UÇTAN UCA ŞİFRELİ MESAJLAŞMANIN ADLİ DELİL DEĞERİ

WhatsApp, Signal ve Telegram Kayıtlarının Teknik ve Hukuki Analizi

Forensic Evidentiary Value of End-to-End Encrypted Messaging: A Technical and Legal Analysis of WhatsApp, Signal and Telegram Records

Derleme Makale / Review Article

Dr. Burak Olgun

burakolgun@solutionhome.net

Solution Home Bilişim Tekn. ve Dan. Hizm., İstanbul

Uçtan Uca Şifreleme • Adli Bilişim • Delil Bütünlüğü • Hukuka Aykırı Delil • Uç Nokta İncelemesi • Bulut Yedeği • CMK m. 134

ÖZET

Uçtan uca şifreleme (End-to-End Encryption — E2EE), günümüz mesajlaşma uygulamalarının standardı hâline gelmiş ve iletişim mahremiyetini güçlendirirken, geleneksel iletişimin denetlenmesi (interception) yöntemlerini büyük ölçüde işlevsiz bırakmıştır. Bu durum, adli bilişim açısından bir paradigma değişimi yaratmıştır: Delil artık iletişim kanalından değil, iletişimin uç noktalarından (endpoint) -- yani cihazlardan ve bulut yedeklerinden -- elde edilmek zorundadır. Bu makale, WhatsApp, Signal ve Telegram kayıtlarının adli delil olarak değerini üç boyutta incelemektedir: (i) uçtan uca şifrelemenin teknik temelleri ve içerik ile meta veri ayrımı; (ii) mesajlaşma verisinin uç nokta incelemesi, bulut yedekleri ve adli araçlarla elde edilme yöntemleri ile bu verinin güvenilirliği ve bütünlüğü; (iii) elde edilen delilin Türk hukuku ve uluslararası içtihat karşısındaki hukuki konumu. EncroChat ve Sky ECC gibi şifreli ağların çökertilmesiyle elde edilen delillerin kabul edilebilirliğine ilişkin güncel Avrupa Birliği Adalet Divanı ve ulusal mahkeme kararları değerlendirilmekte; ekran görüntülerinin manipülasyon riski tartışılmaktadır. Türkiye bağlamında, Ceza Muhakemesi Kanunu'nun 134 ve 135. maddeleri, hukuka aykırı delil yasağı ve Yargıtay'ın güncel içtihadı çerçevesinde, şifreli mesaj kayıtlarının hangi koşullarda hukuka uygun delil sayılacağı ortaya konmaktadır. Çalışma, şifreli mesaj delilinin ancak hukuka uygun biçimde elde edildiğinde, teknik bütünlüğü doğrulandığında ve delil zinciri korunduğunda mahkeme önünde güvenilir olacağını savunmaktadır.

Anahtar Kelimeler: *uçtan uca şifreleme, adli bilişim, mesajlaşma uygulamaları, delil bütünlüğü, hukuka aykırı delil, uç nokta incelemesi, bulut yedeği, ekran görüntüsü, CMK m. 134, EncroChat.*

ABSTRACT

End-to-end encryption (E2EE) has become the standard in contemporary messaging applications and, while strengthening communication privacy, has largely rendered traditional interception methods ineffective. This has produced a paradigm shift for digital forensics: evidence must now be obtained not from the communication channel but from its endpoints -- that is, from devices and cloud backups. This article examines the evidentiary value of WhatsApp, Signal and Telegram records along three axes: (i) the technical foundations of

burakolgun.com

end-to-end encryption and the distinction between content and metadata; (ii) the methods of acquiring messaging data through endpoint examination, cloud backups and forensic tools, together with the reliability and integrity of such data; and (iii) the legal standing of the resulting evidence under Turkish law and international case law. Recent judgments of the Court of Justice of the European Union and national courts on the admissibility of evidence obtained by dismantling encrypted networks such as EncroChat and Sky ECC are assessed, and the manipulation risk of screenshots is discussed. In the Turkish context, the conditions under which encrypted message records may be deemed lawful evidence are set out within the framework of Articles 134 and 135 of the Code of Criminal Procedure, the prohibition of unlawfully obtained evidence and the recent case law of the Court of Cassation. The study argues that encrypted message evidence is reliable before a court only when it is lawfully obtained, its technical integrity is verified and the chain of custody is preserved.

Keywords: *end-to-end encryption, digital forensics, messaging applications, evidence integrity, unlawfully obtained evidence, endpoint examination, cloud backup, screenshot, chain of custody, EncroChat.*

burakolgun.com

1. Giriş

İletişim teknolojisinin son on yıllık gelişimi, mahremiyet ile denetim arasındaki dengeyi kökten değiştirmiştir. Bir zamanlar telefon görüşmeleri ve kısa mesajlar, operatör altyapısında merkezî olarak akar ve yasal bir kararla dinlenebilirdi. Bugün ise milyarlarca insan, WhatsApp, Signal ve Telegram gibi uygulamalar üzerinden, içeriği uçtan uca şifrelenmiş mesajlarla haberleşmektedir. Uçtan uca şifreleme (End-to-End Encryption — E2EE), bir mesajın yalnızca gönderen ve alıcının cihazlarında okunabilir olmasını; arada yer alan uygulama sunucusu da dâhil hiçbir tarafın içeriği çözememesini sağlar. Bu tasarım, iletişim mahremiyeti açısından güçlü bir kazanım; ancak suç soruşturması açısından köklü bir meydan okumadır.

Bu meydan okumanın adli bilişime yansıması nettir: Klasik iletişimin denetlenmesi (iletişimin tespiti, dinlenmesi) yöntemi, E2EE karşısında büyük ölçüde işlevsizleşmiştir. İletişim kanalının ortasından geçen trafik şifreli olduğundan, delil artık kanaldan değil, iletişimin **uç noktalarından** elde edilmek zorundadır. Bir başka deyişle, mesaj içeriğine ulaşmanın yolu, genellikle mesajı gönderen veya alan cihazın kendisinden, ya da bu cihazların verilerini yedeklediği bulut hesaplarından geçer. Bu kayma, hem teknik yöntemleri hem de hukuki çerçeveyi yeniden tanımlamaktadır: Cihaza el koyma, cihazda arama ve bulut verisine erişim, artık soruşturmanın merkezine oturmuştur.

Mesajlaşma kayıtları, günümüzde ceza yargılamasından boşanma davalarına, ticari uyuşmazlıklardan iş hukuku ihtilaflarına kadar geniş bir yelpazede delil olarak sunulmaktadır. Ne var ki bu kayıtların delil değeri, iki temel soruya verilen yanıta bağlıdır. Birincisi **hukukilik**: Kayıt, hukuka uygun bir yöntemle mi elde edilmiştir? Türk hukukunda hukuka aykırı biçimde elde edilen delil, mutlak bir yasak kapsamında hükme esas alınamaz. İkincisi **güvenilirlik/bütünlük**: Kayıt gerçek ve değiştirilmemiş midir? Özellikle ekran görüntüleri, kolayca sahtelenebildiğinden, tek başına zayıf bir delil niteliği taşır. Bu iki eksen, makalenin çözümleme çerçevesini oluşturmaktadır.

Konu, salt teknik bir mesele değildir; hukuki ve etik boyutları da vardır. Şifreli ağların toplu olarak çökertilmesiyle elde edilen delillerin -- EncroChat ve Sky ECC örneklerinde olduğu gibi -- kabul edilebilirliği, Avrupa'da yoğun bir yargısal tartışmanın konusudur. Bu tartışma, mahremiyet hakkı, adil yargılanma hakkı ve etkin suç soruşturması arasındaki gerilimi çıplak biçimde ortaya koymaktadır. Türkiye'de ise Yargıtay, cihazdan elde edilen mesaj kayıtlarının hukuka uygunluğu konusunda giderek daha titiz bir içtihat geliştirmektedir.

Makalenin geri kalanı şu şekilde düzenlenmiştir. İkinci bölüm uçtan uca şifrelemenin teknik temellerini açıklar. Üçüncü bölüm WhatsApp, Signal ve Telegram'ı karşılaştırır. Dördüncü bölüm mesaj verisinin adli yöntemlerle elde edilmesini; beşinci bölüm şifreli ağların toplu çökertilmesini inceler. Altıncı bölüm ekran görüntüsü ve manipülasyon riskini; yedinci bölüm delil bütünlüğünü ele alır. Sekizinci bölüm hukuki çerçeveyi, dokuzuncu bölüm Türkiye bağlamını, onuncu bölüm bilirkişilik önerilerini kapsar. On birinci bölüm sonucu sunar. Çalışma boyunca herhangi bir gerçek dosyaya veya kişiye atıf yapılmamış; yalnızca teknik ve hukuki farkındalık amaçlanmıştır.

burakolgun.com

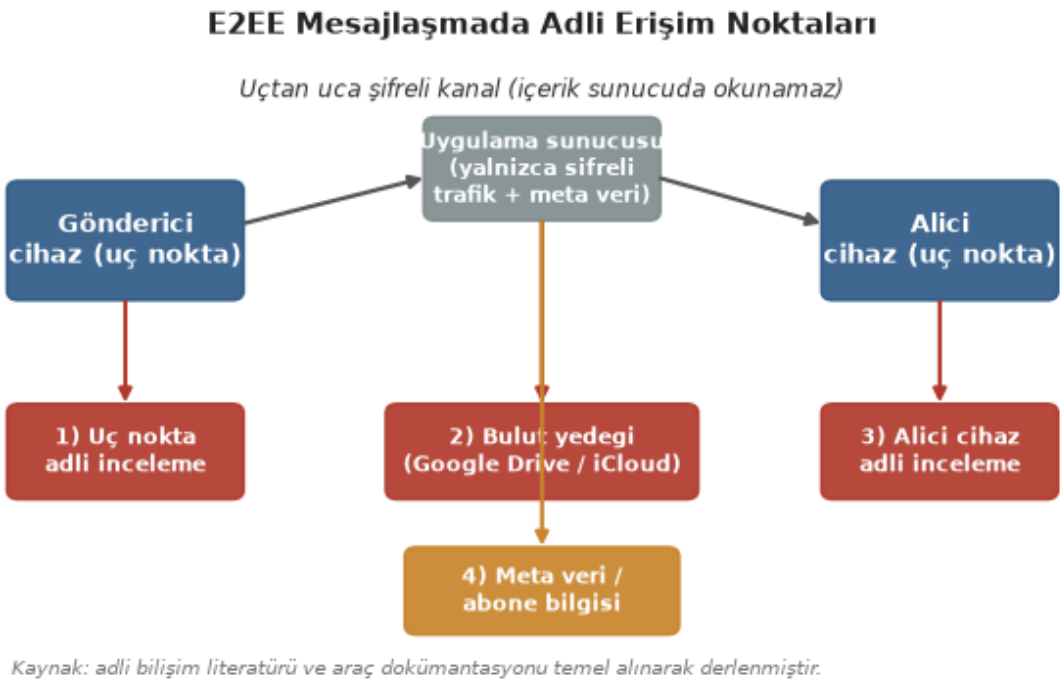
2. Uçtan Uca Şifrelemenin Teknik Temelleri

Şifreli mesaj delilinin adli değerini anlamak için, önce şifrelemenin nasıl çalıştığını ve hangi noktalarda veriye erişilebilir kaldığını kavramak gerekir. Bu bölüm, uçtan uca şifrelemenin temel mekanizmasını, modern protokol tasarımını ve içerik ile meta veri arasındaki kritik ayrımı ele almaktadır.

2.1. Şifreleme, Anahtar Değişimi ve Uç Nokta Kavramı

Şifreleme, bir mesajı yalnızca doğru anahtara sahip tarafın okuyabileceği bir biçime dönüştürme işlemidir. Modern mesajlaşmada iki tür şifreleme bir arada kullanılır. **Simetrik şifreleme**, aynı anahtarla hem şifreleme hem çözme yapar ve hızlıdır; ancak tarafların bu ortak anahtarı güvenli biçimde paylaşması sorununu doğurur. **Asimetrik şifreleme** (açık anahtar kriptografisi) ise her tarafa bir açık (public) ve bir gizli (private) anahtar çifti verir; açık anahtarla şifrelenen mesaj yalnızca ilgili gizli anahtarla çözülebilir. Uygulamalar, anahtar değişimi için asimetrik yöntemleri, mesaj içeriğinin şifrelenmesi için ise simetrik yöntemleri birlikte kullanır.

Uçtan uca şifrelemenin ayırt edici özelliği, şifreleme ve çözme işlemlerinin yalnızca kullanıcıların cihazlarında -- yani **uç noktalarda** (endpoint) -- gerçekleşmesidir. Mesaj, gönderenin cihazında şifrelenir, ağ üzerinden şifreli olarak taşınır ve yalnızca alıcının cihazında çözülür. Uygulama sunucusu, mesajı yalnızca şifreli hâliyle görür ve içeriğini çözemez. Bu tasarımın adli sonucu tayin edicidir: İçerik, ağ ortasında ele geçirilemez; içeriğe ulaşmanın yolu, mesajın çözülmüş hâlde bulunduğu tek yerden, yani uç noktadaki cihazdan (veya o cihazın yedeğinden) geçer. Şekil 1, bu akışı ve adli erişimin mümkün olduğu noktaları göstermektedir.



Şekil 1. E2EE Mesajlaşmada Adli Erişim Noktaları (2025)

2.2. Signal Protokolü ve İleri Gizlilik

Günümüz E2EE mesajlaşmasının teknik omurgasını, açık kaynaklı **Signal Protokolü** oluşturur. Bu protokol yalnızca Signal uygulamasında değil, WhatsApp ve başka platformlarda da mesaj şifrelemesi için kullanılmaktadır. Protokolün en önemli özelliği, **çift mandal** (Double Ratchet) algoritmasıyla her mesaj için ayrı bir şifreleme anahtarı üretmesidir. Bu sayede iki güçlü güvenlik niteliği sağlanır: **İleri gizlilik** (forward secrecy), geçmiş anahtarların ele geçirilmesinin geçmiş mesajları açığa çıkarmamasını; **gelecek gizliliği** (future secrecy veya post-compromise security), bir anahtarın sızmasının gelecekteki mesajları korumaya devam etmesini ifade eder.

Bu tasarımın adli açıdan önemi büyüktür. Her mesajın ayrı anahtarla şifrelenmesi ve bu anahtarların sürekli yenilenmesi, bir noktada ele geçirilen tek bir anahtarla tüm yazışmanın çözülmesini olanaksız kılar. Dolayısıyla iletişimin ortadan pasif biçimde dinlenerek çözülmesi, modern protokoller karşısında pratikte mümkün değildir. Bu gerçek, adli stratejinin neden kaçınılmaz olarak uç noktaya -- çözülmüş verinin bulunduğu cihaza ya da yedeğe -- yöneldiğini açıklar. Şifreleme ne kadar güçlüyse, delilin ağırlık merkezi o kadar cihazın kendisine kayar.

2.3. İçerik ve Meta Veri Ayrımı

Uçtan uca şifreleme, mesajın **içeriğini** korur; ancak iletişime ilişkin **meta veriyi** aynı ölçüde gizlemez. Meta veri, 'ne konuşulduğu' değil, 'kimin kiminle, ne zaman, ne sıklıkla, hangi süreyle' iletişim kurduğu bilgisidir. Kim kime mesaj gönderdi, hangi saatte, hangi IP adresinden bağlandı, hesap hangi telefon numarasına kayıtlı -- bu bilgiler içerik olmasa da soruşturma açısından son derece değerlidir. Nitekim iletişim ağı analizi, çoğu zaman içeriğe hiç ulaşmadan, yalnızca meta veriden anlamlı ilişki haritaları çıkarabilir.

Uygulamalar, topladıkları meta veri miktarı bakımından belirgin biçimde farklılaşır. Bazı uygulamalar asgari meta veri tutmayı bir gizlilik ilkesi olarak benimserken, bazıları iletişim ağına, cihaz bilgisine ve kullanım örüntülerine dair daha geniş veri tutar. Adli açıdan bu ayrım kritiktir: İçeriğe erişilemese bile, servis sağlayıcıdan hukuki yolla temin edilebilecek meta veri veya abone bilgisi, tek başına bir delil değeri taşıyabilir. Bu nedenle bir soruşturmada yalnızca 'mesaj içeriği elde edilebilir mi?' değil, 'hangi meta veri hangi hukuki araçla temin edilebilir?' sorusu da sorulmalıdır.

2.4. İletişimin Denetlenmesinin Sınırları

Klasik iletişimin denetlenmesi (lawful interception), operatör altyapısında akan trafiğin yasal bir kararla dinlenmesine dayanır. Bu yöntem, sabit ve mobil telefon görüşmeleri ile şifresiz kısa mesajlar için hâlâ işlevseldir; ancak uçtan uca şifreli mesajlaşma karşısında büyük ölçüde etkisiz kalır. Bir operatör ya da uygulama sunucusu, iki uç nokta arasında akan şifreli trafiği kaydetse dahi, içeriği çözebilecek anahtara sahip değildir. Sonuç olarak, yasal dinleme kararı elde edilmiş olsa bile, şifreli içerik pratikte okunamaz; ele geçirilen yalnızca anlamsız bir şifreli veri akışıdır.

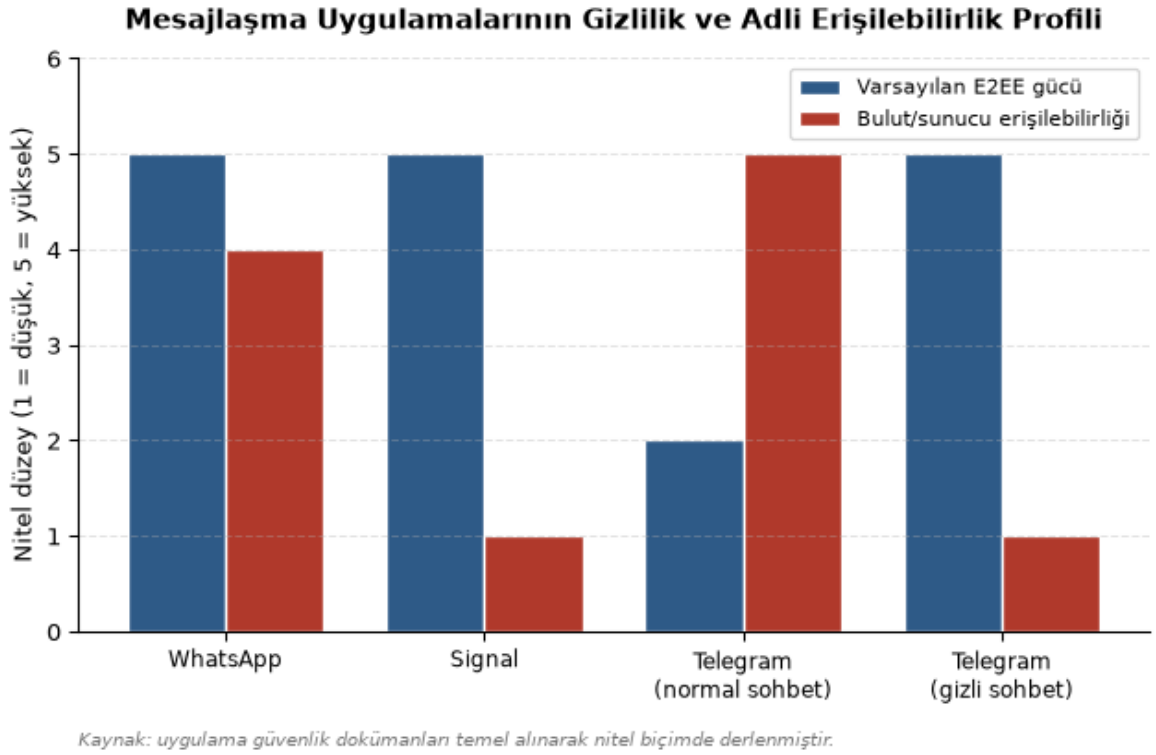
Bu teknik gerçek, adli ve hukuki stratejiyi doğrudan biçimlendirir. İçeriğe ulaşmak için iletişimin denetlenmesi (CMK m. 135) yerine, cihazda arama ve el koyma (CMK m. 134)

burakolgun.com

yolu öne çıkar; çünkü içerik yalnızca uç noktada çözülmüş hâlde bulunur. Bu kayma, yalnızca teknik bir tercih değil, aynı zamanda farklı usul güvencelerinin devreye girmesi anlamına gelir. Dolayısıyla soruşturma makamı, hedeflenen delilin niteliğine göre doğru hukuki aracı -- denetleme mi, arama-el koyma mı -- baştan belirlemek durumundadır. Yanlış aracın seçilmesi, hem sonuçsuz kalır hem de elde edilen delili hukuka aykırı kılabilir.

3. Uygulamaların Karşılaştırmalı Analizi

WhatsApp, Signal ve Telegram, teknik tasarımları ve gizlilik yaklaşımları bakımından önemli farklılıklar gösterir; bu farklar, her birinin adli erişilebilirliğini doğrudan etkiler. Şekil 2 ve Tablo 1, bu karşılaştırmayı özetlemektedir.



Şekil 2. Mesajlaşma Uygulamalarının Gizlilik ve Adli Erişilebilirlik Profili (2025)

3.1. WhatsApp

Dünyanın en yaygın mesajlaşma uygulaması olan WhatsApp, mesaj içeriğini varsayılan olarak Signal Protokolü ile uçtan uca şifreler. Adli açıdan WhatsApp'ın en kritik özelliği, **bulut yedekleme** davranışıdır. Kullanıcılar, sohbet geçmişlerini Android'de Google Drive'a, iOS'ta iCloud'a yedekleyebilir. Tarihsel olarak bu yedekler, cihaz üzerindeki yazışmanın aksine ek bir uçtan uca koruma olmadan tutuluyordu; bu da yedeklerin, ilgili bulut hesabına hukuki erişimle çözülebilmesine olanak tanıyordu. WhatsApp sonradan yedekler için isteğe bağlı uçtan uca şifreleme seçeneği eklemiş olsa da, birçok kullanıcı bu seçeneği etkinleştirmediğinden, bulut yedeği adli açıdan hâlâ önemli bir kaynak olmaya devam etmektedir.

Cihaz üzerinde WhatsApp verisi, şifreli bir veri tabanında saklanır; ancak bu veri tabanının çözüm anahtarı da genellikle cihazda bulunur. Bu nedenle kilidi açılmış (unlocked)

bir cihaza hukuka uygun biçimde erişildiğinde, adli araçlarla yazışmaların, medya dosyalarının ve kişi listelerinin elde edilmesi mümkündür. iOS ve Android yedekleri de -- parolası biliniyorsa -- WhatsApp mesaj veri tabanını içerebilir. Dolayısıyla WhatsApp, güçlü kanal şifrelemesine rağmen, uç nokta ve bulut katmanlarında adli açıdan erişilebilir bir uygulamadır.

3.2. Signal

Signal, gizliliği tasarımının merkezine koyan bir uygulamadır ve adli erişilebilirlik açısından en zorlayıcı olanıdır. Signal, asgari meta veri toplama ilkesini benimser; sunucu tarafında tutulan veri son derece sınırlıdır. Uygulama, cihaz üzerindeki veri tabanını güçlü biçimde şifreler ve varsayılan olarak bulut yedeklemesi sunmaz; bu da 'sunucuda veya bulutta veri arama' yaklaşımını büyük ölçüde işlevsiz bırakır. Bu nedenle Signal verisine erişim, neredeyse tümüyle uç noktadaki cihaza -- ve o cihazın kilidinin açılabilmesine -- bağlıdır.

Adli araçlar, kilidi açılmış bir cihazdan Signal veri tabanını çözüp ayrıştırabilir; ancak cihaz kilitliyse ve şifreleme anahtarları elde edilemiyorsa, Signal verisi pratikte erişilemez kalır. Bu durum, Signal'i gizlilik açısından güçlü, adli açıdan ise ancak fiziksel cihaz erişimi ve kilit açma koşulunda çözülebilir kılar. Signal örneği, modern gizlilik tasarımının adli erişimi cihaz kilidine indirgediğini açıkça göstermektedir.

3.3. Telegram

Telegram, diğer iki uygulamadan önemli bir yapısal farkla ayrılır: **Uçtan uca şifreleme, Telegram'da varsayılan değildir.** Standart 'bulut sohbetleri' (cloud chats), Telegram'ın sunucularında saklanır ve istemci-sunucu şifrelemesiyle korunur; ancak içerik, teknik olarak sunucu tarafında erişilebilir durumdadır. Uçtan uca şifreleme yalnızca kullanıcının özel olarak başlattığı 'gizli sohbetler' (secret chats) için geçerlidir ve bu sohbetler yalnızca ilgili cihazlarda saklanır. Bu tasarım, adli açıdan çift yönlü bir tablo yaratır.

Bir yandan, Telegram'ın bulut sohbetleri sunucuda tutulduğundan, teorik olarak servis sağlayıcıdan temin edilebilir nitelikte bir veri havuzu oluşturur; ancak bu, Telegram'ın hukuki taleplere yanıt politikasına ve ilgili yargı çevresine bağlıdır. Öte yandan, gizli sohbetler uçtan uca şifreli ve cihaza bağlı olduğundan, ancak uç nokta incelemesiyle elde edilebilir. Kullanıcıların çoğunun varsayılan bulut sohbetlerini kullanması, Telegram'ı -- gizli sohbetler dışında -- adli açıdan görece erişilebilir kılar. Bu ayrımın soruşturmada doğru anlaşılması, hangi verinin nereden elde edilebileceğinin belirlenmesi açısından hayatidir.

Tablo 1. WhatsApp, Signal ve Telegram'ın Adli Açıdan Karşılaştırması

Özellik	WhatsApp	Signal	Telegram
Varsayılan E2EE	Evet (tüm sohbetler)	Evet (tüm sohbetler)	Hayır (yalnızca gizli sohbet)
Bulut yedeği	Var (Drive/iCloud)	Yok (varsayılan)	Var (bulut sohbetleri sunucuda)
Sunucuda içerik	Hayır	Hayır	Evet (bulut sohbetleri)
Meta veri düzeyi	Orta	Asgari	Orta–yüksek
Adli erişim yolu	Cihaz + bulut yedeği	Yalnızca cihaz (kilit açık)	Cihaz + (bulut sohbetleri)

burakolgun.com

Not. Kaynak: uygulama güvenlik dokümanları ve adli bilişim literatürü temel alınarak derlenmiştir.

3.4. Grup Sohbetleri ve Çoklu Cihaz Sorunu

Üç uygulamanın ortak bir teknik zorluğu, grup sohbetleri ve çoklu cihaz (multi-device) desteğidir. Bir grup sohbetinde onlarca katılımcı bulunabilir; her katılımcının cihazı, yazışmanın bir kopyasını çözülmüş hâlde tutar. Bu, adli açıdan hem bir fırsat hem de bir karmaşıklık kaynağıdır: Bir katılımcının cihazından elde edilen kayıt, tüm grubun yazışmasını içerebilirken; aynı yazışmanın farklı cihazlardaki kopyalarının çapraz doğrulanması, özgünlük değerlendirmesini güçlendirir. Öte yandan, çoklu cihaz desteği, aynı hesabın birden çok cihazda -- telefon, tablet, masaüstü -- eşzamanlı çalışmasına olanak tanır; bu da delilin birden çok noktada bulunabileceği anlamına gelir.

Çoklu cihaz mimarisi, anahtar yönetimi açısından da önemlidir. Modern uygulamalar, her cihaz için ayrı şifreleme anahtarları yönetir ve yeni bir cihazın hesaba eklenmesi, genellikle diğer katılımcılarda bir güvenlik bildirimi doğurur. Adli açıdan bu bildirimler ve cihaz kayıtları, bir hesaba hangi cihazların ne zaman bağlandığını gösteren değerli izler sunabilir. Bilirkişi, yalnızca mesaj içeriğine değil, bu cihaz ve oturum üstverisine de dikkat etmeli; çünkü bu izler, çoğu zaman içerik kadar aydınlatıcı olabilir.

4. Mesajlaşma Verisinin Adli Yöntemlerle Elde Edilmesi

Şifreli mesaj verisine ulaşmanın yolları, verinin çözülmüş hâlde bulunduğu noktalara göre belirlenir. Bu bölüm, dört ana yaklaşımı ele almaktadır: uç nokta incelemesi, bulut yedekleri, adli araçlar ve kaybolan mesajların özel durumu.

4.1. Uç Nokta (Endpoint) İncelemesi

Uç nokta incelemesi, mesaj verisinin çözülmüş hâlde bulunduğu cihazın -- akıllı telefon, tablet veya bilgisayar -- adli olarak incelenmesidir. Bu, E2EE çağında en doğrudan ve en güvenilir delil kaynağıdır; çünkü mesaj, uç noktada zaten açık (çözülmüş) biçimde bulunmaktadır. İncelemenin başarısı büyük ölçüde iki koşula bağlıdır: cihaza fiziksel erişim ve cihaz kilidinin açılabilmesi. Kilidi açık bir cihazda, mesajlaşma uygulamalarının veri tabanları, medya klasörleri ve önbellekleri adli olarak çıkarılabilir. Kilitli bir cihazda ise, cihazın modeline, işletim sistemi sürümüne ve mevcut adli yöntemlere bağlı olarak erişim mümkün olabilir ya da olmayabilir.

Uç nokta incelemesinde adli ilkelerin titizlikle uygulanması şarttır. İnceleme, mümkün olduğunca cihazın durumunu değiştirmeden yapılmalı; elde edilen veri imajının kriptografik özeti (hash) alınmalı ve inceleme yeniden üretilebilir biçimde belgelenmelidir. Türk hukukunda bu tür bir inceleme, kural olarak Ceza Muhakemesi Kanunu'nun 134. maddesi kapsamındaki 'bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma' hükümlerine tabidir; usule aykırılık, elde edilen delilin hukuka aykırı sayılmasına yol açabilir.

4.2. Bulut Yedekleri

Cihaza doğrudan erişimin mümkün olmadığı durumlarda, bulut yedekleri kritik bir alternatif sunar. Kullanıcılar, mesajlaşma verilerini çoğu zaman bir bulut hesabına -- Google

burakolgun.com

hesabı ya da Apple iCloud -- yedekler. Bu yedekler, uygulamaya ve kullanıcı ayarlarına bağlı olarak, cihazdakine yakın bir yazışma geçmişi içerebilir. Bulut yedeğine erişim, ilgili bulut hizmet sağlayıcısına yöneltilecek hukuka uygun bir talebe veya kullanıcı kimlik bilgilerinin hukuka uygun biçimde elde edilmesine dayanır.

Bulut katmanı, uygulamalar arasındaki farkı en belirgin biçimde ortaya koyan alandır. WhatsApp yedekleri, özellikle isteğe bağlı yedek şifrelemesi etkinleştirilmemişse, adli açıdan zengin bir kaynaktır. Signal, varsayılan olarak bulut yedeklemesi sunmadığından, bu yol Signal için çoğu zaman kapalıdır. Telegram'ın bulut sohbetleri ise zaten sunucuda tutulduğundan, farklı bir hukuki dinamikle -- servis sağlayıcıdan temin -- gündeme gelir. Bu nedenle bir soruşturmanın başında, hedef uygulamanın bulut davranışının doğru anlaşılması, hangi hukuki aracın kullanılacağını belirler.

4.3. Adli Araçlar

Mesajlaşma verisinin cihazdan veya yedekten çıkarılması ve ayrıştırılması, özel adli bilişim araçlarıyla gerçekleştirilir. Sektörde yaygın olarak kullanılan araçlar arasında Cellebrite UFED, Oxygen Forensic Detective ve Magnet AXIOM sayılabilir. Bu araçlar, desteklenen cihazlardan veri çıkarma (extraction), şifreli veri tabanlarını çözme, yazışmaları ayrıştırma (parsing) ve raporlama işlevlerini bir arada sunar. Örneğin, kilidi açılmış bir cihazdan Signal veri tabanı çıkarılabilmekte; şifreleme anahtarları mevcutsa şifreli veri tabanları ayrıştırılabilmektedir. Tablo 2, bu araçların tipik yeteneklerini özetlemektedir.

Tablo 2. Başlıca Mobil Adli Bilişim Araçlarının Tipik Yetenekleri

Araç	Öne Çıkan Yetenek	Tipik Kullanım
Cellebrite UFED	Geniş cihaz desteği, veri çıkarma	Kolluk, adli laboratuvar
Oxygen Forensic Detective	Uygulama ayrıştırma, bulut erişimi	Adli inceleme, uygulama verisi
Magnet AXIOM	Bütünleşik analiz, zaman çizelgesi	Delil ilişkilendirme, raporlama

Not. Kaynak: araç kamuya açık dokümantasyonları temel alınarak derlenmiştir. Karşılaştırma tanıtım amacı taşımaz; yetenekler sürüm ve cihaza göre değişir.

Bu araçların gücü, aynı zamanda bir sorumluluk doğurur. Bir aracın 'mesajları çıkardı' demesi, o mesajların hukuka uygun elde edildiği ya da özgün olduğu anlamına gelmez. Bilirkişi, aracın hangi cihazdan, hangi yöntemle ve hangi anahtar materyaliyle veri çıkardığını belgelemeli; aracın ayrıştırma sürecindeki olası hata ve yorumları eleştirel biçimde değerlendirmelidir. Araç, uzmanın yerini almaz; uzmanın kullandığı bir yardımcıdır.

4.4. Kaybolan (Ephemeral) Mesajlar

Modern mesajlaşma uygulamaları, belirli bir süre sonra otomatik olarak silinen 'kaybolan mesaj' (disappearing/ephemeral message) özelliği sunar. Bu özellik, adli açıdan özel bir zorluk oluşturur; çünkü mesaj, tasarım gereği kalıcı olarak saklanmaz. Bir dönem, önde gelen adli araçlar bu tür mesajların kurtarılmasını resmî olarak desteklemiyordu; ancak zamanla, bazı senaryolarda kaybolan mesajların kurtarılmasına yönelik yetenekler geliştirilmiştir. Yine de kaybolan mesajlar, kalıcı mesajlara kıyasla çok daha kırılgan bir delil kaynağıdır ve bunların yokluğu, bir olayın gerçekleşmediği anlamına gelmez.

burak-ugur.com

Kaybolan mesajlar, delilin geçiciliği ve adli müdahalenin zamanlaması arasındaki ilişkiyi vurgular. Bir cihaza ne kadar erken ve ne kadar doğru yöntemle el konulursa, kaybolan içeriğin -- önbellek, bildirim kayıtları veya kısmi izler yoluyla -- kurtarılma olasılığı o kadar artar. Bu da adli hazırlığın ve hızlı müdahalenin önemini bir kez daha ortaya koyar.

4.5. Canlı ve Bulut Adli Bilişim

Geleneksel adli bilişim, cihazın kapatılıp bir kopyasının (imaj) alınması ve bu kopya üzerinde çalışılması ilkesine dayanır. Ancak şifreli mesajlaşma çağında, bu 'ölü kutu' (dead-box) yaklaşımı her zaman yeterli değildir. Cihaz kapatıldığında veya kilitlendiğinde, bellekte çözülmüş hâlde bulunan anahtarlar ve veriler kaybolabilir. Bu nedenle bazı durumlarda **canlı adli bilişim** (live forensics) -- cihaz çalışır ve kilidi açık durumdayken, bellekteki verinin usulüne uygun biçimde elde edilmesi -- kritik olabilir. Canlı inceleme, uçucu verinin (volatile data) yakalanmasına olanak tanır; ancak cihazın durumunu değiştirdiğinden, azami titizlik ve belgeleme gerektirir.

Bulut adli bilişimi ise, verinin cihazda değil, uzak sunucularda bulunduğu durumları kapsar. Bir kullanıcının bulut hesabına hukuka uygun erişim sağlandığında, mesaj yedekleri, medya dosyaları ve hesap etkinlik kayıtları elde edilebilir. Bulut adli bilişimi, cihaza fiziksel erişimin mümkün olmadığı durumlarda paha biçilmez bir yol açar; ancak sınır ötesi veri erişimi, farklı yargı çevrelerinin hukuki gerekliliklerine ve sağlayıcı politikalarına tabidir. Bu iki yaklaşım -- canlı ve bulut adli bilişim -- klasik cihaz imajı yöntemini tamamlayan, çağdaş bir delil elde etme repertuvarının parçalarıdır.

5. Ağ Üzerinden Toplu Müdahale: EncroChat, Sky ECC ve ANOM

Uç nokta odaklı yöntemlerin yanı sıra, kolluk kuvvetleri son yıllarda şifreli iletişim ağlarını toplu olarak hedef alan büyük ölçekli operasyonlar yürütmüştür. EncroChat, Sky ECC ve ANOM örnekleri, hem bu yaklaşımın gücünü hem de doğurduğu derin hukuki tartışmaları gözler önüne sermektedir.

EncroChat ve Sky ECC, organize suç çevrelerinde yaygın biçimde kullanılan, şifreli iletişime özelleşmiş kapalı platformlardı. 2020 ve 2021'de kolluk kuvvetleri, bu ağların altyapısına sızarak kullanıcıların mesajlarına -- şifreleme çözülmeden önce, uç noktada -- erişmeyi başardı ve milyonlarca mesaj toplandı. ANOM (Operation Trojan Shield) ise farklı bir mantıkla işledi: Kolluk, baştan itibaren kendi kontrolündeki bir şifreli mesajlaşma uygulamasını suç çevrelerine yayarak, iletişimi kaynağından izledi. Bu operasyonlar, çok sayıda tutuklama ve el koymayla sonuçlandı.

Ancak bu delillerin mahkemede kabul edilebilirliği, yoğun bir hukuki tartışmanın konusu olmuştur. Temel sorun, delilin elde ediliş yönteminin -- toplu, sınır ötesi ve savunmanın denetimine kapalı biçimde -- adil yargılanma hakkıyla bağdaşıp bağdaşmadığıdır. Avrupa Birliği Adalet Divanı (ABAD), 30 Nisan 2024 tarihli EncroChat kararında (C-670/22, M.N.), delilin kabul edilebilirliğinin ulusal hukukun meselesi olduğunu; ancak bu değerlendirmenin Avrupa Birliği Temel Haklar Şartı'nın adil yargılanma ve savunma haklarına ilişkin hükümleriyle uyumlu olması gerektiğini belirtmiştir (CJEU, 2024).

burakolgun.com

ABAD kararı sonrasında ulusal mahkemeler, birbirinden farklı sonuçlara ulaşmıştır. Bu farklılık, aynı delil türünün farklı hukuk düzenlerinde nasıl farklı değerlendirilebildiğini çarpıcı biçimde göstermektedir. Tablo 3, çeşitli Avrupa ülkelerindeki güncel kararların bir özetini sunmaktadır.

Tablo 3. EncroChat / Sky ECC Delillerine İlişkin Bazı Güncel Kararlar (2024–2025)

Yargı çevresi	Yaklaşım	Sonuç
ABAD (CJEU, C-670/22)	Kabul edilebilirlik ulusal hukukun meselesi	Adil yargılanma ile uyum şartı
Almanya (Berlin Eyalet M.)	Ulusal ve AB hukukuna aykırılık	Delilin dışlanması
Avusturya (OGH)	Ulusal dayanaksız sınır ötesi soruşturma	Kabul edilemez
İsviçre (Zürih Yüksek M.)	Önceden yetki alınmamış inceleme	Kabul edilemez
Birleşik Krallık	Ulusal usule uygunluk	Delil kabul edildi

Not. Kaynak: 2024–2025 tarihli mahkeme kararlarına ilişkin kamuya açık hukuki analizler temel alınarak derlenmiştir. Kararlar temyiz ve yeni içtihatla değişebilir.

Bu operasyonların bir diğer öğretici boyutu, delilin **denetlenebilirliği** sorunudur. EncroChat ve Sky ECC'de mesajlar, kolluğun teknik yöntemleriyle toplandığından, savunma tarafı çoğu zaman verinin nasıl elde edildiğini, ham hâlinin ne olduğunu ve toplama sırasında bütünlüğünün korunup korunmadığını bağımsız biçimde denetleyememiştir. Oysa adil yargılanmanın temel gereklerinden biri, aleyhe delilin savunma tarafından sınanabilmesidir. Bazı ulusal mahkemelerin delili dışlamasının ardında, tam da bu denetlenememe sorunu yatar: Delilin içeriği ne kadar güçlü olursa olsun, elde edilişi ve bütünlüğü savunmaca denetlenemiyorsa, mahkeme ona güvenle dayanamaz. Bu ilke, teknik yöntemin hukuki meşruiyetle dengelenmesi gerektiğini bir kez daha vurgular.

EncroChat ve Sky ECC deneyimi, adli bilişim ile hukukun kesiştiği noktadaki temel gerilimi özetler: Teknik olarak güçlü ve suçla mücadelede etkili bir delil elde etme yöntemi, hukuki meşruiyet süzgecinden geçmeden mahkeme önünde değer kazanamaz. Bir delilin 'elde edilebilmesi', onun 'kullanılabilir' olduğu anlamına gelmez. Bu ders, Türk hukuku bağlamında da doğrudan geçerlidir.

6. Ekran Görüntüsü ve Manipülasyon Riski

Uygulamada mesaj delili çoğu zaman en basit biçimiyle -- bir ekran görüntüsü (screenshot) olarak -- mahkemeye sunulur. Ekran görüntüsü pratik ve erişilebilir olsa da, delil güvenilirliği açısından en zayıf biçimdir. Nedeni açıktır: Bir ekran görüntüsü, özgün veriyle bağı kopmuş, bağlamından soyutlanmış statik bir imgedir ve günümüz araçlarıyla son derece kolay biçimde üretilebilir veya değiştirilebilir.

Manipülasyon riski çok yönlüdür. Bir yazışma, görüntü düzenleme yazılımlarıyla değiştirilebilir; sahte bir konuşma, gerçek bir arayüz taklit edilerek baştan üretilebilir; hatta gerçek bir mesajın tarih, saat veya taraf bilgisi çarpıtılabilir. Yapay zekâ destekli üretim araçlarının yaygınlaşması, bu riski daha da artırmıştır. Bu nedenle bir ekran görüntüsü, tek başına ve doğrulanmadan, güçlü bir delil olarak kabul edilmemelidir. Ekran görüntüsünün

burakolgun.com

değeri, ancak onu üreten özgün kaynağa -- cihazdaki veri tabanına, sunucu ya da bulut kaydına -- bağlanabildiğinde ortaya çıkar.

Bu nedenle adli iyi uygulama, mümkün olduğunca ekran görüntüsüyle yetinmemeyi; bunun yerine verinin özgün kaynağından, adli yöntemle ve bütünlüğü doğrulanabilir biçimde elde edilmesini gerektirir. Bir mesajın özgünlüğü, yalnızca görsel içeriğiyle değil; kaynağındaki üstveriyle (oluşturma zamanı, gönderen/alıcı tanımlayıcıları, veri tabanı yapısı) ve bu üstverinin iç tutarlılığıyla değerlendirilmelidir. Ekran görüntüsü, olsa olsa bir başlangıç işareti; asıl delil, onu doğrulayan özgün kayıttır.

Yapay zekâ destekli üretim araçlarının olgunlaşması, ekran görüntüsü delilinin güvenilirliğini daha da tartışmalı hâle getirmiştir. Bugün, gerçekçi görünen sahte bir yazışma arayüzü üretmek, birkaç dakikalık bir iştir; hatta var olan bir yazışmanın belirli mesajlarını değiştirmek, iz bırakmadan yapılabilir. Bu gelişme, 'gördüğüme inanırım' anlayışının adli bağlamda artık geçerli olmadığını göstermektedir. Bir ekran görüntüsünün gerçek görünmesi, onun gerçek olduğunu kanıtlamaz; tam tersine, görsel inandırıcılık günümüzde en kolay üretilen niteliktir. Bu nedenle özgünlük, görsel izlenimle değil, ancak özgün kaynağın ve üstverinin teknik incelemesiyle tespit edilebilir.

Bu tablo, adli bilişim uzmanının rolünü daha da merkezî kılmaktadır. Manipülasyonun giderek kolaylaştığı bir ortamda, bir mesajın gerçekliğini yalnızca içeriğine bakarak değil; kaynağındaki veri tabanı yapısını, üstverinin iç tutarlılığını ve varsa çapraz kaynakları inceleyerek değerlendirebilecek uzmanlık, delilin güvenilirliğinin son güvencesidir. Mahkemelerin, doğrulanmamış ekran görüntülerine dayanma eğiliminden uzaklaşıp, özgün kaynağa dayalı adli incelemeyi standart hâline getirmesi, adil yargılanma açısından giderek daha büyük önem taşımaktadır.

6.1. Bir Ekran Görüntüsünü Değerlendirme Adımları

Mahkemeye yalnızca ekran görüntüsü sunulduğunda, bilirkişinin izlemesi gereken bir değerlendirme sırası vardır. Aşağıdaki adımlar, ekran görüntüsünün güvenilirliğini ölçmek için asgari bir çerçeve sunar:

- **Kaynağı sorgula:** Görüntü hangi cihazdan, hangi uygulamadan alındı; özgün kayıt hâlâ erişilebilir mi?
- **Görsel tutarlılık:** Arayüz öğeleri, yazı tipleri, zaman biçimi ve hizalamalar, ilgili uygulamanın gerçek sürümüyle tutarlı mı?
- **Üstveri incelemesi:** Görüntü dosyasının kendi üstverisi (oluşturma zamanı, düzenleme izleri) ile iddia edilen olay zamanı örtüşüyor mu?
- **Özgün kaynakla karşılaştırma:** Mümkünse cihazdaki veri tabanı kaydıyla birebir karşılaştır; tutarsızlık manipülasyon işaretidir.
- **Çapraz kaynak:** Karşı tarafın cihazı, bulut yedeği veya üçüncü bir tanık kaydı, aynı yazışmayı doğruluyor mu?
- **Bağlam bütünlüğü:** Görüntü, yazışmanın kesintisiz bir bölümünü mü yoksa seçilip birleştirilmiş parçaları mı gösteriyor?

burakolgun.com

Bu adımların hiçbiri tek başına kesin sonuç vermese de, birlikte uygulandıklarında bir ekran görüntüsünün güvenilirlik düzeyini anlamlı biçimde ortaya koyar. Kritik olan ilke şudur: Ekran görüntüsü, doğrulanana kadar bir iddiadan ibarettir; delil değeri, ancak özgün kaynağa bağlanabildiği ölçüde doğar. Bu yaklaşım, hem hatalı mahkûmiyetleri önler hem de gerçek delilin hak ettiği ağırlığı kazanmasını sağlar.

7. Delil Güvenilirliği ve Bütünlük

Mesaj delilinin mahkeme önündeki gücü, iki niteliğin bir arada bulunmasına bağlıdır: **özgünlük** (delilin gerçekten iddia edilen kaynaktan geldiği ve değiştirilmediği) ve **bütünlük** (delil zincirinin el koymadan sunuma kadar korunduğu). Bu bölüm, bu iki niteliğin nasıl sağlandığını ele almaktadır.

7.1. Özgünlük ve Üstveri Doğrulaması

Bir mesaj kaydının özgünlüğünü değerlendirmenin en güvenilir yolu, onu özgün kaynağından incelemektir. Cihazdaki mesaj veri tabanı, yalnızca mesaj metnini değil; her mesajın gönderim/alım zaman damgasını, gönderen ve alıcı tanımlayıcılarını, mesaj durum bilgisini ve veri tabanının iç yapısal ilişkilerini de içerir. Bu üstveri, bir mesajın özgünlüğünü doğrulamak için zengin bir zemin sunar; örneğin, bir mesajın zaman damgasının veri tabanındaki diğer kayıtlarla tutarlılığı, manipülasyon belirtilerini ortaya çıkarabilir. Ekran görüntüsünün aksine, özgün veri tabanı, iç tutarlılığı sınanabilir bir delil sunar.

Özgünlük değerlendirmesi, aynı zamanda birden çok kaynağın çapraz doğrulanmasıyla güçlenir. Bir tarafın cihazındaki kayıt, diğer tarafın cihazındaki kayıtla veya bir bulut yedeğiyle karşılaştırıldığında, tutarlılık özgünlüğü destekler; tutarsızlık ise manipülasyon şüphesi doğurur. Bu çapraz doğrulama, özellikle özel hukuk uyuşmazlıklarında -- tarafların yalnızca ekran görüntüsü sunduğu durumlarda -- delilin gerçek değerini ortaya koymak için kritik bir yöntemdir.

7.2. Delil Zinciri ve Hash Doğrulaması

Delil zinciri (chain of custody), bir dijital delilin elde edildiği andan mahkemeye sunulduğu ana kadar geçirdiği tüm aşamaların kesintisiz biçimde belgelenmesidir. Mesaj delili söz konusu olduğunda, bu zincir, cihaza el koyma anından itibaren başlar. El konulan cihazın veya çıkarılan veri imajının kriptografik özeti (hash) alınmalı; bu özet, delilin sonradan değiştirilmediğini matematiksel olarak kanıtlayan bir mühür işlevi görür. İncelemenin her aşaması -- kim, ne zaman, hangi işlemi yaptı -- kayıt altına alınmalıdır.

Hash doğrulaması, dijital delilin bütünlüğünün temel garantisidir. Elde edilen veri imajının hash değeri, inceleme boyunca değişmeden kalmalıdır; herhangi bir değişiklik, hash değerini kökten değiştirir ve böylece tespit edilebilir. İyi bir adli rapor, kullanılan hash algoritmasını, alınan hash değerlerini ve doğrulama adımlarını açıkça belgeler. Bu titizlik, delilin mahkemede sorgulanması hâlinde teknik bulgunun ayakta kalmasını sağlar; eksikliği ise, teknik olarak doğru bir bulgunun bile hukuki değerini zayıflatabilir.

burakolgun.com

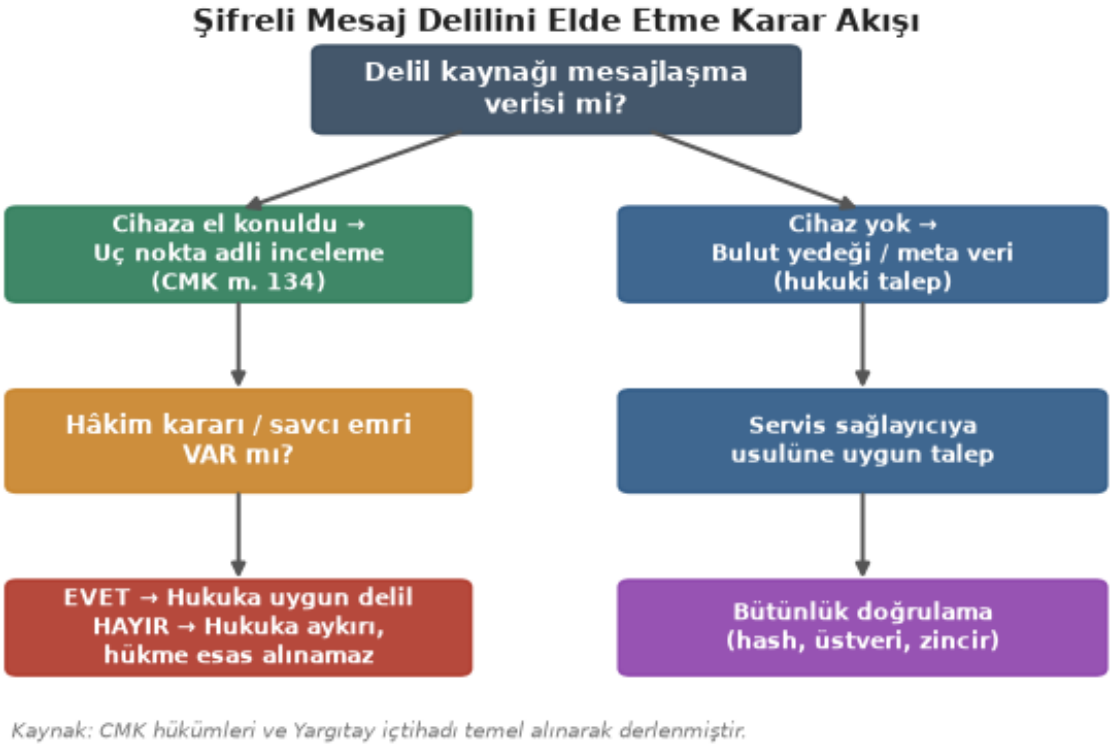
7.3. Bilirkişi Raporu ve Mahkemede Sunum

Teknik olarak sağlam biçimde elde edilmiş ve bütünlüğü doğrulanmış bir mesaj delili bile, mahkemeye anlaşılır ve savunulabilir biçimde sunulmadıkça tam değerini bulamaz. Bir bilirkişi raporu, üç okuyucu kitlesini -- teknik uzman, hukukçu ve hâkim -- aynı anda tatmin etmek durumundadır. Bu nedenle rapor, kullanılan yöntemi (hangi cihaz, hangi araç, hangi çıkarma yöntemi), elde edilen verinin bütünlüğünü (hash değerleri, delil zinciri) ve varılan sonuçların dayanağını, teknik olmayan bir okuyucunun izleyebileceği bir dille ortaya koymalıdır. İyi bir rapor, iddialarını değil, gözlemlerini ve bunların dayanaklarını sunar; yorum ile olguyu özenle ayırır.

Raporun bir diğer sorumluluğu, belirsizlikleri ve sınırları dürüstçe ifade etmektir. Bir mesajın özgünlüğü kesin biçimde doğrulanamıyorsa, bu açıkça belirtilmeli; olasılıksal bir değerlendirme, kesin bir tespit gibi sunulmamalıdır. Aynı biçimde, elde edilemeyen veriler -- kilidi açılamayan bir cihaz, silinmiş bir yedek, kaybolan mesajlar -- raporda not edilmelidir; çünkü bir verinin yokluğu, çoğu zaman yanlış yorumlara açıktır. Bilirkişinin mahkemedeki değeri, bulgularının kesinliğinden çok, yöntemsel dürüstlüğünden ve sınırların farkında olan bir tevazudan gelir. Savunma tarafının raporu sınayabilmesi -- silahların eşitliği ilkesi gereği -- bu şeffaflığın doğrudan bir sonucudur.

8. Hukuki Çerçeve

Şifreli mesaj delilinin değeri, nihai olarak hukuki çerçeve içinde belirlenir. Bu bölüm, konuyu önce Türk hukuku, ardından uluslararası içtihat açısından ele almaktadır. Şekil 3, delilin hukuka uygun elde edilip edilmediğini değerlendiren bir karar akışını göstermektedir.



Şekil 3. Şifreli Mesaj Delilini Elde Etme Karar Akışı (2025)

lgun.com

8.1. Türk Hukuku: CMK, Hukuka Aykırı Delil ve Yargıtay İçtihadı

Türk ceza muhakemesi hukukunda, dijital delillerin elde edilmesi esas olarak Ceza Muhakemesi Kanunu'nun (CMK) 134. maddesi -- 'bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma' -- ile düzenlenmiştir. Bu madde uyarınca, bir şüphelinin kullandığı bilgisayar ve benzeri cihazlarda arama yapılması, kural olarak Cumhuriyet savcısının istemi üzerine hâkim kararına bağlıdır. İletişimin denetlenmesi ise CMK'nın 135. maddesinde ayrıca düzenlenmiştir. Bu usul güvenceleri, keyfî müdahaleye karşı temel bir koruma işlevi görür.

Türk hukukunun en belirleyici ilkelerinden biri, **hukuka aykırı delil yasağıdır.** Anayasa'nın 38. maddesi ve CMK'nın 206/2-a ile 217/2. maddeleri uyarınca, hukuka aykırı yöntemlerle elde edilen deliller reddedilir ve hükme esas alınamaz. Bu yasak, öğretide ve içtihatta mutlak nitelikte kabul edilmektedir; yani delilin içeriği ne kadar önemli olursa olsun, hukuka aykırı biçimde elde edilmişse mahkûmiyete dayanak yapılamaz. Bu ilke, mesaj delilinin elde ediliş yönteminin, içeriği kadar -- hatta ondan önce -- önem taşıdığı anlamına gelir.

Yargıtay, mesaj kayıtlarının hukuka uygun elde edilişi konusunda giderek daha titiz bir içtihat geliştirmektedir. Nitekim Yargıtay 10. Ceza Dairesi'nin 15/05/2024 tarihli bir kararında (2023/15758 E., 2024/18787 K.), CMK'nın 134. maddesine göre alınmış bir hâkim kararı veya yazılı savcı emri olmaksızın, şüphelinin -- rızasıyla dahi -- teslim ettiği telefondaki mesaj kayıtlarının 'ön inceleme ve muhafaza altına alma tutanağı' adı altında incelenmesinin usule aykırı olduğu; bu yolla elde edilen delilin hukuka aykırı sayılıp hükme esas alınamayacağı vurgulanmıştır. Bu karar, uç nokta incelemesinde usul güvencelerinin ne denli kritik olduğunu somutlaştırmaktadır.

Özel hukuk boyutunda ise mesaj kayıtlarının delil değeri, farklı bir dinamiğe tabidir. Yerleşik yaklaşım uyarınca, bir kişinin tarafı olduğu bir yazışmayı, hukuka aykırı bir müdahale olmaksızın ve bizzat kaydetmiş olması hâlinde, bu kaydı delil olarak sunabilmesi mümkün görülmektedir. Buna karşın, tarafı olunmayan bir iletişimin gizlice ele geçirilmesi veya üçüncü kişilerin yazışmalarının hukuka aykırı biçimde elde edilmesi, hem delil yasağına takılır hem de ayrıca suç oluşturabilir. Bu ayrım, uygulamada sıkça karıştırılan ve dikkatle değerlendirilmesi gereken bir husustur.

8.2. Uluslararası İçtihat: ABAD ve Adil Yargılanma

Uluslararası düzlemde, şifreli mesaj delilinin kabul edilebilirliği, adil yargılanma hakkı ekseninde tartışılmaktadır. Beşinci bölümde ele alınan ABAD'ın EncroChat kararı (C-670/22), bu tartışmanın kilometre taşıdır: Karar, delilin kabul edilebilirliğini ulusal hukuka bırakırken, bu değerlendirmenin savunma haklarına ve silahların eşitliği ilkesine saygılı olması gerektiğini vurgulamıştır. Özellikle, savunmanın delilin elde ediliş sürecini ve ham verisini denetleyebilmesi, adil yargılanmanın bir gereği olarak öne çıkmaktadır (CJEU, 2024).

Avrupa İnsan Hakları Sözleşmesi'nin 6. maddesi (adil yargılanma hakkı) ve 8. maddesi (özel hayata ve haberleşmeye saygı hakkı), bu alandaki uluslararası standardın temelini oluşturur. Avrupa İnsan Hakları Mahkemesi içtihadında, delilin hukuka aykırı elde edilmiş olması tek başına her zaman ihlal sayılmasa da, yargılamanın bütün olarak adil olup olmadığı

burakolgun.com

esas alınır; savunmanın delile itiraz edebilme ve onu sınayabilme imkânı belirleyicidir. Bu standart, Türk hukukundaki mutlak delil yasağıyla birlikte değerlendirildiğinde, mesaj delilinin hem elde ediliş yönteminin hem de savunma tarafından denetlenebilirliğinin titizlikle güvence altına alınması gerektiğini ortaya koymaktadır.

8.3. Ortak İlke: Yöntem ile Meşruiyetin Dengesi

Türk hukuku ile uluslararası içtihat, farklı kavramsal araçlar kullansa da ortak bir ilkede buluşur: Bir delilin teknik gücü, onun hukuki meşruiyetinin yerini tutmaz. Türk hukukundaki mutlak hukuka aykırı delil yasağı ile Avrupa içtihadındaki adil yargılanma güvencesi, aynı hedefe -- keyfî ve denetlenemez delil elde etme yöntemlerinin dizginlenmesi -- farklı yollardan hizmet eder. Bu ortak ilke, adli bilişim uzmanı için pratik bir sonuç doğurur: Delili elde etmenin teknik olarak mümkün olması, işin yalnızca yarısıdır; diğer yarısı, o yöntemin hukuki güvencelere ve savunmanın denetim hakkına uygunluğudur.

Bu denge, adli bilişimin geleceği açısından da yön göstericidir. Şifreleme güçlendikçe, kolluk kuvvetleri daha müdahaleci teknik yöntemlere -- cihaz istismarı, uç nokta sızması, toplu veri toplama -- yönelme eğilimindedir. Ancak bu yöntemlerin her biri, mahremiyet ve adil yargılanma haklarıyla yeni gerilimler doğurur. Sürdürülebilir bir denge, ne mahremiyeti mutlaklaştıran ne de suç soruşturmasını felç eden; bunun yerine, açık hukuki dayanağa, yargısal denetime ve savunmanın denetlenebilirliğine dayanan bir çerçevededir. Bilirkişinin rolü, bu çerçevenin teknik ayağını -- yöntemin şeffaflığını ve bulgunun sınanabilirliğini -- güvence altına almaktır.

9. Türkiye Bağlamı ve Uygulama

Türkiye, mesajlaşma uygulamalarının yoğun biçimde kullanıldığı bir ülkedir; bu da mesaj kayıtlarının hemen her tür yargılamada delil olarak gündeme gelmesine yol açmaktadır. Ceza yargılamasında uç nokta incelemesinin usule uygunluğu, özel hukukta ise kaydın tarafınca ve hukuka uygun biçimde elde edilip edilmediği, uygulamada en sık karşılaşılan tartışma başlıklarıdır.

Şifreli mesajlaşmayla ilgili Türk hukukundaki tartışmaların bir bölümü, belirli uygulamaların kullanımının bizzat delil sayılıp sayılamayacağı sorusuyla da ilgilidir. Bu tür tartışmalar, teknik tespit ile hukuki değerlendirmenin ne denli iç içe geçtiğini göstermektedir: Bir uygulamanın bir cihazda yüklü olması, o cihazın sahibinin belirli bir iletişim içeriğine sahip olduğu anlamına gelmez; içeriğin varlığı ve niteliği, ayrı ve titiz bir teknik incelemeyle ortaya konmalıdır. Teknik tespitin sınırlarının hukuki sonuçlarla karıştırılmaması, adli bilişim uzmanının en temel sorumluluklarından biridir.

Kapasite ve eğitim, Türkiye bağlamının belirleyici ihtiyaçlarındandır. Şifreli mesaj delilinin doğru elde edilmesi ve değerlendirilmesi, hem güncel adli araçlara hâkim hem de usul hukukunun inceliklerini bilen uzmanlar gerektirir. Uç nokta incelemesinde CMK m. 134 güvencelerine uyulmaması, ekran görüntüsünün özgün kaynak olmadan kabul edilmesi ya da delil zincirinin belgelenmemesi gibi hatalar, teknik olarak elde edilmiş bir delili hukuken değersiz kılabilir. Bu nedenle kolluk, savcılık ve bilirkişilik düzeyinde ortak bir metodolojik

burakolgun.com

standardın yerleşmesi; hem maddi gerçeğe ulaşma hem de adil yargılanma bakımından kritik önemdedir.

Türk uygulamasında öne çıkan bir diğer zorluk, sınır ötesi veri erişimidir. Başlıca mesajlaşma sağlayıcıları yurt dışında yerleşik olduğundan, meta veri veya sunucu tarafı veriye erişim, uluslararası adli yardımlaşma süreçlerine ve sağlayıcıların hukuki talep politikalarına bağlıdır. Bu süreçler zaman alıcı olabilir; bu da uç nokta incelemesinin -- yani cihaza doğrudan erişimin -- Türk uygulamasında neden bu kadar merkezî bir rol oynadığını açıklar. Cihaz merkezli delil, çoğu zaman en hızlı ve en doğrudan yoldur; ancak tam da bu nedenle usul güvencelerine en çok dikkat edilmesi gereken alandır.

9.1. Temsilî Bir Uygulama Senaryosu

Kavramların somutlaşması için, gerçek bir dosyaya atıf yapmayan, tümüyle temsilî bir senaryo düşünelim. Bir uyuşmazlıkta taraflardan biri, karşı tarafın kendisine tehdit içerikli mesajlar gönderdiğini ileri sürmekte ve delil olarak yalnızca birkaç ekran görüntüsü sunmaktadır. İlk soru hukukilik değil, güvenilirliktir: Bu ekran görüntüleri, kolayca üretilebilir nitelikte olduğundan, tek başına zayıf bir delildir. Doğru yaklaşım, ekran görüntüsünün ötesine geçip, mesajın özgün kaynağına -- iddia sahibinin cihazındaki veri tabanına -- ulaşmaktır.

İkinci aşamada, iddia sahibinin cihazı, rızasıyla ve usulüne uygun biçimde adli incelemeye alınır. Cihazdaki mesaj veri tabanı, ekran görüntüsündeki yazışmayı; gönderim zaman damgalarını, taraf tanımlayıcılarını ve veri tabanının iç tutarlılığını içerecek biçimde doğrulayabilir ya da çürütebilir. Eğer mümkünse, karşı tarafın cihazındaki karşılık gelen kayıtla çapraz doğrulama, özgünlüğü daha da güçlendirir. Bu aşamada bilirkişi, yalnızca 'mesaj var' demez; mesajın üstverisinin tutarlı olup olmadığını, manipülasyon belirtisi taşıyıp taşımadığını da değerlendirir.

Üçüncü aşamada, tüm bulgular bir rapora dönüştürülür. Rapor, incelenen cihazı ve veri imajının hash değerini belgeler; ekran görüntüsü ile özgün kayıt arasındaki tutarlılığı ortaya koyar; ve varsa belirsizlikleri -- örneğin çapraz doğrulama yapılamamışsa bunu -- açıkça belirtir. Bu senaryo, makalenin ana tezini örneklemektedir: Ekran görüntüsü bir başlangıç işareti olabilir, ancak asıl delil onu doğrulayan özgün kayıttır; ve bu kaydın değeri, hukuka uygun elde edilişine, bütünlüğüne ve şeffaf raporlanmasına bağlıdır. Bu senaryo tümüyle açıklayıcı amaçlıdır ve herhangi bir gerçek dosya veya kişiyle ilişkili değildir.

10. Bilirkişi Uygulaması ve İyi Uygulama Önerileri

Yukarıdaki değerlendirmeler, şifreli mesaj delilinin ele alınmasında bilirkişinin ve soruşturma makamının uyması gereken bir dizi iyi uygulama ilkesine işaret etmektedir:

- **Usule öncelik ver:** Delilin içeriğine geçmeden önce, hukuka uygun elde edilip edilmediğini (CMK m. 134/135, hâkim kararı) değerlendir; usulsüz delil hükme esas alınamaz.
- **Özgün kaynağa yönel:** Ekran görüntüsüyle yetinme; mümkün olduğunca cihazdaki özgün veri tabanına veya bulut yedeğine, adli yöntemle ulaş.

burakolgun.com

- **Bütünlüğü belgelendir:** El koyma anından itibaren hash al, delil zincirini kesintisiz kaydet, incelemeyi yeniden üretilebilir biçimde raporla.
- **Üstveriyi doğrula:** Mesajın zaman damgası, taraf tanımlayıcıları ve veri tabanı iç tutarlılığını sınayarak manipülasyon belirtilerini araştır.
- **Çapraz doğrula:** Mümkünse birden çok kaynağı (iki cihaz, cihaz + yedek) karşılaştırarak özgünlüğü destekle.
- **Sınırları açıkça belirt:** Kaybolan mesajların yokluğu, olayın olmadığını kanıtlamaz; teknik tespitin sınırlarını raporda dürüstçe ifade et.
- **Teknik ile hukukiyi ayır:** Bir uygulamanın varlığı ile içeriğin varlığını karıştırma; teknik bulguyu hukuki nitelendirmeden özenle ayır.

Bu ilkeler, yalnızca ceza yargılaması için değil, mesaj kayıtlarının delil olarak kullanıldığı her tür uyuşmazlık için geçerlidir. İş hukuku ihtilaflarında bir çalışanın yazışmaları, boşanma davalarında eşler arası mesajlar, ticari uyuşmazlıklarda müzakere kayıtları -- hepsinde aynı iki soru geçerlidir: Kayıt hukuka uygun mu elde edildi ve özgün mü? Özel hukuk ile ceza hukuku arasındaki usul farklarına rağmen, delilin özgün kaynağa dayanması ve bütünlüğünün doğrulanabilmesi ilkesi ortaktır. Bu nedenle yukarıdaki iyi uygulama önerileri, bilirkişinin hangi yargı kolunda görev yaptığından bağımsız olarak bir temel standart oluşturur.

Bu ilkelerin ortak paydası, teknik yetkinliğin hukuki titizlik ve metodolojik şeffaflıkla birleştirilmesidir. Şifreli mesaj delili, doğru elde edilip doğru değerlendirildiğinde güçlü ve güvenilir bir delildir; yanlış ele alındığında ise hem adil yargılanmayı zedeleyen hem de teknik olarak yanıltıcı bir kaynağa dönüşebilir. Bilirkişinin görevi, bu iki sonuç arasındaki farkı belirleyen titizliği göstermektir.

11. Sonuç

Uçtan uca şifreleme, iletişim mahremiyetini güçlendirirken adli bilişimi köklü bir dönüşüme zorlamıştır. Delil artık iletişim kanalından değil, iletişimin uç noktalarından -- cihazlardan ve bulut yedeklerinden -- elde edilmektedir. WhatsApp, Signal ve Telegram, bu tabloda farklı adli profiller sunar: WhatsApp bulut yedekleriyle görece erişilebilir, Signal yalnızca cihaz kilidi açıldığında çözülebilir, Telegram ise varsayılan bulut sohbetleri nedeniyle kendine özgü bir konumdadır. Bu farkların doğru anlaşılması, hangi verinin nereden elde edilebileceğinin belirlenmesi açısından belirleyicidir.

Bununla birlikte, delilin 'elde edilebilir' olması, 'kullanılabilir' olduğu anlamına gelmez. EncroChat ve Sky ECC deneyiminin gösterdiği gibi, teknik olarak güçlü bir delil elde etme yöntemi, hukuki meşruiyet süzgecinden -- adil yargılanma ve savunma hakları -- geçmeden mahkeme önünde değer kazanamaz. Türk hukukundaki mutlak hukuka aykırı delil yasağı ve Yargıtay'ın güncel içtihadı, mesaj delilinin elde ediliş yönteminin, içeriği kadar önemli olduğunu açıkça ortaya koymaktadır.

Bu makalenin ortaya koyduğu bir diğer örüntü, teknoloji ile hukukun sürekli karşılıklı etkileşimidir. Şifreleme güçlendikçe adli yöntemler uç noktaya, buluta ve canlı incelemeye kaymakta; her yeni yöntem ise yeni hukuki soruları -- mahremiyet, orantılılık, savunmanın

burakolgun.com

denetim hakkı -- gündeme getirmektedir. Yapay zekâ destekli manipülasyonun yaygınlaşması, özgünlük değerlendirmesini eskisinden çok daha kritik hâle getirmiş; ekran görüntüsü gibi yüzeysel delillere güveni sarsmıştır. Bu ortamda adli bilişim uzmanının rolü, geçmişte olduğundan daha merkezî ve daha sorumludur; çünkü bir mesajın gerçekliğini yüzeyin ötesinde değerlendirebilecek yetkinlik, giderek delilin güvenilirliğinin son güvencesi hâline gelmektedir.

Nihai olarak, şifreli mesaj delilinin güvenilirliği üç koşulun bir arada sağlanmasına bağlıdır: hukuka uygun elde etme, teknik bütünlüğün doğrulanması ve delil zincirinin korunması. Ekran görüntüsü gibi kolayca manipüle edilebilen biçimlerle yetinmek yerine, verinin özgün kaynağına ulaşmak ve bütünlüğünü belgelemek, hem adil yargılanmanın hem de maddi gerçeğe ulaşmanın gereğidir. Bilirkişinin sorumluluğu, karmaşık bir teknik gerçeği, sınırlarını gizlemeden ve hukuki çerçeveyi gözeterek, hâkimin güvenle dayanabileceği bir netlikte ortaya koymaktır. Bu denge kurulduğunda, şifreli çağın mesaj kayıtları, adaletin güvenilir tanıkları hâline gelir.

Kaynakça

Anglano, C. (2014). Forensic analysis of WhatsApp Messenger on Android smartphones. *Digital Investigation*, 11(3), 201–213. https://doi.org/10.1016/j.diin.2014.04.003

Cellebrite. (2025). *Navigating the most widely used apps and messaging sources in investigations*. Cellebrite DI Ltd.

Court of Justice of the European Union. (2024, April 30). *Judgment in Case C-670/22 (M.N. — EncroChat)*. CJEU.

Europol. (2021). *Operation Trojan Shield / ANOM: Global law enforcement operation*. European Union Agency for Law Enforcement Cooperation.

Marlinspike, M., & Perrin, T. (2016). *The Double Ratchet algorithm*. Signal Foundation. https://signal.org/docs/

Oxygen Forensics. (2025). *Oxygen Forensic Detective: Application and cloud extraction capabilities*. Oxygen Forensics Inc.

Schneier, B. (2015). *Applied cryptography: Protocols, algorithms, and source code in C* (20th anniversary ed.). Wiley.

Tamma, R., Skulkin, O., Mahalik, H., & Bommisetty, S. (2020). *Practical mobile forensics* (4th ed.). Packt Publishing.

2709 sayılı Türkiye Cumhuriyeti Anayasası. (1982). *Resmî Gazete* (Sayı: 17863). (m. 38, suç ve cezalara ilişkin esaslar).

5271 sayılı Ceza Muhakemesi Kanunu. (2004). *Resmî Gazete* (Sayı: 25673). (m. 134, bilgisayarlarda arama; m. 135, iletişimin denetlenmesi; m. 206, 217, delil yasağı).

Yargıtay 10. Ceza Dairesi. (2024, 15 Mayıs). *2023/15758 E., 2024/18787 K.* (Hukuka aykırı elde edilen telefon kayıtları).

burakolgun.com

Avrupa İnsan Hakları Sözleşmesi. (1950). (m. 6, adil yargılanma hakkı; m. 8, özel hayata ve haberleşmeye saygı hakkı).

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

National Institute of Standards and Technology. (2014). *Guidelines on mobile device forensics* (NIST SP 800-101 Rev. 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-101r1

Magnet Forensics. (2025). *Magnet AXIOM: Mobile and cloud evidence processing*. Magnet Forensics Inc.

Cohen, C., & Park, A. (2023). Forensic analysis of ephemeral messaging applications: Disappearing messages or evidential data? *Forensic Science International: Digital Investigation*, 46, 301608. https://doi.org/10.1016/j.fsidi.2023.301608

Unger, N., Dechand, S., Bonneau, J., Fahl, S., Perl, H., Goldberg, I., & Smith, M. (2015). SoK: Secure messaging. *2015 IEEE Symposium on Security and Privacy*, 232–249. https://doi.org/10.1109/SP.2015.22

Yargıtay Ceza Genel Kurulu. (2021). *Dijital delillerin hukuka uygun elde edilmesine ilişkin ilkeler*. (Karar özeti).

Reitinger, N. (2025). Encrypted messaging and the future of digital evidence. *Journal of Digital Forensics, Security and Law*, 20(1).

burakolgun.com