CEZA MUHAKEMESİNDE İNTERNET TRAFİK BİLGİLERİNE ERİŞİM VE İNTERNET TRAFİK BİLGİLERİNİN DELİL DEĞERİ[*]

ACCESS TO INTERNET TRAFFIC DATA AND IT'S WEIGHT OF EVIDENCE IN CRIMINAL PROCEDURE

Araştırma Makalesi

Fatih BİRTEK[**]

ÖZ

Ceza muhakemesinde bilişim suçlarının yanında diğer pek çok suç bakımından maddi gerçeğin ortaya çıkarılabilmesi için internet trafik verilerine erişim ihtiyacı ortaya çıkmaktadır. Bununla birlikte, internet trafik verilerine müdahale aynı zamanda veri sahibinin dijital özel yaşamına ifade ve haberleşme özgürlüğüne de müdahale anlamına geldiğinden, bu müdahalenin amacının, kapsamının, süresinin belirlenmesi ve müdahalenin kötüye kullanılmasını engelleyecek yasal güvencelere yer verilmesi gerekmektedir. Türk ceza muhakemesinde internet trafik verilerine suç soruşturması ve kovuşturması amacıyla müdahale edilebileceği kabul edilmekle birlikte, bu hususta açık bir kanuni düzenleme bulunmamaktadır. Uygulamada, suç soruşturmasına/ kovuşturmasına ilişkin genel yetki kapsamında bu müdahalenin yapılabileceği kabul edilse de internet trafik verilerinin içeriği ve etkilediği temel haklar nazara alındığında bu tür bir müdahalenin kanun ile açıkça düzenlenmesi gerekmektedir.

Anahtar Kelimeler: İnternet Trafik Verisi, Ceza Muhakemesi, Delil, İspat, Delil Değeri

---

[*] Bu çalışma, "*Ceza Muhakemesinde İnternet Trafik Bilgilerine Erişim ve İnternet Trafik Bilgilerinin Delil Değeri*" başlığıyla sadece sözlü olarak sunulan bildirinin (Bilişim ve Teknoloji Hukuku Sempozyumu, İstanbul Medeniyet Üniversitesi, 3-5 Aralık 2021, İstanbul- Türkiye) güncellenmiş ve genişletilmiş halini oluşturmaktadır. Çalışmayı okuyarak görüşlerini paylaşan ve yazım denetimini yaparak katkı sağlayan Arş. Gör. Fuat İdar BURSA'ya teşekkür ederim.

DOI: 10.32957/hacettepehdf.1841330

Makalenin Geliş Tarihi: 12.12.2025 **Makalenin Kabul Tarihi:** 22.01.2026

[**] Prof. Dr., Sivas Cumhuriyet Üniversitesi Hukuk Fakültesi, Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı

E-posta: fatihbirtek@hotmail.com

ORCID: 0000-0001-7019-0653

Bu makale, Hacettepe Üniversitesi Hukuk Fakültesi Dergisi Araştırma ve Yayın Etiği kurallarına uygun olarak hazırlanmıştır.

ABSTRACT

In criminal proceedings, the interventing of internet traffic data are used to reaching material truth regarding cybercrimes and many other crimes. Intervention of internet traffic data also involves interfering with the data individual's digital privacy, freedom of expression, and freedom of communication. For this reason, the purpose, scope and duration of this intervention must be determined and also legal safeguards must be included to prevent the abuse of the intervention. In Turkish criminal procedure, retained internet traffic data can be intervened for the purposes of criminal investigation, there is no clear legal regulation on this matter. In practice, the interventing of internet traffic data can be considered within the scope of general authority for criminal investigation. Such intervention must be carried out in accordance with fundamental rights, and such intervention must be defined by law.

Keywords: Internet Traffic Data, Criminal Procedure, Evidence, Proof, Weight of Evidence

EXTENDED SUMMARY

Lawful interventions into individuals' "digital private life" for the purpose of obtaining evidence are not only possible in the context of crimes against privacy and the private sphere of life, or direct and indirect cybercrimes, but also all other crimes. However, while Turkish law clearly regulates the interception of internet traffic data for the purposes of preventing crimes and gathering intelligence, the interception of this data for the purpose of criminal investigation/ prosecution is not explicitly regulated.

In criminal proceedings, which adopt a free/ unlimited and conscientious evidence system, with a few exceptions arising from laws and practice, evidence is not limited, nor is there any restriction or hierarchy regarding evidence in terms of its weight of evidence or proof. Therefore, no distinction is made between material evidence and digital evidence in terms of its weight of evidence. The crucial point in terms of weight of evidence is not the content of the evidence, but whether it is part of the material truth within the circumstance of requiring evidence. Any material or digital evidence capable of proving the truth regarding a material fact requiring proof is considered "evidence." Digital evidence is considered "inferential/ indicative" according to the generally accepted classification of evidence in the doctrine (based on the content/content of the evidence). Internet traffic data consists of information/data held by access and hosting providers that provide internet of communication services. Therefore, it is often interpreted by an expert witness.

While documenting internet traffic data accessed during a criminal investigation or prosecution and subjecting it to discovery or expert examination facilitates the discussion of the evidence at trial under Articles 68 and 214 of the Criminal Procedure Act (CPA), the integrity and reliability of digital data can be determined by examining its digital form, not the paper/ document on which it was written.

Even if documented, internet traffic data, which constitutes digital evidence (data), should be considered indicative/ inferantial evidence rather than documentary evidence, and should be interpreted by subjecting it to discovery or expert opinion.

The totality of the traces left by the device used to connect to the internet on the system through which it is connected is defined as a "virtual fingerprint." Examining the traces ("virtual fingerprints") left by the device used for connection in the digital environment (internet) is essentially and also this examination no different from material fingerprint. Just as fingerprints found at a crime scene or on any crime-related object must be identified, transferred to another medium (paper, etc.) for examination, and examined, internet traffic data must also be identified, digitally copied, and examined.

The fundamental basis for the retention/ recording of internet traffic data is the provisions of Law No. 5809 and Law No. 5651.

A review of the definitions in the legislation reveals that internet traffic data held/retained by operators/internet access and hosting providers is, by its nature, a type of "preliminary data" or "brief data." Considering its nature, it is clear that some of this data (IP and subscriber ID information of internet service) constitutes "personal data" capable of identifying a natural person "directly," while others (websites accessed information etc.) constitute "indirectly."

Because internet traffic data is closely related not only to individual data but also to freedom of expression and communication, therefore unlawfully interfering with the privacy of a person's internet traffic information (without a legal basis, legitimate purpose, and in an excessive manner) could lead to a violation of these fundamental rights and freedoms.

The existence of legitimate purposes does not justify the notion that everyone living in a country "might one day commit a crime and should have access to past internet traffic data for this purpose." The existence of legitimate purposes does not justify or justify considering all individuals living in the country as "potential criminals." In practice, it appears that Information Technologies and Communication Council (BTİK) has "unlimited" access to internet traffic data, and public prosecutors and courts can easily access this data within the scope of its "general authority" for criminal investigation and prosecution. However, Articles 160 and 161 of the CPA, which refer to the general authority for criminal investigation, and Article 206 of the CPA, which (indirectly) grants courts the authority to take evidence, fall far short of meeting the "knowability and foreseeability" guarantee regarding interventions into the freedoms protected by internet traffic data.

Considering the precedents of the ECtHR and the Constitutional Court, access to internet traffic data needs to be clearly regulated in the CPA, just as it is for the "get access to communication data" While the detection of communications made via fixed or mobile phones (as per Article 135/6 of the CPA) is possible "*by a judge*

during the investigation process, or by a public prosecutor in cases where delay is deemed undesirable, or by a court decision during the prosecution process" it is inappropriate to consider internet traffic information within the general jurisdiction of criminal investigations/ prosecutions. Furthermore, considering that internet traffic data may relate to communications conducted via the internet (communication applications), the lack of a clear legal regulation on this matter is clearly a deficiency. Given that the interception of internet traffic data for crime prevention purposes (Law No 2559, Annex Article 7/2) and the detection of communications made via fixed/ mobile devices (Article 135/6 of the CPA) are clearly regulated, the lack of explicit regulation in the law of the conditions for get access to internet traffic data, which also includes information regarding communications conducted via the internet (through applications), is a significant deficiency.

This legal gap should be filled by revising Article 135/6 of the CPA: "*The detection of/ get access to suspect and defendant's communication informations and internet traffic data shall be made by the judge during the investigation process, or, in cases where delay is deemed unacceptable, by the public prosecutor, and, in the prosecution process, by a judge/ court decision...*".

GİRİŞ

Günümüzde özel yaşam kavramının gerçek (somut) unsurları dışında dijital (sanal) unsurları da karşımıza çıkmakta ve neredeyse her gerçek kişinin sanal/ dijital bir kişiliği bulunmaktadır. Dijital özel yaşam alanı olarak tanımlayabileceğimiz bu alan, gerçek özel yaşama nazaran çok daha hassas ve tehdide açık bir konumdadır. Zira dijital alanın özelliği gereği, dijital özel yaşam unsurlarına müdahale de kolaylaşmaktadır. Gayri meşru müdahalelerin yanında, ceza muhakemesinde herhangi bir maddi vakıanın ispatı bakımından, bireylerin "*dijital özel yaşam*" alanına da -belirli sınırlamalar içerisinde- müdahale edilebilmektedir. Maddi gerçeğin ortaya çıkarılması, dijital özel yaşama müdahale bakımından meşru bir amaç olarak karşımıza çıkmaktadır.

Maddi gerçeğe ulaşmayı amaç edinen ceza muhakemesinde, ispatı zorunlu herhangi bir maddi vakıa hukuka uygun her tür delille ispat olunabilir. Ceza muhakemesinde deliller arasında bir hiyerarşi bulunmadığı gibi ispat işlevi yönünden kesin delil- takdiri delil ayrımı da bulunmamaktadır. İspatı gereken maddi vakıaya ilişkin gerçeği ispata elverişli herhangi bir delil, hâkimin vicdani kanaatine dayanak teşkil edebilir. Bununla birlikte, ceza

muhakemesi ne pahasına olursa olsun maddi gerçeğe ulaşmayı da meşru kabul etmediğinden, ispat araçlarına (delillere) ulaşılması ve ispat araçlarının duruşmada tartışılarak "delil" niteliği taşıdığı belirlendikten sonra hükme dayanak yapılması hukuk devleti ilkesinin yansıması olarak kabul edilen bir kısım sınırlamalara tabidir.

Bireylerin "*dijital özel yaşam*" alanlarına, delil elde etme amacıyla yapılacak hukuka uygun müdahaleler sadece özel hayata ve hayatın gizli alanına karşı suçlar veya doğrudan ve dolaylı bilişim suçları bakımından değil, diğer bütün suçlar bakımından da söz konusu olabilmektedir[1]. Ancak Türk hukukunda suç işlenmesinin önlenmesi (PVSK Ek Madde 7/2)[2] ve istihbarat elde etme amacıyla (2937 s. Kanun m 6/1-b ve g)[3] internet trafik bilgilerine müdahale, açıkça düzenlendiği halde[4], suç soruşturması/ kovuşturması amacıyla bu bilgilere müdahale açıkça düzenlenmemiştir[5].

---

[1] Suç işlenmesinin önlenmesi amacıyla internet trafik verilerinin tespiti hakkında bkz. Fatih Birtek, 'Suç İşlenmesini Önleme Amacıyla İnternet veri Trafiğinin (İnternet Trafik Bilgilerinin) Tespiti', içinde Fatih Birtek (edt) *Hukuk Devletinde Kolluğun Suç Önleme Yetkisi (Kaynağı, Kapsamı ve Sınırları)* (1. Baskı Adalet Yayınevi 2024) 663 vd.

[2] Polis Vazife ve Selahiyet Kanunu, Kanun Numarası: 2559, Kabul Tarihi: 04.07.1934, RG 14.07.1934/ 2751.

[3] Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu, Kanun Numarası: 2937, Kabul Tarihi: 01.11.1983, RG 03.11.1983/18210.

[4] İstihbari ve suç önleme maksadıyla internet trafik verilerinin tutulması, çalışma konumuz dışında kaldığından bu konuya gerekli olmadıkça değinilmeyecektir.

[5] Yargıtay'a göre önleyici (önleme amaçlı) tedbirler neticesinde elde edilen bulgular ancak *soruşturma başlatılabilmesi için* kullanılabilir, bu bulgulara dayanılarak *hüküm kurulamaz*. Yargıtay CGK, 9-93/95, 17.05.2011. Yargıtay güncel kararlarında bu yaklaşımını değiştirmiştir. Yargıtay'a göre "*MİT'in görevlerini yerine getirirken elde ettiği veya rastladığı terör suçları, sınır aşan örgütlü suçlar veya siber suçlara konu materyalleri adli makamlara veya terörle mücadele konusunda görevli birimlere iletmesinin, MİT'in istihbari bilgi toplama ve görüş bildirme değil, söz konusu suçlar yönünden, bu materyallerin soruşturma veya kovuşturma evrelerinde delil olarak kullanılması için adli makamlarla yaptığı bir paylaşım olarak değerlendirilmesi gerekir. Aksinin kabulü, bir suçun işlendiğini göreviyle bağlantılı olarak öğrenip de yetkili makamlara bildirimde bulunmama halini yaptırım altına alan TCK'nın 279 uncu maddesinin ihlalini gündeme getireceği gibi, kişilere hukuki uyuşmazlıklara ilişkin olarak etkili bir soruşturma ve kovuşturma yapılarak maddi gerçeğin ortaya çıkarılmasını isteme hakkını tanıyan Anayasanın 36 ncı maddesine de aykırılık oluşturacaktır"*, Yargıtay CGK, 16-956/370, 26.09.2017 (*Bu çalışmada yararlanılan kararlara aksi belirtilmedikçe www.kazanci.com (İçtihat Bilgi Bankası) aracılığıyla erişilmiştir*). 2559 sayılı Kanun Ek Madde 7/2 de yer alan düzenlemede, tespit edilen kayıtların en fazla ne kadar süreyle tutulabileceğine dair bir üst sınıra yer verilmediği görülmekle birlikte, düzenlemenin amacı ve elde edilen bulguların ceza yargılamasında delil olarak kullanılamaması bir bütün olarak değerlendirildiğinde, bu türden bir üst sürenin öngörülmemesinin de meşru bir amaca (suç önleme ve terörle mücadele amaçlarına) hizmet ettiği ve bu sebeple de eksiklik olarak nitelendirilemeyeceğini düşünmekteyiz. Bununla birlikte, bütün internet

Çalışmamızda, ceza muhakemesinde delil elde etmek amacıyla dijital özel yaşam unsurlarından birisi olan (ve aynı zamanda ifade özgürlüğü ve haberleşme özgürlüğü gibi özgürlüklerle de ilişkisi bulunan) "*internet trafik bilgilerine*" yapılacak müdahalelerin kanuni çerçevesi AİHM, Anayasa Mahkemesi ve Yargıtay kararları bağlamında ele alınacak ve bu müdahalelerden elde edilen bulguların ispat işlevi (ispat gücü) tartışılacaktır.

I. CEZA MUHAKEMESİNDE İSPAT ARACI OLARAK "DİJİTAL DELİL"

Ceza muhakemesinde soruşturma veya kovuşturma konusu olaya ilişkin olan ve ispatı zorunlu olan maddi vakıalara ilişkin maddi gerçeğin ortaya çıkarılabilmesi için delile ihtiyaç bulunmaktadır. Zira delilsiz mahkûmiyet olmaz.

Serbest ve vicdani delil sistemini benimseyen ceza muhakemesinde kanunlardan ve uygulamadan kaynaklı birkaç istisna dışında, deliller sınırlandırılmadığı gibi ispat işlevi/ gücü bakımından delillere ilişkin herhangi bir sınırlandırmaya veya hiyerarşiye yer verilmemiştir. Bu sebeple ispat işlevi yönünden maddi delillerle dijital bulgular arasında herhangi bir ayrım gözetilmemiştir. İspat işlevi bakımından önemli olan husus delilin muhtevası değil, ispatı zorunlu olan maddi vakıaya ilişkin maddi gerçeğin bir parçası olup olmadığıdır. İspatı zorunlu bir maddi vakıaya ilişkin gerçeği ispata elverişli her türlü maddi veya dijital bulgu "delil" olarak kabul edilir.

---

kullanıcılarının trafik verilerinin tutulmasının/ depolanmasının/ işlenmesinin ölçülü olduğu ve bu tür bir müdahalenin demokratik bir toplumda gerekli ve ölçülü olduğu söylenemez. Açıklama için bkz. Birtek (n 1) 683. PVSK Ek Madde 7/2 hükmünün "belirlilik" ilkesinin sağladığı güvencelerden yoksun olması nedeniyle, bu hükme istinaden toplanan verilerden hareketle "*ön alan soruşturması"* başlatılamayacağı hususunda bkz. Fatih Birtek ve Beyza Nur Topal, 'Dijital İspat Aracı Olarak Sabit veya Ankesörlü Telefonlara İlişkin Arama Kayıtları ve Bu Kayıtların İspat Kuvveti', (2023) (2) GSÜHFD 1149, 1137-1142. Erol Cihan ve Feridun Yenisey, *Ceza Muhakemesi Hukuku* (Beta Yayıncılık 1996) 262; Yenisey, Feridun: *Hazırlık Soruşturması ve Polis* (Beta Yayıncılık 1987) 188; Veli Özer Özbek, *Ceza Muhakemesi Hukuku* (Seçkin Yayınevi 2006) 78-79. Ön alan soruşturmasının mahiyeti ve bu kapsamda yapılabilecek işlemlere ilişkin olarak bkz. Veli Özer Özbek, 'Organize Suçlulukla Mücadele Ön Alan Soruşturmaları', (2002) 4 (2) Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 57- 88; M. Ruhan Erdem, *Ceza Muhakemesinde Organize Suçlulukla Mücadelede Gizli Soruşturma Tedbirleri* (1. Baskı, Seçkin Yayınevi 2001) 210 vd. PVSK Ek Madde 7 kapsamında tutulan verilerin, destekleyici ve yan delil olarak kullanılabileceği hususunda bkz. Veli Özer Özbek, 'Elektronik Ortamda Saklı Bulunan Verilerin ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi' (2001) 59(1-2) İÜHFM, 181, 185 vd.

Dijital bulgular, öğretide genel kabul gören (delilin içeriği/ muhtevası esas alınarak yapılan) delil sınıflandırmasına[6] göre "belirti" içerisinde değerlendirilmektedir[7,8]. İnternet trafik verileri, internet alanında hizmet sunan erişim ve yer sağlayıcılar tarafından tutulan bilgilerden/ datadan oluşan verilerdir. Bu sebeple, çoğu kez bilirkişi tarafından anlamlandırılmaktadır.

Öğretide dijital (sayısal) delilin, ister insan müdahalesi ile isterse bir sistem tarafından otomatik olarak oluşturulsun, gerçekliği kontrol edildikten sonra "*dolaylı delil*" olarak kabul edileceği belirtilse de[9] internet trafik verilerinin her durumda belirti veya dolaylı delil olduğu hususunda mutlak bir kural konulamaz[10]. Özellikle bilişim suçları (doğrudan bilişim

---

[6] Öğretideki sınıflandırmalar ve genel kabul gören sınıflandırma için bkz. Fatih Birtek, *AİHM, Anayasa Mahkemesi ve Yargıtay Kararları Işığında Ceza Muhakemesinde Delil ve İspat* (2. Baskı, Adalet Yayınevi 2017) 76 vd.

[7] Birtek (n 6) 203 vd.

[8] Yargıtay'a göre "*sanıkların cep telefonlarının sinyal bilgilerinin incelenmesi sonucunda, olay tarihinde cep telefonlarının aynı baz istasyonundan sinyal vermesi nedeniyle sanıkların buluştukları iddia edilmekte ise de; baz istasyonlarının geniş bir kapsama alanının olması, büyük şehirlerde birbirine yakın yerlerde oturan, çalışan veya tesadüfen oradan geçmekte olan insanların cep telefonlarının aynı baz istasyonundan sinyal vermesinin olağan bir durum olması göz önüne alındığında, cep telefonlarının aynı baz istasyonu kapsamında sinyal vermesinin sanığın diğer sanıklarla bir araya geldiği ve görüştüğünü kabule imkan vermemektedir*" Yargıtay CGK, 5-247/60, 24.03.2015. ""*ByLock kullanıcılarının tespitleri açısından operatörler tarafından tutulan CGNAT (HIS) kayıtları bir çeşit üst veri olduğu, CGNAT kayıtları <u>özet veri</u> olması nedeniyle <u>bir iz ve emare niteliğinde olduğundan</u> tek başına kişinin gerçek ByLock kullanıcısı olduğunu göstermeyeceği, kişilerin iradeleri dışında ByLock sunucularına yönlendirilmiş olma ihtimalinin bulunduğu…*" Yargıtay 16 CD, 7457/6352, 15.12.2020; 16 CD 1341/3535/, 10.07.2020; Yargıtay 3 CD, 17406/7542, 27.10.2023; Yargıtay 3 CD, 12704/8722, 12.03.2025.

[9] Olgun Değirmenci, *Ceza Muhakemesinde Sayısal (Dijital) Delil* (1. Baskı, Seçkin Yayınevi 2014) 139. Belirtilerin ispat gücü yüksek olsa da tek başına olayı ispat gücü olmadığı hususunda bkz. Cumhur Şahin ve Neslihan Göktürk, *Ceza Muhakemesi Hukuku* (13. Bası Seçkin Yayınevi 2022), 440; Hakan Karakehya, *Ceza Muhakemesi Hukuku* (6. Bası Adalet Yayınevi 2024) 257. Öğretide "*dijital doğrulama*" yapılmak kaydıyla internet trafik bilgilerinin, *üst veri* (meta data) yani "*verinin kaynağını gösteren veri*" olduğu ve internet hizmetini kullanan kişiye ilişkin olarak kesin ve doğrudan bir bilgi vermemesi nedeniyle ancak "delil başlangıcı/ dolaylı delil" olarak kabul edilebileceği öne sürülmektedir. Halid Özkan, 'Ceza Muhakemesinde Ekran Görüntüsü Çıktılarının Delil Niteliği', içinde Yener Ünver (edt) *Ceza Muhakemesi Hukukunda Delil ve İspat, Karşılaştırmalı Güncel Ceza Hukuku Serisi 15* (1. Baskı, Seçkin Yayınevi 2014) 274-275.

[10] Anayasa Mahkemesinin bizim de katıldığımız uygulamasına göre ise sağlamlığı ve güvenilirliği ortaya konulmak kadıyla mahkumiyetin dijital delillere dayanması "*temelsiz ve keyfi bir tutum olarak değerlendirilemez*". Aydın Yavuz ve Diğerleri, 2016/22169, 20/6/2017, par 267. (*Bu çalışmada yararlanılan Anayasa Mahkemesi kararlarına www.anayasa.gov.tr adresinden 30 Kasım 2025 tarihinde erişilmiştir*).

suçları)[11] bakımından internet trafik verileri ispatı zorunlu maddi vakıalara ilişkin olarak tek ve/veya belirleyici delil niteliği taşıyabilir[12]. Bu sebeple, internet trafik verilerinin (ve genel olarak dijital bulguların) mutlak anlamda belirti sayılacağı ve tek başına ve/veya belirleyici delil olarak ispat aracı olarak kullanılamayacağı düşüncesine katılmıyoruz. Yine öğretide haklı olarak vurgulandığı üzere, her dijital verinin delil olarak kabul edilebilmesi de mümkün değildir[13].

Dinamik/ değişken IP kullanımında, suçun işlenmesinde kullanılan dijital aracın kesin olarak tespit edilebilmesi için internet bağlantısının yapıldığı zaman, bağlantı süresi, bağlanılan internet siteleri, bağlantıda indirilen ve yüklenen veri miktarı ve bağlantının sona erdiği zamanın bilinmesi gerekmektedir. İnternet erişim sağlayıcılar tarafından bu veriler tutulmaksızın ve kaydedilmeksizin[14] geçmişe yönelik olarak bu bilgilere erişebilmek ve bu hususta maddi gerçeği ortaya çıkarabilmek mümkün değildir.

---

[11] Bilişim suçları "*Bilişim suçunu bilişim sisteminin ve/veya sistemlerinin dolaylı veya doğrudan bir araç ya da bir hedef ya da her ikisi de olduğu yasadışı eylemler*" olarak tanımlanmaktadır. Tanımlama için bkz. Gülennur Erkan, *Bilişim Sistemine Girme, Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları* (Yayınlanmamış Yüksek Lisans Tezi, YÖK Tez Merkezi 2021) 16. Bilişim suçlarına ilişkin değişik tanımlamalar ve sınıflandırma için bkz Yavuz Erdoğan, *Türk Ceza Kanunu'nda Bilişim Suçları* (1. Baskı, Legal Yayıncılık, 2013) 105. Yargıtay'a göre de "*5237 sayılı Türk Ceza Kanununda bilişim suçları; Bilişim alanında suçlar bölümünde düzenlenmekle beraber, ayrıca çeşitli bölümlerde de bilişim sistemleriyle işlenmesi mümkün olan suç tiplerine yer verilmiştir. Bilişim alanında suçlar bölümünde yer alan 243. maddesinde bilişim sistemine girme, 244. maddesinde sistemi engelleme, bozma, verileri yok etme veya değiştirme, 245. maddesinde banka veya kredi kartlarının kötüye kullanılması suçları düzenlenmiştir. Bunun yanında, Özel hayata ve hayatın gizli alanına karşı suçlar bölümünde yer alan 135. maddesinde kişisel verilerin kaydedilmesi, 136. maddesinde kişisel verileri hukuka aykırı olarak verme veya ele geçirme, 138. maddesinde ise verilerin yok edilmemesi suçları bilişim suçu olarak nitelendirilebilecek şekilde düzenlenmiştir. Öte yandan, 132. maddesinde haberleşmenin gizliliğini ihlal, 124. maddesinde haberleşmenin engellenmesi, 125/2. maddesinde hakaret, 142/2. maddesinin (e) bendinde hırsızlık, 158/1. maddesinin (f) bendinde dolandırıcılık, 226. maddesinde müstehcenlik, 163. maddesinde karşılıksız yararlanma suç tiplerinin bilişim sistemlerinin kullanılması suretiyle işlenmeleri mümkün kabul edilmiştir*". Yargıtay CGK., 15-125/111, 02.04.2013.

[12] Belirtilerin ispat kuvveti hakkında bkz Birtek (n 6) 194 vd. Elektronik haberleşme araçlarıyla işlenen suçlar bakımından internet trafik verilerinin (özellikle IP numarasının ve internete erişimde kullanılan elektronik araca ilişkin bilgilerin) tespit edilmesi gerektiği hususunda bkz Yargıtay 8 CD, 10272/10298, 22.04.2014; 8 CD, 3370/11901, 08.05.2014.

[13] Bahri Öztürk, Durmuş Tezcan ve Mustafa Ruhan Erdem (edt), *Dijital Ceza Muhakemesi Hukuku* (3. Baskı, Seçkin Yayınevi 2024) 402.

[14] Hans Kudlich, 'İnternette Anonim Gezinti Hakkı ve Ceza Hukuku (Anonimleştirilmiş Servis Hizmetlerine İlişkin Hukuki Problem', (Çev. Özlem Yenerer Çakmut) içinde Yener Ünver (edt) Özel Yaşam, Medya ve

II. İNTERNET TRAFİK BİLGİLERİ VE BU BİLGİLERİN TUTULMASI

İnternete bağlanmakta kullanılan aracın internet bağlantısının yapıldığı sistemde bıraktığı izlerin bütünü "sanal parmak izi" olarak tanımlanmaktadır[15]. Bağlantı için kullanılan aracın dijital ortamda (internet ortamında) bıraktığı izlerin ("sanal parmak izlerinin") incelenmesi de esasında parmak izi incelemesinden farklı değildir[16]. Nasıl ki parmak izi incelemesinin yapılabilmesi için suç mahallinde veya suçla ilgili herhangi bir nesnede bulunan parmak izinin tespit edilmesi, inceleme için başka bir ortama (kâğıt vs.) transfer edilmesi ve incelenmesi gerekliyse, internet trafik bilgilerinin de tespit edilmesi, dijital ortamda kopyalanması ve incelenmesi gerekmektedir.

İnternet trafik verilerinin tutulması/ kaydedilmesi konusundaki temel dayanak 5809 sayılı Elektronik Haberleşme Kanunu[17] ve 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun[18] hükümleridir[19].

Ceza Hukuku Karşılaştırmalı Güncel Ceza Hukuku Serisi 7 (1. Baskı, Seçkin Yayınevi 2007) 304. Alman hukukunda belirli bir kullanıcının, hizmet alırken talep etmesi halinde, internet bağlantısına ilişkin bilgilerin –bir program veya yazılım marifetiyle- anonimleştirilmesinin ancak internette suç işleyip işlemediği hususundaki bilginin kendisine aktarılmasının garanti edilmesi halinde mümkün olması gerektiği öne sürülmektedir. Bu durumun bilgi verme yükümlülüğü ve suça iştirak hususunda ortaya çıkardığı tartışmalar için bkz Kudlich (n 14) 320.

15 Tanımlama için bkz. Birtek (n 1) 666.

16 Her iki iz, ispat gücü bakımından farklı nitelik taşımaktadır. Başka bir çalışmada da belirtildiği üzere "*Sanal parmak izinin klasik parmak izinden iki temel farkı bulunmaktadır. Bunlardan ilki dijital olması ve biyolojik parmak izinde olduğu gibi bir kesinlik taşımaması iken; ikincisi ise faile veya bilgisayar kullanıcısına değil, internet ağına bağlanan araca ilişkin olmasıdır*." Birtek (n 1) 666.

17 Elektronik Haberleşme Kanunu, Kanun Numarası: 5809, Kabul Tarihi: 05.11.2008, RG 10.11.2008/ 27050 (Mükerrer).

18 İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Kanun Numarası: 5651, Kabul Tarihi: 04.05.2007, RG 23.05.2007/26530.

19 5809 sayılı Elektronik Haberleşme Kanunu'nun "kapsam" başlıklı m. 2/2'de "*5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun hükümleri saklıdır*" denilmek suretiyle, internet haberleşmesi konusunda 5651 sayılı Kanun hükümlerinin uygulanacağı açıkça ifade edilmiştir. İnternet erişimine ilişkin trafik verilerinin tutulması bakımından 5809 sayılı Kanun kapsamında yetkilendirilen bütün internet servis sağlayıcıları bakımından 5651 sayılı Kanun hükümleri uygulanacağından, çalışmamızda bu Kanun hükümleri esas alınarak bir değerlendirme yapılacaktır.

5651 sayılı Kanun'un "tanımlar" başlıklı 2. maddesinin j bendinde "*Trafik bilgisi: Taraflara ilişkin IP adresi, port bilgisi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerini*" karşılayan bir kavram olarak tanımlanmıştır[20].

İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik[21] m. 3/1-g bendine göre "*Erişim sağlayıcı trafik bilgisi: İnternet ortamında yapılan her türlü erişime ilişkin olarak abonenin adı, kimlik bilgileri, adı ve soyadı, adresi, telefon numarası, sisteme bağlantı tarih ve saat bilgisi, sistemden çıkış tarih ve saat bilgisi, ilgili bağlantı için verilen IP adresi ve bağlantı noktaları*"dır.

Belirtmek gerekir ki; bir bilgisayar ile başka bir bilgisayara (ana bilgisayara) bağlanılarak internete giriş yapılması halinde, ara bağlantıyı sağlayacak bir "*proxy (vekil-ara)*" sunucuya ihtiyaç bulunmaktadır.

İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik m. 3/1-ö'ye göre "*Vekil sunucu trafik bilgisi: İnternet ortamında erişim sağlayıcı tarafından kullanılan vekil sunucu hizmetine ilişkin talebi yapan kaynak IP adresi ve port numarası, erişim talep edilen hedef IP adresi ve port numarası, protokol tipi, URL adresi, bağlantı tarih ve saati ile bağlantı kesilme tarih ve saati bilgisi gibi bilgileri*"ni ifade eder. Aynı Yönetmelik m. 8/1-e'ye göre erişim sağlayıcı "*Kullanıcılarına vekil sunucu hizmeti sunuyor ise; vekil sunucu trafik bilgisini bir yıl saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile*

---

[20] Maddede yer alan "*gibi bilgiler*" ifadesi, 6527 sayılı Kanun ile metinden çıkarıldığından, bu bilgiler/ veriler dışındaki verilerin tutulabilmesi/ kaydedilebilmesi mümkün değildir. Danıştay İDDK de bu değişiklikten hareketle İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik m. 3/1-g bendine yer alan "gibi değerler" ifadesinin iptaline karar vermiştir. Danıştay'a göre maddede yer alan "bilgi" kavramı ile neyin kastedildiğine ilişkin herhangi bir açıklamaya yer verilmediği görüldüğünden, madde metni bu yönüyle belirsiz hâle gelmiştir". Danıştay 13 D, 239/4266, 02.12.2019. Karar için bkz. https://cdn.bartin.edu.tr/personel/ecf292227efb77dbdc4ccb91b19d8031/5-danistay.pdf İptal kararını onayan Danıştay İDDK, 1851/649, 24.02.2022. Karar için bkz UYAP Mevzuat ve İçtihat Programı, https://mevzuat.adalet.gov.tr/

[21] İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik, RG 30.11.2007/26716.

birlikte muhafaza etmek ve gizliliğini temin etmekle" yükümlü tutulmuştur[22]. Erişim sağlayıcısının, internete bu şekilde bağlanılması halinde, vekil sunucu marifetiyle yapılan internet trafiğine ilişkin bilgilerin de tutulması ve saklanması gerekmektedir.

Mevzuatta yer verilen tanımlamalar incelendiğinde, işletmeciler/ internet erişim ve yer sağlayıcılar tarafından tutulan/ tutulması gereken internet trafik verilerinin mahiyeti itibariyle bir tür "*ön veri*"[23] veya "*üst/ özet veri*"[24] olduğu görülmektedir. Bununla birlikte, mezkûr verilerin "ön" veya "özet" veriler olarak nitelendirilmesi, bu verilere erişimin temel hak ve hürriyetlerle ilgisinin bulunmadığı anlamına gelmemektedir. Zira internet trafik bilgisi, IP adresi, port (bağlantı yolu) bilgisi, internet bağlantısının başlangıç ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve abone kimlik bilgileri gibi çok sayıda veriyi içermektedir.

Mahiyeti gözetildiğinde bu verilerin bir kısmının (IP ve abone kimlik bilgileri) "doğrudan", diğer bir kısmının ise (giriş yapılan internet siteleri vs.) "dolaylı olarak" bir gerçek kişiyi tanımlamaya elverişli "kişisel veri" niteliğinde olduğu açıktır[25]. Avrupa Konseyi'nin Ceza Yargılamasında ve Kolluk Teşkilatında Verilerin Korunmasına İlişkin 2016/680 Sayılı Direktif'ine göre ceza yargılaması sırasında kişisel verilerin işlenmesi bakımından da "*hukuka uygun ve adil işleme*", "*belirli, açık ve meşru amaçlarla işleme*", "*amaca uygun, amaçla bağlantılı ve ölçülü işleme*", "*doğru ve güncel halde bulunma*" ve

---

[22] Vekil sunucu bilgilerinin tutulmasındaki amacın, toplu internet hizmeti veren kurum ve kuruluşların kendi kullanıcıların yönelik iç trafik bilgilerini tutmak olduğu hususunda bkz. Servet Yetim, '5651 Sayılı Yasa Kapsamında Tutulan İnternet Trafik Bilgilerinin Özel Hayat ve Hayatın Gizliliği Kapsamında Değerlendirilmesi', (2013) (36) Terazi Hukuk Dergisi, 55, 56-57.

[23] Alman hukukundaki bu tanımlama ve Alman hukukunda bu verilerin tutulması bakımından büyük bir politik mücadele bulunduğu hususunda bkz. Stephan Beukelmann, 'Ceza Hukukuna İlişkin Sınırlar Olmaksızın İnternette Gezinti Yapmak" (Çev. Yener Ünver) içinde Yener Ünver (edt) İnternet Hukuku (Karşılaştırmalı Güncel Ceza Hukuku Serisi 13) (1. Baskı, Seçkin Yayınevi 2013) 294.

[24] *"internet trafik kayıtlarını içeren ve operatörler tarafından tutulan CGNAT (HIS) kayıtları ise bir çeşit üst veridir*" Yargıtay CGK, 16-41/513, 27.06.2019. Bu tür verilerin "tek başına" ispata elverişli olmadığı hususunda bkz. Yargıtay 16. CD, 10769/ 252, 27.01.2021; Yargıtay 3 CD, 12704/8722, 12.03.2025; Yargıtay 3 CD 1479/2313, 04.07.2018.

[25] Birtek (n 1) 669.

"*işlenme amacına uygun süre kadar tutulma*" ilkelerine uygun hareket edilmesi gerekmektedir[26].

Anayasa Mahkemesi'ne göre de "*trafik bilgisi adı altında istenen bilgiler genel anlamda belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin bütün bilgileri ifade eden kişisel veri kavramı içerisindedir"* Yüksek Mahkeme'ye göre ""*Trafik bilgisi adı altında temin edilecek olan bilgiler Anayasa ile teminat altına alınan iletişimin gizliliği, düşünce ve ifadeyi yayma özgürlüğü, haberleşme özgürlüğü, kişisel verilerin korunması gibi birçok temel hakla doğrudan ilgili*"dir[27].

Yukarıda da açıklandığı üzere internet trafik bilgilerinin sadece kişisel verilerle değil aynı zamanda ifade ve haberleşme özgürlükleriyle de yakından ilgisi bulunduğundan, hukuka aykırı olarak (kanuni bir dayanak ve meşru bir amaç olmaksızın ve ölçüsüz bir şekilde) bir kimsenin internet trafik bilgilerine müdahale edilmesi, belirtilen temel hak ve hürriyetlerin ihlaline neden olabilecektir[28]. Bu sebepledir ki; internet trafik bilgilerinin gizliliği esas olmalıdır. Bu verilere yetkisiz ve hukuka aykırı erişim, aynı zamanda kişilik haklarını da tehlikeye sokmaktadır[29]. Bu tehlike öngörülerek 5809 sayılı Elektronik Haberleşme Kanunu'nun m. 51/2 hükmünde şu şekilde bir güvenceye yer verilmiştir: "*Elektronik haberleşmenin ve ilgili trafik verisinin gizliliği esas olup, ilgili mevzuatın ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının rızası olmaksızın haberleşmenin dinlenmesi, kaydedilmesi, saklanması, kesilmesi ve takip edilmesi*

---

[26] Ayrıntılı açıklama ve ilkeler hakkında bkz. Murat Volkan Dülger ve Onur Özkan, 'Kolluk Teşkilatında ve Ceza Yargılamalarında Kişisel Verilerin Korunması: "Unutulan" Direktifin Kapsamlı ve Karşılaştırmalı Analizi' (2020) (42) Ceza Hukuku Dergisi, 85, 99 vd.

[27] Anayasa Mahkemesi, 149/151, 02.10.2014. Anayasa Mahkemesi'ne göre "...***IP adresi…"*** belli bir kişiyi doğrudan veya dolaylı olarak tanımlayabilecek bir veri olduğundan kişisel veri olarak kabul edilmektedir. Aynı yönde bkz Anayasa Mahkemesi, 122/74, 09.04.2014; 74/201, 25.12.2014; 180/30, 19.03.2015.

[28] Amerikan hukukunda IP adres bilgileri ile e posta trafik bilgilerinin mahremiyetinin bulunmadığı ve Anayasa'nın Ek 4. maddesinin (koruma tedbirlerine ilişkin güvenceleri içeren anayasa hükmünün) koruması altında kabul edilmediği hususunda bkz. Deborah Buckner, 'Internet Search and Seizure in United States v. Forrester: New Problems in the New Age of Pen Registers' (2008) 22 (2) BYU Journal of Public Law 499, 501 vd.

[29] BverfGE 120, 274- NJW2008, 822 Knr. 177'den nakleden Beukelmann (n 23) 286.

yasaktır". Bu güvence yok sayılarak internet trafik verilerine müdahale edilmesi, TCK m 132 ve 134 kapsamında cezalandırılabilir bir eylem olarak karşımıza çıkmaktadır.

Anayasa Mahkemesi, hiçbir meşru sebep gösterilmeksizin trafik bilgilerine idari mercilerin doğrudan doğruya ve sınırsız bir erişim imkanının bulunmasını Anayasa'ya aykırı bulmuştur[30].

İnternete bağlanan aracın elektronik sistemler marifetiyle gerçekleştirdiği veri akışının incelenebilmesi "*belli bir adrese [IP adresine] gönderilen veri paketlerinin tamamının toplanması ve bu yolla iletişimin alanının yeniden canlandırılmasına*"[31] bağlıdır. Bu sebeple Anayasa Mahkemesi tarafından da vurgulandığı üzere, trafik bilgilerinin tutulması "*ciddi suçların tespiti, soruşturulması ve kovuşturulmasında kullanılmak*" amacına (meşru amaçların gerçekleştirilmesine) yönelik olmalıdır[32]. Nitekim 5809 sayılı Kanun'un m. 51/2 hükmünde belirtilen "yargısal amaçlar" ve mevzuatta açıkça belirtilen haller dışında, internet trafik bilgilerine sınırsız bir erişimin Anayasal bir dayanağı bulunmadığı gibi bu tür

---

[30] Anayasa Mahkemesi, 5651 sayılı Kanun'un m. 3/4 hükmünde yer alan "*(Ek: 26/2/2014-6527/16 md.; Değişik: 10/9/2014-6552/126 md.) Trafik bilgisi Telekomünikasyon İletişim Başkanlığı tarafından ilgili işletmecilerden* temin *edilir ve hâkim tarafından karar verilmesi hâlinde ilgili mercilere verilir"* düzenlemesi Anayasa Mahkemesi tarafından iptal edilmiştir. Yüksek Mahkeme'ye göre "*Trafik bilgisi adı altında temin edilecek olan bilgiler Anayasa ile teminat altına alınan iletişimin gizliliği, düşünce ve ifadeyi yayma özgürlüğü, haberleşme özgürlüğü, kişisel verilerin korunması gibi birçok temel hakla doğrudan ilgili olup bu bilgilerin TİB tarafından herhangi bir kurala ve sınırlamaya tabi olmaksızın istenildiği zaman ve şekilde elde edilebilir olması temel hak ve özgürlüklerin doğrudan ihlaline sebebiyet vermektedir*". Anayasa Mahkemesi, 01.10.2014 tarih, E. 2014/149, K. 2014/151. Danıştay da benzer bir gerekçeyle Yönetmelik'te yer alan hükmün iptaline karar vermiştir. Danıştay'a göre "*…anılan düzenlemelerin kapsamına giren bir hususun Başkanlık tarafından istenilebilmesi için yasal düzenlemede belirtilen kişilerin bu konuda karar vermesi zorunlu olmasına rağmen, dava konusu düzenleme ile erişim sağlayıcılara, bildirimi için ilgili makamların kararı olması zorunlu olanlar yönünden herhangi bir ayrıma gidilmeksizin Başkanlığın uygun gördüğü bilgileri talep edildiğinde bildirme zorunluluğunun getirildiği, böylece Başkanlığın isteyeceği her türlü bilginin, bu konuda ilgili makamların bir kararı olmasa da Başkanlığa verilmesi gerektiği şeklinde anlaşılmaya sebep olacak şekilde düzenleme yapıldığı görüldüğünden, dava konusu Yönetmeliğin 8. maddesinin 1. fıkrasının (b) bendinde hukuka uygunluk bulunmamaktadır*" Danıştay 13 D, 239/4266, 01.12.2019. Karar için bkz <https://cdn.bartin.edu.tr/personel/ecf292227efb77dbdc4ccb91b19d8031/5-danistay.pdf>

[31] Kudlich (n 14) 304.

[32] Anayasa Mahkemesi, 149/151, 02.10.2014.

bir erişim (ve temel haklara müdahale) demokratik toplumlarda gerekli ve ölçülü bir müdahale olarak da kabul edilemez.

Belirtmek gerekir ki; meşru amaçların bulunması ülkede yaşayan herkesin "*günün birinde suç işleyebileceği ve geçmişe yönelik olarak internet trafik bilgilerine de bu maksatla erişme imkanının bulunması gerektiği*" biçimindeki bir düşünceyi haklı kılmaz. Meşru amaçların mevcut olması, ülkede yaşayan bütün bireylerin "*potansiyel suçlu*" olarak kabul edilmesini haklı ve ölçülü kılmaz[33]. İnternet trafik verilerinin tutulmasındaki amaçlarla bireylerin temel hak ve özgürlüklerinin mahremiyetinin korunması arasında bir denge kurulması gerekmektedir[34]. Bütün bireylerin "potansiyel" suçlu olarak görülerek bütün internet erişim bilgilerinin –sınırsız- bir şekilde toplanması masumiyet karinesiyle bağdaşmaz[35]. Bu sebeple hangi suçlar bakımından (ve hangi koşullarda) internet trafik bilgilerine erişilebileceğinin açık bir şekilde düzenlenmesine ihtiyaç bulunmaktadır. Uygulamada, Bilgi Teknolojileri ve İletişim Kurumunun (BTİK'nin) internet trafik verilerine "sınırsız" erişim imkanının bulunduğu görülmektedir[36].

---

[33] Bu gerekçeyle Avrupa Adalet Divanı, 8 Nisan 2014 tarihli Digital Rights Ireland Ltd. kararında "*herhangi bir ayrım yapmadan her türden verinin bütün Avrupa vatandaşlarını kapsayacak şekilde asgari 6 ay (en fazla 24 ay) süreyle tutulmasının*" ölçülü ve mutlaka gerekli bir müdahale olmadığına karar vermiş (par 56, 64-66) ve bu tür bir müdahaleye imkan tanıyan 2006/24/EC sayılı direktifi iptal etmiştir. Karar metni için bkz. <https://curia.europa.eu/juris/document/document.jsf;jsessionid=BA2896829E49F299F1A18E556FE98C8C?text=&docid=150642&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=14070230> erişim tarihi 30.11.2025.

[34] Birtek (n 1) 672.

[35] David Heger, 'Büyük Veri ve Suçsuzluk Karinesi' içinde Kayıhan İçel ve Yener Ünver (edt) Ceza Hukukunda Robot, Yapay Zekâ ve Yeni Teknolojiler (Karşılaştırmalı Güncel Ceza Hukuku Serisi 21) (1. Baskı, Seçkin Yayıncılık, 2021) 486. Yargıtay 9. CD de "…*amacı ne olursa olsun hiçbir kuruma demokratik bir hukuk devleti olan Türkiye Cumhuriyeti'nde yaşayan insanlar şüpheli görülerek ülke genelini kapsayacak şekilde yetki verilemeyeceği"ne* karar vermiş (Yargıtay 9. CD., 874/7160, 04.06.2008) ve Ceza Genel Kurulu da şüpheliye ulaşabilmek/ şüpheliyi tespit edebilmek için belli bir baz istasyonundan haberleşen bütün kişilerin iletişiminin tespit edilmesini ("*baz sorgu yapılmasını*") hukuka aykırı bulmuştur (Yargıtay CGK, 6-140/222, 15.11.2011).

[36] BTİK'nin 24.10.2018 tarih ve 2018/DK-BSD/314 sayılı kararı ile Abone Desen Bilgileri olarak tanımlanan "*taraflara ilişkin IP adresi, port bilgisi, verilen hizmetin başlama ve bitiş¸ zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgileri*" yine Kurul'un 15.12.2020 tarihli ISS Trafik Log Deseni konulu kararı ile (dinamik IP kullanılan durumlar bakımından tam bir tespit yapılabilmesi için) her saat başı BTK'ye bildirilmesi işletmecilerden talep edilmiştir (BTİK'nin aynı karar çerçevesinde "Anne

Belirtmek gerekir ki; hukukumuzda, istihbari amaçla internet trafik bilgilerine hangi suçlar için başvurulabileceği açıkça 2559 sayılı Kanun'un Ek Madde 7 hükmünde belirtilmiş olmasına rağmen[37], suç soruşturması veya kovuşturması amacıyla internet trafik bilgilerine erişim "*genel yetki*" içerisinde değerlendirilmekte ve suç tipi yönünden bir sınırlandırma yapılmaksızın bütün suçlar bakımından internet trafik bilgilerine erişim mümkün kabul edilmektedir[38].

İnternet trafik bilgilerine, suç soruşturması veya kovuşturması sırasında ihtiyaç duyulabilmektedir[39]. Zira özellikle doğrudan bilişim sistemleri aracılığıyla işlenen ve "salt bilişim suçu" olarak tanımlayabileceğimiz suç tiplerinde ceza muhakemesinin klasik delil

---

Kızlık Soyadı", "Mesleği", "Cinsiyeti", "Uyruğu", "POP Bilgisi", "Adres", "Mail Adresi" ve "Doğum Yeri" gibi bilgileri de talep ettiği aşağıda yer verilen Danıştay kararındaki karşı oy gerekçesinden anlaşılmaktadır). Kurul'un bu kararları, Anayasa Mahkemesi'nin 5651 sayılı Kanun'un m. 3/4 hükmünün iptaline ilişkin kararı ve kararda yer verilen gerekçeler dikkate alındığında, Kurul'un zikredilen her iki kararının ve 2019 yılından bu yana devam eden uygulamanın yasal bir dayanağının bulunmadığı hususunda bkz. Elif Yorgancıoğlu ve Yusuf Tunç Demircan, 'Bilgi Teknolojileri ve İletişim Kurumu Tarafından Toplanan İnternet Trafik Verilerinin Kişisel Verilerin Korunması Hakkı Bağlamında Değerlendirilmesi' (2023) 22 (48) İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, 1189, 1195 vd; Birtek (n 1) 674, dn. 35. Danıştay, sözü edilen Kurul kararının iptali istemiyle açılan davada, iptal istemini reddetmiştir Danıştay, 13 D, 23.05.2023, E. 2019/2412, K. 2023/2555, <www.danistay.gov.tr> erişim tarihi 30 Kasım 2025. Kararın eleştirisi için bkz. Birtek (n 1) 677, dn. 35.

[37] Maddede yer verilen suçlar "*casusluk suçları hariç, 250 nci maddesinin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçlar ile bilişim suçları*"dır. "*250 nci maddesinin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçlar*" ifadesinden anlaşılması gereken ise (Bkz. 6352 s. Kanun m 105 ve 3713 sayılı Terörle Mücadele Kanunu Geçici Madde 14'e göre "*a) Örgüt faaliyeti çerçevesinde işlenen uyuşturucu ve uyarıcı madde imal ve ticareti suçu veya suçtan kaynaklan malvarlığı değerini aklama suçu, b) Haksız ekonomik çıkar sağlamak amacıyla kurulmuş bir örgütün faaliyeti çerçevesinde cebir ve tehdit uygulanarak işlenen suçlar, c) İkinci Kitap Dördüncü Kısmın Dört, Beş, Altı ve Yedinci Bölümünde tanımlanan suçlar (305, 318, 319, 323, 324, 325 ve 332 nci maddeler hariç)*"dır.

[38] Birtek (n 1) 682, dn 51.

[39] 5809 sayılı Elektronik Haberleşme Kanunu'nun m. 51/7 hükmüne göre "*Trafik verileri; trafiğin yönetimi, arabağlantı, faturalama, usulsüzlük/dolandırıcılık tespitleri ve benzeri işlemleri gerçekleştirmek veya tüketici şikâyetleri ile arabağlantı ve faturalama anlaşmazlıkları başta olmak üzere, uzlaşmazlıkların çözümü amacıyla sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı kalmak kaydıyla işlenir ve bu uzlaşmazlıkların çözüm süreci tamamlanıncaya kadar gizliliği ve bütünlüğü sağlanarak saklanır. Katma değerli elektronik haberleşme hizmetlerinin sunulması ya da elektronik haberleşme hizmetlerinin pazarlanması amacıyla ihtiyaç duyulan trafik verileri ile konum verileri anonim hâle getirilerek veya ilgili abonelerin/kullanıcıların açık rızalarının alınması ve sadece işletmeci tarafından yetkilendirilen kişilerle sınırlı kalmak kaydıyla, belirtilen faaliyetlerin gerektirdiği ölçü ve sürede işlenebilir*". Anılan düzenlemeye göre internet trafik bilgileri, internet erişim hizmetine ilişkin özel hukuk uyuşmazlıkların çözümlenebilmesi için de tutulması gereken bilgilerdir.

türleri söz konusu olmadığı gibi neredeyse yegâne "somut" delil internet trafik bilgisi olarak karşımıza çıkmaktadır. Örneğin; TCK m. 243/1 hükmü kapsamında "bilişim sistemine girme" suçunun sübutu bakımından yegâne delil, sisteme giriş yapıldığını gösteren dijital kayıtlardır[40].

Bilişim sistemleri aracılığıyla işlenen ve "*dolaylı bilişim suçları*" olarak tanımlanan suç tipleri bakımından ise klasik deliller (beyan, belge ve belirti) ispat aracı olarak mevcut olsa dahi maddi gerçeğe ulaşılabilmesi için internet trafik bilgilerine ulaşma ihtiyacı söz konusu olabilmektedir[41]. Örneğin; bilişim sistemleri marifetiyle işlenen dolandırıcılık suçu (TCK m 158) bakımından, bilişim sistemi marifetiyle işlenen "*hileli davranışların*" kim tarafından gerçekleştirildiğinin ispatı (failin tespiti) doğrudan doğruya bilişim aracının (bilişim sisteminin) kim tarafından kullanıldığının ispatına bağlıdır[42]. Bu sebepledir ki; internet trafiğine ilişkin olarak tutulan ve depolanan verilerin, suç soruşturması ve kovuşturması amacıyla talep edilmesi 5809 sayılı Elektronik Haberleşme Kanunu'nun m. 51/2 hükmü kapsamında "*yargı kararı*" istisnası içerisinde değerlendirilmelidir.

Doğrudan ve dolaylı bilişim suçlarına ilişkin maddi gerçeğin ortaya çıkarılması bakımından taşıdığı önem sebebiyle kanun koyucu, internet trafik bilgilerinin tutulmasını zorunlu kılmıştır.

---

[40] Avrupa Konseyi Siber Suç Sözleşmesi kapsamında "*depolanmış*" ve "*akış halindeki/ gerçek zamanlı*" internet trafik verilerinin tutulması ve bu verilere erişim hususunda bkz. Yavuz Erdoğan, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri* (1. Bası, Legal Yayıncılık 2018) 164, 257.

[41] Yargıtay'a göre "…*gerçeğin tereddüte mahal vermeyecek şekilde tespiti için paylaşımların yapıldığı sitenin Türkiye Temsilciliğinden bahse konu hesabın kim tarafından kullanıldığının, hesaba erişildiğindeki zaman bilgisinin ve IP numarası ile, IP verisinden kişinin kim olduğunun sorulması, IP ve zaman bilgisi ile abone bilgilerinin temini, bunun mümkün olmaması halinde ise, suça konu paylaşımların yapıldığı telefon bilgisayarın IP numarasının kime ait olduğunun, suç tarihinde kim tarafından kullanıldığının ilgili kurum, şirket ve internet sağlayıcılardan talep edilerek tespit edilmesi, gerektiğinde uzman bilirkişiden rapor alınması*" gerekir. Yargıtay 8 CD, 5557/19, 06.01.2025, <www.kazanci.com> erişim tarihi 30 Kasım 2025.

[42] Ceza muhakemesi açısından ispat aracı olarak kullanılabilecek verilere ilişkin çokluğun (veri bolluğunun), savunma açısından yapılandırılması hususunda savunmanın "*tek başına savaşçı*" haline geldiği ve avukatlar açısından çok büyük bir "*meydan okuma*" olduğu hususunda bkz. Beukelmann (n 23) 296.

5651 s. Kanun'un m. 2/1-e ve 5/3 hükümlerine göre "*hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişi"* yer sağlayıcının, *"yer sağladığı hizmetlere ilişkin trafik bilgilerini bir yıldan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakla yükümlüdür*".

Yine Kanun'un 2/1-e ve 6/1-b hükümleri uyarınca "*kullanıcılarına internet ortamına erişim olanağı sağlayan gerçek veya tüzel kişi" erişim sağlayıcı,* "s*ağladığı hizmetlere ilişkin, yönetmelikte belirtilen trafik bilgilerini altı aydan az ve iki yıldan fazla olmamak üzere yönetmelikte belirlenecek süre kadar saklamakla ve bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini sağlamakl*a" yükümlüdür.

5651 sayılı Kanun'dan kaynaklanan "*tutma ve depolama*" 5809 sayılı Elektronik Haberleşme Kanunu'nun m. 51/2 hükmü kapsamında yer alan "*mevzuatın öngördüğü*" tutma istisnası kapsamındadır.

İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik ile (m. 8/1-b) erişim sağlayıcı "Başkanlığın *[BTİK'nin] uygun gördüğü bilgileri talep edildiğinde bildirmekle*" yükümlü kılındığı halde, bu yetki Danıştay tarafından "*anılan düzenlemelerin kapsamına giren bir hususun Başkanlık tarafından istenilebilmesi için yasal düzenlemede belirtilen kişilerin bu konuda karar vermesi zorunlu olmasına rağmen, dava konusu düzenleme ile erişim sağlayıcılara, bildirimi için ilgili makamların kararı olması zorunlu olanlar yönünden herhangi bir ayrıma gidilmeksizin Başkanlığın uygun gördüğü bilgileri talep edildiğinde bildirme zorunluluğunun getirildiği, böylece Başkanlığın isteyeceği her türlü bilginin, bu konuda ilgili makamların bir kararı olmasa da Başkanlığa verilmesi gerektiği şeklinde anlaşılmaya sebep olacak şekilde düzenleme yapıldığı görüldüğünden*" hukuka aykırı bulunmuştur[43].

[43] Danıştay 13 D, 239/4266, 01.12.2019. Karar için bkz. <https://cdn.bartin.edu.tr/personel/ecf292227efb77dbdc4ccb91b19d8031/5-danistay.pdf> erişim tarihi 30.11.2025.

Ancak aynı Danıştay, bu karardan dört yıl sonra (2023 yılında), BTİK'nin 24.10.2018 tarih ve 2018/DK-BSD/314 sayılı kararı ile Abone Desen Bilgileri olarak tanımlanan "taraflara ilişkin IP adresi, port bilgisi, verilen hizmetin başlama ve bitiş ¸zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgileri" yine Kurul'un 15.12.2020 tarihli ISS Trafik Log Deseni konulu kararı ile (dinamik IP kullanılan durumlar bakımından tam bir tespit yapılabilmesi için) her saat başı BTK'ye bildirilmesini işletmecilerden talep etmesine ilişkin BTİK (Kurul) kararına yönelik iptal istemini reddetmiştir.

Danıştay'a göre "…*5809 sayılı Kanun, 5397 sayılı Kanun (2559 sayılı, 2803 sayılı ve 2937 sayılı Kanunlar), 5271 sayılı Kanun, 671 sayılı Kanun Hükmünde Kararname ve 5651 sayılı Kanunların ilgili maddeleri uyarınca davalı idareye verilen görev ve yükümlülüklerin süresinde, eksiksiz ve aksama olmaksızın yerine getirilebilmesi amacıyla, Kurum'un işletmeciler, kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerden ihtiyaç duyulan her türlü bilgi ve belgeyi almak ve gerekli kayıtları tutmak, işletmecilere bir takım yükümlülükler getirebilmek konusunda kanunî yetkisinin bulunduğu dikkate alındığında, dava konusu Kurul kararlarının yasal dayanağının bulunduğu anlaşılmaktadır."*[44]

Her iki karar arasındaki yaklaşım farklılığının hukuki bakış açısının değişmesinden ziyade "dönemsel koşullardan ve uygulamada ortaya çıkan ihtiyaçlardan" kaynaklandığını düşünmekteyiz. 2023 yılındaki kararda "meşru amaç" ve "demokratik toplumda gereklilik/ ölçülülük" kriterleri bakımından hiçbir değerlendirmenin yapılmamış olması da konuya temel hak ve hürriyetler ekseni açısından bakılmadığını ortaya koyduğundan, içtihat değişikliğinin idari ve adli mercilerin dönemsel ihtiyaçlarının karşılanması amacına yönelik olduğunu değerlendirmekteyiz.

5809 s. Elektronik Haberleşme Kanunu ve 5651 sayılı Kanun hükümleri bir bütün olarak değerlendirildiğinde, internet trafik verilerinin tutulması ve depolanması bakımından Anayasa'nın m. 13 ve 20/son hükümleri kapsamında "*kanunilik/ kanun ile düzenlenme/*

[44] Danıştay, 13 D, 2412/2555, 23.05.2023,< www.danistay.gov.tr> erişim tarihi 30 Kasım 2025.

sınırlanma" koşulunun sağlandığı, temel hak ve hürriyetlere müdahale teşkil eden bu eylemlerin meşru amaçlarının bulunduğu ve bu türden bir sınırlandırmanın demokratik toplumda gerekli (ve ölçülü) bir sınırlandırma olduğu görülmektedir.

Kanun koyucu, "ölçülülük" ilkesinin zorunlu bir sonucu olarak, Kanun'da en fazla iki yıllık süreyle tutulması öngörülen trafik bilgilerinin, bu sürenin sonunda "silinmesi" gerekmektedir. Bununla birlikte Kanun'da "silme" konusunda açık bir yasal düzenlemenin bulunmadığı da ayrıca değerlendirilmelidir[45]. Düşüncemize göre özgürlükler hukuku bakımından, kişisel verilerin "tutulması", sınırlama iken; yasal sürenin sonunda tutulan verilerin "silinmesi", özgürlüktür. Bir temel hak bakımından özgürlük ("silme") asıl; sınırlama ("tutma") istisnadır. Anayasa m 13 uyarınca özgürlük için değil, sınırlama için açık yasal düzenlemeye ihtiyaç vardır. Bu sebeple kişisel verilerin yasal sürenin sonunda "silinmesi" için yasal düzenleme gerekli olmayıp tutma süresinin sonunda kişisel verilerin "silinmesi" gerekir. Nitekim 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) m 7'ye göre işlenmiş kişisel veriler, işlenme sebebi ortadan kalktığında resen veya ilgilinin talebi üzerine veri sorumlusu tarafından "*silinir, yok edilir veya anonim hale getirilir*"[46].

III. ADİL YARGILANMA (GÜVENİLİR DELİL) HAKKI BAKIMINDAN İNTERNET TRAFİK BİLGİLERİNE ERİŞİM

Adil yargılanma hakkı AİHS m. 6 ve Anayasa m. 38'de bir insan hakkı olarak düzenlenmiş ve çifte koruma mekanizması içerisinde kabul edilmiştir. Mahkeme'ye göre mahkûmiyet hükmü tek başına ya da belirleyici bir şekilde bir delile dayanıyorsa bu delilin adil yöntemlerle elde edilmiş ve hakkaniyete uygun bir biçimde değerlendirilmiş olması

[45] Her ne kadar AİHM, AYM ve Yargıtay'ın uygulaması aksi yönde olsa da silinmesi gereken bir verinin silinmemesi ve tutulmaya devam edilmesi hukuka aykırı olduğundan, hukuka aykırı bir şekilde tutulan bir verinin ceza muhakemesinde ispat aracı olarak kullanılabilmesinin mümkün olmadığını düşünmekteyiz. Aksinin kabulü Anayasa m. 20'de ve Kişisel Verilerin Koruması Kanunu'nda kişisel verilerin korunması için yer verilen güvenceleri anlamsız kılar. AİHM ve AYM'nin uygulamasına ilişkin olarak adil yargılanma hakkının mahiyetinden kaynaklanan ve bireysel başvuru yoluna özgü gerekçeler aşağıda ayrı başlıklar altında ele alınacaktır.

[46] KVKK'nin "istisnalar"ı düzenleyen m 28/2-a bendinde "suç önleme veya suç soruşturması" amacıyla yapılan müdahaleler bakımından bazı istisnalar kabul edilse de bu istisnalar bakımından da "*Kanunun amacına ve temel ilkelerine uygunluk ve orantılı olma*" güvencelerine yer verildiği görülmektedir.

gerekmektedir. Bu prensip, "*güvenilir delil hakkı*" olarak da tanımlanmaktadır[47]. Bu hak, ceza muhakemesinde, tek taraflı ve doğruluğu kanıtlanmamış, elde edilmesi ve işlenmesi konusunda güvenilirliği şüpheli bir bulgunun muhakemeye konu edilmesini ve hükme esas alınmasını engellemektedir[48].

Mahkeme, herhangi bir delil türünün ispat gücü veya değerlendirme yönteminden ziyade, "güvenilir delil hakkı"nın ihlâl edilip edilmediğini nazara almaktadır[49]. Bu bağlamda, yargılama iç hukuktaki usul kurallarına uygun yapılmış, ilgili taraf kendi delillerini ve iddialarını sunma fırsatı bulmuş ve bunlar yargılama makamı tarafından gereği gibi dinlenmiş, olayın ve hukuki sorunun bütün unsurları dikkate alınarak yeterli gerekçe ortaya konulmuşsa AİHM başvuruyu temelsiz bulabilir[50].

AİHM uygulamasına göre bir bulgunun delil olarak kabul edilip edilemeyeceği veya bir maddi vakıanın hangi delille ve ne zaman ispat edilmiş sayılacağı konusunda ülkelerin geniş bir takdir hakkı bulunmaktadır[51]. Zira AİHM tarafından yapılan denetimin amacı, ülkedeki iç hukuk normlarının nasıl uygulandığı (yerindeliği) olmayıp soruşturma ve kovuşturma sırasında adil yargılanma hakkına ilişkin güvencelerin hayata geçirilip geçirilmediğidir[52]. AİHS hükümleri ve AİHM denetimi "yargılamanın sonucuna yönelik"

---

47 Dovydas Vitkauskas ve Grigoriy Dikov, *Avrupa İnsan Hakları Sözleşmesi Kapsamında Adil Yargılanma Hakkının Korunması*, (Çev. Serkan Cengiz) Avrupa Konseyi İnsan Hakları El Kitapları (Avrupa Konseyi 2012) 79-81.

48 Fatih Birtek, 'Suç İşlenmesini Önleme Amacıyla PVSK Ek Madde 7 Kapsamında Uygulanan Tedbirlerden Elde Edilen Bilgilerin Ceza Muhakemesinde Delil Olarak Kullanılıp Kullanılamayacağı Sorunu' içinde Fatih Birtek (edt) *Hukuk Devletinde Kolluğun Suç Önleme Yetkisi (Kaynağı, Kapsamı ve Sınırları)* (1. Baskı Adalet Yayınevi 2024) 655.

49 Vitkauskas ve Dikov (n 45) 79-81.

50 Cüneyt Durmaz, 'Esasa İlişkin Kabul Edilemezlik Nedenleri, Bireysel Başvuru İnceleme Usulü ve Kabul Edilebilirlik Kriterleri', Ed. Musa Sağlam (2. Baskı, Anayasa Mahkemesi Yayınları 2013) 233. Birtek (n 6) 350 vd.

51 *Edwards v Birleşik Krallık* (1992) par 34; *Barbera, Messeque ve Jabardo v İspanya* (1998) par 68.

52 *Boner v Birleşik* (1998) par 43; *Baykov v Rusya* (2009) par 89.

(bir bütün olarak adli ve hakkaniyete uygun bir yargılama yapılıp yapılmadığına yönelik) kuralları içermektedir[53].

AİHM, gizli soruşturmacı görevlendirilmesi ve işkence ve gayri insani veya zalimane muamele yasağının ihlal edildiği hallerde başkaca bir değerlendirmeye gerek olmaksızın adil yargılanma hakkının ihlal edildiğini kabul etmektedir[54]. Ancak diğer hallerde, "tuzağa düşürme" niteliği taşımadıkça[55] ve bir delil "tek veya belirleyici" delil olmadıkça, delilin hukuka aykırı olup olmadığını değil bir bütün olarak yargılamanın adil ve hakkaniyete uygun bir karakterde olup olmadığını denetlemektedir. AİHM, delilin hukuka aykırılığına ilişkin iddialardan ziyade, başvuranın meseleyi ulusal mahkemeler önünde ileri sürme fırsatına (savunma hakkına) sahip olup olmadığıyla ilgilenmektedir[56]. AİHM'nin bu yaklaşımı "ikincillik prensibinin" bir yansıması olup AİHM'nin dördüncü derece mahkemesi olarak hareket etmesini engellemektedir[57].

A. AİHM'nin Yaklaşımı

AİHM uygulamasında, iletişimin bütün türlerine ilişkin bilgiler (internet trafik bilgisi de dahil olmak üzere) özel yaşamla ilişkilendirilmekte ve özellikle iletişimde kullanılan mobil hatta ilişkin trafik verilerinin zorunlu olarak depolanması, haberleşme özgürlüğüne yönelik bir müdahale olarak değerlendirilmektedir[58]. Ancak kolluğun/ polisin, kötüye kullanıma ilişkin yasal güvenceler mevcut olmaksızın ve mahkeme kararına dayanmaksızın

---

53 Durmuş Tezcan, Mustafa Ruhan Erdem ve Oğuz Sancakdar, *Avrupa İnsan Hakları Sözleşmesi Işığında Türkiye'nin İnsan Hakları Sorunu* (Seçkin Yayıncılık 2004) 309.

54 Osman Doğru ve Atila Nalbant, *İnsan Hakları Avrupa Sözleşmesi,* 2. Cilt (Avrupa Konseyi ve Yargıtay Başkanlığı Yayını 2013) 641; Birtek (n 6) 355 vd.

55 *Ramanauskas v Litvanya* (2008) par 48, 74.

56 Vitkauskas ve Dikov (n 45) 82.

57 *Schenk v İsviçre* (1998) par 45-49.

58 *Ekimdzhiev ve Diğerleri v Bulgaristan* (2022) par 372-374.

doğrudan internet trafik bilgilerine ve elektronik iletişim aracının sahibine ilişkin (abone vs.) bilgilere erişmesinin Sözleşme'ye[59] uygun olmadığı kabul edilmektedir[60].

AİHM, tedbire muhatap olacak kişi kategorisinin ve tedbire muhatap olacak kişilerin isimlerinin veya tariflerinin yetkili merciin kararında belirtilmesi, masum insanlara ait verilerin sınırsız süreyle tutulmaması, müdahale edilecek bilgilerin türünün, tedbirin alınabileceği koşulların belirlenmesi ve hangi süreyle tutulacağına/arşivleneceğine ve hangi süreyle bilgiye ulaşılabileceğine dair bir sınırlamanın (süre sınırlamasının) kanunda yer alması, kamu makamlarına tanınan takdir yetkisinin kapsamının ve kullanılma şeklinin kanunda makul bir açıklıkta belirtilmesi ve nihayet kötüye kullanımı engelleyecek yasal tedbirlerin bulunması halinde, internet trafik verilerine erişimin Sözleşme'ye uygun olacağı düşüncesini benimsemektedir[61].

Yüksel Yalçınkaya/ Türkiye kararında, internet trafik verilerinin mevzuatta öngörülen süreden daha uzun süre tutulduğu ve mahkûmiyet hükmüne esas alındığı şikayeti bakımından "*başvuran tarafından hem ulusal mahkemeler hem de Mahkeme önünde itiraza konu edilmiş olması*" (par 320) ve "*yasal süre sınırı dışında elde edildiği varsayılsa bile, başvuran tarafından aksi yönde herhangi bir argüman sunulmadığı sürece, bu durumun söz konusu kayıtların teknik doğruluğu üzerinde herhangi bir etkisi olmayacağını*" (par 321) kabul etmiştir[62].

Avrupa Adalet Divanı'nın 06.10.2020 tarihli La Quadrature du Net ve Diğerleri kararına göre ise iletişim aracı sahibinin sivil kimliğine ilişkin bilgilerin herhangi bir süreye sınırlamasına bağlı olmaksızın saklanabilmesi mümkün iken; *trafik ve konum verileri* ise

---

59 Avrupa İnsan Hakları Sözleşmesi, AİHS, 1950 Roma.

60 *Benedik v Slovenya* (2018) par 120-134.

61 AİHM uygulaması ve ilgili kararlar için bkz Birtek (n 1) 678-679.

62 *Yüksel Yalçınkaya v Türkiye* kararı (2023) par 320-321. AİHM bu kararında "*başvuranın aleyhindeki delillere itiraz etme ve savunmasını etkili bir şekilde ve iddia makamıyla eşit bir şekilde yürütme fırsatına sahip olmasını sağlamak için yeterli güvencelerin bulunmadığı*" gerekçesiyle ihlal kararı vermiştir (par 341). Kararın Türkçe çevirisi HUDOC'tan alınmıştır. Bkz. <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-228393%22]}> erişim tarihi 30 Kasım 2025.

ulusal güvenliğe yönelik mevcut veya öngörülebilir "kanıtlanmış" ciddi bir tehdit söz konusu olduğunda kesin olarak belirlenmiş bir süre boyunca saklanabilir. Tehdit devam ederse, süre uzatılabilir[63].

B. Anayasa Mahkemesi'nin Yaklaşımı

Anayasa Mahkemesinin "güvenilir delil hakkı"na yaklaşımı, AİHM ile paralellik arz etmektedir[64]. Anayasa Mahkemesi de işkence ve gayri insani veya zalimane muamele yasağını ihlal eden haller dışında, "tek veya belirleyici delil" mahiyetinde olmadıkça, delilin hukuka aykırılığına ilişkin şikayetleri, kanun yolu şikâyeti olarak değerlendirmektedir. Mahkeme, "…*delillere yönelik hukuka aykırılık iddialarıyla ilgili olarak başvuruculara delillerin gerçekliğine itiraz etme ve kullanılmalarına karşı çıkma fırsatı verilip verilmediğini, bu konuda silahların eşitliği ve çelişmeli yargılama ilkelerinin gözetilip gözetilmediğini, savunmanın menfaatlerinin korunması için onlara yeterli güvenceler sağlanıp sağlanmadığını*" incelemektedir[65].

Mahkemeye göre "*Bir delilin, diğer yan delillerle desteklenmemiş olması, mutlak surette adil yargılanma hakkı bakımından sorun oluşturmaz. Mahkemece hükme esas alınan bir delilin çok kuvvetli olması ve güvenirliği konusunda herhangi bir risk bulunmaması, destekleyici delillere olan ihtiyacın yoğunluğunu azaltır. Buna karşılık, gücü ve güvenilirliği konusunda birtakım şüpheler bulunan bir delilin, suçun sübutu konusunda ulaşılan vicdani kanaat bakımından belirleyici olması halinde, bu durum, hakkaniyete uygun yargılanma hakkı bakımından sorun oluşturabilir*"[66].

Yakın tarihli bir kararında Yüksek Mahkeme, delilin hukuka aykırılığı iddiasına dayanan şikayetlerin bulunduğu adil yargılanma hakkına ilişkin başvurular bakımından *üç aşamalı test* geliştirmiştir. Buna göre hukuka aykırılığı ilk bakışta anlaşılmıyorsa veya

63 Karar için bkz. Birtek (n 1) 679, dn. 44.

64 Anayasa Mahkemesinin yaklaşımı için bkz. Orhan Kılıç (GK), 2014/4704, 01.02.2018, par 42 vd.

65 Orhan Kılıç (GK), 2014/4704, 01.02.2018, par 48; Hacı Karabulut (2), 2020/27959, 20.03.2025, par 63 vd.

66 Gülüzar Erman, 2012/542, 04.11.2014, par 63.

hukuka aykırılık konusunda mahkemelerce yapılmış bir tespit bulunmuyorsa (ilk aşama), tek veya belirleyici delil olarak kullanılmamışsa (ikinci aşama) ve tek veya belirleyici delil olarak mahkumiyete esas alınan delil yargılamanın bütününü hakkaniyete aykırı hale getirmiyorsa (üçüncü aşama) adil yargılanma hakkının ihlal edilmediğine karar vermektedir[67].

Anayasa Mahkemesine göre "*kişisel veri kapsamındaki internet trafik verilerinin mevzuatta belirtilen süre sonunda yok edilmemesi ve hukuka aykırı şekilde kullanılmasının somut olayın koşullarına göre kişilik haklarına yönelik bir eylem olarak kabul edilebilir*"[68]. Bununla birlikte aynı kararda, mevzuatta belirtilen süreden daha uzun süre "tutma" eyleminin ilgili şirketlerin ve BTİK'nin kurumsal faaliyet niteliğindeki işlemlerinden kaynaklanması halinde, kasıtlı veya ihmali bir eylem tespit edilmedikçe, bireysel ceza sorumluluğunun söz konusu olamayacağına (ve bu konuda etkili başvuru yolunun hukuk ve idare mahkemeleri nezdinde tazminat davası yolu olduğuna) işaret etmiştir[69].

Anayasa Mahkemesinin yaklaşımına göre "trafik verileri" daha uzun süre tutulmuş olsa dahi tutulan verilerin suç soruşturması veya kovuşturması sırasında kullanılması ve hükme esas alınması tek başına adil yargılanma hakkını ihlal etmez[70]. Ancak bu verilerin doğruluğunun güvenilirliğinin sınanması için yapılan itirazların ve bilirkişi incelemesi taleplerinin kabul edilmemesi, adil yargılanma hakkını (silahların eşitliği ve çelişmeli yargılama ilkelerini) ihlal eder[71].

---

67 Hacı Karabulut (2), 2020/27959, 20.03.2025, par 67.

68 Erhan Erçıktı (2), 2018/14040, par 48.

69 Erhan Erçıktı (2), 2018/14040, par 51. Erhan Erçıktı (3), 2018/14040, 30.06.2021, par 52.

70 HTS kayıtlarına ilişkin değerlendirme için bkz Murat Albayrak, 2020/16168, 08.03.2023, par 107.

71 Esra Saraç Arslan, 2019/10514, 28.12.2022, par 59.

IV. SUÇ SORUŞTURMASI VE KOVUŞTURMASI SIRASINDA İNTERNET TRAFİK BİLGİLERİNE ERİŞİM VE TRAFİK BİLGİLERİNİN İSPAT ARACI OLARAK KULLANILMASI

İnternet trafik bilgilerinin tutulduğu süre içerisinde (iki yıllık süre sona ermeden) suç soruşturması ve kovuşturması sebebiyle Cumhuriyet savcılıklarının ve ceza mahkemelerinin bu bilgileri –delil elde etme amacıyla- talep edebilmesi mümkündür. Bu tür bir talebin meşru bir amacı ve yasal bir dayanağı (5809 ve 5651 sayılı Kanun hükümleri) bulunduğu halde, CMK'de bu tür bir talebe ve talebin karşılanma biçimine dair açık bir yasal düzenleme bulunmamaktadır.

İnternet trafik bilgilerinin, belli bir internet kullanıcısına (belli bir kişiye) yönelik bilgileri içermesi nedeniyle, önceden "tutulan" ve resmi mercilerin tasarruf ve sorumluluğunda bulunan bu bilgilere erişimin teknik anlamda bir "*arama*" veya "*otomatik veri taraması*" olmadığı kabul edilmektedir[72]. Bu sebeple, internet trafik bilgilerine erişimin CMK m 134 hükmü kapsamında (bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbiri içerisinde) değerlendirilebilmesi de mümkün değildir. Bununla birlikte internet kullanıcısının internet ortamındaki bir haberleşmesine müdahale söz konusu olduğunda ise CMK m 135 hükmü kapsamında iletişimin denetlenmesi koruma tedbirine ilişkin yasal koşulların mevcut olması gerekmektedir[73].

Uygulamada (Yargıtay kararlarından hareketle), internet trafik bilgilerine erişim bakımından ayrı ve özel bir yasal düzenleme bulunmadığından, soruşturma aşamasında CMK m 160-161/1,4 hükümlerine, kovuşturma aşamasında ise CMK m. 206 hükmüne

---

72 Birtek (n 1) 666.

73 İnternet ortamında gerçekleştirilen iletişimin CMK m 135 kapsamında denetlenebilmesi mümkün ise de (telekomünikasyon kavramının içine internet ortamında gerçekleştirilen iletişim de girdiğinden koruma tedbirinin kapsam itibariyle internet ortamında gerçekleştirilen iletişimi de içine aldığı söylenebilirse de) bu tür bir denetimin ne şekilde gerçekleştirileceği hususunda CMK m 135'te herhangi bir düzenlemeye yer verilmemiştir. CMK m 135'in sabit veya mobil telefonlar marifetiyle yapılan iletişim esas alınarak -Kanun'un yürürlüğe girdiği tarihteki iletişim araçları gözetilerek- düzenlendiği ve bu konuda daha detaylı bir düzenlemeye ihtiyaç bulunduğu açıktır.

istinaden internet trafik bilgileri BTİK'den istenebilmektedir[74]. Uygulamada internet trafik bilgileri, Cumhuriyet savcılıkları veya mahkemeler tarafından doğrudan erişim sağlayıcılardan (veya Erişim Sağlayıcıları Birliğinden) değil BTİK'den talep edilmekte ve bilgi talepleri de doğrudan BTİK tarafından karşılanmaktadır.

Uygulamada, internet trafik bilgilerinin maddi gerçeğin ortaya çıkarılabilmesi amacıyla BTİK'den istenmesi bakımından suç soruşturmasına ve kovuşturmasına ilişkin "*genel yetki*"nin yeterli olduğu[75] ve CMK m. 332 hükmü uyarınca bu bilgilerin verilmesi gerektiği kabul edilmektedir[76]. Zira CMK m. 332 hükmüne göre "*Suçların soruşturma ve kovuşturması sırasında Cumhuriyet savcısı, hâkim veya mahkeme tarafından yazılı olarak*

---

[74] 2559 sayılı Kanun'un Ek 6. maddesine eklenen on sekizinci fıkrasında yer alan **"***(Ek fıkra: 2/1/2017-KHK-680/27 md.; Aynen kabul: 1/2/2018-7072/26 md.) Polis, sanal ortamda işlenen suçlarda, yetkili Cumhuriyet başsavcılığının tespiti amacıyla, internet abonelerine ait kimlik bilgilerine ulaşmaya, sanal ortamda araştırma yapmaya yetkilidir. Erişim sağlayıcıları, yer sağlayıcıları ve içerik sağlayıcıları talep edilen bu bilgileri kolluğun bu suçlarla mücadele için oluşturduğu birimine bildirir*." Hükmünü iptal eden Anayasa Mahkemesi (91/10, 19.02.2020), suç soruşturması kapsamında Cumhuriyet savcısının CMK m 161 hükmü uyarınca IP adresinin tespitine karar verebileceğini kabul etmiş ve kolluğa tanınan bu yetkinin "*zorunlu bir toplumsal ihtiyaca karşı gelmediğini*" kabul etmiştir. Bu karar dikkate alındığında kolluğun, istihbarat (suç önleme) amacı dışında -suç soruşturması sırasında- Cumhuriyet savcısının talebi/ yazılı emri olmaksızın, internet abonelerine ilişkin kimlik bilgilerine ulaşma yetkisini kullanamayacağı sonucu ortaya çıkmaktadır.

[75] Yargıtay bu işlemin "genel yetki" kapsamında olduğunu açıkça belirtmese de pek çok kararında HIS (CGNAT) kayıtlarının BTİK'den getirtildikten sonra HTS kayıtları ile eşleştirilip bir sonuca ulaşılması gerektiğini kabul etmektedir. Yargıtay'a göre "*ByLock kullanıcısı olduğunu kabul etmeyen sanıkların ByLock uygulamasını kullandıklarının kuşkuya yer vermeyecek şekilde teknik verilerle tespiti halinde ByLock kullanıcısı olduklarına dair delilin atılı suçun vasfının tayini açısından belirleyici nitelikte olması karşısında; ilgili birimlerden getirtilecek ayrıntılı ByLock tespit ve değerlendirme raporunun CMK'nın 217. maddesi uyarınca sanıklar ve müdafilerine okunup diyecekleri sorulduktan sonra bir karar verilmesi; değerlendirme ve tespit tutanağının temin edilememesi halinde, operatör kayıtları ile eşleştirmesi yapılmak üzere Bilgi Teknolojileri ve İletişim Kurumundan getirtilen CGNAT kayıtları ve dosya içerisindeki HTS sonuçları karşılaştırılıp belirtilen hat üzerinden ByLock kullanan kişinin sanıklar olup olmadıkları doğrultusunda bilirkişiden teknik rapor alınması*…" gerekmektedir. Yargıtay 3 CD 2020/9735, 26.10.2021; 16 CD, 2018/4527, 30.06.2021. Bu karardan da anlaşılacağı üzere Yargıtay, internet trafik bilgisini içeren HIS (CGNAT) kayıtlarına erişimi, genel bilgi ve delil toplama yetkisi içerisinde kabul etmektedir. Alman Ceza Muhakemesi Kanunu (StPO) m. 100/g-3'e göre de iletişime ilişkin (iletişim hizmeti sunucuları dışında tutulan) trafik datalarına erişim genel hükümler kapsamındadır. StPO Türkçe metni için bkz. Feridun Yenisey ve Salih Oktar, *Alman Ceza Muhakemesi Kanunu*, (2. Baskı Beta Basım Yayın, 2015) 115.

[76] 2559 sayılı Kanun'un Ek Madde 7 hükmü kapsamında istihbari (suç önleme) amacıyla "*internet bağlantı adresinin ve internet kaynakları arasındaki veri trafiğinin*" tespiti bakımından hâkim (veya gecikmesinde sakınca bulunan hallerde Kanun'da belirtilen idari mercilerin) kararı zorunlu kılındığı halde; suç soruşturması veya kovuşturması amacıyla bu verilere ulaşmak bakımından açık bir yasal düzenlemenin yapılmamış olması isabetli değildir.

istenilen bilgilere on gün içinde cevap verilmesi zorunludur. Eğer bu süre içinde istenen bilgilerin verilmesi imkânsız ise, sebebi ve en geç hangi tarihte cevap verilebileceği aynı süre içinde bildirilir".

Öğretide de diğer koruma tedbirlerinin alanına girmeyen ve "*üçüncü kişiler*" nezdinde bulunan delillerin (dijital/ sayısal delillerin), soruşturma aşamasında CMK m 161, kovuşturma aşamasında ise CMK m. 206 kapsamında toplanabileceği ifade edilmektedir[77].

Söz konusu yükümlülüğe aykırı davranılması halinde TCK m 257/2 hükmünde düzenlenen "*ihmal suretiyle görevi kötüye kullanma*" suçu söz konusu olur[78] ve bu görev

[77] Değirmenci (n 9) 387; Mustafa Taşkın, *Adli ve İstihbari Amaçlı İletişimin Denetlenmesi* (Seçkin Yayınevi 2008) 83; Nur Centel ve Hamide Zafer, *Ceza Muhakemesi Hukuku* (Yirminci Bası, Beta Basım Yayım 2021), 517; Yener Ünver ve Hakan Hakeri, *Ceza Muhakemesi Hukuku* (24. Baskı, Adalet Yayınevi 2025), 465; Seydi Kaymaz, *Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi* (4. Bası, Seçkin Yayınevi 2015) 133; Feridun Yenisey ve Ayşe Nuhoğlu, *Ceza Muhakemesi Hukuku* (9. Baskı, Seçkin Yayınevi 2021) 467; Öztürk, Tezcan ve Erdem (n 13) 595.

[78] Yargıtay uygulamasına göre adli merciler tarafından CMK m. 332 hükmü kapsamında yazılan müzekkerelere cevap verilmemesi halinde –fail kamu görevlisi sayılmasa dahi- TCK m. 257/2 hükmünde yer verilen ihmal suretiyle görevi kötüye kullanma suçu oluşmaktadır. "*...Somut olayda; sadece 22.09.2010 tarihli müzekkere içeriğinde CMK`nın 332/2. maddesinde belirtilen hususları içeren şerh bulunduğu da gözetilerek, söz konusu müzekkerenin sanığın çalıştığı birime hangi tarihte ulaştığını gösterir posta zimmet listesi ve diğer belgelerin getirtilmesinden ve cevap vermeme eylemi sonucu TCK`nın 257/2. maddesinde öngörülen kamu zararı, kişi mağduriyeti veya kişilere haksız kazanç sağlama unsurlarından birinin bulunup bulunmadığının tartışılmasından sonra hukuki durumunun tayin ve takdiri gerektiği…*" Yargıtay 5 CD, 11302/11423, 27.11.2013. Aksi yöndeki başka bir kararında ise "*A... İletişim Hizmetleri Anonim Şirketinin özel hukuk statüsüne tabi şirket olması sebebiyle Ceza Hukuku uygulamasında (memur) "kamu görevlisi" sayılmayan ve "kamu görevlisi gibi" cezalandırılması olanağı bulunmayan şirket adli yazışmalarından sorumlu olan sanığın, Kadıköy Cumhuriyet Başsavcılığınca yürütülen 2010/4744 Sayılı soruşturma kapsamında şirkete yazılan müzekkerelere süresinde cevap vermeme şeklindeki eyleminin; 5326 Sayılı Kabahatler Kanununun 32. maddesinde düzenlenen emre aykırı davranış niteliğinde olduğu*"na karar verilmiştir. Yargıtay 5 CD, 10258/197, 16.1.2018. Öğretide "*…bilgi verme yükümlülüğünü yerine getirmeyen kamu görevlisi olmayan diğer kişiler, kendisine kanun ile yüklenen görevi yerine getirmede ihmal veya gecikme gösterdiklerinde, soruşturmanın tamamlanmasının gecikmesi bu kapsamda adil yargılanma ilkesinin ve hak arama hürriyetinin ihlali sebebiyle şüphelinin ve müştekinin mağduriyeti söz konusu olacağından, TCK m. 257/2'den sorumlu olaca[ğı]*" öne sürülmektedir. Handan Yokuş Sevük, 'Görevi Kötüye Kullanma Suçu (TCK m. 257)' (2018) 23 (39) Dicle Üniversitesi Hukuk Fakültesi Dergisi, 257, 267-268. Düşüncemize göre de 5237 sayılı Kanun'un m. 6/1-c hükmü kapsamında, adli mercilerin suç soruşturması veya kovuşturması sırasında bilgi veya belge talep ettiği kişi (özel hukuk hükümlerine tabi bir kişi olsa dahi) "*kamu görevinin yürütülmesine… herhangi bir surette…geçici…*" olarak katılan kişi olduğundan ve suç soruşturması ve kovuşturması da bir "kamusal görev" olduğundan, CMK m. 332 hükmünü ihlal eden kişinin eylemi (suçun diğer yasal unsurlarının bulunması halinde) TCK m. 257/2 kapsamında değerlendirilmelidir.

adliyeye ilişkin bir görev olduğundan (failin özel soruşturma veya kovuşturma usulüne tabi olması halinde dahi) doğrudan doğruya soruşturulur (CMK m 161/5)[79].

Düşüncemize göre internet trafik bilgilerine erişimin de tıpkı "*iletişimin tespiti*" işleminde olduğu gibi CMK'de açıkça düzenlenmesine ihtiyaç bulunmaktadır[80]. Sabit veya mobil telefonlarla gerçekleştirilen iletişimin tespiti (CMK m 135/6 uyarınca) "*soruşturma aşamasında hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı, kovuşturma aşamasında mahkeme kararı*" ile mümkün iken; internet trafik bilgilerinin suç soruşturmasına/ kovuşturmasına ilişkin genel yetki içerisinde kabul edilmesi isabetli değildir. Kaldı ki; internet trafik verilerinin internet (iletişim uygulamaları) marifetiyle gerçekleştirilen iletişime ilişkin olabileceği de nazara alındığında, bu hususta açık bir kanuni düzenleme yapılmamasının eksiklik olduğu açıkça ortadadır.

İnternet marifetiyle işlenen suçların çokluğu ve bu suç tiplerinin "*yegâne*" (belirleyici veya "*somut*") delilinin de internet trafik bilgileri olduğu nazara alındığında, bütün suçlar bakımından uygulanabilen bir tedbir olarak başvurulabilmesinin de mümkün olması gerekmektedir. Bu sebeple CMK m 135/6 hükmünün: "*Şüpheli ve sanığın telekomünikasyon*

---

[79] "*...İletişim Hizmetleri A.Ş.'de adli yazışmalardan sorumlu sanığın esasen kamu görevlisi sıfatı bulunmamakla birlikte CMK'nın 332. maddesindeki özel düzenleme uyarınca suçların soruşturma ve kovuşturması sırasında Cumhuriyet savcısı, hâkim veya mahkeme tarafından kendisinden yazılı olarak belge istendiğinde, tıpkı tanık ve bilirkişi görevlendirilmesinde olduğu gibi TCK'nın 6. maddesinde söz edildiği üzere kamusal bir faaliyet olan yargı görevinin işleyişine "herhangi bir surette" katıldığı ve bu anlamda kamu görevlisi sayıldığı, açıklanan sebeple bu yöndeki kabulün görevi kötüye kullanmanın özgü suç olma özelliği ile herhangi bir suretle çelişmediği ve "Suçta ve cezada kanunilik ilkesi" ile bağdaşmayan bir duruma neden olunmadığı, sanığın Kadıköy Cumhuriyet Başsavcılığınca yürütülen soruşturma işlemlerinde yol açtığı gecikmeye bağlı olarak hem adil yargılanma ilkesinin ve hak arama hürriyetinin ihlali sebebiyle şüphelinin ve şikâyetçinin mağduriyetine hem de soruşturma giderlerinin artmasına yol açmak suretiyle kamu zararına sebebiyet verdiği, bu nedenle eyleminin TCK'nın 257. maddesinin ikinci fıkrasında düzenlenen ihmali davranışla görevi kötüye kullanma suçunu oluşturduğu…*", Yargıtay GCK, 5-287/409, 08.10.2020.

[80] Bu türden bir düzenleme ile istihbari amaçlı internet trafik bilgilerine erişim ile suç soruşturması veya kovuşturması amacıyla internet trafik bilgilerine erişim bakımından "karar verecek mercii" bakımından yeknesaklık sağlanarak, yasal düzenleme çelişkisi de giderilmiş olacaktır. Zira 2559 sayılı Kanun'un Ek Madde 7'ye göre suç önleme amacıyla "internet bağlantı adresinin ve internet kaynakları arasındaki veri trafiğinin" tespiti bakımından hâkim (veya gecikmesinde sakınca bulunan hallerde Kanun'da belirtilen idari mercilerin) kararı zorunludur. CMK de ise soruşturma aşamasında -gecikmesinde sakınca bulunup bulunmadığına bakılmaksızın- suç soruşturmasına ilişkin genel yetkiye istinaden bu verilere erişilebilmesi mümkündür.

yoluyla iletişiminin, ***internet trafik bilgilerinin tespiti…***" biçiminde yeniden düzenlenmesine ihtiyaç bulunmaktadır. Bu yolla CMK m 137/3 ve 137/4 hükümlerinde yer alan güvenceler de internet trafik bilgilerine erişim bakımından geçerli olabilecek ve bireyin mahremiyet hakkı ile kişisel verilerinin gizliliği de korunmuş olacaktır.

Şüpheli veya sanığın internet ortamında bir başkası ile iletişim kurması halinde, erişilen internet trafik verilerinin bu haberleşme olgusuna ilişkin olması halinde ise (internet marifetiyle iki kişinin haberleşip haberleşmediği hususunda ise) CMK m 161 ve 206 hükümleri kapsamında suç soruşturmasına veya kovuşturmasına ilişkin genel yetkiye dayanılarak internet trafik bilgilerine erişilebilmesi mümkün değildir. Zira bu halde artık haberleşme olgusuna (iletişimin tespitine) dair bir bilgi ortaya çıkacağından, bu türde bir tespit ancak CMK m 135/6 kapsamında yapılabilecektir[81].

Belirtmek gerekir ki; suç soruşturmasına ilişkin genel yetki olarak adlandırılan CMK m 160, 161 hükümleri ile mahkemelere delil ikame yetkisini (dolaylı olarak) veren CMK m 206 hükmü, internet trafik verilerinin koruduğu hürriyet alanına yönelik müdahaleler bakımından "bilinebilirlik ve öngörülebilirlik" güvencesini karşılamaktan uzaktır[82]. İnternet trafik verilerine erişim (verilerin tespiti), CMK da düzenlenen bir koruma tedbirine (CMK m 135/6 kapsamında iletişimin tespitine) denk bir müdahale olduğundan, Anayasa m 13 uyarınca bu müdahalenin koşullarının CMK'de açıkça düzenlenmesi ve kötüye kullanımı engelleyecek güvenceye bağlanması gerekmektedir[83].

---

[81] CMK m 135/6 hükmüne göre "*Şüpheli ve sanığın telekomünikasyon yoluyla iletişiminin tespiti, soruşturma aşamasında hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı, kovuşturma aşamasında mahkeme kararına istinaden yapılır*".

[82] AİHM'e göre bir temel hakka müdahaleye imkân veren ve yeterli/ uygun güvencelere sahip bir kanuni düzenleme/ dayanak bulunması halinde, her koruma tedbirinin ayrıca düzenlenmesi zorunlu değildir. AİHM, *Wieser and Bicos Beteiligungen GmbH v Avusturya,* (2008) par 54.

[83] "*koruma tedbirlerine eş değer ağırlıkta temel hak ve hürriyete ilişkin müdahalelerde bulunulamayacağı*" düşüncesi için bkz. Fatih Birtek, 'Ceza Muhakemesinde Tanık Hakkında İletişimin Tespiti Koruma Tedbirine Başvurulup Başvurulamayacağı Sorunu' (2022) 17(49) Ceza Hukuku Dergisi, 189, 211.

Usulüne uygun olarak toplanan/ erişilen internet trafik verilerinin ispat gücü açısından bakıldığında; yukarıda da değinildiği üzere her trafik verisinin maddi vakıaların ispatı bakımından delil niteliği taşımayabilir. Her dijital veri (internet trafik verisi) delil değildir.

İnternet trafik verilerinin muhtevası ve ispatı gereken maddi vakıayı kapsayıp kapsamadığı dikkate alınarak bir değerlendirme yapılması gerekmektedir. Dijital veri olması hasebiyle internet trafik verilerinin keşif veya bilirkişi incelemesine konu "belirti/ emare" olduğu ve "dolaylı/ yan/ destekleyici" delil olduğu söylenebilirse de bu hususta mutlak bir kural koyabilmek de mümkün değildir[84]. İspatı gereken maddi vakıanın mahiyetine ve internet trafik verisinin bu vakıayı kapsayıp kapsamadığına (maddi vakıayı temsil edip etmediğine) göre bir değerlendirme yapılarak, tek ve/veya belirleyici delil olarak kabul edilebilmesi de mümkündür. Özellikle doğrudan veya dolaylı bilişim suçları bakımından internet trafik verileri -sağlamlıkları ve güvenilirlikleri test edilmek ve savunmaya bu delile karşı itirazda bulunma imkânı sunulmak kaydıyla- tek ve/veya belirleyici delil olarak kabul edilebilecektir.

Suç soruşturması veya kovuşturması sırasında erişilen internet trafik verilerinin kâğıda dökülmesi, keşfe veya bilirkişi incelemesine konu edilmesi delilin CMK m. 68 ve 214 kapsamında duruşmada tartışılması bakımından bir kolaylık sağlasa da dijital verilerin sağlamlığı ve güvenilirliği, yazılı hale getirildikleri kâğıda/ belge üzerinden değil, bizatihi dijital halleri incelenerek anlaşılabilecektir. Nitekim öğretide de dijital bulgular bakımından delil olarak değerlendirilmesi gereken şeyin, aletin kendisinin değil, içeriğindeki dijital

[84] Bizim de katıldığımız düşünceye göre "*bir ispat aracının güvenilir olup olmadığından hareketle, onun delil veya belirti niteliği yönünde çıkarsamada bulunmak yerinde değildir*". Barış Erman, 'Ceza Muhakemesi Hukukunda Belirti ve İspat Değeri', Prof. Dr. Köksal Bayraktar'a Armağan (2010) 1 GSÜHFD 690-691. Belirti/ emâre, yargılama konusu olaya ilişkin olarak "maddi gerçeğin bir parçasını teşkil edecek şekilde" yakın bir bilgi veriyorsa artık delil hâline gelir. Faruk Erem, *Ceza Usulü Hukuku* (Genişletilmiş Beşinci Bası, AÜHF Yayını (1978) 398.

bulguların delil mahiyetinde olduğu ifade edilmiştir[85]. Belge, dijital veriyi/ datayı somutlaştırsa ve temsil etse dahi delilin muhtevası[86] belge değil, dijital veridir.

Dijital delil (veri) mahiyeti taşıyan internet trafik verileri, kâğıda dökülmüş olsa dahi belge değil, belirti delili kapsamında değerlendirilmeli ve keşfe veya bilirkişi incelemesine konu edilerek anlamlandırılmalıdır[87]. Trafik verilerinin kâğıda dökülmesi, bu verilerin "belge" deliline dönüştüğü anlamına gelmez. Zira kâğıda dökülmüş olsa dahi "kâğıt/ belge" sadece delil olan dijital verinin "taşıyıcısı" mahiyetindedir[88]. İspat işlevi bakımından keşif veya bilirkişi incelemesine konu edilmesi gereken diğer bir deyişle delilin muhtevası olan şey dijital verilerdir (trafik verileridir).

Son olarak belirtmek gerekir ki; internet trafik verilerinin delil olarak kullanılabilmesi için mevzuatta öngörüldüğü şekliyle "zaman damgalı" olarak tutulması/ kaydedilmesi/ saklanması ve adli mercilere de -sağlamlıklarının ve güvenilirliklerinin test edilebilmesi için- zaman damgalı[89] şekilde gönderilmesi gerekmektedir[90]. Yine, savunma hakkı kapsamında verilerin dijital kopyalarının -istemesi halinde- şüphelinin/ sanığın veya müdafiin erişimine açılması, internet trafik verilerini inceleme ve bu veriler hakkında bilirkişi incelemesi

---

85 Öztürk, Tezcan ve Erdem (n 13) 402; Mustafa Özen, *Ceza Muhakemesi Hukuku Dersleri* (6. Baskı, Adalet Yayınevi 2021) 420. Aksi yönde (dijital ortamda olup da okunabilen ve yazılı şekle sahip bulguların belge delili olduğu hususunda) bkz. Karakehya (n 9) 257.

86 Delil muhtevası kavramı için bkz. Birtek (n 6) 22 vd.

87 Değirmenci (n 9) 139 vd.

88 Aksi yöndeki düşünceye göre dijital veriler (bilişim verileri) de yazılı belge kapsamındadır. Nurullah Kunter, Feridun Yenisey ve Ayşe Nuhoğlu, *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku* (18. Baskı, Beta Basım Yayım 2010) 1387.

89 5070 sayılı Elektronik İmza Kanunu m. 3/1-h'ye göre "*Zaman damgası: Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kaydı*" ifade etmektedir. Elektronik İmza Kanunu, Kanun Numarası 5070, Kabul Tarihi: 15.01.2004 , RG 23.01.2004/25355.

90 Burcu Erdoğan, "Bir Kişiyi Suçlamak İçin IP Adresi Yeterli midir?", (t.y.), <http://www.bilisimhukuk.com/2010/02/bir-kisiyi-suclamak- icin-ip-adresi-yeterli-midir/>'den nakleden Doğan Gedik, 'Bilişim Suçlarında IP Tespiti ile Ekran Çıktılarının İspat Değeri' (2019) 1(1) Bilişim Hukuku Dergisi 51, 59.

yaptırma veya yapılmasını isteme ve verilere karşı itirazlarını ileri sürebilme imkanının tanınması gerekmektedir.

SONUÇ

Ceza muhakemesinde gerek doğrudan ve dolaylı bilişim suçları gerekse diğer suçlar bakımından, failin ve suçun delillerinin tespiti için internet trafik verilerine erişim ihtiyacı ortaya çıkabilmektedir. Bununla birlikte, internet trafik verilerine yönelik müdahale gerek dijital özel yaşam alanına, ifade ve haberleşme özgürlüğüne müdahale teşkil edeceğinden, bu tür bir müdahalenin kanunla öngörülmüş olması, meşru bir amacının bulunması ve demokratik toplumda gerekli ve ölçülü bir müdahale olması zorunludur.

Türk ceza muhakemesinde -Yargıtay'ın yeni gelişen uygulamasında- suç soruşturması başlamadan önce idari merciler tarafından idari (hizmetin sunulmasına ilişkin) amaçlarla veya suç önleme amacıyla tutulan/ depolanan internet trafik verileri ispat aracı olarak kullanılabilmektedir. Yine Yargıtay istikrarlı bir biçimde, internet trafik verilerine erişimin suç soruşturmasına/ kovuşturmasına ilişkin genel yetki içerisinde olduğunu kabul etmektedir.

İnternet trafik verilerinin mahiyeti itibariyle kişisel veri niteliğinde olduğundan, özel yaşam, ifade ve haberleşme özgürlükleriyle ilişkisi de nazara alındığında, bu verilere suç soruşturması veya kovuşturması amacıyla erişim bakımından açık bir yasal düzenlemeye ihtiyaç bulunmaktadır. Zira internet trafik verilerine suç önleme amacıyla yapılan müdahalenin (PVSK EK Madde 7/2) ve sabit/ mobil cihazlarla yapılan iletişimin tespitinin (CMK m 135/6'da) açıkça düzenlendiği nazara alındığından, internet yoluyla (uygulamalar marifetiyle) yapılan iletişime ilişkin bilgileri de içeren internet trafik verilerine müdahalenin koşullarının kanunda açıkça düzenlenmemesi önemli bir eksikliktir.

Çalışmada savunduğumuz düşünceler ve öne sürdüğümüz argümanlardan hareketle CMK m 135/6 hükmünün: "*Şüpheli ve sanığın telekomünikasyon yoluyla iletişiminin,* ***internet trafik bilgilerinin tespiti*** *soruşturma aşamasında hâkim veya gecikmesinde sakınca*

bulunan hâllerde Cumhuriyet savcısı, kovuşturma aşamasında mahkeme kararına istinaden yapılır…" biçiminde yeniden düzenlenmesi suretiyle bu yasal boşluğun doldurulabileceğini ve internet trafik verileriyle ilintili özgürlüklerin de tam anlamıyla korunabileceğini düşünmekteyiz.

İnternet trafik verilerinin ilgili Kanun'da belirtilen süreyle sınırlı olarak, zaman damgalı olarak tutulması/ depolanması ve adli mercilerce talep edilerek soruşturma/ kovuşturma dosyasına celbi sonrasında, ispatın konusunu oluşturan maddi vakıanın mahiyetine ve trafik verilerinin maddi vakıanın bütününü kapsayıp kapsamadığı (maddi vakıayı temsil niteliği) tespit edilerek tek ve/veya belirleyici delil olarak ispat gücüne sahip olabileceği gibi keşfe veya bilirkişi incelemesine konu "belirti/ emare" niteliği taşıması ve "*destekleyici/ yan delil*" olarak kabul edilebilmesi de mümkündür.

KAYNAKÇA

Beukelmann S, 'Ceza Hukukuna İlişkin Sınırlar Olmaksızın İnternette Gezinti Yapmak' (Çev. Yener Ünver) içinde Yener Ünver (edt) İnternet Hukuku (Karşılaştırmalı Güncel Ceza Hukuku Serisi 13) (1. Baskı, Seçkin Yayınevi 2013).

Birtek F ve Topal B.N, 'Dijital İspat Aracı Olarak Sabit veya Ankesörlü Telefonlara İlişkin Arama Kayıtları ve Bu Kayıtların İspat Kuvveti', (2023) (2) GSÜHFD 1137-1178.

Birtek F, 'Ceza Muhakemesinde Tanık Hakkında İletişimin Tespiti Koruma Tedbirine Başvurulup Başvurulamayacağı Sorunu' (2022) 17(49) Ceza Hukuku Dergisi 189-216.

Birtek F, 'Suç İşlenmesini Önleme Amacıyla İnternet veri Trafiğinin (İnternet Trafik Bilgilerinin) Tespiti', içinde Fatih Birtek (edt) *Hukuk Devletinde Kolluğun Suç Önleme Yetkisi (Kaynağı, Kapsamı ve Sınırları)* (1. Baskı, Adalet Yayınevi 2024).

Birtek F, 'Suç İşlenmesini Önleme Amacıyla PVSK Ek Madde 7 Kapsamında Uygulanan Tedbirlerden Elde Edilen Bilgilerin Ceza Muhakemesinde Delil Olarak Kullanılıp

Kullanılamayacağı Sorunu' içinde Fatih Birtek (edt) *Hukuk Devletinde Kolluğun Suç Önleme Yetkisi (Kaynağı, Kapsamı ve Sınırları)* (1. Baskı, Adalet Yayınevi 2024) 655.

Birtek F, *AİHM, Anayasa Mahkemesi ve Yargıtay Kararları Işığında Ceza Muhakemesinde Delil ve İspat* (2. Baskı, Adalet Yayınevi 2017).

Buckner D, 'Internet Search and Seizure in United States v. Forrester: New Problems in the New Age of Pen Registers' (2008) 22(2) BYU Journal of Public Law 499-517.

Centel N ve Zafer H, *Ceza Muhakemesi Hukuku* (Yirminci Bası, Beta Basım Yayım 2021).

Cihan E ve Yenisey F, *Ceza Muhakemesi Hukuku* (Beta Yayıncılık 1996).

Değirmenci O, *Ceza Muhakemesinde Sayısal (Dijital) Delil* (1. Baskı, Seçkin Yayınevi 2014).

Doğru O ve Nalbant A, *İnsan Hakları Avrupa Sözleşmesi,* 2. Cilt (Avrupa Konseyi ve Yargıtay Başkanlığı Yayını 2013).

Durmaz C, 'Esasa İlişkin Kabul Edilemezlik Nedenleri, Bireysel Başvuru İnceleme Usulü ve Kabul Edilebilirlik Kriterleri' (edt) Musa Sağlam (2. Baskı, Anayasa Mahkemesi Yayınları 2013).

Dülger MV ve Özkan O, 'Kolluk Teşkilatında ve Ceza Yargılamalarında Kişisel Verilerin Korunması: "Unutulan" Direktifin Kapsamlı ve Karşılaştırmalı Analizi' (2020) (42) Ceza Hukuku Dergisi 85-149.

Erdem, MR, *Ceza Muhakemesinde Organize Suçlulukla Mücadelede Gizli Soruşturma Tedbirleri* (1. Baskı, Seçkin Yayınevi 2001).

Erdoğan Y, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri* (1. Bası, Legal Yayıncılık 2018).

Erdoğan Y, *Türk Ceza Kanunu'nda Bilişim Suçları* (1. Baskı, Legal Yayıncılık, 2013).

Erem F, *Ceza Usulü Hukuku* (Genişletilmiş Beşinci Bası, AÜHF Yayını 1978).

Erkan G, *Bilişim Sistemine Girme, Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları* (Yayınlanmamış Yüksek Lisans Tezi, YÖK Tez Merkezi 2021).

Erman B, 'Ceza Muhakemesi Hukukunda Belirti ve İspat Değeri', Prof. Dr. Köksal Bayraktar'a Armağan, (2010) 1 GSÜHFD 679-701.

Gedik D, 'Bilişim Suçlarında IP Tespiti ile Ekran Çıktılarının İspat Değeri' (2019) 1(1) Bilişim Hukuku Dergisi 51-84.

Heger D, 'Büyük Veri ve Suçsuzluk Karinesi' içinde Kayıhan İçel ve Yener Ünver (edt) Ceza Hukukunda Robot, Yapay Zekâ ve Yeni Teknolojiler (Karşılaştırmalı Güncel Ceza Hukuku Serisi 21) (1. Baskı, Seçkin Yayıncılık 2021).

Karakehya H, *Ceza Muhakemesi Hukuku* (6. Bası, Adalet Yayınevi 2024).

Kaymaz S, *Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi* (4. Bası, Seçkin Yayınevi 2015).

Kudlich H, 'İnternette Anonim Gezinti Hakkı ve Ceza Hukuku (Anonimleştirilmiş Servis Hizmetlerine İlişkin Hukuki Problem', (Çev. Özlem Yenerer Çakmut) içinde Yener Ünver (edt) Özel Yaşam, Medya ve Ceza Hukuku Karşılaştırmalı Güncel Ceza Hukuku Serisi 7 (1. Baskı, Seçkin Yayınevi 2007).

Kunter N, Yenisey F ve Nuhoğlu A, *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku* (18. Baskı, Beta Basım Yayım 2010).

Özbek VÖ, 'Organize Suçlulukla Mücadele Ön Alan Soruşturmaları', (2002) 4(2) Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi 57-88.

Özbek VÖ, *Ceza Muhakemesi Hukuku* (Seçkin Yayınevi 2006).

Özbek VÖ, 'Elektronik Ortamda Saklı Bulunan Verilerin ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi' (2001) 59(1-2) İÜHFM 181-202.

Özen M, *Ceza Muhakemesi Hukuku Dersleri* (6. Baskı, Adalet Yayınevi 2021).

Özkan H, 'Ceza Muhakemesinde Ekran Görüntüsü Çıktılarının Delil Niteliği', içinde Yener Ünver (edt) *Ceza Muhakemesi Hukukunda Delil ve İspat, Karşılaştırmalı Güncel Ceza Hukuku Serisi 15* (1. Baskı, Seçkin Yayınevi 2014)

Öztürk B, Tezcan D ve Ruhan MR, (edt), *Dijital Ceza Muhakemesi Hukuku* (3. Baskı, Seçkin Yayınevi 2024).

Şahin C ve Göktürk N, *Ceza Muhakemesi Hukuku* (13. Bası, Seçkin Yayınevi 2022).

Taşkın M, *Adli ve İstihbari Amaçlı İletişimin Denetlenmesi* (Seçkin Yayınevi, 2008).

Tezcan D, Erdem MR ve Sancakdar O, *Avrupa İnsan Hakları Sözleşmesi Işığında Türkiye'nin İnsan Hakları Sorunu* (Seçkin Yayıncılık 2004).

Ünver, Y ve Hakeri, H, Ceza Muhakemesi Hukuku (24. Baskı, Adalet Yayınevi 2025).

Vitkauskas D ve Dikov G, *Avrupa İnsan Hakları Sözleşmesi Kapsamında Adil Yargılanma Hakkının Korunması*, (Çev. Serkan Cengiz) Avrupa Konseyi İnsan Hakları El Kitapları (Avrupa Konseyi 2012).

Yenisey F ve Nuhoğlu A, *Ceza Muhakemesi Hukuku* (9. Baskı, Seçkin Yayınevi 2021).

Yenisey F, *Hazırlık Soruşturması ve Polis* (Beta Yayıncılık 1987).

Yenisey F ve Oktar S, (2. Baskı, Beta Basım Yayın, 2015).

Yetim S, '5651 Sayılı Yasa Kapsamında Tutulan İnternet Trafik Bilgilerinin Özel Hayat ve Hayatın Gizliliği Kapsamında Değerlendirilmesi', (2013) (36) Terazi Hukuk Dergisi 55-63.

Yokuş Sevük H, 'Görevi Kötüye Kullanma Suçu (TCK m. 257)' (2018) 23(39) Dicle Üniversitesi Hukuk Fakültesi Dergisi 257-316.

Yorgancıoğlu E ve Demircan YT, 'Bilgi Teknolojileri ve İletişim Kurumu Tarafından Toplanan İnternet Trafik Verilerinin Kişisel Verilerin Korunması Hakkı Bağlamında Değerlendirilmesi' (2023) 22(48) İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi 1189-1215.