
# SOCMINT

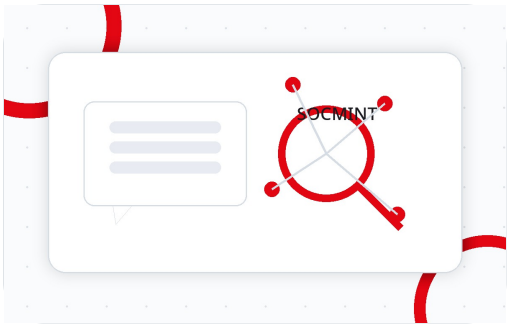
Sosyal Medya İstihbaratı İçin Sade Rehber

Savunma, doğrulama, gazetecilik, güvenlik farkındalığı ve eğitim amacıyla hazırlanmıştır.

# SOCMINT nedir?

SOCMINT, sosyal medyada açıkça görülebilen ya da yetkiyle erişilen verilerin belirli bir araştırma sorusu için toplanması, karşılaştırılması ve doğrulanmasıdır.

Amaç birini izlemek değildir. Amaç, sosyal medyadaki sinyali bağlamına oturtmak ve neyin kanıt, neyin sadece iddia olduğunu ayırmaktır.




## Ana fikirler

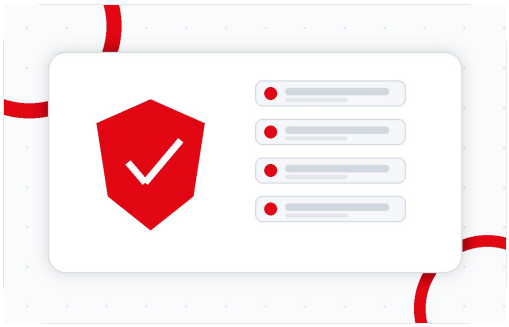
- Yanlış bilgi kontrolü, olay doğrulama, tehdit farkındalığı ve gazetecilikte kullanılır.
- Tek bir gönderi yerine kaynak, zaman, bağlam ve tutarlılık birlikte değerlendirilir.
- Açık profil, sınırsız kullanım izni anlamına gelmez. Kişisel veri sınırı her zaman akılda tutulur.

**Basit örnek**
Bir olay videosu paylaşıldığında videonun yeni mi eski mi olduğunu, nerede çekildiğini ve güvenilir kaynaklarla uyuşup uyuşmadığını kontrol etmek SOCMINT çalışmasıdır.

**Dikkat**
Bu kitapçık taciz, doxxing, yasa dışı takip veya kişisel hedef gösterme için yöntem anlatmaz. Odak savunma, doğrulama ve eğitimdir.

# SOCMINT neden önemlidir?

Sosyal medya kriz anlarında çok hızlı sinyal üretir. Aynı hız, yanlış bilgi ve panik de üretir. SOCMINT bu kalabalığın içinden doğrulanabilir bilgiyi ayırmaya yardım eder.



## Ana fikirler

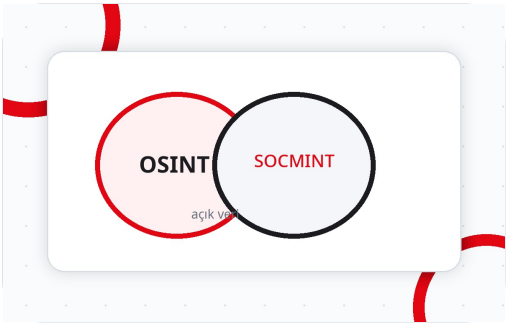
- Gerçek olay ile söylentiyi ayırır.
- Sahte kampanya, taklit hesap ve manipülasyon sinyallerini erken fark ettirir.
- Kurumlara, gazetecilere ve güvenlik ekiplerine bağlam sağlar.
- Yanlış yönlendirme riskini azaltır; acele karar vermeyi engeller.

**Basit örnek**
Bir depremden sonra aynı yardım çağrısı farklı şehir adlarıyla dolaşıyorsa kaynak, zaman ve konum kontrolü yanlış yönlendirmeyi azaltır.

**Dikkat**
En büyük hata tek gönderiye güvenmektir. İyi pratik, iddiayı en az iki bağımsız ve güvenilir kaynakla kontrol etmektir.

# OSINT ile SOCMINT farkı

OSINT, açık kaynaklardan bilgi toplama ve analiz etme yaklaşımıdır. SOCMINT ise bu alanın sosyal medya odaklı bölümüdür. Fark sadece kaynakta değil, verinin doğasındadır.




## Ana fikirler

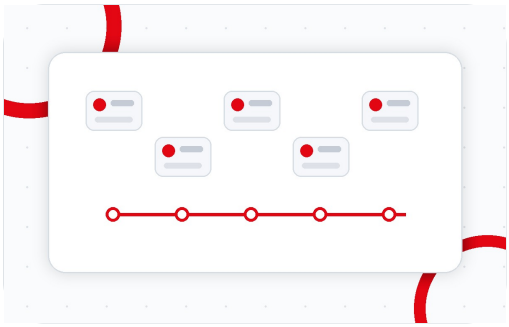
- OSINT daha geniştir: web siteleri, resmi kayıtlar, haberler, haritalar, arşivler ve teknik altyapı verileri buna dahildir.
- SOCMINT daha hızlı, daha kişisel ve daha manipülasyona açık sosyal medya verileriyle çalışır.
- Sosyal medya verisinde bağlam kaybı çok yaygındır; ekran görüntüsü tek başına yeterli değildir.

**Basit örnek**
Bir şirketin alan adını ve resmi sicil kaydını incelemek OSINT olur. Aynı şirket adına açılmış sahte sosyal medya hesabını incelemek SOCMINT alanına girer.

**Dikkat**
SOCMINT, OSINT içinde görülse de mahremiyet etkisi daha yüksektir. Bu yüzden daha sıkı etik süzgeç gerekir.

# Sosyal medya verileri nelerdir?

Bir sosyal medya paylaşımı sadece metinden ibaret değildir. Profil bilgisi, zaman, etkileşim, görsel, bağlantı ve ağ yapısı birlikte değerlendirildiğinde anlam kazanır.



## Ana fikirler

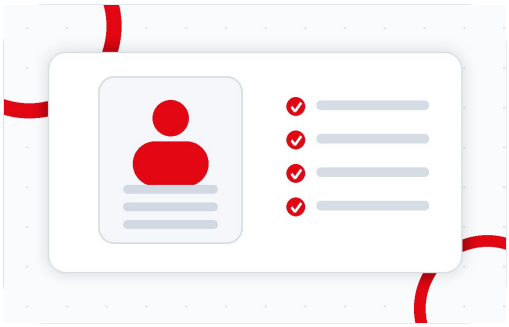
- Profil verileri: kullanıcı adı, biyografi, bağlantılar, hesap yaşı ve herkese açık açıklamalar.
- İçerik verileri: metin, görsel, video, canlı yayın, yorum ve alıntılar.
- Etkileşim verileri: beğeni, paylaşım, yanıt, etiket, mention ve hashtag davranışı.
- Zaman ve bağlam: paylaşım saati, ilk görülme zamanı, silinme veya düzenlenme izleri.

**Basit örnek**
Bir paylaşımın saati, cevap aldığı hesaplar ve aynı iddianın daha önce nerede çıktığı metnin kendisi kadar önemli olabilir.

**Dikkat**
Metadata bazen silinir veya hiç görünmez. Yokluğu, olayın olmadığı anlamına gelmez; sadece o verinin doğrulanamadığını gösterir.

# Profil analizi

Profil analizi, hesabın kendini nasıl sunduğunu ve bu sunumun diğer kanıtlarla uyuşup uyuşmadığını anlamaya çalışır. Burada amaç kişiyi teşhir etmek değil, iddianın güvenilirliğini ölçmektir.



## Ana fikirler

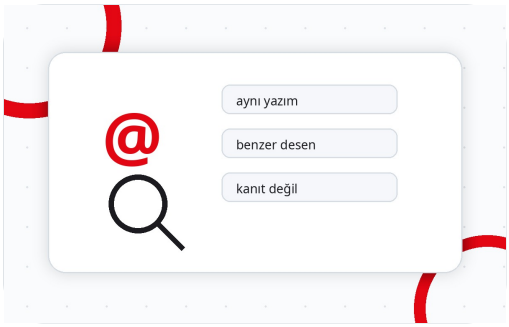
- Kullanıcı adı, biyografi, profil görseli ve bağlantılar birbiriyle tutarlı mı?
- Paylaşım dili, konu alanı ve aktivite ritmi hesabın iddiasını destekliyor mu?
- Hesap resmi kurum veya marka olduğunu söylüyorsa resmi web sitesinden bağlantı var mı?
- Tek başına profil fotoğrafı veya biyografi kanıt sayılmaz.

**Basit örnek**
Kendisini belediye destek hesabı gibi gösteren bir profil, belediyenin resmi web sitesinden veya doğrulanmış hesabından linklenmiyorsa temkinli yaklaşılır.

**Dikkat**
Aile, okul, ev adresi, özel ilişki veya hassas kişisel bilgi peşine düşmek araştırma değil, zarar verici davranıştır.

# Kullanıcı adı araştırması

Kullanıcı adları bazen farklı platformlarda tekrar kullanılır. Bu, özellikle taklit hesap, marka suistimali veya kamuya açık bir iddianın kaynağını anlamak için yararlı olabilir.




## Ana fikirler

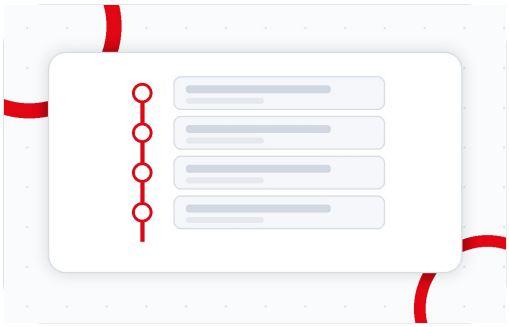
- Önce tam yazımı ve açık görünen varyasyonları kontrol et.
- Aynı kullanıcı adı farklı yerde görünüyorsa bunu kesin kimlik eşleşmesi değil, bağlantı sinyali olarak yaz.
- E-posta, şifre sıfırlama sayfası veya özel veri tabanı gibi yöntemlere başvurma.
- Araştırma sorusuyla ilgisi olmayan hesapları toplamaya çalışma.

**Basit örnek**
Bir yardım kampanyası hesabının eski paylaşımlarında farklı şehir ve farklı marka adları geçiyorsa, bu taklit veya dolandırıcılık sinyali olabilir.

**Dikkat**
Doğru ifade şudur: "Aynı kullanıcı adı şu platformlarda görülüyor; bağlantı ihtimali var." Yanlış ifade: "Kesin aynı kişi."

# Paylaşım geçmişi analizi

Tek bir ekran görüntüsü, sosyal medya akışının küçük bir parçasıdır. Paylaşım geçmişi analizi, iddianın nerede başladığını, nasıl yayıldığını ve bağlamının değişip değişmediğini anlamaya çalışır.



## Ana fikirler

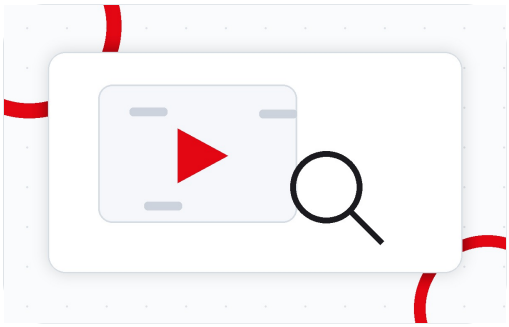
- İlk paylaşımı, tekrar paylaşan hesapları ve iddianın metin değişimlerini ayır.
- Silinen, düzenlenen veya yeniden yüklenen içeriklerde zaman kaydını ayrıca not et.
- Eski içerik yeniymiş gibi sunuluyor mu kontrol et.
- Alıntı ve kesilmiş ekran görüntülerine karşı orijinal bağlantıyı ara.

**Basit örnek**
Bir video önce mizah sayfasında paylaşılmış, sonra "son dakika" başlığıyla dolaşıma sokulmuşsa ikinci bağlam yanıltıcı olabilir.

**Dikkat**
Eski paylaşımları bugünkü bağlamla yargılamak hata üretir. Tarih, ortam ve o günkü olay akışı not edilmelidir.

# Görsel ve video analizi

Görseller sosyal medyada en hızlı yayılan ama en kolay bağlamından koparılan içeriklerdir. Eski, kırpılmış, aynalanmış, başka olaydan alınmış veya yapay olarak üretilmiş olabilirler.



## Ana fikirler

- Tersine görsel arama ve eski arşiv kayıtlarıyla ilk kullanım izini ara.
- Videoda tek kareye değil; tabela, ses, kıyafet, hava, araç ve çevre detaylarına bak.
- Frame çıkarma, aynı videonun farklı yüklemelerini karşılaştırmayı kolaylaştırır.
- Sonucu kesin değilse "eşleşmedi", "kısmen uyuyor" veya "doğrulanamadı" diye yaz.

**Basit örnek**
Kar görüntüsüyle paylaşılan trafik videosunda yol tabelaları başka ülkeye aitse, olay yeri iddiası zayıflar.

**Dikkat**
Özel kişileri yüz tanıma veya benzeri yöntemlerle teşhis etmeye çalışmak ciddi mahremiyet riski doğurur.

# Konum ipuçları

Konum analizi, kamu yararı taşıyan bir olayın nerede yaşandığını doğrulamak için yapılır. Amaç özel adres bulmak değildir. Bu farkı net tutmak gerekir.

## Ana fikirler

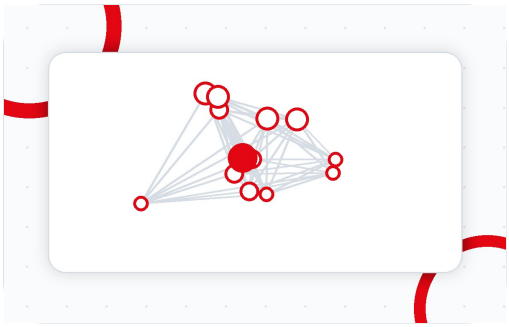
- Tabela, yol çizgisi, bina cephesi, arazi yapısı, bitki örtüsü ve dil ipuçları değerlendirilebilir.
- Hava durumu, gölge yönü ve toplu taşıma gibi açık kaynaklar bağlamı güçlendirebilir.
- Her ipucu tek başına zayıftır; birkaç bağımsız işaret aynı noktayı gösterdiğinde güven artar.
- Emin olunmayan yerde "olası konum" ifadesi kullanılmalıdır.

**Basit örnek**
Bir miting görüntüsündeki meydan heykeli, tramvay hattı ve mağaza tabelası şehir iddiasını kontrol etmek için yeterli ipucu verebilir.

**Dikkat**
Ev, okul, iş yeri veya düzenli rota gibi hassas konumlar paylaşılmamalı; raporda gerekiyorsa bulanıklaştırılmalıdır.

# Ağ ve bağlantı analizi

Sosyal medya ağları, bilginin kimlerden kimlere aktığını göstermeye yardım eder. Fakat takip, beğeni veya etiket her zaman gerçek hayattaki ilişki anlamına gelmez.



## Ana fikirler

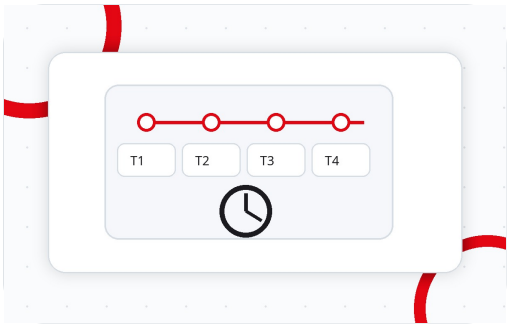
- Mention, yeniden paylaşım, ortak hashtag, aynı bağlantı ve yorum zincirleri akış yönü hakkında sinyal verir.
- Ağ grafiği karar değil, karar vermeye yardımcı araçtır.
- Çok merkezi görünen hesaplar kaynak, toplayıcı, bot ya da sadece popüler kullanıcı olabilir.
- Sonuç yazarken ilişki türünü abartmamak gerekir.

**Basit örnek**
Aynı bağlantıyı 30 hesap birkaç dakika içinde paylaşıyorsa koordinasyon sinyali doğar. Yine de "bot ağı" demeden önce içerik ve hesap davranışı kontrol edilir.

**Dikkat**
Kapalı grupları izinsiz kazımak, kimlik gizleyerek içeri girmek veya kişileri hedef göstermek etik sınırın dışındadır.

# Zaman çizelgesi çıkarma

Zaman çizelgesi, dağınık gönderileri kronolojik kanıta dönüştürür. Özellikle krizlerde "önce ne oldu, sonra ne yayıldı" sorusuna sakin cevap verir.




## Ana fikirler

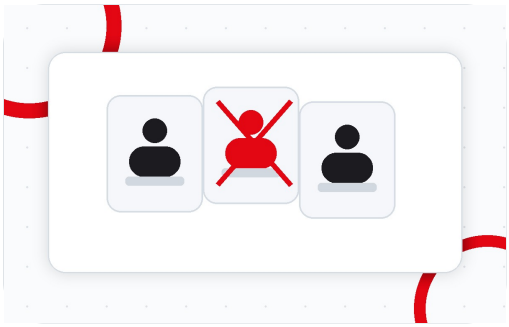
- Her kayıt için kaynak, URL, platform, saat, zaman dilimi, içerik özeti ve güven düzeyi yaz.
- Yerel saat ile UTC karışıklığı çok yaygındır; ikisini mümkünse ayrı göster.
- İlk görülen paylaşım ile olayın gerçekten yaşandığı zaman aynı şey olmayabilir.
- Zaman boşlukları da bulgudur; raporda eksik alan olarak belirtilir.

**Basit örnek**
İddia 21:10'da çıktı, ilk görsel 21:19'da geldi, resmi açıklama 22:05'te yapıldı. Bu akış, söylenti penceresini gösterir.

**Dikkat**
Platform saatleri, ekran görüntüsünü alan kişinin cihaz saatinden farklı olabilir. Saat bilgisini kaynakla birlikte kaydet.

# Sahte hesapları anlama

Sahte hesap tespiti dikkatli yapılmalıdır. Takma ad kullanmak tek başına kötü niyet göstergesi değildir. Bazı insanlar güvenlik veya mahremiyet için gerçek ad kullanmaz.



## Ana fikirler

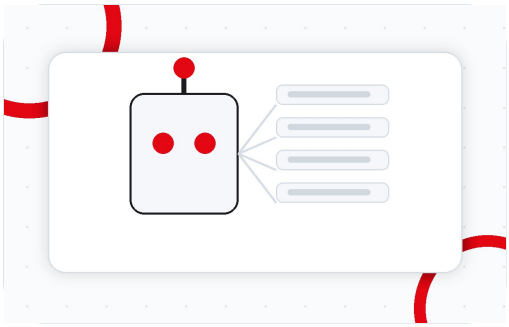
- Yeni açılmış hesap, çalıntı görsel, tutarsız dil ve ani konu değişimi sinyal olabilir.
- Aynı metni kopyalayan hesaplar veya gerçek dışı profil bilgileri ayrıca kontrol edilir.
- Resmi kurum taklidi varsa resmi site, doğrulanmış hesap ve platform güvenlik sayfalarıyla karşılaştırılır.
- Kesin kanıt yoksa "şüpheli" veya "doğrulanamadı" denir.

**Basit örnek**
Dün açılmış bir bağış hesabı resmi logo kullanıyor ama kurum sitesinde geçmiyorsa, kamuya açık şekilde raporlanmadan önce platforma ve kuruma doğrulatılmalıdır.

**Dikkat**
Bir hesabı halka açık biçimde "sahte" diye etiketlemek zarar doğurabilir. Bulgular, kanıt diliyle ve temkinli yazılmalıdır.

# Bot ve koordineli davranışlar

Bot, otomasyonla çalışan hesap demektir. Koordineli davranış ise birden fazla hesabın birlikte hareket etmesidir. İkisi aynı şey değildir ama bazen birlikte görülür.



## Ana fikirler

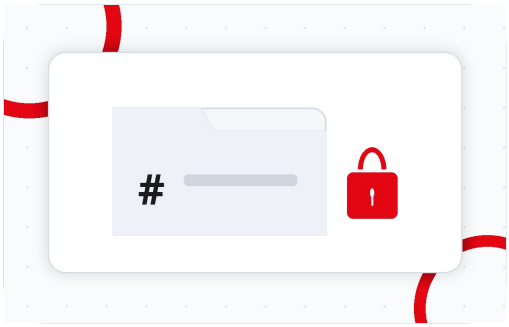
- Aynı metnin tekrar edilmesi, eş zamanlı paylaşım ve aynı kısa bağlantıların kullanılması sinyal sayılabilir.
- 24 saat kesintisiz aktivite, konuşma eksikliği ve aşırı hashtag kullanımı ayrıca incelenir.
- Platform dışından kesin bot kararı vermek zordur; insan incelemesi gerekir.
- Analizde "otomasyon sinyali" ve "koordinasyon sinyali" ayrı tutulmalıdır.

**Basit örnek**
Bir hashtag birkaç dakika içinde çok sayıda hesap tarafından aynı cümleyle paylaşılıyorsa bu koordinasyon sinyalidir; tek başına bot kanıtı değildir.

**Dikkat**
Sık paylaşım yapan gerçek bir kişiye "bot" demek hatalı ve zarar verici olabilir. Kanıt seviyesini açık yaz.

# Kanıt toplama yöntemleri

İyi SOCMINT çalışması tekrar edilebilir olmalıdır. Başka bir araştırmacı, senin hangi veriye bakarak hangi sonuca vardığını anlayabilmelidir.




## Ana fikirler

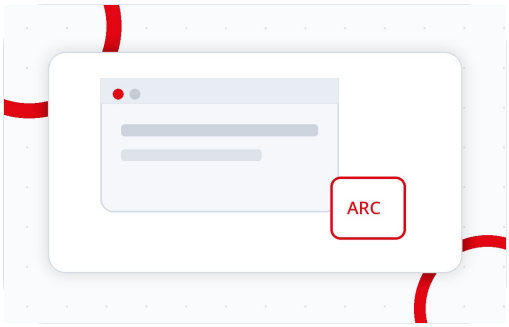
- URL, platform, kullanıcı adı, paylaşım tarihi, erişim tarihi ve kısa bağlam notu kaydedilir.
- Ekran görüntüsü, arşiv bağlantısı ve mümkünse orijinal medya dosyası ayrı saklanır.
- Ham kopya ile çalışma kopyası karıştırılmaz. Dosya adı anlaşılır olmalıdır.
- Gerekmediği halde fazla kişisel veri toplanmaz.

**Basit örnek**
Sadece bir gönderi rapor için yeterliyse tüm profilin ekran görüntüsünü almak yerine ilgili gönderiyi, URL'yi ve bağlamı kaydetmek daha doğrudur.

**Dikkat**
Kanıt toplama, veri yığmak değildir. Toplanan her veri için "buna neden ihtiyacım var?" sorusu sorulmalıdır.

# Ekran görüntüsü ve arşivleme

Ekran görüntüsü pratik bir kayıt yöntemidir ama tek başına zayıf kalabilir. URL, zaman kaydı ve arşiv bağlantısı ile birlikte kullanıldığında daha güvenilir olur.




## Ana fikirler

- Ekranda URL, tarih, saat ve içerik bağlamı mümkün olduğunca görünür olmalıdır.
- Görüntü kırpıldıysa raporda belirtilir; orijinal kopya korunur.
- Wayback Machine veya benzeri arşiv araçları, silinme riskine karşı referans sağlayabilir.
- Hassas bilgi içeren görüntüler paylaşılmadan önce maskeleme yapılmalıdır.

**Basit örnek**
Silinen bir paylaşım sadece kırpılmış görselle değil, arşivlenmiş URL ve yakalama zamanı ile birlikte raporlanırsa daha sağlam durur.

**Dikkat**
Arşiv araçları her içeriği yakalayamaz. Giriş gerektiren, dinamik veya silinmiş içeriklerde eksik kayıt oluşabilir.

# Raporlama nasıl yapılır?

Raporun görevi aracı göstermek değil, sonucu anlaşılır kılmaktır. Okuyan kişi neyin kanıt, neyin yorum, neyin belirsiz olduğunu hızlıca görmelidir.


## Ana fikirler

- Kısa özet, kapsam, doğrulanmış bulgular, sinyaller, değerlendirme, eksikler ve ekler ayrı yazılır.
- [Fact], [Inference] ve [Unverified] etiketleri karmaşayı azaltır.
- Güven düzeyi düşük, orta veya yüksek olarak verilir; nedenini bir cümleyle açıkla.
- Kanıt tablosunda URL, tarih, kaynak ve not alanı bulunur.

**Basit örnek**
[Fact] Video A hesabında 20:14'te göründü. [Inference] Konum büyük olasılıkla X meydanı. [Unverified] Yükleyicinin kimliği doğrulanmadı.

**Dikkat**
Rapor, kesinlik hissi vermek için değil, karar verene doğru belirsizlik seviyesini göstermek için yazılır.

# Etik sınırlar

SOCMINT güçlü bir yöntemdir. Güçlü olduğu için de sınırı net olmalıdır. Her kamuya açık veri, her amaç için kullanılabilir veri değildir.

## Ana fikirler

- Amaç belirli olmalı: neyi doğruluyorum, neden doğruluyorum?
- Orantılılık şarttır: daha az veriyle cevap verilebiliyorsa fazlası toplanmaz.
- Çocuklar, mağdurlar, sağlık, inanç, siyasi görüş ve özel hayat konularında daha yüksek dikkat gerekir.
- Yanıltma, baskı, hedef gösterme ve kitle tacizi araştırma yöntemi değildir.

**Basit örnek**
Bir söylentiyi doğrulamak için resmi hesapları ve kamuya açık olay kayıtlarını kontrol etmek yeterliyse, adı geçen kişinin özel çevresini haritalamaya gerek yoktur.

**Dikkat**
Kendine şu soruyu sor: Bu toplama işlemi daha sonra denetlense savunulabilir mi? Cevap zayıfsa dur.

# Hukuki dikkat noktaları

Bu bölüm hukuki danışmanlık değildir. Yasa, ülkeye ve çalışma bağlamına göre değişir. Yine de SOCMINT çalışmasında kişisel veri ve platform kuralları her zaman dikkate alınmalıdır.

## Ana fikirler

- GDPR ve KVKK benzeri düzenlemeler, sosyal medyadaki kişisel veriler için de önemli olabilir.
- Kamuya açık veri, otomatik olarak serbestçe işlenebilir veri anlamına gelmez.
- Platform şartları, API kullanımı, arşivleme ve otomatik toplama için sınır koyabilir.
- Erişim kontrolünü aşmak, sahte kimlikle kapalı alana girmek veya hassas veri toplamak yüksek risklidir.

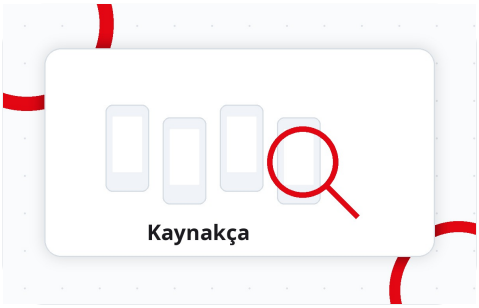
**Basit örnek**
Bir şirket marka taklidi yapan herkese açık hesapları belgeleyebilir; ancak amaç, saklama süresi ve kanıta kimlerin erişeceği önceden belirlenmelidir.

**Dikkat**
Yüksek riskli dosyalarda hukuk ekibi, veri koruma sorumlusu veya kurum politikasına danışmadan geniş veri toplama yapılmamalıdır.

# Sonuç ve kaynakça

SOCMINT, sosyal medyada iz sürmekten ibaret değildir. Değerli tarafı, dağınık sinyalleri sakin şekilde doğrulamak ve gereksiz kişisel veri toplamadan anlamlı bir sonuca varmaktır.

Üç kuralı unutma: iki kez doğrula, sadece gerekli veriyi topla, emin olmadığın yerde belirsizliği açıkça yaz.




## Kaynaklar ve ileri okuma

**Bellingcat Online Investigation Toolkit**
https://bellingcat.gitbook.io/toolkit

**OSINT Framework**
https://osintframework.com/

**Verification Handbook**
https://verificationhandbook.com/

**Verification Handbook 3 - DataJournalism.com**
https://datajournalism.com/read/handbook/verification-3

**First Draft News - resources and verification**
https://firstdraftnews.org/resources/

**European Commission - Data protection in the EU**
https://commission.europa.eu/law/law-topic/data-protection_en

**GDPR legal text - EUR-Lex**
https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

**KVKK - Kişisel Verileri Koruma Kurumu rehberleri**
https://www.kvkk.gov.tr/Icerik/2030/rehberler

**Privacy International - Social Media Intelligence explainer**
https://privacyinternational.org/explainer/55/social-media-intelligence

**Internet Archive - Save pages in the Wayback Machine**
https://help.archive.org/help/save-pages-in-the-wayback-machine/

**Meta Transparency Center**
https://transparency.meta.com/

**TikTok Community Guidelines**
https://support.tiktok.com/en/safety-hc/account-and-user-safety/community-guidelines

**X Transparency Center**
https://transparency.x.com/en

**YouTube Community Guidelines enforcement**
https://transparencyreport.google.com/youtube-policy

**Omand, Bartlett & Miller, Introducing SOCMINT, 2012**
https://www.tandfonline.com/doi/abs/10.1080/02684527.2012.716965

Not: Bu kitapçık hukuki danışmanlık değildir. Yüksek riskli dosyalarda kurum politikası ve yerel mevzuat ayrıca kontrol edilmelidir.