Dijital Delil ve İletişimin Denetlenmesi*

(Digital Evidence and Supervision of Communication)

Çetin ARSLAN**

Öz

"Dijital delil" kavramı ceza muhakemesi hukukunda yeni bir kavramdır. Kısaca *"iddia edilen bir fiilin ispatında kullanılmak istenen veya kullanılan; elektronik ortamda oluşan/ oluşturulan, değiştirilen, iletilen veya saklanan veri, kayıt ve belgeler"*i ifade eden ve "delil" vasfını haiz olduğuna şüphe bulunmayan dijital deliller "sayısal veriler" şeklinde oluşturulmakta ve bu yönü ile "güvenilirlik" bakımından, uygulamada, birtakım sorunları da beraberinde getirmektedir. Delil serbestîsi ilkesi gereği -diğer tüm deliller gibi- maddî gerçeğin ortaya çıkarılmasına hizmet eden bu delillerin hukuka uygun yollardan elde edilmesi zorunlu olup konuya ilişkin CMK md. 134-138 hükümlerinin tadil edilmesinde kanaâtimizce fayda vardır. Nihayet, uygulamadaki sorunların hâlli bakımından bir "adlî bilişim kurumu"nun kurulması son derece isabetli olacaktır.

Anahtar Kelimeler: Dijital/Elektronik Delil, Ceza Muhakemesi, İspat Hukuku

---

* Geliş Tarihi: 29. 10. 2015, Kabul Tarihi: 21.12.2015

** *Prof. Dr., Hacettepe Üniversitesi Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku ABD Başkanı, Hacettepe Üniversitesi Beytepe Yerleşkesi Yenimahalle/ANKARA, cetinarslan@hacettepe.edu.tr.*

Abstract

The concept of "digital evidence" is a new concept in criminal procedure law. Digital evidences which correspond to *"data, records and documents created/modified/saved in electronic environment and used for investigation of a criminal act"* are generated in the form of "numerical data" and -thus- lead to several problems in practice in terms of "reliability". It is needed to gather digital evidence duly (in accordance with legal requirements), which -like all other evidence- serve to reveal the material facts, as a result of the principle of freedom of evidence. It must be stated that art. 134-138 of (Turkish) Criminal Procedure Code should be partially amended, and an instution specialized in the area of digital forensics ought to be constituted for tackling problems in practice.

Keywords: Digital/Electronic Evidence, Criminal Procedure, Law of Evidence

GİRİŞ

Değerli katılımcılar, öncelikle hepinizi saygıyla selamlıyorum. Efendim sunumum, *"Dijital Delil ve İletişimin Denetlenmesi"* başlığını taşıyor[1]. Konunun her açıdan oldukça önemli olduğunu düşünüyorum. Zira ***"delil"*** kavramı ceza muhakemesinin temelidir, bel kemiğidir. Diğer taraftan **dijital delil, sayısal delil** veya **elektronik delil** denilen kavram da nispeten yenidir. Dolayısıyla zaten esasen önemli bir konu olan delil değerlendirmesi konusu, dijital nitelikteki deliller söz konusu olunca daha da önemli bir hal almaktadır. Zira dijital delil, sadece soruşturma ve kovuşturmalarda değil, hemen her konuda, zaman zaman idari işlem ve eylemlerde, deyim yerindeyse hukukun her alanında gündeme oturmaktadır.

Değerli katılımcılar, ceza muhakemesinde uyuşmazlık konusu olayı temsil eden bazı araçlardan faydalanılır ki**,** bunlara **"delil (kanıt/ ispat vasıtası)"** denmektedir[2]. Doktrinde çeşitli açılardan değişik

[1] Sunum*"9. Türkiye Ceza Hukuku Günleri-Adil Yargılanma Hakları ve Anayasa Mahkemesine Bireysel Başvuru Sempozyumu (31 Mayıs - 1 Haziran 2014)"*nda yapılmıştır.

[2] **Centel/Zafer,** Ceza Muhakemesi Hukuku, s. 197; Sözlük anlamıyla ise delil, *"insanı aradığı gerçeğe ulaştırabilecek iz, emare"*dir (http://www.tdk.gov.tr/, 24.05.09)

sınırlandırmalar yapılmakla birlikte[3], ***Kunter***'in yaptığı bir ayrıma göre delilerin üç çeşidi olup, bunlar ***"beyan", "belge"*** ve ***"belirti"***den ibarettir. *"Beyan"* ve *"belge"* delilleri somut olaya özgü, onu doğrudan ispat etmeye yarayan deliller olup, *"**beyanlar**"* kendi içinde *"sanık/şüpheli beyanı, "tanık beyanı"* ve *"sanıktan başka tarafların beyanı"* (katılan, malen sorumlu vs.) olarak üçe; *"**belgeler**"*[4] ise yine kendi içinde, *"yazılı belgeler"*, *"şekil tespit eden belgeler"* ve *"ses tespit eden belgeler"* olarak üçe ayrılmaktadır. Delillerin üçüncü türünü oluşturan *"**belirtiler**"*[5] de yine kendi içinde, *"doğal belirtiler"* (örneğin kan, sperm) ve *"yapay belirtiler"* (örneğin giyilen üniforma, eşyanın kime ait olduğunu gösteren harfler) şeklinde ikiye ayrılmaktadır[6].

Peki dijital delil bu sınıflandırmada nerede yer alır? **Dijital deliller;** *"bir tür yazılı açıklama (belgesi)"* (Kunter, Yenisey, Öztürk*), "ses ve/veya görüntü tespit eden belge"*, *"ortam tespit eden belge"*, *"veri tespit eden belge* (örneğin şüphelinin bilgisayar kayıtlarından çıkarılan kopya)" veya *"ispat edilecek olayın kanıtlanmasına dolaylı olarak yardımcı olan ve vakıa ve iz şeklinde tanımlanan bir belirti"* olarak değişik şekillerde tarif edilebilmektedir.

Peki, dijital delil nedir; bir delilde veya geleneksel bir delilde bulunan vasıflara sahip midir? Bu konuda çeşitli tanımlar yapılmakla birlikte; **dijital veya elektronik delil** *"iddia edilen bir fiilin ispatında kullanılmak istenen veya kullanılan; elektronik ortamda oluşan/ oluşturulan, değiştirilen, iletilen veya saklanan veri, kayıt ve belgeler"* olarak ifade edilmektedir. Bu bağlamda, "dijital delil" ikrar, tanık beyanı vb. gibi belli bir delil tipini değil, delilin özünü veya bir özelliğini ifade etmektedir[7].

---

[3] Deliller çeşitli açılardan ayrıma tabi tutulabilir; bu bağlamda *"doğrudan delil-dolaylı delil"*, *"tamamlayıcıya ihtiyaç duyan delil- duymayan delil"* ve *"beyan, belge, nesne, iz ve vücut parçaları"* şeklinde bir tasnif de yapılmaktadır (bu konuda bkz. **Bıçak**, s. 430-485).

[4] ***"Belge",*** bir somut olayı temsil eden insan yapısı ispat aracı olup; ***"resmi"*** *-ki aksi sabit oluncaya kadar geçerli ve sahteliği sabit oluncaya kadar geçerli olanlar şeklinde ikiye ayrılabilir-* veya *"özel"* nitelikte olabilir.

[5] ***"Belirti",*** olaydan geriye kalan her türlü iz ve eserdir.

[6] **Kunter/Yenisey/Nuhoğlu**, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 612 vd.; **Turhan**, Ceza Muhakemesi Hukuku, s. 156 vd.

[7] **Göksu,** Hukuk Yargılamasında Elektronik Delil, s. 29.

Değerli katılımcılar, bilindiği gibi, elektronik yollar kullanılarak yapılan cihazlar analog veya dijital (sayısal) sinyalleri işleyebilmektedir. Analog sinyaller sürekli bir ölçekte iken, dijital sinyal sürekli olmayan bir ölçekte bulunmaktadır. Keza analog cihazlar sinyalleri doğrudan işlerken, dijital sinyaller sayılara çevrilerek işlenmektedir. Dolayısıyla analog cihazların yarattığı ve sakladığı veriler büyük ölçüde göz veya kulak gibi duyu organlarıyla (örneğin teyp bandı, filmi fotoğraf makinesi) algılanabildikleri halde, dijital cihazlarda veri sayısal halde yaratıldığı ve saklandığı için verilerin orijinalliğinden bahsedebilmek teknik olarak mümkün değildir. Buradaki orijinalliğe ilişkin farkı, medenî hukukta tüzel kişi ile gerçek kişi arasındaki farka benzetmek yanlış olmayacaktır[8]. Yani, "tüzel kişi" ne kadar "kişi" ise, "dijital delil" de o kadar "delil"dir.

Dijital delillere ilişkin bir diğer mesele, güvenilirlik meselesidir. Aidiyet tespiti noktasında zorluklar yaratan bu deliller, değiştirilmeye ve bozulmaya son derece elverişli olup, bu durum dijital verileri delil zincirinin en zayıf halkası haline getirmektedir.

Nitekim dijital delillerin güvenilirliği Yargıtay kararlarında da sık sık tartışılmakta ve bu türden delillerin değerlendirilmesinde dikkatli ve özenli davranılması gerektiğine işaret edilmektedir.

Örneğin, 9. Ceza Dairesi'nin 09.10.2013 tarihli (E. 2013/9110, K. 2013/12351) kararında şu ifadelere yer verilmiştir: *"… Dijital delillerin yapısı gereği manipülasyona açık olduğu bilinmektedir. Diğer delil türlerine göre özellik arz eden bazı yönleri olmakla birlikte dijital deliller de sonuçta, deliller hiyerarşisinin kabul edilmediği, delil serbestîsinin benimsendiği ceza muhakemesi sistemimizde bir ispat aracıdır. İspat aracı olan delilin değerlendirilmesinde, ceza muhakemesi hukukunda bir delil için öngörülen nitelikleri taşıyıp taşımadığı nazara alınıp, genel olarak; somut olayın özellikleri, yüklenen suçun işleniş biçimi, dosyadaki diğer deliller gibi hususlar gözetilip, özel olarak da; delilin temsil ettiği olayın niteliği, ele geçiriliş yeri, şekli ve zamanı, bu delilin sair karakteristik özellikleri gibi hususlar göz önünde bulundurulmalıdır. (…) Dijital deliller de, … diğer tüm deliller gibi … gizlenmeye, değiştirilmeye, bozulmaya elverişlidir. (…) Ancak, dijital delillerin değiştirilebilme kolaylığı ve sanal oluşundan hareketle hükme esas alınama-*

[8] **Göksu,** Hukuk Yargılamasında Elektronik Delil, s. 7-8.

yacak olduğunun ileri sürülmesi delil olgusuna aykırıdır. Kaldı ki, dijital deliller Türk ceza muhakemesi sisteminde ilk kez bu dava ile gündeme gelmiş olmayıp, geçmişte de pek çok davada tartışılmış ve hükme esas alınmıştır…"

Bu çerçevede, 9. Ceza Dairesi kararında da ifade edildiği üzere, dijital delillerin muhakeme sürecinde kullanılabileceği açıktır. Bu durum "***delil serbestîsi ilkesi***"nin bir gereğidir. Fakat, "delil serbestîsi ilkesi" her tür delilin hükme esas alınabileceği anlamına da gelmemektedir. Burada dikkat edilmesi gereken husus, bu delillerin "*olayı temsil edici*, *müşterek*, *akılcı* ve *gerçekçi*[9]" nitelikte ve "*hukuka uygun yollardan elde edilmiş*[10]" olması zorunluluğudur.

Bunun için, belgenin oluşturulduğu, değiştirildiği, yok edildiği veya başkaca bir işleme tabi tutulduğu sistem ve araçların bir bütün olarak incelenip değerlendirilmesi veya doğrulanması gerekmektedir. Bu çerçevede, keşif yapılması, uzmanların tanık olarak dinlenmesi veya bilirkişi raporu[11] istenmesi gerekebilir.

Elektronik delil bir vakıanın doğrudan ispatını sağlayabileceği gibi, tam aksini, yani soruşturma-kovuşturma konusu fiilin fail tarafından işlenmediğini de ortaya koyabilir.

Öte yandan, dijital delillerle ilgili yapılan işlemler ile bunlara ilişkin gözlem ve bulguların muhakeme sürecinde raporlanması ve belgelendirilmesi gerekmektedir[12]. Bu aşamaları genel olarak *karar alma, toplama, inceleme, analiz etme, belge hazırlama ve raporlama* şeklinde özetlemek mümkündür[13].

Dijital delillerde de, değerli katılımcılar, "***yasallık ilkesi***" mutlak surette gözetilmelidir. Bilindiği üzere, Yargıtay Ceza Genel Kurulu,

---

9 Yani delilin muhtevasını sadece hâkimin değil, tarafların da bilmesi/ öğrenmesi.

10 **Kunter/ Yenisey/ Nuhoğlu,** Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 575–579; **Turhan,** Ceza Muhakemesi Hukuku, s. 155–156.

11 *"… Sanık M.B hakkında 2911 sayılı Kanuna aykırılık suçundan kurulan hükümle ilgili olarak; CD'lerin çözümü tarafsız bilirkişiye yaptırıldıktan sonra, sonucuna göre sanığın hukuki durumunun takdir ve tayini gerekirken, eksik soruşturma ile yazılı şekilde hüküm kurulması…"* (9. CD, T. 16.01.2012, E. 2010/2320, K. 2012/682).

12 **Hart, Sarah V.** (Director), *"Forensic Examination of Digital Evidence: A Guide for Law Enforcement"*, U.S. Department of Justice Office of Justice Programs, s. 2.

13 Bkz. **Ergün, İsmail**, Siber Suçların Cezalandırılması ve Türkiye'de Durum, Adalet Yayınevi, Ankara 2008, s. 47-48.

13.12.2011 tarihinde vermiş olduğu bir karar (E. 2011/5-231, K. 2011/262) ile UYAP sisteminde kayıtlı verilerin "delil" niteliğinde olduğunu kabul etmiştir. O gün mevzuatta konuya ilişkin açık bir hüküm bulunmadığından, söz konusu karar mevcut düzenlemelerin yorumu üzerinden verilmiştir. Bu karardan yaklaşık yedi ay sonra ise, 05.07.2012 tarih ve 28344 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren 6352 sayılı kanun ile Ceza Muhakemesi Kanunu'na eklenen 38/A maddesi ile, uygulama açık bir yasal dayanağa kavuşmuştur. Bu bağlamda, söz konusu düzenleme ile, mevcut uygulamaya[14] "yasallık" yönünden getirilmesi muhtemel eleştirilerin de bertaraf edildiğini söylemek mümkündür.

Keza, "teknik araçla izleme" uygulamasının CMK md. 140'ta, "telekomünikasyon yoluyla yapılan iletişimin denetlenmesi" işlemi ile bilgisayar programlarında ve kütüklerinde yapılacak arama, kopyalama ve el koyma işlemlerinin CMK md. 134-138 arasında düzenlenmesi de "yasallık" ilkesi bakımından yerinde olmuştur. Bilindiği üzere, 21.02.2014 tarih ve 6526 sayılı yasa ile CMK md. 134 ve 135'te önemli değişiklikler yapılmıştır. Buna göre, "***bir suç dolayısıyla*** *yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından"* karar verilecektir[15].

Burada dikkat çeken ilk ibare "***bir suç dolayısıyla***" ibaresidir. Buna göre, madde, mahiyeti ve cezası ne olursa olsun her suç tipi için uygulanabilecek, bu çerçevede hükümde öngörülen koruma tedbirlerine hakaret, tehdit gibi görece basit suçlarda dahi başvurulabilecektir. Kanaatimizce, muhakemesinde söz konusu tedbirlere başvurulabilecek suçların maddede katalog halinde gösterilerek sınırlandırılması yerinde olacaktır.

---

[14] UYAP sisteminde kayıtlı verilerin hükme esas alınması uygulamasına ilişkin bir örnek: *"(…) UYAP sistemi kullanılarak çıkartılan nüfus kayıt örneğine göre mağdurun 15 yaşından küçük olduğu anlaşıldığından…" (5. Ceza Dairesi, T. 27.10.2010, E. 2011/5-231, K. 2011/262)*

[15] Avrupa Konseyi Siber Suç Sözleşmesinin 19. Maddesindeki düzenlemeye paraleldir.

Hükümde dikkati çeken bir diğer ibare "***somut delillere dayanan kuvvetli şüphe***" *ibaresidir.* Bu ibare ile takdir hakkının kullanımında keyfiliğin önlenmesi ve denetimin sağlanması için *somut bir ölçü norm* oluşturulmaya çalışılmıştır.

Hükümde dikkati çeken bir diğer ibare ise, "***bilgisayar***" ibaresidir. Hükümde ve madde kenar başlığında kullanılan "bilgisayar" kavramı acaba adı "bilgisayar" olmayan, fakat bilgisayar ile aynı vasıfları taşıyan akıllı telefon benzeri aletleri yahut veri depolamaya yarayan USB gibi cihazları da kapsamakta mıdır? Bu konuya bir açıklık getirilmesi, kanaatimizce, yerinde olacaktır.

134. maddenin ikinci fıkrasında *"bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere* ***elkonulabileceği****"* ifade edilmiştir. Burada, "*elkonulabilir*" ifadesinden "elkoyma" işlemine ancak "kopyalama" bakımından ihtiyaç duyulan hallerde başvurulabileceği açıkça anlaşılmaktadır. Nitekim, ikinci cümlede *"şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edileceği"* belirtilmiş; "delil üretilmesi" ihtimali bu yolla bertaraf edilmeye çalışılmıştır. Ancak, uygulamada bu iki koşula zaman zaman riayet edilmediği görülmektedir.

Üçüncü ve dördüncü fıkrada, elkoyma işlemi sırasında sistemdeki bütün verilerin yedekleneceği ve şüpheliye veya vekiline alınan yedekten bir kopya verilerek ve bu hususun tutanak altına alınacağı belirtilmiştir. Hükmün ilk halinde "*istem üzerine*" gerçekleştirilmesi öngörülen "yedekten kopya verilmesi" işleminin 6526 sayılı kanunla "*her halde zorunlu*" kılınması da, aynı şekilde, şüpheli için getirilmiş yeni bir güvencedir.

Değerli katılımcılar, dijital verilere ilişkin olarak yasada yer verilen koruma tedbirlerinden bir diğeri telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbiridir. Hukuk ve dolayısıyla siyaset gündemini sürekli meşgul eden ve 135. maddede düzenlenen bu tedbir, yapılan değişikliklerle birtakım ek koşullara tabi kılınmıştır.

Maddeye eklenen ilk ibare *"somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı"* ibaresidir. Değişiklik önemli gözükmekle bera-

ber, kanaatimizce gereksizdir; zira "kuvvetli şüphe[16]" ve "bu şüpheye dayanak teşkil edebilecek somut delillerin varlığı" zaten tüm koruma tedbirleri yönünden aranması gereken asgari bir koşul niteliğindedir.

Maddede yapılan bir diğer değişiklik, iletişimin denetlenmesi kararını alma yetkisinin "*ağır ceza mahkemeleri*"ne verilmiş olmasıdır. Buna göre, karar ağır ceza mahkemesi heyetince **oybirliğiyle** alınacaktır. Bu düzenleme ile yasa koyucu, iletişimin denetlenmesi noktasında yaşanan keyfi uygulamaları bertaraf edebilmeyi hedeflemiştir. Fakat, bir sanığın müebbet hapsine karar verilebilmesi için iki hakimin oyu yeterli iken, söz konusu koruma tedbirine başvurulması bakımından oybirliğinin aranmış olması da, CMK sistemine uymayan, şüphesiz, ilginç bir durumdur.

Maddeye göre, verilen kararda, yüklenen suçun türü, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türü, telefon numarası veya iletişim bağlantısını tespite imkân veren kodu, tedbirin türü, kapsamı ve süresi belirtilecektir. Karar, kural olarak, örgüt faaliyeti çerçevesinde işlenen suçlar müstesna, **iki ay** için verilebilecek ve zorunluluk halinde **bir ay** daha uzatılabilecektir. Yani, kural olarak **azami süre üç aydır. Fakat**, **örgüt faaliyeti çerçevesinde işlenen suçlarda,** mahkeme, bu üç aylık süreye ek olarak her defasında bir aydan fazla olmamak ve toplam üç ayı geçmemek üzere sürenin uzatılmasına karar verebilecek, böylelikle azami süre istisnai olarak **altı aya çıkarılabilecektir.**

Yedinci fıkrada ise, gördüğünüz üzere, bir dizi suç tipi sayılmakta ve (telekomünikasyon yoluyla yapılan) iletişimin denetlenmesi tedbirinin ancak bu katalogda yer verilen suçlar bakımından uygulanabileceği belirtilmektedir.

~ ~ ~

Dijital delillere ilişkin Yargıtay uygulamasından biraz bahsedecek olursak, ben, değerli arkadaşlar, Yargıtay kararlarında dijital/sayısal veya elektronik delilin niteliği ve değeri üzerine doğrudan bir kararına rastlamadım. Ancak çeşitli kararlarda, yüksek mahke-

[16] **Centel/Zafer,** değişiklik öncesinde "basit şüphe"nin varlığını yeterli görmekte idi.

menin, bu türden delillere itibar ettiğini ve hatta işyeri güvenlik kamerası[17], MOBESE kamerası ve sair cihaz kayıtlarının bulunup bulunmadığının araştırılmamasını bozma nedeni kabul ettiğini görüyoruz. Örneğin, çocuk pornografisi suçunda sanığın kullandığı elektronik posta adresinde elde edilen verileri (5. CD, 01.10.2007, 2007/ 9856-6957), terör örgütü propagandası yapmak suçunda el konulan CD'lerden (9. CD, 25.10.2010, 2008/21562, 2010/10946), flaş disk, bilgisayar hard disk ve mobil telefon hafızasından elde edilen verileri (9. CD, 2010/12773-10407; kasten insan öldürme ve yaralama suçunda MOBESE kamera kayıtlarının çözümlerini (1. CD, 14.05.2008, 2007/9024, 2008/4006) delil kabul eden Yargıtay, bu dijital verilerin araştırılmamış olmasını bozma nedeni saymıştır.

Elektronik delilden soruşturma veya organlarınca doğrudan yararlanılması delilin bulunduğu ortam ve niteliği itibariyle mümkün olmadığından, **bu delillerin** inceleme ve değerlendirmeye elverişli hale getirilmesi, yani **sanal dünyadan gerçek dünyaya aktarılması gerekmektedir.** Örneğin Yargıtay, insan öldürme suçuna ilişkin olarak önüne gelen bir dosyada, *"… soruşturma aşamasında temin edilen olay anı ve öncesine ilişkin görüntüleri içeren güvenlik kamerası görüntülerinin bilirkişiye çözümlettirilmesi ile çözüm tutanaklarının duruşma sırasında taraflara okunması ve diyeceklerinin sorulması gerektiğine*" işaret etmiş ve "*duruşma heyetince ne zaman ve nerede incelendiği tutanaklardan anlaşılmayan görüntülere istinaden mahkumiyet kararı verilemeyeceğine*" hükmetmiştir. (1. CD, 16.01.2012, 2008/10249, 2012/48)

[17] İşkence ve/veya kötü muamele bağlamında nezarethane kamera (bu çerçevede işyeri kamera) kayıtlarını kural olarak hukuka uygun bir delil kabul etmekte ve hatta bu konuda araştırma yapılması bozma nedeni sayılmaktadır*: "…Olay tarihinde katılan Erkan İmrek ile eşi arasında tartışma yaşanması üzerine olay yerine gelen polisler tarafından katılanı ve eşini Muammer Sencer Polis Merkezine götürüldüğü, dosya arasında karakola alınırken katılanla ilgili 1240 nolu raporla çıkarken tanzim edilen 1290 nolu adli raporlar arasında darp cebir izleri açısından farklılıklar olduğu 13/05/2007 tarihli Adli Tıp Uzmanı tarafından düzenlenen adli raporla tespit edildiği, katılan ve tanık eşinin de soruşturma aşamasından beri tutarlı bir şekilde sanıkların katılanı dövdüklerini iddia etmeleri karşısında, olay tarihindeki nezarethane kamera kayıtları getirtilip incelenmeden ve dosyadaki mevcut delilerin neden mahkumiyete yeter nitelikte olmadığı ayrıntılı olarak kararda tartışılmadan yazılı şekilde karar verilmesi…"* (3. CD, T. 13.02.2013, E. 2011/36421, K. 2013/5261).

MOBESE kamerası ile yapılan kaydı prensip olarak kabul edilebilir bulan Yargıtay, özelikle insan öldürme ve insan öldürmeye teşebbüs suçlarında, "*kolluğun yaptığı rapor ve çözümlemelerle yetinilmemesi ve görüntü kalitesinin yükseltilme olanaklarının araştırılması gerektiğine*" işaret etmektedir. Örneğin, 1. Ceza Dairesi, 2012 tarihli bir kararında, "*MOBESE kamerası görüntülerinin TRT kurumuna gönderilerek, görüntü kalitesinin ileri teknoloji ile iyileştirilmesi imkanının bulunup bulunmadığının sorulması*" gerektiğini belirtmiş, bu usule riayet edilmemiş olmasını "eksik inceleme" addederek yerel mahkeme hükmünü bozma yoluna gitmiştir. (1. CD, 17.10.2012, 2012/2350, 2012/7688)

Değerli katılımcılar, uygulamada sıklıkla yararlanılan bir diğer dijital delil bilgisayarlara ait "**IP numaraları**"dır. Pek çok davanın, özellikle de cinsel taciz, hakaret ve tehdit suçlarına ilişkin davaların çözümünde kilit rol oynayan bu numaralar önemli birer delil teşkil etse de, bu delillerin yan delillerle desteklenmesinde "maddi gerçeğin ortaya konabilmesi" bakımından büyük yarar vardır. 14. Ceza Dairesinin 20.10.2011 tarihli (E. 2011/17352, K. 2011/1065) kararı, bu açıdan, güzel bir örnektir.

Bir davada, şüphesiz, birden çok dijital delilin bulunması mümkündür. Bu gibi hallerde, dijital delillerin tamamının toplanması gerekmektedir. Örneğin, Yargıtay, uyuşturucu ticareti suçuna ilişkin bir davada, bir yandan iletişimin tespitine ilişkin verilerden, diğer yandan ise havalimanı güvenlik kamerası ve MOBESE kamerası kayıtlarından yararlanılabileceğini belirterek, bu delillerin yalnızca bir kısmına dayandırılan yerel mahkeme kararını "eksik inceleme"den bahisle bozma yoluna gitmiştir. (10. CD, 22.01.2013, 2012/20151, 2013/680)

Değerli arkadaşlar, telekomünikasyon yoluyla yapılan iletişimin denetlenmesinde "**tapeler**" de, bilindiği üzere, büyük önem arz etmektedir. Tapelerde yer alan ses kayıtlarına, uygulamada sıklıkla itiraz edildiği görülmektedir. Bu açıdan, itiraz halinde, bu kayıtların analizinin yaptırılması ve sanığa ait olup olmadığının tespit ettirilmesi icap etmektedir. Uyuşturucu ticareti suçundan (10. CD, 07.02.2012, E. 2011/3839, K. 2012/741) iftira suçuna (9. CD, 11.12.2012, E. 2012/3736, K. 2012/14729) pek çok suçta, Yargıtay, bu zorunluluğa dikkat çekmiş ve analiz yaptırılmamasını "eksik inceleme" kabul ederek bozma kararı vermiştir.

Belirtelim ki, tüm bu durumlarda, asıl delil olan bu yan ürünleri/ görünümleri değil, doğrudan doğruya verilerin kendisidir[18].

Değerli katılımcılar, görüldüğü üzere, uygulamada en büyük sıkıntı "dijital delillerin güvenilirliği"ne ilişkin olarak yaşanmaktadır. Dijital delilin ***güvenilirliği*** ve "delil" değeri ise doğrudan bu delillerin ***orijinalliği*** ile ilintili olup Yargıtay bu husus üzerinde hassasiyetle durmaktadır. Örneğin, bir kararda "sanığın işyerine ait güvenlik kamerası kayıtlarının orijinalliğine ve bu kayıtlara ekleme yapılıp yapılmadığına ilişkin olarak bir bilirkişiden rapor istenmesi gerektiğine işaret edilmiş, aksi yöndeki uygulama bozma nedeni kabul edilmiştir. (6. CD, 19.07.2010, 2010/6992, 2010/13757)

Dijital deliller her ne kadar bir olayı açıklar şekilde görünse de, ne zaman, ne şekilde oluşturulduğu ve/veya içeriğine müdahale edilip edilmediği çoğu zaman tespit edilemediğinden, bu delillerin tek başlarına delil olarak kullanılmasına genellikle imkân bulunmamaktadır. Bu nedenle, bu delillerin diğer delillerle birlikte değerlendirilmesi ve teyit edilmesi zorunludur.

Ancak, bazı hallerde, elde tek bir delilin bulunması ve bu delilin de dijital bir delil olması muhtemeldir. Bu gibi durumlarda, delilin çok daha titiz bir şekilde incelenmesi ve en ufak bir tereddütte dahi sanığın beraatı yoluna gidilmesi gerekmektedir. Zira, şüphenin sanık aleyhine yorumlanması halinde cezalandırılan kimsenin masum olması her zaman için ihtimal dahilindedir. Dijital delillerin niteliği dikkate alındığında, riskin bu deliller yönünden çok daha arttığı açıktır. Bu nedenle, örneğin, 13. Ceza Dairesi'nce verilmiş 2013 tarihli bir kararda, "*müştekiye ait iş yerinde bulunan güvenlik kamerasından elde edilen görüntülerin olayın tek delili olması nedeniyle, bu görüntülerin donanıma sahip bilirkişi veya kurumlara incelettirilerek görüntülerdeki kişinin sanık olup olmadığının tereddüde mahal vermeyecek şekilde belirlenmesi gerektiğine*" işaret edilmiş, "*aksi yöndeki uygulamanın bozma nedeni sayılacağı*" belirtilmiştir. (13. CD, 14.01.2013, 2011/28624, 2013/172)

Değerli arkadaşlar, son olarak, delillerin elde edilmesinde başvurulan yöntemin hukuka uygunluğu meselesine değinmek istiyorum. Her delil gibi, dijital delillerde de, delilin hukuka uygun yollardan

[18] **Göksu,** Hukuk Yargılamasında Elektronik Delil, s. 29-30.

elde edilmiş olması hükme esas alınabilmesi bakımından önemlidir. Bu çerçevede, Yargıtay, vermiş olduğu kararlarla, delil elde etmede birtakım hukuka uygunluk nedenlerinin varlığını zaman içerisinde kabul etmiştir.

Yargıtay, bir öğretim üyesinin fakültede şahsi kullanımına tahsis edilen odaya kamera yerleştirmesini ve bu sistem sayesinde odasından yapılan hırsızlığı tespit ettirmesini "hakkın kullanılması (TCK md. 26)" kapsamında değerlendirmiş ve bu yolla elde edilen delilleri "hukuka uygun delil" kabul etmiştir. Örneğin, 13. Ceza Dairesi, 26.03.2012 tarihli (E. 2011/7180, K. 2012/8523) bir kararında, bir öğretim üyesinin fakültede şahsi kullanımına tahsis edilen odaya kamera yerleştirmesini ve bu sistem sayesinde odasından yapılan hırsızlığı tespit ettirmesini "hakkın kullanılması (TCK md. 26)" kapsamında değerlendirmiş ve bu yolla elde edilen delilleri "iddia ve savunma hakkı" bakımından meşru kabul etmiştir. Buna karşılık, 1. Ceza Dairesi, kasten insan öldürme iddiası ile yargılandığı bir davada haksız tahrik indirimi talep eden sanığın dosyaya sunduğu gizli kamera çekimi görüntülerini delil olarak kabul etmemiş; bu görüntüleri esas alarak sanık hakkında haksız tahrik hükmü uygulayan yerel mahkemenin lehteki kararını bozma yoluna gitmiştir. (1. CD, 10.02.2009, 2008/5436, 2009/513)

Hemen belirtelim ki, herhangi bir hukuka uygunluk nedeninin söz konusu olmadığı hallerde alınan ses ve görüntü kayıtları "hukuka uygun delil" kabul edilemeyeceği gibi, ayrıca bu fiiller ilgilileri de tazminat borcu altına sokmaktadır. 4. Hukuk Dairesi, konu ile ilgili bir kararında, davalıların gizlice ses ve görüntü kaydetme biçiminde gerçekleşen eyleminin davacının şeref ve haysiyetine tecavüz etme amacı güdülmemiş olsa bile, 'kişilik haklarına saldırı' teşkil edeceğini kabul etmiş ve fiilin Türk Medeni Kanunu'nun 24. maddesinde yer alan yollama dolayısıyla "manevi tazminat" gerektirdiğine hükmetmiştir. (4. HD, 26.10.2007, 2006/13723, 2007/13089)

~ ~ ~

Evet değerli katılımcılar, teknolojik gelişmelerdeki hıza paralel olarak, yaşamın her alanında olduğu gibi, ceza muhakemesi alanında da dijital delil vazgeçilmez bir araç olarak karşımıza çıkmaktadır. Dijital delil yeni bir delil türü olmayıp, sadece içerdiği elektronik unsur nedeniyle onun bir niteliğini ve özelliklerini vurgulamaktadır.

Dijital delilinin elde edilmesi ve sunumunda usulüne uygun hareket edilmesi hayati bir önem arz etmektedir. Zira, aksi takdirde, delil hukuka aykırı hale gelmekte ve kullanılması mümkün olmamaktadır. Bu süreçte, kasti veya ihmali bir hareket, aslında bir gerçeğin ortaya çıkarılmasına hizmet edebilecek bir değerin, delilin heba olması sonucunu doğurabilmektedir. Dolayısıyla, bu konuda muhakeme süjelerinin eğitilmesi ve konuyla ilgili uzmanların istihdamı üzerinde önemle durulması icap etmektedir.

Bunun yanında, adli bilişim konusunda bilirkişilik yapacak veya talep edildiğinde soruşturma veya savunma makamlarına veya mahkemelere hizmet verebilecek bir "adli bilişim kurumu"na da, kanaatimizce, artık ihtiyaç vardır. Bu çerçevede, hukuk fakültelerinde veya enstitülerinde de adli bilişim derslerine yer verilmelidir.

Güvenilir dijital delillerin "olayı temsil edici" niteliği oldukça yüksektir. Ancak pozitif hukukumuzda mevcut kavram ve kurumların yeterli olmaması nedeniyle, bu konuda ayrıntılı düzenlemeler yapılması yararlı olacaktır. Zira klasik delillerin tanım ve kuralları içerisinde sıkışıp kalınması muhakeme sürecinin sağlıklı bir biçimde yürütülmesine engel teşkil etmekte ve delil değeri yüksek olan dijital delillerden yeterince yararlanılamaması tehlikesini ortaya çıkarmaktadır.

Değerli katılımcılar, bu cümlelerle bana ayrılan sürenin sonuna gelmiş bulunuyoruz. Konuşmamı ilgiyle dinlediğiniz için teşekkürlerimi sunuyor, hepinizi saygıyla selamlıyorum.

KAYNAKÇA

Bıçak, Vahit, Suç Muhakemesi Hukuku, 2. Baskı, Seçkin Yayınevi, Ankara 2011.

Centel, Nur / Zafer, Hamide, Ceza Muhakemesi Hukuku, 9. Baskı, Beta Yayıncılık, İstanbul 2012.

Ergün, İsmail, Siber Suçların Cezalandırılması ve Türkiye'de Durum, Adalet Yayınevi, Ankara 2008.

Göksu, Mustafa, Hukuk Yargılamasında Elektronik Delil, Adalet Yayınevi, Ankara 2011.

Hart, Sarah V. (Director), *"Forensic Examination of Digital Evidence: A Guide for Law Enforcement"*, U.S. Department of Justice Office of Justice Programs, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf, s. 2.

Kunter, Nurullah/ Yenisey, Feridun/ Nuhoğlu, Ayşe, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 15. Baskı, Beta Yayıncılık, İstanbul 2006.

Turhan, Faruk, Ceza Muhakemesi Hukuku, Asil Yayıncılık, Ankara 2006.