. Standart bilgi içeren dosyaların değişikliğe uğramalarında, dosya adı değişikliklerinde ve de yukarıda bahsi geçen herhangi bir tarih zaman damgası değişikliklerinde, giriş değişikliği zaman damgası da güncellenir.[762]

3.3.2. Dijital delillerin ispat gücü

Dijital delil kavramı bir delil türüne işaret etmemektedir. Başka bir deyişle delilin, dijital boyutta bulunduğunu ifade etmektedir. Bu bakımdan dijital delillerin ispat gücü, aynı fiziksel delillerde olduğu gibi olayı temsil ediciliğine göre değişecektir. Bu anlamda dijital delillerin kabul edilebilirliği konusunda sınırların belirli hale getirilmesi adına önerilen bir görüş dijital delillerin kabul edilebilirlikleri bakımından bazı ön kabuller getirmiştir. Buna göre dijital deliller kendiliğinden doğrulanmış sayılan ve sayılmayan deliller olarak ayrılabilecektir. Yapılan bu ayrım ise delili elde eden kişilerin belirli sertifikasyonlara sahip olması veya elde edilen delilin belirli doğrulanmış yollarla elde edilmesi veya edilmemesi şeklinde hayat bulacaktır.[763]

Yine benzer şekilde dijital delillerin tek başlarına kabul edilebilir olup olmadıklarının tespit edilmesi hususunun delilin niteliğine göre belirlenmesi gerektiği belirtilmiştir. Bu bağlamda delil örneğin bir kişi tarafından oluşturulan ve bilişim sisteminde saklanan bir delil ise bunun kabul edilebilmesi bakımından diğer delillerle desteklenmesi hususu aranabilecekken; delil, bilişim sistemi tarafından insan müdahalesi olmaksızın yaratılmışsa burada doğrulanması gereken husus, bilişim sisteminin düzgün işleyip işlemediği olacaktır. Bu bağlamda insan müdahalesi olmaksızın oluşturulan deliller, bilişim sisteminin de düzgün çalıştığının tespit edilmesi ile birlikte tek başlarına delil olarak kabul edilebileceklerdir.[764]

---

[761] "*New Technology File System- Yeni Teknoloji Dosya Sistemi",* Microsoft tarafından eski dosya sisteminin yeniden yapılandırılması suretiyle oluşturulmuştur. NTFS hakkında detaylı bilgi için bkz. Kam Pui Chow, v.d., "The Rules of Time on NTFS File System," ***Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07)*** (2007): 1.

[762] Buskirk and Liu, "Digital Evidence," 21.

[763] İlgili öneri hakkında detaylı bilgi için bkz. Grimm, Capra and Gregory, "Authenticating Digital Evidence," 38 v.d.

[764] Değirmenci, *Sayısal Delil,* 392.

3.3.3. Avrupa insan hakları mahkemesi kararlarında dijital deliller

AİHM, bilişim sistemleri üzerinde gerçekleştirilen arama, kopyalama ve elkoymaların, kişilerin özel hayat hakkına müdahale edebileceğini kabul etmektedir. Ancak söz konusu müdahalede kullanılan nedenlerin, ilgili, yeterli ve hedeflenen amaca göre orantılı olmasını beklemektedir. AİHM, içtihatlarında genellikle bilişim sistemleri üzerinde gerçekleştirilecek aramaların, "yasal" olmasını ve "keyfiliğe ve istismara karşı usul açısından yeterli mekanizmalara sahip" olması hususlarına odaklanmaktadır.[765]

Bu bağlamda *Petri Sallinen ve diğerleri* kararında başvuranın hukuk bürosunda gerçekleştirilen bir arama esnasında bilgisayarlarının ve disketlerinin aranmasıyla ilgili olarak mahkeme öncelikle, uygulanacak tedbirin AİHS m. 8/2 kapsamında hukuka uygun olabilmesi için ihtilaf konusu tedbirin iç hukukta bir temele sahip olması gerektiğini ve tedbirin ilgili kişi hakkında uygulanan kişiler bakımından erişilebilir olması gerektiğini, bu kişilerin ayrıca tedbirin sonuçlarını öngörebilmesini ve tedbirin hukukun üstünlüğü ile uyumlu olmasını gerektiğini belirtmiş, sonucunda ise mevcut davadaki arama ve el koyma tedbirlerinin uygun yasal güvenceler olmaksızın uygulandığını ve uygulanan tedbir neticesinde incelenen imtiyazlı materyalin (bilgisayar, disketler) araştırmaya tabi tutulabileceği durumların uygun bir kesinlikle kaleme alınmadığını bu sebeple de, başvuranların demokratik bir toplumda hukukun üstünlüğü kapsamında hak ettikleri asgari koruma derecesinden yoksun bırakıldıklarını belirterek AİHS m. 8'in ihlal edildiğine karar vermiştir.[766,767]

Farklı olarak AİHM, *Görmüş ve Diğerleri* kararında bilgisayarlar ve buna bağlı olarak kullanılan programlar ve kütüklerle ilgili yapılan aramalarla ilgili bir başvuruyu değerlendirirken ise, AİHS m. 10'da düzenlenen 'İfade özgürlüğü' üzerinde durmuştur. Nitekim AİHM, başvurucuların işyerlerinde yapılan arama neticesinde basılı ve dijital belgelerine el konulmasını, bilgisayarlarında yer alan tüm içeriğin harici disklere kopyalanmasını ancak bu kopyalarda olaylarla ilgisi olmayan bilgilerin de elde edildiğini, söz konusu müdahalenin izlenen amaçla orantısız olduğunu, bu durumun da başvurucuların ifade özgürlüklerine, haber verme haklarına yapılan bir

[765] Değirmenci, *Sayısal Delil,* 97.
[766] Petri Sallinen and Others v. Finland, başvuru no: 50882/99, T. 27/12/2005, https://hudoc.echr.coe.int/tur?i=001-70283 , son erişim: 25.04.2022.
[767] Benzer bir karar için bkz. Yuditskaya And Others v. Russia, başvuru no: 5678/06, T. 12/05/2015, https://hudoc.echr.coe.int/tur?i=001-151037 , son erişim: 25.04.2022.

müdahale olduğunu, bu müdahalenin zorunlu bir sosyal ihtiyacı karşılamadığını, söz konusu müdahalenin demokratik bir toplumda gerekli olmadığını belirterek AİHS m. 10'un ihlal edildiğine hükmetmiştir.[768]

Benzer şekilde *Nagla V. Latvia* kararında yine gazeteci olan başvuranın, suç işlediği şüphesi ile hakkında araştırılma yapılan bir haber kaynağı ile iletişime geçtiği tespit edilen kişisel bilgisayarına ve çok sayıda veri depolama cihazına; bu haber kaynağının kimliğinin açığa çıkarılması adına el konulmuştur. Başvuran gerçekleşen eylemlerle ilgili olarak AİHS m. 10 tarafından güvence altına alınan bilgi alma ve verme hakkının ihlal edildiğini ve bir gazetecilik kaynağının kimliğinin tespit edilmesini sağlayan bilgileri açıklamaya mecbur bırakıldığını ileri sürmüştür. AİHM ise gerçekleştirdiği inceleme neticesinde söz konusu müdahalenin demokratik bir toplumda gerekli olmadığı kanaatine ulaşmış ve AİHS m. 10'un ihlal edildiğine karar vermiştir.[769]

Ek olarak arama kararında gösterilen fiil ile ilgili olmayan verilerde arama yapılması halinde orantısızlık gündeme gelebilecektir. Nitekim AİHM de ölçülülüğe işaret etmekte ve müdahalenin amaçla uyumlu olup olmadığı hususlarını denetlemektedir.[770] Bu bağlamda herhangi bir suçun delili olarak kabul edilemeyecek nitelikte olan başvuranın bilgisayarının, uzun bir süre için alıkonulmasını nedensiz bulmuştur.[771]

3.3.4. Anayasa Mahkemesi kararlarında dijital deliller

Anayasa Mahkemesi, dijital delillerin elde edilmesi konusunda çeşitli incelemelerde bulunmakla birlikte burada yalnızca ihlal kararı vermiş olduğu mülkiyet hakkı, eğitim hakkı, özel hayata saygı hakkı ile haberleşme hürriyeti hakkında yapmış olduğu değerlendirmelere yer verilecektir.

---

[768] Görmüş ve Diğerleri/Türkiye, Başvuru No. 49085/07, T. 19.01.2016, www.hudoc.echr.coe.int/tur?i=001-163484 , son erişim: 25.04.2022. Aktaran: Özel, "Bir Koruma Tedbiri Olarak Arama," 1250.

[769] Nagla V. Latvia, başvuru no: 73469/10, T. 16/10/2013, https://hudoc.echr.coe.int/tur?i=001-122374 , son erişim: 25.04.2022.

[770] Ursula Kilkelly, "Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı," *Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesinin Uygulanmasına İlişkin Kılavuz*, İnsan Hakları El Kitapları No. 1, Ankara (Nisan 2012): 68. Aktaran: Değirmenci, *Sayısal Delil,* 382.

[771] Smirnov v. Russia, başvuru no: 71362/01, T. 12/11/2007, https://hudoc.echr.coe.int/tur?i=001-80953 , son erişim: 25.04.2022, Aktaran Değirmenci, *Sayısal Delil,* 382.

İlk olayda yürütülen bir muhakeme sürecinde başvurucunun cep telefonunu muhafaza altına alınmış ancak hakkında verilen karar kesinleşmiş olmasına rağmen telefonu kendisine iade edilmemiştir. AYM, öncelikle söz konusu telefona el konulmasının sebebinin suçta kullanılması veya suçtan elde edilmesi olmadığını fakat barındırdığı bilgiler neticesin ispat aracı niteliğinde olduğunu değerlendirmiştir. Bu kapsamda cep telefonu hakkında CMK m. 134 kapsamında elkoyma tedbirinin uygulanmasında cep telefonlarının, bilgisayar özelliği taşıdıkları ölçüde bilgisayar olarak kabul edilebileceği gerekçe gösterilerek gerçekleştirilen işlemin, kanuni dayanağının bulunduğu ifade edilmiştir. Buna karşılık başvurucu hakkında verilen kararın kesinleşmiş olması ve başvurucu hakkında başka bir soruşturmanın bulunduğu da iddia edilmediğine göre cep telefonunun içeriğinden elde edilecek bulgular yönünden ispat vasıtası olma ihtimalinin kalmadığı değerlendirilmiştir. Bu koşullarda başvurucunun cep telefonunun iade edilmemesinin kamu yararına yönelik meşru bir amacının bulunmadığı ifade edilmiş ve Anayasa m. 35 kapsamında güvence altına alınan mülkiyet hakkının ihlal edildiğine karar verilmiştir.[772]

Bir diğer başvuru, başvuranın kendisine ait olan ancak el konulan bilgisayarının birebir kopyasının kendisine verilmemesi sonrasında bilgisayar içinde yer alan doktora tezini üniversiteye teslim edememesi nedeniyle eğitim hakkının ihlal edildiği iddialarına ilişkindir. Bu bağlamda başvurucuya ait bir dijital materyal hakkında tatbik edilen elkoyma koruma tedbiri ile başvurucunun eğitim hakkına müdahale edilmiş olduğu belirtilmiş, sonrasında başvurucunun bu konu hakkındaki şikâyetini soruşturma makamlarına taşımış olduğu ve soruşturma ve yargılama makamlarının başvurucunun talebi ile ilgili olarak olumlu ya da olumsuz hiçbir değerlendirmede bulunmadığı tespit edilmiştir. Bu bağlamda başvurucunun koruma tedbirine ilişkin getirilen usuli güvencelerden beş yıl gibi makul olmayan bir süre boyunca ve öngörülemez bir şekilde yararlandırılmadığı değerlendirilmiştir. Sonuç olarak başvurucunun isteminin hâlen yerine getirilmemiş olduğu hususu da dikkate alınarak somut olayda Anayasa m. 42 kapsamında güvence altına alınan eğitim hakkının ihlal edildiği sonucuna ulaşılmıştır.[773]

---

[772] AYM, Ercan Demirbaş Başvurusu, Başvuru no. 2018/20608, T. 15/9/2021, R.G. Tarih ve Sayı: 26/10/2021-31640, https://kararlarbilgibankasi.anayasa.gov.tr/ , son erişim: 25.04.2022.

[773] AYM, Barış Yiğit Başvurusu, Başvuru no. 2016/67924, T. 7/9/2021, https://kararlarbilgibankasi.anayasa.gov.tr/ , son erişim: 25.04.2022.

Son bir başvuru, başvuranın haberleşme programı yoluyla yaptığını ileri sürdüğü yazışmalarının incelenmesi nedeniyle haberleşme hürriyeti ile özel hayata saygı hakkının ihlal edildiğine ilişkindir. AYM bu olayda, başvuranın özel hayatına bir müdahalede bulunulduğunu kabul etmekle birlikte, söz konusu müdahalenin CMK kapsamında alınan bir karar neticesinde gerçekleştirilmesi nedeniyle öncelikle müdahalenin kanuni dayanağının bulunduğunu belirtmiştir. Devamında söz konusu müdahale ile hedeflenen şeyin, suç işlenmesinin önlenmesi ve suç kanıtlarının elde edilmesi amacına yönelik olarak gerçekleştirildiğini belirtilerek müdahalenin haberleşme hürriyeti bakımından meşru bir amaca dayandığını ifade etmiştir. Öte yandan özel hayata saygı hakkı için Anayasada herhangi bir sınırlama nedeni öngörülmemiş olmakla birlikte bu hakkın hiçbir şekilde sınırlandırılması mümkün olmayan mutlak bir hak olduğunun söylenemeyeceği ifade edilmiş ve çeşitli kararlara atıfta bulunularak Anayasa'nın başka maddelerinde yer alan hak ve özgürlükler ile devlete yüklenen ödevlerin özel sınırlama sebepleri gösterilmiş ve bunların hak ve özgürlüklere sınır teşkil edebileceği belirtilmiştir. Açıklananlar neticesinde de güvence altına alınan özel hayata saygı hakkı ile haberleşme hürriyetinin ihlal edilmediğine karar verilmesi gerektiği hüküm altına alınmıştır.[774]

3.4. Delil Yasakları ve Dijital Deliller

3.4.1. Hukuka aykırı delil kavramı

Belirtildiği üzere ceza muhakemesinin amacı, maddi gerçeğin ortaya çıkarılmasıdır. Ancak maddi gerçeğin ortaya çıkarılması demek, her ne pahasına olursa olsun bu amacın gerçekleştirilmesi anlamına gelmemektedir. Gerçekten de aksi bir kabul, pek çok kişisel ve toplumsal değeri tahrip edebilir ve sayısız hak ve özgürlüğün anlamını yitirmesine neden olabilir. Bu noktada karşımıza delil yasakları kavramı çıkmaktadır. Öyle ki hukuk devletine uygun bir şekilde gerçekleştirilen ceza muhakemesi süreçlerinde elde edilen delillerin hukuka uygunluğunun sınırları, delil yasakları ile çerçevelenmektedir.[775]

---

[774] AYM, C.E. Başvurusu, Başvuru no. 2016/436, T. 12/9/2019, https://kararlarbilgibankasi.anayasa.gov.tr/ , son erişim: 25.04.2022.

[775] Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* 398; Tezcan, v.d., *Dijital Ceza Muhakemesi Hukuku,* 435; Yenisey ve Nuhoğlu, *Ceza Muhakemesi Hukuku,* 566; Özbek, Doğan ve Bacaksız, *Ceza Muhakemesi Hukuku,* 662.

CMK'da yer alan koruma tedbirleri insan hak ve özgürlüklerini kısıtlayıcı niteliktedirler. Bu sebeple bu tedbirler uygulanırken muhakeme yönünden doğabilecek zararın ağırlığı ve bunun gerçekleşmesi ihtimalinin yoğunluğu ile orantılı olması gerekecektir. Başka bir ifadeyle, delilden elde edilecek hukuki yarar ile delilin elde edilmesiyle neden olunabilecek zarar arasında, doğacak zararın daha hafif olması gerekecektir.[776] Ek olarak tedbir uygulandığı sırada tedbirin aleyhine uygulandığı kişinin insan hak ve özgürlüklerinin hukuki sınırları aşar biçimde sınırlandırılmamasına ve kişisel verilerinin zarar görmemesine dikkat edilmesi gerekmektedir.[777] Aksi durum, kişilerin temel hak ve hürriyetlerine haksız müdahale sonucunu doğurur ki bu durumda delil hukuka aykırı elde edilmiş olur ve elde edilenler delil olarak değerlendirilemez.[778]

Dijital soruşturmalar, özellikle özel hayatın gizliliği hakkı ve kişisel verilerin korunması hakkı olmak üzere temel hakların önemli bir kısmını ihlal etme potansiyeline sahiptir. Bu nedenle, bu tür soruşturmalar, 23 Kasım 2001'de Avrupa Konseyi tarafından düzenlenen Siber Suçlar Sözleşmesi'nin 15. Maddesinin açıkça gerektirdiği gibi, Orantılılık İlkesi ile uyumlu olmalıdır.

Bu bağlamda dijital delillerin elde edilmesi ile; [779]

- Günümüzde kişilerin özel hayatına ilişkin bilgilerinin çoğunun bilişim sistemlerinde barındırılması sebebiyle, özel hayatın gizliliği hakkı,
- Bilişim sistemlerinin, aynı zamanda veri iletişi amacıyla da kullanılabildiği değerlendirildiğinde, kişinin haberleşme gizliliği,
- İkinci nesil WEB sayfalarının gelişmesi sebebiyle kişilerin artık bilgi tüketicisi yerinde bilgi üreticisi olmaları sebebiyle, kişilerin düşüncelerini yayma hürriyeti,
- Bilişim sistemlerinde kişiyi tanımlayan verilerin tutulması ve işlenmesi sebebiyle, kişisel verilerin usulüne uygun olarak korunması ve kişinin kendi kişisel verileri üzerindeki serbestçe tasarruf hakkı (kısaca kişinin kişisel verilerinin geleceğini belirleme hakkı)

[776] Kızılyar, "Ceza Yargılaması," 76.
[777] Özen ve Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama," 68.
[778] Börekçi, "Bilgisayarlarda, Bilgisayar Programlarında," 11.
[779] Değirmenci, *Sayısal Delil,* 89.

Gibi haklar ihlal edilebilecektir.

Gerçekten kişiye ait bilişim sistemlerinde arama yapılması ve bunlara el konulması, bilişim sistemleri aracıyla kişinin düşüncelerini açıklamak ve yaymak hakkı ile doğrudan bağlantılıdır. Bu bağlamda akış halindeki verilerin ele geçirilmesi de düşünceyi açıklama ve yayma hakkına müdahale eder niteliktedir.[780]

CMK m. 217/2 uyarınca *"Yüklenen suç, hukuka uygun bir şekilde elde edilmiş her türlü delille ispat"* edilebilecektir. Buna göre hukuka aykırı bir şekilde elde edilmiş olan delillerin, muhakemede kullanılabilmesi mümkün değildir. Söz konusu yasak, muhakeme evrelerinin tümünde ve muhakemeye katılan tüm taraflar bakımından geçerlidir.[781]

Hukuka aykırı şekillerde elde edilen deliller, ihlal edilen hakkın niteliğine göre delilin özgünlüğünü etkileyerek delili şüpheli ve hatta kullanılamaz hale getirebileceği gibi kişilerin, Anayasa, Uluslararası sözleşmeler ve kanunlarca düzenlenen ve korunan haklarına da müdahale teşkil edecektir.[782] Bu bağlamda iç hukukta açıkça yasaklanmış yöntemlerle elde edilen deliller, açık bir yasaklama olmasa da ilgili kurallara aykırı biçimde elde edilen deliller ve ayrıca iç hukukta bir düzenleme bulunmayan hallerde de uluslararası ve evrensel kurallara aykırılık oluşturan yöntemlerle ulaşılan deliller hukuka aykırı deliller olarak değerlendirilecektir.[783] Bu bağlamda delil yasakları ile gerçeğin bulunmasının, meşru bir ceza verilmesinin ve temel hak ve özgürlüklerinin korunmasının[784] hedeflendiğini söyleyebiliriz.[785]

Konuyla ilgili olarak mevzuatta bir terminoloji karmaşası söz konusudur. Öncelikle Anayasa m. 38/6 incelendiğinde *"Kanuna aykırı olarak elde edilmiş bulgular, delil olarak kabul edilemez."* hükmü karşımıza çıkmaktadır. Benzer şekilde CMK m. 206/2-a bendi incelendiğinde yine *"kanuna aykırı olarak elde…"* edilen delillerin reddedileceği hüküm altına alınmıştır. Bunlara karşılık CMK m. 217/2 uyarınca yüklenen suçun, *"hukuka uygun bir şekilde elde edilmiş…"* olan her türlü

[780] Değirmenci, *Sayısal Delil,* 105.
[781] Özbek, Doğan ve Bacaksız, *Ceza Muhakemesi Hukuku,* 382.
[782] Değirmenci, *Sayısal Delil,* 390.
[783] Kızılyar, "Ceza Yargılaması," 77.
[784] Yazar burada bir karşılaştırma yaparak delil yasakları ile Kıta Avrupası hukuk sisteminde temel hak ve özgürlüklerin korunmasının; Anglo-Amerikan hukuk sisteminde ise kolluk görevlilerinin disiplin altına tutulmasının hedeflendiğini belirtmiştir. Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* 398- 399.
[785] Özbek, Doğan ve Bacaksız, *Ceza Muhakemesi Hukuku,* 663.

delille ispat edilebileceği, yine CMK m. 230/1-b bendinde hükmün gerekçesinde *"…hukuka aykırı yöntemlerle elde edilen…"* delillerin ayrıca gösterilmesi gerektiği ve son olarak CMK m. 289/1-i bendinde *"Hükmün hukuka aykırı yöntemlerle elde edilen delile dayanması"* halinin, hukuka kesin aykırılık hali sayılacağı belirtilmiştir.[786]

3.4.2. Delil yasaklarının çeşitleri

Delil yasakları genel olarak, elde etme yasakları ve değerlendirme yasakları şeklinde iki grup halinde incelenmektedir. Bu bağlamda elde etme yasakları; ifade almada ve sorguda yasak usuller, aydınlatma yükümlülüğünün yerine getirilmemesi ve delil aracı yasakları şeklinde üç alt başlık altında değerlendirilmektedir.[787]

Yapılan bu ayrım çerçevesinde delil elde etme yasaklarının kapsamına girdiği tespit edilen bir delilin değerlendirilip değerlendirilemeyeceği hususunun mahkemenin takdirine bırakılması gerektiği ve sonuçta verilecek kararın "adil yargılanma hakkı"nı ihlal etmemesi gibi bir durumda bu delillerin hüküm kurulurken kullanılabileceği ileri sürülmüştür.[788] Buna karşılık delil elde etme yasaklarına aykırı bir şekilde elde edilen delillerin aynı zamanda delil değerlendirme yasağı kapsamına da girdiği ve CMK m. 217/2 uyarınca yüklenen suçun, *"hukuka uygun bir şekilde elde edilmiş…"* olan her türlü delille ispat edilebileceği kuralının, hukuka aykırı bir şekilde elde edilmiş olan delillerin, değerlendirmeye alınamayacağı şeklinde anlaşılması gerektiği ifade edilmiştir.[789] Bir adım öteye gidecek olursak yine CMK m. 217/2 uyarınca, herhangi bir hukuk kuralına aykırı olarak elde edilen delillerin, değerlendirme yasağı kapsamında ele alınması gerektiği, başka bir ifadeyle delilin elde edilmesi aşamasında yapılan bir hukuka aykırılığın, delilin değerlendirilememesi anlamına geldiği, bu bağlamda delillerin elde edilmesi yasağı ve değerlendirilmesi yasağı şeklinde bir ayrıma gidilmesinin, yerinde olmadığı ifade edilmiştir.[790]

---

[786] Yenisey ve Nuhoğlu, *Ceza Muhakemesi Hukuku,* 566; Özbek, Doğan ve Bacaksız, *Ceza Muhakemesi Hukuku,* 660.
[787] Özbek, Doğan ve Bacaksız, *Ceza Muhakemesi Hukuku,* 664- 668.
[788] Yenisey ve Nuhoğlu, *Ceza Muhakemesi Hukuku,* 567.
[789] Özbek, Doğan ve Bacaksız, *Ceza Muhakemesi Hukuku,* 667
[790] Öztürk, v.d., *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* 399; Tezcan, v.d., *Dijital Ceza Muhakemesi Hukuku,* 437.

3.4.3. Dijital deliller bakımından delilin yasaklılığı

Bireylerin bilişim sistemlerinde muhafaza altına almış oldukları kişisel verilerinin, CMK'nın m. 134'e aykırı bir biçimde elde edilmesi durumunda bu dijital verilerin yasak delil kapsamında değerlendirilmesi ve ceza yargılamasında kullanılamaması gerekmektedir. Bu durum elbette ilgili makamdan alınmış kararların uygulaması sırasında ortaya çıkacak usulsüz işlemler açısından da geçerli olacaktır. Nitekim Yargıtay Ceza Genel Kurulu vermiş olduğu bir kararda[791] *"kayıtların çözülerek metin hâline getirilmesi için sanık tarafından gösterilen rızanın yeterli olmayacağı"*nı ve *"mutlaka… CMK'nın 134. maddesine göre hâkim kararı alınması gerektiği"*ni ve *"hâkim kararı olmaksızın bilgisayar ve hard disklerde yapılan arama sonucunda elde edilen delillerin hukuka aykırı yöntemlerle elde edilen delil niteliğinde"* olacaklarını belirtmiştir.[792,793]

Tesadüfen elde edilen delillerin hukuka uygunluğu bakımından öncelikle başka bir suça ilişkin olan delil ile tesadüfen karşılaşıldığı sırada ondan önce gerçekleştirilmiş olan işlemlerin hukuka uygun olması gereklidir. Bu bağlamda eğer hukuka aykırı bir arama işlemi yapılırken bir başka suça ilişkin delil elde edilirse bu, tesadüfen elde edilen delil değil, hukuka aykırı delil olacaktır. Benzer şekilde arama kararında aranacak verinin sınırları aşılırsa yahut sınırlar bizzat çizilmezse gerçekleştirilecek bu arama bir keşif aramasına dönüşecektir. Böyle bir arama ise hukuka aykırı bir arama olarak kabul edilebilecektir.[794]

Adli ve Önleme Aramaları Yönetmeliği m. 10/a *"Yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmakla birlikte, karar veya yazılı emirde konu edilmeyen bir delil elde edilirse"* demek suretiyle CMK m. 138/1'de yer alan tesadüfen elde

---

[791] Yar. CGK., E. 2017/961, K. 2019/622, T. 22.10.2019 https://www.lexpera.com.tr/ictihat/Arama , son erişim: 07.04.2022.

[792] Aynı karar, bilişim sistemlerinde yapılan arama ve elkoyma işlemlerinin, hâkim kararı ile yapılsa dahi, yasada belirtilen usul işlemlerine uygun olarak yerine getirilmemesi durumunda da elde edilecek delillerin hukuka aykırı yöntemlerle elde edilmiş sayılacağını ve hükme esas alınmayacaklarını bu sebeple bu işlemlere dayanılarak yapılan diğer adli bilişim aşamalarının da geçersiz sayılacağını belirtmiştir. Başlar, "Adli Bilişim," 69- 70.

[793] Yine aynı kararda şüpheli tarafından rıza ile teslim edilmiş 85 adet film ve oyun CD/DVD'si muhafaza altına alınmış ve bu bağlamda bu materyallerin hukuka uygun yöntemlerle elde edildiği kabul edilmiştir. Kararın bu kısmına getirilen ve bizim de katıldığımız bir eleştiri uyarınca CD/DVD, SD Card, USB gibi çıkarılabilir veri depolama araçları, Adli ve Önleme Aramaları Yönetmeliği m. 17/3'te yer alan *"diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımlar"* kapsamına girmektedir ve bunlar hakkında gerçekleştirilecek arama, kopyalama ve elkoyma işlemlerinde de CMK m. 134 kuralları uygulanmalıdır. Bu sebeple söz konusu olayda elde edilen CD'ler hukuka uygun bir şekilde elde edilmemişlerdir. Bkz. Başlar, "Adli Bilişim," 70- 71.

[794] Değirmenci, *Sayısal Delil,* 440.

edilen delil kavramını genişlettiğini belirtmiştik. Arama konusu fiil ve eşyanın sınırlarının belirlenmesi, tesadüfen elde edilen delil kavramının da sınırlarını çizecektir. Bu sebeple kolluk kuvvetlerinin arama esnasında arama kararında gösterilen sınırların dışına çıkması ve şüphelendiği belli başka bir suça ilişkin verileri araştırması durumunda artık tesadüfen elde edilen delil değil, hukuka aykırı delilden bahsedilecektir.[795]

Ek olarak dijital delillerin hukuka aykırı elde bir şekilde elde edilmesi sonucu delillerin bütünlüğünün ve güvenilirliğinin ihlal edilmesi durumunda TCK'da yer alan bazı suç tipleri oluşabilecektir. Bu bağlamda ihlalin türüne 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) gibi suçlar gündeme gelebilecektir.[796]

[795] Değirmenci, *Sayısal Delil,* 448- 449.
[796] Afandak, "Ceza Muhakemesinde Dijital Deliller," 145- 146.

SONUÇ

Teknolojinin akıl almaz gelişimi gündelik hayatın her alanında kendini göstermektedir. Öyle ki günümüzde insanlar dünyanın öbür ucuna tek bir tık ile ulaşabilmekte ve yanlarında gigabaytlarca veri taşıyabilmektedir. Elbette bu gelişim suç dünyasına da yansımış ve günümüzde suç, artık küresel bir boyut kazanmaya başlamıştır. Teknolojinin hızına yetişmeye çalışan fakat bu konuda pek de başarılı olamayan hukuk sistemleri, dijitalleşen suçların aydınlatılması bakımından elzem olan dijital verilerin elde edilmesi amacıyla ve dijital verilerin delil değeri kazanabilmeleri amacıyla çeşitli kurallar düzenlemeye çalışmaktadırlar. Bu bağlamda ülkemizde de dijital delillerin hukuk sistemimize dahil edilmesinin temel kaynağını oluşturan Ceza Muhakemesi Kanunu m. 134 "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" tedbiri kaleme alınmıştır.

Çalışmamız, dijital deliller, dijital delillerin elde edilmeleri ve muhafazası ve son olarak dijital delillerin değerlendirilmesi ve ispat değerleri olmak üzere üç ana bölümden oluşmaktadır.

Birinci bölümde öncelikle kullanılacak kavram konusunda bir kargaşa olduğu tespit edilmiş ve bu bağlamda elektronik delil kavramı yerine dijital delil kavramının daha doğru bir kullanım olacağı sonucuna ulaşılmıştır. İkinci olarak, dijital delillerin doktrin ve uygulamada çoğunlukla bir delil türü olarak ele alındığı ve belirti deliller arasında değerlendirildiği, gerekçe olarak ise dijital delillerin hassas ve bozulmaya müsait bir yapıda oldukları ve dijital delil ile fail arasında bağlantı kurulmasının her zaman mümkün olmadığı belirtilmiştir. Buna karşılık dijital delillerin bir delil türü olmadığı fakat delilin bulunduğu yapıyı belirttiği tespit edilmiş ve bu bağlamda dijital delillerin diğer delil türlerinden bir farkı olmadığı, somut olayla bağlantısı çerçevesinde yerine göre doğrudan, yerine göre belirti delil niteliğinde olabileceği sonucuna ulaşılmıştır.

Üçüncü olarak, özellikle içtihat hukukunun geçerli olduğu ülkelerde, dijital delillerin mahkemelerin önüne daha sık gelmeleri sebebiyle, dijital delillerin kabul edilebilmeleri bakımından *"bilimsel delil"* standartının geliştirildiği tespit edilmiş ve dijital delillerin, genel olarak delil kurallarına tabi olmalarının yanında, bu kabul edilebilirlik kurallarına da tabi olmaları gerektiği belirtilmiştir.

İkinci bölümde öncelikle Türk hukukunda dijital delillerin nasıl elde edildikleri incelenmiş ve dijital delillerin elde edilmesinin teknik ve hukuki boyutlarının olduğu tespit edilmiştir. Bu bağlamda teknik boyutu oluşturan adli bilişim bilimi incelenmiş ve neticesinde ülkemizde adli bilişim yöntem ve tekniklerine dair herhangi bir düzenleme bulunmadığı tespit edilmiştir. Özellikle içtihat hukukunun geçerli olduğu ülkelerde dijital delillerle temas halinde bulunan adli bilişim uzmanlarının gerçekleştirmeleri gereken işlemlerin detaylı bir biçimde ve rehber şeklinde düzenlendiği gerçeği karşısında hukuk sistemimizde böyle bir düzenlemenin eksikliğinin uygulamada sorunlara neden olduğu sonucuna ulaşılmıştır.

Dijital delillerin elde edilmelerinin hukuki boyutunu oluşturan Ceza Muhakemesi Kanunu m. 134 incelendiğinde ise birçok açıdan eksikliklerin olduğu tespit edilmiştir. Madde kapsamının öncelikle bilgisayarlar, bilgisayar kütükleri ve programları şeklinde belli bazı dijital veri depolama veya oluşturma cihazlarından oluşması bir eksiklik olarak nitelendirilmiştir. Her ne kadar Yargıtay, madde kapsamını yorum faaliyeti çerçevesine genişletse de kullanılması gereken terimin *"bilişim sistemi"* olması gerektiği sonucuna ulaşılmıştır. Hatta buna da ek olarak, veriyi barındıran cihazdan ziyade, bizzat *veri*lerin odak noktasına alınması gerektiği ileri sürülmüş ve bu bağlamda bünyesinde *veri* barındıran tüm cihazların, CMK m. 134 kapsamında değerlendirilmesi gerektiği, böyle bir kabulün, insan hak ve özgürlükleri yönünde olumlu bir adım olacağı sonucuna ulaşılmıştır.

Sonrasında Türkiye'nin de taraf olduğu Siber Suçlar Sözleşmesi uyarınca öngörülen delil elde etme yöntemleri incelenmiş ve CMK m. 134'ün Siber Suçlar Sözleşmesi ile tam olarak uyumlu olmadığı tespit edilmiştir. Bu bağlamda özellikle, suç unsuru barındıran bilişim sistemlerinin içerisinde yer alan verilerin erişilemez hale getirilmesi yahut silinmesi tedbirinin getirilmesinin, uygulamada hali hazırda kanunsuz bir şekilde gerçekleştirilen bu işlemlere dayanak olması bakımından önem arz edeceği sonucuna ulaşılmıştır.

İkinci bölümde son olarak önleyici kolluk tedbirleri çerçevesinde elde edilen dijital delillerin durumunun ne olacağı tespit edilmeye çalışılmış ve bu bağlamda CMK 134'ün, genel arama ve elkoyma hükümlerinin özel bir halini oluşturması sebebiyle ilgili maddede aranan koşulların gerçekleşmediği bir durumda elde edilen materyallerin, başlangıç şüphesine dahi esas alınamayacağı sonucuna ulaşılmıştır.

Son olarak üçüncü bölümde dijital delillerin ispat güçleri belirlenmeye çalışılmış ve bu bağlamda birinci bölümde bahsi geçen kabul edilebilirlik kurallarının önemi vurgulanmıştır. Bu doğrultuda kabul edilebilirlik kurallarının, dijital delillerin hükme esas alınabilmeleri bakımından elzem olduğu ve dijital delillerin ispat güçleri bakımından belirleyici nitelikte oldukları sonucuna ulaşılmıştır.

İkinci olarak dijital delillerin güvenilirlikleri bakımından çeşitli değerlendirmelerde bulunulmuş ve uygulamada, güvenilirliğin tesisi bakımından gerçekleştirilen işlemler tespit edilmiştir. Bu doğrultuda söz konusu işlemlerin olumlu ve olumsuz yanları değerlendirilmiştir.

Üçüncü olarak dijital delillerin elde edilmesi bakımından gerçekleştirilen tedbirlerin, Avrupa İnsan Hakları Mahkemesi ve Anayasa Mahkemesi kararları ışığında nasıl ele alındığı incelenmiş ve AİHM'in konuya çoğunlukla "Özel ve aile hayatına saygı hakkı" kapsamında değerlendirdiği, AYM'nin ise "Mülkiyet hakkı", "Eğitim hakkı" ve yine benzer şekilde "Özel hayatın gizliliği ve korunması hakkı" kapsamında ele aldığı tespit edilmiştir.

Son olarak ise delil yasakları bakımından dijital delillerin yeri tespit edilmeye çalışılmıştır. Bu bağlamda öncelikle mevzuatımızda delil yasakları kavramı konusunda yine bir terminoloji kargaşası olduğu tespit edilmiştir. Devamında ise dijital delillerin elde edilmesi adına çıkarılan arama kararının, CMK m. 134'te yer alan koşulları barındırması gerektiği, yine bu deliller elde edilirken gerçekleştirilen adli bilişim prosedürlerinin, uluslararası standartlara uygun bir şekilde gerçekleştirilmesi gerektiği, aksi durumların delili yasaklı hale getireceği ve bu bağlamda hükme esas alınmasının önünde engel oluşturacağı sonucuna ulaşılmıştır.

Genel olarak bakıldığında yaşanan sıkıntıların çoğunlukla dijital delil kavramının bilinmemesine ve eksik mevzuat hükümlerine dayandığı sonucu ortaya çıkmıştır. Bu bağlamda kanımızca yapılması gereken, öncelikle yargılamanın tüm unsurları bakımından dijital delil farkındalığı yaratılmasıdır. Gerçekten de dijital delillerin yapısının ve özelliklerinin daha iyi bilinmesi, yargılama makamlarının dijital delillere yaklaşımını etkileyecektir. İkinci olarak gerçekleştirilmesi gereken, adli bilişim teknik ve yöntemlerinin, içtihat hukukunda olduğu gibi ayrıntılı bir şekilde bir rehber biçiminde düzenlenmesidir. Uygulamada adli bilişim uzmanları her ne kadar uluslararası standartlarda işlerini gerçekleştirmeye gayret gösterseler de söz konusu

alanda en azından bazı çerçeve hükümlerin bulunmayışı, deliller elde edilirken çeşitli kişisel hak ve özgürlüklere orantısız bir şekilde müdahale ile sonuçlanabilecektir. Son olarak dijital delillerin elde edilmesinin hukuki temelini oluşturan CMK m. 134 hükmünün yeniden düzenlenmesi gerekmektedir. Gerçekten de hüküm, hem kapsam hem de uygulanabilirlik bakımından oldukça eksiklik barındırmaktadır. Ek olarak insan haklarına müdahale konusunda getirilen bazı korumalar, adli bilişim prosedürleri düşünüldüğünde anlamsız kalabilmektedir. Bu bağlamda özellikle adli bilişim uzmanlarının da katılımıyla oluşturulacak bir çalışma ekibinin kaleminde çıkarılacak bir düzenlemenin, yaşanan sıkıntıları ve hukuka aykırılık doğuran halleri önemli ölçüde azaltacağını düşünmekteyiz.

KAYNAKÇA

Abel, Wiebke. "Agents, Trojans and Tags: The next Generation of Investigators.", *International Review of Law, Computers & Technology*, Vol. 23, Nos. 1-2 (March-July 2009): 99-108.

Afandak, Khalil. "Ceza Muhakemesinde Dijital Deliller." Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuk Anabilim Dalı, Ankara-2021.

Aksamitowska, Karolina. "Digital Evidence in Domestic Core International Crimes Prosecutions: Lessons Learned from Germany, Sweden, Finland and The Netherlands." *Journal of International Criminal Justice*, Volume 19, Issue 1 (March 2021): 189-211.

Almulhem, Ahmad and Issa Traore. "Experience with Engineering a Network Forensics System." *Lecture Notes in Computer Science*, vol. 3391 (2005): 62-71.

Ankara Barosu Uluslararası Hukuk Kurultayı: Bilişim ve Hukuk, Cilt- 2 (8 Ocak- 11 Ocak, 2008).

Arslan, Çetin. "Dijital Delil ve İletişimin Denetlenmesi," *Ceza Hukuku ve Kriminoloji Dergisi*, Cilt: 3, Sayı: 2 (2015): 253-266.

Arslan, Çetin. "Hukuk Öğretiminde Adlî Bilişim Türkiye Örneği Bağlamında Bir Değerlendirme." *2nd International Symposium on Digital Forensics and Security (ISDFS'14)*, Houston, TX, (2014): 73-76.

Aydın, Devrim. *Ceza Muhakemesinde Deliller*. Ankara: Yetkin Yayınları, 2014.

Ayözger, A. Çiğdem. *Kişisel Verilerin Korunması.* İstanbul: Beta Yayıncılık, 2016.

Baskın, Onur. *Türk Hukuku Bakımından Kişilik Hakkı Kapsamında Kişisel Verilerin Korunması.* Ankara: Seçkin Yayıncılık, 2021.

Başlar, Yusuf. "Adli Bilişim Sürecinde Karşılaşılan Sorunlar ve Çözüm Önerileri." *Türkiye Barolar Birliği Dergisi*, Cilt: 33, Sayı: 148 (2020): 47-76.

Başlar, Yusuf. "Elektronik Delil ve Ceza Yargılamasında Kabul Edilebilirliğine İlişkin Bir İnceleme." *Legal Hukuk Dergisi*, Cilt: 16, Sayı: 184 (2018): 1655-1688.

Başlar, Yusuf. "Elektronik Delilin Toplanması ve Muhafazası." *Hacettepe Hukuk Fakültesi Dergisi*, C.10 (2020): 77-107. s. 80.

Berghs, Sabine, Geoffrey Stewart Morrison and Caroline Goemans-Dorny. "Electronic Evidence: Challenges and Opportunities for Law Enforcement." *Law, Governance and Technology Series,* ed. Maria Angela Biasiotti, v.d., vol. 39, Cham, Switzerland: Springer, (2018): 75-124.

Biasiotti, Maria Angela. "Present and Future of the Exchange of Electronic Evidence in Europe." *Law, Governance and Technology Series*, ed. Maria Angela Biasiotti, v.d., vol. 39, Cham, Switzerland: Springer, (2018): 13-34.

Biasiotti, Maria Angela, v.d. "Introduction: Opportunities and Challenges for Electronic Evidence Handling and Exchanging Electronic Evidence Across Europe." *Law, Governance and Technology Series,* ed. Maria Angela Biasiotti, v.d., vol. 39, Cham, Switzerland: Springer, (2018): 3-12.

Börekçi, Çağrı. "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde; Arama, Kopyalama ve Elkoyma." Yayınlanmamış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, İstanbul 2020.

Buskirk, Eric Van and Vincent T. Liu. "Digital Evidence: Challenging the Presumption of Reliability." *Journal of Digital Forensic Practice,* vol. 1 (2006): 19-26.

Buzarovska Lazetik, Gordana and Olga Koshevaliska. "Digital Evidence in Criminal Procedures -A Comparative Approach-." *Balkan Social Science Review,* Vol. 2 (December 2013): 63-83.

Carrier, Brian and Eugene H. Spafford. "Getting Physical with the Digital Investigation Process." *International Journal of Digital Evidence,* Volume 2, Issue 2 (Fall 2003): 1-20.

Carrier, Brian. "Open Source Digital Forensics Tools: The Legal Argument." *Research Report* (October 2002) 1-11.

Casey, Eoghan. "Error, Uncertainty and Loss in Digital Evidence." *International Journal of Digital Evidence,* Vol. 1, Issue 2 (2002): 1-45.

Casey, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, Third Edition.* USA California: Academic Press, Published by Elsevier Inc., 2011.

Centel, Nur ve Hamide Zafer. *Ceza Muhakemesi Hukuku*. Yenilenmiş ve Gözden Geçirilmiş Yirminci Bası, İstanbul: Beta Yayıncılık, Eylül 2021.

Chaikin, David. "Network investigations of cyber attacks: the limits of digital evidence." *Crime Law Soc Change*, vol. 46 (2006): 239-256.

Chow, Kam Pui, v.d. "The Rules of Time on NTFS File System." *Second International Workshop on Systematic Approaches to Digital Forensic Engineering* (SADFE'07) (2007): 71-85.

Cirit, Muzaffer Enes. "İletişimin Tespiti, Dinlenmesi ve Kayda Alınması (CMK mad. 135)." Yayınlanmamış Yüksek Lisans Tezi, İstanbul Medipol Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuk Anabilim Dalı, İstanbul, 2018.

Clancy, Thomas K. "The Fourth Amendment Aspects of Computer Searches and Seizure: A Perspective and a Primer." *Mississippi Law Journal*, vol. 75 (2005): 193-286.

Ćosić, Jasmin and Miroslav Bača. "(Im)proving chain of custody and digital evidence integrity with time stamp." *The 33rd International Convention MIPRO* (2010): 1226-1230.

Ćosić, Jasmin, Zoran Ćosić and Miroslav Bača. "An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence." *Journal Of Information And Organizational Sciences*, vol. 35, no. 1 (2011): 1-13.

Çelikel, Serdar. *Kişisel Verilerin Korunması Hukuku Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri*. Ankara: Seçkin Yayıncılık, 2022.

Değirmenci, Olgun. "Adli Bilişimde Önceliklendirme (Triyaj) Yönteminin Ceza Muhakemesi Hukuku Açısından Değerlendirilmesi." *Bilişim Hukuku Dergisi*, C. 2, S. 1 (2020): 47-79.

Değirmenci, Olgun. "Bilgi Toplumunun Delil Türü: Sayısal Deliller ve Bilimselliği." *Terazi Hukuk Dergisi*, Cilt: 9, Sayı: 97 (Eylül 2014): 14-28.

Değirmenci, Olgun. "Yargılama Makamı İçin Şüphe, Müdafi İçin Savunma Nedeni: Adli Bilişimde Özet Değer (Hash Value) Kavramı ve Özet Değer Çakışmasının Ceza Muhakemesine Etkileri." *Terazi Hukuk Dergisi*, C. 13, S. 137 (2018): 120-126.

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

Dingledine, Roger, Nick Mathewson and Paul Syverson. "Tor: The Second-Generation Onion Router," *Naval Research Lab*, Washington DC (2004): 1-17.

Drewer Daniel and Jan Ellermann. "The Online Environment as a Challenge for Privacy and the Suppression of Crime." *Law, Governance and Technology Series*, ed. Maria Angela Biasiotti, v.d., vol. 39, Cham, Switzerland: Springer, (2018): 141-148.

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

Dülger, Murat Volkan. *Kişisel Verilerin Korunması Hukuku.* İstanbul: Hukuk Akademisi Yayınevi, 3. Baskı, 2020.

Emekci, Adem, Emin Kuğu ve Murtaza Temiztürk. "Adli Bilişim Ezberlerini Bozan Bir Düzlem: Bulut Bilişim." *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, Cilt. 2, No. 1 (2016): 8-14.

Epözdemir, Rezan. "Bilişim Sistemlerinde Arama ve Elkoyma Tedbirleri." *Terazi Hukuk Dergisi,* C. 13, S. 142 (2018): 88-98.

Erdem, Merve ve Gürkan Özocak. "Avrupa Konseyi Siber Suç Sözleşmesi ve Türk Hukukuna Etkileri." *4. UBHK Bildiriler Kitabı*, İzmir, (Mayıs 2016): 1-26. http://ozocak.com/Dosyalar/27669f.pdf , son erişim: 10.01.2022.

Favro, Philip J. "A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata." *Boston University Journal of Science & Technology Law*, Vol. 13, Issue 1 (2007): 1-25.

Forgó, Nikolaus, v.d. "Privacy Protection in Exchanging Electronic Evidence in Europe." *Law, Governance and Technology Series*, ed. Maria Angela Biasiotti, v.d., vol. 39, Cham, Switzerland: Springer, (2018): 255-288.

Gedik, Doğan. "Ceza Muhakemesinde Hakimin Delilleri Değerlendirme Serbestliği (Cmk M.217).", *D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN'a Armağan,* C.21, Özel S., (2019): 913-963.

Giordano, Scott M. "Electronic Evidence and the Law." *Information Systems Frontiers*, vol. 6:2 (2004): 161-174.

Göksoy, Resul. "Ceza muhakemesinde dijital delillerin elde edilmesi ve güvenilirliğinin sağlanması." Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, Kamu Hukuku Programı, İzmir 2017.

Grimm, Paul W., Daniel J. Capra and Joseph P. Gregory. "Authenticating Digital Evidence." *Baylor Law Review*, vol. 69, no. 1 (2017): 1-55.

Henkoğlu, Türkay. *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi*. İstanbul: Pusula Yayıncılık, 2. Baskı, 2014.

Horsman, Graeme. "ACPO principles for digital evidence: Time for an update?." *Forensic Science International: Reports*, Volume 2 (2020): 1-6.

Jones, Nigel, v.d. *Bilişim Suçları Eğitim Modülü, Türk Ceza Adalet Sisteminin Etkinliğinin Geliştirilmesi, Avrupa Birliği- Avrupa Konseyi Ortak Projesi*. Ankara: MATBAM Ajans & Reklam & Tanıtım, 2014.

Kaynakçıoğlu, Uğur. "Ceza Muhakemesinde Dijital Deliller." Yayınlanmamış Yüksek Lisans Tezi, Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Haziran 2015.

Kenneally, Erin E. "Gatekeeping out of the Box: Open Source Software as a Mechanism to Assess Reliability for Digital Evidence." *Virginia Journal of Law & Technology*, vol. 6, no. 3 (2001): 1-19.

Kerr, Orin S. "Digital Evidence And The New Criminal Procedure." *Columbia Law Review*, Vol. 105:279 (2005): 279-318.

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

Kızılyar, Murat. "Ceza Yargılamasında Dijital Verilerin Delil Değeri." *Adalet Dergisi*, Sayı: 50 (2014): 72-89.

Kilkelly, Ursula. "Özel Hayata ve Aile Hayatına Saygı Gösterilmesi Hakkı." *Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesinin Uygulanmasına İlişkin Kılavuz, İnsan Hakları El Kitapları No. 1*, Ankara (Nisan 2012): 1-117.

KVKK, Açık Rıza Rehberi, https://kvkk.gov.tr/yayinlar/A%C3%87IK%20RIZA.pdf , son erişim: 14.05.2022.

Leacock, Charles. “Search and Seizure of Digital Evidence in Criminal Proceedings.” *Digital Evidence and Electronic Signature Law Review*, vol. 5 (2008): 221-225.

Magherescu, Delia. “Enhancing Procedure of Using New Means of Technologies in Criminal Proceedings.” *IUS ET SCIENTIA*, Vol. 6, No. 1 (2020): 8-21.

Malin, Cameron H., Eoghan Casey and James M. Aquilina. *Malware Forensics: Investigating and Analyzing Malicious Code*. USA: Elsevier Inc., 2008.

Marcella, Albert J., and Frederic Guillossou. *Cyber Forensics: From Data to Digital Evidence*. Hoboken New Jersey: John Wiley & Sons, 2012.

Marshall, Angus M. *Digital Forensics: Digital Evidence in Criminal Investigation*. Chichester: Wiley-Blackwell, 2008.

McKemmish, Rodney. “What is forensic computing?.” *Australian Institute of Criminology Trends & issues in crime and criminal justice*, Vol. 118 (1999): 1-6.

Mifsud Bonnici, Jeanne Pia, Melania Tudorica and Joseph A. Cannataci. “The European Legal Framework on Electronic Evidence: Complex and in Need of Reform.” *Law, Governance and Technology* Series, ed. Maria Angela Biasiotti, v.d., vol. 39, Cham, Switzerland: Springer, (2018): 189-234.

Mills, David L. *Computer Network Time Synchronization; The Network Time Protocol.* USA: CRC Press, 1st edition, 2006.

Önel, Bünyamin ve Erdal Irmak. “Adli bilişim ve dijital delillerin windows işletim sistemi üzerinde incelenmesi.” *Politeknik Dergisi*, C. 24, S. 3 (2021): 1187-1196.

Önok, Murat. “Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği.” *Prof Dr. Nur Centel'e Armağan, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, C. 19, S. 2 (2013): 1229-1269.

Özbek, Mücahid. “Avrupa Siber Suçlar Sözleşmesinin Türk Ceza Hukukuna Etkileri.” *GSI,* (2015): 73-88. https://docplayer.biz.tr/4315393-Avrupa-siber-suclar-sozlesmesinin-turk-ceza-hukukuna-etkileri.html , son erişim: 15.04.2022.

Özbek, Veli Özer, Koray Doğan ve Pınar Bacaksız. *Ceza Muhakemesi Hukuku*. Ankara: Seçkin Yayıncılık, Genişletilmiş ve Güncellenmiş 14. Baskı, 2021.

Özel, Kadir Can. “Bir Koruma Tedbiri Olarak Arama.” *D.E.Ü. Hukuk Fakültesi Dergisi, Prof. Dr. Durmuş TEZCAN’a Armağan*, C.21, Özel S., (2019); 1217,1266.

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

Öztürk, Bahri, Elif Altınok Çalışkan ve Serkan Seyhan. *Kişisel Verilerin Korunması Hukuku Teorik ve Pratik Çalışma Kitabı*. Ankara: Seçkin Yayıncılık, Güncellenmiş 2. Baskı, 2022.

Öztürk, Bahri, v.d. *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku*. Ankara: Seçkin Yayınevi, Güncellenmiş 15. Baskı, 2021.

Öztürk, Mustafa İlker. “Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri.” Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Fizik İncelemeler ve Kriminalistik Programı, Ankara 2007.

Parker, Donn B. and Susan H. Nycum. “Computer Crime.” *Communications of the ACM*, Volume 27, Issue 4 (April 1984): 313-315.

Redmond, Neil, v.d. “Long Term Evolution Network Security and Real-Time Data Extraction.” *Cyber And Digital Forensic Investigations*, Springer International Publishing, New York, USA, (2020): 201-220.

Robinton, Lily R. “Courting Chaos: Conflicting Guidance from Courts Highlights and the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence.” *Yale Journal of Law and Technology*, vol. 12, no. 2 (2009-2010): 311-347.

Ryan, Daniel J. and Gal Shpantzer. “Legal aspects of digital forensics.” *Proceedings: Forensics Workshop*, (2002): 1-7.

Sammes, Tony and Brian Jenkinsen. *Forensic Computing: A Practitioners Guide*. London: Springer-Verlag, Second Edition, 2007.

Sarsikoğlu, Şenel. “Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı.” *Türkiye Adalet Akademisi Dergisi*, Yıl:6, Sayı:22 (Temmuz 2015): 427-454

Say, Kubilay. “Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi.” Disiplinlerarası Adli Tıp Anabilim Dalı Fizik İncelemeler ve Kriminalistik Bilim Dalı Yüksek Lisans Tezi, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, Ankara, 2006.

Sert, Şeyma. *Kişisel Verilerin Türk Ceza Kanunu Kapsamında Korunması*. Ankara: Seçkin Yayıncılık, 2019.

Schafer, Burkhard and Wiebke Abel. “The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822.”, *Scriptorium,* Volume 6, Issue 1 (April 2009): 106-123.

Schlepphorst, Sebastian, Kim-Kwang Raymond Choo and Nhien-An Le-Khac. “Digital Forensic Approaches for Cloud Service Models: A Survey.” *Cyber And Digital Forensic Investigations,* Springer International Publishing, New York, USA, (2020): 175-199.

Seger, Alexander. “e-Evidence and Access to Data in the Cloud Results of the Cloud Evidence Group of the Cybercrime Convention Committee.” *Law, Governance and Technology Series,* ed. Maria Angela Biasiotti, v.d., vol. 39, Cham, Switzerland: Springer, (2018): 35-42.

Signorato, Silvia. “Electronic Investigations in Italian Criminal Proceedings.” *Law Series of the Annals of the West University of Timisoara*, vol. 2014, no. 1 (2014): 9-22.

Swanson, Charles R., v.d. *Criminal Investigation*, 11th Edition. Boston: McGraw-Hill, 2012.

Şirikçi, Ahmet Serhat ve Nergis Cantürk. “Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi.” *Bilişim Teknolojileri Dergisi*, Cilt 5, Sayı 3 (2013): 29-34.

Tamma, Rohit, v.d. *Practical Mobile Forensics: Forensically investigate and analyze iOS, Android, and Windows 10 devices*. UK: Packt Publishing Ltd, Fourth Edition, 2020.

Taşdemir, Özgür. “Ceza Adaletini Dijitalleştirmek, Büyük Veri Vicdani Kanaate Karşı.” ed., Bilge Y, *Sağlık Alanında Büyük Veri Analitiği ve Uygulamaları*. 1. Baskı, Ankara: Türkiye Klinikleri (2021): 37-55.

Tezcan, Durmuş, v.d. *Dijital Ceza Muhakemesi Hukuku*. ed., Bahri Öztürk, Durmuş Tezcan, Mustafa Ruhan Erdem. Ankara: Seçkin Yayıncılık, Güncellenmiş ve Genişletilmiş 2. Baskı, 2022.

Toroslu, Nevzat ve Metin Feyzioğlu. *Ceza Muhakemesi Hukuku*. Ankara: Savaş Yayınevi, 18. Baskı, Ekim 2018.

TSE, Bulut Bilişim Güvenlik ve Kullanım Standardı, 5. (https://statik.tse.org.tr/upload/tr/dosya/icerikyonetimi/1202/17032015093613-3.pdf erişim tarihi: 01.12.2021).

Turner, Jenia I. "Managing Digital Discovery in Criminal Cases." *Journal of Criminal Law and Criminology*, vol. 109, no. 2 (2019): 237-311.

Turner, Philip. "Unification of Digital Evidence from Disparate Sources (Digital Evidence Bags)." *Digital Investigation*, vol. 2 (2005): 223-228.

U.S. Department of Justice Office of Justice Programs, "Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors", US National Institute of Justice, Washington, USA, January 2007, https://www.ojp.gov/pdffiles1/nij/211314.pdf son erişim: 03.12.2021.

U.S. Department of Justice Office of Justice Programs, "Electronic Crime Scene Investigation: A Guide for First Responders", US National Institute of Justice, Washington, USA, July 2001, https://www.ojp.gov/pdffiles1/nij/219941.pdf son erişim: 03.12.2021.

U.S. Department of Justice Office of Justice Programs, *"Electronic Crime Scene Investigation: A Guide for First Responders"*, US National Institute of Justice, Washington, USA, July 2001, https://www.ojp.gov/pdffiles1/nij/219941.pdf son erişim: 03.12.2021.

U.S. Department of Justice Office of Justice Programs, *"Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders"*, US National Institute of Justice, Washington, USA, November 2009, https://www.ojp.gov/pdffiles1/nij/227050.pdf son erişim: 03.12.2021.

Ünal, Osman Gazi. "Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma." Yayınlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, 2011.

Winick, Raphael. “Searches and Seizures of Computers and Computer Data.” *Harvard Journal of Law & Technology*, vol. 8, no. 1 (1994): 75-128.

Yalçın, Nursel ve Berker Kılıç. “ISO/IEC 27037, ISO/IEC 27041, ISO/IEC 27042 ve ISO/IEC 27043 Standartlarına Göre Sayısal Kanıtlar.” *4th International Symposium on Innovative Approaches in Engineering and Natural Sciences Proceedings*, ISAS (WINTER-2019): 1-6.

Yavuz, Mehmet. “Ceza Muhakemesinde İspat Sorunu.” *TAAD*, Yıl 3, S. 9 (20 Nisan 2012): 151-176.

Yenisey, Feridun ve Ayşe Nuhoğlu. *Ceza Muhakemesi Hukuku*. Ankara: Seçkin Yayıncılık, Güncellenmiş 9. Baskı, 2021.

Yılmaz, Furkan ve Hüseyin Çakır. “Karar Destek Sistemlerinin Mobil Cihaz Adli Bilişimi Süreçlerine Uygulanmasına Yönelik Bir Öneri Çalışması.” *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 7 (2021): 24-45.

Ylönen, Tatu, and Chris Lonvick. “The Secure Shell (SSH) Protocol Architecture.” *RFC* 4251 (2006): 1-30.

Zeigler, Ann D. and Ernesto F. Rojas. *Preserving Electronic Evidence for Trial*. USA: Elsevier Science, 2016.

Zuev, Sergey. “Traditional Values of Criminal Procedure in Terms of IT Development.” *Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT*, (2019): 419-425

TURNİTİN RAPORU

Ceza Muhakemesi Hukukunda Dijital Deliller

ORİJİNALLİK RAPORU

%18	%17	%6	%6
BENZERLİK ENDEKSİ	İNTERNET KAYNAKLARI	YAYINLAR	ÖĞRENCİ ÖDEVLERİ

BİRİNCİL KAYNAKLAR

1	nek.istanbul.edu.tr:4444 İnternet Kaynağı	%2
2	acikerisim.sakarya.edu.tr İnternet Kaynağı	%2
3	dergipark.org.tr İnternet Kaynağı	%1
4	acikbilim.yok.gov.tr İnternet Kaynağı	%1
5	tbbdergisi.barobirlik.org.tr İnternet Kaynağı	%1
6	yayin.taa.gov.tr İnternet Kaynağı	%1
7	Submitted to Istanbul Aydin University Öğrenci Ödevi	<%1
8	www.researchgate.net İnternet Kaynağı	<%1
9	www.ankarabarosu.org.tr İnternet Kaynağı	<%1

10	cdn.istanbul.edu.tr İnternet Kaynağı	<%1
11	kararlarbilgibankasi.anayasa.gov.tr İnternet Kaynağı	<%1
12	docplayer.biz.tr İnternet Kaynağı	<%1
13	dspace.gazi.edu.tr İnternet Kaynağı	<%1
14	Submitted to Dokuz Eylul Universitesi Öğrenci Ödevi	<%1
15	dergipark.gov.tr İnternet Kaynağı	<%1
16	www.mbkaya.com İnternet Kaynağı	<%1
17	acikerisim.iku.edu.tr İnternet Kaynağı	<%1
18	vs1.doczz.it İnternet Kaynağı	<%1
19	koray.peksayar.org İnternet Kaynağı	<%1
20	www.adalet.gov.tr İnternet Kaynağı	<%1
21	www.ozocak.com İnternet Kaynağı	<%1

22	9lib.net İnternet Kaynağı	<%1
23	mafiadoc.com İnternet Kaynağı	<%1
24	Submitted to Bahcesehir University Öğrenci Ödevi	<%1
25	acikarsiv.ankara.edu.tr İnternet Kaynağı	<%1
26	Submitted to Istanbul University Öğrenci Ödevi	<%1
27	forum.barandogan.av.tr İnternet Kaynağı	<%1
28	Submitted to Anadolu University Öğrenci Ödevi	<%1
29	earsiv.cankaya.edu.tr:8080 İnternet Kaynağı	<%1
30	DEĞİRMENCİ, Olgun. "SAYISAL (DİJİTAL) VERİLERDE YAKALAMA SONRASI ARAMA: AMERİKAN YÜKSEK MAHKEMESİNİN RILEY V. CALIFORNIA KARARI SONRASI AMERİKAN HUKUKUNUN DEĞERLENDİRİLMESİ", Türkiye Adalet Akademisi, 2016. Yayın	<%1
31	www.hukukihaber.net İnternet Kaynağı	<%1

32	hukukdergi.yasar.edu.tr İnternet Kaynağı	<%1
33	"Handling and Exchanging Electronic Evidence Across Europe", Springer Science and Business Media LLC, 2018 Yayın	<%1
34	dspace.yasar.edu.tr İnternet Kaynağı	<%1
35	hukuksokagi.com İnternet Kaynağı	<%1
36	www.tankado.com İnternet Kaynağı	<%1
37	www.cesimparlak.com.tr İnternet Kaynağı	<%1
38	www.lexpera.com.tr İnternet Kaynağı	<%1
39	adaylik.adalet.gov.tr İnternet Kaynağı	<%1
40	denetimakademisi.com İnternet Kaynağı	<%1
41	www.atilim.edu.tr İnternet Kaynağı	<%1
42	tez.sdu.edu.tr İnternet Kaynağı	<%1

43	www.openaccess.hacettepe.edu.tr:8080 İnternet Kaynağı	<%1
44	www.yayin.adalet.gov.tr İnternet Kaynağı	<%1
45	dspace.akdeniz.edu.tr İnternet Kaynağı	<%1
46	earsiv.anadolu.edu.tr İnternet Kaynağı	<%1
47	tuncayilcim.av.tr İnternet Kaynağı	<%1
48	ÖZEN, Muharrem and ÖZOCAK, Gürkan. "Adli bilişim, elektronik deliller ve bilgisayarlarda arama ve el koyma tedbirinin hukuki rejimi (CMK M. 134)", Ankara Barosu, 2015. Yayın	<%1
49	www.jurix.com.tr İnternet Kaynağı	<%1
50	www.scribd.com İnternet Kaynağı	<%1
51	www.ceza-bb.adalet.gov.tr İnternet Kaynağı	<%1
52	www.eralp.av.tr İnternet Kaynağı	<%1
53	acikerisim.selcuk.edu.tr:8080 İnternet Kaynağı	<%1

54	qdoc.tips İnternet Kaynağı	<%1
55	www.sgkrehberi.com İnternet Kaynağı	<%1
56	hdl.handle.net İnternet Kaynağı	<%1
57	docplayer.net İnternet Kaynağı	<%1
58	fordefence.com İnternet Kaynağı	<%1
59	pdffox.com İnternet Kaynağı	<%1
60	content.umgc.edu İnternet Kaynağı	<%1
61	openknowledge.worldbank.org İnternet Kaynağı	<%1
62	www.dfrws.org İnternet Kaynağı	<%1
63	Submitted to Istanbul Bilgi University Öğrenci Ödevi	<%1
64	Submitted to Yeditepe University Öğrenci Ödevi	<%1
65	afyonluoglu.org İnternet Kaynağı	<%1

66	m.bianet.org İnternet Kaynağı	<%1
67	www.acarindex.com İnternet Kaynağı	<%1
68	www.isarder.org İnternet Kaynağı	<%1
69	Submitted to Glyndwr University Öğrenci Ödevi	<%1
70	acikerisim.karatay.edu.tr:8080 İnternet Kaynağı	<%1
71	avukatlarasor.net İnternet Kaynağı	<%1
72	dosya.gsu.edu.tr İnternet Kaynağı	<%1
73	gezegen.linux.org.tr İnternet Kaynağı	<%1
74	www.ismailgurocak.av.tr İnternet Kaynağı	<%1
75	Submitted to De Montfort University Öğrenci Ödevi	<%1
76	Submitted to University of Edinburgh Öğrenci Ödevi	<%1
77	legesegitim.com İnternet Kaynağı	<%1

78	moam.info İnternet Kaynağı	<%1
79	LexisNexis Yayın	<%1
80	Submitted to Royal Holloway and Bedford New College Öğrenci Ödevi	<%1
81	Submitted to University of Northumbria at Newcastle Öğrenci Ödevi	<%1
82	acikerisimarsiv.selcuk.edu.tr:8080 İnternet Kaynağı	<%1
83	barandogan.av.tr İnternet Kaynağı	<%1
84	eprints.ugd.edu.mk İnternet Kaynağı	<%1
85	ijmra.us İnternet Kaynağı	<%1
86	archive.org İnternet Kaynağı	<%1
87	dl.acm.org İnternet Kaynağı	<%1
88	Submitted to Hasan Kalyoncu Üniversitesi Öğrenci Ödevi	<%1

89	KARTAL, Adem. "Teknik Araçlarla İzleme ve Elde Edilen Delillerin Değerlendirilmesi", Seçkin Yayıncılık A.Ş, 2014. Yayın	<%1
90	Submitted to Sheffield Hallam University Öğrenci Ödevi	<%1
91	Submitted to Suleyman Demirel University Öğrenci Ödevi	<%1
92	heinonline.org İnternet Kaynağı	<%1
93	onlinelibrary.wiley.com İnternet Kaynağı	<%1
94	www.haber7.com İnternet Kaynağı	<%1
95	www.tchd.org.tr İnternet Kaynağı	<%1
96	www.turkiyeklinikleri.com İnternet Kaynağı	<%1
97	Submitted to Police Academy Öğrenci Ödevi	<%1
98	Submitted to University of Westminster Öğrenci Ödevi	<%1
99	acikerisim.bahcesehir.edu.tr:8080 İnternet Kaynağı	<%1

100	iprgezgini.org İnternet Kaynağı	<%1
101	scholar.valpo.edu İnternet Kaynağı	<%1
102	seckin.com.tr İnternet Kaynağı	<%1
103	www.grafiati.com İnternet Kaynağı	<%1
104	www.jmir.org İnternet Kaynağı	<%1
105	www.seckin.com.tr İnternet Kaynağı	<%1
106	Submitted to Selçuk Üniversitesi Öğrenci Ödevi	<%1
107	academic.oup.com İnternet Kaynağı	<%1
108	cas.adalet.gov.tr İnternet Kaynağı	<%1
109	cbthukuk.net İnternet Kaynağı	<%1
110	doczz.net İnternet Kaynağı	<%1
111	librarycatalog.mef.edu.tr İnternet Kaynağı	<%1

112	www.dtic.mil İnternet Kaynağı	<%1
113	www.springerprofessional.de İnternet Kaynağı	<%1
114	www.ukm.uni-mb.si İnternet Kaynağı	<%1
115	yayin.adalet.gov.tr İnternet Kaynağı	<%1
116	BAŞLAR, Yusuf. "Ceza yargılamasında elektronik delillerin elde edilmesine ve korunmasına ilişkin usul hükümleri", Uyuşmazlık Mahkemesi, 2014. Yayın	<%1
117	Dergipark.Org.Tr İnternet Kaynağı	<%1
118	Submitted to Istanbul Medeniyet Ãniversitesi Öğrenci Ödevi	<%1
119	digitalcommons.law.yale.edu İnternet Kaynağı	<%1
120	www.aghukuk.org İnternet Kaynağı	<%1
121	www.diva-portal.org İnternet Kaynağı	<%1
122	www.hukukmarket.com İnternet Kaynağı	<%1

123	www.tcmevzuat.com İnternet Kaynağı	<%1
124	0-papers-ssrn-com.libweb.hofstra.edu İnternet Kaynağı	<%1
125	Ahmad Fekry Moussa. "Electronic evidence and its authenticity in forensic evidence", Egyptian Journal of Forensic Sciences, 2021 Yayın	<%1
126	Submitted to Ankara University Öğrenci Ödevi	<%1
127	Submitted to University of Dundee Öğrenci Ödevi	<%1
128	YAVUZ, Mehmet. "Ceza muhakemesinde ispat sorunu", TUBITAK, 2012. Yayın	<%1
129	archivaria.ca İnternet Kaynağı	<%1
130	humanities-digital-library.sas.ac.uk İnternet Kaynağı	<%1
131	orcid.org İnternet Kaynağı	<%1
132	www.btk.gov.tr İnternet Kaynağı	<%1
133	www.sgb.gov.tr İnternet Kaynağı	<%1

134	www.vergidunyasi.com.tr İnternet Kaynağı	<%1
135	BİRTEK, Fatih. "Acil yardım çağrıları ve kayıp (şahıs) başvuruları bakımından adres ve konum bilgisinin tespiti ve haberleşme trafik verilerinin kaydedilmesi", Türkiye Adalet Akademisi, 2013. Yayın	<%1
136	Hong Wu, Guan Zheng. "Electronic evidence in the blockchain era: New rules on authenticity and integrity", Computer Law & Security Review, 2020 Yayın	<%1
137	Nacar, Fatma Burcu(Olcay, Bülent). "Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları", Atılım Üniversitesi / Sosyal Bilimler Enstitüsü / Avrupa Birliği Anabilim Dalı, 2013. Yayın	<%1
138	academicrepository.khas.edu.tr İnternet Kaynağı	<%1
139	booklocker.com İnternet Kaynağı	<%1
140	cted.wa.gov İnternet Kaynağı	<%1
141	dag.un.org İnternet Kaynağı	<%1

142	eski.tbd.org.tr İnternet Kaynağı	<%1
143	vs1.doczz.cz İnternet Kaynağı	<%1
144	www.kisdi.re.kr İnternet Kaynağı	<%1
145	www.lifebursa.com İnternet Kaynağı	<%1
146	www.yasader.org İnternet Kaynağı	<%1
147	Ann D. Zeigler, Ernesto F. Rojas. "The Cloud and Other Complexities", Elsevier BV, 2016 Yayın	<%1
148	Submitted to Kocaeli Üniversitesi Öğrenci Ödevi	<%1
149	Submitted to Leeds Beckett University Öğrenci Ödevi	<%1
150	Xiaodong Lin. "Introductory Computer Forensics", Springer Science and Business Media LLC, 2018 Yayın	<%1
151	dergipark.Org.Tr İnternet Kaynağı	<%1
152	ethesis.nitrkl.ac.in İnternet Kaynağı	<%1

153	openaccess.bilgi.edu.tr:8080 İnternet Kaynağı	<%1
154	taad.taa.gov.tr İnternet Kaynağı	<%1
155	tr.wikidea.ru İnternet Kaynağı	<%1
156	www.foodelphi.com İnternet Kaynağı	<%1
157	www.hukukevi.net İnternet Kaynağı	<%1
158	www.isgeurasia.com İnternet Kaynağı	<%1
159	www.konsulhukuk.com İnternet Kaynağı	<%1
160	www.uyusmazlik.gov.tr İnternet Kaynağı	<%1
161	www.veyseldinler.com İnternet Kaynağı	<%1
162	ÖZTÜRK, Ceylan. "CEZA MUHAKEMESİ KANUNU KAPSAMINDA ŞÜPHELİNİN İFADE VE SORGU SIRASINDAKİ HAKLARI", İzmir Barosu, 2014. Yayın	<%1

163	"Ubiquitous Computing and the Internet of Things: Prerequisites for the Development of ICT", Springer Science and Business Media LLC, 2019 Yayın	<%1
164	Lecture Notes in Computer Science, 2005. Yayın	<%1
165	adanabarosu.org.tr İnternet Kaynağı	<%1
166	ayam.anayasa.gov.tr İnternet Kaynağı	<%1
167	aykutdurdagi.com İnternet Kaynağı	<%1
168	dspace.marmara.edu.tr İnternet Kaynağı	<%1
169	ejefuturo.hautetfort.com İnternet Kaynağı	<%1
170	faculty.kfupm.edu.sa İnternet Kaynağı	<%1
171	hfd.aydin.edu.tr İnternet Kaynağı	<%1
172	jurix.com.tr İnternet Kaynağı	<%1
173	kararlaryeni.anayasa.gov.tr İnternet Kaynağı	<%1

174	notoku.com İnternet Kaynağı	<%1
175	openaccess.maltepe.edu.tr İnternet Kaynağı	<%1
176	www.cijic.org İnternet Kaynağı	<%1
177	www.hsk.gov.tr İnternet Kaynağı	<%1
178	www.kolluk.net İnternet Kaynağı	<%1
179	Rafael Braga da Silva. "Updating the Authentication of Digital Evidence in the International Criminal Court", International Criminal Law Review, 2021 Yayın	<%1
180	SARSIKOĞLU, Şenel. "CEZA MUHAKEMESİNDE DELİL VE İSPAT HUKUKU AÇISINDAN ELEKTRONİK DELİL (E-DELİL) KAVRAMI", Türkiye Adalet Akademisi, 2015. Yayın	<%1
181	Shujun Li, Mandeep K. Dhami, Anthony T.S. Ho. "Standards and Best Practices in Digital and Multimedia Forensics", Wiley, 2015 Yayın	<%1
182	Submitted to University of Surrey Öğrenci Ödevi	<%1

183	malisozluk.istanbulsmmmodasi.org.tr İnternet Kaynağı	<%1
184	ssd.eff.org İnternet Kaynağı	<%1
185	www.mahkemeler.net İnternet Kaynağı	<%1
186	www.ncdsv.org İnternet Kaynağı	<%1
187	www.selcukmedj.org İnternet Kaynağı	<%1
188	www5.tbmm.gov.tr İnternet Kaynağı	<%1
189	"Advances in Digital Forensics V", Springer Science and Business Media LLC, 2009 Yayın	<%1
190	Data Protection in a Profiled World, 2010. Yayın	<%1
191	GÜLTEKİN, Özkan. "Olay yeri incelemesindekarşılaşılan sorunlar ve çözüm önerileri", TUBITAK, 2011. Yayın	<%1
192	hukuk.deu.edu.tr İnternet Kaynağı	<%1
193	researchr.org İnternet Kaynağı	<%1

194	www.j-humansciences.com İnternet Kaynağı	<%1
195	www.kararara.com İnternet Kaynağı	<%1
196	yetkin.com.tr İnternet Kaynağı	<%1
197	İNCİ, Z Özen. "CEZA MUHAKEMESİ HUKUKUNDA CUMHURİYET SAVCISI VE SULH CEZA HÂKİMİ (SORUŞTURMA MAKAMLARI) ARASINDAKİ GRİ ALAN: GECİKMESİNDE SAKINCA BULUNAN HAL KAVRAMI VE SORUŞTURMA EVRESİNDE TEMEL HAKLARA MÜDAHALE SORUNU", Ankara Üniversitesi Hukuk Fakültesi, 2016. Yayın	<%1
198	Submitted to Mehmet Akif Ersoy Aniversitesi Öğrenci Ödevi	<%1
199	Submitted to The Scientific & Technological Research Council of Turkey (TUBITAK) Öğrenci Ödevi	<%1
200	Submitted to University of Bradford Öğrenci Ödevi	<%1
201	auosozluk.anadolu.edu.tr İnternet Kaynağı	<%1
202	services.foi.hr İnternet Kaynağı	<%1

203	wiki.pisilinux.org İnternet Kaynağı	<%1
204	ARSLAN, Çetin. "Dijital Delil ve İletişimin Denetlenmesi", İstanbul Üniversitesi Hukuk Fakültesi, 2015. Yayın	<%1
205	www.law.ed.ac.uk İnternet Kaynağı	<%1

ÖZGEÇMİŞ

Adı ve Soyadı: Zeynel Abidin AYHAN

Öğrenim Durumu:

Derece	**Alan**	**Üniversite**	**Yıl**
Lisans (Yüksek Şeref Öğrencisi)	HUKUK	ATILIM ÜNİVERSİTESİ	2015-2019
Yüksek Lisans	KAMU HUKUKU A.B.D.	ATILIM ÜNİVERSİTESİ	2019-2022

Yabancı Diller: İNGİLİZCE

Tarih: 02.06.2022