

UZMAN GÖRÜŞÜ

(BİLİMSEL MÜTALAA)

DOSYA NO : .../...

DAVACI : Örnek Davacı 1

DAVACI VEKİLİ : Av. Örnek Vekil 1

DAVALI : Örnek Davalı 1

DAVALI VEKİLİ : Av. Örnek Vekil 2 – Av. Örnek Vekil 3

TALEPTE BULUNAN : Av. Örnek Vekil 3

UZMANLARDAN İSTENEN : İstanbul Aile Mahkemesi'nin .../... Esas sayılı dosyası kapsamında görülmekte olan boşanma davasında; dosyaya sunulan ve taraflar arasındaki uyuşmazlığa dayanak gösterilen dijital verilerin, WhatsApp yazışmaları, video görüntüleri, kesitler, ilişkin ekran çıktıları

- Teknik olarak doğrulanabilir olup olmadığı,
- Veri bütünlüğü ve güvenilirlik düzeyi,
- Elde edilme yöntemi itibarıyla adli bilişim standartlarına uygunluğu,
- Manipülasyona açık olup olmadığı ve değiştirilebilirlik riski,
- Orijinal veri niteliği taşıyıp taşımadığı,
- Kaynağının teknik olarak tespit edilip edilemeyeceği
- Hususlarının değerlendirilmesi ile;
- Bu tür dijital verilerin tek başına güvenilir ve kesin delil niteliği taşıyıp taşımadığının teknik ve hukuki açıdan delil niteliklerinin incelenmesi talep edilmiştir.

1. DİJİTAL DELİLLERDE TEMEL İLKELER

Dijital deliller, klasik fiziki delillerden farklı olarak son derece kolay çoğaltılabilen, taşınabilen, dönüştürülebilin ve gerektiğinde teknik araçlarla fark edilmesi güç biçimde değiştirilebilen veri türleridir. Bu nedenle bir dijital verinin hukuki ve teknik anlamda delil değeri taşıyabilmesi, yalnızca içeriğinin “iddiayı destekliyor görünmesine” değil; o verinin orijinalliğinin, bütünlüğünün, kaynağının, elde edilme yönteminin ve inceleme sürecinin denetlenebilir şekilde ortaya konulmasına bağlıdır. Başka bir ifadeyle, dijital delilde esas mesele yalnızca “ne görüldüğü” değil, “o görüntünün veya verinin hangi teknik süreçten geçerek dosyaya geldiği”dir. Bu nedenle adli bilişim disiplininde dijital delilin değerlendirilmesi rastgele kanaatle değil belirli temel ilkeler üzerinden yapılır. Türkiye

ANONİMLEŞTİRME NOTU: Bu doküman, FORM Uzman Görüşü Merkezi'nin kamuya açık tanıtım örneğidir. 6698 sayılı KVKK ve müvekkil gizliliği ilkeleri gereğince taraf isimleri, vekil isimleri, dosya numarası ve mahkeme birimi temsili değerlerle değiştirilmiştir. Teknik ve hukuki değerlendirme bölümleri raporun aslındaki içerikle birebir aynıdır.

amacıyla dijital delillerin elde edilmesi, işlenmesi, analizi ve raporlanmasıyla ilgili bir alan olarak tanımlamakta; uluslararası standartlar da aynı biçimde delilin yaşam döngüsü boyunca bütünlük ve izlenebilirliğin korunmasını merkezî ilke olarak kabul etmektedir.

Bu çerçevede dijital deliller bakımından en temel üç ilke; bütünlük, doğrulanabilirlik ve değiştirilemezliktir. Ancak uygulamada bunlara ek olarak izlenebilirlik, tekrarlanabilirlik, usule uygun toplama, uygun muhafaza ve şeffaf raporlama da aynı derecede önem taşımaktadır. Bir çok ulusal ve uluslararası kaynakta dijital delilin ilk tespit anından soruşturma veya inceleme sonuna kadar veri bütünlüğünün korunmasının zorunlu olduğu, veri yaşam döngüsünün her aşamasında tutarlı veri yönetimi ve belgelendirmenin esas olduğu açıkça belirtilmektedir. Aynı şekilde veri bütünlüğünü tehdit eden başlıca unsurlar arasında insan hatası, güvenlik ihlalleri ve yetersiz dokümantasyon gösterilmiştir.

1.1. Bütünlük İlkesi

Bütünlük, dijital verinin elde edildiği andan raporlandığı ana kadar içeriğinde yetkisiz, kontrolsüz veya açıklanamayan herhangi bir değişiklik meydana gelmediğinin gösterilebilmesini ifade eder. Bir dijital delilin bütünlüğü korunmadan yapılan değerlendirme, görünüşte ikna edici olsa bile teknik anlamda kırılıktır. Çünkü dijital veri, doğası gereği bir kopyalama, taşıma, açma, dışa aktarma, ekran görüntüsü alma veya üçüncü kişiye iletme işlemi sırasında dahi değişikliğe uğrayabilir. Bu değişiklik bazen delilin özünü bozmasa da, kimi zaman da verinin anlamını tamamen dönüştürebilir.

Örneğin bir mesajlaşma uygulamasındaki birkaç satırlık yazışmanın ekran görüntüsü alınmış olsun. Bu görüntüde yalnızca belli mesajların görünmesi, önceki ve sonraki konuşma akışının, mesajın hangi cihaza ait olduğunun, gerçekten gönderilip gönderilmediğinin, silinip silinmediğinin veya düzenlenip düzenlenmediğinin tespitine yetmez. Dahası, ekran görüntüsü alındıktan sonra görsel düzenleme araçları ile saat, kişi adı, profil resmi, tarih veya içerik üzerinde değişiklik yapılması mümkündür. Bu durumda dosyaya sunulan görüntü, ilk bakışta “aynı” görünse bile teknik olarak artık ilk verinin güvenli bir yansıması olmayabilir. İşte bütünlük ilkesi tam da bu nedenle, dijital delilin içeriğinden önce onun korunmuş olmasını arar. Genel Kabul edilen bilimsel görüş veri bütünlüğünü doğruluk, tutarlılık ve güvenilirlik temellerine dayandırmakta; toplama ve muhafaza sürecindeki uygun tedbirlerin, dijital delilin savunulabilirliği bakımından zorunlu olduğunu vurgulamaktadır.

Adli bilişim pratiğinde bütünlük çoğunlukla hash değeri ile desteklenir. Hash; bir dosyanın veya imajın matematiksel özeti niteliğinde olup, verideki en küçük değişiklikte dahi farklı sonuç üretir. Bu nedenle hash, “delilin aynı delil olup olmadığı” sorusuna teknik yanıt veren en temel araçlardan biridir. Bir cep telefonundan adli imaj alındığında elde edilen kopyanın hash değeri kaydedilir; daha sonra bu kopya üzerinde yapılan incelemelerde aynı hash değerinin korunup korunmadığı kontrol edilir. Böylece hem ilk elde edilen veri hem de sonradan incelenen veri arasında süreklilik sağlanır. Hash alınmamış veya hash ile doğrulanmamış bir dijital verinin bütünlüğü hakkında kesin kanaat kurmak güçleşir.

1.2. Doğrulanabilirlik İlkesi

Doğrulanabilirlik, sunulan dijital verinin gerçekten iddia edilen kaynaktan gelip gelmediğinin ve içerdiği bilginin orijinal sistem kayıtlarıyla teyit edilip edilemediğinin ortaya konulabilmesidir. Dijital delilin değeri yalnızca içerik benzerliğinden değil, kaynak bağının teknik olarak kurulabilmesinden doğar. Bu nedenle doğrulanabilirlik; cihaz,

uygulama, veri tabanı, sistem kayıtları, zaman damgaları, kullanıcı oturumu, dosya yapısı, mesaj kimlikleri, meta veriler ve gerekiyorsa ağ/sunucu ilişkileri üzerinden incelenir.

Somut bir örnek vermek gerekirse, bir WhatsApp ekran görüntüsünde “karşı tarafın belirli bir ifadeyi kullandığı” görülüyor olabilir. Ancak bu görüntü tek başına şu sorulara cevap vermez: Bu mesaj gerçekten o kişiye ait cihazdan mı gönderildi? Mesaj gönderildiği anda uygulama hesabı kimin kontrolündeydi? Görüntü orijinal sohbet ekranından mı alındı, yoksa sonradan oluşturulmuş bir benzer arayüz mü kullanıldı? Mesaj silinmiş miydi? Cihaz eş zamanlı başka biri tarafından erişilebilir durumda mıydı? Görüntüde görülen zaman bilgisi cihaz saat ayarından mı, sunucu verisinden mi türemektedir? Bu soruların cevabı yalnızca ekran görüntüsünden çıkartılamaz. Doğrulanabilirlik ancak cihazın adli incelemesi, veri tabanı kalıntıları, yedekler, meta veriler ve gerektiğinde ek teknik kayıtlarla desteklendiğinde güç kazanır.

Güncel uluslararası yaklaşım da bu yöndedir. ISO 21043 standardının 2025’te yayımlanan bölümleri, adli süreçte kullanılan terimlerin standartlaştırılması ve gözlemlerden mahkemeye sunulacak görüşe geçişte yorumlama sürecinin şeffaf, denetlenebilir ve alternatif açıklamaları dikkate alan bir yapıda kurulması gerektiğini göstermektedir.

1.3. Değiştirilemezlik İlkesi

Değiştirilemezlik ilkesi, dijital delilin sonradan müdahaleye açık olup olmadığının ve inceleme süreci boyunca orijinal biçiminin korunup korunmadığının değerlendirilmesini ifade eder. Elbette dijital dünyada mutlak anlamda “değiştirilemez” veriden söz etmek teknik olarak her zaman mümkün değildir; ancak adli bilişim bakımından aranan şey, verinin sonradan değiştirilebilme ihtimalinin makul ölçüde bertaraf edilmesi ve bu hususun teknik usullerle gösterilmesidir. Bu nedenle write-blocker kullanılması, adli imaj alınması, hash değerlerinin kaydedilmesi, erişim kayıtlarının tutulması ve inceleme kopyası üzerinde çalışılması gibi yöntemler geliştirilmiştir.

Bu ilke özellikle cep telefonu ve mesajlaşma uygulamaları bakımından kritik önemdedir. Çünkü mobil cihazlar, sürekli çalışan, senkronizasyon yapan, bulut yedekleriyle etkileşen ve kullanıcı müdahalesine açık sistemlerdir. Bir mesaj uygulamasında sohbet silinmesi, düzenlenmesi, arşivlenmesi, dışa aktarılması, farklı cihazlara yansıtılması veya bildirim ekranı üzerinden görünmesi gibi birçok teknik senaryo mevcuttur. Bu nedenle yalnızca görüntüye bakılarak “bu veri değişmemiştir” denilemez.

1.4. Zincirleme Muhafaza ve İzlenebilirlik

Dijital delilin güvenilirliği yalnızca verinin kendisine değil, verinin kim tarafından, ne zaman, hangi cihazdan, hangi yöntemle alındığına ve sonrasında kimlerin eriştiğine de bağlıdır. Buna uygulamada “chain of custody” yani zincirleme muhafaza denilmektedir. Zincirleme muhafaza eksikse, veri teknik olarak doğru görünse bile delilin güvenilirliği tartışmalı hale gelir. Örneğin bir telefon bir süre taraflardan birinin kontrolünde kaldıysa, ekran kilidi bilgisi eşler arasında biliniyorsa, uygulama açık bırakılmışsa veya veri üçüncü

kişilere iletilmişse, sunulan görüntünün ne zaman ve hangi koşullarda elde edildiği belirsizleşir. Bu belirsizlik delilin değerini doğrudan etkiler.

2. EKRAN GÖRÜNTÜLERİNİN SINIRLILIKLARI

Ekran görüntüleri (screenshot), bir dijital cihazın ekranında belirli bir anda görüntülenen verinin piksel tabanlı statik bir kopyası olup, bu veri yapısı itibarıyla orijinal dijital veriden farklı bir niteliğe sahiptir. Bu nedenle ekran görüntüleri, teknik açıdan birincil veri (primary evidence) değil, yalnızca ikincil görsel temsil (secondary representation) olarak kabul edilmektedir.

2.1. Orijinal Veri Niteliği Taşımaması

Mesajlaşma uygulamalarında (WhatsApp, Telegram vb.) gerçek veri; Cihaz içerisindeki veritabanlarında (örneğin WhatsApp için msgstore.db), Uygulama log kayıtlarında, Sunucu tarafı zaman damgalarında (timestamp), Mesaj ID ve oturum kayıtlarında saklanmaktadır.

Ekran görüntüsü ise bu kompleks veri yapısının yalnızca kullanıcı arayüzünde görülen kısmının görsel çıktısıdır. Bu nedenle:

- Veri kaynağına doğrudan erişim sağlamaz
- Teknik doğrulama için gerekli parametreleri içermez
- Delilin kaynağı ile bağ kurulamamasına neden olur
- Bu yönüyle ekran görüntüsü, asıl verinin yerine geçebilecek nitelikte değildir.

2.2. Manipülasyona Açıklık (Değiştirilebilirlik Problemi)

Ekran görüntülerinin en önemli teknik zafiyeti, kolaylıkla değiştirilebilir olmalarıdır.

Günümüzde:

Basit mobil uygulamalar

Gelişmiş grafik yazılımları (Photoshop vb.)

Yapay zeka tabanlı görsel düzenleme araçları kullanılarak aşağıdaki değişiklikler kolaylıkla yapılabilmektedir:

Mesaj içeriklerinin değiştirilmesi

Yeni mesaj eklenmesi veya silinmesi

Tarih ve saat bilgilerinin yeniden düzenlenmesi

Kişi isimlerinin ve profil fotoğraflarının değiştirilmesi

Mesaj sıralamasının yeniden oluşturulması

Özellikle son yıllarda gelişen generatif yapay zeka araçları, gerçekçi sahte ekran görüntüleri üretmeyi teknik olarak son derece kolay hale getirmiştir.



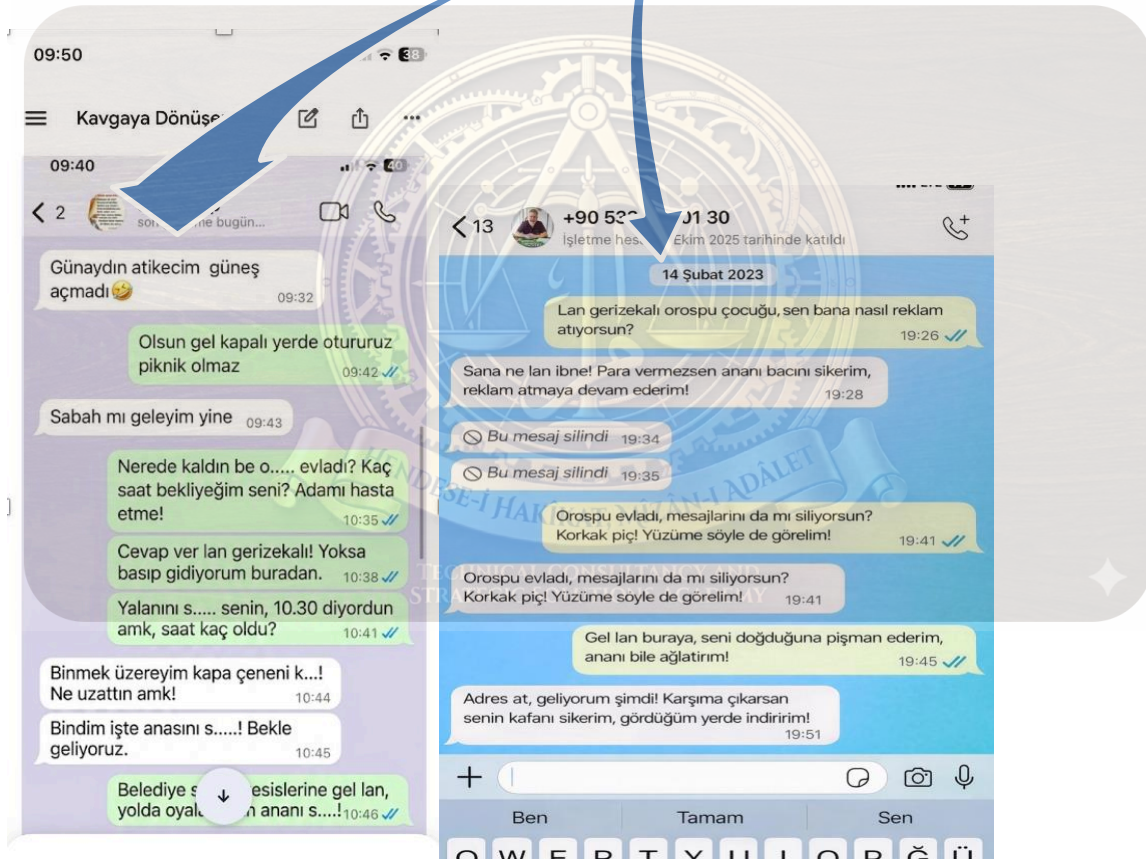
- tespit edilemez
Mesajın hangi cihazdan gönderildiği 2.3. Metadata (Üst Veri) Eksikliği
Dijital delillerin doğrulanabilirliği açısından en kritik unsurlardan biri metadata (üst veri) bilgileridir.
Bir mesajlaşma verisinin doğrulanabilmesi için aşağıdaki teknik bilgiler gereklidir:
- Mesaj ID (benzersiz kimlik)
- Gönderim ve teslim zaman damgaları
- Gönderici/alıcı cihaz bilgileri
- IP ve oturum verileri
- Sunucu kayıtları
Ekran görüntülerinde bu verilerin hiçbiri bulunmaz.
Bu durum şu sonuçları doğurur:
- Mesajın gerçekten gönderilip gönderilmediği belirlenemez
- Zaman bilgisinin doğruluğu teyit edilemez
- Mesajın bütünlüğü kontrol edilemez
Dolayısıyla ekran görüntüsü, teknik olarak doğrulanabilir bir veri seti sunmaz.

KONU İLE ALAKALI DENEYSEL ÇALIŞMALAR

5271 Sayılı Ceza Muhakemesi Kanunu (CMK), Ceza Yargılaması Sırasında Taraflara Bilirkişi Seçme Ve Bilirkişilerin Uzmanlık Görüşünden Yararlanabilme İmkânı Sunmaktadır. Nitekim Anılan Kanun'un 67/6'ncı Maddesinde² "Cumhuriyet Savcısı, Katılan, Vekili, Şüpheli Veya Sanık, Müdafî Veya Kanuni Temsilci, Yargılama Konusu Olayla İlgili Olarak Bilirkişi Raporunun Hazırlanmasında Değerlendirilmek Üzere Ya Da Bilirkişi Raporu Hakkında, Uzmanından Bilimsel Mütalaa Alabilirler." Hükmü Yer

Almaktadır. Tesis Edilen Bu Hüküm, Ceza Yargısındaki Bilimsel Mütalaa Müessesesinin Meşruiyet Kaynağı Mahiyetinde Olduğu CMK'ya Göre, Bilimsel Düşünce Ve Yorumlarını Uzman Görüşü Şeklinde Sunan Uzmanlar Da Esasen Bilirkişi Sıfatını Haiz olacakları Nitekim Kunter Ve Diğerleri (2008) Bilimsel Mütalaa Yoluyla Uzmanlık Görüşüne Başvurulanların Da Görev Ve Yetkileri Bakımından Bilirkişilerle Aynı Durumda Olduğunu İfade Etmektedir. Tayin Edilen Bilirkişilerden Ayrılan Nitelikleri Dikkate Alındığında, Bu Kişilere, Bilirkişi Yerine “Uzman” Denilmektedir.

- Mütalâ Düzenlenirken Konu İle İlgili Mevcut Bilimsel Kaynaklar Yeniden Gözden Geçirildiği Gibi Dosya/Analize Gönderilen Belge İçeriğinin Gerektirmesi Halinde Konu İle Alakalı Derinleşel Çalışmalar Dahi Uzmanca Tasarlanmakta Olduğu .



yukarıda yer alan Resimler Sahte Whatsap Görüntüleri olarak yapılmış yapay zeka ve el ürünleridir.dosya içeriğindeki belgeler değildir.
üstelik sahte mesajların aralarında gerçekte olduğu gibi silinme kayıtlarında yer almaktadır.

2.4. Hash Doğrulaması Yapılamaması

Adli bilişim incelemelerinde veri bütünlüğünün sağlanması için hash algoritmaları (MD5, SHA-1, SHA-256 vb.) kullanılmaktadır.

Hash değeri:

- Verinin dijital parmak izi niteliğindedir
- En küçük değişiklikte dahi tamamen farklı sonuç üretir
- Delilin değişmediğini ispat eder
Ancak ekran görüntüsü:
- Orijinal veri olmadığı için hash karşılaştırmasına tabi tutulamaz
- Başka bir kaynakla eşleştirilemez
- Bütünlük doğrulaması yapılamaz
Bu nedenle ekran görüntüleri, adli bilişim standartlarına göre doğrulanabilir delil kategorisine girmez.

2.5. Zincirleme Delil Güvenliğinin Sağlanamaması

Dijital delillerde en önemli unsurlardan biri de delil zinciridir.

Bu kavram:

- Delilin kim tarafından elde edildiği
- Hangi ortamda saklandığı
- Kimlerin eriştiği
- Ne şekilde mahkemeye sunulduğu
gibi süreçlerin tamamının kayıt altına alınmasını ifade eder.
Ekran görüntülerinde:
- Delilin elde edilme yöntemi belirsizdir
- Orijinal kaynağa erişim yoktur
- Üçüncü kişiler tarafından değiştirilip değiştirilmediği bilinemez
Bu nedenle delil zinciri kırılmış kabul edilir.

3. AYNI KONUTTA YAŞAYAN BİREYLERDE ERİŞİM GERÇEĞİ

Aynı konut içerisinde yaşayan bireyler arasında dijital cihazlara erişim imkânı, teknik ve fiili koşullar gereği önemli ölçüde artmaktadır. Bu durum, özellikle aile hukuku uyuşmazlıklarında sunulan dijital verilerin kaynağı, elde edilme yöntemi ve güvenilirliği bakımından ayrıca değerlendirilmesi gereken kritik bir husustur.

3.1. Fiziksel Erişimin Doğal ve Sürekli Olması

Aynı yaşam alanını paylaşan bireyler;
Günlük yaşam içerisinde aynı ortamda bulunmakta,
Cihazları çoğu zaman ortak alanlarda bırakmakta,
Birbirlerinin kişisel eşyalarına fiilen erişim sağlayabilmektedir.

Bu kapsamda cep telefonları;

Masa, sehpa, yatak başı gibi alanlarda bırakılabilmekte,

Şarjda veya kullanım dışı halde erişilebilir konumda bulunabilmektedir.

Bu tür fiziksel erişim, dışarıdan üçüncü kişilere kıyasla çok daha kolay ve süreklilik arz eden bir durumdur.

3.2. Cihaz Güvenliğinin Pratikte Zayıf Olması

Her ne kadar mobil cihazlarda şifre, PIN, parmak izi ve yüz tanıma gibi güvenlik önlemleri bulunsada, günlük kullanım alışkanlıkları bu önlemlerin etkinliğini zayıflatabilmektedir.

Uygulamada sıklıkla karşılaşılan durumlar:

- Cihazların kilitsiz şekilde bırakılması
 - Şifrelerin eşler arasında paylaşılması
 - Basit ve tahmin edilebilir şifrelerin kullanılması (1234, doğum tarihi vb.)
 - Biyometrik kilidin aktif olmaması veya kolay aşılabilir olması
 - Bildirim ekranından mesaj içeriklerinin görüntülenebilmesi
- Bu nedenlerle cihaz güvenliği teorik olarak mevcut olsa dahi, pratikte erişim engeli çoğu zaman fiilen ortadan kalkmaktadır.

3.3. Uygulama Oturumlarının Açık Kalması

Mesajlaşma uygulamaları (WhatsApp vb.) genellikle kullanıcı deneyimini kolaylaştırmak amacıyla oturumu sürekli açık tutacak şekilde çalışmaktadır.

Bu durum şu sonuçları doğurmaktadır:

Uygulama tekrar şifre sormadan doğrudan açılabilir

Mesaj içerikleri anlık olarak görüntülenebilir

Sohbet geçmişine erişim sağlanabilir

İstenirse yeni mesaj gönderilebilir

Özellikle:

Telefonun kilitsiz bırakılması

Uygulamanın arka planda açık olması gibi durumlarda, başka bir kişi tarafından uygulamaya erişim teknik olarak son derece kolay hale gelmektedir.

3.4. Yetkisiz Kullanım ve Veri Oluşturma İhtimali

Aynı konutta yaşayan bireylerin cihazlara erişebilmesi, yalnızca mevcut verilerin görüntülenmesi ile sınırlı olmayıp, aynı zamanda yeni veri oluşturma veya mevcut veriyi değiştirme ihtimalini de beraberinde getirir.

Bu kapsamda teknik olarak mümkün olan işlemler:

- Mevcut mesajların silinmesi
- Yeni mesaj gönderilmesi
- Sohbet içeriklerinin değiştirilmesi
- Ekran görüntüsü oluşturulması
- Mesajların farklı bağlamda sunulması

Dolayısıyla bir verinin varlığı, o verinin mutlaka cihaz sahibine ait olduğu anlamına gelmemektedir.

3.5. Kullanıcı Kimliği ile Fiili Kullanıcı Ayrımı

Adli bilişimde önemli bir ayrım bulunmaktadır:

Cihaz sahibi ile cihazı fiilen kullanan kişi her zaman aynı kişi olmayabilir.

Aynı ev ortamında:

Hesap bir kişiye ait olabilir. Ancak cihaz farklı bir kişi tarafından kullanılabilir

Bu durum özellikle şu soruları doğurmaktadır:

- Mesajı gerçekten kim gönderdi?
- Mesaj hangi koşullarda oluşturuldu?
- Veriye kim erişti ve ne zaman erişti?

Ekran görüntüleri bu soruların hiçbirine teknik olarak cevap veremez.

3.6. Delilin Elde Edilme Şekline İlişkin Belirsizlik

Ekran görüntülerinin nasıl elde edildiği hususu da kritik önem taşımaktadır.

Aynı konutta yaşayan bireyler açısından:

Cihaz sahibinin bilgisi dışında erişim sağlanmış olabilir

Uygulama açıkken görüntü alınmış olabilir

İçerik seçilerek bağlamından koparılmış olabilir

Bu tür durumlarda:

Delilin elde edilme süreci şeffaf değildir

Delilin hukuka uygunluğu tartışmalı hale gelir

Teknik güvenilirlik ciddi şekilde zedelenir. Bu durum, verinin kim tarafından oluşturulduğu veya elde edildiği konusunda ciddi şüphe oluşturur.

4. ADLİ BİLİŞİM İMAJ ALMA GEREKLİLİĞİ

Dijital verilerin sağlıklı, güvenilir ve teknik olarak doğrulanabilir şekilde incelenebilmesi için, ilgili cihazlardan adli bilişim yöntemlerine uygun biçimde birebir (bit-by-bit) imaj alınması temel bir zorunluluktur.

Adli bilişim imajı; bir dijital cihazın (cep telefonu, bilgisayar, tablet vb.) depolama alanında bulunan tüm verilerin, hiçbir değişikliğe uğratılmadan ve veri bütünlüğü korunarak birebir kopyalanması işlemidir. Bu işlem sırasında yalnızca kullanıcı tarafından görülebilen veriler değil; silinmiş veriler, sistem kayıtları, uygulama veritabanları ve arka plan log kayıtları da dahil olmak üzere tüm veri yapısı eksiksiz şekilde kopyalanır.

4.1. İmaj Almanın Teknik Tanımı ve Kapsamı

Adli bilişim imajı alma işlemi; Cihazın depolama biriminin sektör bazında (low-level) kopyalanmasını, Verinin mantıksal değil, fiziksel düzeyde birebir çoğaltılmasını, Dosya sisteminin tamamının korunmasını amaçlayan teknik bir süreçtir.

Bu kapsamda elde edilen imaj;

Kullanıcı verilerini (mesajlar, medya dosyaları vb.),

Uygulama veritabanlarını (örneğin WhatsApp için msgstore.db),

Sistem loglarını,

Silinmiş ancak geri getirilebilir verileri,

Zaman damgalarını ve erişim kayıtlarını içeren tam ve bütüncül bir veri seti niteliğindedir.

4.2. Orijinal Verinin Korunması İlkesi

Adli bilişim incelemelerinde temel prensiplerden biri;

“Orijinal veriye müdahale edilmeden inceleme yapılması” ilkesidir.

İmaj alma işlemi sayesinde:

Orijinal cihaz üzerinde herhangi bir değişiklik yapılmaz,

İnceleme işlemleri doğrudan cihaz üzerinde değil, alınan imaj üzerinde gerçekleştirilir,

Veri kaybı veya veri değişikliği riski ortadan kaldırılır.

Bu durum, hem teknik hem de hukuki açıdan delilin güvenilirliğini artıran en önemli unsurlardan biridir.

4.3. Veri Bütünlüğünün Sağlanması ve Denetlenebilirlik

İmaj alma işlemi, veri bütünlüğünün korunmasını sağlamakla birlikte, aynı zamanda inceleme sürecinin denetlenebilir olmasına da imkân tanır.

Bu süreçte;

İmaj alma işlemi belirli prosedürlere göre gerçekleştirilir,

İşlem sırasında kullanılan araçlar ve yöntemler kayıt altına alınır,

Elde edilen veri seti üzerinde yapılan tüm analizler tekrar edilebilir nitelikte olur.

Bu sayede, farklı uzmanlar tarafından aynı veri seti üzerinde yapılan incelemeler aynı sonuçları verebilir, bu da bilimsel güvenilirliği sağlar.

5. ADLİ BİLİŞİM İMAJ ALMA İŞLEMLERİNDE EN SAĞLIKLI YÖNTEM OLARAK BYTE-TO-BYTE (BIT-TO-BIT) KOPYALAMA YAKLAŞIMI

Dijital delillerin teknik güvenilirliğinin sağlanabilmesi bakımından en temel husus, incelemeye konu verinin mümkün olan en eksiksiz ve en az müdahale içeren yöntemle elde edilmesidir. Adli bilişim uygulamalarında bu amaçla kullanılan en güvenilir yöntem, genel kabul gören terminolojiyle bit-for-bit, bit-stream copy veya uygulamada sık kullanılan ifade ile byte-to-byte imaj alma yöntemidir. Bu yöntem, yalnızca kullanıcı tarafından görülebilen dosyaların kopyalanmasını değil, depolama ortamında bulunan verinin mantıksal ve fiziksel düzeyde mümkün olan en geniş kapsamda birebir temsiline ulaşmayı hedeflemektedir. NIST kaynaklarında “imaging”, elektronik medyada bulunan verinin bit by bit kopyasının elde edilmesi olarak tanımlanmakta; ayrıca orijinal delile müdahaleden kaçınmak için delilin bit-for-bit bir temsiline alınmasının temel çözüm olduğu belirtilmektedir.

Bu yöntemin üstünlüğü, yalnızca görünen kullanıcı verilerini değil; dosya sistemi yapısını, ayrılmamış alanları, sistem artıklarını, zaman damgası ilişkilerini, bazı silinmiş veri kalıntılarını ve inceleme bakımından sonradan önem kazanabilecek teknik izleri de mümkün olduğunca korumasıdır. Buna karşılık yalnızca mantıksal (logical) veri toplama yöntemlerinde çoğu zaman işletim sistemi ya da uygulamanın kullanıcıya sunduğu görünür içerik alınmakta; ancak depolama katmanındaki bütün teknik bağlam aynı ölçüde korunamamaktadır. NIST’in mobil adli bilişim rehberlerinde ve araç test dokümanlarında da mobil cihazlarda logical acquisition, file system acquisition ve physical acquisition gibi farklı edinim türleri ayrı ayrı tanımlanmakta; fiziksel edinim türünde cihazın fiziksel belleğine ilişkin imajın elde edilmesinden söz edilmektedir. Bu ayrım, her edinim türünün aynı ispat gücünü taşımadığını göstermektedir.

5.1. Byte-to-Byte İmaj Alma Neden Daha Güvenilirdir

Byte-to-byte yaklaşımın en önemli avantajı, veriyi yalnızca “içerik” olarak değil, aynı zamanda “yapı” olarak da korumasıdır. Bir mesajlaşma uygulamasındaki yazışmanın delil değeri çoğu zaman yalnızca metin içeriğinden ibaret değildir. Mesajın bulunduğu veri tabanı, ilişkili zaman kayıtları, ilgili medya referansları, silinmiş kayıt izleri, uygulama artıkları ve sistem düzeyindeki eşleşmeler, verinin gerçekten o cihaza ait olup olmadığını ve ne şekilde oluştuğunu anlamada kritik önem taşır. Bit-for-bit/byte-to-byte imaj alma, işte bu bütünsel yapıyı mümkün olduğunca muhafaza eder.

Bu nedenle adli bilişimde en yüksek güvence, mümkün olan her durumda orijinal ortamın birebir temsiline ulaşmaktır. Çünkü yalnızca görünen dosyaların kopyalanması halinde, sonradan “bu veri gerçekten bu cihazdan mı geldi”, “zaman ilişkileri bozulmuş olabilir mi”, “uygulama dışı aktarım sırasında içerik değişmiş olabilir mi” veya “silinmiş ya da gizli teknik kayıtlar gözden kaçmış olabilir mi” gibi soruların tamamına sağlıklı cevap

vermek zorlaşır. Buna karşılık byte-to-byte imaj, bu tür itirazların teknik olarak değerlendirilmesine çok daha elverişli bir zemin sunar.

5.2. Orijinal Delilin Korunması İlkesi ile İlişkisi

Adli bilişimde temel prensiplerden biri, orijinal delil üzerinde mümkün olan en az işlem yapılmasıdır. Bu ilkenin amacı, inceleme sürecinin kendisinin delili değiştirmesini önlemektir. Bit-for-bit imaj alma yöntemi tam da bu nedenle önemlidir; çünkü uzman, mümkün olduğunca orijinal cihaz üzerinde değil, alınmış doğrulanmış imaj üzerinde çalışır. Delili inceleme sırasında değiştirmemek için delilin bit-for-bit kopyasının alınmasının temel çözüm olduğu açıkça belirtilmektedir.

Bu yaklaşım, raporun ispat gücünü de artırır. Çünkü inceleme süreci sonradan denetlenmek istendiğinde, “inceleme doğrudan cihaz üzerinde yapıldı ve veri değişmiş olabilir” itirazı yerine, “inceleme hash değeri alınmış imaj kopyası üzerinde yapıldı” denilebilmesi çok daha güçlü bir teknik pozisyon oluşturur. Bu, hem bilirkişi incelemesinin tekrarlanabilirliğini artırır hem de karşı denetim imkânı sağlar.

5.3. Byte-to-Byte ile Mantıksal Kopya Arasındaki Fark

Uygulamada sık yapılan hatalardan biri, dışa aktarılan bir sohbet dosyasının, ekran görüntüsünün veya yalnızca seçili verilerin alınmasının “imaj alma” ile karıştırılmasıdır. Oysa mantıksal kopya çoğu zaman yalnızca erişilebilir dosyaları veya uygulamanın sunduğu içerikleri kapsar. Fiziksel/bit-for-bit edinim ise depolama alanının fiziksel veya buna en yakın temsilini hedefler. NIST’in mobil cihaz adli bilişimi belgelerinde, mantıksal edinim, dosya sistemi edinimi ve fiziksel edinim ayrı metodolojiler olarak ele alınmakta; bu da özellikle mobil cihazlar bakımından “her veri alma işlemi aynı düzeyde değildir” sonucunu doğurmaktadır.

Bu fark özellikle WhatsApp gibi uygulamalarda belirgindir. Bir ekran görüntüsü yalnızca kullanıcının o anda gördüğü kısmı gösterir. Bir dışa aktarım dosyası, uygulamanın izin verdiği ölçüde içerik sunar. Buna karşılık byte-to-byte imaj, mümkünse veritabanı dosyalarını, uygulama dizinlerini, ilişkili sistem kayıtlarını ve daha geniş teknik çevreyi muhafaza eder. Bu nedenle delilin gerçekliği, aidiyeti ve bütünlüğü hakkında en güçlü değerlendirme zemini byte-to-byte edinimle oluşur.

5.4. Hash ile Birlikte Değerlendirildiğinde Byte-to-Byte Yaklaşımın Delil Gücü

Byte-to-byte imaj alma işlemi, hash doğrulaması ile birleştiğinde en güçlü hale gelir. Çünkü bit-for-bit kopya, verinin kapsamını; hash ise bu kopyanın inceleme süresince değişmediğini gösterir. Yalnızca “kopya alınmış olması” yeterli sayılmamalı; alınan kopyanın doğruluğu ve sonradan değişmediği de hash değerleri ile kayıt altına alınmalıdır.

Bu bağlamda raporlarda ideal teknik silsile şu şekilde kurulmalıdır: önce cihaz uygun usulle korunur, sonra mümkün olan en kapsamlı edinim yöntemiyle bit-for-bit/byte-to-byte imaj alınır, ardından imajın hash değerleri hesaplanır, daha sonra inceleme bu doğrulanmış imaj üzerinden yürütülür. Bu silsile bulunmadığında, özellikle yalnızca ekran görüntüsü veya seçilmiş veri parçaları üzerinden yapılan değerlendirmelerin ispat gücü düşer.

6. TEKNİK VE HUKUKİ DEĞERLENDİRME

Adli Bilişim İncelemesi (RAM BELLEK VE DİĞERLERİ)



Türk Dil Kurumu sözlüğünde, insanı aradığı gerçeğe ulaştırabilecek iz, emare olarak tanımlanan delil kavramı, bilgisayar ve cep telefonunun insan hayatına ait çok sayıda veriyi sınıflandırılmış bir şekilde depolayan bu cihazların suçun araştırılması ve ortaya çıkarılması sürecinde yaşadığımız zamanın en önemli delil kaynakları haline gelmişlerdir.

Dijital delil olarak adlandırdığımız bu delil kaynaklarının başında ise Bilgisayar incelemeleri ve buna bağlı Hard disk (Sabit disk) gelmektedir. Bilgisayar, veriyi iki şekilde depolamaktadır. Birincisi, işlem esnasında geçici olarak verilerin barındırıldığı Bellek (RAM) olarak bilinen aygıt üzerinde, ikincisi ise işletim sisteminin de barındırıldığı harddisk (sabit disk)’lerdedir.

Bilgisayar, Hard disk ve RAM incelemeleri yaparak özellikle;

- Şirket dolandırıcılıklarında,
- Boşanma davalarında,
- Hakaret – tehdit- şantaj davalarında,
- Bilişim suçlarında,
- İş davalarında,
- Kadına şiddet soruşturmalarında,
- Basın suçları soruşturmalarında,
- Şirket iç denetimlerinde,
- Teftiş kurallarının yaptığı soruşturmalarda,

Vb. vakaların çözümlenebilmesi için Ceza Muhakemeleri Kanunu (CMK) 67. Madde ve Hukuk Muhakemeleri Kanunu (HMK) 293. Madde’lere uygun olarak adli bilişim incelemeleri yapılabilmekte, bunlara ait teknik uzman mütalaası / uzman görüşü hazırlanabilmektedir.

RAM (bellek), bilgilerin geçici olarak depolandığı bir hafıza türüdür. Hali hazırda çalışmakta olan bir bilgisayar üzerinde aktif olan programları ve işlemlerle (son girilen internet siteleri, şifreler/password, son açılmış word, excel, pdf, power point – ppt, vb.) ilgili verileri saklayan bir geçici bellek birimidir. Bu sebeptendir ki RAM (bellek) üzerinden birçok veriye ulaşılabilmesi mümkündür.

Vakaların çözümlenebilmesi için bilgisayar çalışmakta iken belleğin imajının alınması gerekebilir. Unutulmamalıdır ki, RAM (bellek) üzerinde taşınan veriler uçucudur ve sistem kapandığında bu bilgiler kaybolur. RAM (bellek) imajının alınmasıyla, şifreler, çalışan işlemler, pano içeriği vb. gibi birçok veri elde edilebilir. Bu bilgilerin tümü, sistemi kapatmadan veya taşınmasından önce elde edilmelidir.

Sabit diskler verilerin kalıcı olarak depolandığı ve veriye tekrar tekrar ulaşılmasını sağlayan aygıtlardır. Temelde iki tür sabit disk vardır; manyetik olarak veri depolayabilen ve içerisinde cam, seramik veya metal plaka bulunan ve veri kurtarma kabiliyetinin en yüksek olduğu Hard Disc Driver (HDD) ve SSD (Solid State Disc) olarak bilinen ve temel yapı taşı silinebilir programlanabilir salt okunur bellekler (EPROM-Erasable Programmable Read Only Memory) olan disk türüdür. Her iki disk türü üzerinde herhangi bir adli inceleme gerçekleştirmeden önce muhakkak adli kopyalarının çıkarılması gerekmektedir.

İmaj (Adli Kopya), sektör-sektör veya bit-bit denilen şekilde hiçbir veri değişmeden, eksilmeden ve artmadan her veri aynı olacak şekilde, dosya haline bir başka diske aktarılmasıdır. Bu işlem yazılımlar aracılığı ile gerçekleştirilebildiği gibi donanımsal araçlar ile de gerçekleştirilebilir.

İmaj alma işleminden sonra, söz konusu sabit diskler içerisinde veri sızıntısı, veri hırsızlığı, sanayi casusluğu, internet üzerinden gerçekleştirilen dolandırıcılık türleri, banka-kredi kartı dolandırıcılığı, şifreli dosyaların veya sürücülerini analizi, zararlı yazılım analizi ve daha birçok konu üzerinde araştırmalar gerçekleştirilebilir

WhatsApp ekran görüntüleri, hem teknik hem de hukuki açıdan birlikte değerlendirildiğinde, bu tür verilerin tek başına ,ne şekilde alındığı,tarihi saati emei numarsaı belli olmayan maliği belli olmayan cihazın çıktıları kesin ve bağlayıcı delil niteliği taşımadığı değerlendirilmektedir.

Dijital delillerin geçerliliği bakımından, ulusal ve uluslararası adli bilişim standartlarında kabul gören temel kriterler;

- Veri bütünlüğünün korunması
- Kaynağın doğrulanabilir olması
- Verinin değiştirilmediğinin teknik olarak ispat edilebilir olması
- Elde edilme ve muhafaza sürecinin izlenebilir olması

şeklinde sıralanmaktadır.

Dijital delillerin güvenilir ve geçerli kabul edilebilmesi için;

Orijinal veri kaynağına dayanması,

Teknik doğrulama için gerekli metadata verilerini içermesi,

Veri bütünlüğünün hash değerleri ile doğrulanabilir olması,

Delilin elde edilme, muhafaza edilme ve sunulma süreçlerinin denetlenebilir olması (delil zinciri),

Manipülasyona karşı teknik olarak korunabilir nitelikte bulunması gerekmektedir.

Bu kriterleri taşımayan veriler;

Teknik olarak doğrulanabilirlikten yoksun olmakta,
Elde edilme süreci itibarıyla denetlenebilirlik içermemekte,
Veri bütünlüğü güvence altına alınamamakta,
Manipülasyon ihtimali bertaraf edilememektedir.

Ayrıca, aynı yaşam alanını paylaşan bireyler arasında dijital cihazlara erişimin teknik olarak mümkün olması, bu tür verilerin kim tarafından oluşturulduğu ve hangi koşullarda elde edildiği hususunda genel anlamda değerlendirme yapılmasını zorlaştıran bir unsur olarak kabul edilmektedir. Bu durum, dijital verilerin aidiyeti ve güvenilirliği bakımından dikkate alınması gereken önemli bir faktördür.

Bu çerçevede;

Yalnızca görsel çıktılardan ibaret olan ve teknik doğrulama imkânı sunmayan verilerin, dijital delil standartlarını karşılamadığı, bu nedenle tek başına kesin kanaat oluşturabilecek nitelikte güvenilir bir dijital delil olarak değerlendirilmesinin teknik ve bilimsel açıdan mümkün olmadığı kabul edilmektedir.

7. UZMAN HUKUKÇU GÖRÜŞÜ VE NORMATİF ÇERÇEVE

Geleneksel hukuk sistemlerinde deliller çoğunlukla fiziksel nitelikte olup; tanık beyanları, yazılı belgeler ve maddi bulgular üzerinden değerlendirilmektedir. Ancak günümüzde dijital veriler, suçun işlenişine ilişkin en kritik bilgileri içerebilmekte ve çoğu zaman klasik delillerden daha güçlü bir ispat aracı haline gelebilmektedir. Nitekim Türk Ceza Muhakemesi Kanunu kapsamında da delil serbestisi ilkesi benimsenmiş olup, dijital deliller bu çerçevede yargılamada önemli bir yer edinmiştir. Dijital delillerin önemi yalnızca ceza hukuku ile sınırlı değildir. Aynı zamanda özel hukuk uyuşmazlıklarında, boşanma davalarında, ticari davalarda ve idari işlemlerde de belirleyici rol oynayabilmektedir. Örneğin sözleşme ihlalleri, fikri mülkiyet hakları ve kişisel verilerin korunması gibi alanlarda dijital veriler sıklıkla delil olarak kullanılmaktadır. Bu bağlamda Kişisel Verilerin Korunması Kanunu da dijital verilerin işlenmesi ve korunmasına ilişkin önemli düzenlemeler getirmektedir.

Bununla birlikte dijital delillerin kullanımı, beraberinde ciddi hukuki ve teknik sorunları da gündeme getirmektedir.

Özellikle delilin elde edilme yöntemi, bütünlüğünün korunması ve güvenilirliğinin sağlanması gibi konular, yargılamanın adil olup olmadığı açısından kritik önem taşımaktadır.

Avrupa İnsan Hakları Mahkemesi kararlarında da hukuka aykırı elde edilen delillerin yargılamaya etkisi sıkça tartışılmakta ve adil yargılanma hakkı kapsamında değerlendirilmektedir.

Uluslararası doktrinde dijital delilin tanımına ilişkin farklı yaklaşımlar bulunmaktadır. Eoghan Casey dijital delili, “sayısal formatta depolanan veya iletilen ve bir olayın yeniden yapılandırılmasına yardımcı olan bilgi” olarak tanımlamaktadır (Casey, 2011, s. 45).

Benzer şekilde Carrier ve Spafford’a göre dijital delil, bilgisayar sistemleri üzerinde iz bırakan ve teknik analiz yoluyla ortaya çıkarılabilen veri bütünüdür (Carrier & Spafford, 2004).

Türk hukukunda dijital delil kavramı doğrudan tanımlanmamış olmakla birlikte, Ceza Muhakemesi Kanunu çerçevesinde “belge” ve “diğer deliller” kapsamında değerlendirilmektedir. Bu durum, dijital delillerin hukuki statüsünün yorum yoluyla belirlenmesine neden olmaktadır.

Dijital deliller oldukça geniş bir veri kategorisini kapsamaktadır. Bunlar arasında:

- E-posta yazışmaları
 - Sosyal medya paylaşımları
 - IP adres kayıtları
 - Log dosyaları
 - Mobil uygulama verileri
 - GPS ve konum bilgileri
 - Bulut sistemlerinde saklanan veriler
- yer almaktadır.

Bu çeşitlilik, dijital delillerin hem teknik hem de hukuki açıdan çok disiplinli bir incelemeyi gerektirdiğini göstermektedir.

Türk hukukunda dijital delillerin hukuki niteliğine ilişkin açık ve sistematik bir kanuni tanım bulunmamaktadır. Bununla birlikte, doktrinde dijital delillerin hangi delil kategorisi içerisinde değerlendirileceği hususunda çeşitli görüşler ileri sürülmüş olup, bu konuda tam bir görüş birliğinden söz etmek mümkün değildir.

Ulusal doktrinde hâkim görüş, dijital delillerin içerdiği verinin belirli bir düşünceyi, olguyu veya irade beyanını temsil etmesi nedeniyle belge niteliğinde delil olarak değerlendirilmesi mümkün olacağı bunun gerekli merasim şartlarına uyulması halinde ancak mümkün olacağı yönündedir. Nitekim Feridun Yenisey ve Ayşe Nuhoglu, dijital verilerin yazılı delillerle benzer şekilde bilgi taşıyıcı işlev gördüğünü ve bu nedenle belge delili kapsamında ele alınmasının verilerin bütünlüğü korunmuş hali ile isabetli olacağını ifade etmektedir (Yenisey & Nuhoglu, 2020). Bu yaklaşım, özellikle dijital verinin içerik boyutuna odaklanmakta ve verinin temsil ettiği anlamı esas almaktadır.

Bununla birlikte, doktrinde bazı yazarlar dijital delillerin yalnızca içerik boyutuyla değil, aynı zamanda üzerinde bulundukları fiziksel taşıyıcılar itibarıyla da değerlendirilmesi gerektiğini ileri sürmektedir. Bu görüşe göre dijital veriler, tamamen soyut nitelikte olmayıp, mutlaka bir fiziksel ortam (hard disk, USB bellek, sunucu vb.) üzerinde varlık kazandıkları için, bu yönüyle ancak ve ancak **maddi delil niteliği** de taşımaktadır.

Nitekim Brian Carrier, dijital delillerin yalnızca veri olarak değil, aynı zamanda bu veriyi barındıran fiziksel sistemler üzerinden analiz edilmesi gerektiğini vurgulamakta ve dijital incelemenin temelini “fiziksel depolama ortamı” olduğunu belirtmektedir (Carrier, 2006). ***Carrier’a göre dijital delil, hem veri hem de bu verinin bulunduğu fiziksel ortamın birlikte değerlendirilmesini gerektiren bir bütündür.***

Benzer şekilde Eoghan Casey de dijital delillerin analizinde fiziksel taşıyıcının (örneğin disk yapısı, dosya sistemi, veri blokları) belirleyici rol oynadığını ifade etmekte ve dijital

delilin maddi yönünün göz ardı edilmesinin eksik bir değerlendirmeye yol açacağını belirtmektedir (Casey, 2011).

Türk doktrinde de bu yaklaşıma dolaylı olarak temas eden görüşler bulunmaktadır. Özellikle Nur Centel, dijital delillerin klasik delil kategorilerine tam olarak uymadığını ve bu nedenle hem maddi hem de belge unsurlarını birlikte değerlendiren bir yaklaşımın benimsenmesi gerektiğini ifade etmektedir.

Bu bağlamda dijital verinin yalnızca içerik olarak değil, aynı zamanda üzerinde bulunduğu taşıyıcı sistemle birlikte ele alınması gerektiği kabul edilmektedir.

Doktrinde giderek ağırlık kazanan bir diğer yaklaşım ise dijital delillerin **karma (hibrit) nitelikte** olduğu yönündedir. Bu görüşe göre dijital deliller, içerik itibarıyla belge deliline, taşıyıcı unsurları bakımından ise maddi delile yaklaşmaktadır.

Nur Centel ile Hamide Zafer tarafından da desteklenen bu yaklaşım, dijital delillerin çok katmanlı yapısını dikkate alması bakımından daha bütüncül bir çözüm sunmaktadır. Nitekim dijital verinin hem teknik hem de hukuki boyutları birlikte değerlendirildiğinde, klasik delil kategorilerinin bu yeni delil türünü açıklamakta yetersiz kaldığı görülmektedir. Öte yandan, özellikle teknolojik gelişmelerin etkisiyle bazı yazarlar, dijital delillerin klasik delil sistematigi içerisinde değerlendirilmesinin yetersiz kaldığını ve bu nedenle **bağımsız bir delil türü olarak ele alınması gerektiğini** ileri sürmektedir. Bu yaklaşım, dijital delillerin değiştirilebilirlik, kopyalanabilirlik ve uçuculuk gibi kendine özgü teknik özelliklerinden hareketle, geleneksel delil kategorilerinin bu yeni delil türünü açıklamakta yetersiz kaldığını savunmaktadır.

Bu görüş özellikle Anglo-Amerikan ve adli bilişim literatüründe daha belirgin şekilde ortaya konulmuştur. Nitekim Eoghan Casey, dijital delillerin klasik fiziksel delillerden farklı olarak dinamik, kolay manipüle edilebilir ve çok katmanlı bir yapıya sahip olduğunu belirtmekte ve bu nedenle geleneksel delil anlayışının dijital delilleri açıklamakta sınırlı kaldığını ifade etmektedir (Casey, 2011).

Benzer şekilde Brian Carrier, dijital delillerin yalnızca veri içeriği üzerinden değil, aynı zamanda sistem yapısı, dosya sistemi ve zaman çizelgesi gibi çok boyutlu unsurlar üzerinden değerlendirilmesi gerektiğini vurgulamakta ve bu durumun klasik delil kategorilerinden farklı bir yaklaşımı zorunlu kıldığını belirtmektedir (Carrier, 2006).

Ayrıca Peter Sommer de dijital delillerin teknik karmaşıklığı ve değişken yapısı nedeniyle geleneksel delil teorisinin yeniden gözden geçirilmesi gerektiğini ifade etmekte ve dijital delillerin kendine özgü bir kategori olarak değerlendirilmesi gerektiğine işaret etmektedir (Sommer, 2010).

Türk hukuk doktrinde ise dijital delillerin bağımsız bir delil türü olduğu yönünde açık ve sistematik bir teori henüz tam anlamıyla gelişmemiş olmakla birlikte, bazı yazarlar dijital delillerin klasik delil ayrımları içerisinde zorlandığını ve bu nedenle yeni bir sınıflandırma ihtiyacının bulunduğunu dolaylı olarak kabul etmektedir.

Anglo-Amerikan hukuk sisteminde dijital deliller genellikle “electronic evidence” başlığı altında incelenmektedir. Bu sistemde delillerin kabul edilebilirliği belirli kriterlere bağlıdır.

Özellikle ABD hukukunda:

- Delilin güvenilir olması
- Zincirleme muhafazanın korunması
- Delilin değiştirilmemiş olması

gibi unsurlar önem taşımaktadır.

Federal Rules of Evidence kapsamında dijital deliller, “best evidence rule” ve “authentication” ilkeleri çerçevesinde değerlendirilmektedir.

Avrupa İnsan Hakları Mahkemesi, dijital delillerin kullanımını doğrudan düzenlememekle birlikte, bu delillerin elde edilme ve kullanma biçimini **adil yargılanma hakkı (AİHS m. 6)** kapsamında değerlendirmektedir.

Mahkeme, özellikle şu hususlara dikkat etmektedir:

- Delilin hukuka uygun elde edilip edilmediği
- Savunma hakkının ihlal edilip edilmediği
- Delilin yargılamanın sonucuna etkisi

Örneğin *Khan v. United Kingdom* kararında, hukuka aykırı elde edilen delillerin tek başına adil yargılanma hakkını ihlal etmeyeceği, ancak yargılamanın bütünü içinde değerlendirilmesi gerektiği belirtilmiştir.

Dijital delillerin elde edilmesinde en temel ilke, hukuka uygunluktur. Bu ilke, hem ulusal hukukta hem de uluslararası insan hakları hukukunda temel bir yer tutmaktadır.

Türk hukukunda, Türkiye Cumhuriyeti Anayasası’nın 38. maddesi uyarınca hukuka aykırı olarak elde edilen bulgular delil olarak kabul edilemez. Bu düzenleme, dijital deliller açısından da geçerlidir.

Ayrıca Ceza Muhakemesi Kanunu kapsamında:

- Arama (m.116 vd.)
 - Elkoyma (m.123 vd.)
 - Bilgisayarlarda arama ve kopyalama (m.134)
- gibi işlemler açıkça düzenlenmiştir.

Özellikle CMK m.134, dijital delillerin elde edilmesi bakımından özel bir hüküm niteliğindedir ve şu şartları öngörmektedir:

- Hakim kararı (gecikmesinde sakınca varsa savcı kararı)
- Kopyalama işleminin yapılması
- Verilerin bütünlüğünün korunması

Doktrinde Nur Centel, hukuka aykırı şekilde elde edilen dijital delillerin, maddi gerçeğe ulaşmaya hizmet etse bile yargılamada kullanılmaması gerektiğini vurgulamaktadır (Centel vd.).

Dijital delillerin yargılamada kullanılabilirliği, yalnızca elde edilme yöntemine değil, aynı zamanda **güvenilirliği (authenticity)** ve **bütünlüğünün (integrity)** korunmasına da bağlıdır. Dijital verilerin kolaylıkla değiştirilebilir olması, bu delillerin doğruluğunun teknik yöntemlerle ispat edilmesini zorunlu kılmaktadır.

Bu bağlamda dijital delillerin değerlendirilmesinde adli bilişim teknikleri ile hukuki ilkelerin birlikte ele alınması gerekmektedir.

Delil bütünlüğü, dijital verinin elde edildiği andan itibaren **hiçbir şekilde değiştirilmediğinin garanti altına alınması** anlamına gelmektedir. Bu ilke, dijital delilin güvenilirliğinin temelini oluşturur.

Dijital delillerde bütünlük genellikle **hash algoritmaları** kullanılarak sağlanmaktadır. Hash fonksiyonları, bir veri seti için benzersiz bir “özet değer” üretir. Bu değer:

- Veri değiştiğinde tamamen değişir
- Aynı veri için her zaman aynı sonucu verir

Eoghan Casey, hash değerlerinin dijital delillerin bütünlüğünü doğrulamada “altın standart” olduğunu belirtmektedir (Casey, 2011).

En yaygın kullanılan hash algoritmaları şunlardır:

- MD5
- SHA-1
- SHA-256

Örneğin bir hard diskin imajı alındığında:

1. İlk hash değeri alınır
2. Analiz sonrası tekrar hash alınır
3. İki değer karşılaştırılır

Eğer değerler aynıysa, delilin bütünlüğünün korunduğu kabul edilir.

Türk hukukunda bu teknik süreç açıkça düzenlenmemiş olsa da, Ceza Muhakemesi Kanunu m.134 kapsamında “verilerin kopyalanması ve korunması” yükümlülüğü dolaylı olarak bu ilkeyi desteklemektedir.

Delil güvenilirliği, dijital verinin **gerçek kaynağından geldiğinin ve sahte olmadığının ispat edilmesi** anlamına gelmektedir.

Dijital deliller açısından en büyük risklerden biri:

- Veri manipülasyonu
 - Sahte içerik üretimi
 - Yetkisiz erişim
- gibi durumlardır.

Brian Carrier, dijital delillerin güvenilirliğinin sağlanabilmesi için yalnızca teknik doğrulamanın yeterli olmadığını, aynı zamanda **bağlamsal analiz** yapılması gerektiğini belirtmektedir (Carrier, 2006).

Delil güvenilirliğini sağlamak için kullanılan yöntemler:

- Kaynak doğrulama (IP, cihaz kimliği)
- Kullanıcı ilişkilendirmesi
- Zaman damgası analizi
- Log kayıtlarının incelenmesi

Örneğin bir e-posta delilinde:

- Gönderici IP adresi
- Sunucu kayıtları
- Zaman bilgileri

birlikte değerlendirilerek delilin gerçekliği analiz edilir.

Dijital delillerin güvenilirliğini doğrudan etkileyen bir diğer unsur **zincirleme muhafaza (chain of custody)** ilkesidir.

Bu ilke, delilin:

- İlk elde edildiği andan itibaren
 - Her aşamada kimlerin elinden geçtiğinin
 - Hangi işlemlere tabi tutulduğunun
- belgelenmesini ifade eder.

Eoghan Casey, zincirleme muhafazanın korunmadığı durumlarda dijital delilin mahkemede kabul edilme ihtimalinin ciddi şekilde azaldığını vurgulamaktadır.

Zincirleme muhafaza sürecinde:

- Delil kayıt formları tutulur
- Her işlem loglanır
- Yetkisiz erişim engellenir

Eğer bu süreçte bir boşluk oluşursa:

- Delilin değiştirilmiş olabileceği varsayılır
- Savunma tarafı delile itiraz edebilir
- Mahkeme delili reddedebilir

Avrupa İnsan Hakları Mahkemesi, dijital delillerin güvenilirliğini değerlendirirken yalnızca teknik doğruluğa değil, aynı zamanda **yargılamanın bütününe etkisine** bakmaktadır.

Nur Centel'e göre dijital delillerin değerlendirilmesinde teknik uzman görüşü olmaksızın sağlıklı bir karar verilmesi oldukça güçtür.

Dijital delillerin hukuki niteliği ve yargılamadaki rolü, farklı hukuk sistemlerinde çeşitli yaklaşımlarla ele alınmaktadır. Özellikle Anglo-Amerikan hukuk sistemi ile Avrupa kıta hukuku arasında önemli farklılıklar bulunmaktadır. Bununla birlikte, küreselleşme ve dijitalleşme süreci, bu sistemler arasında belirli bir yakınlaşmayı da beraberinde getirmiştir.

Bu bölümde dijital delillere ilişkin yaklaşımlar; **ABD hukuku, Avrupa İnsan Hakları Hukuku ve Avrupa Birliği hukuku** çerçevesinde incelenecektir.

ABD hukuk sistemi, dijital delillerin geliştirilmesi ve uygulanması bakımından en ileri sistemlerden biridir. Bu sistemde dijital deliller genellikle “electronic evidence” başlığı altında değerlendirilmektedir.

ABD’de dijital delillerin kabul edilebilirliği, başta Federal Rules of Evidence olmak üzere çeşitli düzenlemelere tabidir.

ABD hukukunda bir dijital delilin mahkemede kullanılabilmesi için öncelikle **authenticity (doğruluk)** şartını sağlaması gerekmektedir.

Federal Rules of Evidence Rule 901’e göre:

- Delilin iddia edildiği gibi olduğunun gösterilmesi gerekir
 - Bu durum tanık beyanı veya teknik analiz ile ispat edilebilir
- Örneğin:

- E-posta → gönderenin kimliği doğrulanmalıdır
- Sosyal medya paylaşımı → hesabın gerçek sahibi belirlenmelidir

ABD hukukunda dijital deliller açısından önemli bir diğer ilke **“best evidence rule”**dur.

Bu ilkeye göre:

- Belgenin aslı veya güvenilir kopyası sunulmalıdır

Dijital delillerde bu ilke esnek yorumlanmakta ve hash değeri doğrulanmış kopyalar “orijinal” kabul edilmektedir.

ABD hukukunda hukuka aykırı elde edilen deliller, “exclusionary rule” kapsamında genellikle yargılamada kullanılamaz.

Bu ilke özellikle:

- Hukuka aykırı arama
 - İzinsiz veri erişimi
- durumlarında uygulanmaktadır.

Bu yönüyle ABD hukuku, Türk hukukuna benzer şekilde hukuka uygunluk ilkesine büyük önem vermektedir.

Avrupa İnsan Hakları Mahkemesi, dijital delillere ilişkin özel bir düzenleme yapmamakla birlikte, bu delillerin kullanımını **adil yargılama hakkı (AİHS m.6)** çerçevesinde değerlendirmektedir.

Mahkeme’ye göre:

- Delilin hukuka aykırı elde edilmesi tek başına ihlal oluşturmaz
- Yargılamanın bütünü değerlendirilmelidir
Bu yaklaşım, ABD hukukundan farklı olarak daha esnek bir sistem ortaya koymaktadır. AİHM içtihadında dijital delillerle doğrudan veya dolaylı ilgili önemli kararlar bulunmaktadır:

- *Khan v. United Kingdom*
- *Schenk v. Switzerland*
- *Barberà, Messegue and Jabardo v. Spain*

Bu kararlarda Mahkeme, delilin elde edilme şekli kadar:

- Savunma hakkı
- Çelişmeli yargılama
- Delilin ağırlığı

gibi unsurları da dikkate almaktadır.

Avrupa Birliği, dijital deliller konusunda özellikle veri koruma ve sınır ötesi erişim alanlarında önemli düzenlemeler geliştirmiştir.

BOŞANMA DAVALARI ÇERÇEVESİNDE DİJİTAL DELİLLER

Boşanma davalarında dijital delillerin kullanımı bakımından en tartışmalı husus, bu delillerin **hukuka uygun şekilde elde edilip edilmediği** meselesidir. Zira dijital veriler çoğu zaman bireylerin özel hayatına ilişkin en mahrem bilgileri içermekte olup, bu verilere erişim süreci doğrudan temel hak ve özgürlüklerle ilişkilidir.

Bu bağlamda, eşlerden birinin diğerine ait dijital verilere erişim sağlarken başvurduğu yöntemler büyük önem taşımaktadır. Özellikle aşağıdaki durumlar öğretide ve yargı uygulamasında sıklıkla tartışma konusu olmaktadır:

- Eşin cep telefonunun rızası olmaksızın incelenmesi
- Şifre kırma veya hesaplara izinsiz erişim yoluyla mesaj içeriklerine ulaşılması
- Gizli ses veya görüntü kaydı alınması
- Sosyal medya hesaplarının izinsiz şekilde kontrol edilmesi

Bu tür eylemler, kural olarak **özel hayatın gizliliğinin ihlali** niteliği taşıyabileceğinden, elde edilen verilerin hukuka aykırı delil olarak değerlendirilmesi söz konusu olabilmektedir. Nitekim Türkiye Cumhuriyeti Anayasası m.20 ve Avrupa İnsan Hakları Sözleşmesi kapsamında özel hayatın korunması temel bir hak olarak güvence altına alınmıştır.

Bununla birlikte, boşanma davalarının kendine özgü yapısı ve taraflar arasındaki özel ilişki dikkate alındığında, dijital delillerin hukuka uygunluğu meselesi her zaman katı bir şekilde değerlendirilmemektedir. Bu noktada Yargıtay içtihatlarında daha **esnek ve somut olay odaklı bir yaklaşımın benimsendiği** görülmektedir.

Yargıtay'ın genel yaklaşımına göre:

- Hukuka aykırı şekilde elde edilen deliller kural olarak hükme esas alınamaz
- Ancak bazı durumlarda, delilin elde edilme yöntemi ile korunmak istenen menfaat arasında bir denge kurulmaktadır

Bu çerçevede özellikle:

- Delilin elde edilmesinin **zorunlu olup olmadığı**
- Başka şekilde ispat imkânının bulunup bulunmadığı
- Müdahalenin **ölçülü olup olmadığı**

gibi kriterler dikkate alınmaktadır.

Özellikle eşin sadakatsizliğini ispat amacıyla elde edilen bazı dijital deliller bakımından, Yargıtay'ın mutlak bir ret yaklaşımı benimsemediği; aksine somut olayın özelliklerine göre değerlendirme yaptığı görülmektedir. Bu durum, medeni yargılamada **ispat hakkı ile özel hayatın korunması arasındaki dengenin** gözetildiğini göstermektedir.

Yargıtay içtihatları incelendiğinde, dijital delillerin boşanma davalarında giderek artan bir öneme sahip olduğu ve özellikle kusur tespitinde belirleyici rol oynadığı görülmektedir. Teknolojik gelişmelere paralel olarak mahkemeler, dijital iletişim araçlarından elde edilen verileri sıklıkla delil olarak değerlendirmektedir.

Bu bağlamda Yargıtay kararlarında öne çıkan dijital delil türleri şunlardır:

- **WhatsApp ve benzeri mesajlaşma uygulamaları:**
Taraflar arasındaki yazışmalar, sadakat yükümlülüğünün ihlali veya onur kırıcı davranışların ispatında kullanılabilmektedir.
 - **Sosyal medya içerikleri:**
Facebook, Instagram gibi platformlarda yapılan paylaşımlar, tarafların yaşam tarzı, ilişkileri ve davranışları hakkında önemli veriler sunmaktadır.
 - **E-posta yazışmaları:**
Özellikle duygusal ilişkiler veya maddi konular bakımından delil niteliği taşıyabilir.
 - **Fotoğraf ve video kayıtları:**
Tarafların davranışlarını doğrudan gösteren güçlü delil niteliği taşıyabilir. Bununla birlikte, Yargıtay dijital delilleri değerlendirirken otomatik bir kabul mekanizması işletmemekte; her somut olay bakımından belirli kriterler çerçevesinde değerlendirme yapmaktadır.
- Yargıtay uygulamasında dijital delillerin kabul edilebilirliği ve ispat gücü bakımından özellikle şu kriterlerin dikkate alındığı görülmektedir:

1. Delilin Elde Edilme Yöntemi

Delilin hangi yöntemle elde edildiği, değerlendirmede en önemli unsurlardan biridir. Hukuka aykırı yöntemlerle elde edilen deliller kural olarak reddedilmekle birlikte, bazı durumlarda bu kural esnetilebilmektedir.

2. Özel Hayatın İhlali

Delilin elde edilmesi sırasında karşı tarafın özel hayatının ihlal edilip edilmediği incelenmektedir. Bu değerlendirmede:

- Müdahalenin ağırlığı
- Elde edilen verinin niteliği
- Taraflar arasındaki ilişki gibi unsurlar dikkate alınmaktadır.

3. Delilin Güvenilirliği ve Bütünlüğü

Sunulan dijital verinin:

- Manipüle edilip edilmediği
- Orijinal olup olmadığı
- Teknik olarak doğrulanabilirliği incelenmektedir.

4. İspat Gücü

Dijital delilin tek başına mı yoksa diğer delillerle birlikte mi değerlendirileceği önem taşımaktadır. Yargıtay, özellikle:

- Tek başına kesinlik taşımayan dijital verilerin
- Diğer delillerle desteklenmesini

arzu etmektedir.

5. Ölçülülük ve Hakkaniyet

Yargıtay, delilin elde edilmesi ile korunmak istenen menfaat arasında bir denge kurmaktadır. Bu bağlamda:

- Evlilik birliğinin korunması
 - Sadakat yükümlülüğünün ihlali
 - İspat hakkının gerekliliği
- gibi unsurlar birlikte değerlendirilmektedir.

Genel Değerlendirme

Sonuç olarak Yargıtay uygulaması, dijital delillerin boşanma davalarında önemli bir ispat aracı olduğunu kabul etmekle birlikte, bu delillerin kullanımını **mutlak kurallara bağlamak yerine somut olayın özelliklerine göre esnek bir şekilde değerlendirmektedir**. Bu yaklaşım, medeni yargılamanın doğasına uygun olarak **hakkaniyet, ölçülülük ve denge ilkelerini** ön plana çıkarmaktadır.

• BU KAPSAMDA;SONUÇ :

Yalnızca görsel çıktılardan ibaret olan ve teknik doğrulama imkânı bulunmayan verilerin, tek başına güvenilir ve kesin dijital delil olarak kabul edilmesinin teknik ve bilimsel açıdan mümkün olmadığı,

Sağlıklı ve kesin bir değerlendirme yapılabilmesi için, dijital verilerin ilgili cihazlar üzerinden adli bilişim yöntemleri ile elde edilmesi, bu verilerin hash değerleri ile doğrulanması ve incelemenin bu doğrulanmış veri setleri üzerinden gerçekleştirilmesi gerektiği,

Bu şartlar sağlanmadan yalnızca doğrulanamayan veriler üzerinden kesin kanaat oluşturulmasının teknik ve bilimsel açıdan mümkün olmadığı kabul edilmektedir.

Sonuç olarak;

Teknik doğrulama süreçlerinden geçmemiş ve veri bütünlüğü güvence altına alınmamış dijital verilerin, tek başına hükme esas alınabilecek nitelikte güçlü ve güvenilir bir delil olarak değerlendirilmesinin uygun olmadığı sonucuna ulaşılmaktadır.

8. YARGISAL YAKLAŞIM, İÇTİHATLAR VE DELİL DEĞERİNE ETKİSİ

Dijital verilerin delil değeri, yalnızca teknik yeterlilikle değil; aynı zamanda Anayasa, usul hukuku ve yüksek yargı içtihatları çerçevesinde değerlendirilmektedir. Türk hukuk sisteminde delilin kabul edilebilirliği bakımından temel ölçüt; delilin yalnızca içerik itibarıyla değil, elde edilme yöntemi, doğrulanabilirliği ve denetlenebilirliği itibarıyla da hukuk düzeni ile uyumlu olmasıdır.

Bu kapsamda Anayasa'nın 38/6. Maddesinde;

“Kanuna aykırı olarak elde edilmiş bulgular, delil olarak kabul edilemez.”

Hükmü yer almakta olup, aynı doğrultuda HMK m.189/2 hükmü de;

“Hukuka aykırı elde edilmiş deliller, bir vakıanın ispatında dikkate alınamaz.”

Şeklinde düzenlenmiştir.

7.1. Hukuka Aykırı Elde Edilen whatsapp Kayıtlarının Delil Niteliği

Yargıtay 2. Hukuk Dairesi'nin;

2023/5012 E., 2024/1780 K. Sayılı kararında;

eşin bilgisi ve rızası dışında, WhatsApp Web üzerinden elde edilen yazışma kayıtlarının hukuka aykırı delil niteliğinde olduğu değerlendirilmiş ve bu verilerin kusur belirlemede dikkate alınamayacağı belirtilmiştir.

Bu kararın önemi;

Dijital verinin içeriğinden ziyade

elde edilme yönteminin belirleyici olduğunun açıkça ortaya konulmasıdır.

7.2. Cihazdaki Verinin Otomatik Delil Sayılmaması

Yargıtay 2. Hukuk Dairesi;

2021/563 E., 2021/1768 K.

sayılı kararında;

eşin evde bıraktığı telefonda bulunan mesajların, doğrudan kusur belirlemesine esas alınamayacağını belirtmiştir.

Bu yaklaşım şu gerçeği ortaya koymaktadır:

Bir cihazda veri bulunması, o verinin mutlaka cihaz sahibi tarafından oluşturulduğunu ispatlamaz.

7.3. Kaynağı Doğrulanamayan Yazışmaların Delil Niteliği

Yargıtay 3. Hukuk Dairesi'nin;

2023/287 E., 2023/1549 K.

sayılı kararında;

göndericisi ve kaynağı teknik olarak doğrulanamayan WhatsApp yazışmalarının, delil başlangıcı olarak dahi kabul edilemeyeceği belirtilmiştir.

Bu karar doğrudan şu ilkeyi ortaya koymaktadır: Teknik olarak doğrulanamayan veri, hukuken de güvenilir kabul edilmez.

7.4. İçtihatların Ortak Sonucu

Yukarıda belirtilen Yargıtay kararları birlikte değerlendirildiğinde;

yüksek yargının dijital delillere yaklaşımında aşağıdaki temel ilkelerin benimsendiği anlaşılmaktadır:

Delilin içeriğinden önce elde edilme yöntemi önemlidir

Hukuka aykırı elde edilen veriler doğrudan dışlanır

Kaynağı doğrulanamayan veriler delil sayılmaz

Ekran görüntüsü tek başına yeterli kabul edilmez

Dijital veriler ancak teknik olarak doğrulanırsa değer kazanır

Bu içtihatlar doğrultusunda;

yalnızca ekran görüntüsü şeklinde sunulan, teknik doğrulama imkânı bulunmayan, elde edilme yöntemi denetlenemeyen ve orijinal veri ile bağlantısı kurulamayan dijital verilerin, tek başına kesin ve delil olarak kabul edilmesi mümkün değildir.

Bu nedenle;

dijital verilerin hukuki değerlendirmeye konu edilebilmesi için, ilgili cihazlardan adli bilişim yöntemleri ile imaj alınması, hash doğrulaması yapılması ve incelemenin bu doğrulanmış veri seti üzerinden gerçekleştirilmesi gerekmektedir.

9. GENEL DEĞERLENDİRME

Dijital verilerin güvenilirliğinin değerlendirilebilmesi, bu verilerin elde edilme, saklanma ve sunulma süreçlerinin teknik olarak doğrulanabilir olmasına bağlıdır. Bu kapsamda, bir dijital verinin güvenilir kabul edilebilmesi için;

Hangi cihaz veya sistem üzerinden elde edildiğinin belirlenebilir olması,

Verinin kim tarafından oluşturulduğu veya erişildiğinin tespit edilebilir olması,
 Elde edilme sürecinde herhangi bir değişikliğe uğrayıp uğramadığının denetlenebilir olması,
 Sunulan verinin orijinal veri ile birebir örtüştüğünün teknik olarak doğrulanabilmesi gerekmektedir.
 Bu unsurların sağlanamadığı durumlarda, dijital verilerin güvenilirliği ve doğruluğu teknik olarak kesin şekilde ortaya konulamaz.
 Bunun yanında;
 Görsel çıktılar (ekran görüntüleri vb.) doğası gereği manipülasyona açık veri türleri olup, Metadata (üst veri) içermemeleri nedeniyle teknik doğrulama imkânı sunmamakta,
 Hash doğrulamasına uygun olmamaları sebebiyle veri bütünlüğü güvence altına alınamamakta,
 Delilin elde edilme ve muhafaza sürecine ilişkin zincirleme güvenlik (chain of custody) sağlanamadığından denetlenebilirlikten yoksun kalmaktadır.

Bu tür teknik eksiklikler birlikte değerlendirildiğinde, söz konusu nitelikteki verilerin yüksek derecede belirsizlik ve şüphe barındırdığı kabul edilmektedir.
 Ayrıca, aynı yaşam alanını paylaşan bireyler arasında dijital cihazlara erişimin teknik olarak mümkün olması; verinin gerçek kaynağı, oluşturulma iradesi ve bağlam bütünlüğü hususlarında genel değerlendirmeyi güçleştiren bir faktör olarak kabul edilmektedir. Bu durum, dijital verilerin aidiyeti ve güvenilirliği açısından dikkate alınması gereken önemli bir teknik risk unsurudur.

Bu çerçevede;
 teknik doğrulama imkânı bulunmayan, elde edilme süreci denetlenemeyen ve veri bütünlüğü güvence altına alınamayan dijital verilerin, güvenilirlik düzeyi düşük ve manipülasyon ihtimali bertaraf edilememiş veriler olarak değerlendirilmesi gerektiği kabul edilmektedir.

10. SONUÇ

DIJİTAL VERİLER, TAMAMEN SOYUT NİTELİKTE DEĞİLDİR

Mutlaka bir fiziksel ortam (hard disk, usb bellek, sunucu vb.) Üzerinde varlık kazandıkları için, bu yönüyle ancak ve ancak **maddi delil niteliği** de taşıyabilmektedir. yani dosyay sunulduğu şekli ile maddi delil niteliği yoktur.

"Karşı tarafın sunduğu sadece (çıktı) veya resim dosyasıdır. Asıl delil o telefonun,veya Hdd,veya vs içindeki manyetik izlerdir. O izler mahkemeye getirilmediği sürece ortada hukuken geçerli bir 'maddi delil' yoktur".

sadece "yetersiz" değil, "**şüpheli ve tehlikeli**" bir veri halindedir. **Aleyhe delil olamaz:**
 Çünkü teknik olarak doğrulanabilir (hash, imaj vb.) değil. **Lehe olabilir**

MUTLU ZAMANLAR ÇELİŞKİSİ **"Eşlerin son derece mutlu oldukları ve herhangi bir şikayetlerinin olmadığı zamanlarda"** bu kayıtların oluşturulmuş olması,ihtimali ortadan kalmadığı verilerin tarihleri ve saatleri ile alındığı hts kayıtlarının dosyada olmadığı

Dijital veriler üzerinde sağlıklı ve kesin bir kanaat oluşturulabilmesi için, ilgili cihazlardan adli bilişim usullerine uygun şekilde imaj alınması, mümkün olan en kapsamlı veri edinim

yöntemlerinin uygulanması, elde edilen veri setlerinin hash değerleri ile doğrulanması ve incelemenin bu doğrulanmış veriler üzerinden yürütülmesi gerekmektedir.

Bunun yanında, özellikle aynı yaşam alanını paylaşan kişiler arasında cihazlara erişim ihtimalinin bulunması, verinin gerçek kaynağı, oluşturulma iradesi ve bağlam bütünlüğü konularında ayrıca dikkatli değerlendirme yapılmasını zorunlu kılmaktadır.

Dijital delillerin teknik ve hukuki geçerliliğinin sağlanabilmesi için;

- Orijinal veri niteliği taşıması,
 - Teknik olarak doğrulanabilir olması,
 - Veri bütünlüğünün hash değerleri ile güvence altına alınması,
 - Elde edilme ve muhafaza süreçlerinin denetlenebilir olması,
 - Adli bilişim standartlarına uygun yöntemlerle elde edilmesi gerekmektedir.
- Bu kriterleri karşılamayan veriler;
- Orijinal veri niteliğinden yoksun olmakta,
 - Teknik doğrulama imkânı sunmamakta,
 - Değiştirilebilir ve manipülasyona açık bir yapı arz etmekte,
 - Veri bütünlüğü güvence altına alınamamakta,
 - Elde edilme süreci bakımından denetlenebilirlik içermemektedir.

11. SONUÇ VE KANAAT

Yapılan teknik inceleme, adli bilişim ilkeleri, dijital delillerin güvenilirliğine ilişkin kabul görmüş standartlar ve uzman hukukçu görüşünde açıklanan hukuki esaslar birlikte değerlendirildiğinde;

Yalnızca görsel çıktılardan ibaret olan, teknik doğrulama imkânı sunmayan, orijinal veri ile bağlantısı kurulmamış, elde edilme süreci denetlenemeyen ve veri bütünlüğü hash değerleri ile güvence altına alınmamış dijital verilerin, tek başına güvenilir ve kesin dijital delil olarak kabul edilmesinin teknik, bilimsel ve hukuki açıdan mümkün olmadığı değerlendirilmektedir.

Belli olmayan ortamdan, belirsiz sürede, belirsiz telefonda, veya cihazdan, belirsiz tarihte, belirsiz olan uzunluğunun korunup korunmadığı belli olmayan, Cımbızla seçilmiş, aralardan çıkarılmış bütünlüğe sahip olmayan, veri sırasında eşlerin son derece mutlu oldukları ve herhengibir şikayetleri olmadığı zamanlarda ama hangi zamanlarda belirsizliği kurgulu ve seneryoya sahip ve sürekli güvenilir olmayan kayıtlarla elde edilen bu temsili görüntülerin

- **Manipülasyon Riski ve Güvensizlik:** Sunulan ekran görüntüleri, günümüz teknolojisinde (AI, Photoshop, sahte sohbet uygulamaları) saniyeler içinde gerçeğinden ayırt edilemeyecek şekilde üretilebilen, manipülasyona en açık veri türüdür. Bu verilerin meta-veriden (metadata) yoksun olması, onların doğruluğunun denetlenmesini imkansız kılmaktadır.

- **Aidiyet Sorunu (Erişim Gerçeği):** Tarafların aynı yaşam alanını paylaştığı gerçeği göz önüne alındığında, cihazın fiziksel güvenliğinin zayıflığı ve eşlerin birbirinin şifresine erişebilme ihtimali; söz konusu mesajların **Davalı tarafından değil, cihaz sahibinin (veya cihazı elinde bulunduranın) (Davacı dahi Olamayabilir Meçhul) iradesiyle oluşturulmuş olabileceği** yönünde ciddi bir teknik şüphe doğurmaktadır.
- **Delil Zinciri ve Hukuka Aykırılık:** Verilerin elde edilme yöntemi belirsiz olup, "zincirleme muhafaza" (chain of custody) kuralı ihlal edilmiştir. Yargıtay'ın yerleşik içtihatları uyarınca, kaynağı teknik olarak doğrulanamayan ve hukuka aykırı elde edilen bu tür görsel çıktıların kusur belirlemesinde dikkate alınması taraf aleyhine sonuç verebilir.
- **Bağlamdan Koparılmış Kurgu:** Dosyaya sunulan görsellerin; belirli bir zaman dilimini yansıtmayan, belli olmayan ortamlardan ve belirsiz cihazlardan elde edildiği anlaşılmaktadır. Bu kayıtların, eşlerin son derece mutlu olduğu ve herhangi bir şikayetlerinin bulunmadığı dönemlere ait veriler arasından **"cimbızla seçilerek"** çıkarıldığı, bütünlükten yoksun ve süreklilik arz etmeyen bir **kötü niyetli kurgu/senaryo** ürünü olması muhtemeldir.
- **Adli Bilişim Zorunluluğu:** Bilimsel ve teknik açıdan, bu verilerin "kesin delil" sayılabilmesi için ilgili cihazlardan adli bilişim standartlarında **"byte-to-byte imaj"** alınması ve hash değerleriyle doğrulanması şarttır. Bu prosedür işletilmeden hazırlanan iddialar, teknik bir varsayımdan öteye geçemez.
- **Hukukçu uzmanca belirtilen dijital delillerin yalnızca içerik boyutuyla değil, aynı zamanda üzerinde bulundukları fiziksel taşıyıcılar itibarıyla da değerlendirilmesi gerektiği.** Bu görüşe göre dijital veriler, tamamen soyut nitelikte olmayıp, mutlaka bir fiziksel ortam (hard disk, USB bellek, sunucu vb.) üzerinde varlık kazandıkları için, bu yönüyle ancak ve ancak **maddi delil niteliği** de taşımakta olacağı bu nedenle alındığı cihazlarında deleil ile bütün nitelikte olacağı ve birlikte sunumu veya onlardan nasıl ne şekilde koparıldığı veya byte byte nasıl alındığı ve kim tarafından alındığı (Fen adamı ,Bilişim uzmanı,Kolluk)) açık imza ve ünvan ile nacak bütünlük kazanacaktır demektedir. hal böyle ise dosyadaki temsili resmlerin **Sunulan ekran görüntülerinin;** orijinal veri niteliği taşımadığı ,Değiştirildiği,ve bu şekli ile'de, her an değiştirilebilir müdahaleye açık olduğu ve veri bütünlüğü ispatlanamadığı için **aleyhe kesin ve güvenilir bir delil olarak kabul edilmesinin teknik, bilimsel ve hukuki açıdan mümkün olmadığı fakat lehe delil olabileceği** mütalaa olunur.Heyetimizce hazırlanan UZMAN raporumuzda yapılan değerlendirmelerin dosya içerisindeki bilgi ve belgelere göre, her bir uzmanın diğerinden müstakil uzmanlık alanı çerçevesinde yaptığı bir inceleme olduğu 25.03.2026

Nihai hukuki takdir Sayın Mahkemeye ait olmak üzere, bilgilerinize arz olunur.

Saygılarımızla

Örnek Uzman 1
Bilgisayar Mühendisi

Av.Dr. Örnek Uzman 2
Örnek Üniversite Hukuk
Fakültesi Bilişim ve Usul Hukuku
Öğretim Üyesi

MEVZUAT

- Ceza Genel Kurulu, E.2017/12-243, K.2018/356, T.10.04.2018 kararında ise; 'Uzman görüşü, yargılamada taraflara eşit silah imkânı sağlayan tamamlayıcı delil niteliğindedir'
- Taraflarca sunulan uzman görüşünün dikkate alınmaması, uzman görüşü hakkında olumlu ya da olumsuz bir karar verilmemesi, uzman görüşünün neden dikkate alınmadığının gerekçesinin gösterilmemesi (mahkeme uzman görüşünü tek başına hükme esas alamaz. Ancak bu görüşün yok sayılması hukuki dinlenilme hakkının ihlali olur).
- Hukuki dinlenilme hakkının üçüncü unsuru ise kısaca dikkate alınma hakkı olarak ifade edilmektedir. Buna göre, tarafların yargılama ile ilgili bilgi sahibi kılınmaları ile açıklama yapmalarına veya delil ibraz etmelerine yahut delile ulaşmalarına imkân tanınması yeterli olmayıp, bu açıklamalar veya deliller hâkim tarafından kabul görmediği takdirde, bunun sebeplerinin yani gerekçesinin de mutlaka gösterilmesi gerekir. Bir talebin hangi kanun hükmüne, hangi hukuki sebebe dayanılarak reddedildiği gösterilirse, dikkate alınma unsuru da karşılanmış olur. Bir talebin, beyanın veya delilin neden dikkate alınıp alınmadığı ancak gerekçeden anlaşılır. Nitekim bu özel önemine binaen Anayasa'nın 141. maddesinde bütün mahkemelerin hertürlü kararının gerekçeli karar olarak yazılacağına açık şekilde işaret edilmektedir. Hukuki dinlenilme hakkı ceza muhakemesi hukuku açısından da çok büyük önem arz etmektedir; zira hukuki dinlenilme hakkı yoluyla sanık, yargılamanın objesi olmaktan çıkartılıp süjesi olma konumuna yükseltilmiş olur
- Yargıtay **15 Huk dairesi 2015/5127E, 2016/4635 KBilirkişi** raporu ile Uzman görüşünün çelişmesi halinde yeni bilirkişi raporu alınması gerekir.



TECHNICAL CONSULTANCY AND
STRATEGIC SOLUTIONS ACADEMY

- **7. Ceza Dairesi?Nin 14.06.2006 Tarih Ve 2005/13562, 2006/11585 Sayılı Kararında Aynen Şu Görüşlere Yer Verilmektedir:** Isanıklar Müdafilerinin Diyecekleri Sorulmadan Hükme Dayanak Yapılması Ve Hüküm Tarihinde İbraz Edildiği Anlaşılan Bilimsel Mütalaayı Hazırlayan Doç. Dr. Adem Sözüer?In Uzman Tanık Olarak Dinlenmesine Rağmen Bilimsel Mütalaaya Karşı Diyeceklerini Bildirmek Üzere Süre İsteyen Sanıklar Müdafilerinin Bu İstekleri Reddedilerek Savunma Hakkının Kısıtlanması Yasaya Aykırıdır
-

Yargıtay 15 HD 2015/5127 E 2016/4635 K Say 10.11.2016 Tarihli Kararda

Mahkeme Özellikle Özel Ve Teknik Bilgiyi Gerekiren Konularda Tarafın Sunduğu Uzman Görüşünün Dava Konusuyla İlgili Olması Halinde Mutlaka Değerlendirmek Zorundadır Demektedir

Yargıtay 15 HD 2015/5127 E 2016/4635 K say 10.11.2016 tarihli kararda mahkeme özellikle özel ve teknik bilgiyi gerektiren konularda tarafın sunduğu uzman görüşünün dava konusuyla ilgili olması halinde mutlaka değerlendirmek zorundadır demektedir

7. Ceza Dairesi?Nin 14.06.2006 Tarih Ve 2005/13562, 2006/11585 Sayılı Kararında Yerleşik Yargıtay İçtihatları

Yargıtay, Bu Hususun Yerine Getirilmesine Özel Önem Vermektedir. Nitekim 7. Ceza Dairesi?Nin 14.06.2006 Tarih Ve 2005/13562, 2006/11585 Sayılı Kararında Aynen Şu Görüşlere Yer Verilmektedir: Isanıklar Müdafilerinin Diyecekleri Sorulmadan Hükme Dayanak Yapılması Ve Hüküm Tarihinde İbraz Edildiği Anlaşılan Bilimsel Mütalaayı Hazırlayan Doç. Dr. Adem Sözüer'in Uzman Tanık Olarak Dinlenmesine Rağmen Bilimsel Mütalaaya Karşı Diyeceklerini Bildirmek Üzere Süre İsteyen Sanıklar Müdafilerinin Bu İstekleri Reddedilerek Savunma Hakkının Kısıtlanması Yasaya Aykırıdır?. Yeni Çıkış İle Bu Kurumun Kabul Ediliş Gerekçesi, ?Kolektif Hüküm Verilmesinde Rolü Olan Taraflara Da Bilirkişi Seçmek Yetkisini Vererek, Onların Da Teknik İstisnadan Faydalanabilmesi?[23] Ve ?Uygulamada Uzman Mütalalarının Eskiye Oranla, Daha Yakın İncelemeye Alınması Ve Bunlara Yargılamada Değer Verilmesi?[24] Olarak Açıklanmaktadır. Ceza Muhakemesine Egemen Olan ?Delil Serbestisi? İlkesine Dayandırılan Bu Yeni Kurum, Uygulamada Bilirkişilerin Denetlenmesine Hizmet Etmekte; ?Bilirkişilik Kurumunun Oto-Kontrol Sistemi? Olarak Nitelendirilmektedir[25]. Uzman Mütalaası Şeklinde Nitelendirilen Bu Özel Bilirkişilik Uygulamasının Ab Ülkeleri Hukuk Sisteminde De Mevcut Olduğu, Anglo-Sakson Hukukundan Kıta Avrupasına Ve Oradan Türk Hukukuna Girdiği Belirtilmektedir[26]. Mahkemece Seçilen (Resmî) Bilirkişiye Başvurulan Konularda, Taraflarca Özel Olarak Bir Uzmandan Alınacak Mütalâa, Bilirkişi Raporunun Hazırlanmasından Önce Veya Bilirkişi Raporunun Hazırlanması Sırasında Değerlendirilmek Üzere Kullanılabileceği Gibi; Bilirkişi Raporunun Düzenlenmesinden Sonra Ve Bilirkişi Raporu Hakkında Da Alınabilir[27], İlginç Bir Ayrıntı Da, Taraflarca Temin Edilen Bu Uzman Bilimsel Mütalaanın ?Özel Ve Teknik Bilgi? İle Sınırlı Olmaması, ?Hukuki Bilgi? Alanına Yönelik Olarak Da Kullanılabiliyor Olmasıdır[28]. Özbek?In De Yerinde Olarak Vurguladığı Gibi, Artık Hu



TECHNICAL CONSULTANCY AND
STRATEGIC SOLUTIONS ACADEMY