İSTANBUL UNIVERSITY PRESS

Ceza Hukuku ve Kriminoloji Dergisi
Journal of Penal Law and Criminology

Ceza Hukuku ve Kriminoloji Dergisi
Journal of Penal Law and Criminology,
JPLC 2025, 13 (2): 452–481

https://doi.org/10.26650/JPLC2025-1774958
Başvuru | Submitted 31.08.2025
Revizyon Talebi | Revision Requested 12.11.2025
Son Revizyon | Last Revision Received 08.01.2026
Kabul | Accepted 08.01.2026

Araştırma Makalesi | Research Article

Açık Erişim | Open Access

AB Cezai Konularda İş Birliği Hukukunda Telekomünikasyon Verilerinin Sınır Ötesi Elde Edilmesi, Aktarımı Ve Delil Değeri: Encrochat Operasyonu Örneği

Evidentiary Value of Data from Cross-Border Interception and Transfer in EU Cooperation Law in Criminal Matters: Case Example of the Operation Encrochat

Erdem İzzet Külçür [1] & Rüveyda Enes [2]

[1] İbn Haldun Üniversitesi, Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı, İstanbul, Türkiye
[2] İbn Haldun Üniversitesi, Hukuk Fakültesi, İstanbul, Türkiye

Öz

Bu çalışma, Encrochat operasyonunda başvurulan soruşturma tedbirlerinin cezai konularda Avrupa Birliği (AB) iş birliği hukukundaki yasal altyapısını, özellikle telekomünikasyon verilerinin sınır ötesinde elde edilmesi ve sınır ötesine aktarılan bu verilerin delil değerini ve bu bağlamda ortaya çıkan diğer hukuki tartışmaları incelemektedir. Makalede öncelikle Encrochat'in teknik yapısı, suç örgütleri tarafından tercih edilme nedenleri ve 2020 yılında Fransa ile Hollanda öncülüğünde yürütülen uluslararası operasyonun seyri ele alınmıştır. Ardından, operasyonda başvurulan üç temel iş birliği enstrümanı olan ortak soruşturma ekipleri (JITs), spontane bilgi paylaşımı ve Avrupa Soruşturma Emri'nin (ASE) hukuki altyapısı ve Encrochat operasyonundaki uygulamaları incelenmiştir. Çalışmanın hukuki tartışmalar bölümünde, elde edilen verilerin hem ulusal hukuk (özellikle Alman ceza muhakemesi hukuku) hem de AB hukuku bakımından geçerliliği, ölçülülük ilkesi, anayasal çekirdek alan koruması, kamu düzeni ve adil yargılanma hakkı ekseninde, Alman Anayasa Mahkemesi (BverfG), Alman Federal Yargıtayı (BGH), Berlin Eyalet Mahkemesi ve Avrupa Birliği Adalet Divanı (ABAD) kararları ile doktrindeki görüşler doğrultusunda karşılaştırmalı olarak incelenmiştir. Sonuç bölümünde, Encrochat operasyonunun organize suçla mücadelede teknoloji ve uluslararası iş birliğinin etkinliğini ispatladığı, ancak delil elde etme ve kullanma süreçlerinin temel haklar ve usulî güvenceler açısından ciddi hukuki tartışmalara kapı araladığı tespit edilmiştir.

Abstract

This study examines the legal framework of European Union cooperation law in criminal matters with regard to the investigative measures employed in the Encrochat operation, particularly the evidentiary value of materials obtained through cross-border interception of communications and subsequently transferred across borders. The article first outlines Encrochat's technical structure, its appeal to criminal organizations, and the 2020 international operation led by France and the Netherlands. It then considers the legal framework and implementation of the three main cooperation instruments employed: joint investigation teams (JITs), spontaneous exchange of information, and the European Investigation Order (EIO). Particular attention is given to the evidentiary use of intercepted data under national law—especially German criminal procedure law—and EU law, with a focus on proportionality and legality. The analysis addresses issues such as the protection of private life, ordre public, and fair trial guarantees, drawing on case law from the German Constitutional Court, the Federal Court of Justice, the Berlin Regional Court, and the CJEU, as well as academic commentary. The study concludes that while the Encrochat operation highlights the potential of technology and international cooperation against organized crime, it also exposes significant legal tensions concerning fundamental rights and procedural safeguards.

Atıf | Citation: Külçür, E. İ. & Enes, R. (2025). AB Cezai Konularda İş Birliği Hukukunda Telekomünikasyon Verilerinin Sınır Ötesi Elde Edilmesi, Aktarımı Ve Delil Değeri: Encrochat Operasyonu Örneği. *Ceza Hukuku ve Kriminoloji Dergisi–Journal of Penal Law and Criminology*, *13*(2), 452-481. https://doi.org/10.26650/JPLC2025-1774958

Sorumlu Yazar | Corresponding author: Erdem İzzet Külçür erdem.kulcur@ihu.edu.tr

Anahtar Kelimeler Encrochat · Sınır Ötesi İletişim Dinleme · Adli İş Birliği

Keywords Encrochat · Cross-border Interception of Telecommunication · Judicial Cooperation

Extended Summary

The Encrochat operation, launched under the leadership of France and the Netherlands in 2020, represents one of the most significant examples of international cooperation against drug trafficking and organized crime recently. Encrochat, a cryptographic communication system widely adopted by criminal networks, offers advanced encryption technologies specifically designed to resist law enforcement surveillance. The dismantling of this network not only disrupted organized crime activities on a global scale but also raised critical questions regarding the collection, transfer, and admissibility of intercepted data as evidence in criminal proceedings. This study focuses on these questions within the framework of the European Union (EU) judicial and police cooperation law in criminal matters and seeks to assess the evidentiary value of cross-border telecommunications interception through the lens of the Encrochat case.

The article begins by outlining the operation's background and highlighting why Encrochat devices—equipped with dual operating systems, panic deletion functions, and limited connectivity—were attractive to criminal organizations. The investigation, supported by Europol and Eurojust, led to the infiltration of Encrochat servers and the interception of millions of messages, triggering prosecutions across several European jurisdictions. The unprecedented scope of data collection and its subsequent use in trials have, however, sparked legal controversies at both national and EU levels.

Methodologically, the study adopts a comparative approach. It analyses national perspectives, particularly German criminal procedure law, alongside EU cooperation instruments and case law. Special attention is given to decisions of the German Federal Court of Justice (BGH), the German Constitutional Court (BVerfG), the Berlin Regional Court (LG), and the Court of Justice of the European Union (CJEU). These judicial perspectives combined with doctrinal debates allow for a nuanced evaluation of the extent to which investigative measures taken during the Encrochat operation comply with fundamental rights and legal safeguards.

Three EU cooperation instruments are examined in relation to the operation: joint investigation teams (JITs), spontaneous exchange of information, and the European Investigation Order. JITs facilitated real-time coordination between French and Dutch authorities, while spontaneous information exchange enabled Encrochat data to be transmitted rapidly to other jurisdictions, such as Germany and the United Kingdom. The EIO, in turn, provided a framework for the subsequent transfer of evidence into domestic proceedings. Although these mechanisms proved effective in operational terms, they raised concerns regarding procedural safeguards, transparency, and the balance of competence between national and EU authorities.

The study identified several key areas of legal debate. At the national level, German courts questioned the admissibility of evidence collected abroad, focusing on whether foreign interception measures could be assessed under domestic standards. Central issues included the principle of proportionality, the scope of constitutional protection for private life and communication, and the potential exclusion of evidence obtained in violation of cooperation rules. The BGH emphasized the principle of free judicial evaluation of evidence, while the Berlin Regional Court expressed doubts about the transparency of the data collection process and the ability of defendants to challenge the reliability of the intercepted material.

At the EU level, the legality of the investigative measures was scrutinized considering defense rights and fair trial guarantees. The CJEU was asked to clarify whether public prosecutors were competent to issue EIOs and whether the secrecy surrounding Encrochat's technical infiltration undermined the fairness of proceedings. Concerns about the asymmetry of information between prosecution and defense and the inability of defendants to verify the integrity of the data highlighted tensions between efficient law enforcement and the protection of fundamental rights.

Rather than providing a definitive conclusion, the study stresses the dual character of the Encrochat operation. On the one hand, it demonstrates the effectiveness of advanced technology and cross-border cooperation in tackling organized crime. On the other hand, it reveals substantial legal uncertainties concerning evidentiary law, particularly the admissibility of encrypted communication data considering constitutional guarantees and procedural safeguards.

By situating the Encrochat operation within both national and EU legal frameworks, the article contributes to broader debates on cross-border evidence, digital surveillance, and the future of judicial cooperation in Europe. It suggests that while instruments such as JITs, spontaneous information exchange, and the EIO are indispensable in practice, their use must be carefully balanced against fundamental rights to ensure legitimacy and long-term acceptance within the rule of law. In this way, the Encrochat case becomes not only a milestone in law enforcement but also a catalyst for evolving legal discussions on the admissibility and reliability of cross-border digital evidence.

Giriş

Organize suçlarla mücadele, devletlerin güvenlik politikalarının en öncelikli gündemlerinden biri olmaya devam etmektedir. Küreselleşmenin ve teknolojinin ivme kazanmasıyla birlikte suç örgütleri de uluslararası ölçekte faaliyet göstermeye başlamış; uyuşturucu ticaretinden kara para aklamaya, silah kaçakçılığından siber suçlara kadar pek çok alanda sınır ötesi örgütlenmeler kurulmuştur. Bu gelişmeler karşısında ulusal makamların tek başına yürüttüğü geleneksel soruşturma yöntemlerinin yetersiz kaldığı görülmüş ve devletlerin daha yakın ve etkin adli ve polisiye iş birliği modelleri geliştirme ihtiyacı ortaya çıkmıştır. Avrupa Birliği (AB), özellikle 1990'lı yıllardan itibaren sınır aşan suçlarla mücadelede koordinasyonu güçlendirmek üzere çok sayıda kurumsal ve hukuki düzenlemeyi hayata geçirmiştir.[1] Bu bağlamda Eurojust ve Europol gibi adli ve polisiye iş birliği mekanizmaları ile özel (gizli) soruşturma tedbirlerinin uygulanmasını da içeren karşılıklı adli yardımlaşma, ortak soruşturma ekipleri, Avrupa Soruşturma Emri gibi iş birliği araç ve yöntemlerine ilişkin hukuki düzenlemeler ceza soruşturmalarının etkinliğini artırmak amacıyla devreye sokulmuştur. Ancak bu araçların kullanımı, çoğu zaman temel hakların korunması ile suçla mücadelede etkinlik arasındaki hassas dengeyi gündeme getirmektedir.

Bu denge sorununu en açık şekilde ortaya koyan örneklerden biri, 2020 yılında Fransa ve Hollanda öncülüğünde gerçekleştirilen Encrochat operasyonudur. Uçtan uca şifreleme teknolojisiyle donatılmış Encrochat telefonları, suç örgütleri tarafından gizli iletişim aracı olarak yaygın biçimde kullanılmaktaydı. Yetkililer tarafından gerçekleştirilen operasyon sonucunda on binlerce şifreli mesajın ele geçirilmesi, Avrupa çapında binlerce kişinin yakalanmasına ve milyarlarca Euro değerinde mal varlığına el konulmasına yol açmıştır.

Encrochat operasyonunun hukuki önemi, yalnızca teknik boyutuyla değil, aynı zamanda farklı ülkelerin yargı makamlarının ortak hareket etmesini gerektiren iş birliği mekanizmalarıyla da ilgilidir. Operasyonda başvurulan üç temel araç olan ortak soruşturma ekipleri (Joint Investigation Teams - JITs, bundan böyle JIT olarak anılacaktır), spontane bilgi paylaşımı ve Avrupa Soruşturma Emri (ASE), AB'nin cezai konularda iş birliği hukukunun temel taşlarını oluşturmaktadır. Bu araçların pratikte nasıl işlediği, hangi hukuki zeminlere dayandığı ve sınır aşan suçlarla mücadelede ne tür sonuçlar doğurduğu, Encrochat operasyonu özelinde somut biçimde gözlemlenmiştir. Ancak bu iş birliği mekanizmalarının kullanımı başta devletlerin egemenlik yetkilerinin sınırları olmak üzere, ve fakat özellikle, elde edilen verilerin hukuka uygunluğu ve delil değeri bağlamında anayasal çekirdek alan koruması, ölçülülük ilkesi, kamu düzeni ve adil yargılanma hakkı gibi konularda yeni tartışmalar doğurmuştur.

Nitekim Alman mahkemelerinin Encrochat verilerinin delil olarak kullanılmasına ilişkin farklı kararları bu tartışmaların somut yansımalarıdır. Alman Federal Yargıtayı (BGH), elde edilen verilerin ceza yargılamasında kullanılabilirliğini kabul etmiş[2] ancak Berlin Eyalet Mahkemesi (LG) Avrupa Birliği Adalet Divanı'na (ABAD) başvurarak adil yargılanma hakkı ve delil bütünlüğü bakımından ciddi hukuki sorunlar ile sürmüştür.[3]

[1] Yeşim Yılmaz, Avrupa Birliği Ceza Hukukunda Organize Suçlulukla Mücadele, *TAAD*, Yıl:8, Sayı:31 (Temmuz 2017), s. 727.

[2] BGH, Beschluss vom 2. März 2022 – 5 StR 457/21.

[3] Landgericht Berlin, I Az.: 525 KLs 8/22 279 Js 30/22 StA Berlin, T: 19.12.2024.

ABAD'ın değerlendirmeleri delillerin güvenilirliği ve şeffaflığı sağlanmadığında sanığın savunma hakkının ihlal edileceğini ortaya koymuştur. Böylelikle Encrochat davası, AB hukukunda karşılıklı tanıma ve güven ilkelerinin sınırlarını, delil elde etme ve kullanma süreçlerindeki şeffaflık gerekliliklerini ve ulusal mahkemelerin hareket alanını sorgulatan bir dönüm noktası haline gelmiştir.

Bu çalışmanın önemi, tam da bu kesişim noktasında ortaya çıkmaktadır. Zira Encrochat operasyonu, bir yandan organize suçla mücadelede teknoloji ve uluslararası iş birliğinin vazgeçilmezliğini kanıtlarken, diğer yandan elde edilen verilerin delil değeri konusunda ciddi hukuki sorunları gündeme getirmiştir. Özellikle telekomünikasyon verilerinin sınır ötesinde elde edilmesi ve elde edilen verilerin sınır ötesine aktarımı sonucunda ulusal yargılamalarda kullanılabilirliği, devlet egemenliği, bireyin temel haklarının korunması ve AB'nin bütünleşik adli iş birliği sistemi tartışmaya açılmıştır.

Çalışmada öncelikle Encrochat sisteminin yapısı, suç örgütleri tarafından neden tercih edildiği ve operasyonun seyri ele alınacaktır. Ardından JIT, spontane bilgi paylaşımı ve ASE gibi iş birliği araçlarının operasyon özelindeki uygulamaları değerlendirilecektir. Sonraki bölümde ise Encrochat verilerinin ulusal hukuk (özellikle Alman ceza muhakemesi hukuku) ve AB hukuku bakımından delil değeri tartışılacak, anayasal çekirdek alan koruması, ölçülülük ilkesi ve adil yargılanma hakkı gibi ilkeler ışığında karşılaştırmalı bir analiz yapılacaktır. Bu bağlamda, Encrochat operasyonu yalnızca suç örgütlerine karşı yürütülen başarılı bir polis operasyonu olmanın ötesinde, AB iş birliği hukukunun sınırlarını test eden ve delil hukukuna dair önemli tartışmalar doğuran bir vaka olarak değerlendirilmektedir. Bu makale, söz konusu tartışmalara katkı sunmayı, ulusal ve ulusüstü hukuk düzenleri arasındaki gerilimi ortaya koymayı ve gelecekte benzer operasyonlarda izlenebilecek hukuki yaklaşımlara ışık tutmayı hedeflemektedir.

I. Encrochat'in Yapısı ve Kullanım Amacı

Organize suç örgütlerinin bir dönem yaygın olarak kullanıldığı Encrochat uçtan uca şifreli iletişim sunan kripto bir iletişim aracıdır.[4] Hem Android hem de Encrochat işletim sistemi tabanlı çalışabilen bu cihazlar genellikle Samsung, BlackBerry, BQ Aquaris X2 gibi cihazlardan modifiye edilmiştir. Encrochat telefonlar, iki farklı modda açılabilmektedir. Cihazın güç düğmesine basıldığında Android işletim sistemi ana ekranı açılmakta, güç düğmesi ile ses düğmesine aynı anda basıldığında ise gizli bir şifrelenmiş bölüm (Encrochat) açılarak cihazın asıl amacına uygun şekilde gizli iletişim sağlaması mümkün hale gelmektedir.[5] Bir kullanıcının diğer kullanıcı ile iletişim kurabilmesi için o kullanıcıya özgü kullanıcı kimliğini bilmesi gerektiği bu sistemde gönderilen bir mesaj cihazlar arasındaki Encrochat sunucusundan geçerken şifrelenmekte, alıcı cihaza ulaştığında ise deşifre edilmektedir.[6]

Öte yandan telefonlardaki tüm verilerin anında silinmesi için tasarlanmış özel PIN kodu (panik silme), art arda yanlış parola girilmesi durumunda tüm verilerin silinmesi, bayi/yardım masası (help-desk) tarafından mesajların uzaktan silinebilmesi, Encrochat telefonlarının mobil veri yerine yalnızca Wi-Fi sinyali kullanması gibi özellikler bu telefonları suç örgütlerine mensup kişiler için cazip hale getirmiştir. Kullanıcıya bağlı herhangi bir cihaz ya da sim kart kaydı gerektirmeyen bu cihazlarda kamera, mikrofon, GPS ve USB veri bağlantı noktası da bulunmadığından normal bir arama yapılması veya internet kullanımı mümkün değildir. Önceden yüklenmiş uygulamalarla birlikte satılan bu cihazlarla yalnızca kullanıcılar arası SMS gönderimi, not

[4] Encrochat şirketinin websitesi için: https://encrophone.com/en/ (web sayfasında yer alan son güncelleme tarihi 16.01.2025 olup tarafımızdan son erişim tarihi 20.08.2025'tir.)

[5] John Scheerhout, "The 'secret server' used in the killing of John Kinsella – and what it reveals about the scale of the illegal gun trade in Manchester", Manchester Evening News, 9 July 2020, Erişim Adresi: https://www.manchestereveningnews.co.uk/news/greater-manchester-news/secret-server-used-killing-john-18563462, Erişim Tarihi: 26.12.2024.

[6] A, B, D & C v. Regina [2021] EWCA Crim 128, para. 11.

oluşturma veya sesli mesaj gönderimi ve depolaması yapılabilmektedir.[7] Bu uygulamalar arasında mesajlaşma uygulaması 'Encrochat', sesli arama hizmeti 'Encrotalk' ve kullanıcıların şifreli özel notlar yazmasını sağlayan 'Encronotes' yer almaktadır.[8]

Encrochat'in sahip olduğu özel şifreleme teknolojisinin kolluk kuvvetlerinin iletişim içeriklerine erişmesini ve cihazların yerini tespit etmesini engellemek üzere tasarlandığı görülmektedir. Encrochat cihazları uluslararası ölçekte yaklaşık 1.000 Euro'ya satılırken, 7/24 destek sağlayan altı aylık Encrochat hizmeti aylık 1.500 civarında bir fiyatla satılmıştır.[9] Herhangi bir şubesi, merkezi, satış ofisi ya da yetkili temsilcisi bulunmayan Encrochat, 2020'nin başlarında büyük çoğunluğunun suç faaliyetlerine karıştığı muhtemel olan yaklaşık 60.000 kullanıcısı ile şifreli dijital iletişimin en büyük sağlayıcılarından birisi olmuştur.[10]

II. Encrochat Operasyonu

Encrochat operasyonu, organize suçla mücadelede dijital araçların ve uluslararası iş birliğinin nasıl kritik bir rol oynadığını gösteren son yılların en önemli kurumlararası ortak operasyon örneğidir. 2020 yılında Fransa ve Hollanda önderliğinde başlatılan bu operasyon, Europol ve Eurojust'un koordinasyonunda gerçekleştirilmiştir. Operasyon, suç şebekelerinin yaygın olarak kullandığı şifreli iletişim ağı Encrochat'in çökertilmesi ve ele geçirilen verilerin organize suçlarla mücadelede kullanılması açısından büyük önem arz etmektedir. Küresel ölçekte organize suç gruplarına ağır darbe vuran bu operasyon suçla mücadelede önemli bir dönüm noktası olmuştur.

Encrochat operasyonuna giden yol ilk olarak Fransız makamlarının 2017 ve 2018 yıllarında gerçekleştirdiği organize suç operasyonları sırasında şüphelilere ait Encrochat cihazlarını ele geçirmesi ile başlamıştır. Ele geçirilen cihazlar üzerinde yapılan araştırmalar sonucunda Encrochat'in Fransa'nın Roubaix şehrinde yer alan sunucuları (*server*) kullandığı ortaya çıkarılmış, bunun üzerine Lille savcılığı Kasım 2018'de Encrochat soruşturmasını başlatmıştır. Soruşturma, 2019 yılının başlarında Avrupa Birliği'nden sağlanan fonların ardından hız kazanmıştır.[11] Bu kapsamda Fransız makamları Eurojust nezdinde bir dosya açarak elindeki verileri Encrochat kullanıcılarının önemli bir kısmının ikamet ettiği Hollanda'nın yetkili makamları ile paylaşmıştır. 1 Nisan 2020 tarihinde gelindiğinde Fransız mahkemesi Fransız savcılığının Fransa'da yer alan sunuculara teknik bir araç yerleştirilerek Encrochat cihazlarında depolanan (durağan) verilere (stored data) erişim talebine izin vermiştir.[12]

Fransız makamları uyguladıkları erişim yönteminin teknik ayrıntılarını askeri sır olarak kabul etmiş olsa da[13] uzmanlar ve mahkemeler bu yöntemi ayrıntılarıyla açıklayabilmişlerdir.[14] Buna göre Fransız yetkililer

[7] Thomas Wahl, 'Germany: Federal Court of Justice Confirms Use of Evidence in Encrochat Cases' (2022) 1 eucrim 36.

[8] https://encrophone.com/en/ Erişim Tarihi: 24.12.2024.

[9] Europol, "Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe", 2 July 2020, Erişim Adresi: https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe, Erişim Tarihi: 21.12.2024.

[10] Ibid.

[11] Sky News, 'Encrochat: What it is, who was running it, and how did criminals get their encrypted phones?' (3 July 2020), Erişim Adresi: https://news.sky.com/story/encrochat-what-it-is-who-was-running-it-and-how-did-criminals-get-their-encrypted-phones-12019678 Erişim Tarihi: 29 Aralık 2024.

[12] Wahl, 'Germany: Federal Court of Justice Confirms...', 36.

[13] Thomas Wahl, 'ECJ Ruled in Encrochat Case' (2024) 1 eucrim 41.

[14] İngiliz mahkemeleri operasyonun teknik yönünü şu şekilde açıklamıştır: "Her bir (Encrochat) cihaz(ın)da Realm ve RAM olmak üzere iki tür hafıza bulunmaktadır. Realm, uygulamaların arşiv kaydını ve kullanılacak veriyi tutarken, daha hızlı ve geçici nitelikte olan RAM ise uygulama açıkken uygulamanın çalışması için uygulama ve veri kayıtlarını tutarak işlemcinin (CPU) faaliyetlerini desteklemektedir. Encrochat uygulaması açıldığında uygulamanın programı ve verileri işlemci tarafından mesaj alıp göndermek üzere Realm'den RAM'e çekilmektedir. Kullanıcının hazırladığı mesaj uygulamanın kendisi için ilk olarak RAM'de tutulmakta, gönder komutu verildiğinde ise uygulama bu mesajı şifrelemekte ve Encrochat sunucusuna iletilmek üzere telsiz çipine (radio chip) ve antenine göndermektedir. Mesaj, Encrochat sunucusundan geçtikten ve alıcının mesaj kuyruğuna ulaştıktan sonra, alıcı cihaz açılıp Encrochat uygulaması çalıştırıldığında alıcı cihaza ulaşmış olmaktadır. Sonrasında

uygulama güncellemesi görünümünde bir Truva atı (Trojan) yazılımı hazırlayarak bunu tüm Encrochat kullanıcılarına güncelleme bildirimi olarak göndermiştir. Söz konusu sızma yazılımı, kullanıcıların güncellemeyi indirmesi üzerine cihazlarda depolanmış halde bulunan (silinmediği takdirde son 7 gün içindeki iletişimini kapsayan) tüm verileri (1. Aşama) ve ayrıca bu andan itibaren kullanıcıların hazırladıkları mesajları (2. Aşama) toplayarak Fransız polisine aktarmıştır.[15] Verilere sağlanan erişim sayesinde Encrochat cihazlarının IMEI numaraları, kullanıcı adları, mesajlar, görseller, meta veriler (tarih, saat, okuma durumu), notlar, adres defteri, şifreler, WiFi ağları, konum bilgileri gibi veriler toplanmıştır.[16]

Encrochat şirketi kolluğun sızma girişimini başlangıçta bir uygulama hatası olarak değerlendirip bir güncelleme ile çözmeye çalışmış olsa da cihazlar tekrar kötü amaçlı yazılımla hedef alınarak bu defa kilit ekranı şifreleri değiştirilmiştir.[17] 12-13 Haziran 2020 gecesi Encrochat şirketinin kolluk kuvvetlerinin sisteme sızdığını fark ederek kullanıcılarına artık cihazların güvenliğini garanti edemediklerini bu nedenle cihazların hemen kapatılıp fiziksel olarak imha edilmesini tavsiye eden bir uyarı mesajı göndermesi üzerine uygulanan adli tedbire son verilmiştir.[18]

Operasyon sonucu elde edilen ilk bulgulara göre 66 binin üzerinde Hollanda menşeli SIM kartın sistemde kayıtlı olduğu, Fransa'daki cihazların %63.7'sinin suç faaliyetlerinde kullanıldığı, kalan cihazların ise kısmen pasif durumda olduğu veya henüz değerlendirme konusu yapılmadığı sonucuna varılmıştır.[19] 2023 yılı Haziran sonu verilerine göre Encrochat operasyonu sonucunda;

- Operasyonun yürütüldüğü Fransa ve Hollanda da dahil olmak üzere dünya genelinde 197'si yüksek profil olmak üzere toplamda 6.558 kişi yakalanmıştır. Yargılamalar sonucunda mahkûm edilen sanıklara toplamda 7.134 yıl hapis cezası verilmiştir.
- Operasyon sonucunda 739,7 milyon Euro nakit paraya el konulmuş, 154,1 milyon Euro değerinde varlık ve banka hesapları dondurulmuştur.
- Yüksek miktarda uyuşturucu maddeye (30,5 milyon hap kimyasal uyuşturucu, 103,5 ton kokain, 163,4 ton esrar, 3,3 ton eroin) el konulmuştur.
- Ayrıca 271 adet gayrimenkule, 971 adet motorlu araca, 83 adet tekne ve 40 uçağa el konulmuştur.

alıcı cihaz şifreli mesajı deşifre etmekte ve mesajı RAM hafızasına almaktadır. Burada mesaj, alıcının gönderici için belirlediği takma isimle birleştirilmekte, mesaj ekranda gösterilmekte veya diğer alıcılara gönderilmek için hazırda tutulmaktadır. Uygulama veya cihaz kapatıldığında mesaj, silinmediği takdirde, Realm'e gönderilmektedir(...) Encrochat'e yerleştirilen gizli yazılımın amacı mesajların cihazlardan çekilmesidir. Diğer bir deyişle mesajlar, göndericinin cihazından çıktıktan sonra ya da alıcının cihazına ulaşmadan önce ele geçirilmemektedir. Nitekim mesajların kolluk görevlileri tarafından ele geçirildiklerinde şifresiz olmaları da bu tespiti desteklemektedir. Dolayısıyla mesajlar henüz gönderen cihazda şifrelenmeden ve alıcı cihazda deşifre edilmeden önce ele geçirilmiştir. Kolluk sunucusuna (C3N) çekilen veriler gönderici ve alıcı cihazlardaki verilerin bir kopyasıdır. Şu halde, 1. Aşamada elde edilen veriler Realm'den kopyalanarak kolluk sunucusuna aktarılırken, 2. Aşamada elde edilen veriler, bu sırada Encrochat uygulaması açık olduğundan, gönderici cihazın RAM hafızasında tutulan verilerden kopyalanarak kolluk sunucusuna aktarılmıştır. Daha önce de belirtildiği üzere, uygulama açık olduğu sürece veriler RAM hafızasında depolanmakta ve Realm'e gönderilmemektedir(...) Özetle, gönderici cihaz açısından mesajlar cihazın RAM hafızasında depolanan, gönder komutu verilmediği için henüz şifrelenmemiş ve dolayısıyla alıcıya aktarılmamış olan verilerin kopyalanarak kolluk sunucusuna aktarılması suretiyle; alıcı cihaz açısından ise alıcı cihaza vararak alındı olarak işaretlenen ve o anda Realm'de mevcut olan verilerle (ör. göndericiye verilen ad ile) ya da uygulamanın açılmasıyla birlikte RAM'de bulunan verilerle paketlenmiş halde bulunan (dolayısıyla göndericiden alıcıya aktarım halinde bulunmayan, fakat aktarım sonrasında depolanmış) verilerin kopyalanarak kolluk sunucusuna aktarılmasıyla suretiyle ele geçirilmiştir. Şu halde verilerin aktarım (akış) halindeyken (real time data) değil depolanmış haldeyken (stored data) ele geçirildiği kabul edilmelidir." A, B, D & C v. Regina [2021] EWCA Crim 128, paras. 148-153. Belirtmek gerekir ki İngiliz mahkemesinin teknik açıdan yapmış olduğu bu ayırım uygulanan tedbirin İngiliz hukuku bakımından nitelendirmesini değiştirmemektedir. Zira 2016 Investigatory Powers Act kanununa göre bir iletişim ister 4. maddenin 4(a) fıkrasına göre anlık/akış halinde olsun ister 4(b) fıkrasına göre aktarım öncesi ya da sonrası depolanmış/durağan olsun iletişimin dinlenmesi (interception of communication) tedbiri kapsamında kabul edilir. Türk hukuku açısından ise bu teknik ayırım hukuki nitelendirmeyi değiştirmekte, anlık/akış halinde iletişim verilerinin elde edilmesi CMK. md. 135 kapsamına girerken depolanmış/durağan iletişim verilerinin elde edilmesi ise CMK. md. 134 kapsamına girmektedir.

[15] A, B, D & C v. Regina [2021] EWCA Crim 128, para. 12. Ayrıca bkz. Milana Pisaric, 'Encrypted Mobile Phones' (2021) 11 Thematic Conference Proceedings of International Significance 189.

[16] Landgericht Berlin, I Az.: 525 KLs 8/22 279 Js 30/22 StA Berlin, T: 19.12.2024, para. 78.

[17] Sky News, 'Encrochat: What it is, who was running it...' (n 6).

[18] Kate Cox, "Police Infiltrate Encrypted Phones, Arrest Hundreds in Organized Crime Bust", ArsTechnica, 2 July 2020, Erişim adresi: https://arstechnica.com/tech-policy/2020/07/police-infiltrate-encrypted-phones-arrest-hundreds-in-organized-crime-bust/, Erişim Tarihi: 29.12.2024.

[19] BGH, Beschluss vom 2. März 2022 – 5 StR 457/21, para. 8.

- Son olarak 923 ateşli silaha, 21.750 mermiye ve 68 patlayıcıya el konulmuştur.[20]

Europol ve Eurojust destekli operasyonda elde edilen verilere göre Encrochat Hollanda, İspanya, Birleşik Krallık, Almanya ve İtalya'da çok sayıda ciddi suçun işlenmesinde kullanılmıştır.[21] Encrochat'in 122 ülkede kullanıcısının olduğu, yalnızca Almanya'da 4600 kullanıcısının bulunduğu tespit edilmiştir.[22] Ayrıca Encrochat cihazlarının satışından 56 milyon Euro gelir elde eden üç Hollanda vatandaşı örgüt üyeliği ve kara para aklama suçlamalarıyla tutuklanmıştır.[23]

Encrochat'in Türkiye'de bulunan kullanıcılarına ilişkin veriler Türk yetkili makamları ile de paylaşılmıştır. İstanbul Cumhuriyet Başsavcılığı bünyesinde yürütülen uyuşturucu madde ticareti soruşturması kapsamında İstanbul merkezli 9 ilde düzenlenen Kafes-44 adlı operasyon ile Türkiye'de ve Avrupa'da ele geçirilen 37 ton uyuşturucu maddeden sorumlu oldukları tespit edilip gözaltına alınan 43 şüpheliden 23'ü tutuklanmış, 20'si hakkında adli kontrol tedbiri uygulanmış, suç örgütüne ait toplam değeri yaklaşık 20 milyar TL olan 147 arsa, 56 konut, 8 apartman, 74 işyeri, 53 lüks araç, tekne, 53 şirketin hisseleri, 64 banka hesabı, 7 kiralık kasa ile çok sayıda ziynet eşyası, nakit para ve soğuk cüzdana el konulmuştur.[24]

Operasyonun etkileri yeni soruşturmalara yol açarak Avrupa çapında organize suç ağlarının çözülmesine katkı sağlamıştır.[25] Örneğin, Encrochat'in kullanıldığı Almanya'yı ilgilendiren uyuşturucu madde ithali ve ticareti suçlarına ilişkin veriler Europol tarafından Alman Federal Kriminal Dairesi'ne (*Bundeskriminalamt*) iletilmiş, Siber Suçlar Dairesi de (*Zentralstelle zur Bekämpfung der Internetkriminalität*) kimliği belirsiz kişiler hakkında bu suçları işlemek ve planlamaktan soruşturma başlatmıştır. İşbu soruşturma kapsamında 2 Haziran 2020 tarihinde Fransız makamlarına hitaben bir Avrupa Soruşturma Emri düzenlenerek Almanya'yı ilgilendiren Encrochat verilerinin Alman makamlarına nakli ve ceza yargılamasında delil olarak kullanılması için izin talep edilmiştir. Fransız makamları her iki talebi de 2000 tarihli Cezai İşlerde Adli Yardımlaşma AB Sözleşmesi ve 2001 tarihli Ek Protokolü uyarınca 13 Haziran 2020 tarihinde kabul etmiştir.[26] İlgili Encrochat verileri Almanya Savcılığı Siber Suçlar Dairesi tarafından faillerin bulunduğu yer savcılıklarına iletilmiş, açılan çok sayıda ceza davasında delil olarak kullanılmıştır.[27]

Encrochat Operasyonu, sadece suç örgütlerine yönelik bir darbe değil, aynı zamanda şifreli iletişim sistemlerinin nasıl kötüye kullanılabileceğini ve bu tür teknolojilere karşı alınabilecek önlemleri göstermesi açısından da önemli bir örnek teşkil etmiştir. Bu operasyon, Fransa ve Hollanda'nın liderliğinde yürütülse de birçok Avrupa ülkesinin yanı sıra Europol ve Eurojust gibi kuruluşların da desteğiyle küresel bir boyut kazanmıştır. Eurojust'un koordinasyonunda 13 ülke bu süreçte yer almıştır.[28] Operasyonun neticesinde makalenin sonraki bölümünde bahsedileceği gibi ele geçirilen verilerin delil olarak kullanılmasının hukukiliği yeni tartışmalara yol açsa da Encrochat operasyonu, organize suç örgütleriyle mücadelede hem teknoloji hem de uluslararası iş birliğinin önemi açısından etkili bir örnek olmaktadır.

[20] Europol, "Dismantling Encrypted Criminal Encrochat Communications Leads to Over 6,500 Arrests and Close to EUR 900 Million Seized", 2023, Erişim adresi: https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochat-communications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized, Erişim Tarihi: 27.11.2024.

[21] BGH, Beschluss vom 2. März 2022 – 5 StR 457/21, para. 11.

[22] Thomas Wahl, "AG: Encrochat Data Can, in Principle, Be Used in Criminal Proceedings", eucrim, 2023, 3, s. 264.

[23] NL Times, "Dutch trio made millions by selling EncroChat encrypted phones to criminals", 28.02.2024, Erişim adresi: https://nltimes.nl/2024/02/28/dutch-trio-made-millions-selling-encrochat-encrypted-phones-criminals, Erişim Tarihi: 28.07.2025.

[24] TRT Haber, "Kafes-44 Operasyonunda 23 Şüpheli Tutuklandı", 24.02.2024, Erişim Adresi: https://www.trthaber.com/haber/turkiye/kafes-44-operasyonunda-23-supheli-tutuklandi-839849.html Erişim Tarihi: 07.08.2025.

[25] Europol, "Dismantling Encrypted Criminal Encrochat Communications", 2023.

[26] BGH, Beschluss vom 2. März 2022 – 5 StR 457/21, paras. 21, 22.

[27] Söz konusu ceza davalarının künyesi için bkz. BGH, Beschluss vom 2. März 2022 – 5 StR 457/21, para. 24.

[28] Eurojust, "Encrochat: Dismantling of an encrypted network used by criminal group", 2020, Erişim Adresi: https://www.eurojust.europa.eu/ar2020/7-casework-crime-type/72-encrochat-dismantling-encrypted-network-used-criminal-groups, Erişim tarihi: 27.11.2024.

III. Encrochat Operasyonu'nun Cezai Konularda AB İş Birliği Hukuku Altyapısı

Çalışmamızın bu aşamasında Encrochat operasyonu kapsamında başvurulan üç önemli AB iş birliği hukuku enstrümanı olan ortak soruşturma ekibi, spontane bilgi paylaşımı (ihbar) ve Avrupa soruşturma emri kurumları hakkında genel bilgiler verdikten sonra bu yöntemlerin Encrochat operasyonunda nasıl kullanıldığına ve soruşturmaya nasıl fayda sağladığına değineceğiz.

A. Ortak Soruşturma Ekipleri

Sınır aşan suçlarla etkili mücadelede geleneksel adli iş birliği yöntemlerinin sınırları, Avrupa Birliği (AB) düzeyinde daha dinamik ve esnek araçlara olan ihtiyacı ortaya çıkarmıştır. Bu bağlamda, Ortak Soruşturma Ekipleri (*Joint Investigation Teams* – JITs, bundan böyle JIT olarak anılacaktır), özellikle sınır aşan organize suçlar, terörizm, insan kaçakçılığı ve mali suçlar gibi karmaşık yapılarla mücadelede kullanılan ileri düzey bir iş birliği modeli olarak geliştirilmiştir.[29] JIT'leri kısaca birden fazla ülkenin adli ve kolluk makamlarının belirli bir amaç ve süre için oluşturdukları, eş zamanlı operasyonları ve delil paylaşımını mümkün kılan geçici soruşturma birimleri olarak tanımlamak mümkündür.[30]

İlk kez 1999 tarihli AB Tampere Zirvesi'nde sınır aşan suçlarla mücadelede öncelikli bir araç olarak gündeme gelen JIT'ler 29 Mayıs 2000 tarihli AB Cezai Konularda Karşılıklı Adli Yardım Sözleşmesi'nin 13. maddesiyle hukuki zemine oturtulmuş, fakat söz konusu hükmün yürürlüğe girmesindeki gecikmeler sebebiyle aynı düzenlemeler ilk olarak 13 Haziran 2002 tarih ve 2002/465/JHA sayılı Ortak Soruşturma Ekiplerine Dair AB Konseyi Çerçeve Kararı ile daha işlevsel bir forma kavuşmuştur.[31]

JIT'lere dair hukuki düzenlemeleri JIT'lerin uygulamadaki etkinliğini artıracak kurumsal altyapısı ve diğer kurumlar ile olan iş birliği mekanizmalarının oluşturulması takip etmiştir. Bu bağlamda örneğin AB Ceza Adaleti İş Birliği Ajansı (*European Union Agency for Criminal Justice Cooperation* – Eurojust) uygulamada JIT kurulmasına teknik destek sağlamakta, operasyonel koordinasyonu kolaylaştırmakta ve çeşitli kalemlerde mali destek sunmaktadır.[32] Ayrıca JIT'lerin etkinliğini artırmak amacıyla 2005'te kurulan Ulusal JIT Uzmanları Ağı, her yıl düzenlenen toplantılarla ülkeler arası deneyim paylaşımı sağlamaktadır. Bu ağın sekreterliği 2011 yılından bu yana Eurojust bünyesinde yürütülmektedir.[33]

Öte yandan AB Kolluk İşbirliği Ajansı (*European Union Agency for Law Enforcement Cooperation* – Europol), JIT'lere istihbarat, analiz, teknik ve mali destek sağlamakta, özellikle siber suçlar ve uyuşturucu kaçakçılığı gibi alanlarda uluslararası veri tabanlarını kullanarak olaylar arasındaki bağlantıları ortaya çıkarmaktadır.

[29] EMPACT 2023 RESULTS isimli raporda, göçmen kaçakçılığı ile mücadelede 8, insan ticareti ile mücadelede 39, sentetik uyuşturucular/yeni psikoaktif maddelerin kaçakçılığı suçuyla mücadelede ise 1 JIT'ın aktif bir şekilde çalışmaya devam ettiğini açıklanmıştır. EMPACT, "2023 Results Factsheets", 4–6, 16, Erişim adresi: https://www.europol.europa.eu/publications-events/publications/empact-2023-results-factsheets#downloads, Erişim Tarihi: 21.07.2025.

[30] AB Konseyi Çerçeve Kararı 2002/465/JHA, md. 1.

[31] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, art. 13; Council Framework Decision 2002/465/JHA of 13 June 2002 on joint investigation teams. İşbu Çerçeve Karar 18 Şubat 2022 tarihinde yürürlüğe giren Directive (EU) 2022/211 of the European Parliament and of the Council of 16 February 2022 amending Council Framework Decision 2002/465/JHA, as regards its alignment with Union rules on the protection of personal data adlı Direktif ile yapılan eklemelerle birlikte AB kişisel verileri koruma düzenlemeleri ile uyumlu hale getirilmiştir.

[32] 2018 tarihli Eurojust Tüzüğü'ne göre bu kurumsal destek; seyahat ve konaklama giderleri, delil taşıma, tercüme ve adli uzmanlık gerektiren hizmetlerin finansmanı gibi pek çok alanı kapsamaktadır. Regulation (EU) 2018/1727 of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust) OJ L 295, 21.11.2018. Ayrıca, ekip üyelerinin teknik donanım eksikliklerini gidermek amacıyla Eurojust tarafından çeşitli ekipmanlar (mobil yazıcı, akıllı telefon, laptop vb.) da geçici olarak temin edilebilmektedir. Eurojust, Joint Investigation Teams Practical Guide, 2021, 73-74, Erişim Adresi: https://www.eurojust.europa.eu/publication/jits-practical-guide, Erişim Tarihi: 29.12.2024. Ayrıca bkz. Nusret Alper Pazarcıklı, 'Avrupa Birliği Cezai Konularda Adli İşbirliği Birimi ile Avrupa Birliği Savcılığı Ofisi Arasındaki İşbirliği İlişkisi' (2024) 14(1) Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi, 290.

[33] Eurojust, JITs Network, Erişim Adresi: https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/jits-network, Erişim Tarihi: 16.07.2025. Ayrıca Sabine Gless, Internationales Strafrecht, 3rd edn, Helbing Lichtenhahn Verlag, Basel 2021, 188–189.

Europol görevlileri, 2016 tarihli Tüzük kapsamında JIT faaliyetlerine doğrudan katılabilmektedirler.[34] Bu şekilde Europol'ün varlığı, operasyonel kararların eşgüdüm içinde alınmasını ve anlık bilgi paylaşımını da mümkün kılmaktadır.

JIT yalnızca ulusal makamların bir araya gelmesiyle oluşturulan bir model değildir. Örneğin Avrupa Başsavcılığı Ofisi (*European Public Prosecutor's Office* – EPPO, bundan böyle EPPO olarak anılacaktır), özellikle AB bütçesine yönelik dolandırıcılık ve sınır aşan mali suçlar alanında yürüttüğü soruşturmalarda JIT modelinden faydalanmaktadır. Esasen EPPO, AB üyesi devletlerin delege savcılarından oluşan ulus üstü bir birim olarak bir nevi sürekli JIT oluşumudur. Ancak AB üyesi olmakla birlikte EPPO'ya katılmayan devletler ile ya da JIT öngören bir uluslararası sözleşmeye taraf olmakla birlikte AB üyesi olmayan devletlerle yapılacak ortak soruşturmalarda EPPO, JIT kurabilme yetkisine sahiptir.[35] Öte yandan Uluslararası Ceza Mahkemesi de örneğin Ukrayna'da işlenen savaş suçları kapsamında Litvanya, Polonya ve Ukrayna arasında kurulan JIT'e dâhil olmuştur.[36] Bu tür örnekler, JIT'lerin sadece AB içinde değil aynı zamanda uluslararası kuruluşlarla da entegre biçimde çalışabileceğini göstermektedir.

JIT'lerin en önemli avantajlarından biri hız ve esnekliktir. Klasik adli yardımlaşma (*mutual legal assistance* – MLA) talepleri, resmi yazışmalar ve çeviri prosedürleri nedeniyle zaman alıcıdır. Oysa JIT'lerde bu tür bürokratik işlemler azaltılarak üyeler birbirleriyle doğrudan iletişim kurabilmekte, dolayısıyla karşılıklı güven daha etkin ve hızlı tesis edilmekte,[37] ve zaman baskısı olan soruşturmalarda daha hızlı sonuç alınabilmektedir.[38] Esneklik açısından da JIT'ler klasik sistemlere göre daha uyarlanabilir bir yapıya sahiptir. Operasyon planları olayların akışına göre değiştirilebilmekte ve JIT üyeleri anlık gelişmelere karşı hızlı refleks gösterebilmektedir.

Delil toplama ve kullanım süreçlerinde de JIT'lerin önemli avantajları bulunmaktadır. Ekip üyeleri birlikte delil toplayabildiği için hem ulusal hukuklarında gösterilen usule uygun işlem yapılmakta hem de diğer ülkelerin bu delillere doğrudan erişimi sağlanmaktadır. Bu durum, mükerrer ifade alma gibi gereksiz tekrarların önüne geçmektedir. Ayrıca JIT anlaşmalarında, elde edilen verilerin taraf ülkelerde kullanılabilmesini sağlayan hükümler yer almakta ve bu sayede delil transferi için ayrıca adli yardımlaşma talebinde bulunma zorunluluğu ortadan kalkmaktadır.[39]

JIT'ler maliyet etkinliği bakımından da klasik yöntemlere kıyasla avantajlıdır. JIT'ler sayesinde tekrarlayan işlemler azalmakta, zaman ve emek israfı önlenmektedir. Eurojust ve diğer AB kuruluşlarının JIT'lere sağladığı mali destek ulusal makamlar için bir diğer avantaj olup bu şekilde devletler, sınır aşan iş birliği maliyetlerinin ulusal bütçeler üzerindeki etkisini azaltmaktadır.[40] Örneğin, 2017–2019 arasında 37 JIT'in masrafı Eurojust tarafından finanse edilmiş ve toplamda 1 milyon Euro'dan fazla kaynak aktarılmıştır.[41]

[34] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) [2016] OJ L135/53, art 4(1)(d).

[35] EPPO, Note on EPPO's Participation in JIT's, 22.07.2021, 2021/LS-28/JC-RR-LDM, 2–3; Eurojust, Joint Investigation Teams: Practical Guide, 2021, 17 vd.

[36] Yang, S. ve Tan, Y., The Joint Investigation Team in Ukraine: Challenges and Opportunities for the International Criminal Court, European Papers, C. 8, S. 3, 2023, 1122.

[37] Eurojust, Supporting judicial authorities in the use of joint investigation teams factsheet, 2020, 2, Erişim Adresi: https://www.eurojust.europa.eu/sites/default/files/assets/2020_06_jits_factsheet_en.pdf Erişim Tarihi: 21.12.2024.

[38] UNODC & Eurojust, UNODC and Eurojust promote Joint Investigation Teams for Central Asian countries, 4–6 Haziran 2024, Viyana, Erişim adresi: https://www.unodc.org/unodc/en/organized-crime/CASC/en/news/2024/unodc-and-eurojust-promote-joint-investigation-teams-for-central-asian-countries.html Erişim Tarihi: 27.04.2025.

[39] Eurojust, Joint Investigation Teams: Practical Guide, Luxembourg: Publications Office of the European Union, 2021, s. 8-10. Ayrıca bkz. Avrupa Birliğinde Cezaî Konularda Uluslararası Adlî İş Birliği, Adalet Bakanlığı Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü Yayını, Editör: Ahmet Ulutaş, Ankara: Eylül 2021, s. 114.

[40] Eurojust, Supporting Judicial Authorities Factsheet, 2020, 3, Erişim Adresi: https://www.eurojust.europa.eu/publication/supporting-judicial-authorities-use-joint-investigation-teams-factsheet, Erişim Tarihi: 27.12.2024.

[41] Eurojust, Third JIT Evaluation Report, 2020, 22, Erişim Adresi: https://www.eurojust.europa.eu/publication/third-jit-evaluation-report Erişim Tarihi: 29.12.2024.

JIT'lerin organize suçlarla mücadelede ne kadar etkili olabileceğini gösteren birçok örnek operasyon gerçekleştirilmiştir. Örneğin, Pachtou Operasyonu 2005 yılında Europol'ün desteğiyle, Fransa, İtalya, İngiltere, Yunanistan ve Türkiye'nin katılımıyla yapılan bir operasyonudur. Binlerce yasadışı göçmenin AB'ye kaçak olarak sokulmasını sağladıkları şüphesiyle 30'dan fazla adreste arama yapılmış toplamda 53 şüpheli yakalanmıştır.[42] Bir diğer örnek ise, "Shylock" operasyonudur. Dünya çapında Microsoft Windows çalıştıran en az 30.000 bilgisayarı etkileyerek çevrimiçi bankacılık sistemlerine giren bir yazılım olan Shylock'un siber saldırıları 2014 yılında, İngiltere, ABD, İtalya ve Türkiye'nin yer aldığı bir ortak soruşturma ekibi tarafından başarıyla engellemiştir.[43] Bu örnek, JIT'lerin sadece geleneksel suçlarla değil, aynı zamanda siber suçlarla mücadelede de ne kadar etkili olduğunu ortaya koymaktadır.

Nihayet Encrochat operasyonunda JIT yöntemine Fransa ve Hollanda adli ve kolluk makamlarının katılımıyla başvurulmuştur. Fransa'daki Encrochat soruşturması Mart 2020'de "Emma 95" kod adıyla Jandarma bünyesinde kurulan 60 personelden oluşan görev gücü tarafından Lille soruşturma hâkimi gözetiminde yürütülmüştür. Daha sonra Fransız Jandarması 10 Nisan 2020 tarihinde Eurojust'ın rehberliğinde ve Europol'ün de katılımıyla Hollanda kolluk birimleriyle JIT anlaşması yapmıştır.[44] Operasyonun Hollanda ayağı "Lemont" kod adıyla yüzün üzerinde kolluk görevlisinin katılımı ile ve soruşturma hâkiminin gözetiminde yürütülmüştür.

Fransa ve Hollanda yetkili makamları arasında bir JIT oluşturulması ve JIT'in etkin kullanımı ve koordinasyonu noktasında AB ajansları önemli bir rol üstlenmiştir. Başta Eurojust, bünyesinde gerçekleştirilen 9 JIT koordinasyon toplantısı kapsamında tüm ekibi güvenli bir ortamda bir araya getirmiş, paralel veya bağlantılı soruşturmaları tespit etmiş, potansiyel yetki çatışmalarını çözüme kavuşturmuş, en elverişli adli iş birliği aracının ne olacağına karar vermiş, bu kapsamda özellikle çok sayıda ASE'nin düzenlenmesini koordine etmiştir.[45] Öte yandan ortak operasyonun bilgi merkezini oluşturan Europol, sahip olduğu teknik ve personel kapasitesi ile JIT ortaklarından anlık olarak gelen milyonlarca mesaj ve verinin teyidini (*cross-check*) ve kapsamlı analizini gerçekleştirmiş, JIT ortakları ile birlikte verilerin ilgili ülkelere gönderimini ve koordinasyonunu sağlamıştır.[46]

Bu kapsamda, elde edilen bilgi ve istihbarat -operasyon tarihinde yürürlükte bulunan- spontane bilgi paylaşımına dair Kolluk Kuvvetleri Arasında Bilgi ve İstihbarat Paylaşımını Kolaylaştırmaya İlişkin Konsey Çerçeve Kararı[47] uyarınca şüphelilerin bulunduğu –JIT'e dahil olmayan Almanya, İngiltere, İsveç ve Norveç gibi- diğer AB ülkelerinin kolluk birimleri ile de paylaşılarak bu ülkelerde organize suç örgütleri tarafından işlenen öldürmeye teşebbüs dahil şiddet suçları, yolsuzluk ve büyük çaplı uyuşturucu madde kaçakçılığı suçlarına yönelik çok sayıda soruşturmanın başlatılmasına ön ayak olmuştur.[48]

[42] Eurochannel, 3 Famous Police Operations by Europol, Erişim Adresi: http://www.eurochannel.com/en/3-Famous-Police-Operations-by-Europol.html Erişim Tarihi: 21.12.2024.

[43] Europol, Global Action Targeting Shylock Malware, Erişim Adresi: https://www.europol.europa.eu/media-press/newsroom/news/global-action-targeting-shylock-malware Erişim Tarihi: 21.12.2024.

[44] Eurojust, Annual Report 2020: Criminal Justice Across Borders in the EU, 29, Erişim Adresi: https://www.eurojust.europa.eu/publication/annual-report-2020-criminal-justice-across-borders-eu#:~:text=In%202020%2C%20Eurojust%20has%20registered,drugs%20worth%20EUR%203%20billion Erişim Tarihi: 21.12.2024.

[45] Eurojust, Annual Report 2020, n 37, 29.

[46] Ibid.

[47] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006. İşbu Çerçeve Karar'ın yerini 22.05.2023 tarihinde yürürlüğe giren Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA almıştır.

[48] Europol, Dismantling of an Encrypted Network Sends Shockwaves Through Organised Crime Groups Across Europe, Erişim Adresi: https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe Erişim Tarihi: 21.12.2024.

B. Spontane Bilgi Paylaşımı

Avrupa Birliği'nin birlik vatandaşlarının güvenliğinin sağlanması genel stratejisi kapsamında başvurduğu önemli araçlardan biri de kolluk iş birliğinin temelini oluşturan bilgi ve istihbarat paylaşımıdır.[49] Güncel ve doğru bilgi ve istihbarata zamanında erişim suçun ve suç faaliyetlerinin kolluk makamları tarafından başarıyla tespit edilmesi, önlenmesi ve soruşturulması noktasında kritik önem arz etmektedir.[50] Bu doğrultuda hazırlanan Direktif ile AB üye devletlerinin yetkili kolluk makamları bir katalog suçun[51] tespiti, önlenmesi, soruşturulması noktasında faydalı olacağına inandığı ilgili ve gerekli bilgi ve istihbaratı bir talebe gerek olmaksızın ilgili üye devlet yetkili kolluk makamıyla paylaşacaktır.[52] Bu yönüyle spontane bilgi paylaşımı, geleneksel talepname (*letters rogatory*, *letter of request*) bazlı iş birliği araçlarından (ör. adli yardımlaşma) farklı olarak, bir üye devletin kendi inisiyatifiyle diğer üye devlete bilgi vermesini ifade etmektedir.[53] Belirtmek gerekir ki spontane bilgi paylaşımı diğer mevcut uluslararası veya AB adli iş birliği enstrümanlarının uygulanmasına engel değildir;[54] dolayısıyla adli makamların yetkilerinin önüne geçilmez. Daha ziyade diğer adli iş birliği yöntemlerini tamamlayan ve destekleyen bir araç niteliğinde görülmektedir.

Bilgi ve/veya suçla ilgili istihbarat kavramı kolluk makamları nezdindeki her tür bilgi ve veriyi kapsamaktadır. Bu kapsama, kamu ve özel hukuk tüzel kişiler nezdinde olup da zorlayıcı bir tedbire başvurulmasına gerek olmaksızın kolluk makamlarının erişimine açık olan her türlü bilgi ve veri de dâhildir.[55] Üye devletler, bilgi veya istihbarat elde etmek için zorlayıcı tedbirlere başvurmak zorunda olmamakla birlikte böyle bir tedbirin uygulanması suretiyle elde edilen bilgi ve istihbaratı birbiriyle paylaşacaklardır.[56]

Bir delilin spontane bilgi paylaşımı yoluyla elde edilmesi ile adli yardımlaşma yoluyla elde edilmesi arasında, delil değeri, usulî güvenceler ve yargısal denetim bakımından bazı yapısal farklılıklar bulunmaktadır. Spontane bilgi paylaşımı, çoğu zaman kolluk makamları arasında önceden alınmış bir adli merci talebine dayanmaksızın gerçekleşen ve esas itibarıyla istihbari nitelik taşıyan bir iş birliği biçimi olup, bu tür bilgilerin tek başına mahkûmiyete esas delil olarak kullanılabilmesi güçtür.[57] Özellikle dijital deliller bakımından, spontane bilgi paylaşımı yoluyla elde edilen verilerin ilk elde edilme aşamasına, muhafaza zincirine (chain of custody) ve veri bütünlüğünü güvence altına alan teknik işlemlere ilişkin bilgilerin çoğu zaman eksik, belirsiz ya da gizli olması, savunmanın delilin güvenilirliğini etkin biçimde denetlemesini güçleştirmektedir.[58] Bu doğrultuda, ayrıca, kolluk iş birliği kapsamında paylaşılan bilgi ve istihbaratın yargı mercileri önünde delil olarak kullanılabilmesi veya, adli yardımlaşmada olduğu gibi, paylaşım amacı dışında başka bir amaçla kullanılabilmesi ancak bilgiyi sağlayan devletin açık rızası ile mümkündür.[59] Buna karşılık

[49] Directive (EU) 2023/977, 2. gerekçe paragrafı.

[50] Directive (EU) 2023/977, 4. gerekçe paragrafı.

[51] Bu suçlar Avrupa Yakalama Emri'ne dair FD 2002/584/JHA md. 2(2)'de belirtilmiştir.

[52] Directive (EU) 2023/977, art. 7(2). Spontane bilgi paylaşımı ayrıca Budapeşte Siber Suçlar Sözleşmesi, md. 26 ve Europol Veri İşleme ve Aktarma Kodu uyarınca da yapılabilmektedir. Eurojust, 5th Annual Sirius EU Electronic Evidence Situation Report, 2023, 64–65, Erişim Adresi: https://www.eurojust.europa.eu/publication/sirius-eu-electronic-evidence-situation-report-2023, Erişim Tarihi: 24.12.2024.

[53] Direktif, üye devlet kolluk makamlarına bilgi ve istihbarat paylaşma noktasında doğrudan bir yükümlülük öngörmemiştir. Boudewijn de Jonge & Barry de Vries, Data-Driven Investigations in a Cross-Border Setting: Experiences from the Netherlands, eucrim, 3/2024, 218.

[54] Directive (EU) 2023/977, art. 1(2).

[55] Directive (EU) 2023/977, arts 2(4), 2(7).

[56] Directive (EU) 2023/977, art 1(3)(a).

[57] Anna-Maria Osula, 'Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data', Masaryk University Journal of Law and Technology, (2015) 9, p. 52, 53., UNODC, Trafficking in Persons & Smuggling of Migrants: Guidelines on International Cooperation, 2010, p. 25. Ancak bu durum bir bilginin kolluk makamları arası spontane bilgi paylaşımı yoluyla elde edilmiş olmasının onun kullanımını otomatik olarak hukuka aykırı hale getirdiği şeklinde anlaşılmamalıdır. Mutual Legal Assistance Manual, Council of Europe, Belgrade, 2013, p. 9, 11.

[58] Fran Casino, Claudia Pina, Pablo López-Aguilar, Edgar Batista, Agusti Solanas ve Constantinos Patsakis, 'SoK: Cross-Border Criminal Investigations and Digital Evidence', *Journal of Cybersecurity,* Volume 8, Issue 1, 2022, p. 8.

[59] Directive (EU) 2023/977, arts 1(4), 4(5)(f).

adli yardımlaşma, uluslararası sözleşmelere ve iç hukuka dayalı olarak belirli usul kuralları ile yargısal denetim mekanizmalarına tabi bir iş birliği rejimi sunduğundan, bu yolla elde edilen delillerin belgelendirilmesi ve denetlenmesi mümkün olmakta; süreç şeffaf bir biçimde yürütülmekte, söz konusu deliller bizatihi yargılamada kullanılmak üzere paylaşılmakta ve bu nedenle hukuki güvenilirliği ve delil değeri daha yüksek kabul edilmektedir. Bu da, AİHM'in adil yargılanma hakkının ayrılmaz bir unsuru olarak gördüğü, savunmanın delilin kaynağını, elde edilme yöntemini ve güvenilirliğini sorgulayabilmesi hakkını güvence altına alarak delilin hukuka uygun olarak kullanılabilirliğini sağlar.[60] Bu çerçevede uygulamadaki baskın görüş, spontane bilgi paylaşımının soruşturmayı başlatmaya veya yönlendirmeye elverişli olduğunu kabul etmekle birlikte, mahkûmiyete esas alınacak delillerin kural olarak adli yardımlaşma kanalıyla elde edilmesinin hem hukuki güvenlik hem de adil yargılanma hakkı bakımından daha uygun olduğu yönündedir.[61]

Şifreli iletişim verilerinin elde edilmesi amacıyla bir soruşturma tedbirine başvuran devlet makamları başka bir devletin bu içeriklerden haberinin olmadığına inanıyorsa, bu durumda o ülkenin ASE veya MLA yoluna başvurması beklenemeyeceğinden, ilgili tedbiri bizzat uygular ve sonucunda o ülkeye soruşturma başlatabilmesi için gönüllü olarak haber verir.[62] 27 Mart 2020 tarihinde Encrochat operasyonunu yürüten JIT de, bu doğrultuda, Europol'ün kullandığı SIENA (*Secure Information Exchange Network Application* - Güvenli Bilgi Değişim Ağı Uygulaması) sistemi üzerinden Üye Devletlerin kolluk birimlerine gönderdiği mesajda analiz amacıyla ve JIT üyelerinin rızasına bağlı olmak kaydıyla ceza soruşturması ve kovuşturmalarında kullanmak amacıyla Encrochat verilerini gönderebileceklerini belirtmiştir. Alman BKA ve Frankfurt savcılığı söz konusu veriler ile ilgilendiklerini belirtmişler ve 3 Nisan - 28 Haziran 2020 tarihleri arasında Almanya'da kullanılan cihazlara ait verilere erişim sağlamışlardır.[63] İlgili veriler aynı usulle ayrıca Norveç, İsveç ve Birleşik Krallık ile de paylaşılmıştır.[64]

C. Avrupa Soruşturma Emri

Encrochat soruşturmasında Europol üzerinden Almanya'ya gönderilen verilerin incelenmesi sonucunda uyuşturucu madde ticareti, silah ticareti, karapara aklama, örgüt kurma gibi çok sayıda ağır suçun Almanya'da işlendiği kanaatine varılmış ve soruşturma başlatılmıştır.[65] Verilerin polisiye kanallardan paylaşımı sonrasında 2 Haziran 2020 tarihinde Frankfurt savcılığı Fransız makamlarına hitaben düzenlediği ASE ile Fransız makamlarının elinde bulundurduğu Almanya'yı ilgilendiren Encrochat verilerinin paylaşılmasını ve ceza yargılamasında kullanılmasına izin verilmesini talep etmiştir. Her iki talep de 13 Temmuz 2020 tarihinde Fransız hâkimi tarafından onaylanmıştır.[66] Bu başlık altında Avrupa Soruşturma Emri'nden (bundan böyle ASE olarak anılacaktır) genel hatlarıyla bahsedeceğiz.

ASE, AB ülkeleri arasında, daha önce yalnızca delil dondurma taleplerini düzenleyen Çerçeve Kararı'nın[67]

[60] ECtHR, Yalçınkaya v. Türkiye, 26.09.2023, Başvuru No: 15699/20, paras. 324-241.

[61] UNODC, Trafficking in Persons & Smuggling of Migrants: Guidelines on International Cooperation, 2010, p. 17, 25., Council of Europe Cybercrime Convention Committee, Report on Practices regarding spontaneous information and MLA, (2025), p. 10.

[62] Eurojust, 5th Annual Sirius EU Electronic Evidence Situation Report, 2023, 64, Erişim Adresi: https://www.eurojust.europa.eu/publication/sirius-eu-electronic-evidence-situation-report-2023, Erişim Tarihi: 24.12.2024.

[63] CJEU (Grand Chamber), Judgment of 30 April 2024, paras. 24–25, Erişim Adresi: https://curia.europa.eu/juris/document/document.jsf?text=&docid=285365&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=156936, Erişim Tarihi: 21.12.2024.

[64] Eurojust, Annual Report 2020, 30.

[65] BGH, Beschluss vom 2. März 2022 – 5 StR 457/21, para. 19.

[66] Bundesgerichtshof (BGH), Beschluss vom 2. März 2022 – 5 StR 457/21, Erişim Adresi: https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2022/2022038.html, Erişim Tarihi: 21.03.2025.

[67] Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence, Official Journal L 196, 2003, 2.8.

ve yalnızca mevcut olan delillerin paylaşılmasını düzenleyen Avrupa Delil Emri Çerçeve Kararı'nın[68] kapsam ve işlevlerini genişleten ve birleştiren bir adli iş birliği yöntemidir.[69] ASE aracılığıyla bir Üye Devlet yetkili makamı (düzenleyen makam) yürütmekte olduğu ceza soruşturması veya kovuşturması kapsamında bir diğer Üye Devlet yetkili makamına (yerine getiren makam) henüz toplanmamış bir delili toplamasını ve/veya toplamış olduğu bir delili paylaşmasını emredebilir (md. 1/1). ASE'nin temel amacı, sınır ötesi iş birliğini artırmak ve delil toplama işlemlerini standart bir çerçeveye oturtmaktır. Düzenleyen adli makam bu emri re'sen düzenleyebileceği gibi savunma hakkının kullanılması kapsamında şüpheli, sanık veya müdafiin istemiyle de düzenleyebilir (md. 1/3).

ASE kapsamında bir başka AB üyesi devlette elde edilebilecek bilgiler şunlardır: yerine getiren devletin elinde bulunan veya bir suç soruşturması veya kovuşturması amacıyla kendi hukukuna göre elde edebileceği bilgi ve deliller, yerine getiren makamın bir ceza soruşturması veya kovuşturması çerçevesinde doğrudan erişebileceği adli veya polisiye veri tabanlarında depolanan bilgiler, tanık, bilirkişi, mağdur, şüpheli veya sanığın ya da üçüncü bir kişinin dinlenmesi, yerine getiren devlet hukukuna göre kısıtlayıcı (zorlayıcı) nitelikte olmayan herhangi bir soruşturma tedbiri, belirli bir telefon numarasına veya IP adresine aboneliği bulunan kişilerin kimlik tespitinin yanı sıra; tutuklunun geçici nakli, video- veya telekonferans aracılığıyla dinleme, bankacılık ve finansal hesap ve faaliyet bilgilerin elde edilmesi, kontrollü teslimat, gizli soruşturmacı tedbiri, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi gibi tedbirler özel olarak düzenlenmiştir (madde 22, vd.).

ASE, JIT kurulması ve bu kapsamda delil toplanması ve paylaşılması durumları haricinde kalan her türlü soruşturma tedbirinin uygulanması için düzenlenebilir (md. 3). İlgili soruşturma tedbirinin yerine getiren ülkede uygulanması amacıyla bir ASE düzenlenebilmesi için bu soruşturma tedbiri için düzenleyen ülke hukukunda aranan şartların mevcut olması gerekir (madde 6/1-b).

ASE Direktifi sınır ötesinde uygulanacak telekomünikasyon yoluyla yapılan iletişimin denetlenmesi (interception of telecommunications)[70] tedbiri rejimini ilgili kişinin bulunduğu devletin teknik yardımına ihtiyaç bulunup bulunmamasına göre ikiye ayırmıştır. Dinlenecek kişinin bulunduğu ülke devletinin teknik yardımı gereken durumlarda ASE düzenlenmesi gerekli olup yerine getiren devlet direktifin 11. maddesindeki ret sebeplerini (ör. basın ve ifade özgürlüğü, *ne bis in idem*, katalog suçlar, vd.) ve ek olarak yerine getiren devletin iç hukukuna göre aynı şartlarda söz konusu tedbire başvurulup başvurulamayacağını değerlendirecektir (md. 30/5). Buna karşın dinlenecek kişinin bulunduğu üye devletin teknik yardımına ihtiyaç duyulmayan hallerde tedbiri uygulayan devletin ülkesinde tedbir uygulanan devlete haber verme yükümlülüğü bulunmaktadır (md. 31). Bildirimi alan üye devletin yetkili makamları, uygulanan iletişimin denetlenmesi tedbirinin iç hukuktaki benzer bir davada onaylanmayacak olması halinde tedbirin uygulanmasını önleyebileceği ya da

[68] Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters, Official Journal L 350, 2008, 30.12. Bu Çerçeve Karar, Regulation (EU) 2016/95 of the European Parliament and of the Council of 20 January 2016 repealing certain acts in the field of police cooperation and judicial cooperation in criminal matters ile yürürlükten kaldırılmıştır. Bu Düzenleme ise 22.02.2016 tarihinde yürürlükten kalkmıştır.

[69] European Parliament and Council of the European Union, Directive 2014/41/EU regarding the European Investigation Order in criminal matters, Official Journal L 130, 2014, 1–2.

[70] Belirtmek gerekir ki ASE Direktifi kapsamında iletişimin denetlenmesi "interception of telecommunications" tedbiri içerisine hangi yöntemlerin girdiğine dair Üye Devletler arasında üzerinde uzlaşı bulunan bir tanım bulunmamakla birlikte, trafik verisinin ve IP adresinin tespiti konuları hariç olmak üzere, bir telekomünikasyon bağlantısı kullanmak suretiyle meta veriye, içerik verisine, konum verisine, iletişim içeriğine, depolanmış veriye veya anlık iletişim verisine erişim sağlayan soruşturma tedbirlerinin, sızma (spyware) veya uzaktan arama (remote search of computers) gibi yöntemlerin iletişimin denetlenmesi tedbiri kapsamında değerlendirildiği görülmektedir. EuroCoord, EIO Code of Best practices – Proposals for 100 Best Practices, March 2019, paras. 301, 360, 361. Bu doğrultuda, somut olay açısından Alman Ceza Muhakemesi Kanunu'nun 100a maddesinde öngörülen telekomünikasyon yoluyla yapılan iletişimin denetlenmesi (Telekommunikationsüberwachung) tedbirinin de anlık iletişimin gerek klasik olarak dinlenmesini gerek bir yazılım yüklemek (spyware) suretiyle kaynağında izlenmesini gerekse cihazda depolanmış iletilen iletişim içeriklerinin ele geçirilmesini kapsadığı ilgili ABAD kararında belirtilmiştir. Bkz. Court of Justice of the European Union, Criminal proceedings against M.N. (Case C-670/22), ECLI:EU:C:2024:372, 30 April 2024, para. 14. (Bundan böyle CJEU, Criminal proceedings against MN olarak anılacaktır.)

uygulanan tedbire son verebileceği gibi, uygun olduğu hallerde, tedbir suretiyle elde edilmiş olan materyallerin kullanılmamasına ya da belirleyeceği şartlar altında kullanımının sınırlandırılmasına karar verebilir (md. 31/3).

Yerine getiren devlet, direktifin 11. maddesinde sayılan engellerden birinin mevcudiyeti halinde ASE'ni her zaman ihtiyari olarak reddedebilir.[71] Ret yetkisinin kullanılmaması halinde ASE'nin derhal yerine getirilmesi gerekmektedir (madde 13/1).

IV. Hukuki Sorunlar ve Görüşler

Encrochat verilerinin ceza yargılamalarında delil olarak kullanılabilirliğine ilişkin hukuki sorunları ulusal hukuk ve AB hukuku düzleminde olmak üzere iki ayrı bölümde ele alacağız. Bu doğrultuda konuyu, Encrochat verilerinin (A) ulusal hukuka uygunluğu ve delil değeri kapsamında (1) Fransa'da uygulanan soruşturma tedbirinin hangi ülke hukukuna göre değerlendirileceği, (2) adli yardımlaşma yoluyla aktarılan delillerin ulusal ceza yargılamasında kullanılabilmesinin hukuki dayanağı (a) adli iş birliği hukuku kapsamında uluslararası hukukun temel ilkeleri yönünden, (b) kamu düzeni yönünden, (c) adli iş birliği hukuku düzenlemeleri yönünden, (d) anayasal çekirdek alan koruması ve ölçülülük ilkesi yönünden ve (e) ceza muhakemesi kuralları bakımından; (B) Avrupa Birliği hukukuna uygunluğu ve delil değeri kapsamında ise (1) bilgi ve delilin AB hukukundaki gerekliliklere aykırı olarak elde edilmesinin delilin ulusal ceza yargılamasında şüpheli aleyhine dışlanmasını gerektirip gerektirmediği, bu doğrultuda (a) ASE Direktifi 'ne göre ASE'nin yalnızca hâkim tarafından düzenlenmesi gerekip gerekmediği, (b) Alman savcılığınca düzenlenen ASE'nin Direktif 'in 6/1 maddesine uygunluğu, (i) şüpheli ve sanık haklarının korunup korunmadığı, (ii) gereklilik ve orantılılık şartlarına uyulup uyulmadığı ve (iii) ilgili soruşturma tedbirine iç hukukta aynı koşullarda başvurulabilirlik yönünden ele alacağız. Mahkeme karar ve görüşleri sırasıyla Alman Federal Yargıtayı (*Bundesgerichtshof* – BGH, bundan böyle BGH olarak anılacaktır), Avrupa Birliği Adalet Divanı (ABAD), Berlin Eyalet Mahkemesi (*Landesgericht* Berlin - LG) ile doktrindeki görüşler çerçevesinde ele alınmıştır. Ayrıca gerekli açıklama ve dayanakların yeterli bir şekilde ortaya konulmaması nedeniyle yapılan bir bireysel başvuruyu esasına girmeden reddeden Alman Anayasa Mahkemesi (*Bundesverfassungsgericht* – BverfG) kararındaki tespitlere de yeri geldiğince değineceğiz.

A. Encrochat Verilerinin Ulusal Hukuka Uygunluğu ve Delil Değeri

1. Fransa'da Uygulanan Soruşturma Tedbirinin Alman Makamlarınca Fransız Hukukuna Göre Değerlendirilip Değerlendirilmeyeceği Sorunu

Bu soru Encrochat davasındaki temel hukuki sorunlardan biri olmamakla birlikte, yabancı bir ülkede elde edilip de başka ülkeye aktarılan delillerin hangi ülke hukukuna uygunluğunun araştırılacağı bir öncül mesele olarak BGH tarafından açıklığa kavuşturulmuştur. BGH bu konuda kendi içtihadına atıfta bulunarak "yabancı ülkede uygulanan tedbirin (Alman makamları tarafından) yabancı hukuktaki standartlara uygunluğunun incelenmesinin mümkün olmadığını, kaldı ki delil aktarımı için de böyle bir ön koşul bulunmadığını..." söyleyerek bu konuda kesin bir prensip ortaya koymuştur. BGH devamla, "bir delil değerlendirme yasağının varlığının münhasıran ulusal hukuka göre belirlenecek bir konu olduğunu" ve "Fransız ve Alman hukuklarında belli bir soruşturma tedbirine başvurulması için gerekli olan koşullar arasındaki farklılığın ulusal

[71] Zorunlu ve ihtiyari ret nedenlerine yer veren 2002/584/JI sayılı Avrupa Yakalama Emri'ne dair Çerçeve Karar'ın aksine Avrupa Soruşturma Emri Direktifi'nde öngörülen ret nedenleri yalnızca ihtiyari niteliktedir. Nathalie Laurer, Informationshilfe im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, Nomos, Baden-Baden, 2018, 167.

yargılamada delilin değerlendirilmesi aşamasında telafi edileceğini" söylemiştir.[72] Şu hâlde her ulusal makam kullanacağı delilin hukuka uygunluğu bakımından yalnızca kendi hukukunu uygulayarak bir değerlendirme yapacaktır.

2. Adli Yardımlaşma Yoluyla Aktarılan Delillerin Ulusal Ceza Yargılamasında Kullanılabilmesinin Hukuki Dayanağı

BGH hukuki sorunun iç hukuka göre ele alınacağını belirledikten sonra aktarılan Encrochat verilerinin delil değerinin iç hukukta hangi kurala göre belirleneceği ile ilgilenmiştir. BGH'ya göre, Encrochat verilerinin ve genel olarak bir delilin ister bizatihi ülkede ister adli yardımlaşma yoluyla elde edilmiş olsun, ceza yargılamasında kullanılabilmesinin Alman hukukundaki yasal dayanağı Alman CMK. md. 261'de düzenlenen "hâkimin delilleri serbestçe değerlendirme ilkesi"dir.[73] Adli yardımlaşma kapsamında yabancı ülkeden açıkça ceza yargılamasında kullanılmak amacıyla aktarılan verilerin ceza yargılamasında kullanılabilmesine ilişkin olarak bunun ötesinde ayrıca özel bir hukuki dayanağa gerek bulunmamaktadır.[74]

BGH'ya göre her ülkenin kendi anayasal ve ceza yargılaması düzeni ve buna göre belirlenmiş koruma tedbirleri bulunduğundan ve kendi hukukuna göre bir tedbir uygulayan yabancı ülkeden Alman hukukunu uygulaması kural olarak beklenemeyeceğinden bu durum tek başına delil değerlendirme yasağı olarak kabul edilemez.[75] BGH'ya göre, Alman hukukunda Alman makamlarınca verilen kararlara göre değil de başka bir üye devletin kendi hukukuna göre verdiği bir kararla elde edilen delillerin adli yardımlaşma yoluyla aktarımına dayanan bilgilerin delil olarak kullanımı yasağı ancak; (a) uluslararası hukukun temel bir ilkesinin ihlali gibi adli iş birliği hukukunda kabul edilen bir sebepten, (b) kamu düzenine aykırılıktan, (c) adli iş birliği hukuku düzenlemelerinden veya iç hukukta elde edilen delillerde olduğu gibi (d) doğrudan anayasadan veya (e) diğer ceza muhakemesi hukuku kurallarından kaynaklanabilir.[76] Encrochat verilerinin Almanya'da delil olarak kullanılabilirliği meselesi aşağıda bu kriterler ışığında ele alınmıştır.

a. Adli İş Birliği Hukuku Kapsamında Uluslararası Hukukun Temel İlkeleri

BGH uluslararası adli iş birliği hukukunun temel ilkeleri kapsamında devlet egemenliği ve insan hakları ilkeleri bağlamında üstünkörü bir inceleme yapmıştır. Devlet egemenliği yönünden BGH, aktarılan verilerin kullanım amacının sınırlanıp sınırlanmadığına ve Almanya'ya sirayet eden sınır ötesi iletişim dinleme nedeniyle Alman makamlarına haber verme yükümlülüğüne bakmıştır. Buna doğrultuda, Fransız makamlarının somut olayda aktardıkları verilerin Almanya'da kullanım amacını sınırlamamış olmasını, diğer bir deyişle ceza yargılamalarında kayıtsız şartsız kullanılmasına onay vermiş olmasını başka bir devletin Almanya'nın egemenlik haklarına müdahalesi bulunmadığı şeklinde yorumlamıştır.[77] Öte yandan BGH, Fransız makamlarının ASE Direktifi md. 31'e aykırı olarak Almanya'daki iletişimi Alman makamlarından izinsiz ve Alman makamlarına haber vermeden izlemiş olmalarını -bu maddenin genel olarak üye devletlerin egemenlik haklarını koruduğunu kabul etmesine rağmen-[78] devlet egemenliği ilkesine aykırı olarak değerlendirmemiştir. BGH'ya göre bunun nedeni, Alman makamlarının kendilerine aktarılan Encrochat verileri sonrasında ülkelerinde uygulanan iletişimin dinlenmesi tedbirine karşı sessiz kalmış olmalarıdır. Dolayısıyla bu sessizlik söz konusu tedbire onay verildiği şeklinde yorumlanmıştır.[79]

---

[72] Thomas Wahl, Cornelia Riehle & Anna Pingen, News – European Union, eucrim – The European Criminal Law Associations' Forum, No. 1, 2022, 37; Andrea Leonhardt, Die Europäische Ermittlungsanordnung in Strafsachen, Springer, Wiesbaden, 2017, 92.

[73] BGH, Beschluss vom 2. März 2022 – 5 StR 457/21, para. 25.

[74] Ibid, para. 74

[75] Ibid, paras. 72, 73.

[76] Ibid, para. 32.

[77] Ibid, para. 33.

[78] Bkz. Ibid, para. 40.

[79] Ibid, para. 40.

Ayrıca insan hakları ilkeleri yönünden de BGH, somut olayda bireyi koruyucu nitelikteki bir uluslararası hukuk kuralına açık bir aykırılığın mevcut olmadığını belirtmiştir.[80]

b. Kamu Düzeni Yönünden

BGH kamu düzeni kriterini somut olaya uygularken Encrochat sisteminin yapısal özelliklerine odaklanmıştır. Fransız makamları açısından Encrochat, elde edilen verilerin analizine göre, özellikle ciddi miktarda uyuşturucu madde ticareti olmak üzere münhasıran suç faaliyetlerini kolaylaştırmak amacıyla oluşturulmuş, polis erişimine karşı çeşitli önlemleri barındıran gizli bir suç ağı niteliğindedir. Dolayısıyla kullanıcılar, normal bir satış kanalından elde edilemeyecek böyle bir telefonu ciddi bir tutar ödeyerek satın almakla salt bu nedenle kara para aklama, uyuşturucu madde veya silah ticareti gibi organize suçların şüphelisi haline gelirler. Her bir kullanıcıya sirayet eden bu suç şüphesi nedeniyle, şüpheden ari sebepsiz bir kitlesel izlemeden, kitlesel veri değerlendirmesinden ve dolayısıyla istihbari bir tedbirden bahsedilemez.[81] Söz konusu ağır suçların işlendiğini gösterir somut suç şüphesi ve delil durumu karşısında devletin anayasal olarak vatandaşını koruma görevi ve suçla etkin mücadele ödevi gereğiyle Encrochat verilerinin belli bir zaman dilimi içinde elde edilmesine yönelik (Fransız) hâkim kararıyla ve hâkim gözetimde gerçekleştirilen işlemde kamu düzenine aykırılık bulunmamıştır.[82]

c. Adli İş Birliği Hukuku Düzenlemeleri Yönünden

Alman yüksek mahkemesi içtihatları bir adli iş birliği hukuku düzenlemesine aykırılığın delil değerlendirme yasağını doğurabilmesi için ihlal edilen kuralın birey haklarını koruyan bir niteliğe sahip olmasını aramaktadır.[83] Bu bağlamda BGH, iletişimin dinlendiği ülkenin teknik desteğine gerek olmadan uygulanan sınır ötesi iletişim dinleme tedbiri kapsamında ilgili ülkeye haber verme yükümlülüğünü düzenleyen ASE Direktifi md. 31/3 hükmünün Alman hukukundaki karşılığı olan Uluslararası Adli İş Birliği Kanunu (IRG) md. 91g/6 hükmünü ele almıştır. İlgili hükme göre:

"Almanya Federal Cumhuriyeti'nin teknik yardımına ihtiyaç duyulmadan telekomünikasyon yoluyla yapılan iletişimin sınır ötesi gözetimine ilişkin bir talep söz konusuysa ve söz konusu soruşturma tedbiri benzer bir iç hukuk vakasında onaylanmayacak idiyse, talepte bulunan üye devletin yetkili makamına derhal, en geç talebin alınmasından itibaren 96 saat içinde aşağıdaki hususlar bildirilmelidir:

1. *Gözetlemenin gerçekleştirilemeyeceği veya sona erdirilmesi gerektiği,*
2. *Gözetlenen kişi Almanya Federal Cumhuriyeti'nin yetki alanında bulunduğu sırada toplanan bilgilerin kullanılamayacağı veya yalnızca belirli koşullar altında kullanılabileceği; bu koşullar ve bunların gerekçeleri de bildirilmelidir."*

Mahkemeye göre buradaki haber verme yükümlülüğü genel itibariyle esasen devlet egemenliği ve yabancı ülkede veri kullanımı ile ilgilidir ve bireysel koruma yönü zayıftır. Bu nedenle ihlali durumunda iç hukukta otomatik olarak delil yasağına yol açmaz.[84] Kaldı ki bu maddeye göre, iletişimin Almanya'da dinlenmesi nedeniyle Alman makamlarının bu tedbirin aynı koşullar altında Almanya'da benzer davalarda uygulanamayacak olması halinde 1 ve 2 numaraları bentlerde yer alan sonuçları Fransa'ya bildirmesi gerekirdi. Ancak BGH, Alman makamlarının somut olayda söz konusu tedbire sessiz kalmasını bu tedbire onay verildiği şeklinde yorumlamıştır.[85]

[80] Ibid, para. 33.

[81] Ibid, para. 37.

[82] Ibid, para. 36.

[83] Ibid, para. 38.

[84] Ibid, paras. 38-41.

[85] Ibid, para. 40.

d. Anayasal Çekirdek Alan Koruması Ve Ölçülülük İlkesi Yönünden

BGH, Encrochat verilerinin yargılamada kullanılabilirliğini değerlendirirken, kişisel verilerin korunmasına ilişkin anayasal güvenceleri dikkate almış ve özellikle özel yaşamın çekirdek alanına yönelik müdahalelerin mutlak delil yasağını doğurabileceğini belirtmiştir. Ancak bu koruma yalnızca bireyin en mahrem alanına –örneğin dini iç dünyasına, aile içi duygusal ilişkilerine veya kişinin kendi alanı gibi kamusal denetime kapalı yönlerine– yönelik dinlemeleri kapsarken suç planlaması ve icrası çerçevesinde yapılan iletişimler bu çekirdek alan korumasının dışında tutulmaktadır. Encrochat yazışmalarının içeriği değerlendirildiğinde, bunların bireysel mahremiyeti değil, organize uyuşturucu ticareti faaliyetlerini konu aldığı, dolayısıyla çekirdek alan müdahalesi oluşturmadığı sonucuna varılmıştır.[86]

BGH bir bilginin yargılama sırasında delil olarak kullanılmasının bir temel hakka (ör. telekomünikasyonun gizliliği hakkı, özel hayatın gizliliği haklarına) müdahale niteliğinde olacağı durumlarda anayasal çekirdek alan koruması (hakkın özü) ve ölçülülük denetiminin yapılmasını zorunlu görmektedir. Fakat ölçülülük testi bakımından mahkeme, iç hukuktaki bir ceza soruşturması kapsamında bizatihi ülkede veya adli yardımlaşma yoluyla yabancı bir ülkede elde edilen deliller ile bir yabancı ülke makamının kendi ulusal ceza soruşturması kapsamında elde etmiş olup da başka bir ülkeye aktardığı (spontane bilgi paylaşımı) bilgilerin o ülkede delil olarak kullanılabilirliğini adli iş birliği hukuku ve AB düzenlemelerindeki özellikler[87] nedeniyle birbirinden ayırmaktadır.[88] Bir defa ilk iki durumda Alman adli makamlarının kendi yargı yetkilerine dayanarak yürüttükleri bir soruşturma kapsamında aldıkları bir soruşturma tedbiri kararı mevcut olacağından temel haklara yapılacak müdahalelerin kontrolü ve sınırlandırılması zaten söz konusu tedbire karar verildiği anda Al.CMK hükümlerinin doğrudan ve lafzen uygulanması suretiyle (ör. özel ağırlığa sahip suçlar veya nitelikli şüphe seviyesi ile) yapılacaktır. Ancak somut olayda olduğu gibi, başka bir ülkenin (Fransa'nın) kendi yargı yetkisine dayanarak yürüttüğü bir ceza soruşturması kapsamında kendi hukukuna göre temel haklara müdahale ettiği bir durumda söz konusu sınırlandırma yapılamıyorsa –ve bu karar karşılıklı tanıma ilkesi gereği – ya da yabancı bir devlet işlemi olması nedeniyle Alman Anayasası açısından bir müdahale olarak kabul edilemeyip-[89] Almanya'da esas yönünden değerlendirilemiyorsa- iki ülkenin müdahale koşulları arasındaki olası farklılıkların delillerin (Almanya'da) kullanıldığı aşamada –ve bu aşamadaki bilgi ve delil duruma göre- dengelenmesi gerekmektedir. İşte bu son durumda BGH söz konusu dengelemeyi yaparken, müdahale derecesi benzer ağırlıkta olan soruşturma tedbirlerinde ölçülülüğü sağlayan kullanım kısıtlamalarının temel düşüncesinden yararlanılabileceğini belirtilmiş ve somut olaydaki tedbirin ağırlığını ve her türlü olası dezavantajın önlenmesi gerekliliğini de dikkate alarak en yüksek koruma seviyesine sahip olan kullanım kısıtlaması olarak online aramalar ve ortam dinlemesi yoluyla elde edilen delillerin hangi amaçlarla kullanılabileceğini düzenleyen Al.CMK md. 100e, paragraf 6 hükmünü ölçülülük testi bakımından esas almıştır.[90] Böylece BGH, ilk iki durumda –tedbire karar verileceği andaki şüphe, bilgi ve delil durumuna göre- doğrudan

[86] Ibid, paras. 61–64; aynı yönde BVerfG, Beschluss vom 1 November 2024 – 2 BvR 684/22, para. 99.

[87] Mahkeme'nin bu kararında ayrıntısına girmediği adli iş birliği hukuku ve AB düzenlemelerinin özellik yaratan yönü karşılıklı tanıma ilkesidir. AB ceza adalet sisteminde üye devletler arasındaki adli iş birliğinin temelini oluşturan bu ilke, bir devlette hukuka uygun şekilde elde edilen delillerin diğer devletlerce tanınmasını öngörür. Bu ilkenin benimsendiği ASE Direktifi'nin 9. maddesine göre, emri yerine getiren makam ASE'yi normalde kendi iç hukukunda söz konusu işlem için gerekli görebileceği ek formaliteleri talep etmeksizin tanıyacak ve kendi hukukunun temel ilkelerine aykırı olmadığı müddetçe düzenleyen makamın açıkça belirttiği formaliteler ve usuller doğrultusunda yerine getirecektir. Bkz. Kai Ambos, European Criminal Law, CUP, 2018, 457, n. 89; Bernd Hecker, Europäisches Strafrecht, Springer, Heidelberg, 2017, 428, n. 57. Bu bağlamda, bir delilin yalnızca emri yerine getiren devletin iç hukukundaki şekil şartlarına uymaması gerekçesiyle reddedilmesi, karşılıklı tanıma ve güven ilkesini zedeleyici bir tutum olarak değerlendirilmektedir. Ambos, 460, n. 92. Şu hâlde, kendi yargı yetkisine dayanarak bir soruşturma yürüten devletin bu kapsamda delil elde etmeye yönelik aldığı bir tedbir kararı üzerinde, bu karar adli yardımlaşma yoluyla başka bir üye devlette yerine getirilecek olsa da daha fazla denetim yetkisi bulunmaktadır.

[88] BGH, Beschluss vom 2. März 2022 – 5 StR 457/21, paras. 65, 66, 67.

[89] Bu yönde bkz. Frank Peter Schuster, Verwertbarkeit im Ausland gewonnener Beweise im deutschen Strafprozess, Duncker & Humboldt, Berlin, 2006, 243.

[90] BGH, Beschluss vom 2. März 2022 – 5 StR 457/21, paras. 68, 70.

ve lafzen ve tümüyle olaya uygulanabilecek olan bir maddeyi, son durumda –delilin kullanılacağı andaki şüphe, bilgi ve delil durumuna göre- dolaylı olarak ve (ölçülülüğe ilişkin hususlarla sınırlı olarak) kısmen göz önünde bulundurmuştur.

Al.CMK md. 100e, paragraf 6 hükmüne göre, online aramalar (md. 100b) ve ortam dinlemesi (md. 100c) tedbirleri kapsamında elde edilen veriler, bu kapsamda izlenen/dinlenen kişilerin rızası olmaksızın, diğer ceza soruşturmalarında yalnızca bu tedbirlerin uygulanabileceği (katalog) bir suçun aydınlatılması veya böyle bir suçun şüphelisinin yerinin tespit edilmesi amacıyla kullanılabilmektedir.[91] Online arama tedbirinde ölçülülük ilkesini somutlaştıran sınırlayıcı koşul olarak suçun her bir somut olayda özel ağırlığa sahip olması ve olayın başka yollarla aydınlatılmasının ya da şüphelinin yerinin tespit edilmesinin önemli ölçüde zorlaşmış ya da umutsuz olması koşullarına yer verilmiştir (Al.CMK. md. 100b/1-2,3).[92] Dikkat edilirse burada göz önünde bulundurulan hüküm, söz konusu delilin elde edilmesi için (*Beweiserhebung*) gerekli olan şartları (ör. suç şüphesini) değil elde edilen delillerin kullanım (*Beweisverwertung*) amaçlarını düzenlemektedir. Bu doğrultuda BGH, söz konusu kriterleri olaya uygularken tedbirin uygulandığı andaki şüphe durumunu değil delilin kullanıldığı andaki verileri ve bilgi durumu dikkate alarak, mahkûmiyete konu düşük miktarın üzerindeki (somut olayda %70 etkin madde oranına sahip 5kg kokain, %10 etkin madde oranına sahip 3kg esrar) katalogda yer alan uyuşturucu madde ticareti suçunun ağır bir suç olması, söz konusu iletişim içerikleri olmadan olayın aydınlatılmasının mümkün olmaması ve iletişim içeriklerinin özel hayatın çekirdek alanına ilişkin olmaması nedeniyle delil kullanımının ölçülülük ilkesiyle uyumlu olduğuna karar vermiştir.[93]

Ancak BGH ayrıca, söz konusu kriterler yönünden Encrochat verilerinin kullanılabilirliğini "varsayımsal ikame müdahale" (*hypothetischer Ersatzeingriff*) doktrini[94] çerçevesinde delilin elde edilmesine ilişkin hukuki şartlara göre de değerlendirmiştir. BGH'ya göre şayet söz konusu (*ex-post*) veriler baştan itibaren doğrudan bir katalog suçun aydınlatılması amacıyla elde edilmiş olsaydı hukuken kullanılabilir nitelikte olacaklardı. Mevcut durumda, veriler farklı bir müdahale yoluyla temin edilmiş olmakla birlikte, *kullanım anında* (*ex-post*) bu veriler ciddi bir katalog suç şüphesinin aydınlatılmasına hizmet etmekte ve nitelikli şüphe seviyesinin varlığını da bizzat bu veriler ortaya koyabilmektedir. Dolayısıyla, delillerin elde edilme tarzından bağımsız olarak, verilerin kullanımı anındaki hukukî duruma bakıldığında, katalog suça ilişkin nitelikli bir şüphe mevcut olduğundan ve bu şüphe mevcut verilerden hareketle ortaya konulabildiğinden, bu verilerin ceza soruşturmasında kullanılmasına ilişkin hukuka aykırılık söz konusu değildir.[95]

BGH'nın söz konusu hukuki sorunu ele alış tarzı bakımından dikkat çeken noktalar, ölçülülük testi bakımından gerekli olan müdahale unsurunun Alman makamları açısından delilin elde edilmesiyle (*Beweiserhebung*) değil –spontane bilgi paylaşımı nedeniyle- delilin kullanılmasıyla (*Beweisverwertung*) oluştuğu, dolayısıyla müdahalenin ölçülü olup olmadığının bu andaki (*ex-post*) koşullara göre, diğer bir deyişle ilgili tedbirlere başvurulabilecek bir katalog suçun ve buna yönelik nitelikli şüphe seviyesinin varlığı bakımından tedbire karar verildiği andaki değil elde edilen delillerin kullanıldığı andaki bilgi ve delil durumuna göre değerlendirmesidir. Belirtelim ki BGH'nın bu yaklaşımı Alman Federal Anayasa Mahkemesi tarafından anayasaya uygun bulunmuştur. Anayasa Mahkemesi, delil kullanma yasağını sonuçlayacak ihlali çekirdek alana yapılacak müdahaleler ile sınırlamış, bunun dışındaki hukuka aykırılıkların ölçülülük testini geçmesi halinde

[91] Martin Böse, Verwertung im Ausland gewonnenner Beweismittel im deutschen Strafverfahren, ZStW 114, 2002, 92, 148.

[92] BGH, Beschluss vom 2. März 22022 – 5 StR 457/21, para. 69.

[93] Ibid, para. 71.

[94] Bu öğretiye göre, hukuka aykırı bir kamu gücü müdahalesinin, aynı sonucun hukuka uygun yollarla da elde edilebileceği varsayımıyla değerlendirilmesini ifade eder. Bu yaklaşıma göre, müdahalenin şeklen hukuka aykırı olması (ör. arama kararı olmaksızın yapılan aramalar), eğer aynı müdahalenin hukuk düzenine uygun biçimde yapılabilecek olduğu varsayımıyla değerlendirilebiliyorsa, bu durum hukuka aykırılığı ortadan kaldırmasa da ihlalin sonuçlarını etkisiz kılabilir veya mazur görebilir. Christoph Safferling, Strafprozessrecht, 3. Auflage, Heidelberg: C.F. Müller, 2021, § 5 rn. 84 ff.

[95] BGH, Beschluss vom 2. März 2022 – 5 StR 457/21, para. 70.

–ki mahkemeye göre BGH bu testi Al.CMK. md. 100e ve 100b maddelerini olaya kıyasen uygulayarak doğru bir şekilde gerçekleştirmiştir- delil kullanma yasağını sonuçlamayacağını belirtmiştir.[96]

e. Ceza Muhakemesi Kuralları Bakımından

BGH Encrochat kayıtlarının somut davada delil olarak kullanılmasını engelleyecek herhangi bir ceza muhakemesi kuralının bulunmadığını belirtmiştir.[97]

B. Encrochat Verilerinin Avrupa Birliği Hukukuna Uygunluğu ve Delil Değeri

1. AB Hukukunda Öngörülen Koşullara Aykırı Olarak Elde Edilen Bilgi ve Delillerin Ulusal Ceza Yargılamasında Şüpheli Aleyhine Dışlanmayı Gerektirip Gerektirmeyeceği Sorunu

Alman eyalet mahkemelerinin Encrochat verilerini esas alarak verdikleri mahkûmiyet kararları hukukçular arasında tartışmalara yol açmıştır. Söz konusu kararlara esas kitlesel Encrochat verilerinin başta polisiye kanallar aracılığıyla aktarıldığı ve bunu takiben çıkarılan Avrupa Soruşturma Emri ile söz konusu operasyonları Almanya'da yargı denetimi olmaksızın sadece otomatik olarak tasdik etme saikinin güdüldüğü ve özellikle ASE Direktifinin 31. maddesine uyulmamasının delillerin kullanımının hukukiliği üzerinde sonuçlarının olması gerektiği ileri sürülmüştür.[98] Bu iddiaya karşın Alman kolluk makamları, verilerin Alman Federal Polis Dairesi tarafından Europol sunucuları üzerinden çekilmiş olması, Frankfurt savcılığının sonradan ASE düzenlemiş olması ve düzenlenen ASE'nin Encrochat operasyonunu denetleyen Fransız hâkim tarafından yerine getirilmiş olması nedeniyle elde edilen verilerin ceza yargılamasında kullanılabileceğini ileri sürmüştür.[99]

Bu hukuki sorun BGH nezdinde temyiz gerekçesi olarak ileri sürülmemiş olmakla birlikte gerek BGH tarafından gerekse BGH kararına uymayan Berlin Eyalet Mahkemesi'nin bu hukuki sorunu ABAD önüne taşımasıyla birlikte ABAD tarafından ele alınmıştır. Bu noktada ilk olarak BGH'nın yaklaşımını ele aldıktan sonra Berlin Eyalet Mahkemesi'nin ABAD'a yönelttiği sorulara yönelik ABAD görüşünü inceleyeceğiz.

BGH görüşü: Belirttiğimiz üzere ASE düzenlenmeden önce, Fransız ve Alman polis makamları arasındaki veri paylaşımı veya iş birliği sırasında olası bir adli yardımlaşma kurallarına aykırılık BGH nezdindeki temyiz başvurusunda ileri sürülmemiştir. BGH öncelikle ceza muhakemesi amacıyla sınır ötesi bilgi paylaşımının, Cezai Konularda AB Karşılıklı Yardımlaşma Sözleşmesi[100] kuralları kapsamında (md. 7)[101], resmi bir yardım talebi olmadan da mümkün olduğunu ve böyle bir bilgi alışverişinden elde edilen verilerin kullanımı için, ASE ile elde edilen verilere kıyasla daha yüksek bir koşulun aranmadığının ve dolayısıyla delil olarak kullanılmasında bir engel bulunmadığının altını çizmiştir.[102] Ayrıca Fransız makamlarının ASE Direktifi kapsamında Alman makamlarına haber verme yükümlülüğünü (md. 31) ihlal etmesinin delilin kullanılmasını tek başına yasaklayan bir durum olmadığı, nitekim verinin kullanımının –haber veren ülke makamları tarafından- sonradan onaylanmasından da aynı sonucun çıktığı, dolayısıyla açık bir hukuki hatanın bariz olmadığı ifade

[96] BVerfG, Beschluss vom 1 November 2024 – 2 BvR 684/22, para. 99.

[97] BGH, Beschluss vom 2. März 2022 – 5 StR 457/21, para. 76.

[98] Wahl, 'Germany: Federal Court of Justice Confirms...', 37.

[99] Thomas Wahl, Attempt for Second Reference for Preliminary Ruling in Encrochat Case, eucrim, No. 1, 2024, 44.

[100] Council of the European Union, Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, Official Journal C 197, 12 July 2000, 1–23.

[101] *"Madde 7: Spontane bilgi paylaşımı 1. Üye Devletlerin yetkili makamları, ulusal hukuklarının sınırları dâhilinde, cezalandırılması veya ele alınması bilginin verildiği tarihte alıcı makamın yetkisi dâhilinde olan suçlar ve madde 3(1)'de atıfta bulunulan hukuk kurallarının ihlalleri ile ilgili olarak, bu yönde bir talep olmaksızın, bilgi paylaşımında bulunabilirler. 2. Bilgi veren makam, ulusal hukuku uyarınca, bu bilgilerin alıcı makam tarafından kullanılmasına ilişkin koşullar koyabilir. 3. Alıcı makam bu koşullarla bağlı olacaktır."* Spontane bilgi paylaşımı konusu, taraf olduğumuz uluslararası adli iş birliği sözleşmelerindeki ilgili hükümlere paralel olarak, Türk hukukunda 6706 sayılı kanunun 7/2 maddesinde düzenlenmiştir: Adlî mercilerce, yürütülen bir soruşturma veya kovuşturma kapsamında başka bir devletin ceza soruşturması başlatmasına neden olabilecek bilgilerin öğrenilmesi hâlinde, talep olmaksızın bu bilgiler, ilgili devlete gönderilmek üzere Merkezî Makama bildirilebilir.

[102] Wahl, 'Germany: Federal Court of Justice Confirms...', 37.

edilmiştir.[103] Kaldı ki, gerek adli iş birliği hukukunun sistematiğinden gerekse kanun gerekçesinden, sınır ötesi iletişim dinlemesi tedbiri kapsamında ilgili ülkeye haber verme yükümlülüğünün bireyi delilin haber verilmesi gereken ülkede (olay açısından Almanya'da) kullanımına karşı değil, haber vermesi gereken ülkede (olay açısından Fransa'da) kullanımına karşı koruduğu sonucunun çıktığı kabul edilmiştir.[104] BGH, Fransız veya Alman makamlarının, sanıkların bireysel haklarını koruyan kuralları kasıtlı veya sistematik şekilde aşmaya çalıştığına dair somut veya ikna edici bir delil bulunmamasını da gerekçe olarak kullanmıştır.[105] Sonuç olarak BGH ilgili Encrochat verilerinin mevcut durumda ağır suçların yargılanmasında delil olarak kullanılabileceğine karar vermiştir.[106]

ABAD görüşü: İşbu hukuki sorun BGH kararı doğrultusunda karar veren Almanya'daki çoğu eyalet mahkemesinin aksine konuyu ayrıca AB hukuku bağlamında da ele alan Berlin Eyalet Mahkemesi tarafından bu konuda AB hukukunun yorumlanması amacıyla ABAD'a yöneltilmiştir.[107] İşbu hukuki sorunla bağlantılı olan sorular ve ABAD'ın yorumu şu şekildedir:

a. ASE Direktifi'ne Göre ASE'nin Yalnızca Hâkim Tarafından Düzenlenip Düzenlenemeyeceği Sorunu

ABAD, ASE Direktifi'nde ASE düzenlemeye yetkili makamların tanımlandığını[108] ve bu kapsamda hâkim ve mahkemenin yanı sıra savcıların da ASE düzenleme yetkisine sahip olduğunu ve bunun için herhangi bir makamdan (somut olayda hâkimden) onay almasına gerek olmadığını belirtmiştir. Ancak burada dikkat edilmesi gereken kritik husus, Alman savcılığının düzenlediği ASE'nin konusunun daha önce Fransız makamları tarafından Fransız hukukuna göre elde edilen iletişim verilerinin Almanya'ya aktarılmasına yönelik olması olup sıfırdan delil elde etmek amacıyla iletişimin dinlenmesi tedbirinin uygulanmasına yönelik olmamasıdır. Dolayısıyla elde bulunan mevcut delillerin aktarılmasına yönelik verilecek bir karar için aranan şartlar yeni bir delil elde etmek için verilecek bir karar için aranan şartlara bağlı tutulmamıştır. Nitekim Al.CMK md. 100e/1 uyarınca iletişimin dinlenmesi tedbirine münhasıran mahkeme/hâkim karar verebilirken (*Richtervorbehalt*), 100e/6-1 uyarınca daha önce –hâkim kararıyla- elde edilmiş olan delillerin belirli şartlarda başka amaçlarla (başka ceza yargılamalarında) kullanılması mümkündür. İşte bu son duruma bağlı olarak Alman hukukunda savcılığın daha önce hâkim/mahkeme kararıyla elde edilmiş iletişimin dinlenilmesi verilerini başka bir soruşturmada kullanmak için doğrudan isteyebileceği kabul edildiğinden, AB hukuku bakımından da benzer bir işlem için hâkim onayı olmaksızın savcılığın ASE düzenleyebileceği kabul edilmiştir.[109]

b. Alman Savcılığınca Düzenlenen ASE'nin Direktif 'İn 6/1 Maddesine Uygunluğu Sorunu[110]

Zikredilen hukuki sorunun çözümüyle ilgili uygulanacak norm ASE Direktifinin 6/1 maddesinde şu şekilde yer almaktadır:

> *"Düzenleyen makam, bir ASE'yi yalnızca aşağıdaki koşulların karşılanması durumunda düzenleyebilir:*

[103] Alman Cezai Konularda Uluslararası Adli İş Birliği Kanunu, md. 92b, c.2: "Für einen anderen Zweck oder als Beweismittel in einem gerichtlichen Verfahren dürfen sie nur verwendet werden, wenn der übermittelnde Staat zugestimmt hat". Benzer hüküm Türk hukukunda da yer almaktadır: 6706 sayılı Kanun, md. 6/1: "Adlî iş birliği kapsamında gelen bilgi ve belgeler, gönderen devlet izin vermedikçe, talebe konu olan soruşturma veya kovuşturma ya da infaz işlemleri dışında kullanılamaz."

[104] BGH, Beschluss vom 2. März 2022 – 5 StR 457/21, para. 41.

[105] Ibid, para. 59.

[106] Bundesgerichtshof (BGH), Beschluss vom 2. März 2022 – 5 StR 457/21.

[107] Court of Justice of the European Union, Criminal proceedings against M.N. (Case C-670/22), ECLI:EU:C:2024:372, 30 April 2024, para. 126. (Bundan böyle CJEU, Criminal proceedings against MN olarak anılacaktır.)

[108] Avrupa Soruşturma Emri Direktifi, md. 2/1-c.

[109] CJEU, Criminal proceedings against MN, paras. 69-77.

[110] Ibid, paras. 84-85.

(a) ASE'nin düzenlenmesi, şüpheli veya sanığın hakları dikkate alındığında 4. maddede belirtilen yargılamaların amacı bakımından gerekli ve orantılıdır, ve

(b) Aynı koşullarda iç hukuktaki benzer bir davada ASE'de belirtilen soruşturma tedbir(ler)ine başvurulabilmelidir."

i. **Şüpheli ve Sanık Haklarının Korunup Korunmadığı**

ABAD, Direktif'in 6/1-a maddesinde zikredilen "şüpheli veya sanık haklarının dikkate alınması" koşulu bakımından, ASE Direktifi'nin ilginin temel haklarına saygı gösterilip gösterilmediğinin yargısal denetimini garanti altına aldığını, dolayısıyla ceza muhakemesi sürecinde şüpheli veya sanığın olayın tespitinde baskın etkiye sahip bilgi ve deliller üzerinde etkin bir değerlendirmede bulunamadığı durumlarda ulusal ceza mahkemelerinin adil yargılanma hakkının ihlal edildiğini tespit ederek söz konusu bilgi ve delili dışlamaları gerektiğini belirtmiştir.[111]

Wahl'e göre Encrochat verilerine bir Trojan yazılımı vasıtasıyla erişilmiş olduğu bilinmekle birlikte, bu erişimin teknik ayrıntılarının Fransız makamlarınca askeri sır niteliğinde kabul edilerek açıklanmamış olması, ABAD'ın delil kullanma yasağı için aradığı savunma makamının mahkûmiyete esas alınan bir delil üzerinde etkin bir değerlendirmede bulunamaması koşulunun gerçekleşmesine yol açmıştır. ABAD, aktarılan verilerin bütünlüğünün[112] ve güvenilirliğinin en azından delilin yetkili Alman makamlarına teslim edildiği anda savunma makamı tarafından incelenebilmesi gerektiğini söylemiştir. Ancak Wahl, ABAD'ın savunmanın delil bütünlüğünü/güvenilirliğini test edebilmek için hangi veriye erişiminin mümkün olduğunu ve etkin bir değerlendirme kriterinden uygulamada neyin anlaşılacağını açıkça belirtmemiş olmasının söz konusu hukuki sorunların mahkemeler önünde ortaya çıkmaya devam edeceği şeklinde yorumlamıştır.[113]

Nitekim ABAD görüşü sonrasında Berlin Eyalet Mahkemesi, Encrochat verilerinin yargılamada delil olarak kullanılmasının sanığın adil yargılanma hakkını ihlal ettiğini gerekçeli biçimde ortaya koymuştur. Mahkemeye göre adil yargılanma hakkı yalnızca mahkeme önündeki usuli güvenceleri değil, aynı zamanda delillerin elde edilmesi ve yargılamada kullanılması sürecinde şeffaflığın sağlanmasını da kapsamaktadır. Bu bağlamda, sanığın ve müdafiin delillerin kaynağını, elde ediliş yöntemini ve teknik özelliklerini sorgulayabilmesi gerekir. Ancak somut olayda Encrochat verileri bakımından bu şeffaflık sağlanamamıştır. Gerçekten de Fransız makamları veri toplama sürecini askeri gizlilik gerekçesiyle açıklamaktan imtina etmiş, Alman makamları ise veri analizinde kullanılan teknik altyapıya ilişkin kodları, yöntemleri, filtreleme algoritmalarını açıklamamış, kullanmış olduğu BKA-Tool ve Realm/JSON uzantılı dosya formatlarına erişim izni vermemiştir. Bu nedenle savunma makamı, verilerin nasıl filtrelendiğini, hangi cihazdan ne şekilde alındığını ve hangi teknik altyapının kullanıldığını bilmeden hareket etmek zorunda bırakılmıştır.[114]

Berlin Eyalet Mahkemesi, bu durumu bilgi asimetrisi ve silahların eşitliği (*Waffengleichheit*) ilkesine açık bir aykırılık olarak değerlendirmiştir. Alman Savcılığı; Europol, Alman Kriminal Polis Dairesi ve Fransız Jandarması aracılığıyla veri elde etme ve işleme süreçlerine (chain of custody) dair detaylı teknik bilgiye sahipken, savunmanın bu bilgilere ulaşması sistematik biçimde engellenmiştir. Dahası, Encrochat mesajlarının içeriği

[111] Ibid, para. 131.

[112] Veri bütünlüğünün sağlanması verilerin orijinal halleri üzerinde teknik inceleme yapılması ile mümkün olmaktadır. Görsel veriler açısından, EXIF verileri gibi meta veriler, dosyanın oluşturulma zamanı, yeri ve kullanılan ekipman bilgileri gibi birçok teknik ayrıntıyı içererek verilerin orijinal halleri üzerinde değişiklik yapılıp yapılmadığını belirlemeye yardımcı olur. Bunun yanında, veri bütünlüğü, hash algoritmaları (örn. SHA-1, MD5) ile güvence altına alınır. Aynı veri her defasında aynı hash değerini üreteceğinden, dijital delillerin önce ve sonra alınan hash değerlerinin karşılaştırılması, dosyanın değiştirilmediğini ve delil olarak kullanılabilirliğini teyit edecektir. Aksi halde yazışma ya da görüntü formatında aktarılan veriler fotokopi belgeden farksız olacağı gibi delilin sonradan üretilip üretilmediği veya üzerinde değişiklik yapılıp yapılmadığı da tespit edilemeyecektir. Ersan Şen, Buğra Şahin, Doğa Ceylan, Sky ECC İletişim Sağlayıcısından Elde Edilen Delillerin Hukukiliği, https://sen.av.tr/tr/makale/sky-ecc-iletisim-saglayicisindan-elde-edilen-delillerin-hukukiligi Erişim tarihi: 29 Temmuz 2025.

[113] Wahl (n 86) 43.

[114] Landgericht Berlin, vom 19.12.2024, I Az.: 525 KLs 8/22, 279 Js 30/22 StA Berlin, paras. 185, 323.

çoğu zaman bağlamdan kopuk, karşı yazışmaları eksik, zamansal veya teknik verilerden yoksun şekilde sunulmuştur. Savunma makamı hangi mesajların kime ait olduğunu, hangi cihazdan ne zaman gönderildiğini anlayamamış, bu durum, delillerin doğruluğunu denetlemeyi fiilen imkânsız hale getirmiştir. Mahkemeye göre, adil yargılanma hakkının özü, savunmanın yalnızca suçlamalara cevap vermesini değil, aynı zamanda AİHS. md. 6/3-d uyarınca iddia tanıklarını sorguya çekme hakkı kapsamında, verilerin güvenilirliğine ve bütünlüğüne ilişkin tüm bilgileri (gerçekliği, olayı temsil gücü, elde edilme koşulları, vs.) sorgulayabilmesini gerektirmektedir. Bu sağlanmadığında, delilin güvenilirliği zedelenir ve ceza yargılaması demokratik hukuk devleti ilkesine aykırı şekilde yürütülmüş olur. Bu nedenle, mahkeme Encrochat verilerinin delil değerlendirme yasağı (*Beweisverwertungsverbot*) kapsamında değerlendirilmesi gerektiğine karar vermiştir.[115]

ii. **Gereklilik ve Orantılılık Şartlarına Uyulup Uyulmadığı**

Direktif'in 6/1-a maddesinde yer alan gereklilik ve orantılılık koşulları bakımından ABAD, söz konusu delillerin yerine getiren devlet yetkili makamları (Fransa) tarafından önceden toplanmış olup da düzenleyen devlete (Almanya) aktarıldığını göz önünde bulundurarak, şu yorumları yapmıştır:

1) Gereklilik ve orantılılık şartları 4. maddede belirtilen yargılamanın amaçları (düzenleyen devlet hukukuna göre suç teşkil eden bir eylemin yargılanması amacı) doğrultusunda düzenleyen devlet tarafından düzenleyen devletin iç hukukuna göre incelenecektir.[116]
2) ASE'nin yerine getiren devlet makamlarının daha önce toplayıp da elinde bulundurdukları bir delilin aktarılması amacıyla düzenlenmesi halinde, düzenleyen devlet hukuku aksini gerektirmedikçe, ASE'nin düzenlendiği anda ilgili her bir kişi için ciddi bir suça dair somut olgulara dayalı şüphe şartının aranması gerekli değildir.[117]
3) Yargılama aşamasında adil yargılanma hakkının sağlanması kaydıyla, dinleme tedbirinden elde edilen verilerin bütünlüğünün/güvenilirliğinin tedbirin teknik yönündeki gizlilik nedeniyle doğrulanamaması ASE'nin düzenlenmesine engel değildir. Kaldı ki veri bütünlüğü/güvenilirliği konusu ASE'nin düzenlendiği anda değil, ancak verilerin düzenleyen makama iletilmesinden sonra değerlendirilebilir.[118]

i. **İlgili Soruşturma Tedbirine İç Hukukta Aynı Koşullarda Başvurulabilirlik**

ABAD, Direktif'in 6/1-b maddesinde yer alan, ASE'ye konu soruşturma tedbirine "aynı koşullarda iç hukuktaki benzer bir davada başvurulabilirlik" koşulu yönünden ise yerine getiren devlet makamlarınca daha önceden toplanmış olan bir delilin *aktarılması* için gerekli olan koşulları belirli bir soruşturma tedbiri aracılığıyla henüz toplanmamış bir delilin *toplanması* için gerekli olan koşullardan ayırmaktadır. Somut olayda delilin ilk kez toplanması değil de toplanmış olan delillerin aktarılması söz konusu olduğundan aranacak şartlar düzenleyen devlet hukukundaki delil toplama şartlarına tabi değildir.[119] Ayrıca ABAD, Fransız makamlarının söz konusu delili Almanya'da –ve onların menfaatine- toplamış olmasını bu noktada ilgisiz gördüğü gibi AB hukukundaki karşılıklı güven ve tanıma temel ilkeleri nedeniyle düzenleyen devlet makamlarının aktarılan delilin yerine getiren devlet makamlarınca elde edilme usulünün hukuka uygunluğunu inceleyemeyeceğinin de altını çizmiştir.[120]

[115] Landgericht Berlin, vom 19.12.2024, I Az.: 525 KLs 8/22, 279 Js 30/22 StA Berlin, paras. 282, 284–323.

[116] CJEU, Criminal proceedings against MN, para. 88.

[117] Ibid, para. 89.

[118] Ibid, para. 90.

[119] Münhasıran hâkimin karar vermeye yetkili olduğu tedbirlerde bu koşulun hukuk devletinin kaçınılmaz bir gereği olarak konulduğu, bu koşulun sağlanmamasının delil değerlendirme yasağını sonuçlayacağı yönünde bkz. Schuster, 248-249.

[120] CJEU, Criminal proceedings against MN, paras. 91-100.

Öte yandan ABAD, bu hukuki soruna yönelik ayrıca Direktif'in 31/3 maddesi kapsamında bir yorum yapmıştır. Bu madde iletişimin dinlenebilmesi için kişinin bulunduğu üye devletin teknik yardımına ihtiyaç duyulmayan hallerde ilgili üye devlete haber verme yükümlülüğünü düzenlemektedir. Bu durumda söz konusu tedbirin "haber verilen üye devletin iç hukukunda benzer bir davada onaylanabilir olması" gerekmektedir. Aksi takdirde haber verilen üye devlet, iletişimin dinlenmesi tedbirine engel olabileceği gibi gerekirse ülkesinde elde edilen herhangi bir materyalin ilgili hakkında kullanılmasını yasaklayabilir ya da belirteceği şartlarda kullanımını sınırlayabilir (md. 31/3). ABAD, "tedbirin iç hukuktaki benzer bir davada onaylanabilir olması" koşuluna vurgu yaparak bu koşulun yalnızca ilgili devletin egemenliğini koruma amacıyla konulmadığını ayrıca ilgili tedbirin uygulanabilmesi için gerekli olan şartların incelenmesi suretiyle (birey lehine) sağlanan güvenceleri de temin ettiğini ifade etmiştir.[121] Şu hâlde, iletişimin denetlenmesi tedbiri –AB Temel Haklar Şartı md. 7'de düzenlenen- özel hayata ve haberleşmeye saygı hakkına müdahale teşkil ettiğinden telekomünikasyonun sınır ötesi dinlenmesine ilişkin direktifin 31. maddesinin aynı zamanda ilgili kişinin haklarını korumayı amaçladığı ve bunun elde edilen verilerin haber verilen devletteki ceza muhakemesinde kullanımına da sirayet edeceği belirtilmiştir.[122] Dolayısıyla tedbire maruz kalan kişinin korunması ilgilinin tedbiri uygulayan devletteki (Fransa) yasal imkânlardan faydalanabilirliğine indirgenemeyecektir. Buradaki koruma yükümlülüğü esasen, ilgilinin uygun hukuki denetim yollarına başvurmasının gerektiği haber verilen devlettedir.[123]

Wahl'e ve Schuster'e göre burada kastedilen benzer işlem Alman CMK'nın 100e maddesinde düzenlenen online arama tedbiridir ki bu tedbire başvurulabilmesi için en azından somut bir suç şüphesinin varlığı gerekmektedir.[124] Böylelikle belirsiz bilgi sistemlerine kitlesel erişime müsaade edilmemektedir. Hatta bu tedbire başvurmak için gerekli olan hâkim kararı, diğer soruşturma tedbirlerinde olduğu gibi yerel hâkim tarafından değil, eyalet mahkemesindeki özel yetkili hâkim tarafından verilmeliydi. Somut olayda uygulanan soruşturma tedbirinin hukukiliği bilgi paylaşımı süreçlerinde Alman hukukuna göre incelenmediği için ve daha geniş kapsamlı imkânlar sunan Fransız hukukuna dayanılmakla yetinildiği için böyle bir uygulama kabul edilemez bir *forum shopping* örneği oluşturmuştur.[125]

Berlin Eyalet Mahkemesi, ABAD'ın ve Wahl'in görüşleri doğrultusunda, Fransa'nın Encrochat cihazlarından Almanya'daki kullanıcıların verilerini toplarken Almanya'yı usulüne uygun olarak (ASE Direktifi, md. 31) bilgilendirmediğini, Fransa'nın bu yükümlülüğü ihlal etmesinin –ve Alman savcılığının polisiye kanallardan aktarılan bilgiler sonrası ASE Direktifi md. 31/3'e göre yargısal denetimi yapacak yetkili makama –olayda Stuttgart Eyalet Mahkemesine- dosyayı iletmemesinin- Alman hâkiminin –özellikle ilgili tedbire aynı şartlarda Alman hukukuna göre başvurulabilirlik açısından- denetim yapmasını engellediğini, bu ihlalin Alman savcılarının bilgisi dâhilinde gerçekleştiğini ve Alman makamlarının da bu ihlale katkıda bulunduklarını tespitinde bulunmuştur.[126] Nitekim ilgili tedbire Almanya'da başvurulabilmesi için gerekli olan suç şüphesi yönünden mahkeme, bir kimsenin salt gizli iletişim sağlayan bir cihaza sahip olmasının onun suç faaliyeti içinde bulunduğuna dair çıkarım yapmayı ve bu nedenle iletişimin denetlenmesini gerektirmediğini belirtmiştir. Mahkeme burada şu kıyaslamayı yapmıştır: bir kimsenin elinde bir manivela ile dolaşması onun muhtemelen bir evi soyacağı şüphesiyle arama kararı verilmesini yetmez. Encrochat sistemine devlet tara-

[121] Ibid, paras. 120–124.

[122] Ibid, para. 124.

[123] Wahl (n 86) 43.

[124] Wahl (n 86) 43. Somut suç şüphesi olmadan yapılan adli dinlemelerin hukuk devletinin gerekleriyle ve AİHS. md. 8/2'de düzenlenen özel ve aile hayatına saygı hakkının sınırlama sebepleri ile uyuşmadığı yönünde bkz. Schuster, 242-243.

[125] Wahl (n 86) 43.

[126] LG Berlin I (525 KLs) 279 Js 30/22 (8/22) – Beschluss vom 19. Dezember 2024, paras. 205–208.

fından erişim sağlanmadan önce kullanıcılara yönelik bir suç şüphesi söz konusu olmadığı gibi kullanıcıların kim olduğu dahi belli değildir.[127]

Öte yandan Berlin Eyalet Mahkemesi'ne göre, Al.CMK. md. 100b'de öngörülen soruşturma tedbirine karar verildiği anda gerekli olan somutlaştırılmış yeterli bireysel şüphe şartının oluşmamış olması nedeniyle Almanya'da yapılsa usulsüz sayılacak bir işlem Fransa üzerinden dolaylı şekilde (*forum shopping*) yapılmış olur –ki bu da hukuku dolanma yasağına (*Umgehungsschutz*) takılır. Bireyi koruyucu nitelikteki adli iş birliği hukuku kurallarının –ki ABAD, ASE Direktifi. md. 31/1 ve 31/6'nın bu nitelikte olduğunu kabul etmiştir-[128] ihlalinin delil kullanma yasağını doğuracağı kabul edildiğinden somut davada Encrochat delillerinin kullanılması yasağı kaçınılmazdır.[129] Berlin Eyalet Mahkemesi aynı sonuca ASE Direktifi md. 6/1-b uyarınca ASE'ye konu talebin talep eden ülkenin hukukuna göre o delilin geçerli olacağı durumlarda düzenlenebileceği koşulu üzerinden de ulaşmıştır. Diğer bir deyişle, eğer bu delil Almanya'da yasal olarak kullanılamayacaksa, başka ülkeden getirilen şekliyle de kullanılamayacaktır.[130]

Görüleceği üzere Berlin Eyalet Mahkemesi, ASE Direktifi md. 31/3 uyarınca gerekli olan yargı denetiminden kaçırılarak gerçekleştirilen tedbiri varsayımsal olarak Alman hukukuna göre değerlendirmiş ve mevcut şartlarda Alman hukukuna göre bu tedbire başvurulamayacak olduğuna karar vererek söz konusu denetimi bir anlamda sonradan yerine getirmiştir. Ayrıca Alman hukukuna göre başvurulamayacak bir soruşturma tedbiriyle elde edilen delillerin ASE yoluyla başka bir ülkeden transfer edilmesinin de (*forum shopping*) delilin kullanılmasını hukuka uygun hale getirmeyeceğinin vurgulanmasını da önemli görüyoruz.

Sonuç ve Değerlendirme

Encrochat operasyonu, dijitalleşen dünyada gerek suç örgütlerinin iletişim teknolojilerini nasıl kötüye kullandığını gerekse kolluk kuvvetlerinin sofistike teknik yöntemler ile suç örgütleri içindeki gizli iletişimi ve suç faaliyetlerini nasıl ortaya çıkardığını gözler önüne sermiştir. Encrochat operasyonunun başarısında yalnızca geliştirilmiş siber güvenlik ve bilişim teknolojilerinin kullanılması değil aynı zamanda farklı ülkelerin yetkili makamlarının teknik ve uzmanlık bilgi ve tecrübesinin bir araya getirilmesine, ortak operasyonun eş zamanlı, hızlı ve esnek bir şekilde koordine edilmesine ve yürütülmesine imkân sağlayan ortak soruşturma ekiplerinin (JITs) kurulması da önemli rol oynamıştır. Keza spontane bilgi paylaşımı ve Avrupa soruşturma emri gibi klasik adli iş birliği yöntemlerinin ötesindeki iş birliği araçları da özellikle elde edilen bilgilerin sınır ötesi ceza muhakemesi süreçlerinde etkin bir şekilde kullanılabilmesi noktasında yasal altyapıyı sağlayarak önemli bir rol oynamıştır. Gerçekten de suç faaliyetlerinin işlendiği yabancı ülkelere aktarılan veriler yüzlerce soruşturmaya, tutuklamaya ve yüksek değerde malvarlığına el konulmasına yol açmıştır. Ne var ki, teknik başarı ve etkin iş birliğinin yanında, böylesine geniş ölçekli bir müdahalenin hukuka uygunluğu, ölçülülüğü, bireyin temel haklarının korunması rejimiyle uyumu ve özellikle elde edilen verilerin mahkûmiyet kararlarına esas alınıp alınamayacağı konuları tartışmaların odağına yerleşmiştir. Yukarıda görüşlerine ayrıntılarıyla yer verdiğimiz yüksek mahkeme kararlarından çıkan sonuçlar şu şekildedir:

- AB adli iş birliği hukukunun temel ilkesi olan karşılıklı tanıma ilkesinin bir gereği olarak;
  - Yabancı ülkede (olayda Fransa'da) uygulanan bir soruşturma tedbirinin (Alman makamları tarafından) yabancı hukuktaki standartlara uygunluğunun incelenmesi mümkün değildir.

[127] Berlin Landgericht lässt Encrochat-Daten nicht zu, Der Spiegel https://www.spiegel.de/panorama/justiz/berlin-landgericht-laesst-encrochat-daten-nicht-zu-a-6dd9be2e-f558-40fa-9995-2f8136581f8e Erişim tarihi: 21 Aralık 2024.

[128] CJEU, Criminal proceedings against MN, paras. 120-125.

[129] Landgericht Berlin, vom 19.12.2024, I Az.: 525 KLs 8/22 279 Js 30/22 StA Berlin, paras. 201-246.

[130] Ibid, paras. 247-253.

- ASE'nin yerine getiren devlet makamlarının daha önce toplayıp da elinde bulundurdukları bir delilin aktarılması amacıyla düzenlenmesi, yabancı bir adli makama yönelik sıfırdan bir delil toplama emri düzenlenmesinin tabi olduğu şartlara bağlı değildir. Delilin toplanması (*Beweiserhebung*), aktarılması (*Beweisübermittlung*) ve kullanılması (*Beweisverwertung*) birbirinden bağımsız hukuki işlemlerdir. Delilin aktarılması amacıyla ASE düzenlenirken, ilgili delilin elde edilme usul ve esaslarına dair düzenleyen devlet hukukunda öngörülen şartlar aranmayacaktır. Bu doğrultuda, somut olayda olduğu gibi, ASE'nin düzenlendiği anda ilgili her bir kişi için ciddi bir suça dair somut olgulara dayalı şüphe şartının aranması da gerekli değildir.
- Aynı şekilde, ASE düzenlemeye yetkili makam (somut olayda savcılık) diğer bir AB ülkesinde sıfırdan delil elde etmek amacıyla ve hâkim kararı gerektiren bir tedbire başvurmuyor da yalnızca yabancı makamların daha önce böyle bir tedbire başvurup da elde ettikleri bir delilin kendi ülkesine aktarılması amacıyla ASE düzenliyorsa ve kendi iç hukukunda başka bir adli makamın daha önce toplamış olduğu bir delili bu şekilde bizzat talep etmeye yetkili ise hâkim onayına gerek olmaksızın ASE düzenlemeye de yetkilidir.
- Kullanılacak delilin hukuka uygun olup olmadığını belirleme noktasında aranacak şartlar delilin bizatihi ülkede veya adli yardımlaşma yoluyla yurt dışında elde edilmesi ile yabancı devlet makamlarınca spontane bilgi paylaşımı (ihbar) yoluyla aktarılması arasında farklılık gösterir. Zira ilk iki durumda anayasal ölçülülük testi kendi yargı yetkisini kullanan makam tarafından ilgili tedbire karar verilirken yapılırken üçüncü durumda ise kendi yargı yetkisini kullanarak delili elde eden yabancı devlet makamı tarafından yapılacaktır. Şu halde bir mahkeme yabancı makam yerine geçerek onun kararını değiştiremez ya da değerlendiremez. Spontane bilgi paylaşımı üzerine delili alan ve kendi yargı yetkisi kapsamında yargılamada kullanacak mahkeme ölçülülük testini -ya da başka bir değerlendirme kapsamında ilgili usul ve esasları (özellikle şüphe koşulunu)- delili kullanacağı andaki hukuki duruma ve şartlara göre (ex-post) yapacaktır. Bu değerlendirmeleri yaparken şayet yabancı ülkede uygulanan tedbirin ulusal hukukta birebir karşılığı yoksa o halde koşulları ve güvenceleri söz konusu tedbire en yakın ve fakat ondan daha hafif nitelikte olmayan muadil bir tedbir için öngörülen koşulları (ör. katalog suç, nitelikli (kuvvetli) suç şüphesi, son çare olma, vd.) *kıyasen* uygulayarak karar verebilir. Bu noktada dikkat çekmek istediğimiz husus, burada muadil bir tedbirin usul ve esaslarının kıyasen dikkate alınması delil elde etmek için değil ölçülülük değerlendirmesi ile ilgili olduğu için koruma tedbirlerinin kanuniliği bağlamında ele alınmayacaktır.

- Alman Federal Yargıtayı, bir adli iş birliği hukuku düzenlemesine aykırılığın delil değerlendirme yasağını sonuçlayabilmesi için ihlal edilen kuralın birey haklarını koruyan bir niteliğe sahip olmasını aramış, bu bağlamda, sınır ötesi iletişim dinleme tedbiri kapsamında ilgili ülkeye haber verme yükümlülüğünün bireyi delilin haber verilmesi gereken ülkede (olay açısından Almanya'da) kullanımına karşı değil, haber vermesi gereken ülkede (olay açısından Fransa'da) kullanımına karşı koruduğunu, haber verilmesi gereken ülke açısından ise daha çok o devletin egemenliğini korumayı amaçladığını kabul etmiştir. Kanaatimizce BGH'nın haber verme yükümlülüğünün ayrıca kişisel verilerin yurt (olayda Almanya) dışında kullanımına ilişkin olduğunu söylemesine rağmen konuyu bireyi koruyan bir temel hak olan kişisel verilerin korunması hakkı kapsamında ele almamış olması ya da bu bağı zayıf görmüş olması doğru olmamıştır.
- Ancak AB hukukunu yorumlamakla esas görevli olan ABAD tam tersi yönde bir karar vererek haber verme yükümlülüğü kuralı ile yalnızca ilgili devletin egemenlik haklarının korunmadığını, ayrıca haber verilen devletin, ihlali halinde tedbirin kısmen ya da tamamen tüm sonuçlarıyla ortadan kaldırılmasını sağlayacak olan "ilgili tedbirin üye devletin iç hukukunda benzer bir davada onaylanabilir olması" şartını

incelemek suretiyle benzer bir tedbire başvurulurken iç hukukta (birey lehine) öngörülen güvenceleri temin etmesi gerekeceğini ifade etmiştir. Bu yorumu takip eden Berlin Eyalet Mahkemesi, ilgili tedbire Almanya'da başvurulabilmesi için gerekli olan suç şüphesi yönünden, bir kimsenin salt gizli iletişim sağlayan bir cihaza sahip olmasının onun suç faaliyeti içinde bulunduğuna dair çıkarım yapmayı ve bu nedenle iletişimin denetlenmesini gerektirmediğini belirtmiştir. Dolayısıyla Alman hukukuna göre başvurulamayacak bir soruşturma tedbiriyle elde edilen delillerin ASE yoluyla başka bir ülkeden aktarılmış olmasının *forum shopping* sayılacağını ve bu usulün böyle bir delilin kullanılmasını hukuka uygun hale getirmeyeceğini vurgulamıştır.

- Şüpheli ve sanık haklarının korunmasını teminat altına alan ASE Direktifi md. 6/1-a bağlamında, ceza muhakemesi sürecinde şüpheli veya sanığın olayın tespitinde baskın etkiye sahip bilgi ve deliller üzerinde etkin bir değerlendirmede bulunamadığı durumlarda ulusal ceza mahkemelerinin adil yargılanma hakkının ihlal edildiğini tespit ederek söz konusu bilgi ve delili dışlamaları gerekmektedir. Aktarılan Encrochat verilerinin kaynağının, elde ediliş yönteminin, teknik özelliklerinin sanık ve müdafi tarafından sorgulanamaması ve onların erişimine açılmaması, delil bütünlüğü, güvenliği ve şeffaflığının sağlanamamasına neden olur, bu durum silahların eşitliği ilkesine aykırı olur, adil yargılanma hakkını ihlal eder ve delil değerlendirme yasağını sonuçlar.
- Netice itibariyle ABAD, Encrochat verilerinin elde ediliş ve aktarılış tarzının hukuka aykırı olmadığını, fakat özellikle adil yargılanma ve savunma hakkının gerekleri yerine getirilmeden kullanımının hukuka aykırı olacağını ifade etmiştir.

Yabancı ülke makamları ile delil konusunda yapılan iş birliği yalnızca adli iş birliği kapsamında gerçekleşmek zorunda olmadığı gibi (ör. polisiye iş birliği) adli yardımlaşma kapsamında da gerçekleşmek zorunda değildir (ör. spontane bilgi paylaşımı). Bu noktada, uygulanan farklı yöntemlerin farklı hukuki nitelikleri haiz olabileceği, farklı kurallara tabi olabileceği ve farklı hukuki sonuçlar doğurabileceği gözden kaçırılmamalı, bu nedenle gerekli hukuki tartışmalar adli ve polisiye iş birliği hukukunun özelliklerine ve kurallarına uygun ve özenli bir şekilde yapılmalıdır.

Bu doğrultuda, yabancı ülke makamlarınca gönderilen bir delilin hangi yöntem ve hukuki altyapı ile gönderildiğinin tespiti son derece önemlidir. Spontane bilgi paylaşımı yoluyla daha önceden elde edilmiş bir delilin aktarılması söz konusu olduğunda Alman Federal Yargıtayı (BGH) ve çok sayıda Alman Eyalet Mahkemesi'nin Encrochat verilerinin hukukiliğini dar bir perspektifle yalnızca özel yaşamın çekirdek alanına müdahale olup olmadığı yönüyle değerlendirmesine, meşru müdahale (sınırlama) sebebi olarak delillerin salt ağır suçların aydınlatılmasında kullanılacak olmasını yeterli görmesine ve sonuç olarak devletin ceza muhakemesi çıkarlarına üstünlük tanımasına karşın ABAD ve Berlin Eyalet Mahkemesi'nin hukuki tartışmaları daha detaylı ve teknik yönlerden ele almasının, şeffaflık ilkesi, adil yargılanma ve savunma hakkı bağlamında incelemiş olmasının ve sonuç olarak insan haklarıyla daha uyumlu olan yaklaşımının hukuken daha doğru ve isabetli olduğuna inanıyoruz. Özellikle BGH'nın, neticeten devletin ağır suçları ortaya çıkarma ödevine ağırlık vermesi ve fakat bunu yaparken ele aldığı farklı hukuki sorunlara –gerekli ya da zorunlu olmamasına rağmen- yeknesak çözüm bulma gayreti göstermesi, sorunlara olan yaklaşımının objektiflikten uzaklaştığı, devletin çıkarlarını öncelemek için kamusal ve bireysel hukuki menfaatler arasında kurulması gereken dengeyi zorlayıcı argümanlarla devletin menfaatleri lehine bozduğu izlenimini vermiştir. Buna karşın özellikle ABAD'ın yorumları farklı hukuki sorunları her birinin kendi hukuki altyapısı ve niteliği içinde çözmeye çalışması daha objektif ve denge gözeten bir karar olduğu izlenimi vermiştir. Bu yorumları izleyen Berlin Eyalet Mahkemesi'nin vermiş olduğu karar ise uluslararası adli ve polisiye iş birliği alanının yalnızca egemenlik ve etkinlik odaklı olmadığını aynı zamanda bireyin temel haklarının korunmasına ve ölçülülük ilkesinin gereklerine hizmet ettiğini bir kez daha hatırlatmıştır.

Encrochat operasyonu ve takip eden yargısal süreçler ceza adaleti sistemlerinin organize suçlarla mücadelede nasıl bir yaklaşım benimsemesi gerektiğine dair önemli dersler vermektedir. Uluslararası adli ve polisiye iş birliği alanındaki modern yöntemler bu tür suçlarla mücadelede işlevselliği ve etkinliği artırırken aynı zamanda bireylerin özel hayatının gizliliğine saygı hakkı, kişisel verilerin korunması, adil yargılanma ve savunma hakkı açısından ciddi riskler de barındırmaktadır. Gelecekte benzer operasyonlarda bireyin temel haklarının ölçülü bir şekilde korunmasını gözeten, teknik imkânların ötesinde şeffaflığı ve yargısal denetimi garanti eden bir yaklaşım benimsenmelidir. Aksi halde, kısa vadede elde edilen polisiye başarılar, uzun vadede bireylerin temel haklarına zarar vererek hukuk devletinin temel taşlarını zayıflatabilir. Bu bağlamda, Encrochat verilerine ilişkin yargı kararları, temel haklara dayalı bir denge kurulmasının kaçınılmaz olduğunu göstermektedir.

Encrochat verileri yetkili Türk makamlarıyla da paylaşılmış olup bu verilere dayalı olarak ülkemizde de çok sayıda organize suç operasyonu düzenlenmiştir. Bu makalenin son teslim tarihi itibariyle bu konuda henüz Bölge Adliye Mahkemeleri ve Yargıtay tarafından verilmiş bir karara ulaşılamamıştır. Özellikle Encrochat verilerinin delil değeri bakımından işbu çalışmadaki tespit ve değerlendirmelerin gelecekte verilecek yargı kararlarına ve bu kararlar ile ilgili yapılacak akademik çalışmalara bir ölçüde karşılaştırmalı hukuk perspektifi sunacağına inanıyoruz.

Hakem Değerlendirmesi: Dış bağımsız.
Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.
Finansal Destek: Yazar bu çalışma için finansal destek almadığını beyan etmiştir.
Teşekkür: Makalenin değerlendirme süreçlerinde gösterdikleri destek ve rehberlik için Editör ve Alan Editörü hocalarımıza, nazik yardımları için editöryal asistanlara ve yayın ofisi çalışanlarına içten teşekkürlerimizi sunarız.

Peer Review: Externally peer-reviewed.
Conflict of Interest: The author has no conflict of interest to declare.
Grant Support: The author declared that this study has received no financial support.

Yazar Bilgileri / Author Details

Erdem İzzet Külçür (Doktor Öğretim Üyesi)
[1] İbn Haldun Üniversitesi, Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı, İstanbul, Türkiye
0000-0002-8301-0241 erdem.kulcur@ihu.edu.tr

Rüveyda Enes (Yüksek Lisans Öğrencisi)
[2] İbn Haldun Üniversitesi, Hukuk Fakültesi, İstanbul, Türkiye
0009-0003-4933-6306 ruveyda.enes01@gmail.com

Bibliyografya | Bibliography

01net. (2020, 2 Temmuz). Comment les gendarmes ont siphonné Encrochat, la messagerie chiffrée des criminels. https://www.01net.com/actualites/comment-les-gendarmes-ontsiphonne-encrochat-la-messagerie-chiffree-des-criminels-1942589.html Erişim tarihi: 24 Aralık 2024.

Ambos, K. (2018). *European Criminal Law*, Cambridge University Press.

Avrupa Birliğinde Cezaî Konularda Uluslararası Adlî İş Birliği, Adalet Bakanlığı Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü Yayını, Editör: Ahmet Ulutaş, Ankara: Eylül 2021.

Böse, M. (2002). Verwertung im Ausland gewonnenner Beweismittel im deutschen Strafverfahren. *Zeitschrift für die gesamte Strafrecht-swissenschaft (ZStW)*, 114.

Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A. & Patsakis, C. (2022). SoK: Cross-Border Criminal Investigations and Digital Evidence, *Journal of Cybersecurity,* Volume 8, Issue 1, 1-18.

Council of Europe Cybercrime Convention Committee. (2025). Report on Practices regarding spontaneous information and MLA.

Cox, K. (2020, 2 Temmuz). Police infiltrate encrypted phones, arrest hundreds in organized crime bust. *ArsTechnica*. https://arstechnica.com/tech-policy/2020/07/police-infiltrate-encrypted-phones-arrest-hundreds-in-organized-crime-bust/ Erişim tarihi: 29 Aralık 2024.

Der Spiegel. (t.y.). Berlin Landgericht lässt Encrochat-Daten nicht zu. https://www.spiegel.de/panorama/justiz/berlin-landgericht-laesst-encrochat-daten-nicht-zu-a-6dd9be2e-f558-40fa-9995-2f8136581f8e Erişim tarihi: 21 Aralık 2024.

EPPO. (2021, 22 Temmuz). *Note on EPPO's participation in JITs* (2021/LS-28/JC-RR-LDM).

Eurochannel. (t.y.). 3 famous police operations by Europol. http://www.eurochannel.com/en/3-Famous-Police-Operations-by-Europol.html Erişim tarihi: 21 Aralık 2024.

EuroCoord, EIO Code of Best practices – Proposals for 100 Best Practices, March 2019.

Eurojust. (2023). *5th annual Sirius EU electronic evidence situation report*. https://www.eurojust.europa.eu/publication/sirius-eu-electronic-evidence-situation-report-2023 Erişim tarihi: 24 Aralık 2024.

Eurojust. (2020). *Encrochat: Dismantling of an encrypted network used by criminal group*. https://www.eurojust.europa.eu/ar2020/7-casework-crime-type/72-encrochat-dismantling-encrypted-network-used-criminal-groups Erişim tarihi: 27 Kasım 2024.

Eurojust. (t.y.). *JITs network*. https://www.eurojust.europa.eu/judicial-cooperation/practitioner-networks/jits-network Erişim tarihi: 16 Şubat 2025.

Eurojust. (2020). *Supporting judicial authorities in the use of joint investigation teams factsheet*. https://www.eurojust.europa.eu/sites/default/files/assets/2020_06_jits_factsheet_en.pdf Erişim tarihi: 21 Aralık 2024.

Eurojust. (2021). *Joint investigation teams: Practical guide*. https://www.eurojust.europa.eu/publication/jits-practical-guide Erişim tarihi: 29 Aralık 2024.

Eurojust. (2020). *Third JIT evaluation report*. https://www.eurojust.europa.eu/publication/third-jit-evaluation-report Erişim tarihi: 21 Aralık 2024.

Europol. (2023, 27 Haziran). Dismantling encrypted criminal Encrochat communications leads to over 6,500 arrests and close to EUR 900 million seized. https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochat-communications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized Erişim tarihi: 27 Kasım 2024.

Europol. (2020, 2 Temmuz). Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe. https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe Erişim tarihi: 21 Aralık 2024.

Europol. (2014, 10 Temmuz). Global action targeting Shylock malware. https://www.europol.europa.eu/media-press/newsroom/news/global-action-targeting-shylock-malware Erişim tarihi: 21 Aralık 2024.

Eurojust. (2021). *Annual report 2020: Criminal justice across borders in the EU*. https://www.eurojust.europa.eu/publication/annual-report-2020-criminal-justice-across-borders-eu#:~:text=In%202020%2C%20Eurojust%20has%20registered,drugs%20worth%20EUR%203%20billion Erişim tarihi: 21 Aralık 2024.

Gless, S. (2021). *Internationales Strafrecht* (3. Aufl.). Basel: Helbing Lichtenhahn Verlag.

Hecker, B. (2012). *Europäisches Strafrecht* (4. Aufl.). Heidelberg: Springer.

Laurer, N. (2018). *Informationshilfe im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen*. Baden-Baden: Nomos.

Leonhardt, A. (2017). Die Europäische Ermittlungsanordnung in Strafsachen. Wiesbaden: Springer.

Mutual Legal Assistance Manual, Council of Europe, Belgrade, 2013.

NL Times. (2024, 28 Şubat). Dutch trio made millions by selling EncroChat encrypted phones to criminals. https://nltimes.nl/2024/02/28/dutch-trio-made-millions-selling-encrochat-encrypted-phones-criminals Erişim tarihi: 28 Temmuz 2025.

Osula, A.M. (2015). Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data, *Masaryk University Journal of Law and Technology*, 9.

Pazarcıklı, N. A. (2024). Avrupa Birliği Cezai Konularda Adli İşbirliği Birimi ile Avrupa Birliği Savcılığı Ofisi Arasındaki İşbirliği İlişkisi 14(1) *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi*, 267-296.

Pisaric, M. (2021). Encrypted mobile phones. In Thematic Conference Proceedings of International Significance (Vol. 11, pp. 183–191).

Scheerhout, J. (2020, 9 Temmuz). The 'secret server' used in the killing of John Kinsella – and what it reveals about the scale of the illegal gun trade in Manchester. Manchester Evening News. https://www.manchestereveningnews.co.uk/news/greater-manchester-news/secret-server-used-killing-john-18563462 Erişim tarihi: 26 Aralık 2024.

Schuster, F. P. (2006). *Verwertbarkeit im Ausland gewonnener Beweise im deutschen Strafprozess*. Berlin: Duncker & Humboldt.

Sky News. (2020, 3 Temmuz). Encrochat: What it is, who was running it, and how did criminals get their encrypted phones? https://news.sky.com/story/encrochat-what-it-is-who-was-running-it-and-how-did-criminals-get-their-encrypted-phones-12019678 Erişim tarihi: 29 Aralık 2024.

TRT Haber. (2024, 24 Şubat). Kafes-44 operasyonunda 23 şüpheli tutuklandı. https://www.trthaber.com/haber/turkiye/kafes-44-operasyonunda-23-supheli-tutuklandi-839849.html Erişim tarihi: 7 Ağustos 2025.

UNODC, Trafficking in Persons & Smuggling of Migrants: Guidelines on International Cooperation, 2010.

UNODC & Eurojust. (2024, 4–6 Haziran). UNODC and Eurojust promote joint investigation teams for Central Asian countries. Viyana. https://www.unodc.org/unodc/en/organized-crime/CASC/en/news/2024/unodc-and-eurojust-promote-joint-investigation-teams-for-central-asian-countries.html Erişim tarihi: 27 Nisan 2025.

Wahl, T., Riehle, C., & Pingen, A. (2022). News – European Union. *eucrim – The European Criminal Law Associations' Forum*, 1, 4–37.

Wahl, T. (2022). Germany: Federal Court of Justice confirms use of evidence in Encrochat cases. *eucrim*, 1, 36–37.

Wahl, T. (2023). AG: Encrochat data can, in principle, be used in criminal proceedings. *eucrim*, 3, 264–265.

Wahl, T. (2024). ECJ ruled in Encrochat case. *eucrim*, 1, 40–43.

Wahl, T. (2024). Attempt for second reference for preliminary ruling in Encrochat case. *eucrim*, 1, 44.

Yang, S., & Tan, Y. (2023). The joint investigation team in Ukraine: Challenges and opportunities for the International Criminal Court. *European Papers*, 8(3), 1121–1124.

Yılmaz, Y. (2017). Avrupa Birliği Ceza Hukukunda Organize Suçlulukla Mücadele, *TAAD*, Yıl:8, Sayı:31.

MEVZUAT

Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union. (2000).

Council Framework Decision 2002/465/JHA of 13 June 2002 on Joint Investigation Teams.

Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence. Official Journal L 196, 2 August 2003.

Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union. Official Journal L 386, 29 December 2006.

Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters. Official Journal L 350, 30 December 2008.

Council of the European Union. (2000). Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union. Official Journal C 197, 12 July 2000.

Directive (EU) 2022/211 of the European Parliament and of the Council of 16 February 2022 amending Council Framework Decision 2002/465/JHA, as regards its alignment with Union rules on the protection of personal data.

Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA.

European Parliament and Council of the European Union. (2014). Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order in criminal matters. Official Journal L 130, 1 May 2014.

European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/794 of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol). Official Journal L 135, 24 May 2016.

European Parliament and Council of the European Union. (2018). Regulation (EU) 2018/1727 of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust). Official Journal L 295, 21 November 2018.

Regulation (EU) 2016/95 of the European Parliament and of the Council of 20 January 2016 repealing certain acts in the field of police cooperation and judicial cooperation in criminal matters.

MAHKEME KARARLARI

Bundesgerichtshof (BGH), Beschluss vom 2. März 2022 – 5 StR 457/21.

Bundesverfassungsgericht, Beschluss vom 1 November 2024 – 2 BvR 684/22.

Court of Justice of the European Union. Criminal proceedings against M.N. (Case C-670/22), ECLI:EU:C:2024:372, 30 April 2024.

ECtHR, Yalçınkaya v. Türkiye, 26.09.2023, Başvuru No: 15699/20.
Landgericht Berlin, Urteil vom 19.12.2024, I Az.: 525 KLs 8/22 279 Js 30/22 StA Berlin.
A, B, D & C v. Regina [2021] EWCA Crim 128.