

IP Adreslerinin Delil Değeri

Dijital çağın hukuk dünyasına en köklü etkilerinden biri, şüphesiz elektronik delil kavramının giderek daha belirleyici bir konuma yükselmesidir.

Av. Burak Üçüncü · 27 Şubat 2026 · 9 dk okuma

Dijital çağın hukuk dünyasına en köklü etkilerinden biri, şüphesiz elektronik delil kavramının giderek daha belirleyici bir konuma yükselmesidir. Bu dönüşümün merkezinde ise IP adresleri yer almaktadır. Günümüzde ceza davalarından hukuk uyuşmazlıklarına, fikri mülkiyet ihlallerinden kişilik haklarına yönelik saldırılara kadar geniş bir yelpazede IP adresleri, yargılama süreçlerinin vazgeçilmez bir unsuru haline gelmiştir. Ancak IP adreslerinin delil değerini doğru biçimde kavrayabilmek için öncelikle bu kavramın teknik altyapısını, ardından hukuki çerçevesini ve nihayet yargısal pratikte karşılaşılan sorunları bütüncül bir yaklaşımla ele almak gerekmektedir.

Yirmi yılı aşkın hukuk pratiğinde gözlemlediğim en önemli değişimlerden biri, mahkemelerin IP adresi kavramına yaklaşımının dramatik biçimde evrilmesidir. İlk yıllarda bir IP adresinin tespiti neredeyse kesin bir kimlik belirleme aracı olarak kabul edilirken, bugün hem teknik gerçeklikler hem de Yargıtay içtihatları, bu bakış açısının ne denli eksik ve yanıltıcı olabileceğini açıkça ortaya koymuştur. IP adresinin tek başına bir kişiyi değil, yalnızca bir ağ bağlantı noktasını işaret ettiği gerçeği, hukukçuların zihnine yerleşmesi gereken temel bir ilkedir.

BÖLÜM II

IP Adresinin Teknik Yapısı ve Türk Hukukunda Yeri

IP adresi, yani İnternet Protokolü adresi, bir bilgisayar ağına bağlı her cihaza atanan benzersiz sayısal tanımlayıcıdır. Teknik olarak IPv4 standardında 32 bitlik, IPv6 standardında ise 128 bitlik bir sayı dizisinden oluşan bu adresler, internet üzerindeki iletişimin temel yönlendirme mekanizmasını oluşturur. Ancak hukukçuların sıklıkla gözden kaçırdığı kritik bir ayrım vardır ki IP adresi bir cihazı, bir kişiyi veya bir fiziksel konumu doğrudan temsil etmez; yalnızca belirli bir zaman diliminde belirli bir ağ bağlantısını tanımlar. Bu ayrım, delil değerlendirmesinin tamamına nüfuz eden ve her aşamada göz önünde bulundurulması gereken temel bir ilkedir.

Türk hukuk sisteminde IP adreslerinin delil olarak kullanılmasının yasal çerçevesi, birden fazla mevzuat tarafından çizilmektedir. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, bu alandaki temel düzenlemeyi oluşturmaktadır. Kanunun erişim sağlayıcılara ve yer sağlayıcılara yüklediği trafik bilgisi saklama yükümlülüğü, IP adreslerinin delil olarak elde edilebilmesinin hukuki zeminini teşkil eder. Bununla birlikte 5271 sayılı Ceza Muhakemesi Kanunu'nun iletişimin tespiti, dinlenmesi ve kayda alınmasına ilişkin hükümleri

ile 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun veri işleme şartlarına dair düzenlemeleri de bu çerçevenin ayrılmaz parçalarıdır.

BÖLÜM III —

Dinamik ve Statik IP Adresleri

IP adreslerinin delil değerini etkileyen en temel teknik ayrım, statik ve dinamik IP adresleri arasındaki farktır. Statik IP adresi, bir internet servis sağlayıcısı tarafından belirli bir aboneye kalıcı olarak tahsis edilen ve değişmeyen adrestir. Genellikle kurumsal aboneliklerde, sunucu barındırma hizmetlerinde ve özel iş hatlarında tercih edilen statik IP adresleri, doğası gereği daha güçlü bir delil değeri taşır. Zira belirli bir statik IP adresinin belirli bir aboneye ait olduğu, servis sağlayıcı kayıtlarından nispeten kolay bir şekilde tespit edilebilir ve bu tespit, zaman faktöründen bağımsız olarak geçerliliğini korur.

Dinamik IP adresleri ise bambaşka bir tablo ortaya koyar. Türkiye'deki bireysel internet aboneliklerinin büyük çoğunluğunda kullanılan dinamik IP adresleri, internet servis sağlayıcısının havuzundan geçici olarak atanır ve bağlantı her kurulduğunda veya belirli periyotlarla değişebilir. Bu durum, delil değerlendirmesi açısından son derece önemli bir sonuç doğurur. Dinamik bir IP adresinin belirli bir aboneyle ilişkilendirilmesi, mutlaka o IP adresinin kullanıldığı kesin tarih ve saat bilgisini gerektirir. Saat bilgisindeki birkaç dakikalık bir sapma bile, tamamen farklı bir aboneye işaret edebilir. Dolayısıyla dinamik IP adreslerinin delil olarak kullanılabilmesi için log kayıtlarındaki zaman damgalarının son derece hassas ve güvenilir olması zorunludur.

Uygulamada sıklıkla karşılaştığım bir sorun, savcılık veya kolluk kuvvetlerinin IP adresi sorgulamalarında yeterli zaman hassasiyeti göstermemesidir. Örneğin bir internet sitesine yapılan hakaret içerikli bir paylaşımın IP adresi tespit edildiğinde, bu IP adresinin ilgili internet servis sağlayıcısına sorulması sırasında yalnızca tarih bilgisi verilip saat bilgisinin ihmal edildiği durumlarla karşılaşyoruz. Dinamik IP tahsisinin saatlik hatta dakikalık periyotlarla değişebildiği düşünüldüğünde, bu tür bir ihmalin masum bir kişinin şüpheli konumuna düşmesine yol açabileceği açıktır. Yargıtay da birçok kararında bu hassasiyete dikkat çekmiş ve zaman bilgisi eksik olan IP tespitlerinin tek başına mahkumiyet için yeterli olmadığını vurgulamıştır.

BÖLÜM IV —

CGNAT ve IP Adresi Tespitinde Yaşanan Büyük Sorun

Son yıllarda IP adreslerinin delil değerini en derinden sarsan teknik gelişme, kuşkusuz [CGNAT](#) yani Carrier Grade Network Address Translation uygulamasıdır. IPv4 adres havuzunun tükenmesiyle birlikte dünya genelinde ve Türkiye'de internet servis sağlayıcıları, CGNAT teknolojisine yoğun biçimde başvurmaya başlamıştır. Bu teknolojinin özünde tek bir genel IP adresi, aynı anda yüzlerce hatta binlerce abonenin internet trafiğini taşımak üzere paylaştırılır. Başka bir deyişle, dışarıdan bakıldığında aynı IP adresini kullanan yüzlerce farklı hane veya işyeri olabilir.

CGNAT'ın hukuki sonuçları son derece ciddidir ve Türk yargı pratiğinde henüz yeterince anlaşılmamış bir alan olarak karşımıza çıkmaktadır. CGNAT ortamında bir IP adresinin belirli bir aboneye atfedilebilmesi, yalnızca IP adresi ve zaman bilgisiyle mümkün değildir; bunun yanında kaynak port bilgisinin de bilinmesi zorunludur. Port kavramı, teknik olarak bir IP adresi üzerinden gerçekleştirilen farklı bağlantıları birbirinden ayırt etmeye yarayan sayısal bir tanımlayıcıdır. Bir IP adresi bir apartman binasının sokak numarası gibi düşünülürse, port numarası o binadaki daire numarasına benzetilebilir. CGNAT ortamında aynı IP adresini

paylaşan farklı aboneler, farklı port aralıkları kullanır ve ancak bu port bilgisi sayesinde trafiğin hangi aboneye ait olduğu belirlenebilir.

Ne var ki uygulamada karşılaşılan tablo oldukça kaygı vericidir. Birçok internet servis sağlayıcısı CGNAT port tahsis kayıtlarını ya hiç tutmamakta ya da yetersiz süreyle saklamaktadır. Bu durumda, bir suçun işlendiği tarihten birkaç hafta sonra başlatılan bir soruşturmada, ilgili port bilgisine ulaşmak fiilen imkansız hale gelmektedir. Dahası, 5651 sayılı Kanun'un trafik bilgisi saklama yükümlülüğünün CGNAT port kayıtlarını kapsadığı şüphesiz iken maalesef bu kayıtlar her zaman yeterli şekilde tutulmamaktadır.

Bu meseleyi somutlaştırmak gerekirse, bir hakaret davasında şüphelinin tespiti için elde edilen IP adresinin CGNAT arkasında olduğu durumlarda, aynı anda o IP adresini paylaşan dört yüz farklı abone olabilir. Port bilgisi olmadan yapılan bir tespit, bu dört yüz aboneden herhangi birine işaret edebilir. Bu gerçeklik, ceza hukukunun en temel ilkelerinden biri olan şüpheden sanık yararlanır ilkesiyle doğrudan çatışma yaratır. Zira dört yüzde bir olasılıkla bir kişiyi suçlamak, makul şüphenin çok ötesinde bir belirsizlik barındırmaktadır.

BÖLÜM V

Port Kavramı ve Hukuki Önemi

Port kavramı, hukukçuların büyük çoğunluğunun yeterince aşına olmadığı ancak dijital delil değerlendirmesinde hayati öneme sahip teknik bir unsurdur. Bir bilgisayar veya ağ cihazı, aynı IP adresi üzerinden eş zamanlı olarak binlerce farklı bağlantı kurabilir. Her bir bağlantı, 0 ile 65535 arasında bir port numarasıyla tanımlanır. Bir web sitesine erişim genellikle 80 veya 443 numaralı hedef portlarından gerçekleşirken, bağlantıyı başlatan cihaz kendi tarafında rastgele bir kaynak port numarası kullanır. İşte CGNAT ortamında kritik olan bilgi, bu kaynak port numarasıdır.

CGNAT olmayan klasik yapılarda port bilgisi, delil tespiti açısından genellikle ikincil öneme sahiptir; zira IP adresi ve zaman bilgisi, aboneyi tespit etmek için yeterlidir. Ancak CGNAT yapısında durum kökten değişir. CGNAT cihazı, her abonenin trafiğini farklı bir dış port aralığına çevirir. Örneğin abone A'nın trafiği 10000-10999 port aralığına, abone B'nin trafiği 11000-11999 port aralığına yönlendirilir. Dolayısıyla suçla ilişkilendirilen bağlantının kaynak port numarası bilinmeden, hangi abonenin o bağlantıyı gerçekleştirdiğini tespit etmek mümkün değildir.

Türk yargı pratiğinde port bilgisinin önemine ilişkin farkındalık giderek artmakla birlikte, hâlâ ciddi eksiklikler bulunmaktadır. Savcılık makamlarının internet servis sağlayıcılarına gönderdiği müzakerelerde port bilgisi talep edilmemekte, ya da talep edilse bile servis sağlayıcıları bu bilgiyi temin edememektedir. Özellikle mobil internet bağlantılarında CGNAT kullanımının neredeyse evrensel hale geldiği günümüzde, port bilgisi olmaksızın yapılan IP tespitleri, hukuki açıdan son derece zayıf bir zemin üzerinde durmaktadır.

BÖLÜM VI

Türk Yargı Pratiğinde IP Adresinin Delil Değerlendirmesi

Yargıtay, IP adreslerinin delil değerine ilişkin önemli içtihatlar geliştirmiştir. Genel yaklaşım, IP adresinin tek başına mahkumiyet için yeterli olmadığı, ancak diğer delillerle desteklendiğinde güçlü bir belirti oluşturabileceği yönündedir. Yargıtay'ın birçok kararında, IP adresinin yalnızca bir internet bağlantısını tanımladığı, o bağlantıyı kullanan kişiyi doğrudan göstermediği vurgulanmıştır. Bu yaklaşım, ceza hukukunun temel ilkeleriyle uyumlu ve teknik gerçekliği doğru yansıtan bir değerlendirmedir.

Özellikle **bilişim suçları**, hakaret, tehdit ve kişilik haklarına saldırı davalarında IP adresi tespiti genellikle soruşturmanın başlangıç noktasını oluşturur. Ancak bu başlangıç noktasından mahkumiyete giden yolda, pek çok ek delilin toplanması zorunludur. Şüphelinin o tarih ve saatte ilgili internet bağlantısını fiilen kullanıp kullanmadığı, evde başka kullanıcıların bulunup bulunmadığı, cihaz üzerinde dijital iz ve bulguların mevcut olup olmadığı, şüphelinin teknik bilgi ve beceri düzeyi, olaya ilişkin bir mobilin bulunup bulunmadığı gibi hususların ayrı ayrı araştırılması gerekmektedir.

Anayasa Mahkemesi de bireysel başvuru kararlarında, IP adresine dayalı tespitlerin adil yargılanma hakkı bağlamında dikkatle değerlendirilmesi gerektiğine işaret etmiştir. Özellikle masumiyet karinesi çerçevesinde, bir IP adresinin belirli bir kişiyle eşleştirilmesindeki teknik belirsizliklerin, sanık aleyhine yorumlanamayacağı vurgulanmıştır. Bu yaklaşım, Avrupa İnsan Hakları Mahkemesi'nin dijital delillere ilişkin genel tutumu ile de uyumludur.

IP adresinin delil olarak kullanılabilmesi için yalnızca teknik doğruluğu değil, aynı zamanda delil zincirinin bütünlüğü de sağlanmalıdır. Log kayıtlarının elde edilmesinden mahkemeye sunulmasına kadar geçen süreçte, bu kayıtların değiştirilmediğinin, manipüle edilmediğinin ve doğru biçimde muhafaza edildiğinin ortaya konması zorunludur. 5271 sayılı CMK'nın dijital delillere ilişkin genel hükümlerinin yanı sıra, Adli Bilişim inceleme standartları da bu süreçte belirleyici rol oynamaktadır.

Uygulamada sıklıkla karşılaşılan sorunlardan biri, internet servis sağlayıcılarının log kayıtlarını ne formatta, ne süreyle ve hangi güvenlik önlemleri altında sakladıklarına ilişkin standartların yetersizliğidir. Bir servis sağlayıcısının mahkemeye sunduğu log kaydının, ne zaman oluşturulduğu, üzerinde herhangi bir değişiklik yapıp yapılmadığı ve bütünlüğünün nasıl korunduğu sorularına tatmin edici yanıtlar verilememesi, o delilin güvenilirliğini ciddi biçimde zedelemektedir. Zaman damgalarının NTP sunucularıyla senkronize olup olmadığı, kayıt sistemlerinin yedekleme mekanizmaları ve erişim kontrolleri gibi teknik detaylar, hukuki süreçte mutlaka sorgulanması gereken hususlardır.

Bilirkişi incelemelerinde de IP adresine dayalı tespitlerin değerlendirilmesi özel bir uzmanlık gerektirmektedir. Ne yazık ki Türk yargı sisteminde bilişim alanında yetkin bilirkişi sayısı oldukça sınırlıdır ve mevcut bilirkişilerin bir kısmı da CGNAT, port tahsisi gibi güncel teknik konularda yeterli bilgiye sahip değildir. Bilirkişi raporlarında IP adresinin belirli bir aboneye ait olduğunun tespit edilmesiyle yetinilip, bu tespitin gerçek kişiyi ne ölçüde tanımladığı sorusunun irdelenmemesi, hatalı mahkumiyet riskini artıran ciddi bir eksikliklerdir.

BÖLÜM VII —

Sonuç ve Değerlendirme

Tüm bu teknik ve hukuki gerçeklikler ışığında, IP adreslerinin delil değerine ilişkin şu temel sonuçlara ulaşmak mümkündür. IP adresi, dijital soruşturmanın vazgeçilmez bir başlangıç noktasıdır; ancak tek başına bir kişiyi kesin olarak tanımlama kapasitesine sahip değildir. Statik IP adreslerinin delil değeri, dinamik IP adreslerine kıyasla görece daha yüksektir; ancak statik IP adreslerinde bile, o bağlantıyı fiilen kimin kullandığı sorusu açık kalır. CGNAT teknolojisinin yaygınlaşması, IP adresinin delil değerini radikal biçimde zayıflatmış olup, port bilgisi olmaksızın yapılan tespitler hukuki açıdan neredeyse anlamsız hale gelmiştir.

Türk hukuk sisteminin bu teknik gerçekliklere uyum sağlaması acil bir gerekliliktir. Servis sağlayıcıların CGNAT port tahsis kayıtlarını yeterli süreyle saklamasını zorunlu kılan açık yasal düzenlemeler yapılmalıdır.

Savcılık ve kolluk kuvvetleri, IP adresi sorgularında port bilgisini de talep etme konusunda eğitilmeli ve bu bilginin önemi hakkında bilinçlendirilmelidir. Bilirkişi havuzlarına dijital delil konusunda gerçek uzmanlığa sahip kişilerin dahil edilmesi ve mevcut bilirkişilerin bu alanda sürekli eğitim alması sağlanmalıdır.

Hâkimler ve savcılar açısından ise en önemli ilke, IP adresine aşırı güven duymaktan kaçınmaktır. Her IP tespitinde, adresin dinamik mi statik mi olduğu, CGNAT kullanılıp kullanılmadığı, port bilgisinin mevcut olup olmadığı, VPN veya proxy kullanımı ihtimali, halka açık ağ paylaşımı olasılığı ve delil zincirinin bütünlüğü sorularının sistematik biçimde sorulması gerekmektedir. Aksi takdirde, dijital dünyanın karmaşıklığı göz ardı edilerek verilen kararlar, hem adalet duygusunu zedeleyecek hem de telafisi güç hak ihlallerine yol açacaktır.

Dijital delil hukuku, sürekli gelişen ve dönüşen teknolojik altyapıya paralel olarak kendini yenilemek zorundadır. IPv6'ya geçiş sürecinin hızlanmasıyla CGNAT sorununun kısmen çözülmesi beklenebilir; ancak bu geçiş tamamlanana kadar mevcut sorunların bilincinde olmak ve hukuki değerlendirmeleri buna göre yapmak, hukuka uygunluk için vazgeçilmez bir gerekliliktir. IP adresleri, dijital soruşturmanın yapbozundaki önemli parçalardan yalnızca biridir; ancak tek parçadan bütün resmi çıkarmaya çalışmak, her zaman hatalı sonuçlara götürme riski taşımaktadır.

Son olarak vurgulanması gereken bir husus da uluslararası boyuttur. İnternetin sınır tanımayan yapısı, IP adresine dayalı tespitlerin sıklıkla uluslararası hukuki yardımlaşma süreçlerine taşınmasına neden olmaktadır. Budapeşte Siber Suç Sözleşmesi çerçevesindeki işbirliği mekanizmaları, Türkiye'nin taraf olduğu ikili adli yardımlaşma anlaşmaları ve Avrupa Konseyi'nin elektronik delil alanındaki yeni düzenlemeleri, bu konuda sürekli takip edilmesi gereken dinamik bir uluslararası hukuk alanı oluşturmaktadır. Hukukçuların bu karmaşık çok katmanlı yapıyı kavraması ve müvekkillerinin haklarını etkili biçimde savunabilmesi için, teknik bilgiyle hukuki bilgiyi sentezleyen bütüncül bir bakış açısına sahip olmaları artık bir tercih değil, mesleki bir zorunluluktur.

Çevrimiçi sürüm: <https://burakucuncu.com.tr/ip-adreslerinin-delil-degeri>