IMSI CATCHER (STINGRAY): YASAL DİNLEME Mİ, GİZLİ GÖZETİM Mİ?

Derleme Makale / Review Article

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

Anahtar Kelimeler: *IMSI Catcher • Stingray • IMSI • 5G SUPI/SUCI • Downgrade Saldırısı • CMK • Mahremiyet*

burakolgun.com

ÖZET

IMSI Catcher (IMSI yakalayıcı), gerçek bir mobil şebeke baz istasyonunu taklit ederek kapsama alanındaki tüm mobil cihazları kendi üzerinden bağlanmaya zorladıktan sonra cihazlara ait IMSI/SUCI numaraları, konum bilgileri ve belirli konfigürasyonlarda iletişim içeriklerini elde eden elektronik bir gözetim cihazıdır. Bu teknoloji; kolluk birimleri tarafından meşru suç soruşturmalarında kullanılmakla birlikte devlet dışı aktörler, ticari gözetim şirketleri ve organize suç örgütleri tarafından da konuşlandırılabilmektedir. Bu derleme makale; IMSI Catcher teknolojisinin teknik çalışma prensiplerini, 2G'den 5G'ye hücresel ağ güvenliğinin evrimini, 5G NSA ve SA mimarilerindeki kalıcı açıkları, downgrade saldırısı mekanizmasını, 5G SUPI/SUCI mekanizmasının sınırlılıklarını, hedef dışı kişilerin mahremiyet haklarına etkiyi, ticari gözetim pazarının boyutunu, tespit araçlarını ve metodolojilerini, uluslararası yargısal gelişmeleri, AİHM içtihadını, Carpenter v. United States kararının etkisini, Almanya ve Fransa gibi ülkelerin yasal çerçevelerini ve Türk hukukundaki değerlendirmeleri kapsamlı biçimde ele almaktadır.

Anahtar Kelimeler: *IMSI catcher, stingray, IMSI yakalayıcı, baz istasyonu taklitçisi, 5G SUPI, SUCI, downgrade saldırısı, 5G NSA, hücresel ağ güvenliği, gözetim teknolojisi, CMK 135, AİHM, Carpenter v. United States*

ABSTRACT

An IMSI Catcher is an electronic surveillance device that mimics a genuine mobile network base station, forcing all mobile devices in its coverage area to connect through it, thereby obtaining IMSI/SUCI numbers, location

information, and in some configurations, communication content. This technology is used by law enforcement agencies in legitimate criminal investigations, but can also be deployed by non-state actors, commercial surveillance companies, and organized crime. This review article comprehensively addresses the technical operating principles of IMSI Catchers, the evolution of cellular network security from 2G to 5G, persistent vulnerabilities in 5G NSA and SA architectures, the downgrade attack mechanism, limitations of the 5G SUPI/SUCI mechanism, the impact on privacy rights of non-targeted individuals, the scale of the commercial surveillance market, detection tools and methodologies, international judicial developments, ECtHR case law, the impact of Carpenter v. United States, legal frameworks in Germany and France, and evaluations in Turkish law.

Keywords: *IMSI catcher, stingray, false base station, cell site simulator, 5G SUPI, SUCI, downgrade attack, 5G NSA, cellular security, surveillance technology, CMK 135, ECHR, Carpenter v. United States, privacy, GDPR*

1. Giriş

Mobil iletişim, günümüzde kişisel ve kurumsal iletişimin baskın biçimini oluşturmaktadır. Dünya genelinde altı milyarı aşkın mobil aboneyle çalışan hücresel ağlar, yalnızca bireysel iletişimin değil; finans işlemlerinin, sağlık sistemlerinin ve kritik altyapıların da taşıyıcısıdır. Bu bağımlılık, mobil ağ altyapısının güvenliğini hem bireyler hem kurumlar hem de devletler açısından stratejik bir mesele haline getirmektedir.

IMSI Catcher — ticari adıyla Stingray, Hailstorm, DRTBox veya Yellowstone — bu stratejik güvenlik alanının en tartışmalı teknolojilerinden biridir. Başlangıçta yalnızca askeri ve istihbarat birimlerinin erişebildiği bu cihazlar, 2010'ların ortasından itibaren ticari piyasaya açılmış; SkyQuest'in (2024) piyasa analizine göre küresel IMSI Catcher pazarının 2023 yılında 179,3 milyon dolar değerine ulaştığı ve 2032 yılına kadar yüzde 9,4'lük bileşik yıllık büyüme oranıyla 402,5 milyon dolara çıkması öngörülmektedir.

Bu büyüme yalnızca meşru kolluk kullanımını yansıtmamaktadır. Gamma Group, Trovicor ve çeşitli İsrail merkezli şirketlerin ürettiği ticari IMSI Catcher sistemleri; otoriter yönetimler tarafından muhalif ve gazetecilere karşı kullanılmakta, şirket casusluğu operasyonlarında konuşlandırılmakta ve organize suç örgütleri tarafından hedeflerin takibinde kullanılmaktadır. İnfiShark (2026) bu tabloyu şöyle tanımlamaktadır: 'IMSI Catcher konuşlandırması çoğu yargı çevresinde çok az yasal denetimle yapılmaktadır.'

Bu makalenin amacı, IMSI Catcher teknolojisini hem teknik hem hukuki boyutlarıyla ve gerçek derinliğiyle ortaya koymaktır. 2G'den 5G'ye uzanan güvenlik mimarisinin evrimi, hâlâ devam eden güvenlik açıkları, ticari gözetim pazarı, tespit yöntemleri ve Türkiye'nin bu tablodaki konumu makaleyi yapılandıran temel eksenlerdir.

burakoguz.com

2. Teknik Mimari: Man-in-the-Middle Saldırısının Anatomisi

2.1 GSM Protokolünün Temel Güvenlik Açığı

IMSI Catcher teknolojisinin tüm yapısı, GSM (2G) protokolünün tasarım aşamasında yerleştirilen tek taraflı kimlik doğrulama mimarisinden beslenmektedir. Palindrome Tech (2025) bu temel zafiyeti şöyle tanımlamaktadır: 'Bu temel mimari kusur onlarca yıl boyunca düzeltilmeden kaldı: Mobil cihaz ağa kimliğini kanıtlamak zorundaydı, ancak ağın cihaza kimliğini kanıtlama yükümlülüğü yoktu.' Bu çift taraflı güvencenin yokluğu, sahte bir baz istasyonunun gerçek baz istasyonu olarak kabul görmesine kapı aralamaktadır.

GSM protokolünde IMSI (International Mobile Subscriber Identity), bir SIM kartı üzerindeki aboneliği benzersiz biçimde tanımlayan 15 haneli bir sayıdır. İlk ağ bağlantısında ve ağ bağlantısı kesilip yeniden kurulduğunda cihaz, kural olarak IMSI'sini açık metin (plaintext) olarak havaya vermektedir. Zetier (2025) bu durumu şöyle özetlemektedir: '2G ve 3G protokollerinde IMSI'ler üç koşulda açık metin olarak iletilmektedir; bu durum IMSI'nin atfetme ve coğrafi konumlama için kullanılmasına olanak tanıyan bir kişisel tanımlayıcı gizliliği açığına yol açmaktadır.'

Entropy Survival (2026), bu açığın pratik boyutunu somutlaştırmaktadır: '2024 itibarıyla dünya genelinde 850 milyonu aşkın insan ağırlıklı olarak 2G ağlara bağlı kalmaya devam etmektedir. ABD'de 4G kapsamasının geniş olduğu bölgelerde bile 2G ağlar kırsal alanlarda aktif olup acil durum yedek sistemi işlevi görmektedir. Bu durum pratikte her modern telefonun 2G kapasitesini koruduğu ve downgrade saldırılarına karşı savunmasız kaldığı anlamına gelmektedir.'

2.2 IMSI Catcher'ın Çalışma Döngüsü

IMSI Catcher'ın operasyonel döngüsü beş aşamada gerçekleşmektedir. Birinci aşamada cihaz, çevresindeki gerçek baz istasyonlarından daha güçlü bir sinyal yayar; mobil cihazlar en güçlü sinyale bağlanma eğiliminde olduğundan sahte istasyona kayar. İkinci aşamada sahte istasyon bağlanan cihaza IMSI ve IMEI bilgisini gönderme talebi iletir.

Üçüncü aşamada bu bilgiler alındıktan sonra cihaz gerçek şebekeye yeniden bağlanabilir ya da bağlı tutularak trafik proxy yöntemiyle gerçek şebeke üzerinden iletilir. Dördüncü aşamada gelişmiş konfigürasyonlarda IMSI Catcher, 2G şifreli veya şifresiz iletişimi deşifre etmeye, SMS içeriklerini ele geçirmeye ya da sesli iletişimi dinlemeye geçer. Beşinci aşamada elde edilen IMSI/IMEI verileri operatör kayıtlarıyla eşleştirilerek kişi kimliği belirlenir ve konum izleme süreci başlar (InfiShark, 2026).

2.3 Pasif ve Aktif IMSI Catcher Tipleri

IMSI Catcher'lar çalışma moduna göre iki temel kategoride incelenir. Pasif IMSI Catcher'lar, baz istasyonu taklidi yapmaksızın yalnızca havada dolaşan sinyal trafiğini dinleyerek IMSI/IMEI bilgilerini toplar. Bu mod yalnızca şifrelenmemiş ya da zayıf şifreleme kullanan ağlarda (2G, bazı 3G konfigürasyonlarda) etkindir. Aktif IMSI Catcher'lar ise baz istasyonu taklidi yöntemini kullanarak cihazları kendi üzerine çekmektedir.

burakoglu.com

Aktif cihazların sunduğu gelişmiş konfigürasyon yetenekleri şunlardır: Şifrelenmemiş ses ve SMS içeriklerinin ele geçirilmesi (yalnızca 2G/A5-0 modunda), cihazı devre dışı bırakma (Denial of Service), hedef cihaza sahte SMS veya arama yönlendirme ve cihazı 2G'ye düşürme (downgrade attack). 2024 yılında Shoghi Communications'ın piyasaya sürdüğü araçsal IMSI Catcher sistemi, 2G'den 5G'ye tüm nesillerde çalışabilme kapasitesi, GPS tabanlı hedef konumlama ve radyo ortamının yüksek hızlı taranmasını tek bir platformda birleştirmektedir (SkyQuest, 2024).

2.4 Downgrade Saldırısı: 5G Cihazları 2G'ye Zorlamak

Downgrade (düşürme) saldırısı, modern 4G veya 5G telefonları savunmasız 2G ağlara bağlanmaya zorlamanın teknik mekanizmasıdır. Entropy Survival (2026) bu mekanizmayı açıklamaktadır: 'Saldırgan, 4G'nin mevcut veya güvenilmez olduğunu iddia eden sinyaller yayar. Telefonun otomatik ağ seçimi bunu geçerli ağ koşulu olarak yorumlar ve gönüllü biçimde 2G'ye düşer. Kullanıcı bu değişiklikten habersizdir; cihaz normalde çalışmaya devam eder.'

Palindrome Tech (2025), bu saldırının 5G NSA konfigürasyonlarındaki kalıcılığını vurgulamaktadır: '5G'nin ilk yaygın konuşlandırılması 5G Non-Standalone (NSA) modunda gerçekleşmektedir; bu mod mevcut 4G çekirdeğini kullanmaktadır. Bu nedenle 4G'nin açıklarının büyük bölümü miras alınmakta ve downgrade saldırılarının tehdidi varlığını sürdürmektedir.' Zetier (2025) ise bu dinamiği şöyle somutlaştırmaktadır: '5G çok aşamalı bir dağıtım sürecidir ve 5G NSA dağıtımlarının tamamı 4G ile aynı açıklara sahiptir.'

Teknik mekanizma şu şekilde işlemektedir: Sahte baz istasyonu, sistem bilgi bloklarında (SIB) 4G ağının mevcut olmadığını ya da sinyal kalitesinin yetersiz kaldığını bildiren yanlış parametreler yayınlar. Cihaz bu bilgiyi yasal ağ koşulları olarak kabul ederek 2G'ye geçer; ancak bu geçiş sırasında kimlik doğrulama sürecinde IMSI açık metin olarak iletilmektedir (Preeß Mattsson ve Nakarmi, 2021; Dabrowski et al., 2014).

Tablo 1. *IMSI Catcher Yeteneklerinin Nesle Göre Karşılaştırması*

Yetenek	2G (GSM)	3G (UMTS)	4G (LTE)	5G NR
IMSI/IMEI toplama	Evet (açık metin)	Evet (saldırıyla)	Sınırlı	SA: Çok Zor / NSA: Zor
Konum tespiti	Evet	Evet	Evet	SA: Sınırlı / NSA: Evet
SMS içerik dinleme	Evet (A5/0)	Zor	Hayır	Hayır
Ses içerik dinleme	Evet (A5/0)	Zor	Hayır	Hayır
Downgrade saldırısı	N/A	2G'ye mümkün	2G'ye mümkün	NSA: Mümkün / SA: Güç
DoS (servis engeli)	Evet	Evet	Kısmi	Azalmış ama mevcut

Not. Kaynak: 3GPP (2019); Palindrome Tech (2025); Zetier (2025); Entropy Survival (2026); InfiShark (2026) temel alınarak derlenmiştir.

3. Hücresel Ağ Güvenliğinin Evrimi: 2G'den 5G'ye

3.1 GSM (2G): Güvenlik Tasarım Tercihleri ve Kalıcı Açıkları

GSM standardı 1980'lerin sonunda tasarlanmış; güvenlik gereksinimleri dönemin hesaplama kapasitesi, regülatör endişeleri ve öncelikli amaç olan şebeke interoperabilitesi gözetilerek biçimlendirilmiştir. A5/1 şifreleme algoritması, güçlü kriptografik eleştiriler almış; A5/2 ise ihracat kısıtlamaları nedeniyle kasıtlı olarak zayıflatılmıştır. A5/0 modu ise hiç şifreleme yapmamaktadır.

Bu tasarım seçimlerinin birleşimi, GSM ağlarını pasif dinlemeye karşı yalnızca sınırlı bir koruma sunacak biçimde şekillendirmiştir. Aktif IMSI Catcher saldırıları açısından ise temel güvenlik açığı yapısal bir nitelik taşımaktadır: Ağ kendini doğrulamak zorunda olmadığından, sahte bir baz istasyonunu gerçeğinden ayırt eden kriptografik mekanizma mevcut değildir (Dabrowski et al., 2014).

3.2 UMTS (3G): Karşılıklı Kimlik Doğrulama ve Kalan Zafiyetler

Üçüncü nesil (3G) UMTS standardı, GSM'nin en kritik eksikliğini gidermek amacıyla karşılıklı kimlik doğrulama (mutual authentication) gerekliliğini getirmiştir: Hem cihaz ağa hem de ağ cihaza kimliğini kriptografik olarak kanıtlamak zorundadır. Bu ilerleme, salt baz istasyonu taklidi yöntemini teorik olarak olanaksız kılmaktadır.

Bununla birlikte 3G'de iki kritik açık varlığını korumaktadır. Birincisi, başlangıç bağlantı aşamasında cihazın gerçek kimliğini (IMSI) açık metin olarak iletmesi gerekmektedir; bu iletim henüz ağın kimliği doğrulanmadan gerçekleşmektedir. İkincisi, 3G'nin 2G'ye düşürme (fallback) özelliğini zorunlu olarak desteklemesi, saldırganların cihazları 3G'den 2G'ye aktarabilmesine imkân tanımaktadır. Bu açıklar, 3G'nin aktif IMSI Catcher'lara karşı yalnızca kısmi koruma sağlaması anlamına gelmektedir (Preeß Mattsson ve Nakarmi, 2021).

3.3 LTE (4G): Güçlü Şifreleme, Zayıflayan Kimlik Gizliliği

Dördüncü nesil LTE standardı, şifreleme ve bütünlük koruma algoritmalarını önemli ölçüde güçlendirmiş; 3G'deki zayıf şifreleme optionlarını büyük ölçüde geride bırakmıştır. LTE aynı zamanda bağlantı başlangıcında karşılıklı kimlik doğrulamayı standart hale getirmektedir. Bu gelişmeler, içerik dinleme ve aktarım güvenliğini belirgin biçimde iyileştirmiştir.

Bununla birlikte LTE, IMSI Catcher tehdidini tam anlamıyla ortadan kaldıramamaktadır. Belirli koşullarda — özellikle cihaz ağa ilk kez bağlandığında ya da geçici kimlik (TMSI) bilgisi yokken — IMSI açık metin olarak iletilebilmektedir. Bunun yanı sıra downgrade saldırısı vektörü 4G üzerinden de işleyebilmektedir: Sahte bir LTE baz istasyonu, cihazı tanımlayan zayıf algoritmaları seçecek biçimde güvenlik görüşmesini (security negotiation) manipüle edebilmektedir (MDPI, 2024).

Pratik bir perspektiften Zetier (2025) şu değerlendirmeyi yapmaktadır: 'Yıllar boyunca pek çok yanlış yapılandırılmış kuleyle karşılaştım; bu nedenle bir downgrade bağlantısının savunmasız olduğunu varsayardım. Mobil operatörler de SUCI'yi hiç kullanmayabilir. Bu açığın pratikte ne ölçüde yaygın olduğundan emin değilim, ancak sıfır olmadığına inanıyorum.'

burakbilgin.com

3.4 5G NR: SUPI/SUCI Mekanizması ve Kalan Açıklar

3.4.1 SUPI ve SUCI: Kavramsal Çerçeve

5G New Radio (NR) standardı, IMSI Catcher tehdidine karşı tasarım düzeyinde köklü bir yeniliği beraberinde getirmiştir. Thales Group (2021), bu mekanizmayı şöyle açıklamaktadır: '5G yeni bir tanımlayıcı yarattı: SUPI (Subscription Permanent Identifier). Cihazlar SUPI'yi havaya vermemektedir. Bunun yerine SUCI (Subscription Concealed Identifier) adı verilen şifreli bir anahtar iletilir. Bir saldırgan SUCI'yi ele geçirse bile bu bilgi işe yaramaz ve veri toplamak için kullanılamaz. Bu bir çeşit maskedirya; her seferinde değişir.'

Teknik olarak SUCI, SUPI'nin ağın açık anahtarıyla Eliptik Eğri Entegre Şifreleme Şeması (ECIES) kullanılarak şifrelenmesiyle oluşturulmakta ve her kullanımda yeniden üretilmektedir. Bu tek seferlik ephemeral key yapısı, SUCI'yi tekrar oynatma saldırılarına karşı da korumaktadır. InfiShark (2026) değerlendirmesine göre, '5G Standalone (SA) formunda IMSI toplamayı ve engelleme saldırılarını önemli ölçüde güçleştirmektedir.'

3.4.2 SUCI Uzunluk Açığı: Ericsson/Nori Çalışması

5G SUCI mekanizmasının önemli bir zafiyeti, Ericsson araştırmacıları Preeß Mattsson ve Nakarmi'nin 2021 tarihli 'Nori' çalışmasında belgelenmiştir. Bu araştırmada 3GPP TS 33.501 standardında belirlenen ECIES profillerinin kritik bir güvenlik açığı içerdiği saptanmıştır: SUCI şifreleme AES-CTR modunu kullandığından, şifreli metin düz metinle aynı uzunluktadır. Ağ Spesifik Tanımlayıcıların (NSI) değişken uzunluk kullandığı durumlarda, bu özellik 1-anonimlik sorununa yol açmaktadır: Bireysel aboneler kolaylıkla tanımlanabilmekte ve izlenebilmektedir.

Nori çalışmasının önerisi şudur: 3GPP ve GSMA'nın, değişken uzunluklu tanımlayıcılar daha yaygın kullanım kazanmadan önce SUCI için dolgu (padding) mekanizmasını standartlaştırması ve önermesi güçlü biçimde tavsiye edilmektedir. Ericsson'ın (2024) bu bulgulara verdiği yanıtta şu çözüm önerisi öne çıkmaktadır: '3GPP'nin CSP'lerin sabit uzunluklu abonelik kimliği kullanmasını ya da değişken uzunluklu kodları aynı uzunluğa getirmesini önermesi.'

3.4.3 5G SUCI-Catcher Saldırısı: ACM WiSec 2021 Kanıtı

5G mimarisinin bile SUCI'ya dayalı izleme saldırılarına karşı tam koruma sağlamadığı, ACM WiSec 2021 konferansında sunulan proof-of-concept çalışmayla gösterilmiştir. Bu çalışmada araştırmacılar, 5G Standalone ağında SUCI tabanlı saldırının mümkün olduğunu ortaya koymuştur. Araştırmacılar şifreli SUCI'ları yakalamakta ve Kimlik Doğrulama ve Anahtar Anlaşması (AKA) prosedürü aracılığıyla bağlantı kurmaktadır. Hedef kişinin kimliği zaten biliniyorsa, saldırgan bu kişiyi hedefleyen bir yoklama gerçekleştirerek alanın içinde olup olmadığını tespit edebilmektedir (ACM WiSec, 2021).

Bu bulgu kritik bir sınırlılığı ortaya koymaktadır: 5G SUCI mekanizması, kimliği bilinmeyen bireylerin toplu IMSI toplamasını önlemekte oldukça başarılıdır. Ancak kimliği zaten bilinen bir kişinin takibinde, AKA prosedürü üzerinden linkability (bağlanabilirlik) hâlâ mümkündür. Bu durum, hedefli gözetim bağlamında 5G'nin tam bir güvenlik garantisi sunmadığını göstermektedir.

burokrasi.com

3.4.4 5G SA ile NSA'nın Güvenlik Farkı

5G dağıtımında iki temel mimari mevcuttur. Non-Standalone (NSA) modunda 5G radyo erişim ağı mevcut 4G (LTE) çekirdeğiyle birlikte çalışmaktadır. Bu yapı, 4G'nin tüm güvenlik açıklarını miras aldığı anlamına gelmektedir. MDPI'nin (2024) 5G NSA üzerine yürüttüğü deneysel çalışma, geliştirilen test ortamında IMSI sızıntısı, Numb ve Downgrade saldırılarının 5G NSA ağında pratikte çalıştığını doğrulamıştır.

Standalone (SA) modunda ise 5G hem radyo hem çekirdek ağı içermekte; SUPI gizleme ve diğer gelişmiş güvenlik özellikleri tam anlamıyla devreye girmektedir. Lightreading (2023), Standalone 5G'nin güvenlik özelliklerini şöyle değerlendirmektedir: 'Zorunlu geçici ve rastgele telefon kimliklerinin sağladığı mahremiyet bunların başında gelmektedir. Ancak mevcut Release 16 spesifikasyonunda belirlenen bazı özellikler hâlâ isteğe bağlı kalmakta, bu da operatörlere hangi korumaları uygulayacaklarını seçme imkânı tanımaktadır.'

Tablo 2. *5G SA ve NSA Mimarilerinin Güvenlik Karşılaştırması*

Güvenlik Özelliği	5G NSA	5G SA
SUPI gizleme (SUCI)	Kısmi (4G çekirdeği nedeniyle sınırlı)	Tam (ECIES ile zorunlu)
Karşılıklı kimlik doğrulama	4G'den miras (zayıf)	5G AKA ile güçlü
Downgrade saldırısı riski	Yüksek	Düşük (ama sıfır değil)
IMSI sızıntısı riski	Orta-Yüksek	Düşük (Nori açığı hariç)
SUCI Catcher saldırısı	Mümkün	Hedefli saldırıda mümkün
2G/3G legacy açıkları	Tamamı geçerli	Etkisizleştirilmiş

Not. Kaynak: Palindrome Tech (2025); MDPI (2024); Zetier (2025); Preeß Mattsson & Nakarmi (2021); Lightreading (2023) temel alınarak derlenmiştir.

4. Toplu Veri Toplama: Orantısız Etki ve Hassas Bağlamlar

4.1 Hedef Dışı Bireylerin Verilerinin Toplanması

IMSI Catcher'ın en tartışmalı boyutu, kapsama alanındaki tüm mobil cihazlardan veri topluyor olmasıdır. Bir kolluk birimi belirli bir şüpheliyi hedef alarak IMSI Catcher konuşlandırdığında, aynı alanda bulunan yüzlerce ya da binlerce masum kişinin de IMSI/IMEI bilgileri ve konum verileri toplanmaktadır. EFF'nin (SLS, tarihsiz) belgelediği Baltimore vakasında polis, 2007 ile 2015 yılları arasında çoğunlukla yargısal yetki almaksızın IMSI Catcher'ı 4.300'den fazla kez kullanmıştır.

Bu durumun hukuki yansıması, 'genel arama' yasağıyla doğrudan çelişmektedir. EFF (SLS, tarihsiz), sorunu şöyle ifade etmektedir: 'Hücre sitesi simülatörleri kapsama alanındaki herkesi, suç işledikleri iddialanmayan büyük çoğunluk dahil, mahremiyetini ihlal etmektedir. Bunlar, arama emirlerinin 'özellikle' aranacak kişi veya şeyi tanımlaması şartıyla çelişen genel aramalar niteliğindedir.'

4.2 Hassas Bağlamlardaki Özel Riskler

Belirli mekânlarda IMSI Catcher kullanımı, özellikle ağır mahremiyet ihlali riskleri taşımaktadır. Bu riskler beş kritik bağlamda somutlaşmaktadır.

Sağlık tesisleri: Hastaların konum bilgileri ziyaret edilen bölüme ilişkin sağlık bilgisi ifşa etme riski barındırmaktadır. Hastane onkoloji, psikiyatri veya HIV kliniği koridorunda toplanan bir IMSI, o kişinin sağlık durumuna ilişkin bir bilgi ifşası anlamına gelebilir.

Hukuk büroları ve mahkeme binaları: Avukat-müvekkil iletişiminin gizliliği tehlikeye girebilmektedir. Bu bağlamda IMSI Catcher kullanımı, hukuki temsil hakkını da zedelemektedir.

Dini ibadet alanları ve siyasi toplantı mekânları: İnanç ve siyasi görüş gibi özel kategori verilerin dolaylı olarak elde edilmesi söz konusu olmaktadır. EFF, ABD'de devlet görevlilerinin Stingray cihazlarını kitlesel protesto gösterileri sırasında konuşlandırdığını ve binlerce kişinin kimlik bilgisini derlediğini belgelemiştir (ESPLawyers, tarihsiz).

Basın toplantıları ve muhabir toplantı noktaları: Kaynak gizliliğinin bozulma riski gündemdedir. Gazetecilerin kaynaklarıyla fiziksel buluşma sırasında uygulanan IMSI Catcher, kaynak kimliğini deşifre edebilir.

Parallel construction (paralel inşa) riski: ABD'de Harris Corporation ile imzalanan gizlilik sözleşmeleri, polis birimlerini IMSI Catcher kullanımını mahkemeden gizleme yoluna itmiştir. Bu uygulama 'paralel inşa' olarak adlandırılmakta; delil gerçek kaynağından farklı bir yolla elde edilmiş gibi gösterilmektedir. InfiShark (2026), bu pratiği şöyle tanımlamaktadır: 'Harris Corporation'ın gizlilik sözleşmeleri, savcıları davaları düşürmeye, delillerin nasıl elde edildiğini yanlış beyan etmeye ya da sanıklara kullanılan gözetim yöntemleri hakkında bilgi vermemeye yöneltmiştir.'

5. Ticari Gözetim Sektörü ve Piyasa Boyutu

5.1 Küresel IMSI Catcher Pazarı

IMSI Catcher teknolojisi, yalnızca devlet kurumlarına özgü bir alan olmaktan çıkmış; giderek büyüyen bir ticari endüstriye dönüşmüştür. SkyQuest (2024) piyasa araştırmasına göre, küresel IMSI Catcher pazarının 2023 yılında 179,3 milyon dolar değerinde olduğu ve 2032 yılına kadar yüzde 9,4 yıllık büyüme oranıyla 402,5 milyon dolara ulaşması beklenmektedir. Business Research Insights (2024) ise bu rakamı 2024 için 196,1 milyon dolar olarak tahmin etmekte ve 2033 yılına kadar yüzde 7 büyüme öngörmektedir.

Bu büyümenin başlıca itici güçleri arasında ulusal güvenlik talebindeki artış, istihbarat toplama gereksinimlerinin derinleşmesi ve kriminal faaliyetlerin önlenmesi için kolluk kapasitesinin artırılması isteği sayılmaktadır. Yapay zeka entegrasyonu bu sektörü de dönüştürmektedir: SkyQuest'in (2024) raporunda belirtildiği üzere, AI entegre IMSI sistemleri yüksek değerli hedefleri daha hızlı tanımlayabilmekte, gerçek zamanlı tehdit tespitini iyileştirmekte ve gözetim hassasiyetini artırmaktadır.

Shoghi Communications'ın 2024'te piyasaya sürdüğü araçsal IMSI Catcher sistemi bu dönüşümün simgesi niteliğindedir: 2G'den 5G'ye tüm nesillerde çalışabilen, GPS tabanlı hedef

kurakolgun.com

konumlama ve yüksek hızlı radyo ortamı taraması sunan sistem, resmi olarak 'hükümet kurumları ve kolluk birimleri için' sunulduğunu beyan etmektedir (SkyQuest, 2024).

5.2 Ticari Gözetim Şirketleri ve İhracat Kaygıları

Gamma Group (İngiltere/Almanya), BAE Systems Applied Intelligence, Trovicor (Almanya) ve çeşitli İsrail merkezli şirketler; ticari IMSI Catcher sistemleri üretip pazarlamaktadır. İnsan hakları kuruluşları, bu sistemlerin otoriter yönetimler tarafından muhalefet, gazeteci ve aktivistlere yönelik kullanıldığını kapsamlı biçimde belgelemiştir. AB'nin Temmuz 2023'te yürürlüğe giren ihracat kontrol düzenlemeleri, ticari gözetim teknolojilerinin üçüncü ülkelere ihracatına sınırlamalar getirmiştir.

IMSI Catcher'ların ticari kullanımındaki bir diğer kritik endişe, kurumsal casusluktur. Rekabetçi istihbarat amaçlı ya da iş müzakerelerinde konuşlandırılan IMSI Catcher'lar, şirket sırlarına ve personelin kişisel verilerine erişim sağlayabilmektedir. Bu kullanım, neredeyse tüm yargı çevrelerinde açıkça yasal olmakla birlikte tespit edilmesi son derece güçtür.

6. Hukuki Çerçeve: Uluslararası Durum

6.1 AİHM İçtihadı ve Temel Standartlar

Avrupa İnsan Hakları Mahkemesi, telekomünikasyon gözetimi alanında oluşturduğu içtihat aracılığıyla devlet uygulamalarının sınırlarını belirlemektedir. Zakharov/Rusya (Büyük Daire, 2015) kararı bu alandaki en kapsamlı AİHM kararlarından birini oluşturmaktadır. Bu kararda mahkeme, gizli gözetim uygulamalarının AİHS'nin 8. maddesiyle bağdaşabilmesi için erişilebilir, öngörülebilir ve keyfi uygulamaya karşı korumalı yasal bir dayanağa ihtiyaç duyulduğunu hükme bağlamıştır. Özellikle toplu gözetim sistemleri, bireysel şüphe olmaksızın milyonlarca kişiyi izleme kapasitesi taşıdığından bu ölçütleri karşılayamamaktadır.

Szabó ve Vissy/Macaristan (2016) kararı ise toplu ve hedefsiz telekomünikasyon gözetiminin AİHS'nin 8. maddesi kapsamında hak ihlaline yol açtığını açıkça ortaya koymuştur. Bu içtihat, IMSI Catcher kullanımı için zorunlu olan kriterleri şöyle belirlemektedir: Bireysel müdahaleye özel hukuki dayanak, yargısal ya da bağımsız idari denetim, gereklilik ve orantılılık değerlendirmesi ile hedef dışı verinin imhası için açık prosedür. Bu kriterler, toplu IMSI Catcher kullanımının doğası gereği AİHM içtihadıyla çeliştiğine işaret etmektedir.

6.2 ABD Hukukundaki Gelişmeler ve Carpenter Kararı

ABD'de IMSI Catcher hukuku, tarihsel olarak derin bir tutarsızlık göstermiştir. InfiShark (2026), bu tablonun temel çelişkisini şöyle özetlemektedir: 'ABD Adalet Bakanlığı 2015 yılında federal ajansların acil durumlar veya ulusal güvenlik davalarının dışında hücre sitesi simülatörlerini kullanmadan önce arama emri almasını zorunlu kılan bir politika yayımlamıştır. Daha önce pek çok ajans IMSI Catcher'ları arama emirleri için gereken daha yüksek ispat standardı yerine daha düşük kalem kaydı emirleri (pen register orders) aracılığıyla kullanıyordu.'

burakoguz.com

Bu tabloda dönüm noktası sayılan karar, Carpenter v. United States (2018) davası olmuştur. Yüksek Mahkeme, uzun süreli hücresel konum verisi (CSLI) toplamanın arama sayılacağına ve mahkeme kararı gerektirdiğine hükmetmiştir. National Security Law Brief'in (tarihsiz) değerlendirmesine göre: 'Bu dava artık esas itibarıyla polis yetkililerinin IMSI catcher'ı her kullandıklarında arama emri almalarını gerektirmektedir; çünkü bir IMSI, CSLI ve daha fazlasını toplamaktadır.' Bu yorumun yaygın kabulü, ABD'deki federal ve eyalet uygulamalarını yeniden biçimlendirmeye başlamıştır.

ESPLawyers'ın (tarihsiz) davalar analizine göre, 2015 yılında United States v. Andrews davasında polis arama emri olmaksızın Stingray kullandığı için mahkeme bu delili Dördüncü Değişiklik kapsamında mahremiyet korumasına dayanarak dışlamıştır. Baltimore'da ise polisin 2007 ile 2015 arasında 4.300'den fazla IMSI Catcher operasyonu yürüttüğü, bu operasyonların büyük çoğunluğunun yargısal denetimden yoksun olduğu, sonradan pek çok mahkûmiyetin yeniden incelemeye alındığı belgelenmiştir.

2021 tarihli Cell-Site Simulator Warrant Act, federal düzeyde arama emrini zorunlu kılan ve topladığı kişinin hedef olmadığı verilerin silinmesini öngören yasal çerçeveyi oluşturmayı hedeflemektedir. Bununla birlikte yasanın uygulanması tutarsız kalmaya devam etmekte; California gibi bazı eyaletler daha kapsamlı düzenlemeler benimsemiştir (EFF-SLS, tarihsiz).

6.3 Almanya: StPO 100i ve Avrupa'nın Referans Modeli

Almanya, IMSI Catcher kullanımını Ceza Usul Kanunu'nun (Strafprozessordnung — StPO) 100i. paragrafında açıkça düzenleyen ülkeler arasındadır. Bu düzenleme kapsamında IMSI Catcher; yalnızca ciddi suçların soruşturulmasında, mahkeme kararıyla ve son çare ilkesine bağlı olarak kullanılabilmektedir. Kapsama alanındaki hedef dışı bireylerin verilerinin derhal imha edilmesi yasal zorunluluktur.

Alman uygulaması, iki temel ilkenin yasal metne yansıtılması bakımından uluslararası referans model olarak değerlendirilmektedir: Bireyselleştirilmiş yargısal yetki zorunluluğu ve hedef dışı veri için anında imha yükümlülüğü. Bu model, toplu IMSI Catcher kullanımını hukuki olarak imkânsız kılmaktadır; çünkü her kullanım ayrı bir mahkeme emrini gerektirmektedir.

6.4 Türk Hukuku Bağlamı

6.4.1 CMK 135 ve Bireysellik Çelişkisi

Türkiye'de IMSI Catcher teknolojisini doğrudan düzenleyen özel bir yasal çerçeve mevcut değildir. Bu boşlukta uygulanabilecek temel yasal dayanak, telekomünikasyon iletişiminin denetlenmesini düzenleyen CMK'nın 135. maddesidir. Bu madde; iletişim denetimini hâkim kararına bağlamakta, gecikmesinde sakınca bulunan hallerde savcılık kararına imkân tanımakta, ancak bu kararın yirmi dört saat içinde hâkim onayına sunulmasını zorunlu kılmaktadır.

CMK 135'in IMSI Catcher kullanımına uygulanmasındaki kritik gerilim şöyle tanımlanabilir: Bu madde belirli bir kişinin iletişiminin denetlenmesini öngörürken, IMSI Catcher tanımı gereği kapsama alanındaki tüm cihazları etkilemektedir. Toplu veri toplama

niteliği, CMK 135'in bireyselleştirilmiş denetim şartıyla bağdaşmaz görünmektedir. Bu çelişki, IMSI Catcher'ın mevcut yasal çerçevede meşru bir kullanım alanının tanımlanmasını zorlaştırmaktadır.

6.4.2 KVKK Boyutu

6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) açısından değerlendirildiğinde, IMSI ve IMEI numaraları bir kişiyi tanımlamaya yarayan veriler olarak kişisel veri statüsündedir. KVKK Kurulunun 2024 Yılı Faaliyet Raporu (2025), KVKK'nın kişisel verilerin açık rıza ya da yasal yükümlülük olmaksızın işlenemeyeceği ilkesini uygulamaya devam ettiğini göstermektedir.

Hâkim kararı olmaksızın IMSI Catcher aracılığıyla yürütülen toplu IMSI toplamanın KVKK kapsamında kişisel veri ihlali oluşturabileceği değerlendirilmektedir. Özellikle telekomünikasyon ve lokasyon verilerinin işlenmesi, KVKK'nın 6. maddesinde özel kategori veri olarak tanımlanan biyometrik ve sağlık verileriyle dolaylı ilişki içinde olabilmekte; bu durum koruma yükümlülüklerini daha da ağırlaştırmaktadır.

6.4.3 5651 Sayılı Kanun ve Dijital Gözetim Evrimi

Türkiye'de 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, ağırlıklı olarak çevrimiçi içerik denetimini düzenlemekle birlikte dijital gözetim altyapısına ilişkin geniş yorumlara da zemin oluşturmaktadır. Nisan 2026'da TBMM'de kabul edilen son değişiklikler kapsamında sosyal medya platformlarına yönelik kimlik doğrulama ve içerik yükümlülükleri genişletilmiştir.

Bu değişikliklerin, dijital gözetim altyapısının IMSI Catcher gibi araçlarla entegrasyon boyutuyla henüz tartışılmadığı görülmektedir. Bununla birlikte dijital gözetim teknolojilerinin ve toplanan kişisel veri türlerinin yasal çerçevesinin bütüncül biçimde ele alınması, Türk mevzuatının önündeki önemli bir boşluk olarak durmaktadır.

6.4.4 Türkiye'de Düzenleyici Çerçeve Önerileri

Türkiye'nin IMSI Catcher kullanımını açıkça düzenleyen bir yasal çerçeveden yoksun olması; hem meşru güvenlik operasyonlarını belirsizlik içinde bırakmakta hem de bireylerin mahremiyet güvencelerini zayıflatmaktadır. Bu eksikliğin giderilmesi için aşağıdaki düzenleyici bileşenler önerilmektedir.

- **Bireyselleştirilmiş yargısal yetki:** Her kullanım için somut suç şüphesine dayanan hâkim kararı zorunlu tutulmalıdır.
- **Hedef dışı veri yükümlülüğü:** Kapsama alanında toplanan hedef dışı bireylere ait veriler en geç kırk sekiz saat içinde imha edilmeli ve bu yükümlülük yasal olarak teminat altına alınmalıdır.
- **Hassas bağlam kısıtlaması:** Hukuk büroları, hastaneler, ibadet yerleri ve basın etkinlikleri çevresinde kullanım özel yargısal onay gerektirmelidir.
- **Şeffaf denetim mekanizması:** Bağımsız bir denetim kurumuna yıllık kullanım istatistiklerinin raporlanması sağlanmalıdır.
- **5G geçiş teşviki:** Operatörlerin 2G/3G altyapısını kademeli kapatmasının teşvik edilmesi, IMSI Catcher saldırı yüzeyini daraltacaktır.

buraburun.com

7. IMSI Catcher Tespiti: Teknik Savunma Mekanizmaları

7.1 Yazılım Tabanlı Tespit Araçları

IMSI Catcher varlığını tespit etmeye yönelik yazılım araçları, üç temel kategoride sınıflandırılabilir. Birinci kategoride açık kaynaklı mobil uygulamalar yer almaktadır. SnoopSnitch, Qualcomm yongaseti içeren kök erişimli Android telefonlarda çalışmakta; beklenmedik sinyal düşüşlerini, sessiz SMS bağlantılarını ve hileli baz istasyonlarına olan bağlantıları tespit ederek kullanıcıyı uyarmaktadır (Cloudwards, 2025).

AIMSICD (Android IMSI-Catcher Detector), hücre ağı parametrelerini izleyerek bilinen baz istasyonu veritabanlarıyla karşılaştırmaktadır. Şüpheli göstergeler arasında eksik komşu listeleri, olağandışı konum alan kodları ve öte kule davranışının göstergesi olabilecek zamanlama avansları yer almaktadır. Zimperium'a (tarihsiz) göre, SnoopSnitch 100.000 ila 500.000 indirme basamağında bulunurken, AIMSICD yalnızca iki indirme sayısıyla neredeyse aktif bakımından yoksundur.

EFF'nin Crocodile Hunter projesi, Yazılım Tanımlı Radyo (SDR) ve Raspberry Pi ya da Linux sistemine dayanan bir donanım aracıdır. Yakındaki baz istasyonlarının yayın sinyallerini sürekli izlemekte ve analiz için bir veritabanına yükleme yapabilmektedir (InfiShark, 2026).

7.2 Tespit Araçlarının Sınırlılıkları

Tespit uygulamalarının ciddi sınırlılıkları göz önünde bulundurulmalıdır. Entropy Survival (2026), bu sınırlılıkları üç başlık altında özetlemektedir: Birincisi, sınırlı donanım erişimi: Modern akıllı telefonlar, güvenlik ve pil yönetimi gerekçesiyle uygulamaların düşük seviyeli radyo donanımına erişimini bilerek kısıtlamaktadır. Bu durum uygulamaların temel IMSI Catcher göstergelerini tespit etme kapasitesini önemli ölçüde azaltmaktadır.

İkincisi, yanlış pozitif ve negatif oranları: Gerçek ağ koşulları — değişen sinyal gücü, handoff (baz istasyonu geçişi) ve servis bölgesi sınırları — IMSI Catcher göstergeleriyle üst üste gelebilmektedir. Uygulamanın AIMSICD hakkındaki değerlendirmesine göre, uygulama meşru ağları IMSI Catcher aktivitesine sahip olarak tanımlamada yanlış pozitif üretebilmektedir (Cloudwards, 2025). Üçüncüsü, gelişmiş IMSI Catcher'lar bu tespiti zorlaştıracak biçimde tasarlanmış olabilmekte; sinyal parametrelerini gerçek bir baz istasyonuna yakın tutarak tespiti engelleyebilmektedir.

7.3 Donanım Tabanlı ve Kurumsal Tespit Sistemleri

Kurumsal ölçekte IMSI Catcher koruması için donanım tabanlı çözümler gündeme gelmektedir. Zimperium (tarihsiz), bu alandaki yaklaşımı şöyle tanımlamaktadır: 'Daha güvenilir donanım seçenekleri birkaç akıllı telefon kullanıcısını tek bir konumda (iş merkezi veya askeri üs gibi) korumak için mantıklıdır. Tipik konfigürasyon, yakındaki baz istasyonlarının yayın sinyallerini sürekli izleyen ve veriyi analiz için bir veritabanına yükleyebilen sabit bir gömülü sistemi içerir.'

Büyük şirketler ve yüksek güvenlik ortamları için FirstPoint, ComSec ve SecurCube gibi kurumsal çözümler, hem ağ parametrelerini izlemek hem de şüpheli aktiviteyi gerçek

burakbgn.com

zamanlı olarak raporlamak üzere tasarlanmıştır. Bu sistemlerin kurumsal güvenlik politikalarına entegrasyonu, özellikle kritik altyapı, bankacılık ve savunma sektörleri için stratejik bir öneme sahiptir.

Tablo 3. *Başlıca IMSI Catcher Tespit Araçlarının Karşılaştırması*

Araç	Tür	Platform	Doğruluk	Temel Kısıt
SnoopSnitch	Mobil uygulama	Android (Qualcomm)	Orta	Kök erişimi + Qualcomm şart
AIMSICD	Mobil uygulama	Android (kök)	Orta-Düşük	Güncellenmemiş; yanlış pozitif
EFF Crocodile Hunter	Donanım + yazılım	Raspberry Pi/Linux	**Yüksek**	Teknik uzmanlık gerektirir
FirstPoint / ComSec	Kurumsal donanım	Sabit sistem	**Yüksek**	Kurumsal maliyet; seçici kapsam
Spectrum analizör	Donanım	Özel cihaz	**Yüksek**	Uzmanlık + pahalı ekipman

Not. Kaynak: InfiShark (2026); Entropy Survival (2026); Zimperium (tarihsiz); Cloudwards (2025) temel alınarak derlenmiştir.

8. 2G/3G Sunset Takvimi ve Geçiş Döneminin Güvenlik Boyutu

IMSI Catcher tehditinin en önemli uzun vadeli belirleyicisi, 2G ve 3G ağlarının kapatılma takvimini. Bu süreç bölgeden bölgeye son derece farklı bir seyir izlemektedir. Entropy Survival (2026), bu tabloyu şöyle ortaya koymaktadır: 'ABD'de operatörler 3G'yi 2025'e kadar tamamen kapatmayı planlarken, 2G çoğu alanda 2026-2027 yılına kadar aktif kalacaktır. Avrupa ülkeleri 2G/3G kapatılmasını 2025-2030 yılları arasında hedeflemektedir. Pek çok gelişmekte olan ülke bir on yıl daha 2G altyapısını koruyacaktır. Küresel dolaşım gereklilikleri, kendi ülkelerinde kapatmış olan ülkelerin bile bu ağları uluslararası ziyaretçiler için desteklemesini zorunlu kılmaktadır.'

Türkiye'nin 5G geçiş takvimi, IMSI Catcher tehdidinin ülkedeki seyri açısından belirleyicidir. BTK'nın yayımladığı 5G frekans planlaması kapsamında Türkiye'nin 5G SA altyapısına geçişinin tamamlanması uzun vadede gerçekleşeceği öngörülmektedir. Bu süreçte NSA dağıtımı yaygın olacağından, 2G/3G ağların da aktif kalacağından ve downgrade saldırılarının etkili olmaya devam edeceği bir geçiş dönemi kaçınılmazdır.

Bu tablonun pratik sonucu şudur: 5G'nin IMSI Catcher tehdidini tam anlamıyla ortadan kaldırması için SA altyapısının yaygınlaşması, 2G/3G ağların kapatılması ve NSA güvenlik açıklarının giderilmesi gerekmektedir. Bu üç koşulun eş zamanlı sağlanması önümüzdeki on yılın ötesine taşan bir süreç gerektirecektir.

9. Patent ve Yeni Nesil 5G IMSI Catcher Sistemleri

5G SUPI/SUCI mekanizmasının geleneksel IMSI Catcher tekniğini engellediği bilinmektedir; ancak bu engeli aşmayı hedefleyen yeni nesil sistemlerin patent kayıtlarında belgelenmesi

dikkat çekicidir. ABD Patent No. 12328588, 5G ağlarında IMSI yakalama için bir sistem ve yöntemi kapsamaktadır. Patentin açıklamasına göre sistem; hem 5G hem de alt nesil baz istasyonlarını taklit eden iki ayrı verici içermektedir.

Patentin temel teknik yaklaşımı şöyledir: Sistem, Yasal Müdahale (LI) iletişim arayüzü üzerinden ilgili SUPI'ye karşılık gelen 5G tanımlayıcısını çekirdek ağdan alır. Ardından hedef cihazın bu 5G tanımlayıcısıyla sahte istasyona bağlanmasını sağlar; eşleşme onaylanırsa cihazı alt nesil sisteme (4G veya 2G) kaydeder ve böylece geleneksel IMSI Catcher tekniklerini uygulayabilir hale gelir (USPTO, 2025).

Bu patent, üç önemli çıkarımı gündeme taşımaktadır. Birincisi, 5G SA altyapısında bile yasal müdahale arayüzüne erişim sağlanabildiğinde IMSI Catcher benzeri sistemlerin çalışabileceği tescil edilmiştir. İkincisi, bu tür sistemlerin geliştirme faaliyeti açıkça sürmektedir. Üçüncüsü, patentin 'yasal müdahale' çerçevesinde sunulması, bu teknolojinin tasarım amacının hukuki çerçeve içinde kalmak olduğuna işaret etmektedir; ancak ticari zincirden çıktıktan sonra kontrolün nasıl sağlanacağı ayrı bir soru olarak kalmaktadır.

10. Önerilen Düzenleyici Çerçeve ve Politika Önerileri

IMSI Catcher kullanımının meşru adli ve güvenlik amaçlarıyla sınırlı tutulabilmesi için kapsamlı bir düzenleyici çerçeve zorunludur. Uluslararası uygulamalar ve akademik literatür ışığında bu çerçevenin bileşenleri aşağıda sistematik biçimde sunulmaktadır.

10.1 Yasal Güvenceler

- **Bireyselleştirilmiş yargısal yetki:** Ağır suçların soruşturulmasıyla sınırlı, somut şüpheye dayanan mahkeme kararı. Genel ya da önleyici IMSI Catcher kullanımı yasal olarak yasaklanmalıdır.
- **48 saatlik hedef dışı veri imha yükümlülüğü:** Kapsama alanında toplanan hedef dışı bireylere ait veriler en geç kırk sekiz saat içinde güvenli biçimde imha edilmeli; bu süreç denetim kaydıyla belgelenmelidir.
- **Hassas bağlam özel onay gerekliliği:** Sağlık tesisleri, hukuk büroları, ibadet yerleri, basın toplantısı alanları ve siyasi etkinlik mekânlarında kullanım için üst yargı makamı onayı zorunlu tutulmalıdır.
- **Non-disclosure agreement (NDA) yasağı:** Üretici ile kolluk kurumları arasındaki gizlilik sözleşmeleri, yargı bilgilendirme yükümlülüğünün önüne geçemez.

10.2 Şeffaflık ve Denetim Mekanizmaları

- **Yıllık kullanım istatistikleri raporu:** Hangi kurumların, kaç kez, hangi suç kategorilerinde IMSI Catcher kullandığı bağımsız denetim kurumuna yıllık raporlanmalıdır.
- **Sanık bilgilendirme yükümlülüğü:** Sanıklar aleyhinde IMSI Catcher delili kullanılıyorsa savunma bu yöntemden haberdarlık hakkına sahip olmalıdır.
- **Parlamento denetimi:** Güvenlik birimleri, kullanımın toplam kapsamını ve delil etkisini ilgili parlamenter komisyona düzenli aralıklarla raporlamalıdır.

burakgun.com

10.3 Teknik Güvenceler

- **5G SA altyapısına öncelikli geçiş:** Operatörlerin 5G Standalone altyapısına geçişi ve 2G/3G ağların kademeli kapatılması teşvik edilmelidir.
- **SUCI padding standardizasyonu:** Ericsson/Nori çalışmasının (2021) önerdigi SUCI uzunluk dolgu mekanizmasının 3GPP standardına dahil edilmesi için regülatör baskısı uygulanmalıdır.
- **Kurumsal IMSI Catcher tespiti altyapısı:** Hassas tesisler (mahkemeler, parlamento, sağlık kurumları) için donanım tabanlı IMSI Catcher tespit sistemleri zorunlu hale getirilmelidir.

11. Sonuç

IMSI Catcher teknolojisi, hücresel iletişim altyapısının onlarca yıldır giderile memiş bir tasarım açığından beslenen ve bu açıkla birlikte evrilen bir gözetim aracıdır. 2G'nin yarattığı tek taraflı kimlik doğrulama boşluğu, 3G ve 4G kuşaklarında kısmen giderilmeye çalışılmış; ancak downgrade saldırısı vektörü, geriye dönük uyumluluk zorunluluğu ve 5G NSA dağıtımının 4G açıklarını miras alması nedeniyle tehdit tamamen ortadan kalkamamıştır.

5G SA mimarisinin getirdiği SUPI/SUCI mekanizması, geleneksel toplu IMSI toplama saldırısını Standalone dağıtımlarda fiilen işlevsiz kılmaktadır. Bununla birlikte Nori çalışmasının ortaya koyduğu uzunluk açığı, ACM WiSec 2021'de gösterilen 5G SUCI-Catcher proof-of-concept ve Patent No. 12328588 gibi gelişmeler; 5G'nin tam bir güvenlik garantisi sunmadığını net biçimde ortaya koymaktadır. Üstelik 5G SA altyapısının küresel ölçekte yaygınlaşması en az on yıllık bir süreç gerektirmektedir.

Ticari IMSI Catcher pazarı, 2033'te 400 milyon doları aşacak şekilde büyümeye devam etmektedir. Bu büyüme yalnızca meşru kolluk kullanımını değil; otoriter gözetim, kurumsal casusluk ve organize suç uygulamalarını da kapsamaktadır. Teknolojinin bu geniş potansiyel kötüye kullanım yelpazesi, güçlü yasal çerçevelere olan ihtiyacı kaçınılmaz kılmaktadır.

Türkiye açısından bu tablonun önemi son derece büyüktür. CMK 135'in bireysellik şartı ile IMSI Catcher'ın doğasındaki toplu veri toplama niteliği arasındaki çelişki, yasal belirsizliği derinleştirmektedir. KVKK'nın kişisel veri koruma çerçevesi, bu alandaki açığı kısmen örtebilmekle birlikte IMSI Catcher'a özgü bir düzenlemenin yokluğu hem hukuki belirlilik hem de insan hakları güvencesi açısından ciddi bir eksiklik olarak kalmaya devam etmektedir.

Sonuç olarak IMSI Catcher meselesi, teknik bir güvenlik sorununu aşarak demokratik devlet ilkesinin örgüsüne dokunan bir soru haline gelmiştir: Suçluları takip etme meşru amacı, masum insanların verilerini toplu elde etme aracını meşrulaştırabilir mi? Uluslararası içtihat bu soruya net bir yanıt vermektedir: Yalnızca bireyselleştirilmiş yargısal denetim, orantılılık ilkesi ve hedef dışı verinin güvenceli imhası bu gerilimi meşru zemine taşıyabilir.

kurakoglu.com

Kaynakça

3GPP. (2012). Security architecture (TS 33.102, Release 11). 3rd Generation Partnership Project.

3GPP. (2019). Security architecture and procedures for 5G system (TS 33.501, Release 15). 3rd Generation Partnership Project.

ACM WiSec. (2021). 5G SUCI-catchers: Proof-of-concept attack in 5G standalone networks. Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks. https://dl.acm.org/doi/abs/10.1145/3448300.3467826

Business Research Insights. (2024). IMSI catcher market size and forecast 2024-2033. https://www.businessresearchinsights.com/market-reports/imsi-catcher-market-106084

Carpenter v. United States, 585 U.S. 296 (2018).

Cell-Site Simulator Warrant Act of 2021, S. 2122, 117th Cong. (2021).

Chapman, R. C. (2017). The outer limits: IMSI-catchers, technology, and the future of the Fourth Amendment. Pepperdine Law Review, 44(4), 1101–1142.

Cloudwards. (2025, November 21). How to block StingRay surveillance: Detection and protection. https://www.cloudwards.net/how-to-block-stingray-surveillance/

Dabrowski, A., Pianta, N., Kleissner, C., Shulman, H., Steiner, M., & Weippl, E. (2014). IMSI-catch me if you can: IMSI-catcher-catchers. Proceedings of the 30th Annual ACSAC, 246–255. https://doi.org/10.1145/2664243.2664272

Electronic Frontier Foundation (EFF) / Street Level Surveillance. (tarihsiz). Cell-site simulators / IMSI catchers. https://sls.eff.org/technologies/cell-site-simulators-imsi-catchers

Entropy Survival. (2026, March 5). IMSI catcher explained: How cell surveillance works. https://entropysurvival.com/blogs/news-views/imsi-catcher-guide

Ericsson. (2024, April 4). Privacy by subscription ID length variation. Ericsson Blog. https://www.ericsson.com/en/blog/2024/4/privacy-by-subscription-id-length-variation

ESPLawyers. (tarihsiz). Stingray device cases in court: Privacy, surveillance, and legal battles. https://esplawyers.com/judicial-developments/stingray-device-cases-in-court-privacy-surveillance-and

European Court of Human Rights. (2015). Roman Zakharov v. Russia, Application No. 47143/06 (Grand Chamber).

European Court of Human Rights. (2016). Szabó and Vissy v. Hungary, Application No. 37138/14.

InfiShark. (2026, March 26). Stingray devices: How IMSI catchers work. https://infishark.com/blogs/learn/stingray-devices-how-imsi-catchers-work

KVKK. (2025). 2024 Yılı Faaliyet Raporu. Kişisel Verileri Koruma Kurumu, Ankara.

Lightreading. (2023, November 14). 5G defends against IMSI catchers — but implementation is critical. https://www.lightreading.com/security/5g-defends-against-imsi-catchers---but-implementation-is-critical/d/d-id/771471

burakgun.com

MDPI. (2024). Security vulnerabilities in 5G Non-Stand-Alone networks: A systematic analysis and attack taxonomy. Electronics, 13(1), Article 2. https://www.mdpi.com/2624-800X/4/1/2

National Security Law Brief. (tarihsiz). IMSI catchers and potential 4th Amendment violations. https://www.nationalsecuritylawbrief.com/post/imsi-catchers-and-potential-4th-amendment-violations

Palindrome Tech. (2025, August 1). An evolutionary analysis of cellular network security: Vulnerabilities and protections from 2G to 5G. https://palindrometech.com/applied-security-research-blog

Park, C., Park, J., Nyang, D., & Yeom, D. (2017). White-Stingray: Evaluating IMSI catcher detection applications. Proceedings of WOOT 2017, USENIX.

Preeß Mattsson, J., & Nakarmi, P. K. (2021). Nori: Concealing the concealed identifier in 5G. arXiv preprint arXiv:2105.10440. https://arxiv.org/pdf/2105.10440

Shaik, A., Borgaonkar, R., Asokan, N., Niemi, V., & Seifert, J.-P. (2016). Practical attacks against privacy and availability in 4G/LTE mobile communication systems. Proceedings of NDSS 2016. https://doi.org/10.14722/ndss.2016.23236

SkyQuest. (2024). IMSI catcher market size and share 2025-2032. https://www.skyquestt.com/report/imsi-catcher-market

Thales Group. (2021, May 26). 5G SIM, security and privacy for IMSIs. https://www.thalesgroup.com/en/worldwide-digital-identity-and-security/mobile/magazine/5g-sim-security-and-privacy-imsis

Total Secure Defence. (2024, March 14). Are IMSI catchers legal? Legal implications of using IMSI catchers. https://totalsecuredefence.com/2024/03/are-imsi-catchers-legal-legal-implications-of-using-imsi-catchers/

United States Patent and Trademark Office. (2025). US Patent No. 12328588: System and method for IMSI catching in 5G networks. https://image-ppubs.uspto.gov/dirsearch-public/print/downloadPdf/12328588

Wikipedia. (2026, February 25). IMSI-catcher. https://en.wikipedia.org/wiki/IMSI-catcher

Zetier. (2025, April 28). Did 5G kill the IMSI catcher? https://zetier.com/5g-imsi-catcher/

Zimperium. (tarihsiz). IMSI catcher. Mobile Security Glossary. https://zimperium.com/glossary/imsi-catcher

burakoguz.com