5G İLE BİRLİKTE DEĞİŞEN KONUM VERİSİ
Daha Hassas mı, Daha Tehlikeli mi?

Küçük Hücre Mimarisi, Santimetre Düzeyinde Konum ve Mahremiyet Paradoksu

Bir Telekomünikasyon Mühendisi ve Mahremiyet Hukuku Uzmanıyla Söyleşi

Söyleşi / Interview

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

Anahtar Kelimeler: *5G • Konum Tespiti • Küçük Hücre • Geofence • Mahremiyet*

ÖZET

Dördüncü nesil (4G) hücresel ağlarda baz istasyonu kayıtları, yüzlerce metreden onlarca kilometreye uzanan geniş kapsama alanları nedeniyle yalnızca kaba konum tespitine olanak tanımaktaydı. Beşinci nesil (5G) ağlar ise bu tabloyu köklü biçimde değiştirmektedir: Yoğun küçük hücre (small cell) konuşlandırması, milimetre dalga bantları ve 3GPP Release 16-18'de tanımlanan ileri konumlandırma teknolojileri sayesinde 5G, kapalı alanlarda santimetre, açık alanlarda birkaç metre düzeyinde konum hassasiyeti sunabilmektedir. Bu dönüşüm, adli soruşturmalar açısından devrimsel bir fırsat sunarken bireysel mahremiyet için eşi görülmemiş bir tehdit oluşturmaktadır. Bu söyleşide; 5G konumlandırma teknolojisinin teknik temelleri, 4G ile karşılaştırmalı hassasiyet analizi, adli vakalarda fırsat ve sınırlılıklar, geofence arama kararlarının hukuki tartışması, operatör veri politikaları, GDPR ve AİHM çerçevesinde mahremiyet değerlendirmesi ile 6G'ye uzanan perspektif ele alınmaktadır.

Anahtar Kelimeler: *5G konumlandırma, küçük hücre, PRS, TDOA, RTT, AoA, AoD, geofence, konum mahremiyeti, 3GPP Release 16, adli telekomünikasyon, GDPR, Dördüncü Değişiklik*

ABSTRACT

In fourth-generation (4G) cellular networks, base station records allowed only coarse location determination due to coverage areas spanning from hundreds of meters to tens of kilometers. Fifth-generation (5G) networks are radically

transforming this landscape: through dense small cell deployment, millimeter-wave bands, and advanced positioning technologies defined in 3GPP Releases 16–18, 5G can deliver centimeter-level accuracy indoors and a few meters outdoors. This transformation presents a revolutionary opportunity for forensic investigations while simultaneously creating an unprecedented threat to individual privacy. This interview addresses the technical foundations of 5G positioning technology, comparative accuracy analysis with 4G, opportunities and limitations in forensic cases, the legal debate over geofence search warrants, operator data policies, privacy assessment under the GDPR and ECHR frameworks, and the perspective extending toward 6G.

EDİTÖR NOTU: Bu söyleşi, 5G ağlarının getirdiği konum verisi hassasiyetini hem teknik hem hukuki boyutlarıyla ele almaktadır. Herhangi bir davaya, kişiye ya da kuruma doğrudan atıf yapılmamış; amaç teknik ve hukuki farkındalık oluşturmaktır.

I. 5G Konumlandırma Teknolojisi: Teknik Temeller

SORU: 4G ile karşılaştırdığımızda 5G ağları konum tespitinde gerçekte ne kadar farklı bir tablo sunuyor?

Bu fark, derece farkı değil; tür farkıdır. 4G LTE'de bir kullanıcının konumu, baz istasyonu kaydı (Cell-ID) aracılığıyla belirlendiğinde yüzlerce metre ile onlarca kilometre arasında değişen bir belirsizlik payı söz konusudur. Bu geniş alan; kentsel ortamlarda birkaç yüz metreye, kırsal alanlarda onlarca kilometreye çıkabilir. Timing Advance (TA) parametresiyle bu alan bir halka dilimi şeklinde daraltılabilse de sonuç hâlâ oldukça kaba bir tahmindir.

5G ise bu tabloya üç temel yenilikle yaklaşıyor. **Birincisi, fiziksel mimari:** 5G küçük hücreleri (small cells), makro baz istasyonlarının kapladığı geniş alanlara kıyasla çok daha küçük coğrafi bölgelere hizmet verir. Kentsel ortamlarda her birkaç yüz metrede bir küçük hücre bulunduğundan, Cell-ID kaydının işaret ettiği alan dramatik biçimde daralır. Bu tek başına bile konum hassasiyetini ciddi ölçüde artırır.

İkincisi, yeni konumlandırma sinyalleri: 3GPP Release 16 ile 5G NR, native konumlandırma desteği için tasarlanmış **Positioning Reference Signals (PRS)** adlı yeni referans sinyalleri tanımlamıştır. Bu sinyaller; geniş bant genişliği (FR1'de 100 MHz'e, mmWave FR2'de 400 MHz'e kadar), beamforming kabiliyeti ve Massive MIMO anten dizileri sayesinde LTE'nin çok ötesinde bir konum çözünürlüğü sunar.

Üçüncüsü, yeni ölçüm yöntemleri: Dwivedi ve diğerleri (2021), 3GPP Rel-16 ile 5G'ye gelen konumlandırma tekniklerini kapsamlı biçimde analiz etmiştir: *Round-Trip Time (RTT)* terminal ile baz istasyonu arasındaki sinyal gidiş-dönüş süresini ölçer; *Time Difference of Arrival (TDOA)* terminale birden fazla baz istasyonundan gelen sinyallerin varış zaman farklarını kullanır; *Angle of Arrival (AoA)* ve *Angle of Departure (AoD)*, Massive MIMO anten dizileri aracılığıyla sinyalin geldiği açıyı saptayarak konumu

üçgenler. Bu tekniklerin kombinasyonu, tek bir yöntemin yapamayacağı hassasiyeti mümkün kılar.

HASSASİYET TABLOSU: *3GPP Rel-16: Kapalı alanda 3 m, açık alanda 10 m. Rel-17: Kapalı IIoT alanında 20 cm yatay / 1 m dikey. Rel-18: Taşıyıcı faz ölçümü ile santimetre düzeyi. Bu değerler, GSM'in 'yüzlerce metre' belirsizliğiyle kıyaslandığında neredeyse GPS düzeyinde bir hassasiyete işaret etmektedir.*

SORU: Santimetre düzeyinde konum hassasiyeti demek ne anlama geliyor somut olarak? Hangi teknoloji bunu mümkün kılıyor?

Bu soruyu yanıtlamak için önce 'konum hassasiyeti' kavramını operasyonel biçimde tanımlamak gerekiyor. Konum hassasiyeti, terminalin gerçek konumu ile hesaplanan konum tahmini arasındaki hatanın belirli bir olasılık düzeyinde (genellikle %90) kaldığı mesafedir. 3 metre %90'lık hassasiyet demek, tahminlerin %90'ının gerçek konumdan en fazla 3 metre uzakta olduğu anlamına gelir.

Bu hassasiyeti sağlayan teknolojilerin başında 3GPP Release 18 ile gelen **taşıyıcı faz (carrier phase — CP) ölçümleri** gelir. Geleneksel yöntemler sinyalin gücünü ya da varış zamanını ölçerken, CP ölçümü radyo dalgasının fazını —dalganın hangi noktasında olduğunu— saptamaktadır. Bu yöntem, faz uzunluğunun milimetre boyutunda olması nedeniyle çok daha ince bir konum granülaritesi sunar. 5G HUB Technologies (2024) ve Nokia'nın (tarihsiz) teknik dokümanları bu tekniğin IIoT (Industrial Internet of Things) senaryolarında santimetre düzeyi hassasiyet sağladığını belgelemektedir.

Bir diğer kritik etken, **bantların genişlemesi**dir. LTE'de maksimum 20 MHz olan bant genişliği, 5G NR'da FR1'de 100 MHz'e, milimetre dalga FR2 bantlarında ise 400 MHz'e çıkmaktadır. TDOA gibi zamana dayalı yöntemlerde bant genişliği doğrudan zaman çözünürlüğünü belirler; daha geniş bant, daha kısa zaman kesimi, daha doğru mesafe tahmini anlamına gelir. 3GPP'nin (2022) yayımladığı Rel-17 konumlandırma geliştirmeleri dokümanı bu ilişkiyi matematiksel olarak ortaya koymaktadır.

SORU: Küçük hücre mimarisi konum hassasiyetini nasıl etkiliyor? Bu sadece teknik bir ayrıntı mı, yoksa paradigma değişikliği mi?

Paradigma değişikliği. Makro baz istasyonları, birkaç kilometre yarıçaplı alanlara hizmet eder ve bu alanlardaki herhangi bir kullanıcı o istasyona bağlanabilir. Küçük hücrelerin — mikro, piko ve femto hücreler— kapsama alanı ise 50 ila 300 metre arasındadır. Bu, Cell-ID kaydının başlı başına sağladığı konum tahminini makro bir baz istasyonuna kıyasla onlarca kat daraltır.

ISACA Journal'da yayımlanan kapsamlı çalışma (2024), bu durumu özetliyor: '5G'nin sunduğu coğrafi hassasiyet derecesi ve toplanabilen yüksek veri hacmi, kullanıcıların rızası olmadan gözetim amacıyla kullanılabilir.' Bu tespit, küçük hücre yoğunluğunun hem konum çözünürlüğünü hem de olası gözetim kapasitesini aynı anda artırdığına dikkat çekmektedir.

> Özellikle millimetre dalga (mmWave) bantlarında çalışan 5G hücreleri, 50–200 metre yarıçaplı son derece küçük coğrafi alanları kapsar. Bu ortamlarda Cell-ID kaydı; belirli bir sokağa, belirli bir binanın cephesine hatta büyük kapalı alanlarda belirli bir kata işaret edebilir. LTE'nin 'semt içinde' söyleyebildiği şeyi, 5G 'hangi binanın önünde' düzeyinde söyleyebilir hale gelmektedir.

Tablo 1. *GSM'den 5G'ye Konum Hassasiyetinin Evrimi*

Nesil	Teknik	Tipik Hassasiyet	Mekanizma	Standart
2G (GSM)	Cell-ID	100 m – 35 km	Baz istasyonu koordinatı	ETSI GSM
2G+ (GSM)	Cell-ID + TA	~550 m (1 TA birimi)	Gidiş süresi halkası	3GPP TS 04.08
3G (UMTS)	Cell-ID + RTT	50 m – 5 km	Yuvarlak gidiş süresi	3GPP TS 25
4G (LTE)	E-CID, OTDOA	40 m – 2 km	Gelişmiş Cell-ID, TDOA	3GPP Rel. 9
5G Rel-16	PRS, RTT, TDOA, AoA/AoD	Kapalı: 3 m / Açık: 10 m	Geniş bant + çok antenli	3GPP Rel-16
5G Rel-17	PRS + CP	IIoT: 20 cm / Açık: <5 m	CP + iyileştirilmiş PRS	3GPP Rel-17
5G Rel-18	Taşıyıcı faz (CP) + LPHAP	**Santimetre düzeyi**	Faz ölçümü + bant birleştirme	3GPP Rel-18

Not. Kaynak: Dwivedi et al. (2021); 3GPP (2022); RCR Wireless (2022); 5G HUB Technologies (2024); Nokia (tarihsiz) temel alınarak derlenmiştir. IIoT: Industrial Internet of Things; CP: Carrier Phase; LPHAP: Low Power High Accuracy Positioning.

II. Adli Fırsat: 5G Konum Verisi Soruşturmalarda Ne Sağlıyor?

> **SORU: 5G'nin sunduğu bu artırılmış hassasiyet, adli soruşturmalarda somut olarak hangi yeni imkânları açıyor?**

Adli açıdan bu değişimin anlamını şu şekilde somutlaştırabiliriz: 4G döneminde bir şüphelinin o gün o semtte olduğu söylenebiliyordu; 5G döneminde ise belirli bir binanın önünde mı, içinde mi, yoksa onlarca metre ötesinde mi olduğu tespit edilebilir hale gelebilir. Bu, özellikle aşağıdaki senaryolarda belirleyici bir fark yaratmaktadır:

Cinayet ve ağır suç soruşturmaları: Bir mağdurun ya da şüphelinin belirli bir anda olay yeriyle gerçekten çakışıp çakışmadığının tespiti, 4G'de belirsizliğini koruyan çok sayıda davayı 5G ile netleştirebilir. 4G'de 'o hücre alanı içindeydi' derken 5G ile 'o binanın girişine 30 metre mesafedeydi' diyebilmek, mahkeme sürecinde niteliksel olarak farklı bir delil oluşturur.

Organize suç ve terör: Birden fazla şüphelinin hareketlerinin eş zamanlı ve yüksek hassasiyetle izlenmesi; buluşma noktalarının tespiti, koordineli hareketin belgelenmesi ve keşif faaliyetlerinin yeniden inşası açısından 5G veri yoğunluğu ve hassasiyeti çok daha güçlü bir analitik temel sunmaktadır.

Olayların yeniden inşası: Bir kavga, trafik kazası ya da kalabalık ortamında gerçekleşen bir olay söz konusu olduğunda, 5G ağının yoğun küçük hücre yapısı; olaya karışanların birbirlerine olan fiziksel mesafesini ve hareketlerini çok daha ayrıntılı biçimde yeniden oluşturmaya imkân tanır. Springer Nature üzerinden yayımlanan 5G ağ adli bilişimi çalışması (Arshad et al., 2018), bu ağlarda elde edilebilecek konum kanıtlarının kalitesinin önceki nesillerle kıyaslanamayacak düzeye ulaştığını vurgulamaktadır.

SORU: Bu hassasiyet artışının adli süreçteki sınırlılıkları neler? Her şey bu kadar parlak mı görünüyor?

Hayır, önemli sınırlılıklar var ve bunların dürüstçe ifade edilmesi metodolojik zorunluluktur. 'Santimetre hassasiyet' ifadesi, kontrollü deney koşullarında ya da endüstriyel fabrika (IIoT) ortamlarında elde edilen değerleri yansıtmaktadır; gerçek bir şehrin kaotik radyo ortamında bu değerlere ulaşmak çok daha güçtür.

Birinci sınırlılık: **Standart operatör kayıtlarının bu hassasiyeti içermemesi.** 5G ağları teknik olarak santimetre hassasiyeti sunabilse de bir operatörün standart HTS (Historical Traffic Signalling) kaydına hangi veri düzeyinin düştüğü, ülkeden ülkeye ve operatörden operatöre farklılaşmaktadır. Operatörler genellikle fatura ve ağ yönetimi amacıyla kaydettikleri veriyi depolar; konum bilgisi çoğunlukla baz istasyonu kimliğiyle sınırlıdır. Bu kısıt, 5G'nin teorik hassasiyetinin pratikte her zaman kullanılabilir olmadığı anlamına gelir.

İkinci sınırlılık: **Geriye dönük analiz paradoksu.** 5G konumlandırmasının yüksek hassasiyeti, gerçek zamanlı ölçümlere dayanır. Geçmişe yönelik bir adli soruşturma söz konusu olduğunda, o andaki ağ koşulları —hücre yükü, engelleyici nesneler, atmosfer— yeniden oluşturulamaz. Hargreaves ve Chivers'ın (2016) HTS analizindeki metodolojik çerçevesi burada da geçerliliğini korur: Geriye dönük ölçüm doğrulaması mümkün değildir.

Üçüncü sınırlılık: **Çok yollu yayılım ve kentsel engeller.** Millimetre dalga bantları, beton duvarlardan, yağmurdan ve hatta yoğun insan kalabalığından ciddi ölçüde etkilenir. Bu koşullar, sinyal yolunu karmaşıklaştırarak konum tahmininde teorik değerlerin çok üstünde hatalar üretebilir. IIoT fabrika ortamında geçerli olan hassasiyet, açık havada kalabalık bir kentsel ortamda otomatik olarak geçerli değildir.

ADLİ UYARI: *5G'nin teorik konum hassasiyeti ile operatörün standart kaydına yansıyan veri ve geriye dönük adli analizde kullanılabilecek bilgi arasında önemli bir uçurum bulunmaktadır. Bu uçurumun göz ardı edilmesi, daraltılmış baz analizindeki hataların bir üst versiyonunu üretir.*

SORU: 5G'nin sunduğu bu konum verisi, 4G HTS analizinde karşılaştığımız daraltılmış baz sorununu çözüyor mu?

Bu son derece önemli bir soru ve yanıtı iki katmanlı. **Teorik katmanda:** Evet, 5G ağları 4G'ye kıyasla çok daha küçük kapsama alanları ve çok daha yüksek hassasiyet sağlayabilir. Eğer operatör gerçek zamanlı konumlandırma verilerini kayıt altına alıyorsa ve bu veri adli süreçte kullanılabiliyorsa, 4G'nin kaba tahminlerinin çok ötesine geçilebilir.

Pratik katmanda: Hayır, 4G HTS analizindeki temel sorunlar 5G'de de varlığını sürdürmektedir. Standart operatör kaydı hâlâ öncelikle baz istasyonu kimliğini içerir; bu bilgi 5G küçük hücresiyle birleşince kapsama alanı daralır ancak kesin konum bilgisi vermez. Geriye dönük doğrulama imkânsızlığı devam eder. Telefon-kullanıcı özdeşleştirme sorunu çözülmüş değildir. Dolayısıyla 5G, daraltılmış baz analizinin meşruiyetini sağlamaz; bu analizin 4G dönemindeki mantıksal hataları 5G'de de geçerliliğini korur. 5G'nin sunduğu gerçek fırsatlar başkadır: İleride açıklayacağım gerçek zamanlı konum servisleri ve geofence uygulamaları.

III. Mahremiyet Tehdidi: 5G Gözetim Kapasitesini Nasıl Dönüştürüyor?

SORU: 5G'nin konum hassasiyeti neden bu denli büyük bir mahremiyet tehdidi oluşturuyor?

Bu soruyu yanıtlamak için önce şunu hatırlatayım: Konum verisi, diğer kişisel veri türlerinden farklı olarak **gerçek dünyadaki davranışların haritalanması** anlamına gelir. Birisinin nereye gittiğini, ne zaman gittiğini, kiminle aynı anda aynı yerde bulunduğunu biliyor olmak; hasta olduğunda hangi hastaneye gittiğini, hangi dini mekânları ziyaret ettiğini, hangi siyasi toplantılara katıldığını, kimlerle buluştuğunu dolaylı olarak ortaya çıkarır.

4G'de bu bilgiler kaba ve belirsizdi: Bir kişinin o semtte olduğu biliniyordu, ama hangi binada olduğu bilinemiyordu. 5G ile bu belirsizlik dramatik biçimde azalıyor. Bir şehrin 5G altyapısına sahip olan —ya da bu veriye erişen— aktör, bireylerin günlük hareketlerini bina ve kat düzeyinde izleyebilir hale gelebilir.

ISACA Journal (2024), bu durumu şu sözlerle çerçeveler: '5G'nin sunduğu coğrafi hassasiyet derecesi ve yüksek hacimli veri toplama kapasitesi, kullanıcıların rızası olmadan gözetim amacıyla kullanılabilir.' Canzittu ve diğerleri (2021), PMC'de yayımladıkları çalışmada 5G'nin konum mahremiyetini doğrudan tehdit eden üç yeni boyut getirdiğini tespit ediyor: Daha hassas konumlandırma sinyalleri, OTT (over-the-top) hizmet sağlayıcılarına konum bilgisi aktarımı ve yapay zeka tabanlı konum çıkarımı araçları.

SORU: 'OTT hizmet sağlayıcılarına konum bilgisi aktarımı' derken ne kastediyorsunuz? Bu nasıl çalışıyor?

Bu mesele çok az konuşulan ama son derece önemli bir boyut. 5G mimarisinin sunduğu ağ API'leri, operatörlerin belirli yetkili üçüncü taraflara —uygulama geliştiricileri, reklam şirketleri, akıllı şehir platformları— gerçek zamanlı ya da gecikmeli konum verisi sağlamasına teknik olarak olanak tanımaktadır. Bu, 4G'de standart olarak mevcut olmayan bir özellik.

3GPP Release 16 ile tanımlanan Location Management Function (LMF) mimarisi ve 5G core API'leri, ağ içi konumlandırma verilerini harici sistemlere açabilmektedir. Bu entegrasyon, örneğin bir alışveriş merkezi uygulamasının 5G ağından kullanıcının içerideki tam konumunu santimetre hassasiyetiyle öğrenmesine —teknik olarak— imkân tanıyabilir.

Tabii ki yasal çerçeve bunu sınırlar; ancak teknik kapasite mevcuttur ve kullanıcının bu veri akışından habersiz olma riski taşıdığı anlamına gelir.

Canzittu ve diğerleri (2021), bu riski 'OTT tehdit vektörü' olarak tanımlamakta ve mevcut gizlilik düzenlemelerinin bu aktarım zincirini denetlemek için yeterli olmadığını savunmaktadır. GDPR bağlamında değerlendirildiğinde bu aktarım; açık rıza, meşru menfaat ya da sözleşme ifası gerekçelerinden birini gerektirmekte ve veri aktarımının kapsamı ile amacının kullanıcıya şeffaf biçimde açıklanmasını zorunlu kılmaktadır.

SORU: Geofence arama kararları nedir ve 5G bu tartışmayı nasıl alevlendiriyor?

Geofence arama kararı (geofence warrant), kolluk birimlerinin belirli bir coğrafi alan ve zaman diliminde o bölgede bulunan tüm cihazların konum verilerini üçüncü taraflardan — Google, Apple, operatörler— talep ettiği bir soruşturma tekniğidir. Temelde 'Bu sokakta, bu saatte hangi telefonlar vardı?' sorusuna yanıt arar.

Bu teknik, 4G döneminde Google'ın Sensorvault veritabanı üzerinden kullanılmaya başlanmıştır. Uygulamanın hukuki meşruiyeti tartışmalıdır: ABD'de Dördüncü ve Beşinci Devre Mahkemeleri 2024'te birbiriyle çelişen kararlar vermiştir. Columbia Üniversitesi Hukuk Fakültesi incelemesine (2025) göre *United States v. Chatrie* (4. Devre, 2024) davası, geofence kararının Dördüncü Değişiklik kapsamında arama sayılmadığına hükmederken 5. Devre aksi yönde karar vermiştir. Dava, ABD Yüksek Mahkemesi'ne taşınmak üzere 2026'da certiorari onayı almıştır.

5G bu tartışmayı iki katlı alevlendiriyor. **Birincisi, alan sorununu büyütüyor:** 4G geofence'i, yüzlerce metrelik kapsama alanı nedeniyle suçla hiçbir ilgisi olmayan çok sayıda kişiyi kapsama alırdı. 5G'nin küçük hücre yapısıyla hem hedef alan daraltılabilir — ki bu savunucuların istediği— hem de çok daha yüksek hassasiyette veri elde edilebilir — ki bu eleştirmenleri endişelendiriyor.

İkincisi, yeni aktörler yaratıyor: Google, 2024 sonunda konum geçmişini Sensorvault'tan cihaza taşıma kararını hayata geçirdi. Bu karar, geofence taleplerine yanıt verme kapasitesini fiilen kısıtladı. Ancak düşünce kuruluşu TLPC'nin Haziran 2025'te yayımladığı politika raporu, Google'ın bu adımının yarattığı boşluğu operatörlerin ve diğer konum veri sağlayıcılarının doldurabileceğine dikkat çekiyor. 5G operatörleri, daha zengin ve hassas konum verisiyle bu yeni tablonun merkezine oturabilir.

GEOFENCE PARADOKSİ: *Geofence kararları masum kişileri suç soruşturmalarına dahil eder; sanıkların suçsuz oldukları kanıtlanana kadar verilerine el konulmuş olur. 5G'nin hassasiyeti bu riski azaltabilir; ancak veri zenginliğini artırarak mahremiyet ihlaline zemin hazırlar. İki kenar keskin bir bıçak.*

Tablo 2. *5G Konum Verisinin Adli Fırsatları ve Mahremiyet Tehditleri*

Boyut	Adli Fırsat	Mahremiyet Tehdidi
Konum hassasiyeti	Olay yerini kimin kapladığını santimetre düzeyinde belirleyebilme	Dini, tıbbi, siyasi mekân ziyaretlerinin bina düzeyinde izlenmesi
Küçük hücre yoğunluğu	Hareket örüntüsünün çok daha ince granülaritede yeniden inşası	Şehir içi her hareketin dakika dakika belgelenmesi
OTT veri aktarımı	Yasal çerçevede üçüncü taraf konum verisi zenginleştirmesi	Rızasız konum verisi üçüncü şirketlere ulaşabilir
Gerçek zamanlı izleme	Şüpheli takibinde anlık konum güncellemesi	Yetkisiz aktörlerin anlık gözetim kapasitesi
Yüksek veri hacmi	İletişim ağı ve sosyal örüntü analizi için zengin veri	Büyük ölçekli toplu gözetim için hammadde
AI tabanlı konum çıkarımı	Mevcut veriden örtük örüntülerin analizi	Söylenmeyen davranışların tahmin edilmesi

Not. Kaynak: ISACA (2024); Canzittu et al. (2021); TLPC (2025); Davidson & Byers (2026) temel alınarak derlenmiştir.

IV. Hukuki Çerçeve: GDPR, AİHM ve Türk Hukuku

> **SORU: Avrupa hukuku bu durumu nasıl ele alıyor? GDPR 5G konum verisi için yeterli bir koruma sunuyor mu?**

GDPR (Genel Veri Koruma Yönetmeliği), konum verisini açıkça **kişisel veri** olarak tanımlamaktadır. Hassas konum verisi —dini mekân, sağlık kurumu veya siyasi toplantı alanını işaret eden— ise özel kategori veri statüsüne girebilir ve daha yüksek koruma eşiğine tabi tutulabilir. Bu çerçevede 5G operatörlerinin topladığı konum verisi; meşru amaç, açık rıza ya da yasal yükümlülük olmaksızın işlenemez ve üçüncü taraflarla paylaşılamaz.

Bununla birlikte GDPR'nin 5G gerçekliğiyle uyumu tartışmalıdır. Canzittu ve diğerleri (2021), mevcut düzenlemenin OTT aktarım zincirini —operatörden API aracılığıyla uygulama geliştiricisine oradan reklam ağlarına— tam olarak denetleyemediğini öne sürmektedir. Hassas konum verilerinin işlendiği her halkada sorumluluk tespiti ve denetimi, düzenleyici kapasiteyi zorlayan bir komplekslikte dir.

AİHM içtihadı da bu alanda net bir çerçeve sunmaktadır. *Zakharov/Rusya (2015)* ve *Szabó ve Vissy/Macaristan (2016)* kararları; telekomünikasyon verilerine toplu ve hedefsiz erişimin Sözleşme'nin 8. maddesi kapsamında özel hayata saygı hakkını ihlal ettiğine hükmetmiştir. Bu içtihatlar, 5G'nin sunduğu yüksek hassasiyetli konum verisine yönelik toplu erişim mekanizmalarının meşruiyetini temelden sorgulamaktadır. Müdahalenin zorunlu, orantılı ve somut bir suç şüphesine dayalı olması gerekmektedir.

> **SORU: Türk hukuku 5G konum verisinin toplanması, işlenmesi ve adli kullanımı açısından nasıl bir çerçeve sunuyor?**

6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), kişisel veri olarak konum bilgisini kapsamaktadır. KVKK'ya göre konum verisi; açık rıza, yasal yükümlülük ya da

meşru menfaat gerekçelerinden biriyle işlenebilir. Hassas veri kategorileri için ise açık rıza zorunlu tutulmaktadır. Konum verisinin hangi hassasiyet düzeyinde 'hassas' nitelik kazandığı meselesi ise 5G bağlamında henüz netleşmemiş bir yorumlama sorunudur.

Adli kullanım açısından CMK 135. maddesi, elektronik iletişimin denetlenmesini; 138. madde ise tesadüfen elde edilen delillerin kullanımını düzenlemektedir. 5G'nin sunduğu gerçek zamanlı yüksek hassasiyetli konum verisi, bu çerçevede ya önceden mahkeme kararıyla talep edilecek ya da operatörün mevcut HTS kaydından geriye dönük çekilecektir. Teknik açıdan mevcut HTS kayıtlarının 5G'nin teorik hassasiyetini tam olarak yansıtıp yansıtmayacağı ise operatör politikasına bağlıdır.

Önemli bir boşluk olarak şunu belirtmek gerekir: Türkiye'de 5G ticari dağıtımı 2025–2026 dönemi itibarıyla başlamaktadır. 5G konum verisinin KVKK ve CMK çerçevesinde nasıl değerlendirileceğine ilişkin içtihat henüz oluşmamıştır. Bu dönemin, hem adli uygulamacılar hem hukuk akademisyenleri hem de düzenleyiciler açısından izlenmesi büyük önem taşımaktadır.

V. Google'ın Politika Değişikliği ve Geofence'in Geleceği

SORU: Google'ın 2024 sonunda Sensorvault'u kaldırması geofence tartışmasını nasıl değiştirdi?

Bu gelişme geofence tartışmasının en önemli dönüm noktalarından biridir. Google, yıllarca konum geçmişini merkezi Sensorvault veritabanında saklamış ve kolluk birimlerinin bu veritabanına geofence kararlarıyla erişmesine olanak tanımıştır. Aralık 2024'te yürürlüğe giren politika değişikliğiyle Google, kullanıcıların konum geçmişini Sensorvault yerine doğrudan cihazlarında saklamaya ve varsayılan saklama süresini kısaltmaya başladı.

Suffolk Üniversitesi Hukuk Fakültesi dergisindeki analiz (2025), bu değişikliğin pratikte geofence taleplerini büyük ölçüde işlevsiz kılacağını öngörmektedir: Cihazda saklanan veri, Google sunucusuna yöneltilecek mahkeme kararıyla elde edilemez; bunun için cihaza doğrudan fiziksel erişim gerekir.

Ancak TLPC'nin politika raporu (2025) kritik bir uyarıda bulunmaktadır: Google'ın bu adımı yarattığı boşluğu diğer aktörler dolduracaktır. 5G operatörleri, akıllı şehir platformları, reklam ağları ve konuma dayalı hizmet sağlayıcıları; farklı saklama politikaları ve farklı hukuki işbirliği eşikleriyle konum verisi birikiminde yeni odak noktaları haline gelebilir. Davidson ve Byers'ın (2026) çalışması bu sorunun —dinamik mekânsal örnekleme ve uygun geofence yarıçapının belirlenmesi— hâlâ çözümsüz olduğunu matematiksel olarak ortaya koymaktadır.

SORU: Geofence tartışması önümüzdeki dönemde nereye gidiyor? Yüksek Mahkeme bu soruyu çözebilecek mi?

ABD Yüksek Mahkemesi'nin 2026 Ocak'ta *Chatrie v. United States* davasında certiorari onaylaması, bu soruyu nihayet çözüme kavuşturabileceğini düşündürüyor. Ancak Yüksek Mahkeme'nin kararı yalnızca ABD hukukunu bağlar; uluslararası tablo ülkeden ülkeye farklılaşmaya devam edecektir.

Temel hukuki gerilim şu iki ilke arasındadır: **Üçüncü taraf doktrini** (third-party doctrine), bireyin gönüllü olarak bir üçüncü tarafa verdiği bilgi üzerinde gizlilik beklentisi olamayacağını söyler; bu doktrinde konum verisi operatöre ya da Google'a gönüllü olarak aktarılmış sayılır. **Mosaic teorisi** ise *Carpenter v. United States* (2018) kararında şekillenmeye başlamış; uzun süreli ve kapsamlı dijital gözetimin bir bütün olarak anlamlı bir konum hikayesi oluşturduğunu ve arama sayılması gerektiğini savunur.

5G bu ikinci teoriye güçlü bir zemin sağlamaktadır: Santimetre hassasiyetinde ve sürekli güncellenen konum verisi, üçüncü taraf doktrininin öngördüğü sıradan veri paylaşımının çok ötesinde bir gözetim kapasitesi oluşturduğunu somutlaştırmaktadır. Yüksek Mahkeme'nin bu noktayı nasıl ele alacağı, dijital çağın en kritik mahremiyet kararlarından biri olacaktır.

VI. 6G ve Ötesi: Tahmin mü, Gerçek Zamanlı İzleme mi?

SORU: 6G araştırmaları konum verisi açısından hangi yeni boyutlar getiriyor?

6G, konum ve iletişimi tek bir sistemde birleştiren **ISAC (Integrated Sensing and Communication)** konsepti üzerine kurgulanmaktadır. Bu yaklaşımda radyo dalgaları hem haberleşme hem de çevre algılama amacıyla —tıpkı bir radar gibi— kullanılacaktır. Canzittu ve diğerleri (2021), bu gelişmeyi açıkça ifade ediyor: 'Konum mahremiyeti, alt-milimetre dalga iletiminin çok daha hassas konum çıkarımı sağlayacağı 6G ağlarında çok daha büyük bir risk haline gelecektir.'

Bunun anlamı şudur: 6G, yalnızca kullanıcının cihazının konumunu değil; kullanıcının fiziksel pozisyonunu, hareketini, hatta belirli ölçüde nesnelerin ve kişilerin oda içindeki konumunu tespit edebilir. Bir 6G baz istasyonu, kapsama alanındaki bir odada kaç kişinin bulunduğunu ve bunların nerede durduğunu —duvarların arkasını dahil ederek— 'görebilir' hale gelebilir. Bu, adli soruşturmalar için devrimsel bir araç; mahremiyet için ise emsalsiz bir tehdit.

Yapay zeka tabanlı konum çıkarımı da bu tabloya eklenmektedir: Geçmiş hareket örüntülerinden öğrenen makine öğrenmesi modelleri, yalnızca mevcut veriyle değil; gelecekteki muhtemel konumu da tahmin edebilir. Bu 'tahmine dayalı konum' kapasitesi, suç önleme perspektifinden çekici görünse de bireylerin henüz gerçekleşmemiş eylemlerine göre gözetlenmesi meselesini de gündeme taşır.

SORU: Son olarak: Bu tablo karşısında bir vatandaş olarak ne yapılabilir? Ve düzenleyiciler ne yapmalı?

Bireysel düzeyde pratik adımlar sınırlı ama anlamlı:

- Konum servislerini yalnızca kullanım sırasında etkin tutun; arka plan konum erişimini kısıtlayın.
- Hangi uygulamaların konum iznine sahip olduğunu düzenli olarak denetleyin; gerekli olmayanları iptal edin.
- VPN kullanımı IP adresini gizler; ancak operatör düzeyindeki baz istasyonu kaydını engelleyemez. Bunu bir mahremiyet aracı olarak aşırı güvenmek hatalıdır.

- Sensör erişimini kısıtlayan gizlilik odaklı mobil işletim sistemleri (GrapheneOS gibi) daha kapsamlı koruma sunar; ancak kullanım zorluğu vardır.
- Konum geçmişi saklama seçeneklerini uygulama ve platform düzeyinde dikkatlice değerlendirin; Google Timeline, Apple Significant Locations gibi özellikleri gözden geçirin.

> Düzenleyici düzeyde ise şu adımlar öncelikli olmalıdır: **Birincisi,** 5G operatörleri için konum verisi saklama standartlarının minimum düzeyde tutulması ve açık yasal çerçeveye bağlanması. **İkincisi,** OTT aktarım zincirine ilişkin şeffaflık yükümlülüklerinin güçlendirilmesi; kullanıcının hangi verinin kime aktarıldığını gerçek zamanlı olarak görebilmesi. **Üçüncüsü,** geofence arama kararlarına orantılılık, kapsam sınırlılığı ve zorunluluk kriterleri getirilmesi. Dördüncüsü ve belki en önemlisi: 5G ve 6G'nin sunduğu konumlandırma kapasitesi, mevcut hukuki çerçevelerden önce geliştirilerek düzenleyicilerin sürekli 'yakalamaya çalıştığı' bir teknolojiyi doğurmuştur. Bu farkın kapatılması; akademi, sanayi, sivil toplum ve düzenleyicilerin sürekli diyalogunu zorunlu kılmaktadır.

— Söyleşi Sonu —

Kaynakça

3GPP. (2022). 5G NR positioning enhancements, Release 17 (TR 38.857). 3rd Generation Partnership Project.

Arshad, J., Khan, M. A., Abbas, A., Iqbal, W., Amjad, M. F., Abbas, H., & Rashid, I. (2018). Towards 5G cellular network forensics. EURASIP Journal on Information Security, 2018(1), 14. https://doi.org/10.1186/s13635-018-0078-7

Canzittu, M., Karray, M., Maruta, S., & Vaton, S. (2021). Location-privacy leakage and integrated solutions for 5G cellular networks and beyond. Sensors (MDPI), 21(15), 5135. https://doi.org/10.3390/s21155135

Columbia Undergraduate Law Review. (2025). Mapping the future of surveillance: Geofence warrants and the risks of Chatrie. https://www.culawreview.org/journal/mapping-the-future-of-surveillance-geofence-warrants-and-the-risks-of-chatrie

Congress.gov. (2026, January 22). Geofence warrants and the Fourth Amendment. CRS Legal Sidebar LSB11274. https://www.congress.gov/crs-product/LSB11274

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

Davidson, M., & Byers, J. (2026). The problem of dynamic spatial sampling and geofence surveillance. arXiv preprint arXiv:2603.28958. https://arxiv.org/pdf/2603.28958

Dwivedi, S., Shreevastav, R., Munier, F., Nygren, J., Siomina, I., Lyazidi, Y., Shrestha, D., Lindmark, G., Ernström, P., Stare, E., Razavi, S. M., Muruganathan, S., Masini, G., Busin, Å., & Gunnarsson, F. (2021). Positioning in 5G networks. IEEE Communications Magazine, 59(11), 38–44. https://arxiv.org/pdf/2102.03361

5G HUB Technologies. (2024, March 17). Precision and power: The evolution of 5G NR positioning from Release 16 to 18. https://5ghub.us/precision-and-power-the-evolution-of-5g-nr-positioning-from-release-16-to-18/

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

ISACA. (2024, Volume 6). The impact of 5G: Unpacking security and privacy concerns. ISACA Journal. https://www.isaca.org/resources/isaca-journal/issues/2024/volume-6/the-impact-of-5g-unpacking-security-and-privacy-concerns

Nokia. (tarihsiz). The evolution of 5G New Radio positioning technologies [White paper]. https://d1p0gxnqcu0lvz.cloudfront.net/documents/Nokia_The_Evolution_of_5G_New_Radio_Positioning_Technologies_White_Paper_EN.pdf

RCR Wireless. (2022, April 27). What 5G NR positioning enhancements are in Release 17? https://www.rcrwireless.com/20220427/featured/5g-nr-positioning-enhancements-in-rel-17

Rangan, S., Rappaport, T. S., & Erkip, E. (2014). Millimeter-wave cellular wireless networks: Potentials and challenges. Proceedings of the IEEE, 102(3), 366–385. https://doi.org/10.1109/JPROC.2014.2299397

Sensors (MDPI). (2024). Survey on 5G physical layer security threats and countermeasures. Sensors, 24(17), 5523. https://doi.org/10.3390/s24175523

TLPC (Technology Law & Policy Clinic). (2025, June). Geofence warrants: A model state policy. University of Colorado. https://tlpc.colorado.edu/wp-content/uploads/2025/06/TLPC-Geofence-Report-June-2025.pdf