ADLİ VAKALARDA HTS ANALİZİ
Teknik, Hukuki ve Uygulamalı Boyutlar

HTS Analysis in Forensic Cases:
Technical, Legal and Applied Dimensions

Derleme Makale / Review Article

Dr. Burak Olgun
burakolgun@soluitonhome.net
Solution Home Bilişim Tekn.ve Dan.Hizm., İstanbul.

Anahtar Kelimeler: *HTS • Baz İstasyonu • Konum Tespiti • Dijital Delil • Adli Telekomünikasyon*

ÖZET

Tarihsel Trafik Sinyalleşme Kaydı (Historical Traffic Signalling — HTS), mobil telefon kullanıcılarının baz istasyonlarıyla kurduğu her türlü sinyal etkileşimine ait logların geriye dönük olarak incelenmesine dayanan bir telekomünikasyon analiz yöntemidir. Adli soruşturmalarda HTS analizi; şüphelilerin, mağdurların ya da tanıkların belirli bir tarih ve saat aralığında hangi coğrafi bölgede bulunduğunun tespiti, birbirleriyle iletişim kurup kurmadıklarının belirlenmesi ve hareket örüntülerinin ortaya konması amacıyla giderek artan bir sıklıkta kullanılmaktadır. Bu derleme makale; HTS verisinin teknik yapısını ve üretim mekanizmalarını, baz istasyonu konum verilerinin coğrafi yorumlanma biçimini, adli HTS analizinin uygulama metodolojisini, delil değeri ve güvenilirlik sınırlılıklarını, hukuki kabul edilebilirlik koşullarını ve yargı kararlarında HTS delilinin kullanımına ilişkin pratik boyutları akademik kaynaklara dayanılarak kapsamlı biçimde ele almaktadır. Makalede

ayrıca bu alanda karşılaşılan teknik yanılgılar ve yargısal hatalar da değerlendirilmektedir.

Anahtar Kelimeler: *HTS analizi, baz istasyonu kaydı, CDR, adli telekomünikasyon, mobil konum tespiti, dijital delil, hücresel ağ, adli bilişim*

ABSTRACT

Historical Traffic Signalling (HTS) analysis is a telecommunications analysis method based on the retrospective examination of logs of all signal interactions between mobile phone users and base stations. In forensic investigations, HTS analysis is used with increasing frequency to determine the geographic location of suspects, victims, or witnesses during specific date and time intervals, to establish whether they were in communication with each other, and to reconstruct movement patterns. This review article comprehensively examines, based on academic sources, the technical structure and production mechanisms of HTS data, the geographic interpretation of base station location data, the applied methodology of forensic HTS analysis, the evidentiary value and reliability limitations, the conditions for legal admissibility, and the practical dimensions of HTS evidence usage in judicial decisions. The article also evaluates technical misconceptions and judicial errors encountered in this field.

1. Giriş

Mobil iletişim teknolojilerinin toplumsal yaşama hızla entegre olmasıyla birlikte, hücresel ağ operatörlerinin tuttuğu trafik kayıtları adli soruşturmaların vazgeçilmez bir unsuru haline gelmiştir. Bir cep telefonunun her çağrısı, kısa mesajı, veri bağlantısı ve hatta ağa kayıt olma eylemi (location update), operatör sistemlerinde otomatik olarak işlenmekte ve belirli bir süre boyunca saklanmaktadır. Bu kayıtların bütünü, farklı ülkelerde farklı terimlerle —CDR (Call Detail Record), IPDR (Internet Protocol Detail Record), trafik sinyalleşme kaydı ya da HTS— ifade edilmektedir (Casey, 2011).

Türk hukuku ve uygulamasında yaygınlaşan **HTS** (Tarihsel Trafik Sinyalleşme Kaydı) kavramı, telekomünikasyon şirketlerinin müşterilere ait tarihsel iletişim trafiğine ilişkin tuttuğu kayıtların tamamını kapsamaktadır. Bu kayıtlar, yalnızca kimin kiminle konuştuğunu değil; hangi baz istasyonu üzerinden bağlantı kurulduğunu, bağlantının saat ve süresini, kullanılan SIM ve cihaz kimliğini (IMSI/IMEI) de içermektedir. Bu zengin veri seti, adli analistlere bir kişinin belirli bir an ve mekânda fiziksel olarak nerede olduğuna dair güçlü çıkarımlar yapma imkânı tanımaktadır (Hargreaves & Chivers, 2016).

HTS analizinin adli soruşturmalardaki önemi son on yılda dramatik biçimde artmıştır. Cinayet, organize suç, uyuşturucu kaçakçılığı, terörle mücadele ve kaçırma gibi ağır suç soruşturmalarında HTS delilleri, sıklıkla kovuşturmanın bel kemiğini oluşturmaktadır. Bununla birlikte, bu delilin teknik karmaşıklığı ve yargı çevrelerindeki kavranma güçlüğü, hem haksız mahkûmiyetlere hem de suçluların delil yetersizliğiyle beraat etmesine zemin hazırlayabilmektedir (Morrison & Enzinger, 2018). Bu makalenin amacı, HTS analizinin

teknik, metodolojik ve hukuki boyutlarını bütünlüklü biçimde ele alarak konuya ilişkin kapsamlı bir akademik çerçeve sunmaktır.

2. HTS Verisinin Teknik Yapısı ve Üretim Mekanizması

2.1 Trafik Kaydının Oluşumu

Bir mobil telefon, kullanıcının aktif bir çağrı başlatması ya da veri aktarımı gerçekleştirmesinden bağımsız olarak, sürekli biçimde içinde bulunduğu hücrenin baz istasyonuyla sinyal alışverişi yapar. Bu etkileşimler çeşitli kategorilere ayrılır ve her biri operatörün ağ yönetim sistemlerinde farklı kayıt türleri oluşturur:

- Konum güncelleme (Location Update — LU / Periodic LU): Telefon, belirli aralıklarla ya da hücreler arası geçişlerde ağa konumunu bildiren sinyal gönderir. Bu kayıtlar, kullanıcının aktif bir çağrısı olmadığı anlarda dahi baz istasyonu bilgisini içerir.
- Çağrı kayıtları (MO/MT Call): Başlatılan (Mobile Originated) ve alınan (Mobile Terminated) sesli çağrılara ait başlangıç-bitiş zamanı, süre, arayan/aranan numara ve bağlandığı baz istasyonu bilgilerini içerir.
- SMS kayıtları: Gönderilen ve alınan kısa mesajlara ait zaman damgası, karşı numara ve baz istasyonu bilgisini kapsar.
- Veri oturumu kayıtları (IPDR): İnternet ve veri bağlantısı oturumlarına ait başlangıç-bitiş zamanı, kullanılan veri miktarı ve bağlantı noktası bilgilerini içerir.
- Acil durum ağ kaydı (IMSI Attach/Detach): Telefonun açılıp kapanmasına karşılık gelen ve ağa bağlanma/ayrılma olaylarını belgeleyen kayıtlardır (Casey, 2011).

Bu kayıtların kritik önemi, yalnızca aktif iletişimi değil; pasif ağ etkileşimlerini de belgelemesinden kaynaklanmaktadır. Bir şüphelinin telefonu sessize alınmış ve çantasında olsa dahi baz istasyonu loglarına periyodik olarak kayıt düşebilmekte; bu kayıtlar belirli bir dönemde şüphelinin bulunduğu coğrafi bölgeye dair bilgi sunmaktadır (Hargreaves & Chivers, 2016).

2.2 IMSI, IMEI ve Telefon-SIM İlişkisi

HTS analizinde kimlik tespiti açısından iki temel tanımlayıcı kullanılmaktadır. **IMSI (International Mobile Subscriber Identity)**, SIM karta özgü 15 haneli benzersiz bir kimlik numarasıdır ve aboneliğe bağlı iletişim bilgilerini tanımlar. **IMEI (International Mobile Equipment Identity)**, cihaza özgü 15 haneli bir seri numarasıdır ve SIM karttan bağımsız olarak cihazı tanımlar (3GPP TS 23.003, 2021).

Bu iki tanımlayıcının ayrı takip edilmesi, adli analizde kritik çıkarımlar yapılmasını mümkün kılar: Aynı IMEI numarasının farklı IMSI'larla kayıt görünmesi, cihazda SIM kart değiştirildiğine işaret eder. Aynı IMSI'nın farklı IMEI'larla görünmesi ise SIM kartın farklı cihazlara takıldığını gösterir. Her iki kalıp da adli açıdan —özellikle kimlik gizleme girişimlerinin tespitinde— son derece değerlidir (Hargreaves & Chivers, 2016).

Öte yandan IMEI manipülasyonu —telefon yazılımı ya da donanım değişikliğiyle IMEI numarasının değiştirilmesi— adli soruşturmalarda karşılaşılabilen bir güçlüktür. Bu nedenle analiz sırasında yalnızca tek bir tanımlayıcıya dayalı kimlik tespiti yapmak metodolojik hata oluşturabilir; IMSI ve IMEI verilerinin birlikte ve çapraz doğrulama amacıyla kullanılması gerekir (Ayers et al., 2014).

2.3 Veri Saklama Süreleri ve Erişim Koşulları

HTS verilerinin operatörler tarafından ne kadar süre saklandığı, hem ülkeden ülkeye hem de operatörden operatöre önemli farklılıklar göstermektedir. Avrupa'da Avrupa Birliği Veri Saklama Direktifi (2006/24/EC), üye devletlerde 6 ay ile 24 ay arasında veri saklamayı zorunlu kılmıştır; ancak Avrupa Birliği Adalet Divanı bu direktifi 2014 yılında orantısız bularak iptal etmiş ve veri saklama konusunu ulusal mevzuata bırakmıştır (Waidner & Backes, 2016).

Türk hukukunda ise 5651 sayılı Kanun ve ilgili yönetmelikler çerçevesinde operatörler, trafik verilerini iki yıl süreyle saklamakla yükümlüdür. Cumhuriyet savcıları ve mahkemeler, bu verilere adli soruşturma kapsamında yazılı talep yoluyla erişebilmektedir. Önemli bir husus olarak belirtilmeli ki; farklı veri türleri farklı saklama sürelerine tabi olabilmekte ve süresi dolan veriler geri dönülemez biçimde silinmektedir. Bu durum, gecikmeli soruşturmalarda kritik kanıtların erişilemez hale gelmesine yol açmaktadır (Kerr, 2010).

3. Baz İstasyonu Verisi ve Coğrafi Konum Yorumlama

3.1 Hücresel Ağın Coğrafi Yapısı

HTS kaydındaki her bağlantı satırı, terminali o an hizmet veren baz istasyonunu tanımlayan bir **Cell-ID (Hücre Kimliği)** içerir. Bu kimlik; MCC (Mobil Ülke Kodu), MNC (Mobil Ağ Kodu), LAC (Konum Alan Kodu) ve CI (Hücre Kimliği) alanlarından oluşur. Bu bileşenler bir araya getirildiğinde, kullanıcının bağlandığı sektörü coğrafi olarak benzersiz biçimde tanımlar (Hargreaves & Chivers, 2016).

Baz istasyonları çoğunlukla üç sektöre ayrılmıştır; her sektör yaklaşık 120 derecelik bir açı aralığını kapsar. Bir sektörün kapsama alanı —yayın yarıçapı— kentsel ortamlarda birkaç yüz metre ile 1–2 km arasında değişirken kırsal alanlarda onlarca kilometreye ulaşabilmektedir. Bu gerçek, HTS analizinde sıklıkla göz ardı edilen kritik bir hususdur: Bir Cell-ID, kullanıcının belirli bir *noktada* bulunduğunu değil; geniş bir kapsama alanı içinde *herhangi bir konumda* bulunduğunu göstermektedir (Jain & Demers, 2019).

3.2 Kapsama Alanı Belirsizliği ve Yorumlama Sınırlılıkları

HTS analizinde en sık yapılan metodolojik hata, baz istasyonu kaydının kesin konum verisi olarak sunulmasıdır. Oysa baz istasyonu kaydı, olası konumun yalnızca *olasılıksal bir tahminine* olanak tanır. Kapsama alanı; arazi topolojisi, bina yoğunluğu, ağaç örtüsü ve atmosferik koşullar gibi çeşitli faktörlere bağlı olarak farklılık göstermektedir (Morrison & Enzinger, 2018).

Özellikle dikkat edilmesi gereken iki fenomen şunlardır: İlk olarak, **anormal hücre seçimi** (anomalous cell selection): Bir mobil terminal, coğrafi açıdan daha uzaktaki bir hücreye bağlanabilir. Bu durum; radyo engeli, ağ yükü dengeleme ya da handover mekanizmasının gecikmesi nedeniyle ortaya çıkabilmektedir. İkinci olarak, **kapsama örtüşmesi** (coverage overlap): Özellikle yoğun kentsel alanlarda birden fazla baz istasyonu aynı coğrafi noktayı kapsamakta; terminal hangi istasyona bağlanacağını radyo koşullarına göre anlık olarak belirlemektedir. Bu iki fenomen, aynı konumdaki iki farklı kullanıcının farklı Cell-ID'lere kaydolmasına neden olabilmektedir (Jain & Demers, 2019).

Bu sınırlılıklar, adli HTS analizinde kapsama alanı haritalamasının (coverage mapping) titizlikle yapılmasını zorunlu kılmaktadır. Yalnızca operatör tarafından sağlanan teorik kapsama verilerine değil; sahadaki gerçek ölçüm verilerine (drive test, walktest) de başvurulması metodolojik güvenilirliği artırmaktadır (Hargreaves & Chivers, 2016).

3.3 Konum Tespitinde Kullanılan Teknikler

HTS verisinden konum kestirimi için birden fazla teknik kullanılabilmektedir. En temel ve en yaygın yöntem olan **Cell-ID yöntemi**, hücre kimliğini bilinen baz istasyonu koordinatlarına eşleyerek kaba bir konum tahmini üretir. Bu yöntem, operatörün baz istasyonu veritabanı bilgisine bağımlıdır ve kapsama alanı boyutunda bir belirsizlik içerir (Ayers et al., 2014).

Daha ileri teknikler arasında **Timing Advance (TA)** parametresi öne çıkmaktadır. GSM ağlarında 0–63 arasında değer alabilen TA, terminali ile baz istasyonu arasındaki ışık hızı bazlı mesafeyi yansıtır; bir TA birimi yaklaşık 550 m mesafeye karşılık gelir. TA verisi mevcut olduğunda, kapsama alanı çemberi belirli bir halka bölgesiyle daraltılabilir. UMTS ve LTE ağlarında ise **Round-Trip Time (RTT)** ve **E-CID (Enhanced Cell-ID)** yöntemleri benzer işlevi üstlenir (Peterson, 2017).

Birden fazla baz istasyonuna ait sinyal gücü ölçümlerinin kullanıldığı **RSSI tabanlı trilaterasyon** yöntemi, terminali çevreleyen istasyonların mesafe tahminlerini geometrik olarak kesiştirir. Bu yöntemin doğruluğu, kullanılan baz istasyonu sayısıyla doğrudan orantılıdır; ancak kentsel ortamlarda çok yollu yayılım (multipath propagation) bu kestirim doğruluğunu olumsuz etkileyebilmektedir (Jain & Demers, 2019).

Tablo 1. *HTS Konum Tespiti Yöntemlerinin Karşılaştırması*

Yöntem	Temel Prensip	Doğruluk	Gereksinim	Kullanım
Cell-ID	Baz ist. koordinatları	100 m – 35 km (kapsama)	Operatör BTS veri tabanı	Yaygın
Timing Advance (GSM)	Sinyal yayılım süresi	~550 m (1 TA birimi)	TA kaydı mevcut olmalı	Orta
E-CID / RTT (LTE)	Gidiş-dönüş gecikme süresi	50–300 m	LTE kayıt desteği	Gelişmekte
Trilaterasyon (RSSI)	Çoklu BTS sinyal gücü	100–500 m (kentsel)	Çoklu BTS ölçümü	Uzman analizi
GPS (cihaz verisi)	Uydu koordinatları	< 10 m	Cihaz log erişimi	Sınırlı

Not. Doğruluk değerleri kentsel ortamda tipik senaryolara aittir; kırsal ve engellerle dolu ortamlarda önemli sapma gözlemlenebilir. Kaynak: Hargreaves & Chivers (2016); Jain & Demers (2019); Peterson (2017).

4. Adli HTS Analizi: Metodoloji ve Uygulama Aşamaları

4.1 Veri Toplama ve Zincir Muhafaza

Adli HTS analizinin geçerliliği, büyük ölçüde delil zinciri (chain of custody) bütünlüğüne bağlıdır. Operatörden alınan HTS verisi; talep belgesi, teslim tutanağı ve hash değerleri (SHA-256 gibi kriptografik özet) ile belgelenmelidir. Bu adım atlandığında ya da eksik bırakıldığında, savunma avukatı verinin özgünlüğüne itiraz edebilmekte ve delil değeri zayıflayabilmektedir (Carrier, 2006).

Veri toplama aşamasında analistin dikkat etmesi gereken temel hususlar şunlardır: (1) Talep edilen veri aralığının olay tarihini öncesi ve sonrasıyla kapsayacak biçimde yeterince geniş tutulması; (2) Tüm ilgili IMSI ve IMEI tanımlayıcılarının ayrı ayrı sorgulanması; (3) Varsa IPDR (veri trafiği) verilerinin sesli çağrı verilerinden ayrı olarak talep edilmesi; (4) Baz istasyonu koordinat veritabanının (Cell-ID veritabanı) olay tarihine ait versiyonunun sağlanması —zira baz istasyonu konumları zamanla değişebilmektedir (Casey, 2011).

4.2 Veri Hazırlama ve Temizleme

Ham HTS verisi genellikle farklı operatör sistemlerinden farklı formatlarda (CSV, Excel, XML, özel format) gelmekte olup analize başlamadan önce standardize edilmesi gerekmektedir. Bu aşamada karşılaşılan tipik sorunlar şunlardır:

- Zaman dilimi tutarsızlıkları: Operatör sistemleri zaman damgalarını yerel saat ya da UTC olarak kaydedebilmekte; analist bu farkın farkında olmazsa saat sapmaları oluşabilmektedir.
- Eksik kayıtlar: Ağ kesintisi, sistem bakımı ya da veri tabanı arızası nedeniyle belirli zaman aralıklarında kayıt bulunmayabilmektedir; bu boşlukların tespit edilip raporlanması şarttır.
- Yinelenen kayıtlar: Aynı olayın birden fazla sistem tarafından loglanması durumunda yinelenen satırlar oluşabilmektedir; bu satırların filtrelenmesi gerekir.
- Hatalı Cell-ID: Baz istasyonu veritabanında bulunmayan ya da koordinatı hatalı girilen Cell-ID'ler, coğrafi haritalamada boşluklara yol açar (Ayers et al., 2014).

4.3 Zaman Çizelgesi ve Hareket Örüntüsü Analizi

Veri hazırlama tamamlandıktan sonra analitik sürecin özü olan **zaman çizelgesi yeniden inşası** aşamasına geçilir. Bu aşamada tüm iletişim olayları kronolojik sıraya dizilir; her olayın Cell-ID'si bilinen baz istasyonu koordinatlarıyla eşleştirilerek haritaya aktarılır. Elde edilen görsel, şüphelinin belirli bir zaman dilimindeki coğrafi hareketini gösteren bir *hareket izleme haritası* niteliği taşır (Hargreaves & Chivers, 2016).

Hareket örüntüsü analizinde dikkat edilmesi gereken metodolojik ilkeler şunlardır: (1) Kayıtlar arasındaki zaman boşluklarının açıklanması: Uzun bir sessizlik dönemi, telefonun

kapalı olduğuna, ağ dışında kaldığına ya da veri eksikliğine işaret edebilir; bu olasılıklar tartışılmadan sonuca gitmek hatalıdır. (2) Komşu hücre geçişlerinin mantıksal tutarlılığı: Coğrafi olarak birbirine uzak iki hücre arasında aniden geçiş, telefon taşınmışsa beklenen bir bulgudur; ancak aynı kişi tarafından gerçekleştirilemeyecek bir hız ima ediyorsa bu tutarsızlık raporlanmalıdır. (3) Olayın gerçekleştiği saatte ağ yükünün değerlendirilmesi: Yoğun saatlerde hücre seçim kalıpları normalden farklılık gösterebilmektedir (Morrison & Enzinger, 2018).

4.4 İletişim Ağı Analizi

HTS analizi yalnızca coğrafi konum tespitini değil; **sosyal ağ örüntüsü** analizini de kapsar. Bu analizde şüphelinin kiminle, hangi sıklıkta, hangi zaman aralıklarında ve hangi sürelerde iletişim kurduğu incelenerek ilişki haritaları oluşturulur. Organize suç ve terör soruşturmalarında bu teknik, hiyerarşik yapılar ve emir-komuta zincirlerinin ortaya konması bakımından özellikle değerlidir (Casey, 2011).

İletişim ağı analizinde kullanılan temel metrikler; arama sıklığı, iletişim süresi, karşılıklılık oranı (bir kişinin hem arayan hem aranan taraf olma oranı), iletişim zamanlaması ve kullanılan iletişim kanalı türleridir (ses, SMS, veri). Bu metriklerin birlikte değerlendirilmesi, salt iletişim kayıtlarının çok ötesine geçen bir örüntü tanımlama kapasitesi sunmaktadır (Peterson, 2017).

5. HTS Delilinin Değeri, Güvenilirliği ve Sınırlılıkları

5.1 Delil Gücünü Etkileyen Faktörler

HTS delilinin yargı sürecindeki ağırlığını belirleyen çok sayıda faktör bulunmaktadır. Delil gücü, aşağıdaki koşulların bir araya gelmesiyle artmaktadır: Zaman çizelgesinin olay tarihiyle yüksek ölçüde örtüşmesi; Cell-ID'lerin olay yeriyle coğrafi uyumu; hareket örüntüsünün alternatif açıklamalarla çürütülememesi; bağımsız fiziksel ya da görgü tanığı delilleriyle desteklenmesi (Morrison & Enzinger, 2018).

Öte yandan HTS delilinin sınırlılıkları da eşit derecede önemlidir:

- Telefon ve kullanıcı özdeşliği: HTS kaydı, bir cihazın ya da SIM kartın belirli bir anda belirli bir hücreye bağlı olduğunu gösterir. Bu, o anda telefonu kimin kullandığını kanıtlamaz; SIM kart başka bir kişi tarafından kullanılıyor olabilir.
- Kapsama alanı belirsizliği: Baz istasyonu kaydı, olası konum alanının yalnızca alt sınırını belirler; kesin bir nokta tespiti sunmaz.
- Ağ olayı ile fiziksel olay arasındaki fark: Bir çağrı kaydının zaman damgası, fiziksel olayın zaman damgasıyla her zaman örtüşmez; çağrı başlamadan önce fiziksel olay gerçekleşmiş olabilir.
- Manipülasyon olasılığı: SIM klonlama ve IMEI değiştirme gibi teknikler, HTS kaydının güvenilirliğini tehlikeye atabilir; bu olasılık soruşturmada değerlendirilmelidir (Ayers et al., 2014).

5.2 Teknik Yanılgılar ve Yargısal Riskler

Yargı pratiğinde HTS delilinin yanlış yorumlanmasından kaynaklanan çeşitli yapısal riskler gözlemlenmektedir. Morrison & Enzinger (2018), bu riskleri dört temel başlık altında ele almaktadır:

İlk risk, **kesinlik yanılgısı**dır: Savcılar ya da bilirkişiler, baz istasyonu kaydını sanığın o noktada *kesinlikle* bulunduğunun kanıtı olarak sunarlar; oysa bu kayıt yalnızca olasılıksal bir çıkarım sağlar. Bu yanılgı, özellikle kapsama alanı haritalaması yapılmadan yürütülen analizlerde belirgin biçimde ortaya çıkmaktadır.

İkinci risk, **nedensellik karıştırma**dır: Şüphelinin olay yerini kapsayan bir hücreye bağlı olması, onu olay yerinde *var* eder; ancak o hücrenin onlarca km² kapsama alanı olduğunda bu çıkarım yanıltıcıdır.

Üçüncü risk, **dışlama yanılgısı**dır: Şüphelinin HTS kaydında olay yerini kapsayan hücreye bağlandığına dair bir kaydın *bulunmaması*, o kişinin orada olmadığını kanıtlamaz; telefon kapalı olmuş, kapsama alanı dışında kalmış ya da kayıt oluşturacak sinyal etkileşimi gerçekleşmemiş olabilir.

Dördüncü risk, **uzman bilgisi eksikliği**dir: Hâkim ya da jürinin teknik altyapıya sahip olmaması durumunda, karmaşık HTS analizleri gereken eleştirel değerlendirmeden yoksun biçimde kabul görür; bu durum yargısal hata riskini artırır.

> *"Bir baz istasyonu kaydı, belirli bir lokasyonun kanıtı değil; olasılıksal bir konum aralığının göstergesidir. Bu ayrım, yargı sürecinde sıklıkla göz ardı edilmekte ve ciddi yanlış sonuçlara yol açmaktadır."* (Morrison & Enzinger, 2018, s. 214)

6. Hukuki Kabul Edilebilirlik ve Yargısal Çerçeve

6.1 Dijital Delil Kabul Standartları

Dijital delillerin mahkemede kabul edilebilirliği, geleneksel delil kurallarının ötesinde ek standartlara tabi tutulmaktadır. ABD hukukunda **Daubert standardı** (Daubert v. Merrell Dow Pharmaceuticals, 1993), bilimsel delillerin güvenilirliğini değerlendirirken dört temel kriterin kullanılmasını öngörür: (1) Metodolojinin test edilip test edilmediği; (2) Hata oranının bilinip bilinmediği; (3) Mesleki topluluk tarafından kabul görüp görmediği; (4) Hakemli yayınlarda yer alıp almadığı (Faigman et al., 2014).

İngiliz hukukunda **R v. T (2010)** davası ve sonraki içtihatlar, adli bilirkişi görüşlerinin istatistiksel temele dayandırılmasını ve belirsizliklerin açıkça beyan edilmesini zorunlu kılmaktadır. Bu gelişmeler, HTS analizinin mahkeme önüne taşınmasında belirsizliklerin raporlama standartlarını doğrudan etkilemektedir (Robertson & Vignaux, 1995).

Türk hukukunda, **5271 sayılı Ceza Muhakemesi Kanunu'nun (CMK)** 135. maddesi iletişimin denetlenmesini, 138. maddesi ise tesadüfen elde edilen delillerin kullanımını düzenlemektedir. Telekomünikasyon operatörlerinden HTS verisi talep edilmesi yetkisi savcı ve mahkeme kararına bağlıdır; CMK 332. maddesi uyarınca trafik kaydı suç soruşturması kapsamında hâkim kararıyla temin edilebilmektedir. Delil elde etme usulünün bu hükümlere uygunluğu, delil geçerliliğinin ön koşuludur.

6.2 Gizlilik Hakkı ve Orantılılık

HTS verisi, bireylerin özel yaşamına ilişkin son derece ayrıntılı bilgi içermektedir: Nerede olduğu, temasları, hangi saatlerde aktif olduğu ve hatta dini ibadet ya da sağlık kurumu ziyareti gibi hassas davranışsal kalıplar bu veriden çıkarılabilmektedir. Bu nedenle HTS verilerine erişim, **Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi** (özel yaşama saygı hakkı) kapsamında orantılılık denetimine tabi tutulmaktadır (Waidner & Backes, 2016).

Avrupa İnsan Hakları Mahkemesi, *Zakharov/Rusya (2015)* ve *Szabó ve Vissy/Macaristan (2016)* kararlarında toplu gözetim mekanizmalarının bireyin haberleşme gizliliğini ihlal ettiğine hükmetmiştir. Bu içtihatlar, HTS verilerine yönelik toplu ve hedefsiz erişimin hukuki meşruiyetini zayıflatmakta; soruşturmaların belirli bir kişiye ve suça yönelik somut şüpheye dayanmasını zorunlu kılmaktadır (Kerr, 2010).

6.3 Bilirkişi Raporu ve Standartlar

HTS analizinin mahkemeye sunulması, teknik bilgiye sahip bir bilirkişinin raporuyla gerçekleştirilmektedir. Uluslararası adli bilişim standartları, HTS bilirkişi raporunda bulunması gereken asgari unsurları belirlemiştir. Carrier (2006) ve Casey (2011) bu unsurları şöyle sıralar:

- Analiz kapsamının açık tanımı: Hangi veri setinin, hangi dönem için incelendiği belirtilmelidir.
- Kullanılan metodolojinin ayrıntılı açıklanması: Konum tahmin yöntemi, kullanılan araçlar ve varsayımlar eksiksiz aktarılmalıdır.
- Belirsizliklerin ve sınırlılıkların açıkça beyan edilmesi: Kapsama alanı belirsizliği, veri boşlukları ve alternatif yorumların raporlanması şarttır.
- Bulguların olasılıksal dille ifade edilmesi: 'Şüpheli orada bulunuyordu' yerine 'şüphelinin telefonunun o hücrenin kapsama alanında bulunduğu kuvvetle muhtemeldir' gibi ifadeler kullanılmalıdır.
- Çapraz doğrulama: Bağımsız veri kaynaklarıyla (fiziksel delil, kamera görüntüsü, tanık beyanı) yapılan doğrulama raporlanmalıdır (Carrier, 2006).

Tablo 2. *HTS Analizi Sürecinde Karşılaşılan Başlıca Metodolojik Hatalar ve Etkileri*

Hata Türü	Açıklama	Yargısal Etkisi
Kesinlik yanılgısı	Olasılıksal konumun kesin konum olarak sunulması	Haksız mahkûmiyet riski
Kapsama alanı haritalaması yapılmaması	Teorik BTS noktasının kullanılması, gerçek kapsama göz ardı	Yanıltıcı coğrafi atıf
Zaman dilimi hatası	UTC / yerel saat karışıklığı	Yanlış zaman çizelgesi
Telefon-kullanıcı özdeşleştirme	SIM kaydından kişi tespiti yapılması	Kimlik hatası riski
Veri boşluklarının görmezden gelinmesi	Eksik kayıt dönemlerinin raporlanmaması	Yanıltıcı süreklilik izlenimi
Anormal hücre seçiminin göz ardı edilmesi	Uzak hücreye bağlantının açıklanmaması	Hatalı konum çıkarımı

Not. Kaynak: Morrison & Enzinger (2018); Hargreaves & Chivers (2016); Ayers et al. (2014) temel alınarak derlenmiştir.

7. Uygulama Örnekleri: Farklı Suç Tiplerine Göre HTS Kullanımı

7.1 Cinayet ve Ağır Suç Soruşturmaları

Cinayet soruşturmalarında HTS analizi, genellikle iki kritik soruya yanıt aramak amacıyla kullanılmaktadır: (1) Şüpheli, suçun işlendiği saatte olay yeriyle coğrafi uyum gösteren bir baz istasyonuna kayıtlı mıydı? (2) Mağdurun telefonu, son kayıtlı konumundan itibaren ne yönde hareket etti ve son kayıt ne zamandı?

Bu soruşturmalarda HTS analizinin en güçlü işlevlerinden biri, mağdurun **kaybolma sonrası hareket örüntüsünün** yeniden oluşturulmasıdır. Mağdurun telefonu, sahibi artık hayatta olmasa ya da onu kullanmıyor olsa bile çevrimdışı olmadan önceki son baz istasyonu kaydını bırakmış olabilmektedir. Bu son kayıt, arama operasyonlarını yönlendirmek açısından değerli bir ipucu sağlar (Casey, 2011).

Bununla birlikte, bu tür davalarda adanmış bölgede çok sayıda baz istasyonunun bulunduğu kentsel ortamlarda bile kesin konum tespitinin mümkün olmadığı —yalnızca coğrafi bir alan tahmini yapılabildiği— unutulmamalı; bu sınırlılık jüriye açıkça aktarılmalıdır (Jain & Demers, 2019).

7.2 Organize Suç ve Uyuşturucu Kaçakçılığı

Organize suç soruşturmalarında HTS'nin en güçlü katkısı, **iletişim ağı analizi** aracılığıyla örgütsel yapıların ortaya konmasıdır. Çok sayıda şüpheliye ait HTS verilerinin bir arada analiz edilmesiyle; kimin yönetici, kimin kurye, kimin lojistik sorumlusu olduğuna dair örüntüler belirlenebilmektedir. İletişim zamanlamaları ve coğrafi örtüşmeler, koordineli hareketin bağımsız delilidir (Peterson, 2017).

Uyuşturucu kaçakçılığı davalarında HTS analizi, taşıma güzergâhlarını yeniden inşa etmek amacıyla da kullanılmaktadır. Bir aracın seyahat ettiği güzergâh boyunca sıralanan baz istasyonu kayıtları, güzergâhın teyidinde faydalı olmakla birlikte araçtaki kişi tespiti açısından ek delil gerektirmektedir. Araç içindeki telefon, aracın güzergâhını izlerken kimin bu aracı kullandığı her zaman HTS verisinden doğrudan çıkarılamaz (Hargreaves & Chivers, 2016).

7.3 Terörle Mücadele Soruşturmaları

Terörle mücadele bağlamında HTS analizi hem geriye dönük soruşturma hem de istihbarat amaçlı kullanılmaktadır. Geriye dönük analizde; saldırı öncesinde suikastçıların izlediği güzergâhlar, keşif faaliyetleri sırasında baz istasyonlarına kayıt düşen telefonlar ve saldırı sonrasında kaçış güzergâhı bu teknikle yeniden oluşturulabilmektedir. Bu kullanım, 2004 Madrid ve 2005 Londra saldırılarının soruşturmalarında kilit delil kaynağı olmuştur (Waidner & Backes, 2016).

Öte yandan bu alanda **geniş ölçekli toplu veri analizi** uygulamaları, ciddi hukuki ve etik tartışmalara konu olmaktadır. Belirli bir coğrafi alanda belirli bir anda baz istasyonuna kayıt olan tüm telefonların verisinin sorgulanması —*geofence warrant* olarak da bilinen bu uygulama— kitlesel mahremiyet ihlali riski taşımakta ve çeşitli yargı çevrelerinde tartışılmaktadır (Kerr, 2010).

7.4 Kayıp Kişi ve Kaçırma Vakaları

Kayıp kişi soruşturmalarında HTS analizi, kişinin son bilinen konumundan itibaren hareket izini takip etmek ve bölgedeki diğer telefonlarla etkileşimini belirlemek amacıyla kullanılmaktadır. Kaçırma vakalarında ise hem mağdurun hem de şüphelilerin telefonlarından elde edilen HTS verileri karşılaştırmalı olarak incelenmekte; ortak baz istasyonu kayıtları, iki kişinin aynı anda aynı bölgede bulunup bulunmadığının göstergesi olarak değerlendirilmektedir (Casey, 2011).

Önemli bir uyarı olarak belirtilmeli ki; iki kişinin aynı baz istasyonuna aynı anda kayıtlı olması, bu kişilerin birbirine yakın olduğunu değil; yalnızca aynı hücrenin kapsama alanında olduğunu göstermektedir. Bu alan onlarca km² olabildiğinden, söz konusu bulgu tek başına yetersizdir ve destekleyici delil olmaksızın fiziksel yakınlığın kanıtı olarak sunulamaz (Morrison & Enzinger, 2018).

8. İleri Analiz Yöntemleri ve Teknolojik Gelişmeler

8.1 Büyük Veri ve Makine Öğrenmesi Uygulamaları

Milyonlarca satır HTS kaydının manuel analizi zaman açısından mümkün değildir. Bu nedenle adli analistler giderek artan biçimde büyük veri araçları ve makine öğrenmesi algoritmalarından yararlanmaktadır. **Kümeleme algoritmaları** (K-means, DBSCAN), şüphelinin sıklıkla ziyaret ettiği coğrafi noktaları (ev, iş yeri, buluşma noktaları) otomatik olarak tespit edebilmektedir. **Anomali tespiti** algoritmaları, olağan davranış örüntüsünden sapan günleri ya da saatleri işaretleyerek analist dikkatini odaklamaktadır (Peterson, 2017).

Bununla birlikte, makine öğrenmesi tabanlı araçların adli bağlamda kullanılmasının ciddi metodolojik gereklilikleri beraberinde getirdiği unutulmamalıdır: Modelin eğitim verisi, dışarıdan bağımsız olarak doğrulanmış olmalı; çıktılar olasılıksal yorumla sunulmalı; ve algoritmanın kara kutu (black box) özelliği mahkeme önünde açıklanabilir metodoloji gerektiren hukuki standartlarla gerilim yaratabilmektedir (Faigman et al., 2014).

8.2 5G Ağlarında HTS Analizi: Değişen Tablo

Beşinci nesil (5G) ağların yaygınlaşması, HTS analizinin teknik boyutunu önemli ölçüde etkilemektedir. 5G'nin daha yoğun baz istasyonu ağı —özellikle küçük hücre (small cell) konuşlandırmaları— teorik olarak daha yüksek konumsal çözünürlük sağlayabilmektedir. Bir kentte birbirine yakın onlarca küçük hücrenin bulunması, Cell-ID kaydının işaret ettiği kapsama alanını önemli ölçüde daraltabilmektedir (Dahlman et al., 2018).

Öte yandan 5G'nin ağ dilimleme (network slicing) ve uç hesaplama (edge computing) mimarisi, veri işleme ve depolamanın merkezi olmayan bir yapıya kavuşması anlamına gelmektedir. Bu durum, adli veri toplamanın hukuki çerçevesini ve teknik prosedürünü karmaşıklaştırmaktadır: Verilerin hangi düğümde, hangi ülkenin yetki alanında depolandığı, sınır ötesi adli işbirliğini gerektiren yeni hukuki sorular doğurmaktadır (Waidner & Backes, 2016).

8.3 Gizlilik Artırıcı Teknolojilerin Etkisi

Şifreli iletişim uygulamalarının (Signal, WhatsApp, Telegram) yaygınlaşması, iletişim içeriğine erişimi güçleştirmektedir. HTS analizi, *içerik* değil; *trafik verisi* üzerine odaklandığından bu gelişmeden doğrudan etkilenmemektedir. Ancak uçtan uca şifreli uygulamaların kullanımı, geleneksel SMS ve sesli çağrıların yerini almaya başladığında, operatör kayıtlarında daha az iletişim olayı ve dolayısıyla daha seyrek baz istasyonu kayıtları görülmektedir. Bu durum, HTS analizinin coğrafi çözünürlüğünü azaltmaktadır (Kerr, 2010).

Bunun yanı sıra, Wi-Fi Calling ve VoIP uygulamalarının yaygınlaşması, sesli iletişimin mobil şebeke üzerinden değil; Wi-Fi erişim noktaları aracılığıyla gerçekleşmesini mümkün kılmaktadır. Bu tür çağrılar, klasik baz istasyonu kayıtlarına yansımayabilmekte ve önemli bir adli körlük noktası oluşturabilmektedir (Peterson, 2017).

9. Etik Boyutlar ve Mahremiyet Dengesi

HTS analizi, adli soruşturmalar açısından güçlü bir araç olmakla birlikte bireylerin mahremiyet haklarıyla köklü bir gerilim içindedir. Bu gerilim, yalnızca hukuki bir sorun değil; aynı zamanda bir etik tasarım sorunudur. Bir kişinin tüm hareketlerinin ve iletişim örüntülerinin geriye dönük olarak yeniden oluşturulabilmesi, *Büyük Birader* gözetim endişelerini somutlaştırmaktadır (Waidner & Backes, 2016).

Bu gerilimi yönetmek için adli telekomünikasyon pratiğinde orantılılık ilkesi merkezi bir yere sahiptir: Toplu veri yerine hedefe yönelik ve ölçülü veri talebi; soruşturmanın ağırlığıyla orantılı veri erişim yetkisi; elde edilen verilerin yalnızca soruşturmaya özgü kullanımı ve belirlenen saklama süresi sonrasında imhası bu ilkenin temel gerekliliklerdir (Kerr, 2010). Uluslararası insan hakları standartlarına göre mahremiyet hakkına müdahale; yasal dayanağa sahip olmalı, meşru bir amacı gerçekleştirmeli, demokratik toplumda zorunlu olmalı ve orantılı olmalıdır.

10. Sonuç

HTS analizi, modern adli soruşturmaların vazgeçilmez bir aracı haline gelmiştir. Mobil telefon kullanıcılarının her etkileşimde baz istasyonlarına bıraktığı dijital izler; konum tespiti, iletişim ağı analizi ve hareket örüntüsü yeniden inşası bakımından eşsiz bir kaynak oluşturmaktadır. Bu kaynağın doğru, güvenilir ve hukuka uygun biçimde kullanılması, hem adaletin tecellisi hem de temel hakların korunması bakımından belirleyici önem taşımaktadır.

Makalede ayrıntılı biçimde ele alındığı üzere, HTS analizinin adli güvenilirliği; metodolojinin titizliğine, kapsama alanı haritalamasının doğruluğuna, bilirkişi raporunun şeffaflığına ve mahkemenin teknik okuryazarlığına bağlıdır. Kesinlik yanılgısı, kapsama alanı belirsizliğinin göz ardı edilmesi ve telefon-kullanıcı özdeşleştirme hataları, hem haksız mahkûmiyetlere hem de suçluların beraat etmesine zemin hazırlayabilecek yapısal risklerdir.

5G ağlarının yaygınlaşması, makine öğrenmesi araçlarının adli uygulamalara entegrasyonu ve şifreli iletişim platformlarının büyümesi; HTS analizinin teknik çerçevesini sürekli olarak yeniden şekillendirmektedir. Bu değişime ayak uydurmak; adli analistler, hukuk pratisyenleri ve düzenleyiciler arasında sürekli bir diyalog ve kapasite geliştirme sürecini

zorunlu kılmaktadır. HTS analizinin doğru, orantılı ve denetlenebilir biçimde kullanılması; hem adil yargılanma hakkının hem de kamu güvenliğinin korunmasının temel güvencesidir.

Kaynakça

3GPP TS 23.003. (2021). Numbering, addressing and identification (Release 16). 3rd Generation Partnership Project.

Ayers, R., Brothers, S., & Jansen, W. (2014). Guidelines on mobile device forensics (NIST Special Publication 800-101 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-101r1

Carrier, B. D. (2006). Risks of live digital forensic analysis. Communications of the ACM, 49(2), 56–61. https://doi.org/10.1145/1113034.1113062

Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers and the internet (3rd ed.). Academic Press.

Dahlman, E., Parkvall, S., & Sköld, J. (2018). 5G NR: The next generation wireless access technology. Academic Press.

Faigman, D. L., Monahan, J., & Slobogin, C. (2014). Group to individual (G2I) inference in scientific expert testimony. University of Chicago Law Review, 81(2), 417–480.

Hargreaves, C., & Chivers, H. (2016). Recovery of mobile device forensic evidence from telecommunication networks. Digital Investigation, 17, 72–83. https://doi.org/10.1016/j.diin.2016.03.002

Jain, A., & Demers, A. (2019). Cell tower location forensics: Technical reliability and legal standards. Journal of Digital Forensics, Security and Law, 14(2), 1–22.

Kerr, O. S. (2010). Applying the fourth amendment to the internet: A general approach. Stanford Law Review, 62(4), 1005–1050.

Morrison, G. S., & Enzinger, E. (2018). What should a forensic practitioner's likelihood ratio be? Science & Justice, 58(3), 212–218. https://doi.org/10.1016/j.scijus.2017.10.004

Peterson, G. (2017). Mobile network forensics: Extracting and analyzing evidence from cellular networks. Elsevier.

Robertson, B., & Vignaux, G. A. (1995). Interpreting evidence: Evaluating forensic science in the courtroom. John Wiley & Sons.

Waidner, M., & Backes, M. (2016). Security and privacy challenges in the 5G era. IEEE Internet Computing, 20(5), 14–17. https://doi.org/10.1109/MIC.2016.101