OSINT: AÇIK KAYNAK İSTİHBARATI ADLİ DELİL OLABİLİR Mİ?

Derleme Makale / Review Article

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

Anahtar Kelimeler: *OSINT • Açık Kaynak İstihbaratı • Dijital Delil • Bellingcat • Berkeley Protokolü • UCM • AİHM*

ÖZET

Açık Kaynak İstihbaratı (Open Source Intelligence — OSINT), kamuya açık kaynaklardan sistematik biçimde veri toplayarak analiz eden bir istihbarat ve soruşturma disiplinidir. Sosyal medya paylaşımları, uydu görüntüleri, coğrafi etiketli içerikler, forum kayıtları, haber arşivleri, tescil ve sözleşme veritabanları bu disiplinin temel ham maddesini oluşturmaktadır. Bellingcat ve Mnemonic gibi kuruluşların MH17, Ukrayna çatışması ve Suriye iç savaşına ilişkin belgeleme çalışmaları, OSINT metodolojisinin uluslararası mahkemelerde fiilen kullanıldığı ya da kullanımının tartışıldığı bir gerçekliğe işaret etmektedir. 2022'de OHCHR ve UC Berkeley tarafından yayımlanan Berkeley Protokolü, OSINT soruşturmaları için uluslararası metodoloji standartlarını ilk kez sistematik biçimde kodlamıştır. Bu derleme makale; OSINT'in tarihsel köklerini, temel teknik metodolojilerini, araç ekosistemini, coğrafi konum ve doğrulama yöntemlerini, Mnemonic arşivleme yaklaşımını, Berkeley Protokolü standartlarını, MH17 ve Ukrayna davası örneklerini, Uluslararası Ceza Mahkemesi ve AİHM bağlamındaki delil kabul tartışmalarını, yapay zeka ve deepfake tehdidini, Türk hukuku kapsamındaki değerlendirmeleri ve OSINT araştırmacılarının etik ve güvenlik sorumluluklarını kapsamlı biçimde ele almaktadır.

Anahtar Kelimeler: *OSINT, açık kaynak istihbaratı, dijital delil, Bellingcat, Berkeley Protokolü, UCM, Uluslararası Ceza Mahkemesi, AİHM, coğrafi doğrulama, uydu görüntüsü, Mnemonic, deepfake, Türk hukuku, CMK 217, dijital doğrulama*

burakolgun.com

ABSTRACT

Open Source Intelligence (OSINT) is an intelligence and investigation discipline that systematically collects and analyzes data from publicly available sources. Social media posts, satellite imagery, geotagged content, forum records, news archives, and registration databases constitute the primary raw materials of this discipline. The documentation work of organizations like Bellingcat and Mnemonic on MH17, the Ukraine conflict, and the Syrian civil war points to a reality in which OSINT methodology is actually being used or debated for use in international courts. The Berkeley Protocol, published by OHCHR and UC Berkeley in 2022, codified international methodology standards for OSINT investigations systematically for the first time. This review article comprehensively addresses OSINT's historical roots, core technical methodologies, tool ecosystem, geolocation and verification methods, Mnemonic's archiving approach, Berkeley Protocol standards, MH17 and Ukraine case examples, evidence admissibility debates in the ICC and ECHR, AI and deepfake threats, evaluations within Turkish law, and the ethical and security responsibilities of OSINT researchers.

Keywords: *OSINT, open source intelligence, digital evidence, Bellingcat, Berkeley Protocol, ICC, ECHR, geolocation, satellite imagery, Mnemonic, deepfake, Turkish law, digital verification, chain of custody*

1. Giriş

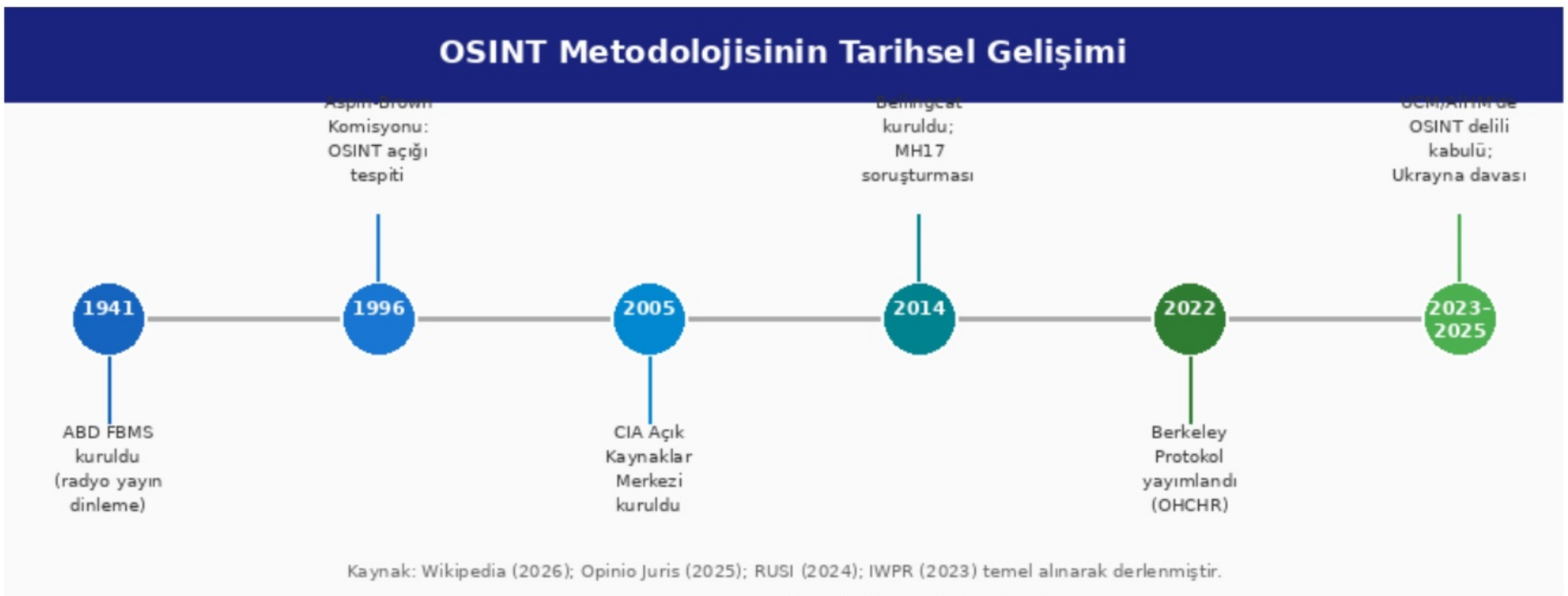
İkinci Dünya Savaşı yıllarında ABD Dışişleri Bakanlığı'na bağlı Yabancı Yayın İzleme Servisi (FBMS), 1941'de radyo dinleme merkezleri aracılığıyla düşman ülkelerin açık yayınlarından istihbarat derlemeye başladı. O dönemde 'Açık Kaynak İstihbaratı' kavramı henüz kullanılmıyor; ancak temel ilke — kamuya açık bilginin sistematik biçimde toplanıp analiz edilmesi — zaten işliyordu. Aradan geçen seksen yılda bu ilke, internet çağının getirdiği veri bolluğuyla birlikte tanımlanamaz ölçüde büyüdü ve 'dijital çağın parmak izi bilimi' olarak nitelendirilen OSINT disiplinine dönüştü (Wikipedia, 2026).

Günümüzde bir araştırmacı; Twitter/X arşivleri, Google Earth'ün tarihsel görüntüleri, Maxar uydu fotoğrafları, Telegram kanal kayıtları ve WHOIS tescil veritabanları kombinasyonuyla askeri birliklerin hareketlerini izleyebilmekte, savaş suçu delillerini belgeleyebilmekte ya da şüphelilerin kimliğini tespit edebilmektedir. Salisbury zehirleme olayında Rus GRU ajanlarının kimliğini tespit eden, MH17'yi düşüren füzenin Rusya'ya ait olduğunu kanıtlayan, Bucha'daki katliam fotoğraflarının coğrafi konumunu doğrulayan Bellingcat; bu disiplinin pratikteki gücünü tartışmasız biçimde sergilemiştir (IWPR, 2023).

Bununla birlikte OSINT'in adli delil olarak kullanılması — istihbarat üretmekten temelden farklı bir süreçtir. Bir bilgiyi elde etmek ile o bilgiyi mahkemede kanıtlamak arasındaki mesafe; özgünlük doğrulama, zincir muhafaza, metodolojik şeffaflık ve yargısal kabul kriterleri gibi zorlu gerekliliklerle doludur. Opinio Juris'te Dirisu'nun (2025) belirttiği üzere, 'başlıca sorun standartlaştırılmış metodolojilerin yokluğudur; bu durum, delil

kurallarının uygulanmasını karmaşıklaştırmakta ve güvenilirlik ile ispat değerinin tutarlı biçimde değerlendirilmesini engellemektedir.'

Bu makalenin amacı, OSINT disiplinini hem teknik hem hukuki boyutlarıyla derinlemesine incelemektir. OSINT araçları ve metodolojileri, Berkeley Protokolü standartları, uluslararası yargısal gelişmeler, Türk hukukundaki değerlendirmeler ve yapay zekanın yarattığı yeni tehditler makalenin eksenlerini oluşturmaktadır.



Şekil 1. *OSINT Metodolojisinin Tarihsel Gelişimi (1941–2025)*

2. OSINT: Kavramsal Çerçeve ve Tanımlar

2.1 Resmi Tanımlar ve Kapsam

ABD Anayurt Güvenliği Bakanlığı (DHS), OSINT'i 'kamuya açık bilgiden üretilen, belirli bir istihbarat gereksinimini karşılamak amacıyla uygun bir kitleye zamanında toplanarak işlenen ve iletilen istihbarat' olarak tanımlamaktadır. NATO, OSINT'i 'kamuya açık bilgiden ve sınırlı dağıtımlı ya da erişimli diğer sınıflandırılmamış verilerden elde edilen istihbarat' şeklinde ifade etmektedir. AB ise 'eyleme dönüştürülebilir istihbarat üretmek için açık kaynaklardan bilgi toplama ve analiz etme süreci' tanımını benimsemektedir (Wikipedia, 2026).

Bu tanımların ortak noktası 'kamuya açıklık' ilkesidir. OSINT, yetkisiz erişim, bilgisayar sistemine sızma ya da gizli kaynaklardan bilgi elde etmeyi kapsamaz; aksine bu yollarla elde edilen bilgi OSINT değil, farklı bir hukuki statü taşır. Bu ayrım, hem etik hem de delil hukuku açısından kritik öneme sahiptir: Kamuya açık kaynaktan derlenen verinin elde etme aşamasında özel bir yetkiye ihtiyaç bulunmamaktadır; ancak bu durum verinin otomatik olarak mahkemede kabul edilebilir olduğu anlamına gelmemektedir (OSINT FR, 2023).

2.2 İstihbarat ile Delil Arasındaki Temel Fark

OSINT'in adli bağlamdaki en temel gerilimi, istihbarat ile delil arasındaki yapısal farktır. Springer Nature (2017) bu farkı şöyle özetlemektedir: 'İstihbarat ve delil temelden birbirinden farklıdır ve her delil bir ölçüde istihbarat sağlayabilse de tersi her zaman doğru değildir.

İstihbaratın delil olarak kullanılabilmesi için, diğer herhangi bir delil türüyle aynı adli standartları karşılaması ve aynı hukuki engelleri aşması gerekmektedir.'

Bu ayrımın pratik sonucu şudur: OSINT analistleri, soruşturmayı yürütürken aynı zamanda olası bir yargısal süreci de gözetmek zorundadır. AFCEA'nın (2023) değerlendirmesine göre, OSINT'in delil olarak sunulabilmesi için üç kriter karşılanmalıdır: Kaynağın net ve yasal biçimde tanımlanması, verinin değiştirilmemiş ya da manipüle edilmemiş olduğuna dair güvenilirlik güvencesi ve kanıtı sağlayan kişinin bağımsızlığı ile güvenilirliği.

2.3 OSINT Alt Disiplinleri

OSINT, kaynak türüne göre birkaç alt disipline ayrılmaktadır. SOCMINT (Social Media Intelligence), sosyal medya platformlarından — Twitter/X, Telegram, Instagram, TikTok, VKontakte — bilgi toplama ve analiz etme sürecidir. Özellikle Bellingcat'in Ukrayna soruşturmalarında SOCMINT, askeri ekipmanların tespiti ve kimlik doğrulama açısından birincil veri kaynağı işlevi görmüştür.

GEOINT (Geospatial Intelligence) uydu görüntüleri, haritalama verileri ve coğrafi analizden elde edilen istihbaratı kapsamaktadır. TECHINT (Technical Intelligence) silah sistemleri, araçlar ve ekipmanların açık kaynaklardan teknik analizini ifade eder. FININT (Financial Intelligence) ise şirket kayıtları, tescil bilgileri ve halka açık finansal verilerden elde edilen analizi tanımlamaktadır (Wikipedia, 2026).

3. OSINT Araç Ekosistemi



Şekil 2. *OSINT Araç Ekosistemi — Altı Kategori ve Temsili Araçlar (2025)*

3.1 Ağ ve Altyapı Araçları

Shodan, 'İnternete bağlı cihazlar için arama motoru' olarak tanımlanan, sunuculardan IoT cihazlarına uzanan her türlü çevrimiçi altyapıyı indeksleyen bir platformdur. Siber güvenlik profesyonelleri ve dijital araştırmacılar tarafından açık port tespiti, yazılım sürüm analizi ve coğrafi tehdit haritalama amacıyla kullanılmaktadır. Shodan'ın 2025 güncellemesiyle AI tabanlı tehdit tahmin özellikleri eklendiği belirtilmektedir (Web Asha Technologies, 2026).

theHarvester ve Recon-ng, e-posta adresleri, alan adları ve IP bilgilerini açık kaynaklardan toplayarak hedef profili oluşturmak amacıyla kullanılan komut satırı araçlarıdır. WHOIS sorguları ve ARIN/RIPE kayıtları, alan adı mülkiyeti ve ağ altyapısına ilişkin tescil bilgilerine erişim sağlamaktadır. Bu araçlar özellikle siber suç soruşturmalarında ve kurumsal due diligence süreçlerinde yaygın biçimde kullanılmaktadır.

3.2 Bağlantı Analizi: Maltego

Maltego, OSINT araçları ekosisteminin en kapsamlı bağlantı analizi ve veri görselleştirme platformlarından biridir. Araç, alan adları, IP adresleri, e-postalar, sosyal medya profilleri ve şirket kayıtları gibi varlıklar arasındaki ilişkileri grafik formatında görselleştiren 'dönüşüm' (transform) mekanizmasıyla çalışmaktadır. Karmaşık soruşturmalarda gizli bağlantıları ortaya çıkarmak için kritik bir araç işlevi görmektedir (Web Asha Technologies, 2026).

Salisbury zehirleme soruşturmasında Maltego ve Shodan kombinasyonu, Rus GRU ajanlarının seyahat ve dijital izlerini takip etmek için kullanılmış; pasaport bilgileri, seyahat kayıtları ve önceki seyahat verileri analiz edilerek şüphelilerin hareketleri farklı ülkelere bağlanabilmiş ve devlet destekli müdahale iddiasını destekleyen kanıtlar elde edilmiştir (Web Asha Technologies, 2026).

3.3 Arşivleme ve Geçmişe Yönelik Araçlar

Wayback Machine (archive.org), internet içeriklerinin tarihsel kopyalarını saklayan en kapsamlı web arşiv hizmetidir. Hukuki süreçlerde silinmiş veya değiştirilmiş web içeriklerinin önceki halini belgelemek için kullanılmaktadır. Ketcham'ın (2025) aktardığı Gates Rubber v. Bando Chemical Industries davasında, dijital içeriğin özgünlük standartlarına ilişkin yargısal değerlendirmelerde archive.org kayıtları referans alınmıştır.

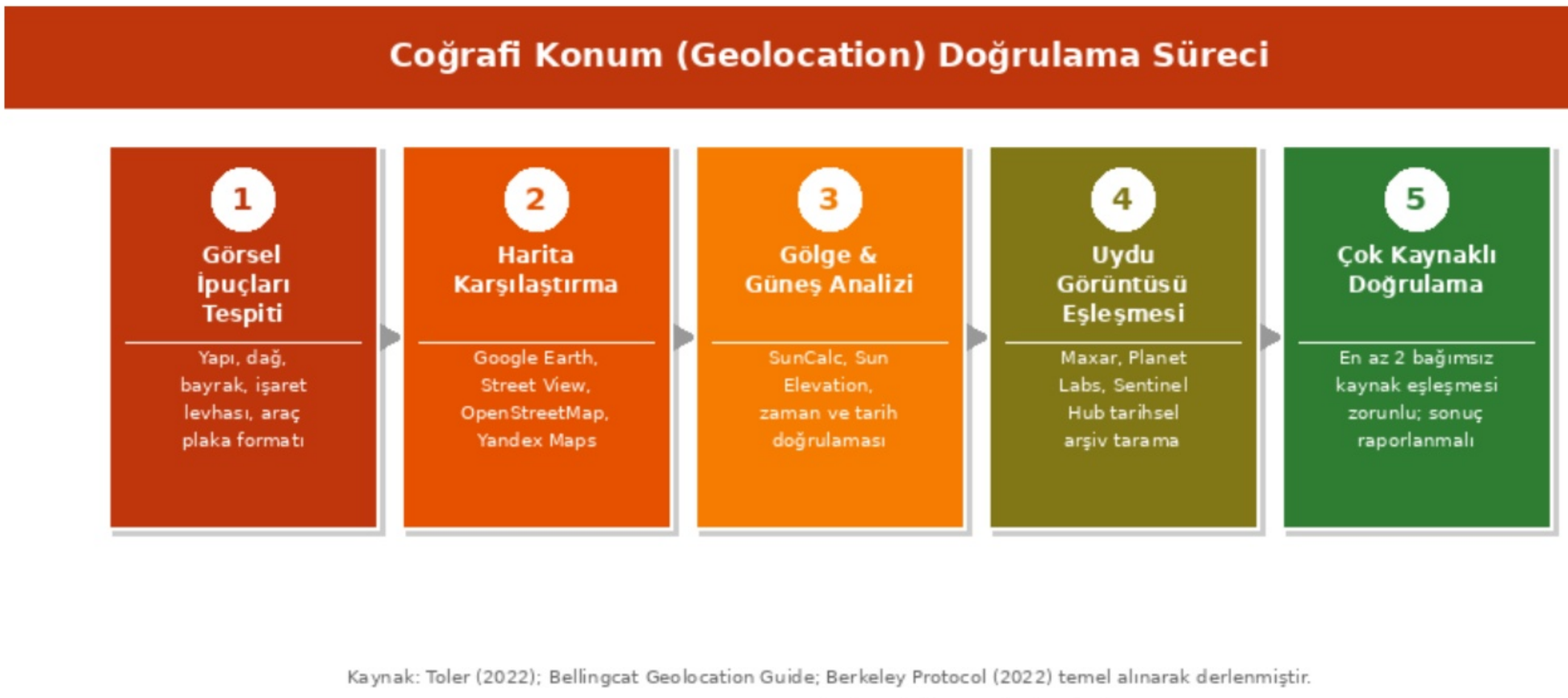
Intelligence X, sızdırılmış veritabanları, derin web içerikleri ve tarihsel web anlık görüntülerini indeksleyen özelleşmiş bir arşiv platformudur. E-posta adresleri, alan adları, IP'ler veya belgeler üzerinden güçlü arama yapma imkânı sunan bu platform, tehdit istihbaratı ve adli araştırmalar için önemli bir kaynak niteliği taşımaktadır (OSINT Byle, 2025).

3.4 1 TRACE ve Entegre Platformlar

2024'te piyasaya sürülen 1 TRACE, sosyal medya, coğrafi, siber ve finansal OSINT disiplinlerini tek bir güvenli entegre sistemde birleştiren yeni nesil bir platformdur. ISO 27001:2022 sertifikasyonu, hükümetler, kolluk birimleri ve kurumsal kullanıcılar tarafından güvenle kullanılmasına zemin hazırlamaktadır. Kripto para işlemlerini takip eden özelliği,

dijital para birimlerinin suç faaliyetlerinde artan kullanımına karşı kritik bir araç işlevi görmektedir (OSINT Byle, 2025).

4. Temel OSINT Teknikleri: Metodoloji ve Doğrulama



Şekil 3. *Coğrafi Konum (Geolocation) Doğrulama Sürecinin Beş Aşaması*

4.1 Coğrafi Konum Analizi: Metodoloji ve Araçlar

Coğrafi konum analizi (geolocation), bir görüntü ya da videonun çekildiği konumun görsel ipuçlarından belirlenmesidir. Bellingcat'in (2023) geolocation kılavuzuna göre bu analiz beş aşamada yürütülmektedir. Birinci aşamada görüntüdeki yapılar, manzara özellikleri, bayraklar, araç plaka formatları, işaret levhaları ve bitki örtüsü gibi görsel ipuçları sistematik biçimde kataloglanır.

İkinci aşamada bu ipuçları Google Earth, Google Street View, OpenStreetMap ve Yandex Haritalar gibi araçlarla karşılaştırılır. Üçüncü aşamada SunCalc veya benzeri araçlar kullanılarak görüntüdeki gölge açısından güneşin o andaki konumu hesaplanır; bu hesaplama hem çekim saatini hem de tarihini bağımsız biçimde doğrulama imkânı sunar. Dördüncü aşamada Maxar, Planet Labs veya Copernicus Sentinel uydu görüntüleri ile karşılaştırma yapılır. Beşinci ve son aşamada en az iki bağımsız kaynaktan doğrulama sağlanmadan sonuç kesinleştirilmez.

Coğrafi konum analizinin güvenilirliğini etkileyen en kritik faktör uzman bağımlı yorumlamadır. Aynı görüntüden farklı analistler farklı konumlara ulaşabilmektedir; bu durum mahkeme bağlamında bilirkişi alanında ciddi metodolojik kaygılar doğurmaktadır. AFCEA (2023), bu nedenle coğrafi konum bulgularının kör yöntemle birden fazla analist tarafından bağımsız olarak doğrulanmasını önermektedir.

4.2 Uydu Görüntüsü Analizi

Ticari uydu görüntüsü, OSINT'in en güçlü bileşenlerinden biridir. Maxar Technologies, Planet Labs ve Airbus Defence & Space, 50 cm'e kadar inen yer çözünürlüklü görüntüler sunmaktadır;

bu çözünürlük araç sayımı, inşaat takibi, hasar değerlendirmesi ve toplu mezar tespiti gibi adli uygulamalara olanak tanımaktadır. Reuters Institute'ün (2023) raporuna göre Bellingcat'in TimeMap aracı, uydu görüntüsüyle desteklenerek Ukrayna'da 1.094 bombalama, silahlı saldırı ve hava saldırısı vakasını zaman ve coğrafya üzerinde konumlandırmıştır.

Uydu görüntüsünün adli bağlamda kullanımı çeşitli metodolojik gereklilikleri beraberinde getirmektedir: Görüntü edinme tarihi ve saatinin bağımsız kaynaktan doğrulanması, görüntü kalitesi ve çözünürlük raporlanması, atmosferik bozulmaların (bulut örtüsü, sis) açıklanması ve uydu sağlayıcısının sertifika zincirinin belgesi. Bu gerekliliklerin karşılanması, uydu görüntüsünün adli delil olarak sunulmasında temel güvenilirlik kriterlerini oluşturmaktadır.

4.3 Zaman Doğrulaması: Kronolokalmasyon

Bir görüntünün ne zaman çekildiğinin bağımsız olarak belirlenmesi, OSINT metodolojisinin en teknik ve titizlik gerektiren boyutlarından birini oluşturmaktadır. Dört temel kronolokalmasyon tekniği kullanılmaktadır: EXIF metadata analizi — görüntü dosyasına gömülü çekim tarihi/saati bilgisi; ancak bu verinin sosyal medya platformları tarafından silindiği unutulmamalıdır.

Güneş gölge analizi, görüntüdeki gölgelerin uzunluğu ve açısından SunCalc veya Suncalc3 araçlarıyla güneşin o andaki konumunu hesaplayarak tarihi daraltır. Hava arşivi karşılaştırması, görüntüdeki hava koşullarını belirli bir bölge için tarihsel meteoroloji kayıtlarıyla eşleştirir. Bağlamsal zaman işaretleri ise görüntüdeki gazete başlıkları, takvimler veya belirli olayların izleri gibi içerik ipuçlarından tarih aralığı çıkarmayı kapsar.

4.4 EXIF Metadata ve Dijital Parmak İzi

Dijital görüntü ve video dosyalarına gömülü EXIF (Exchangeable Image File Format) metadata; çekim tarihi/saati, GPS koordinatları, cihaz marka-model ve yazılım sürümü gibi adli açıdan değerli bilgiler içerebilmektedir. ExifTool, bu veriye erişmek için yaygın kullanılan açık kaynaklı araçların başında gelmektedir. Web Asha Technologies'in (2026) değerlendirmesine göre ExifTool ve Creepy, metadata çıkarımı, görüntü coğrafi konumlama ve çevrimiçi kimlik izleme için dijital adliyeciler tarafından yaygın biçimde kullanılmaktadır.

EXIF metadata sınırlılıkları açısından ise kritik bir husus şudur: Twitter/X, Facebook ve Instagram gibi büyük sosyal medya platformlarının büyük çoğunluğu, içerik yüklenirken EXIF verisini otomatik olarak siliyor ya da üzerine yazıyor. Bu durum, görüntünün asıl çekilen cihazdan değil platformdan alındığı durumlarda EXIF verisinin bulunmamasının 'görüntü sahte' anlamına gelmediğini göstermektedir. Metadata yokluğu değil, diğer doğrulama yöntemleriyle tutarlılık esas ölçüt olmalıdır.

Tablo 1. *Başlıca OSINT Tekniklerinin Karşılaştırmalı Değerlendirmesi*

Teknik	Araçlar	Adli Değer	Temel Sınırlılık
Coğrafi Konum	Google Earth, SunCalc, Wikimapia	Yüksek (doğrulanırsa)	Uzman bağımlı yorumlama; çapraz doğrulama zorunlu

Teknik	Araçlar	Adli Değer	Temel Sınırlılık
Uydu Görüntüsü	Maxar, Planet Labs, Sentinel	**Çok Yüksek**	Sağlayıcı sertifikası; çözünürlük sınırı
Sosyal Medya Arşivi	Wayback Machine, archive.today	Orta-Yüksek	Silinmiş içerik eksikliği; platform EXIF silme
EXIF Metadata	ExifTool, Jeffrey's Exif Viewer	Orta (tamamlayıcı)	Platform tarafından otomatik siliniyor
Gölge/Güneş Analizi	SunCalc, Suncalc3	Orta-Yüksek	Hassas tarih/saat gerektirir; bulut/gölge engeli
Bağlantı Analizi	Maltego, Gephi	Yüksek (ağ tespiti)	VPN/Tor ile gizlenebilir; uzmanlık gerektirir
Altyapı Tarama	Shodan, Censys, WHOIS	Orta	Dinamik IP atamalar; cloud hosting anonimleştirme

Not. Kaynak: Toler (2022); OSINT Byle (2025); Web Asha Technologies (2026); AFCEA (2023) temel alınarak derlenmiştir.

5. Mnemonic / Syrian Archive: Kriptografik Bütünlük Modeli

5.1 Dijital İçeriğin Korunması Sorunu

Sosyal medya içeriklerinin geçici niteliği, OSINT arşivlemesinin önündeki en kritik engeli oluşturmaktadır. Twitter/X, YouTube ve Facebook'ta paylaşılan ve potansiyel delil niteliği taşıyabilecek içerikler; platform kuralları, devlet talepleri ya da içerik sahibinin kararıyla herhangi bir anda silinebilmektedir. 2013'te kurulan Mnemonic (önceki adıyla Syrian Archive), bu tehdide karşı geliştirilen en kapsamlı yanıtı temsil etmektedir: 5 milyonu aşkın dijital içeriğin sistematik biçimde arşivlenmesi ve kriptografik bütünlüğünün güvence altına alınması (IWPR, 2023).

5.2 SHA-256 Hash ve Adli Bütünlük

Mnemonic'in temel metodolojik katkısı şudur: Her arşivlenen içerik, kayıt anında SHA-256 kriptografik hash değeri hesaplanarak depolanmaktadır. Bu yaklaşım, içeriğin sonradan değiştirilmediğini matematiksel olarak kanıtlamayı mümkün kılmaktadır. InCyber News'ün (2024) raporladığı Ritu Gill'in Forensic OSINT uygulaması da benzer bir ilkeyle çalışmaktadır: 'Web'den toplanan içeriklerin hash değerini hesaplayarak 'özgünlük mührü' işlevi gören hash, dijital delilin mahkemede kabul edilebilir olmasını sağlamaktadır.'

Bu yöntem; geleneksel fiziksel delil zinciri muhafazasının dijital dünyaya uyarlanmış biçimini temsil etmektedir. Dijital delil bütünlüğünü sağlamanın kritik önemi şuradan kaynaklanmaktadır: Herhangi bir piksel değişikliği veya metadata düzenlemesi hash değerini değiştirmekte; bu durum tamamen değiştirilemez bir doğrulama mekanizması sunmaktadır. Blockchain tabanlı notarizasyon da bu alanda MDPI'de (2025) yayımlanan araştırmada önerilen tamamlayıcı yöntemler arasında yer almaktadır.

6. Berkeley Protokolü: Uluslararası Metodoloji Standardı



Şekil 4. *Berkeley Protokolü'nün 6 Aşamalı Soruşturma Döngüsü (OHCHR/UC Berkeley, 2022)*

6.1 Protokolün Doğuşu ve Kapsamı

Berkeley Protokolü on Digital Open Source Investigations, OHCHR (BM İnsan Hakları Yüksek Komiserliği Ofisi) ve UC Berkeley Hukuk Fakültesi İnsan Hakları Merkezi'nin üç yıllık ortak çalışmasının ürünü olarak 2022'de yayımlanmıştır. Uluslararası ceza, insancıl hukuk ve insan hakları ihlalleri soruşturmalarında dijital açık kaynak bilgisinin tanımlanması, toplanması, korunması, doğrulanması ve analiz edilmesi için minimum mesleki standartları belirleyen bu belge, alanın tarihindeki ilk kapsamlı metodoloji çerçevesini oluşturmaktadır (OHCHR, 2022).

Protokolün temel felsefesi, araç bağımsızlığıdır: Hızla evrilen teknoloji ortamında belirli araçlara bağımlı kurallar yerine metodolojik ilkeler ve etik çerçeve belirlenmiştir. Bu sayede protokol, yeni araçlar ve platformlar ortaya çıktığında da geçerliliğini koruyabilen 'yaşayan bir belge' niteliği kazanmaktadır. UC Berkeley İnsan Hakları Merkezi Direktörü Alexa Koenig protokolü 'dünya çapındaki açık kaynak soruşturmalarının hukuki standartlarını güçlendirecek, 21. yüzyıl yöntemlerini kullanan yaşayan bir belge' olarak tanımlamıştır (Lexology, 2020).

6.2 Altı Aşamalı Soruşturma Döngüsü

Berkeley Protokolü'nün en önemli katkılarından biri, Bölüm 6'da açıklanan altı aşamalı soruşturma döngüsüdür. Fortuna'nın (2025) değerlendirmesine göre bu döngü, 'ad hoc dijital araştırmacılığı metodolojik açıdan sağlam delil toplamaya dönüştürmektedir.'

Birinci aşama — Planlama ve Amaç Belirleme: Soruşturmanın hukuki çerçevesi, hedefler ve etik kısıtlar belirlenir. Hangi delil türlerinin aranacağı, hangi platformların taranacağı ve güvenlik protokollerinin neler olduğu bu aşamada netleştirilir.

İkinci aşama — Çevrimiçi Arama ve Keşif: Arama stratejileri ve parametreleri belgelenerek sistematik kaynak tarama yürütülür. Kullanılan arama terimleri, platform ve tarih filtrelerinin kaydı metodolojik şeffaflık açısından zorunludur.

Üçüncü aşama — Toplama ve Arşivleme: Belirlenen içerikler hash değerleri hesaplanarak arşivlenir. İçerik kayıt anında dondurulmalı; Wayback Machine veya Hunchly gibi araçlarla zaman damgalı kopya oluşturulmalıdır.

Dördüncü aşama — Doğrulama ve Çapraz Kontrol: Her kritik bulgu, bağımsız kaynaklardan en az iki kez teyit edilir. Coğrafi konum, zaman doğrulaması ve kaynak güvenilirliği ayrı ayrı ele alınmalıdır. Kör doğrulama — analistlerin birbirlerinin sonuçlarını bilmeden bağımsız çalışması — en güçlü yaklaşım olarak önerilmektedir.

Beşinci aşama — Analiz ve Değerlendirme: Toplanan verinin bütünü analiz edilerek sonuçlar ve güven düzeyleri belirlenir. Alternatif açıklamalar açıkça ele alınmalı; yüzde yüz kesinlik iddiasından kaçınılmalıdır.

Altıncı aşama — Raporlama ve Yasal Sunum: Kullanılan metodoloji, araçlar, doğrulama yöntemleri ve sınırlılıklar şeffaf biçimde belgelenir. Sonuçlar olasılıksal dille sunulur; kesin kimlik iddiaları hukuki savunulabilirlik açısından son derece risklidir.

6.3 Protokolün Beş Temel İlkesi

Berkeley Protokolü'nün özünde beş temel ilke yatmaktadır. RESET.ORG'un (2024) özetine göre bu ilkeler şöyle sıralanmaktadır:

- **Hukuki uyum:** Toplama faaliyeti ilgili ülke ve uluslararası hukukla uyumlu olmalıdır.
- **Etik sorumluluk:** Mahremiyet hakları ve hassas toplulukların korunması gözetilmelidir.
- **Metodolojik güvenilirlik:** Prosedürler tekrarlanabilir ve şeffaf olmalıdır.
- **Güvenlik:** Araştırmacıların, tanıkların ve ilk müdahale edenlerin dijital ve fiziksel güvenliği korunmalıdır.
- **Sürekli öğrenme:** Protokol, değişen teknoloji ortamına göre güncellenen yaşayan bir belge niteliği taşımaktadır.

7. Uluslararası Dava Örnekleri: OSINT Sahada

7.1 MH17 Davası: OSINT'in Belirleyici Rolü

2014 yılında Doğu Ukrayna üzerinde düşürülen MH17 Boeing 777, 298 kişiyi hayatından ederdi. Rusya müdahaleyi reddederken Bellingcat araştırmacıları, yalnızca açık kaynaklarla füzeyi Rusya menşeli BUK sistemine bağlayan kapsamlı bir delil zinciri oluşturdu. Araştırma metodolojisi şu adımları kapsıyordu: Sosyal medyada paylaşılan fotoğrafların coğrafi konumlanması; kalkış noktasının birden fazla görsel ipucuyla Ukrayna'daki bir tarlaya

bağlanması. Gölge analiziyle çekim saatinin doğrulanması. Uydu görüntüleriyle yol güzergahının izlenmesi. Sızdırılmış telefon dinleme kayıtlarıyla silah sisteminin kimliğinin teyit edilmesi.

Bellingcat'in bulguları daha sonra Avustralya, Belçika, Hollanda, Malezya ve Ukrayna'dan oluşan Ortak Soruşturma Ekibi (JIT) tarafından doğrulandı. SIDN Fonu CEO'su Valerie Frissen'in değerlendirmesine göre, 'Bellingcat'in MH17 davasındaki çalışması, OSINT'e dayalı bir yaklaşımın gönüllülerin yorulmak bilmez çalışmasıyla birleştiğinde belirleyici delil üretebileceğini kanıtlamıştır' (SIDN, 2022).

AİHM boyutunda ise Bellingcat'in çalışmaları doğrudan atıf almıştır. Bellingcat'in (2023) aktardığına göre, Ukrayna'yı temsil eden avukatlar Bellingcat ve diğer kaynaklarca derlenen Rusya'nın Ukrayna'daki müdahalesi, MH17 ve sınır ötesi topçu saldırıları ile Doğu Ukrayna'daki Rus askeri personeline ilişkin bulguları delil olarak sundu. Rusya tarafı açık kaynak delillerine itiraz etti; ancak Pavloka Eğitim Kampı fotoğrafına yönelik manipülasyon iddiası AİHM tarafından reddedildi. Bu karar, açık kaynak delilinin uluslararası insan hakları yargısı tarafından değerlendirmeye alınabileceğinin kritik emsal niteliğini taşımaktadır.

7.2 Ukrayna Savaşı ve 'Hesap Verebilirlik Ağı'

2022'deki Rusya'nın Ukrayna'yı işgali, OSINT soruşturmacıları için hem en büyük vaka hem de en kapsamlı sınama ortamı oldu. RUSI'nin (2024) raporuna göre Ukrayna ve müttefikleri, Mart 2023'teki 'Adalet için Birlik' konferansında 'hesap verebilirlik ağı' (web of accountability) kavramını benimsedi. Bu ağ; devlet kurumları, UCM, sivil toplum kuruluşları ve OSINT araştırmacılarını koordineli bir belgeleme yapısında bir araya getirmektedir.

Temmuz 2024'teki Okhmadit çocuk hastanesine yönelik saldırı, bu koordinasyonun en çarpıcı örneğini sundu. RUSI'nin (2024) aktardığına göre: 'Ukrayna'daki ve dünyanın dört bir yanındaki OSINT analistleri, hastaneye çarpan Kh-101 füzesinin yapısını ve bileşenini hızla tespit etti; bu durum Rusya'nın saldırıyı örtbas etme fırsatını ortadan kaldırdı ve OSINT'in Kremlin'i hesap verebilir kılmadaki artan önemini teyit etti.'

IWPR'ın (2023) raporuna göre Bellingcat ve Küresel Hukuki Eylem Ağı (GLAN), 2022 yılı sonunda Adalet ve Hesap Verebilirlik Birimi (J&A Unit) adıyla ortak bir girişim başlattı. Bu girişimin hedefi, katı delil standartlarına uyan OSINT soruşturmaları yürütme yöntemlerini tasarlamak, uygulamak ve öğretmektir. Dönüm noktası kararına ilişkin Bellingcat'in aktarımı şöyledir: 'Yemen davası daha önce başladı ve MH17 soruşturmasında yaygın biçimde kullanıldı. AİHM duruşmasında Bellingcat hakkında iki paragraf yer alıyor; bulgularımız, bizi 'amatör' olarak değil kendi değeri üzerinden değerlendiriyor. Bu çalışmamızın olumlu bir tanınmasıdır.'

7.3 Skripal Zehirleme Davası: Kimlik Tespitinde OSINT

Rus ajan Sergei Skripal'in 2018'deki zehirleme davasında OSINT, kamuoyunun takip ettiği bir şeffaflık modeli ortaya koydu. İngiliz istihbaratı şüphelileri belirledi; Bellingcat ve The Insider ise pasaport bilgileri, otel rezervasyonları, havalimanı güvenlik görüntüleri ve Maltego ile Shodan aracılığıyla takip edilen dijital izler kullanarak her iki kişinin de Rus askeri istihbarat servisi GRU'ya bağlı olduğunu kamuoyu önünde belgeledi (Web Asha Technologies, 2026).

Bu dava, OSINT'in sıradan kolluk soruşturmasını nasıl tamamlayabileceğini ve kamuoyu nezdinde devlet hesap verebilirliğini nasıl güçlendirebileceğini gösteren bir referans noktası haline gelmiştir. Resmi açıklamadan önce kamuoyuna sunulan OSINT bulguları, diplomatik baskının oluşmasında belirleyici bir rol üstlendi.

8. Uluslararası Yargısal Çerçeve: UCM, AİHM ve Ulusal Mahkemeler

8.1 Uluslararası Ceza Mahkemesi ve Dijital Delil

UCM Usul ve Kanıt Kuralları'nın 69. Kuralı, delil değerini güvenilirlik, kaynağın bütünlüğü, özgünlük ve yargılamayı olumsuz etkilememe koşullarına bağlamaktadır. Bu genel çerçeve, OSINT delilinin teorik olarak UCM'e sunulabilmesine kapı aralamaktadır. Leiden Journal'ın (Cambridge, 2023) kapsamlı araştırmasına göre, dijital açık kaynak delili sosyal medya platformlarına gönderilen kullanıcı üretimi içerik olarak belgesel delil kategorisinde değerlendirilmektedir.

Leiden Journal (2023) araştırması, delil değerlendirmesinde odanın 'köken, kaynak ya da yazar ile ilgili olaylar içindeki rolü, kalemin oluşturulduğu andan odaya sunulduğu ana kadarki zincir muhafazası ve diğer ilgili hususları' incelediğini ortaya koymaktadır. Bu değerlendirme kriterleri, OSINT arşivlerinin nasıl yapılandırılması gerektiğine ilişkin somut bir metodolojik kılavuz sunmaktadır.

Opinio Juris'te Dirisu'nun (2025) değerlendirmesine göre, Berkeley Protokolü öncesi dönemde sivil toplum kuruluşları ve bağımsız araştırmacıların yürüttüğü OSINT çalışmaları 'resmi kurumsal desteği zaman zaman yoksun bırakılmış; delil kabul edilebilirliği, metodolojik tutarlılık ve hukuki güvenilirlik sorunlarıyla boğuşmuştur.' Protokol, bu dönemin açıklarını kapatmayı hedefleyen ilk yapısal girişimi temsil etmektedir.

8.2 Bellingcat'in UCM Soruşturmasındaki Rolü

UCM'nin Ukrayna'da savaş suçu soruşturması başlatmasının ardından (2022), Bellingcat, Ukrainian Witnesses ve Mnemonic tarafından derlenen açık kaynak belgelerinin resmi soruşturma dosyasına dahil edilip edilmeyeceği tartışmaya açıldı. Bellingcat'in savcılığa sunumu bu bağlamda tarihsel bir belge niteliği taşımaktadır. HHRG Kongre ifadesinde (Grozev, 2022) şunlar yer alır: 'Yemen soruşturmasında geliştirdiğimiz metodoloji; olayları kayıt altına alan özel bir ekip oluşturmayı ve bu ekibi editoryal ekipten izole etmeyi kapsıyor. Bu yöntem daha önce bir İngiliz common law hâkimi tarafından mahkemelerde kullanılmak üzere kabul edilebilir bulunmuştu.'

8.3 İngiltere Common Law ve Yemen Davası Emsal Kararı

Bellingcat'in Yemen çalışmasında geliştirdiği metodolojinin İngiliz common law çerçevesinde test edilmesi ve kabul görmesi, OSINT metodoloji standardizasyonu tarihinin dönüm noktalarından birini oluşturmaktadır. IWPR'ın (2023) aktarımına göre: 'Yemen davası bir köşe taşıydı. Açık kaynakları kullanma süreci daha önce başladı ve MH17 davasında yaygın biçimde

kullanıldı. AİHM duruşmasında iki paragraf yalnızca Bellingcat'e ayrılmış; bulgularımız, bizi amatör olarak değil, kendi değeri üzerinden değerlendiriyor.'

Bu karar, OSINT metodolojisinin kuralcı bir hukuk sisteminde dahi kabul görebileceğini; ancak bunun için sistemli dokümantasyon, editoryal bağımsızlık ve izole delil toplama sürecinin zorunlu olduğunu ortaya koymaktadır.

8.4 Ulusal Mahkemeler ve Sosyal Medya Delili

Ulusal mahkemelerde OSINT kökenli sosyal medya delili, farklı yargı çevrelerinde farklı kabul standartlarına tabi tutulmaktadır. Springer Nature'ın (2017) değerlendirmesine göre, İngiltere ve Galler'de 'duyuma dayalı delil' (hearsay) yasal istisnalar aracılığıyla geniş ölçüde kabul görmektedir ve OSINT materyalleri bu tanım kapsamına girebilmektedir. Fransız ceza hukukunda ise Ceza Usul Kanunu'nun 427. maddesi 'serbest delil' ilkesini benimsemekte; suçlar her türlü delil aracıyla ispatlanabilmektedir (OSINT FR, 2023).

Bununla birlikte OSINT FR'nin (2023) vurguladığı kritik ayrım şudur: 'OSINT faaliyeti kapsamında yasal hukuki dayanağa sahip ve hukuki ilkelere uygunluğu sağlayan koşullarda toplanan bilgi, davada delil olarak otomatik olarak kabul edilmez. Delil üretimi ile delilin kabul edilmesi arasındaki farka dikkat etmek gerekmektedir.'

9. Yapay Zeka Tehdidi: Deepfake, Dezenformasyon ve OSINT

9.1 Deepfake'in OSINT Metodolojisine Etkisi

Büyük dil modelleri ve görüntü üretim yapay zekasının olgunlaşması, OSINT analizinin karşılaştığı en yeni ve en tehlikeli tehdidi oluşturmaktadır. Gerçek görünen ama tamamen sentetik olan görüntü, video ve sesler üretilebilmesi, geleneksel görsel doğrulama tekniklerini potansiyel olarak geçersiz kılmaktadır: Coğrafi konum analizi, gerçek bir fotoğraf varsayımına dayanır; yapay zeka tarafından oluşturulmuş arka planlı bir görüntü için bu yaklaşım anlamsızlaşır. Gölge ve güneş analizi yalnızca gerçek ortam fotoğrafları için çalışır.

Medium'daki Ketcham'ın (2025) değerlendirmesine göre dijital delil otantikliği sorunu hukuk pratiklemesinde giderek daha kritik hale gelmektedir. Bu tehdidin karşı tarafça kasıtlı olarak kullanıldığı durumlar da belgelenmiştir: Rusya'nın Ukrayna davasında Bellingcat fotoğraflarına yönelik manipülasyon iddiaları, mahkemelerde deepfake enstrümanlaştırmasının bir örneğini oluşturmaktadır. AİHM bu itirazı reddetti; ancak böyle iddiaların artacağı öngörülmektedir.

9.2 Tespit ve Provenance Teknolojileri

Deepfake tehdidine yanıt olarak iki temel teknolojik yaklaşım gelişmektedir. C2PA (Coalition for Content Provenance and Authenticity) standardı, görüntü ve videoların üretim zincirini kriptografik olarak belgeleyen bir endüstri standardıdır. İçeriğin hangi cihazda, hangi yazılımla ve hangi zaman diliminde üretildiğini kriptografik olarak kaydeder; bu kayıt sonradan değiştirilemez niteliktedir.

InVID/WeVerify araç seti, video doğrulama için geliştirilmiş açık kaynaklı bir platformdur. Bellingcat'in araç kitinde de yer alan bu set; video karelerini ters görüntü aramasına sokma, metadata çıkarımı ve manipülasyon belirteçlerini analiz etme imkânı sunmaktadır. Amnesty International'ın Digital Verification Corps, bu araçları kullanarak ters görüntü arama, coğrafi konum ve gölge analizinde uzmanlaşmış gönüllü ekipleri eğitmektedir (Lexology, 2020).

9.3 Devlet Destekli Dezenformasyon ve Kirletme Stratejisi

OSINT'in adli değerini zedelemeye yönelik en sofistike strateji, çevrimiçi ortamı sahte ama inandırıcı içerikle doldurmaktır. Bu strateji üç amaçla kullanılabilmektedir: Gerçek OSINT bulgularının gürültü içinde kaybolmasını sağlamak; otantik delilin güvenilirliğini zedelemek için sahte alternatifler sunmak; araştırmacıları yanlış yönlere sevk etmek. Rusya'nın MH17 davasında izlediği bilgi stratejisi, pek çok akademisyen tarafından bu tür bir 'epistemic sabotaj' örneği olarak incelenmiştir.

Bu tehdidin OSINT metodolojisine yanıtı çok katmanlı doğrulama zorunluluğu ve şüpheci varsayımlardır: Tek bir kaynak, ne kadar güvenilir görünse görünsün, yeterli değildir. Kaynağın motivasyonu, kimlik doğrulaması ve bağımsız teyit Berkeley Protokolü'nün bu nedenle merkezi ilkelerine alınmıştır.

10. Adli OSINT Araçları ve Blockchain Doğrulama

10.1 Açık Kaynak Adli Araçların Mahkeme Kabul Edilebilirliği

PLOS ONE'da (2025) yayımlanan araştırma, açık kaynaklı adli araçların (Autopsy, ProDiscover Basic) ticari araçlarla (FTK, Forensic MagiCube) karşılaştırıldığında mahkeme kabul edilebilirliği açısından dört temel sorunla karşılaştığını ortaya koymuştur: Açık kaynak dijital adli araçların yetenek ve kullanılabilirliği, bu araçlarla üretilen dijital delilin güvenilirlik ve bütünlüğü, araçların şeffaflığı ve açık kaynaklı araçların kullanımını düzenleyen referans ve standartların eksikliği.

Araştırmanın temel bulgusu şudur: Kontrollü test ortamlarında açık kaynaklı araçlar, ticari muadilleriyle karşılaştırılabilir performans sergilemektedir. Bununla birlikte bu araçların mahkemede kabul görmesi için standartlaştırılmış doğrulama çerçevelerinin geliştirilmesi zorunludur. Bu standartların yokluğu, mahkemelerin açık kaynaklı araçlara ticari araçlara kıyasla daha şüpheci yaklaşmasına yol açmaktadır.

10.2 Blockchain Tabanlı OSINT Arşivleme

MDPI'de Future Internet dergisinde (2025) yayımlanan araştırma, OSINT kanıt bütünlüğünü sağlamak için blockchain tabanlı notarizasyon ve görüntü doğrulama mekanizmalarını mevcut adli iş akışlarıyla entegre eden beş aşamalı bir çerçeve önermektedir: Tanımlama, elde etme, kimlik doğrulama, koruma ve doğrulama. Blockchain tabanlı yaklaşımın hash tabanlı yöntemlere göre temel üstünlüğü, değişmezliğin merkezileşmemiş bir güven altyapısıyla

desteklenmesidir: Hash bir sunucuda değiştirilebilirken, blockchain kaydını değiştirmek teorik olarak imkânsızdır (MDPI, 2025).

11. Türk Hukuku Bağlamında OSINT

11.1 CMK 217 ve Dijital Delil Çerçevesi

Türk ceza muhakemesi hukukunda dijital delile ilişkin genel çerçeve CMK'nın 217. maddesiyle sağlanmaktadır: Mahkeme, hükmünü yalnızca duruşmada ortaya konmuş ve hukuka uygun biçimde elde edilmiş delillere dayandırabilir. İstanbul Avukat Firması'nın (tarihsiz) değerlendirmesine göre, 'Türk mahkemelerinde dijital içeriğin kabul edilebilirliği otomatik değildir — katı yasal uyumluluk gerektirmektedir; yasal elde etme, kimlik doğrulama ve zincir muhafaza bunların başında gelmektedir.'

Türk hukukunda CMK 134, bilgisayar sistemleri için arama ve elkoyma prosedürünü düzenlemektedir. OSINT özelinde kritik soru şudur: Kamuya açık bir kaynaktan derlenen bilgi, CMK anlamında hukuka uygun yollarla elde edilmiş sayılır mı? Açık kaynak verisi, niteliği gereği elde etme aşamasında özel bir yetkiye ihtiyaç gerektirmemektedir; bu durum CMK 134'ün arama ve elkoyma prosedürüne değil, doğrudan CMK 217'nin genel kabul standardına tabi olduğu anlamına gelmektedir. Ancak elde etme yöntemi hukuka uygun olsa bile delil değeri, özgünlük, bütünlük ve metodolojik güvenilirlik unsurlarına bağlıdır.

11.2 Türkiye'de Dijital Delil Pratiği

Türk mahkemelerinde OSINT kökenli sosyal medya paylaşımları yaygın biçimde delil olarak sunulmaktadır. İstanbul Avukat Firması'nın (tarihsiz) bildirdiğine göre, 'Türk avukatlar ses dosyalarının delil olarak sunulmasında sertifikalı transkript ve manipülasyon olmadığını doğrulayan uzman görüşü eşliğinde sunmaktadır.' OSINT delilinde bu ilke de geçerlidir: Sosyal medya içeriklerinin özgünlüğüne itiraz giderek artmakta ve mahkemeler dijital adli bilişim uzmanı bilirkişiden destek talep etmektedir.

KVKK (6698 sayılı Kanun) açısından ise kamuya açık sosyal medya verisi de kişisel veri statüsündedir. Bu veriyi toplamak ve analiz etmek, KVKK'nın amaçla sınırlılık ilkesi gereğince meşru bir zemine oturtulmalıdır. Adli soruşturma amacıyla OSINT yürüten kolluk birimlerinin bu yasal çerçeveyi gözetmesi zorunludur; bu zorunluluk, OSINT delilinin mahkemede itirazla karşılaşmaması için temel ön koşulu oluşturmaktadır.

11.3 Türkiye'de 5651 Kapsamındaki Gelişmeler

Türkiye'nin internet düzenleyici çerçevesini oluşturan 5651 sayılı Kanun'da 2022-2026 yılları arasında yapılan değişiklikler — özellikle dezenformasyon ve sosyal medya platform yükümlülüklerine ilişkin düzenlemeler — OSINT metodolojisi açısından önemli bir gerilim yaratmaktadır. İstanbul Avukat Firması'nın (2025) değerlendirmesine göre, 5651'in içerik engelleme mekanizması sayesinde Türkiye'de erişilemeyen sosyal medya içeriklerinin yurt dışı arşivlerden OSINT aracılığıyla elde edilmesi teorik olarak mümkündür; ancak bu içeriklerin mahkemede sunulması ayrı bir metodolojik dikkat gerektirmektedir.

12. Standartlar, Metodolojik Öneriler ve Etik

12.1 Araştırmacı Güvenliği

OSINT araştırmacılarının güvenliği, Berkeley Protokolü'nün merkezi ilkelerinden biridir. Devlet aktörlerini araştıran OSINT analistleri ciddi fiziksel tehlikelerle karşılaşabilmektedir; bazı ülkelerde tutuklama ve yargılanma vakaları belgelenmiştir. Dijital güvenlik açısından ise araştırmacılar, hedefleri tarafından tanınmama riski taşımaktadır: Bir sosyal medya hesabına erişim girişimi, hesap sahibini araştırıldığından haberdar edebilir; bu durum hem soruşturmanın seyrini hem de araştırmacının güvenliğini tehdit eder.

12.2 Etik Sınırlar: Mahremiyet ve Hukuki Uyum

OSINT araştırmacılarının karşılaştığı en temel etik gerilim, kamuya açık bilginin toplanması ile mahremiyet hakkının çatışmasıdır. AFCEA'nın (2023) aktardığı Koops'un uyarısı bu gerilimi somutlaştırmaktadır: 'Bilgi toplama sürecinin kendisi zarar vermese de son koleksiyonun kişiyi tanımlayan ayrıntılı bir profil sunması mümkündür; bu durum, verinin her bir unsurunun açık kaynaklardan gelmesine karşın gizlilik ihlali oluşturabilir.'

Özellikle Türkiye'de KVKK'nın 'veri minimizasyonu' ilkesi, OSINT çalışmalarının belirli bir soruşturma amacıyla sınırlı tutulmasını gerektirmektedir. İlgili kişinin kamuya açık hesabından yapılan sistematik ve kapsamlı veri kazımanın (data scraping) hukuki sınırları tartışmalı olmaya devam etmektedir. SSC Legacy'nin (2022) vurgusu bu bağlamda önemlidir: 'Polis, dördüncü değişiklik kapsamındaki anayasal korumalar ve yurt dışındaki GDPR gibi veri koruma çerçeveleri kapsamında kısıtlamalarla karşı karşıya kalmaktadır.'

12.3 Kapsamlı Metodolojik Öneriler

OSINT delilinin hukuki süreçlerde kabul edilebilirliğini güçlendirmek için

- **İçerik arşivleme protokolü:** Tüm kaynak içerikler, mümkün olan en kısa sürede hash değeri hesaplanarak arşivlenmelidir. Hunchly gibi adli amaçlı araçlar tercih edilmelidir.
- **Çok kaynaklı doğrulama:** Her kritik bulgu, bağımsız kaynaklardan en az iki kez teyit edilmeli; tek kaynak bulmalar savunulamaz düzeyde kırılgandır.
- **Kör doğrulama:** Analistlerin birbirlerinden haberdar olmadan bağımsız çalışması, metodolojik bütünlüğü önemli ölçüde güçlendirir.
- **Metodoloji şeffaflığı:** Kullanılan araçlar, teknikler, belirsizlik payı ve alternatif açıklamalar raporlanmalıdır. Sonuçlar olasılıksal dille sunulmalı, kesin iddialardan kaçınılmalıdır.
- **Uzman bilirkişi eşliği:** Mahkeme süreçlerinde OSINT bulgularının sunulması, Daubert/CMK 63-67 standardını karşılayan bilirkişi aracılığıyla yapılmalıdır.
- **Deepfake risk değerlendirmesi:** Her görsel delil için InVID/WeVerify veya benzeri araçlarla sentez içerik taraması yapılmalı; belirsizlik raporlanmalıdır.

- **Araştırmacı güvenlik protokolü:** Özellikle devlet aktörlerini içeren soruşturmalarda sock puppet hesap kullanımı, erişim kayıtlarının gizlenmesi ve güvenli iletişim kanalları standart prosedür olmalıdır.

Tablo 2. *Berkeley Protokolü Öncesi ve Sonrası OSINT Uygulamalarının Karşılaştırması*

Boyut	Protokol Öncesi (pre-2022)	Protokol Sonrası (post-2022)
Metodoloji standardı	Araştırmacıya ve kuruluşa göre değişen	6 aşamalı döngü; OHCHR onaylı çerçeve
Kriptografik bütünlük	Seçmeli uygulamalar (Mnemonic istisnası)	Hash+arşivleme zorunluluk olarak önerildi
Güvenlik çerçevesi	Araştırmacı takdirine bırakılmış	Sistematik dijital ve fiziksel güvenlik ilkeleri
Yargısal kabul	Vaka bazlı; tutarsız	Protokol uyumu, kabul olasılığını artırıyor
Etik çerçeve	Kuruluş politikalarına bağlı	5 temel ilke; mahremiyet ve orantılılık dahil
Kurumsal meşruiyet	Tartışmalı; 'amatörler' algısı	AİHM, UCM ve ulusal mahkemeler tarafından tanınma

Not. Kaynak: Opinio Juris (2025); OHCHR (2022); IWPR (2023); Bellingcat (2023) temel alınarak derlenmiştir.

13. Sonuç

Açık kaynak istihbaratı, 1941'deki radyo dinleme operasyonlarından 2024'teki Okhmadit hastane saldırısının füze kimliğinin tespitine uzanan seksen yıllık bir dönüşüm geçirmiştir. Bu dönüşümün son on yılı özellikle çarpıcıdır: Sosyal medyanın veri bolluğu, uydu görüntüsünün ticari erişilebilirliği ve Maltego, Shodan, Wayback Machine gibi güçlü analiz araçlarının yaygınlaşması, OSINT'i bir araştırma yöntemi olmaktan çıkarıp bağımsız bir bilim dalının sınırlarına taşımıştır.

Bununla birlikte OSINT'in adli delil olarak kullanımı henüz olgunlaşma sürecini tamamlamamıştır. Berkeley Protokolü, bu sürecin dönüm noktasını simgelemektedir: OSINT soruşturmacılığını metodolojik açıdan savunulabilir bir disipline dönüştürme yolunda atılan ilk sistematik adım. MH17 davasında Bellingcat'in bulgularının JIT tarafından doğrulanması ve AİHM'de Bellingcat delilinin tartışmaya açılması, bu dönüşümün ne kadar hızlı gerçekleştiğini somutlaştırmaktadır.

Yapay zeka ve deepfake teknolojisinin yükselişi, OSINT'in güvenilirliğine yönelik şimdiye kadarki en sofistike tehdidi oluşturmaktadır. Bu tehdidin üstesinden gelmek için C2PA provenance standardizasyonu, InVID/WeVerify gibi doğrulama araçları ve kriptografik bütünlük mekanizmalarının yaygınlaştırılması zorunludur. Teknik önlemlerin yanı sıra metodolojik şeffaflık ve çok katmanlı doğrulama kültürü de bu alandaki standart gereklilikler olmalıdır.

Türkiye bağlamında ise OSINT metodolojisinin hukuk pratiğine entegrasyonu henüz emekleme aşamasındadır. CMK 217'nin genel dijital delil standardı, OSINT'e özgü

gereklilikleri karşılamak için yeterli olmayabilir. Açık kaynak verilerinin nasıl elde edildiğinin, doğrulandığının ve raporlandığının standartlaştırılması; adli bilişim uzmanlarının ve yargı mensuplarının bu alanda eğitilmesi; KVKK çerçevesinin OSINT kullanım örnekleriyle açıklığa kavuşturulması, Türk hukukunun dijital çağa uyum sürecinin kritik gündem maddeleri arasında yer almaktadır.

Sonuç olarak, OSINT 'adli delil olabilir mi?' sorusunun yanıtı şudur: Evet, olabilir — ancak bu yalnızca doğru metodoloji, kriptografik bütünlük, metodolojik şeffaflık ve uzman bilirkişi desteğiyle mümkündür. Bu dört koşulun sağlanmadığı OSINT delili, hukuki süreçlerde zarar verecek düzeyde kırılgandır; doğruluk iddiaları ne kadar güçlü olursa olsun. Berkeley Protokolü'nün çizdiği çerçeve, bu dört koşulun en iyi nasıl sağlanacağını gösteren en kapsamlı kılavuzu bugün için sunmaktadır.

Kaynakça

AFCEA International. (2023, September 1). The rise of OSINT: Few rules, many opportunities. Signal Media. https://www.afcea.org/signal-media/intelligence/rise-osint-few-rules-many-opportunities

Bellingcat. (2023a). Geolocation guide: How to geolocate images. https://www.bellingcat.com/resources/how-tos/geolocation

Bellingcat. (2023b, March 28). How open source evidence was upheld in a human rights court. https://www.bellingcat.com/resources/2023/03/28/how-open-source-evidence-was-upheld-in-a-human-rights-court/

Dirisu, D. M. (2025, April 28). Institutionalization: A way forward to prove the role of open-source intelligence to the courts. Opinio Juris. https://opiniojuris.org/2025/04/28/institutionalization-a-way-forward-to-prove-the-role-of-open-source-intelligence-to-the-courts/

Fortuna, A. (2025, November 5). Setting standards for digital investigations in the age of open source intelligence. https://andreafortuna.org/2025/11/05/setting-standards-for-digital-investigations-in-the-age-of-open-source-intelligence

Grozev, C. (2022, March 16). Open source investigation and the documentation of war crimes in Ukraine [Congressional testimony]. House Foreign Affairs Subcommittee on Europe, Energy, the Environment and Cyber. https://docs.house.gov/meetings/FA/FA14/20220316/114520/HHRG-117-FA14-Wstate-GrozevC-20220316.pdf

InCyber News. (2024, February 11). OSINT in the judicial process: A growing phenomenon. https://incyber.org/en/article/osint-in-the-judicial-process-a-growing-phenomenon/

Institute for War and Peace Reporting (IWPR). (2023). Integrating OSINT into justice processes. https://iwpr.net/global-voices/integrating-osint-justice-processes

Istanbul Lawyer Firm. (tarihsiz). How digital evidence works in Turkey. https://istanbullawyerfirm.com/blog/digital-evidence-admissibility-turkey

Istanbul Lawyer Firm. (2025). Understanding the 2025 amendments to Turkey's internet law. https://istanbullawyerfirm.com/blog/turkey-internet-law-changes-2025

Ismail, A., Ariffin, K. A. Z., Abdullah, M. T., Rauf, M. A., Mohd Zin, N. A., & Murad, M. A. A. (2025). The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. PLOS ONE, 20(9), e0331683. https://doi.org/10.1371/journal.pone.0331683

Ketcham, T. (2025, December 17). OSINT in the legal industry: More suits, less trenchcoats. Medium. https://medium.com/@tom.ketcham/osint-in-the-legal-industry-22608ca48f26

Leiden Journal of International Law / Cambridge Core. (2023). Closing cases with open-source: Facilitating the use of user-generated open-source evidence in international criminal investigations. https://doi.org/10.1017/S092215652300023 7

Lexology. (2020, December 22). The Berkeley Protocol on Open Source Investigations. https://www.lexology.com/library/detail.aspx?g=88065c49-c099-4bee-835f-e15e183587ec

MDPI / Future Internet. (2025). A blockchain-based framework for OSINT evidence collection and identification. Future Internet, 17(12), Article 551. https://www.mdpi.com/1999-5903/17/12/551

OHCHR / UC Berkeley Human Rights Center. (2022). Berkeley Protocol on Digital Open Source Investigations. United Nations Human Rights Office of the High Commissioner. https://www.ohchr.org/en/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source-investigations

OSINT Byle. (2025, June 4). Top 15 OSINT tools in 2025. Medium. https://osintbyle.medium.com/top-15-osint-tools-in-2025-leading-platforms-osint-investigations-platforms-2771871b7bb6

OSINT FR Community. (2023, May 4). OSINT: What admissibility of the information collected in litigation? https://osintfr.com/en/osint-what-admissibility-of-the-information-collected-in-litigation-4-4/

RESET.ORG. (2024, February 2). The Berkeley Protocol is setting international standards for digital open source investigations. https://en.reset.org/the-berkeley-protocol-is-setting-international-standards-for-digital-open-source-investigations/

Reuters Institute for the Study of Journalism. (2023, February 21). How Bellingcat collects, verifies and archives digital evidence of war crimes in Ukraine. https://reutersinstitute.politics.ox.ac.uk/news/how-bellingcat-collects-verifies-and-archives-digital-evidence-war-crimes-ukraine

Royal United Services Institute (RUSI). (2024). Puzzling pieces: OSINT and war crime accountability in Ukraine. https://www.rusi.org/explore-our-research/publications/commentary/puzzling-pieces-osint-and-war-crime-accountability-ukraine

SIDN. (2022, April 1). Bellingcat uses open-source information to expose wrongdoing. https://www.sidn.nl/en/news-and-blogs/bellingcat-uses-open-source-information-to-expose-wrongdoing

Springer Nature. (2017). Following the breadcrumbs: Using open source intelligence as evidence in criminal proceedings. In A. Staniforth & P. Griffiths (Eds.), Routledge companion to UK counter-terrorism (pp. 213-228). https://link.springer.com/chapter/10.1007/978-3-319-47671-1_18

SSC Legacy. (2022). Open Source Intelligence (OSINT) and the law. https://ssclegacy.com/2017/11/15/open-source-intelligence-osint-and-the-law/

Web Asha Technologies. (2026). Real-world applications of OSINT: Exploring successes and failures. https://www.webasha.com/blog/real-world-applications-of-osint-exploring-successes-and-failures

Wikipedia. (2026). Open-source intelligence. https://en.wikipedia.org/wiki/Open-source_intelligence

burakolgun.com