

BİLİŞİM HUKUKU

Elektronik Delillerin İspat Gücü

Av. Burak Üçüncü · 23 Mayıs 2025 · 17 dk okumaGüncelleme: 25 Mayıs 2025

Geleneksel hukuk sistemlerinde delil, çoğu zaman fiziksel bir varlıkla özdeşleştirilmiş; tanık beyanı, yazılı belge, noter tasdiki veya görsel kayıt gibi unsurlar üzerinden değerlendirilmiştir. Ancak dijitalleşmenin hayatın her alanını dönüştürmesiyle birlikte, artık hukuki uyumsuzluklarda sunulan delillerin büyük bir kısmı elektronik nitelik taşımaktadır. WhatsApp yazışmaları, e-posta, sunucu logları, IP kayıtları, kamera sistemlerinin dijital çıktılarına kadar geniş bir yelpazede karşımıza çıkan bu yeni delil türü, geleneksel ispat araçlarına kıyasla farklı riskler, avantajlar ve teknik incelikler barındırmaktadır.

Türk hukukunda elektronik deliller, hem ceza hem de özel hukuk yargılamalarında gitgide artan oranda kullanılmakta, hatta bazı davalarda tek ve en önemli delil türü olarak karşımıza çıkmaktadır. Ne var ki elektronik verilerin kolay üretilebilir ve değiştirilebilir olması, bunların güvenilirlik kriterleri açısından ayrıca değerlendirilmesini gerektirmektedir. Üstelik yalnızca delilin kendisi değil, elde ediliş yöntemi, muhafazası, karşı tarafa sunulma biçimi ve mahkemece değerlendirilmesi de başlı başına hukuki tartışma konusudur.

Elektronik delillerin ispat hukukunda giderek daha merkezi bir yere oturduğu bu yeni dönemde, hem delil sunan tarafın hem de delile itiraz edenin, teknik bilgiyle donanmış bir hukuki muhakeme gücüne sahip olması gereklidir. Aksi takdirde, dijital çağın en güçlü araçlarından biri, aynı zamanda en zayıf halkaya dönüşebilir.

BÖLÜM II

Elektronik Delilin Tanımı ve Özellikleri

Yargılamalarda başvuru delil türlerinden biri olan elektronik delil, tanım itibarıyla klasik delil anlayışının ötesinde, kendine özgü yapısal ve teknik niteliklere sahiptir. Elektronik delil kavramını sağlıklı şekilde değerlendirebilmek için öncelikle bu delilin dayanağını oluşturan elektronik verinin ne olduğunu ortaya koymak gerekir.

Elektronik veri; doğrudan gözle görülemeyen, yalnızca elektriksel bir akım vasıtasıyla anlam kazanan, elektrik kesildiğinde ise görünürlüğünü kaybeden dijital nitelikteki bilgidir. Bu veriler, sabit disk, SSD, mobil cihaz hafızası, USB bellek, hafıza kartı gibi fiziksel ortamlar üzerinde "sayıların dili" olarak da bilinen ikili sistemle (binary – 1 ve 0) kodlanarak saklanır. Bu haliyle, fiziksel bir biçimden ziyade, sayısal bir varlık olarak değerlendirilir.

Elektronik delil kavramı, yalnızca bir bilişim cihazını değil, o cihazda üretilen, kaydedilen, işlenen ya da iletilen bütün dijital verileri kapsayan geniş bir hukuki terimdir. Bu yönüyle "dijital delil" kavramını da içine alır ve daha bütüncül bir çerçeve sunar. Adli bilişim bilimi ise, bu verilerin elde edilmesi, incelenmesi ve mahkemede kullanılabilir hâle getirilmesiyle ilgilenen özel bir uzmanlık alanıdır.

Elektronik delilleri klasik (fiziki) delillerden ayıran ve ispat hukukunda ayrı bir değerlendirme gerektiren bazı belirgin nitelikler bulunmaktadır:

1. Gizli (Latent) Yapı: Elektronik deliller çoğu zaman doğrudan görülemez. Verinin varlığı fark edilse bile içeriğine erişim özel bilgi ve teknik donanım gerektirir. Bu nedenle delilin ortaya çıkarılması, elde edilmesi ve sunulması özel yazılımlar, donanımlar ve uzman müdahalesi ile mümkündür.

2. Kolay Kopyalanabilirlik: Elektronik veriler, klasik belgelerden farklı olarak birden çok defa, içerik açısından birebir kopyalanabilir. Bu durum, mahkemede "hangi veri asıl delildir" sorusunu gündeme getirir ve delilin bütünlüğünün teknik yollarla garanti altına alınmasını zorunlu kılar.

3. Değiştirilebilirlik ve Tahrife Açıklık: Elektronik veriler, doğaları gereği son derece kırılgandır. Basit bir yazılım müdahalesiyle kolayca değiştirilebilir ya da silinebilirler. Aynı zamanda manyetik alan, nem, ısı gibi çevresel etkenlerden de etkilenmeleri mümkündür. Bu nedenle elde edildikleri andan itibaren zincirleme bütünlük ilkesine uygun şekilde muhafaza edilmeleri gerekir.

4. Gizlenebilirlik ve Şifreleme İmkânı: Elektronik deliller, yalnızca görünür veriyle sınırlı değildir. Gelişmiş kriptografi yöntemleriyle şifrelenmiş, sıkıştırılmış veya saklanmış veriler barındırabilir. Bu tür verilerin varlığı ancak özel analiz yöntemleriyle tespit edilebilir.

5. Tamamen Yok Edilmesinin Zorluğu: İlginç bir biçimde, elektronik veriler tamamen ortadan kaldırılmak istendiğinde, bu genellikle başarılı olmaz. Silinmiş veriler, adli bilişim teknikleriyle geri getirilebilir. Bu yönüyle elektronik delil, fiziki delillerden ayrılarak "geri döndürülebilir kanıt" özelliği taşır.

Adli bilişim biliminin ilgi alanı artık yalnızca masaüstü bilgisayarlarla sınırlı değildir. Sunucular, e-posta sistemleri, veri tabanları, mobil cihazlar, tabletler, ağ geçitleri, bulut sistemleri, çevrimiçi uygulamalar ve nesnelerin interneti (IoT) gibi platformlar da adli analiz kapsamında değerlendirilmekte, elektronik delil üretme ve inceleme süreçleri çok daha karmaşık bir hâl almaktadır.

Elektronik delilin doğası gereği taşıdığı bu teknik ve hukuki farklılıklar, onu hem potansiyel olarak güçlü bir ispat aracı hem de yüksek dikkat gerektiren bir risk alanı hâline getirir. Bu nedenle delilin ispat gücü ve güvenilirliği, yalnızca içeriğine değil, elde ediliş biçimine, değişime uğrayıp uğramadığına, teknik doğrulamasının yapılmış olup olmadığına göre değerlendirilmelidir.

BÖLÜM III

Türk Hukukunda Elektronik Delilin Niteliği ve İspat Vasıtası Olarak Yeri

Hukuk Muhakemeleri Kanunu (HMK), elektronik ortamdaki verileri ve bunlara benzer bilgi taşıyıcılarını açıkça "belge" olarak kabul etmiştir. HMK m.199 hükmü, "Uyuşmazlık konusu vakıaları ispata elverişli yazılı veya basılı metin, senet, çizim, plan, kroki, fotoğraf, film, görüntü veya ses kaydı gibi veriler ile elektronik ortamdaki veriler ve bunlara benzer bilgi taşıyıcıları bu Kanuna göre belgedir" şeklindedir. Bu geniş tanım sayesinde, elektronik verilerin hukuk yargılamasında delil olarak kullanılmasının önü açılmıştır.

Elektronik delil tabiri, bir delilin *tipini* (senet, tanık gibi) değil, onun *oluşturulma* ve *iletilme biçimini* tanımlar.

Hukukumuzda deliller, ispat gücüne göre tasnif edilmekte olup, temel olarak kesin deliller ve takdiri deliller olmak üzere ikiye ayrılır. Kesin deliller, hakim açısından bağlayıcı nitelikte olup, kanunda özel olarak belirtilmiş veya ispat gücü yüksek olan delillerdir. Takdiri deliller ise hakimin serbestçe takdir edeceği

delillerdir. Elektronik delilin ispat gücü, doğrulama mekanizmalarının varlığına ve güvenilirliğinin ispatına bağlı olarak bu ayrıma tabi tutulur.

5070 sayılı Elektronik İmza Kanunu ve Türk Borçlar Kanunu (TBK) m.15, güvenli elektronik imza ile oluşturulan belgelerin elle atılmış imza ile aynı sonuçları doğuracağını hükme bağlamıştır. HMK m.205/2 de, usulüne göre güvenli elektronik imza ile oluşturulan belgelerin senet hükmünde sayılacağını açıkça düzenlemiştir. İcra ve İflas Kanunu (İİK) m.8/a da benzer bir düzenleme içermektedir. Kayıtlı Elektronik Posta Sistemi'ne (KEP) ilişkin hizmet sağlayıcı tarafından tutulan kayıtlar da HMK m.205 f.2 ve KEP Yönetmeliği m.15 uyarınca senet hükmünde kabul edilmektedir. Bu belgelerin "senet hükmünde" kabul edilmesi, onların **kesin delil** niteliği taşıdığı anlamına gelir. Güvenli elektronik imza ve KEP, elektronik belgenin aidiyetini, bütünlüğünü ve gönderilip gönderilmediğini (KEP özelinde) büyük ölçüde garanti altına aldığı için bu yüksek ispat gücüne sahiptir.

Esas olan ve ispat hukuku açısından değer taşıması gereken, elektronik verinin bulunduğu asıl ortamdır. Elektronik belgelerin çıktısı, belgenin yazılı şekilde cisim bulmuş bir kopyasıdır. Çıktı alındığında, veriye ilişkin üstveri (oluşturulma tarihi, kim tarafından oluşturulduğu vb.) veya varsa elektronik imza gibi tüm kritik bilgiler genellikle görünmez. Bu durum, çıktının güvenilirliği ve bütünlüğü konusunda şüpheler yaratır. Güvenli e-imzalı belgenin basılı çıktısı veya taranmış hali, belgede imza doğrulaması yapmaya imkan tanımaz. İbraz mümkün olduğunca elektronik ortamda yapılmalıdır.

BÖLÜM IV

Elektronik Delilin Güvenilirlik ve Geçerlilik Şartları

Bir elektronik verinin mahkeme huzurunda delil olarak kabul edilebilmesi, yalnızca teknik bir kayıt olmasıyla değil; aynı zamanda belirli hukuki ve adli kriterleri karşılamasıyla mümkündür. Elektronik delilin ispat gücünden söz edilebilmesi için, aşağıda yer verilen temel şartların sağlanmış olması gerekir:

1. Hukuka Uygunluk (Kabul Edilebilirlik):

Delilin elde edilme süreci, hem maddi hukuka hem de usul hukukuna uygun olmalıdır. Hukuka aykırı yollarla elde edilen bir veri — örneğin gizlice kayda alınan bir konuşma, yasa dışı erişimle elde edilmiş bir e-posta içeriği — Türk hukuk sisteminde genel kural olarak delil niteliği taşımaz. Bu ilke, HMK m.189/2 ve CMK m.206/2-a'da açıkça yer bulmuştur.

2. Özgünlük ve İlliyet Bağ:

Sunulan delilin, somut olayla doğrudan ilgili olması; yani olayla arasında açık bir nedensellik bağının kurulabilmesi gerekir. Verinin neye delil teşkil ettiği açık olmalı; varsayım ya da dolaylı ima ile yetinilmemelidir. Elektronik delil, doğrudan ihtilaf konusu olguya temas etmelidir.

3. Bütünlük ve Değişmezlik:

Elektronik delilin elde edildiği ilk andan itibaren herhangi bir şekilde değiştirilmediğinin ya da müdahale edilmediğinin teknik yollarla doğrulanabilir olması gerekir. Bu kapsamda, zaman damgası (timestamp), hash değerleri (SHA-256, MD5 gibi) ve zincirleme bütünlük raporları, delilin muhafazasında kritik rol oynar. Delil bütünlüğü zedelenmiş bir veriye güvenilemez.

4. Güvenilirlik ve İzlenebilirlik:

Delilin hangi kaynaktan, hangi yöntemle, hangi kişi veya sistem aracılığıyla elde edildiği açıkça belgelenmelidir. Delilin aidiyeti, zaman bilgisi, cihaz türü gibi teknik meta veriler, şüpheye yer vermeyecek

şekilde ortaya konmalıdır. Aynı veri, farklı uzmanlarca incelendiğinde aynı sonucu veriyorsa, bu güvenilirliğin bir göstergesidir.

5. İnandırıcılık ve Anlaşılabilirlik:

Sunulan elektronik delil, mahkeme heyetince anlaşılabilir ve yorumlanabilir olmalıdır. Karışık, teknik jargona boğulmuş, neye delalet ettiği izah edilemeyen bir veri, karar vericinin kanaatini etkilemez. Delilin mahkeme önünde akla, mantığa ve hayatın olağan akışına uygun şekilde sunulması, ispat gücünü doğrudan etkiler.

Elektronik deliller, doğaları gereği hassas, kırılgan ve müdahaleye açık yapıdadır. Bu nedenle klasik delillerden farklı olarak, teknik müdahale süreci başlı başına bir hukukî sürece dönüşür. Delilin elde edilmesi, muhafazası, çözümlemesi ve sunumu, belirli standartlar çerçevesinde yürütülmediği takdirde, delilin ispat gücü zayıflar; hatta hukuken hiç sayılabilir. Dolayısıyla elektronik delil sunan tarafın yalnızca veriyi paylaşması değil; bu verinin nasıl elde edildiğini, neden güvenilir olduğunu ve neden somut uyuşmazlıkla ilgili olduğunu hukuken gerekçelendirmesi gerekir. Özellikle özel hayatın gizliliği, haberleşmenin gizliliği ve kişisel veri güvenliği gibi hukuki sınırlar gözetilmeden elde edilmiş elektronik kayıtlar, delil değil, ihlal konusu hâline gelebilir.

Elbette Burak. Aşağıda, verdiğin metni bir bilişim hukukçusunun üslubuyla yeniden kurguladım. Anlatımı daha doğal, sistematik ve gerekçeli hâle getirirken, teknik açıklamaları hukuki bağlama oturttum:

BÖLÜM V

Elektronik Delillerde Güvenilirliğin Sağlanması ve Doğrulama Mekanizmaları

Bir elektronik verinin delil değeri taşıyabilmesi, yalnızca varlığına değil; elde ediliş süreci, içeriği, değiştirilip değiştirilmediği ve dava konusu olayla ilişkisine dair tüm yönleriyle güvenilirliğinin ortaya konmasına bağlıdır. Bu güvenilirlik, hem teknik hem de hukuki bazı doğrulama yöntemlerinin birlikte kullanılmasıyla mümkündür.

Teknik Güvenlik Araçları

1. Hash Değeri (Özet Değer):

Hash, bir elektronik verinin bütünlüğünü doğrulamak için kullanılan matematiksel bir “parmak izi”dir. Dosya üzerinde herhangi bir değişiklik yapıldığında hash değeri de otomatik olarak değişir. Bu nedenle delilin ilk elde edilme anında ve bilirkşi incelemesinden hemen önce alınan hash değerlerinin karşılaştırılması, delilin süreç boyunca bozulmadığını ortaya koyar. Özellikle adli bilişim raporlarında bu değerlerin yer alması, verinin hukuki bütünlüğünün teknik teminatıdır.

2. Zaman Damgası:

Zaman damgası, bir verinin belirli bir tarih ve saatte var olduğunu ispatlayan elektronik bir mühürdür. Delilin oluştuğu anı sabitlemek açısından önemlidir. E-imza sistemleri ve Kayıtlı Elektronik Posta (KEP) gibi araçlarla birlikte kullanıldığında, delilin geçmişe dönük oluşturulmadığını ortaya koyma yönünden yüksek ispat gücüne sahiptir.

3. Delil Zinciri:

Elektronik verinin elde edildiği andan itibaren kimlerin elinden geçtiği, hangi ortamda saklandığı, ne zaman, nerede, nasıl incelendiği ve mahkemeye nasıl sunulduğu ayrıntılı biçimde kayda alınmalıdır. Bu sürece “delil

güvenlik zinciri" denir. Zincirin herhangi bir halkasında şüphe oluşursa, delilin bütünlüğü de tartışmalı hâle gelir. Özellikle ilk müdahale anı bu açıdan kritik öneme sahiptir.

4. Üstveri (Metadata):

Elektronik belgelerin ne zaman oluşturulduğu, kim tarafından üretildiği, ne zaman değiştirildiği gibi bilgileri içeren teknik veri katmanıdır. Delilin zaman ve kişiyle ilişkisini ispatlamak bakımından önemlidir. Bilgisayar sistemlerinde, e-postalarda, dijital fotoğraflarda ve belgelerde bu tür üstveri doğrudan tespit edilebilir.

Hukuki ve Usuli Doğrulama Yolları

1. Tarafların Beyanı ve Hakimin İncelemesi:

Hukuk Muhakemeleri Kanunu m.210 ve devamı maddeleri uyarınca, mahkeme, delilin içeriği ve kaynağı konusunda tarafları dinleyerek, elektronik verinin aidiyetini ve elde ediliş biçimini değerlendirebilir. Bu, delilin en temel güvenilirlik kontrolüdür.

2. Adli Bilişim Bilirkişiliği:

Elektronik verilerin teknik açıdan incelenmesi ve güvenilirliklerinin saptanmasında en etkili yöntem, bilirkişi incelemesidir. Adli bilişim bilirkişisi, delilin:

- Gerçekliğini,
- Bütünlüğünü,
- Kaynağını,
- Değişime uğrayıp uğramadığını

uzmanlık bilgisiyle değerlendirir. Bu incelemenin uluslararası standartlara (örneğin ISO 27037, NIST 800-86) uygun yürütülmesi, yargılama sürecine doğrudan etki eder.

Unutulmamalıdır ki, bilirkişilik yalnızca teknik uzmanlık değil; aynı zamanda adli muhakeme mantığını bilen, delilin hukuki sonuçlarını da kavrayabilen kişiler tarafından yürütülmelidir. Aksi hâlde rapor, yalnızca teknik bir analizle sınırlı kalır ve yargılama bakımından yetersiz olur.

3. Uzman Görüşü (Tarafta Bilirkişiliği):

HMK m.293 çerçevesinde taraflar, kendi seçtikleri adli bilişim uzmanlarından mütalaa alabilirler. Bu uzman görüşü, hâkime teknik konularda yol gösterici olur. Tarafta bilirkişi raporları, delil niteliğinde değilse de, hâkimin kanaat oluşturmada etkili olabilir. Ancak bu mütalaaların masrafı talep eden tarafa aittir ve yargılama gideri kapsamında değerlendirilmez.

4. Elektronik Keşif:

HMK m.288 ve devamı maddeleri uyarınca hâkim, delilin fiziksel olarak yerinde incelenmesine veya elektronik keşif yapılmasına karar verebilir. Bu durum özellikle:

- Kurumsal sunucularda saklanan veriler,
- Bulut tabanlı sistemlerde yer alan dijital belgeler,
- Büyük veri kümeleri (big data)

için tercih edilir. Elektronik keşif sırasında adli bilişim uzmanının hazır bulunması, hem teknik doğrulama açısından hem de sürecin kayıt altına alınması açısından önem taşır.

Sonuç olarak, bir elektronik verinin delil niteliği taşıyabilmesi, yalnızca ne içerdiğiyle değil, **nasıl elde edildiği, kim tarafından işlendiği ve değiştirilip değiştirilmediği** ile doğrudan ilgilidir. Bu nedenle güvenilirliğin sağlanması, teknik araçlarla hukuki usullerin birlikte işletildiği bir doğrulama süreci gerektirir. Bu sürece dair en küçük ihmal, delilin geçerliliğini zedeleyebilir; buna karşılık, eksiksiz belgelenmiş ve teknik olarak doğrulanmış bir elektronik delil, mahkeme nezdinde yüksek ispat gücüne sahip olacaktır.

BÖLÜM VI

Hukuka Aykırı Yollarla Elde Edilen Elektronik Deliller

Elektronik delillerin yargılamada kullanımına ilişkin en tartışmalı meselelerden biri, söz konusu delilin hangi yöntemle elde edildiği ve bu yöntemin hukuka uygunluk taşıyıp taşımadığıdır. Zira bir verinin içeriği ne kadar açık, ne kadar etkileyici olursa olsun, eğer hukuka aykırı şekilde elde edilmişse, bu durum delilin ispat gücünü doğrudan ortadan kaldırabilir.

Hukuk Muhakemeleri Kanunu'nun 189. maddesinin 2. fıkrası bu konuyu açık biçimde düzenlemiştir:

"Hukuka aykırı şekilde elde edilmiş deliller, bir vakıanın ispatında dikkate alınamaz."

Ancak buradaki asıl sorun, bir delilin ne zaman ve hangi koşullarda hukuka aykırı sayılacağına dair kanunda açık ve genel geçer bir kriterin bulunmamasıdır. Bu nedenle uygulamada değerlendirme çoğu zaman somut olayın özelliklerine göre hâkimin takdirine bırakılmıştır.

Özellikle elektronik deliller bakımından bu konuda doktrinde iki temel görüş öne çıkar:

1. Mutlak Yasağa Dayanan Görüş:

Bu yaklaşıma göre, hukuka aykırı şekilde elde edilmiş delillerin yargılamada hiçbir şekilde kullanılmasına izin verilmemelidir. Gerekçe olarak, hukuka aykırılık kabul edildiğinde delilin sunulması, meşrulaştırıcı etki yaratacağından, bu durum hukukun üstünlüğüne zarar verir.

2. Göreli Yasak ve Dengeleme Görüşü:

Bu yaklaşım ise delilin elde ediliş yönteminin değil, delilin kendisiyle ilgisinin esas alınması gerektiğini savunur. Bazı hâllerde delilin elde edilişinde küçük usul eksiklikleri ya da üçüncü kişinin rızası gibi durumların, delilin tamamının dışlanması haklı kılmayacağı görüşündedir. Özellikle dürüstlük kuralı, hakkın kötüye kullanılması yasağı ve ispat hakkı bu değerlendirmede dikkate alınır.

Bu bağlamda bazı hukukçular, "delilin elde ediliş süreci ne kadar ağır bir temel hakkı ihlal ediyorsa, o delilin yargılamaya katılması da o ölçüde yasaktır" görüşünü savunur. Buradaki ölçüt, delilin elde edilmesiyle elde edilen bilginin orantılı olup olmadığıdır.

Yargıtay içtihatları da zaman zaman bu konuda farklı eğilimler göstermiştir. Özellikle özel hayatın gizliliği ile hak arama özgürlüğü arasındaki dengenin kurulmasında somut olayın şartlarına göre değerlendirme yapılmaktadır.

Yargıtay Hukuk Genel Kurulu'nun 26.03.2002 tarihli, 2002/2-617 E., 2002/648 K. sayılı kararında, boşanma davasına konu bir olayda, eşin, birlikte yaşadıkları evde diğer eşin kişisel eşyaları arasında bulunduğu özel nitelikteki belgeleri mahkemeye sunması hukuka aykırı kabul edilmemiştir. Gerekçede, tarafların aynı çatı altında yaşadığı, özel alanların net çizgilerle ayrılmadığı ve eşlerin birbirlerinin eşyalarına erişim imkânı

bulunduđu belirtilmiřtir. Buradan hareketle, birlikte yařanan mekânda elde edilen bir verinin mutlak řekilde özel hayat ihlali sayılabileceđi vurgulanmıřtır.

Ancak bu yaklařım mutlak deđildir. Aynı kararda, eřin diđer eře ait özel bir mesajlařmayı onun bilgisi ve rızası dıřında, dıř kaynaklı bir cihazdan (örneğin bulut hesabından ya da yedeklemesinden) alarak mahkemeye sunması hâlinde bunun hukuka aykırı sayılabileceđi belirtilmiřtir. Çünkü burada artık yalnızca ortak yařam alanı deđil, kiřinin özel dijital mahremiyet alanı ihlal edilmektedir.

İřverenin iřçisine ait özel mesajları veya kamera kayıtlarını rızası olmaksızın kaydetmesi ve bunları delil olarak sunması da sıklıkla gündeme gelen bir diđer durumdur. Bu tür olaylarda Yargıtay, deđerlendirmeyi genellikle řu kriterlere göre yapmaktadır:

- İřverenin gözetim ve denetim yetkisi sınırında mı hareket ettiđi?
- İřçiye bu gözetimin yapıldıđı önceden bildirilmiř mi?
- Elde edilen kayıt açıkça özel hayatın gizli alanını mı ihlal ediyor?

Eđer iřveren, haber vermeden iřçinin sesini ya da görüntüsünü kayda almıř ve bu kayıt bir suçu ortaya koyma dıřında bir amaca hizmet ediyorsa, Yargıtay çoğunlukla bu tür kayıtların hukuka aykırı delil niteliđinde olduđunu kabul etmekte ve mahkemede kullanılmasına izin vermemektedir.

Kısacası, elektronik delillerde hukuka aykırılık denetimi, sadece teknik kurallara bađlı bir mesele deđildir. Her somut olayda;

- **delilin elde ediliř yöntemi,**
- **verinin içerdıđi bilginin ađırlıđı,**
- **taraflar arasındaki hukuki iliřki,**
- **ve ihlalin temel haklara etkisi**

birlikte deđerlendirilmelidir. Aksi hâlde ya hak arama özgürlüğü zarar görür ya da özel hayatın dokunulmazlıđı hiçe sayılır. Hukukun amacı, bu iki hakkı dengeli biçimde koruyabilmektir.

BÖLÜM VII —

Elektronik Belgelerin Mahkemeye Sunulması ve İbrazı

Hukuk Muhakemeleri Kanunu m.219, belgenin ibrazına iliřkin genel hükümleri düzenlerken, elektronik belgeler de bu kapsamda deđerlendirilmektedir. Bu çerçevede, elektronik nitelikteki verilerin yargılamaya konu edilmesi hâlinde, belgenin çıktı alınmıř bir örneđiyle birlikte, mahkemece gerekli görölmesi hâlinde orijinal elektronik formatta da sunulması gerekir. Buradaki amaç, belgenin incelenebilirliđini ve içeriđinin tarafsız biçimde deđerlendirilebilirliđini sađlamaktır.

Tarafların Delil Bildirme Yükümlölüğü ve Somutlařtırma

Taraflar, dayandıkları delilleri — elektronik belgeler dâhil olmak üzere — HMK m.119 ve 129 hükümleri uyarınca dava ve cevap dilekçelerinde açıkça belirtmek ve bu belgeleri, dilekçelerin karřılıklı verilmesi süreci içinde mahkemeye sunmakla yükümlüdürler. Elleriinde bulunmayan belgeler hakkında ise HMK m.194 uyarınca:

- Hangi belgelerin istenildiğini,
- Bu belgelerin kimde bulunduğunu,
- Ve ilgili belge ile neyin ispatlanmak istendiğini

açıkça ifade etmeleri gerekir. Bu, taraflarca getirilme ilkesi ile somutlaştırma yükümlülüğünün doğal bir sonucudur. Aksi hâlde yargılamanın belirsizleşmesi ve delil disiplininin zayıflaması söz konusu olur.

Dilekçeler aşaması geçildikten sonra, genel kural olarak artık yeni delil sunulamaz. Bu, yargılamada teksif ilkesinin (delillerin bir defada ve eksiksiz sunulması gerekliliği) bir sonucudur. Ancak HMK m.145 gibi istisnai hükümler, bazı durumlarda delil bildiriminin gecikmeli yapılmasına imkân tanır (örneğin, belgenin daha sonra elde edilmesi veya varlığından yeni haberdar olunması gibi durumlar).

Elektronik Belgenin Aslının İncelenmesi ve Üçüncü Kişiden İbraz

HMK m.219/2'ye göre, mahkeme, gerek re'sen gerekse taraflardan birinin talebi üzerine, bir belgenin — elektronik belge dâhil — aslının incelenmesine karar verebilir. Elektronik belge söz konusu olduğunda, bu “asıl”dan kasıt, çoğunlukla verinin orijinal dijital dosya formatı (örneğin .eml uzantılı bir e-posta veya sistem log dosyası) olacaktır.

Bu noktada HMK m.220 ve 221 hükümleri devreye girer. Söz konusu hükümler, gerek karşı tarafta gerekse üçüncü bir kişide bulunan belgenin ibrazını konu edinir. Belge sahibi kişi, mahkemece verilen ibraz kararına uygun hareket etmekle yükümlüdür. Ancak burada önemli bir ayrım yapılmalıdır:

- **İbraz yükümlülüğü bir zorunluluk değil**, yerine getirilmediği takdirde **aleyhe sonuçlara katlanılacak bir usuli yüküdür**.
- Mahkeme, ibraz etmeyen taraf veya üçüncü kişi aleyhine delil değerlendirmesi yapabilir; ancak doğrudan zorlama uygulayamaz (disiplin yaptırımları hariç).

Kişisel Veri Niteliğindeki Elektronik Belgelerin İbrazi

Elektronik bir belge içeriğinde kişisel veriler yer alıyorsa, bu durumda ibraz yükümlülüğü Anayasa m.20 ve Türk Medeni Kanunu m.23 ve devamı hükümleri çerçevesinde özel bir değerlendirmeye tabi tutulmalıdır. Her ne kadar kişisel verinin varlığı ibrazdan kaçınmayı mutlaklaştırmasa da, şu ilkeler dikkate alınır:

- **Özel hayatın gizliliği ve kişilik hakkının sınırları**
- Kişisel verinin işlenmesinin **kanuni zorunluluğa dayanıp dayanmadığı**
- Kamu yararı veya yargılama faaliyetinin gerekliliği gibi **hukuka uygunluk sebeplerinin varlığı**

Bu kapsamda, örneğin bir sosyal medya mesajının, e-posta yazışmasının ya da işyeri sisteminde tutulmuş bir personel bilgisinin ibrazı isteniyorsa; veri sahibinin açık rızası yoksa, ancak hâkimin orantılılık ve zorunluluk ilkelerine dayanarak verdiği bir kararla bu veri ibraz edilebilir. Yani özel hayatın korunması, yargılamayı mutlak şekilde kilitleyen bir engel olarak görülmemelidir; ancak sınırsız da değildir.

Büyük Hacimli Elektronik Verilerde Örneklem Yöntemi

Elektronik delillerin çoğu zaman yüksek hacimli veri setlerinden oluşması, mahkemeye ibraz sürecinde teknik zorluklar doğurabilir. Örneğin bir sunucu kaydının tamamının mahkemeye sunulması veya

yedeklenmiş bir diskin her dosyasının ayrı ayrı incelenmesi hem taraflar hem de bilirkişilik açısından ciddi zaman ve kaynak maliyeti doğurur.

Bu tür durumlarda, uluslararası uygulamalarda da yaygın biçimde kabul gören örnekleme (sampling) yöntemi, Türk hukukunda da uygulanabilir bir yaklaşımdır. Hakim veya bilirkişi, sistemli ve tarafsız bir biçimde seçilecek veri dilimleri üzerinde inceleme yaparak, delilin bütünü hakkında çıkarım yapabilir. Önemli olan, örneklemenin:

- Tesadüfi değil; somut olayla ilişkili olarak metodolojik yapılması,
- Taraflara denetim imkânı sunacak biçimde şeffaf yürütülmesi,
- Teknik raporla desteklenmesi

şartlarına uygun biçimde gerçekleştirilmesidir.

Sonuç olarak, elektronik belgelerin mahkemeye sunumu, yalnızca bir belgenin çıktısının alınarak dosyaya eklenmesiyle sınırlı bir işlem değildir. Bu süreç, hem teknik güvenilirliği hem de hukuki geçerliliği birlikte gözeten; usuli hakları, özel hayatı ve ispat düzenini dengeleyen bir yargılama aracıdır. Elektronik delillerin ibrazında yapılacak her tercih, bir yandan adil yargılanma hakkına, diğer yandan kişisel hakların ihlal edilmemesi ilkesine temas eder. Bu nedenle hem uygulayıcıların hem de taraf avukatlarının, ibraz sürecine sadece içerik değil, şekil ve yöntem bakımından da hâkim olması zorunludur.

Elbette Burak. Aşağıda, verdiğin paragrafı daha güçlü, sistematik ve hukukçunun üslubuna uygun biçimde yeniden yazdım. Gerekli yerlerde kavramsal netlik sağladım ve iç tutarlılığı artırdım:

BÖLÜM VIII —

Değerlendirme

Elektronik deliller, çağdaş yargılamanın ayrılmaz bir parçası hâline gelmiş ve artık yalnızca teknik uzmanların değil, hukukçuların da doğrudan temas ettiği bir delil türü olarak öne çıkmıştır. Hukuk Muhakemeleri Kanunu, güvenli elektronik imza ve KEP gibi araçları “senet” hükmünde belge olarak kabul etmekle, elektronik verilerin delil niteliğini yasal zemine oturtmuştur. Ancak bu normatif çerçevenin işlerlik kazanabilmesi için, elektronik delillerin güvenilirliği konusunda ortaya çıkan her şüphenin teknik ve hukuki denetime açık şekilde çözümlenmesi gerekir.

Bu noktada, adli bilişim incelemeleri vazgeçilmezdir. Çünkü elektronik bir verinin, hangi yöntemle elde edildiği, üzerinde oynama yapıp yapılmadığı, gerçekliğiyle ihtilaf konusu arasında nasıl bir illiyet bağı kurduğu, çoğu zaman yalnızca teknik analizle ortaya konulabilir. Özellikle verinin elde edilmiş biçimi hukuka aykırıysa, ya da bütünlüğü bozulmuşsa, bu delilin ispat gücünden söz etmek mümkün olmayacaktır.

Bu nedenle bilirkişi olarak görevlendirilecek adli bilişim uzmanlarının yalnızca teknik yeterlilikle sınırlı kalmaması, aynı zamanda hukuki süreçleri ve delil değerlendirme standartlarını da anlamlandırabilecek bir yetkinliğe sahip olması gerekir. Teknik veri, ancak doğru bir hukuki bağlam içinde yorumlandığında hükme esas olabilir.

Ayrıca [bilişim avukatları](#) ve hâkimler başta olmak üzere tüm hukuk uygulayıcılarının, elektronik delillerin taşıdığı teknik karmaşıklıkla hukuki inceliklerin iç içe geçtiği bu alanda bilinçli hareket etmeleri, yargılamanın sağlığı açısından elzemdir. İbraz edilen belgelerin yalnızca yazıcı çıktılarıyla yetinilmemeli; verinin elektronik

ortamda, bütünlüğü korunarak ve doğrulanabilir şekilde sunulması sağlanmalıdır. Gerek duyulduğunda, gecikmeksizin uzman görüşüne başvurulmalı; aksi hâlde delilin hem güvenilirliği hem de geçerliliği tartışmalı hâle gelecektir. Sonuç olarak, elektronik delillerin yargılama sürecinde etkin ve güvenli bir biçimde kullanılabilmesi için; hukuk ve teknolojinin birlikte çalıştığı, [disiplinlerarası bir yaklaşımın benimsenmesi](#) gerekmektedir. Bu yaklaşım yerleştiği ölçüde, elektronik deliller hem usule hem de maddi gerçeğe daha sağlıklı biçimde hizmet edecektir.

Çevrimiçi sürüm: <https://burakucuncu.com.tr/elektronik-delillerin-ispata-gucu>