BİLİŞİM SUÇLARINDA IP TESPİTİ İLE EKRAN GÖRÜNTÜLERİ ÇIKTILARININ İSPAT DEĞERİ

Evidence Value of Ip Address Detection and Screenshot Print Outs in Cybercrimes

Doğan Gedik*

Öz

Bilişim teknolojilerindeki baş döndürücü gelişmeler, gerek maddi hukuka gerekse muhakeme hukukuna ilişkin yeni sorunları da beraberinde getirmiştir. İnternet ve bilişim teknolojilerindeki gelişmelerin yarattığı sorunlar, yalnızca yeni suç tiplerinin ortaya çıkması veya klasik suçların yeni işlenme şekilleriyle sınırlı kalmamış; buna bağlı olarak soruşturma ve delillendirme ile mevzuata dair yeni sorunların da ortaya çıkmasına neden olmuştur. Bu çalışmada; bilişim suçlarında uygulaması oldukça çok olan IP adresi (numarası) tespiti ile ekran görüntüleri fiziksel çıktılarının, ceza muhakemesinde ispat değeri üzerinde durulacaktır.

Anahtar Kelimeler: Dijital Delil, IP Numarası, Ekran Görüntüsü Çıktısı, İspat.

* Dr., İstanbul Bölge Adliye Mahkemesi Hâkimi, dogangedik@hotmail.com, ORCID: 0000-0001-6131-9726.

Makale Gönderim Tarihi: 27.03.2019.

Makale Kabul Tarihi: 18.05.2019.

Abstract

Developments in information Technologies bring new problems to both substantive and procedural law. These problems are not only limited to new crime types or the new ways to commit classical crimes but also affect evidence and cause issues related to body of laws. In this work, the importance of IP address detection and screenshot print outs, which are widely encountered in cybercrimes, as evidence in criminal procedure will be examined.

Keywords: Digital Evidence, IP Number, Screenshot, Evidence.

I. GİRİŞ

Son yılların en hızlı büyüyen bilişim sektörü olan internet; sınırları tanımlanamayan, kuralları konamayan, demokratik bir platform olarak kabul edilmekte;[1] bireylere, gerçek kimliğini gizleme veya başka bir ad kullanma imkânı da sağlayarak kendisini ve düşüncesini serbestçe ifade etme hürriyeti tanımaktadır.[2] Bu gelişme, dünyayı küçük bir köy haline getirirken, bilgisayar ortamında sesli ve görüntülü her türlü sohbet, özel hayatın paylaşılması, internet üzerinden alışveriş gibi birçok yeni gelişmelere öncülük etmiş, sonuçları olumlu veya olumsuz yeni alışkanlıklar kazandırmıştır.[3] Nitekim gelişen iletişim teknolojileri ile insanların hayatında önemli bir yer edinen sosyal medya,[4] hemen her yaştan, cinsiyetten ve kültürden insanların çevrelerini genişleteceği, iletişim kurabileceği, bilgi ve

---

1 Buna ilişkin örnek olarak, bkz. Ceren Yegen, "Demokratik Ve Yeni Bir Kamusal Alan Olarak Sosyal Medya," *Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi* 1, no. 2 (Aralık 2013): 119*ff*.

2 Servet Yetim, "Bilişim Suçları ve Etkin Mücadele Yöntemleri," *Terazi Hukuk Dergisi* 9, no. 95 (Temmuz 2014): 80*ff*.; Ufuk Taşçı ve Ali Can, "Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014," *Fırat Üniversitesi Sosyal Bilimler Dergisi* 25, no. 2 (2015): 229.

3 Taşçı ve Can**,** "Siber Suçlarla Mücadele," 230.

4 Bkz. Fehmi Şener Gülseren, "İnternet Ortamında İşlenen Hakaret Suçları," *LAÜ Sosyal Bilimler Dergisi* 4, no. 1 (Nisan 2013): 16; Yegen, "Yeni Bir Kamusal Alan," 120*ff*.; Ceren Çubukçu ve Berrin Atiker, "Sosyal Medya ve Bilişim Suçları," Academia, erişim tarihi Mayıs 5, 2019, https://www.academia.edu/31785425/ Sosyal_Medya_ve_Bilişim_Suçları. 2000'li yılların ortalarında Web 2.0 teknolojisinin kullanılmaya başlanması ile birlikte sosyal medya kavramı herkesin hayatına girmiştir. Sosyal medya, bireylerin internette birbirleriyle yaptığı paylaşımlar, diyaloglar ve sosyal ağ uygulamalarından oluşan bir dijital platformu ifade etmektedir. Örneğin kullanıcıların, kendi içeriklerini ürettiği ve paylaştığı Facebook, Youtube, Flickr gibi web ağları; yazarların, okurlarına bilgi, görüş ve düşüncelerini aktardıkları bloglar; anlık paylaşımların yapıldığı Twitter gibi mikro bloglar ve bunların yanında, e-posta ve sohbet siteleri, iletişim ve mesajlaşma programları, forumlar, diğer bir deyişle, kişilerin internet yoluyla yaptıkları tüm bilgi ve içerik paylaşımları sosyal medyayı oluşturmaktadır.

deneyimlerini paylaşıp üzerinde tartışmalar yapabileceği bir platform haline gelmiştir.[5]

İnternet ve bilişim teknolojilerindeki gelişmelerle birlikte bireyin kişisel, ekonomik, siyasi ve sosyal birçok faaliyeti sanal ortama taşınmış, günlük hayata dair ne varsa sanal ortamda yaşanır olmuştur. Bu şekilde internet ve dolayısıyla sosyal ağların, kullanıcılarının bireysel ve sosyal yaşamlarına kolaylık ve katkı sağlayarak hayatın merkezine yerleşmesi, adeta vazgeçilmez hale gelmesi suçluluk olgusuna da davetiye çıkarmıştır. Nitekim bu durum hem bazı yeni suç tiplerinin ortaya çıkmasına neden olmuş, hem de hakaret, tehdit, şantaj ve dolandırıcılık gibi klasik suçların bilişim sistemleri aracı kılınmak suretiyle işlenmesine zemin hazırlamıştır. Ancak bilişim dünyasındaki gelişme yalnızca yeni suç tiplerinin ortaya çıkması veya klasik suçların yeni işlenme şekilleriyle sınırlı kalmamış; buna bağlı olarak soruşturma ve delillendirme ile mevzuata dair yeni sorunların da ortaya çıkmasına neden olmuştur. Zira suç mahalli genişleyerek fiziksel alandan dijital ortama kaydığı gibi klasik delillerden farklı özellikler taşıyan, bilgisayar ve benzeri cihazlar ile bilişim sistemlerinden elde edilen bir delil türü (dijital/sayısal delil) ile delillendirme sürecini (adli bilişim) ortaya çıkarmıştır. Böylece bilişim teknolojilerindeki gelişmeler, gerek maddi hukuka gerekse muhakeme hukukuna ilişkin yeni sorunları da beraberinde getirmiştir.

Bu çalışmada, ağırlıklı olarak sosyal ağlar üzerinden işlenen suçlar olmak üzere bilişim suçlarının soruşturulmasında adeta bir anahtar vazifesi gören IP adresi (numarası) tespiti ile gerek şikayetçi/ihbarcı kişi veya kurumların şikayete ekledikleri gerekse soruşturma makamlarının dosyaya dahil ettiği ekran görüntüleri fiziksel çıktılarının, ceza muhakemesinde ispat değeri üzerinde durulacaktır.

---

[5] Gülçin Cebecioğlu ve İpek Beyza Altıparmak**,** "Dijital Şiddet: Sosyal Paylaşım Ağları Üzerine Bir Araştırma," *Sakarya University Journal of Education* 7, no. 2 (2017): 424; Yegen, "Yeni Bir Kamusal Alan," 120; Gürkan Özocak**,** "Sosyal Medyada İşlenen Suç Tipleri Ve Suçluların Tespiti," Özocak Hukuk & Danışmanlık, erişim tarihi Mart 11, 2019, http://www.ozocak.com/Dosyalar/a104b3.pdf.

II. IP TESPİTİNİN İSPAT DEĞERİ

A. Kavram ve IP Tespiti

İnternet hizmetlerini kullanmak için gerekli olan tüm yazılımlar ve bağlantı yazılımları TCP/IP protokollerine uygun olarak iletişim kurar ve işlem görürler. Bu protokoller kümesinin ulaşım katmanında TCP (Transfer Code Protocol), yönlendirme katmanında ise IP (Internet Protocol) protokolü bulunmaktadır. TCP/IP protokolü dâhilinde her bilgisayarın tanınmasını sağlayan ve birbirinden ayıran bir IP adresi vardır.[6]

IP adresi,[7] internete bağlanmak isteyen bilgisayarlara internet servis sağlayıcıları tarafından atanan benzersiz bir kimlik numarasıdır. Günümüzde bilgisayar dışında internet bağlantısı sağlayabilen akıllı telefonlar, televizyonlar, tabletler de IP adresi almaktadır.[8]

---

6 Elif Gökşen, "Türk Ceza Muhakemesinde Dijital Verilerin Delil Değeri" (yayımlanmamış yüksek lisans tezi, Galatasaray Üniversitesi, 2014), 31.

7 IP adresi: "Belirli bir ağa bağlı cihazların birbirini tanımak, birbirleriyle iletişim kurmak ve birbirlerine veri yollamak için kullandıkları, İnternet Protokolü standartlarına göre verilen adres," İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik m. 3/1-h.

8 Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku* (Ankara: Seçkin Yayıncılık, 2014), 694*ff*.; Murat Volkan Dülger ve Gözde Modoğlu, *Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri ile İnternet İletişim Hukuku (Uygulama Rehberi)* (Ankara: Türk Ceza Adalet Sisteminin Etkinleştirilmesi Avrupa Birliği/Avrupa Konseyi Ortak Programı, 2014), 109*ff*. İnternete bağlandığınızda sizin bilgisayarınızın da bir IP adresi vardır. ISS'nize telefon numarasını çevirip bağlandığınızda, aslında o ISS'de yer alan bir sunucu bilgisayara bağlanıyorsunuz demektir. Bu sunucu bilgisayar, bağlantı sırasında kullandığınız kullanıcı ismi ve şifrenize göre elindeki boş adreslerden birini (örneğin 212.172.xxx.xxx gibi) İnternet Protokolü (IP) numarasını bilgisayarınıza atar. Bu yüzden her bağlantıda IP adresinizin son numarası değişir. Ancak IP numaranız değişse bile sunucudaki LOG kayıtlarında hangi tarihte ve saatte hangi IP adresinin hangi telefon numarasına tahsis edildiği saklanır. Artık internette dolaşırken sizin kimliğiniz aldığınız IP numaranızdır. Siz de Web sitelerine, e-posta kutularına bağlanırken size atanmış olan bu IP adresini kullanırsınız. Bazı IP adresleri ise sabittir (static IP), yani IP adresleri hiç değişmez. Bir Web sitesinin adresi her yazıldığında bulunabilmesi için IP adresi genellikle sabittir.

Böylece internete bağlanan her cihaz bir IP numarası almakta ve diğer cihazlarda bu cihaza IP adresi ile ulaşmaktadırlar. IP numarası, servis sağlayıcı tarafından boşta olan bir numaranın verilmesi suretiyle her bağlantıda değişebileceği[9] gibi, erişim sağlayıcılar tarafından, ADSL abonelerine verilenlerde olduğu şekliyle statik de olabilir.[10] Bu nedenle IP adresleri kendi içinde statik ve dinamik olmak üzere ikiye ayrılmaktadır.[11]

IP numarası sayesinde bağlı olan abone ve lokasyon bilgilerine ulaşmak mümkün hale gelmektedir. Bu özelliği dolayısıyla IP adresi (numarası), sanal âlemde bilişim sistemi kullanıcılarını tanımlayan en önemli ayırt edici unsur olarak karşımıza çıkmaktadır.

Yukarıdaki açıklamadan da anlaşıldığı üzere bilişim suçlarında veya bilişim sistemleri araç olarak kullanılması suretiyle işlenen suçlarda, gerek failin gerekse lokasyonun belirlenmesi için IP adres bilgisine ihtiyaç bulunduğu kuşkusuzdur. Soruşturmada yol alınması, en nihayetinde delillendirilmesi noktasında IP kayıtlarının düzenli ve doğrulanabilir/kanıtlanabilir şekilde tutulmuş olmasının da önemi büyüktür. IP adresi belirlenmeye çalışılırken, zaman bilgilerine (tarih, saat, dakika, saniye) ve yurtdışından temin edilecekse saat farkına da dikkat edilmelidir. Yanlış bildirilen bir IP numarası, soruşturmanın seyrini değiştirebildiği gibi olayla ilgisi olmayan kişi/kişilerin şüpheli veya sanık olmasını da sonuçlayabilmektedir.[12] Nitekim 5651 sayılı

---

[9] Bu değişkenlik nedeniyle IP numarasının kullanıldığı tarih ve saatin kaydedilmesi oldukça önemlidir; zira, ancak bu tarih ve saate göre o sırada hangi bilgisayarın söz konusu IP numarasına sahip olduğu belli olur.

[10] Burcu Erdoğan, "Bir Kişiyi Suçlamak İçin IP Adresi Yeterli midir?," *digiSophia*, erişim tarihi Ekim 1, 2018, http://www.digisophia.com/Article/Details/61.

[11] "Statik IP adresi; hiçbir zaman değişmeyen, kalıcı bir IP adresidir. Dinamik IP adresi ise bir cihaza, internete her bağlanışında yeniden tanımlanan yani geçici bir IP adresidir. Statik IP adresleri bilgisayara, bir admin tarafından manuel olarak atanır. Dinamik IP adresleri ise bilgisayar arayüzü ya da sunucu yazılımı tarafından, otomatik olarak atanır. IP adresleri, servis sağlayıcı tarafından, statik olacak şekilde de tanımlanabilir." "IP Adresim Nedir," CHIP Online, erişim tarihi Mayıs 25, 2019, https://www.chip.com.tr/ip-adresim-nedir.

[12] Erdoğan: "Özellikle Kredi kartı dolandırıcılığı olarak adlandırılan suçlarda mahkemeler sadece bankanın sunmuş olduğu IP bilgisinden yola çıkmaktadır.

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, taraflara ait IP adresi bilgisini *"trafik bilgisi"* içinde kabul etmiş (m. 2/1-j; ve "*erişim sağlayıcıları*" (m. 6/1-b), "*yer sağlayıcıları*" (m. 5/3) ile "*toplu kullanım sağlayıcıları*"na (m. 7/2) trafik bilgilerini tutma yükümlülüğü yüklemiştir.[13] 5651 sayılı Kanuna dayanarak çıkarılan "İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik" de "*erişim sağlayıcı"*nın, trafik bilgisini bir yıl

Ancak bu aşamada verilen rakamlardaki en ufak bir hata dolayısı ile soruşturmanın seyrinin tamamen değişeceği düşünülmüş müdür? Bankalar bu bilgileri zaman damgalı olarak vermişler midir? Birçok yargılamada, IP bilgilerinin kaynağının güvenilir olup olmadığının araştırılması gerekirken, araştırma yapılmadığı gözlemlenmektedir. Çoğu zaman verilen IP ile ilgili sağlanan bilgilerin doğru kabul edilmesi sonucu yanlış mahkumiyet kararı verilebildiği gibi, bir çok sanık da internet bağlantılarının şifresiz olduğu ya da IP bilgisinin değiştirilmiş olabileceği savunmaları ile (başkaca delil yoksa) beraat ettikleri görülmüştür. Peki, gerçek sanıkların bıraktığı izler nerededir, ne yazık ki soruşturma makamları, bu sorunun cevabını halen verebilecek nitelikte değildir. Sayı üretmek zor olmadığından soruşturmanın yönünün ya da davanın seyrinin yetkisiz kimseler tarafından tutulan ve güvenli olmayan bilgiler doğrultusunda yönlendirmek verilen hükmün güvenilirliğini de tartışma konusu haline getirir." "Bir Kişiyi Suçlamak."

13 5651 sayılı Kanunda "trafik bilgisi", taraflara ilişkin IP adresi, verilen hizmetin başlama ve bitiş zamanı, yararlanılan hizmetin türü, aktarılan veri miktarı ve varsa abone kimlik bilgilerini (m. 2/1-j; "erişim sağlayıcı", kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri (m.2/1-e); "yer sağlayıcı", hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri (m. 2/1-m); "toplu kullanım sağlayıcı", kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayanı (m. 2/1- i) ifade eder şekilde tanımlamıştır.

İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik 3. maddesinde "erişim sağlayıcı trafik bilgisi"ni, "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 gibi bilgileri" (m.3/1-g); "yer sağlayıcı trafik bilgisi"ni, "İnternet ortamındaki her türlü yer sağlamaya ilişkin olarak; kaynak IP adresi, hedef IP adresi, bağlantı tarih ve saat bilgisi, istenen sayfa adresi, işlem bilgisi (GET, POST komut detayları) ve sonuç bilgileri gibi bilgileri" (m.3/1-ş) ifade eder şekilde tanımlamıştır.

saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü, oluşan verilerin dosya bütünlük değerlerini zaman damgası[14] ile birlikte muhafaza etmek ve gizliliğini temin etmekle (m. 8/1-b); "*yer sağlayıcı*"nın da trafik bilgisini altı ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle (m. 7/1-c) yükümlü olduğunu belirtmiştir. 11.04.2017 tarihli ve 30035 sayılı Resmi Gazetede yayınlanan "*İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik*" de ticari olsun olmasın internet toplu kullanım sağlayıcılarına; kendi iç ağlarında dağıtılan IP adres bilgilerini, kullanıma başlama ve bitiş zamanını ve bu IP adreslerini kullanan bilgisayarların tekil ağ cihaz numarasını (MAC adresi) gösteren bilgileri, hedef IP adresi, bir veya birden fazla IP adresinin portlar aracılığı ile kullanıcılara paylaştırılması yöntemi ile sunulan internet erişim hizmetinde kullanıcıya tahsis edilen gerçek IP ve port bilgilerini, elektronik ortamda kendi sistemlerine kaydetmek ve iki yıl süre ile saklamakla yükümlendirmiştir (m. 4-5). Aynı yönetmelik toplu kullanım sağlayıcıları için kamera kayıt yükümlülüğü de getirmiştir. Düzenlemeye göre "Güvenlik amacıyla işyerlerinin giriş ve çıkışlarını görecek şekilde yüksek çözünürlüklü (en az 3 mega piksel) ve "IR" (gece görüşlü) kamera kayıt sistemi kurulur. Bu sistem aracılığıyla elde edilen kayıtlar doksan gün süreyle saklanır ve bu kayıtlar yetkili makamlar haricindeki kişi ve kuruluşlara verilemez" (m. 9/1-ğ).[15]

---

[14] 5070 sayılı Elektronik İmza Kanununda "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 eder*" olarak tanımlanmıştır. Zaman damgaları belli bir verinin belirtilen bir tarihte var olduğunu kanıtlarlar. Zaman damgası sunucusu, zaman damgalarını imzalamak için açık anahtar teknolojisini kullanarak, verinin bütünlüğünü ve belirli bir tarihteki varlığını onaylar. Sertel Şıracı, "İnternet Kanununa Göre Log Tutma," Av. Sertel Şıracı, erişim tarihi Şubat 02, 2019, https://www.sertels.av.tr/avukat/hukuk/bilisim-hukuku/internet-kanununa-gore-log-tutma.html.

[15] 5651 Sayılı Kanun ile ilgili üzere yönetmelikler, tebliğler, genelgeler, Bakanlar Kurulu Kararları gibi ikincil mevzuatı da içeren internet hukukuna ilişkin güncel mevzuat ve içtihatlara dair kaynak için, bkz. Mehmet Bedii Kaya, "İnternet Hukuku, Mevzuat & İçtihat," Mehmet Bedii Kaya, erişim tarihi Mayıs 25, 2019, https://www.mbkaya.com/hukuk/internetmevzuat.pdf.

Erdoğan'ın belirttiği üzere, bütün bu yasal hükümlerde, trafik bilgilerini hangi kurumların tutması gerektiği, nasıl tutması gerektiği ve gizliliğini sağlamaları gerektiği açıkça yazılmış, ancak yasal süreçte bunların nasıl sunulması gerektiği konusunda hiç bir usul belirtilmemiştir. Ancak verilerin zaman damgası ile saklanması gerektiği belirtildiğine göre, bu verilerin delil niteliğinde olabilmesi için değişmemiş ve bozulmamış halde olduğunu gösteren bir biçimde mahkemeye sunulması gerektiğini de çıkarabiliriz.[16]

B. IP Tespitinin İspat Değeri

Uygulamada bir başkasının bilişim sistemine girme, sosyal medya hesaplarını (örneğin Facebook) veya e-posta adreslerini ele geçirme gibi bilişim suçlarında ya da sosyal paylaşım siteleri üzerinden kişisel verileri yayma, hakaret veya şantajda bulunma örneğindeki gibi bilişim sistemleri aracı kılınarak işlenen suçlarda faile ulaşmak için en yaygın kullanılan yöntem, suça konu işlem yapılırken kullanılan IP numarasının tespit edilmesi[17] ve daha sonra IP

---

16 Erdoğan, "Bir Kişiyi Suçlamak."

17 Belirtelim muhatap yurtdışı merkezli ve Türkiye temsilciği yok ise IP numarasının tespiti ancak "Uluslararası Adli İstinabe" yoluyla mümkündür. Bununla birlikte ABD merkezli sosyal ağlar (Facebook, Twitter, YouTube), sınırlı bazı suçlar dışında istinabe yoluyla trafik bilgi taleplerini karşılamamaktadır. Örneğin Facebook, çocuk pornosu, intihar vakaları, öldürme gibi suçlar dışında bilgi paylaşımına yanaşmamaktadır. Söz gelimi hakaret suçu konulu soruşturmalarda yapılan istinabelerde olumlu sonuç alınamamaktadır. Bu sebeple uygulamada şirket merkezinin yurt dışında olduğu ve delile ulaşmanın mümkün olmadığı gerekçe gösterilerek takipsizlik kararı verildiği gibi mahkûmiyeti gerektirir delil elde edilmediği gerekçesiyle beraat kararı da verilebilmektedir. Örneğin, "Sanığın, bahse konu facebook hesabının kendisi tarafından oluşturulmadığına yönelik savunması, şikâyete konu hesabın oluşturulduğu bilgisayarın IP adres bilgilerinin tespit edilememiş olması, katılanın eşi olan tanık Zeynep, duruşmada alınan ifadesinde, iddiayı doğrular mahiyette beyanda bulunmuş ise de, tanığın görgüye dayanmayan ve maddi delille desteklenmeyen anlatımına dayalı olarak iddiaya konu eylemleri gerçekleştirenin sanık olduğu sonucuna varılamayacak olması, Adalet Bakanlığı Uluslararası Hukuk ve Dış İlişkiler Genel Müdürlüğünün, "İnternet Ortamında İşlenen Suçlarda Uluslararası Ceza İstinabe İşlemleri" başlıklı yazısında yer verdiği, "ABD mevzuatına göre (18 U.S.C. §

numarasının tahsis edildiği internet abonesinin belirlenmesidir.[18] Ancak bu yöntem doğru olmakla birlikte, bu tür suçlara ilişkin soruşturmalarda yapılan en yaygın hatalardan biri de, IP numarası belirlendiğinde, tahsis edildiği internet abonesinin hemen "şüpheli" sıfatıyla soruşturmaya dahil edilmesi, hakkında doğrudan dava açılabilmesi ve hatta sadece IP tespitine dayanarak mahkum edilmesidir. Oysa bu, yanlış bilgi veya kolaycılıktan kaynaklanan bir tutumdur.[19] Nitekim adli bilişim esaslarına uygun yürütülen bazı soruşturmalarda, olayla ilgisi bir yana abonenin olaydan haberi dahi olmadığı görülmüştür. Bu nedenle dijital ortamda veri bazlı işlemi gerçekleştiren kişinin tespit edilmesi, diğer delil ve yöntemlerle verinin "kişiselleştirilmesi" gerekmektedir.[20]

Anlaşıldığı üzere bilişim suçlarında soruşturmanın yönlendirilmesi ve nihayetinde faile ulaşılması bakımından IP numarasının

2703 – f) internet ortamında işlenen suçlara dair trafik bilgileri, yer sağlayıcılar veya erişim sağlayıcılar tarafından 90 gün süreyle saklanmaktadır. Bu süre içinde resmi otoritelerce başvurulduğunda anılan saklama süresine 90 gün daha ilave edilmektedir." açıklamalarına, olayın üzerinden geçen zaman dilimine ve dosya kapsamına nazaran, gelinen aşamada, savunmanın aksine maddi bir delil elde edilmesi imkânının bulunmaması karşısında, sanığın mahkumiyetine yeter, her türlü derecede şüpheden uzak, kesin ve inandırıcı delil bulunmaması sebebiyle üzerine atılı hakaret ve verileri hukuka aykırı olarak verme veya ele geçirme suçlarından dolayı CMK'nın 223/2-e maddesi gereğince beraatine karar verilmesi gerekirken, dosyada mevcut delillerden hangilerine hangi sebeplerle itibar edildiği irdelenmeyip, yasal, yeterli ve geçerli bir gerekçeye dayanılmaksızın, yazılı şekilde sanık hakkında mahkumiyet kararı verilmesi" Yar. 12. CD, E.2015/4151, K.2016/259, 13.01.2016, (UYAP). Uluslararası istinabe konusunda ayrıca, bkz. Özocak, "Sosyal Medyada İşlenen."

[18] Örneğin, "hesaba Konya ilinde İ. H. Ç. adına kayıtlı bir IP adresinden girilerek gerçekleştirildiğinin tespit edilmesi karşısında İ. H. Ç.in konuya ilişkin beyanının alınması, sonucuna göre sanığın hukuki durumunun değerlendirilmesi gerektiği gözetilmeden eksik araştırma ve inceleme ile yazılı şekilde hüküm kurulması," Yar. 2. CD, E.2016/14036, K.2018/14990, 06.12.2018, (UYAP).

[19] Dülger, *İnternet İletişim*, 695.

[20] Kişiselleştirme kavramı için, bkz. Olgun Değirmenci, *Ceza Muhakemesinde Sayısal (Dijital) Delil* (Ankara: Seçkin Yayıncılık, 2014), 404*ff.*; Koray Doğan, *Kuşkudan Sanık Yararlanır İlkesi* (Ankara: Seçkin Yayıncılık, 2016), 295. Nitekim Yargıtay içtihatlarında sıkça geçen "IP adresini kullanan abonenin sanıkla bağlantısı araştırılıp" ifadesi kişiselleştirmeye vurgu yapmaktadır.

tespiti oldukça önemli bir eşiktir.[21] Ancak hem IP numarasının tespiti hem de bundan yola çıkarak failin tespiti, suçun sanal ortamda işlenmesinden kaynaklı kendine özgü zorlukları ihtiva etmekte ve adli makamları daha ihtiyatlı olmaya zorlamaktadır. Gerçekten de tespit edilen IP numarasını kullanan abonenin adresi internet kafe, otel veya alışveriş merkezi gibi yerler çıktığında failin tespiti zorluk arzetmektedir.[22] Yukarıda zikrettiğimiz 5651 sayılı Yasa ve ikincil

---

[21] Yunus Balı: "Öncelikle, nereye veya kime ait olduğu bilinmeyen bir IP numarası için "Whois" sorgulaması yapılır. "Whois" sorgulaması sonucunda söz konusu IP'nin kullanıcılara tahsis işlemlerini gerçekleştiren organizasyona yani servis sağlayıcıya ulaşılmış olur. Bu aşamaya kadar herkes genel bir tespit yapabilir. Yani bir IP'nin hangi ülkeden, hangi şehirden bağlandığı yukarıdaki gibi basit bir işlemle tespit edilebilir. Ancak o IP numarasının kim tarafından kullanıldığının tespiti isteniyorsa, bu bilgi yasal yollardan elde edilmesi gereken ve yargı makamları tarafından yapılacak bir tespitle verilebilen bir bilgidir." "IP Numarası Tespiti," Dijitaldeliller, erişim tarihi Aralık 1, 2018, http://www.dijitaldeliller.com/ip_tespiti.html.

[22] "Sanığın aşamalardaki savunmalarında; suç tarihinde internet cafe sahibi olduğunu, evde ve iş yerinde kablolu internet kullandığını, atılı suçu kabul etmediğini belirtmesi karşısında; sanığın iş yerinde bulunan modemin kablosuz bağlantı (wifi) özelliği olan modem olup olmadığı ve buna göre de dışarıdan üçüncü bir kişinin haricen bağlantı yapıp yapmayacağı araştırılıp, ayrıca tespit edilen IP numarasının statik mi yoksa dinamik mi olduğu kurumdan sorulup, yapılacak bu tespitler ile sanığın savunmasının örtüşüp örtüşmediği, IP numarasının kopyalanması, kablosuz veya kablolu bağlantı ile internet hattına girilerek havale işlemi yapılmasının mümkün olup olmadığı hususlarının araştırılarak, yapılan eylemin üçüncü bir kişi tarafından gerçekleştirme olasılığının bulunup bulunmadığı hususlarının aydınlatılması için somut olaya ilişkin konusunda uzman bilirkişi incelemesi yaptırılarak sonucuna göre sanığın hukuki durumunun takdir ve tayini gerektiği gözetilmeden, eksik inceleme ile mahkûmiyet hükmü kurulması" Yar. 2. CD, E.2018/6474, K.2018/1368, 20.11.2018, (UYAP).

"Sanığın internet cafe çalıştırdığını, merkez bilgisayara bağlı 30 adet bilgisayar bulunup tek hat üzerinden internete bağlanıldığını, bu bilgisayarlardan böyle bir işlem yapılmış olabileceğini savunması karşısında; merkez bilgisayar ve buna bağlı başka bilgisayarın bulunup bulunmadığı, işlemin hangi bilgisayardan yapıldığı, merkez bilgisayarda suça konu işlemlere ilişkin bir kaydın bulunup bulunmadığı, GSM şirketi tarafından IP adresi yanında PORT numarası verilip verilmediği, PORT bilgisine ulaşıldığında birden fazla kişiye verilen IP'nin belirlenen saatte kim tarafından kullanıldığı tespit edilmeden ayrıca mağdurun kredi kartı bilgileri haksız olarak ele geçirilerek internet üzerinden kontör yük-

mevzuat uyarınca müşterilerine şifreli veya şifresiz şekilde kablosuz internet hizmeti sağlayan bu tür yerlerin; hem iç IP dağıtım loglarını elektronik ortamda kendi sistemlerine kaydetmek, hem de bu bilgilerin doğruluğunu, bütünlüğünü ve gizliliğini teyit eden değeri kendi sistemlerine günlük olarak kaydedip saklamak yükümlülükleri bulunmaktadır.[23] Bu nedenle zaman geçirilmeden bu kayıtların, kamera kayıtlarıyla birlikte temin edilmesi gerekmektedir.[24] Ancak işletmecilerin her zaman kayıt tutma yükümlülüğünü mevzuata uygun şekilde yerine getirdiklerinden söz etmek mümkün görünmemekte, bu da failin belirlenmesini zorlaştırmaktadır.

Diğer taraftan tespit edilen adres konut çıktığında ise uygulamada başta abone görünen kişi olmak üzere, duruma göre konutta yaşayan diğer kişilerin de ifadesine başvurulmaktadır. Ancak böyle bir durumda kişi veya kişilerin suçlamayı kabul etmemesi veya örneğin 3. kişiler tarafından şifresi kırılmak suretiyle internete girilmiş olabileceği şeklinde savunmada bulunulması[25] halinde, soruşturmanın derinleştirilmesi, özellikle adli bilişim yöntemleriyle failin belir-

leme işlemi yapıldığı iddia olunduğundan, kontör yüklendiği belirlenen telefon hatlarının, suç tarihindeki hat sahipleri ve kullanıcıları araştırılıp, tanık sıfatıyla dinlenerek ve tüm deliller birlikte değerlendirilerek sonucuna göre sanığın hukuki durumunun tayini ve takdiri gerektiği gözetilmeden, eksik araştırma ile yazılı şekilde karar verilmesi," Yar. 8. CD, E.2014/11582, K.2013/9756, 6.5.2014, (UYAP).

[23] 5651 sayılı Kanun kapsamında yer alan erişim sağlayıcılar, yer sağlayıcılar, içerik sağlayıcılar, internet toplu kullanım sağlayıcılarının yükümlülükleri konusunda ayrıntılı bilgi için, bkz. Yasemin Durnagöl, "5651 Sayılı Kanun Kapsamında İnternet Aktörlerine Getirilen Yükümlülükler İle İdari Ve Cezai Yaptırımlar," *Türkiye Adalet Akademisi Dergisi* 2, no. 4 (2011): 382*ff*.

[24] "Oluşa ve tüm dosya kapsamına göre, katılanın mail adresine girildiği tespit edilen IP numarası adına kayıtlı olan sanığın internet kafe işlettiğini ve tüm bilgisayarların aynı IP'ye bağlı olduğunu beyan etmesi üzerine beraat kararı verilmiş ise de, IP numarasının internet kafeye ait olup olmadığı hususu ve bilgisayarlara ait LOG kaydı bulunup bulunmadığı araştırılmadan eksik inceleme ile yazılı şekilde beraat kararı verilmesi" Yar. 8. CD, E.2013/2357, K.2014/7186, 20.03.2014, (UYAP).

[25] Gerçekten de kablosuz modem belli bir abone adına kayıtlı IP adresi üzerinden hizmet vermektedir. Eğer modem şifrelenmemiş veya uygulamadaki tabiriyle şifresi kırılmışsa, sinyalinin ulaştığı her yerden internete bağlanmak mümkün hale gelmektedir. Aynı yönde, bkz. Değirmenci, *Sayısal (Dijital) Delil*, 406.

lenmesi yoluna gidilmesi gerekmektedir.[26] Bilişim sisteminde yer alan verinin, işlendiği iddia edilen suçun delili olup olmadığı, delil niteliğinde ise doğru ve inanılır olup olmadığı hususlarında teknik bilgiye ihtiyaç duyulabilecektir. Bu şekilde çözümü uzmanlık ve teknik bilgi gerektiren durumlarda delillerin değerlendirilmesine imkan sağlamak bakımından bilirkişiden istifade edilecektir.[27]

---

[26] "Sanığın suçlamayı kabul etmeyerek, kablosuz modem kullanıldığından hattının başkaları tarafından girilip kullanılmış olabileceğine ilişkin savunması karşısında; bildirilen IP numaralarının bağlı bulunduğu internet hattında ne özellikte modem kullanıldığı, kablolu veya kablosuz olup olmadığı, şifreli olup olmadığı, modemden başka kullanıcıların internete bağlanılıp bağlanılmadığının belirlenmesi açısından ilgili internet sağlayıcısından bilgi istenmesi ve sanığa ait bilgisayar getirtilip uzman bilirkişi tarafından LOG kayıtları incelenerek sonucuna göre" Yar. 8. CD, E.2016/12634, K.2017/4967, 03.05.2017, (UYAP).

"…bir e-postanın kimden geldiğinin tespiti için de, ilk olarak e-postayı gönderen IP adresinin bulunması, daha sonra da bulunan IP adresinin belirtilen tarih ve saatte hangi abone tarafından kullanıldığının ve o abonenin kimlik ve açık adres bilgilerinin talep edilmesi, bulunan IP adresini kullanan abonenin sanıkla bağlantısının araştırılarak tespiti gerekir." Yar. 11. CD, E.2008/16570, K.2009/101, 28.01.2009, (UYAP).

"Sanığın, bahse konu elektronik posta adresi ile sahte facebook hesabının sahibi ve kullanıcısı olmadığını, kablosuz ağ üzerinden internet hizmeti aldığı ve kablosuz modemine şifre koymadığından üçüncü kişilerin hattına giriş yapıp, kendisinden habersiz iddiaya konu eylemleri gerçekleştirmiş olabileceğini ifade etmesi, sanığın savunmasını doğrular mahiyette, sanığa ait bilgisayar ve modem üzerinde yapılan teknik inceleme sonucu hazırlanan 21.03.2012 tarihli bilirkişi raporunda, ..." Yar. 12. CD, E.2013/20187, K.2014/11414, 12.05.2014, (UYAP).

[27] Değirmenci, *Sayısal (Dijital) Delil*, 402. "23.10.2008 tarihli bilirkişi raporunda, sanık B.Yalçın'ın bilgisayarına bağlı modem hattının kablosuz olması durumunda modemin markasına göre değişmekle beraber 500 metre alan içerisinde herhangi bir şahsın bilgisayarı ile 88.229.208.155 IP numarasından suç konusu paranın havale edilmiş olabileceği belirtildiğinden; bilgisayar ve internet kullanmayı bilmediğini, bilgisayarın sadece çocuklarının dersleri için kullanıldığını savunan sanık B. Yalçın'ın bilgisayarının, modemin ve dosyanın bütünüyle bilişim suçlarından anlayan tercihen bilgisayar mühendisi bir bilirkişiye tevdi edilerek adı geçen sanığın bilgisayarına bağlı modemin türünün tespit edilmesi, modem hattının kablosuz olması durumunda hattın güvenliği için gerekli önlemlerin alınıp alınmadığı, sanığın internet bağlantısına dışarıdan girilip girilemeyeceği, IP numarasının değiştirilmesinin mümkün olup olmadığı, sanığın bilgisayarına virüs gönderilerek bilgilerinin alınıp alınmadığı konularında rapor düzenlettirilmesi, gerekirken bu hususlar araştırılmadan eksik soruşturma ile hüküm kurulması" Yar. 13. CD, E.2012/3887, K.2013/15354, 21.05.2013, (UYAP).

Dijital birçok veri gibi (ister statik atanmış olsun ister dinamik olsun) IP adreslerinin de çeşitli yöntemlerle (örneğin Proxy vasıtasıyla gerçeği gizlenerek veya başka kullanıcıya ait IP numarası kopyalanarak) değiştirilebilmesi mümkün[28] olup bu tür durumlarda faile ulaşmak da o kadar güçtür. Diğer yandan IP adresi, teknik açıdan çoğu zaman doğrudan bir bilgisayarı veya bir kişiyi göstermekten ziyade, yalnızca bir internet aboneliğini gösterebilir.[29] Abonelik ise bir kişiyle sınırlandırılamayacak olup, internete bağlanma hakkı olan hesaba erişimi olan herkesi işaret etmektedir.[30] Bu nedenle yukarıda izah edilen kolaycı bir yaklaşımın yerine tespit edilen IP'nin diğer teknik verilerle, söz gelimi kişiye ait bilgisayar, cep telefonu gibi elektronik cihazların adli içerik incelemesi ile MAC adresinin tespitiyle desteklenmesi gerekir[31] ki, sanığın suçu işlediğine dair

---

[28] Dijital verilerin en önemli özelliklerinden biri de kolaylıkla değiştirilebilir, bozulabilir ve yok edilebilir olmalarıdır. Bu konuda, bkz. Değirmenci, *Sayısal (Dijital) Delil*, 132*ff*., 405**.** Nitekim Gülsel Öykü Özç**e**lik: "TCP yönlendirmesi, "proxy" sunucular, paket yönlendirmeleri, web ve e-posta isimleri, IP adresi ve e-posta adresi ele geçirme, oturum engelleme, DNS yanıltma gibi uygulamalar söz konusu delile şüpheden arındırılmış bir delil olarak yaklaşılmasını imkansız kılar." "IP Adresleri Tek Başına Delil Olabilir Mi? IP Adreslerine Yargılamada Ne Kadar Güvenilir?," TAG Hukuk Bürosu, erişim tarihi Ekim 1, 2018, taghukuk.com/wp-content/uploads/2018/04/ip_adreslerinin_delil_niteliği.pdf.

[29] "…IP numarasının kullanılan bilgisayarı göstermeyip internetle olan bağlantıyı göstermesi.., kesin delil bulunmadan varsayımlarla hüküm kurulamayacağı cihetle tebliğnamedeki bozma düşüncesine katılınmamıştır" Yar. 8. CD, E.2012/21817, K.2013/25428, 24.10.2013, (UYAP).

[30] Özçelik**, "**IP Adresleri."

[31] "Maddi gerçeğin ortaya çıkarılması açısından, suç tarihinde sanığın ve katılanın kullandığı facebook hesaplarına girmeye elverişli bilgisayar, telefon, tablet vb. cihazların neler olduğunun ve halen taraflarda olup olmadığının tespitine çalışılması, tespiti halinde bu cihazlardan, aksi durumda halen kullandıkları cihazlardan "Ümmüye Şoleum" isim ve soyismiyle açılan facebook adresinin ve tespit edildiği takdirde buna bağlı mail adresinin kullanılıp kullanılmadığı, kullanıldığı tespit edildiği takdirde hangi tarihler arasında girildiği, ayrıca soruşturma aşamasında dosyaya sunulan facebook çıktısı örnekleri esas alınmak suretiyle, internet servis sağlayıcısı ve IP adresinin tespit edilip edilemeyeceği hususunda, bilişim alanında uzman bilirkişilerden rapor aldırılması ayrıca sözkonusu hesabın üzerindeki bilgilerden yola çıkarak açık kaynak araştırması yapılmak suretiyle ve sonucuna göre sanığın hukuki durumunun belirlenmesi" Yar. 4. CD, E.2014/32543, K.2018/21151, 05.12.2018, (UYAP).

şüphe ortadan kalksın ve bu yönde hüküm kurulabilsin.[32] Gerçekten de suçun kesin şekilde ispatlanabilmesi için adreste arama yapılması; bilgisayar veya bilgisayar özelliği taşıyan tablet, akıllı telefon ve hatta smart tv gibi cihazlar tespit edilip, CMK'nın 134. maddesi gereğince bu cihazlarda içerik araması yapılması gerekebilir. Bununla birlikte CMK'nın 134. maddesine göre arama yapılırken suç ile uygulanacak tedbir arasındaki dengenin de gözetilmesi[33] ve elbette ki CMK 134.maddede düzenlenen koruma tedbirinin koşullarının da gerçekleşmesi gerekmektedir.[34] Zaten, cihazlar formatlanmışsa veya özel programlar kullanılarak içerik silinmişse aranılan içeriğe ulaşma şansı da azalmaktadır.[35]

---

[32] Özçelik, "IP Adresleri."

[33] "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma 5271 Sayılı CMK'nın 134. maddesinde düzenlenmiş olup, CMK'nın 116 ve 123. maddeleri arasında yer alan arama koruma tedbirinin özel bir görünümünü oluşturmaktadır. CD, DVD, flash bellek, disket, harici ve dahili harddisk, bilgisayar özelliği içeren noktaları bakımından akıllı telefon ve benzerlerinden elde edilen ve tamamı "dijital delil" olarak adlandırılan, suistimale müsait olan verilerin; sıhhatini ve güvenliğini sağlamak amacıyla ve bireyin özel hayatına, kişisel verilerine yönelik olumsuz tesirleri göz önünde tutularak "son çare" olarak başvurulabilecek "özel koşullara bağlı" bir koruma tedbiri olması nedeniyle, genel adli aramadan ayrıksı ve istisnai olarak, ayrıntılı düzenlenmiş olup, bu hallerde arama kararının yalnızca hakim tarafından verilebileceği öngörülmüştür" Yar. 16. CD, E.2015/2056, K.2017/5023, 21.09.2017, (UYAP).

[34] "Ceza muhakemesi hukukunda, elektronik delillerin toplanması, bir başka deyişle bilgisayarlarda yapılacak delil araştırması Ceza Muhakemesi Kanunu'nun 134. maddesinde düzenlenmiştir… Şu unutulmamalıdır ki, delil araştırmasının bu aşamasında CMK tarafından öngörülen usule eksiksiz bir biçimde uyulması delillerin hukuki olması ve ceza yargılamasında verilecek hükme esas teşkil edebilmesi açısından son derece önemlidir" Özocak, "Sosyal Medyada İşlenen."

"…CMK'nın 134. maddesi uyarınca bilgisayar ve bilgisayar kütükleri üzerinde arama yapılmasına dair hakim tarafından verilmiş bir karar bulunmadığı cihetle, arama sonucu 2 adet harddiskte bulanan 471 adet filmin hukuka aykırı şekilde elde edilmiş delil niteliğinde olması sebebiyle hükme esas alınamayacağı ve atılı suçlamayı kabul etmeyen sanık hakkında hukuka aykırı şeklinde elde edilmiş bu delil dışında mahkumiyetine yeterli başkaca bir delil de bulunmadığı gözetilmeden, beraati yerine yazılı şekilde mahkumiyetine karar verilmesi" Yar. 19. CD, E.2015/11396, K.2016/1087, 02.02.2016, (UYAP).

[35] Dülger ve Modoğlu, *Soruşturma ve Kovuşturma*, 162.

Yukarıdaki açıklamalar ışığında sonuca bağlayacak olursak; IP adresi (numarası), adres sahibi tarafından suçun işlendiğini doğrudan göstermez.[36] Bu nedenle IP adresi soruşturma için bir sonuç değil, ancak başlangıç noktası olarak kabul edilebilir.[37] IP numarası kullanılarak tespit edilen adreste sadece internet abonesi yaşasa dahi o kişi ikrarda bulunmadıkça veya diğer delillerle desteklenmedikçe, sadece IP numarası esas alınarak o kişi hakkında mahkumiyet hükmü verilmesi doğru değildir.[38] Dolayısıyla IP adresi, tek başına mahkûmiyeti gerektiren bir delil niteliği taşımayacak**,** ancak ikrar veya başkaca destekleyici deliller de varsa mahkumiyet kararı verilebilecektir. Yargıtay'ın yaklaşımı da bu yöndedir.[39]

---

[36] Değirmenci, *Sayısal (Dijital) Delil*, 108, 405.

[37] Dülger, *İnternet İletişim*, 695-696.

[38] Aynı yönde, bkz. Doğan, *Kuşkudan Sanık*, 295.

[39] "Sanık S. Kaya'nın tüm aşamalarda atılı suçu işlemediğini savunduğu, katılan şirketin hesabından alındığı belirtilen paranın sanık tarafından alındığına veya sanığın hesabına aktarıldığına ilişkin maddi delil ve tanık beyanı bulunmadığı ve sanık S. Kaya'nın katılan tarafa ait paranın çekilmesi için şifre bilgilerinin gönderildiği telefon hattını kullandığı iddia olunan diğer sanık S. Adgu'yu da tanımadığı ve yakınana ait internet bankacılığı hesabına girilmek suretiyle paranın başka hesaplara aktarılmasında kullanılan bilgisayarın sanık S. Kaya'nın internet cafe olarak kullandığı işyerindeki bilgisayar olmasının tek başına sanığın atılı suçu işlediğini ispata yetmeyeceği gözetildiğinde; sanığın atılı hırsızlık suçunu işlediğine dair delillerin nelerden ibaret olduğu karar yerinde denetime olanak sağlayacak şekilde açıklanmadan, " …söz konusu IP numarasının kullanıldığı bilgisayarın sanık S. Kayanın işletmekte olduğu internet cafede kullanıldığı…" şeklindeki yetersiz gerekçeyle sanık Sinan Kaya'nın atılı suçtan mahkûmiyetine karar verilmesi, yasaya aykırıdır" Yar. 12. CD, E.2012/18065, K.2012/45207, 06.11.2012, (UYAP).

"Dosya kapsamına göre; sanığın, bir süre duygusal boyutta arkadaşlık ilişkisi içerisinde olduğu şikayetçinin müstehcen fotoğraflarını, onun bilgisi dışında, bir sosyal paylaşım sitesine koyduğu iddiasına konu olayda, şikayetçinin beyanında geçen sosyal paylaşım sitesine onun adına üyelik işlemlerinin yapıldığı bilgisayarın internet servis sağlayıcısı ve internet servis sağlayıcısı tarafından verilen IP adresinin tespit edilmesi, tespit edilen IP adresinin belirtilen tarih ve saatte hangi abone tarafından kullanıldığının ve o abonenin kimlik ve açık adres bilgilerinin belirlenmesi, IP adresini kullanan abonenin sanıkla bağlantısı araştırılıp, gerektiğinde sanığın iş yerinde ve evinde kullandığı bilgisayarlar üzerinde bilişim uzmanı üç kişilik bilirkişi marifetiyle inceleme yapılarak, söz konusu üye

profilinin, sanığın kullanımında olan bilgisayar aracılığıyla oluşturulup oluşturulmadığı hususunun belirlenmesi; şikayetçinin 31.08.2009 tarihli şikayet dilekçesi de göz önüne alınarak, iddia olunan suç tarihinde şikayetçi ve sanığın abonesi olduğu telefon hatları araştırılıp, bu tarihten önceki ve sonraki altı aylık görüşme detaylarını gösterir HTS raporları istenilerek, toplanan tüm deliller birlikte değerlendirilerek, iddia ve savunmanın doğruluk derecesi açıklığa kavuşturulduktan sonra sanığın hukuki durumunun takdir ve tayini gerekirken, eksik incelemeye dayalı olarak, sanığın beraatine karar verilmesi", Yar. 12. CD, E.2013/7154, K.2013/16476, 17.06.2013, (UYAP).

"10/10/2008 tarihli ve 03/11/2008 tarihli alınan bilirkişi raporlarına göre; olay tarihinde müştekinin hesabından internet yoluyla yapılan para havalesinin bir kısmının Taksim şubesindeki hesaptan çekilmesi sırasında alınan kamera kayıtlarının incelenmesinde; 2 kişinin bankamatikten para çektiğinin tespit edildiği, bu iki kişi ile sanıkların fotoğraflarının bilirkişice incelenmesinde aynı şahıslar olmadığının belirlendiği, ancak mahkemece sanıklar lehine olan bu delillerin kararın gerekçesine dayanak kabul edilerek çelişkiye neden olunduğu, 10.10.2008 tarihli bilirkişi raporunda, sanık Şükrü Ünal'ın bilgisayarına bağlı modem hattının kablosuz olması durumunda modemin markasına göre değişmekle beraber herhangi bir şahsın bilgisayarı ile 85.97.170.132 IP numarasından suç konusu paranın havale edilmiş olabileceği belirtildiğinden; sanık Ş. Ü'ın bilgisayarının, modemin ve dosyanın bütünüyle bilişim suçlarından anlayan tercihen bilgisayar mühendisi bir bilirkişiye tevdi edilerek adı geçen sanığın bilgisayarına bağlı modemin türünün tespit edilmesi, modem hattının kablosuz olması durumunda hattın güvenliği için gerekli önlemlerin alınıp alınmadığı, sanığın internet bağlantısına dışarıdan girilip girilemeyeceği, IP numarasının değiştirilmesinin mümkün olup olmadığı, sanığın bilgisayarına virüs gönderilerek bilgilerinin alınıp alınmadığı konularında rapor düzenlettirilmesi gerekirken bu hususlar araştırılmadan eksik soruşturma ile hüküm kurulması" Yar. 13. CD, E.2012/6530, K.2013/16693, 30.05.2013, (UYAP).

"4-Suça konu havale işleminin yapıldığı IP nosunun Türk Telekom ve diğer internet servis sağlayıcılarından araştırılıp işlemin yapıldığı yer ve bilgisayarın tespiti cihetine gidilmesi, işlemi yapan bilgisayar ve telefon hattı sahibinin tespiti durumunda olay ile ilgili bilgi ve görgüsüne başvurulması, 5-Sanığa ait olan ve ayrıca suça konu işlemin yapıldığı tespit edilecek olan modemlerin, bilgisayar kasalarının ve yukarıda belirtilen hususlarıda içeren dosyanın bütünüyle bilişim suçlarından anlayan tercihen bilgisayarlar mühendisi bir bilirkişiye tevdi edilerek bilgisayarlara bağlı modem türlerinin tespit edilmesi, modem hatlarının kablosuz olması durumunda hattın güvenliği için gerekli önlemlerin alınıp alınmadığı, internet bağlantısına dışarıdan girilip girilemeyeceği, IP numarasının değiştirilmesinin mümkün olup olmadığı, bilgisayarlara virüs gönderilerek bilgilerinin alınıp alınmadığı suça konu işlemin ne şekilde nereden yapıldığı konularında rapor düzenlettirilmesi, sonucuna göre tüm deliller çervesinde sa-

III. EKRAN GÖRÜNTELERİ ÇIKTILARININ İSPAT DEĞERİ

A. Ekran Görüntü Çıktısı Kavramı

Ekran görüntüsü, görüntü sergileme aracı olan monitör/ekran vasıtasıyla bireylere ulaşan ışık demeti yansımasıdır. Ekrandaki bu görüntünün siber ortamda sayısal olarak anlık birebir nüshasının alınması işlemine ise "ekran görüntüsü almak/yakalamak" (=printscreen, screenshot) denmektedir. Başta bilgisayar olmak üzere bir çok elektronik cihaz (örneğin akıllı telefonlar) bir ekrana sahiptir. Bu ekrana yansıyan görüntü ve siber ortamdaki veri karşılığı aslında başlı başına bir çıktıdır (=output). Bu nedenle ekran görüntüsü çıktılarını ikiye ayırarak incelemek gerekir.[40]

Bunlardan ilki, ekran görüntüsü sayısal çıktılarıdır. Işık demeti yansımasıyla oluşan ve ekrana yansıyan anlık görüntülere "ekran görüntüsü dijital/sayısal çıktısı" adı verilmektedir. Herhangi bir işleme tabi tutulmayan bir bilgisayarda masaüstü görüntüsü bile aslında arka planda çalışan programlar nedeniyle ve hâlihazırda bir görüntüyü yansıttığı için "çıktı" sayılmaktadır. Ekran görüntüsü dijital/sayısal çıktıları geçici olduklarından ve o an itibariyle ekran görüntüsünün videoya kaydedilmesi veya ekran görüntüsünün ya-

nığın hukuksal durumunun değerlendirilmesi gerekirken, bu konularda kovuşturma genişletilmeden sanığın eksik kovuşturmayla cezalandırılmasına karar verilmesi" Yar. 13. CD, E.2012/1947, K.2013/18603, 06.06.2013, (UYAP).

"Sanığın, katılanın kredi kartı bilgilerini ele geçirerek internet üzerinden alışveriş yaptığının iddia olunması karşısında; gerçeğin kuşkuya yer bırakmayacak şekilde belirlenebilmesi bakımından, olaya konu kredi kartı kullanılarak yapılan siparişlerin verildiği bilgisayar veya bilgisayarlara ait IP numaraları üzerinden, siparişin verildiği adresin ve burada oturan kişinin araştırılması, alışveriş yapılan işyerlerinden siparişlerin kim ya da kimler tarafından yapıldığının, mal veya hizmetin kime ve nereye sağlandığının sorulması, alışverişe ilişkin faturaların işyerlerinden temin edilmesi sonrasında tüm deliller birlikte değerlendirilip sonucuna göre sanığın hukuki durumunun tayin ve takdiri gerekirken eksik incelemeyle yazılı şekilde karar verilmesi" Yar. 11. CD, E.2012/1017, K.2013/8345, 21.05.2013, (UYAP).

[40] Halid Özkan, "Ceza Muhakemesinde Ekran Görüntüsü Çıktılarının Delil Niteliği," iç. *Ceza Muhakemesi Hukukunda Delil ve İspat*, ed. Yener Ünver (Ankara: Seçkin Yayıncılık, 2014), 270-271.

kalaması yapılamadığı sürece tekrar edilebilir nitelikte değiller. Bu nedenle de ceza muhakemesinde ispat aracı olmak için zayıftırlar. Nitekim Amerikan Federal Mahkemesi de "web sitesi ekran görüntülerine" şüphe ile yaklaşılması gerektiğini söylemektedir.[41]

Bir diğer ekran görüntüsü çıktı türü ise "ekran görüntüsü fiziki/yazıcı çıktıları"dır. Bunlar, ekrandaki görüntünün yakalanması ve fotoğrafının çekilmesi sonrasında bir yazıcı yardımıyla görüntünün kağıt vb. materyal üzerine yazdırılmasıdır. Bazen bu çıktı bir web sitesinin o andaki görüntüsü olabilmektedir. Bir web tarayıcısı açıkken doğrudan fiziki çıktı alınması halinde URL linki ve çıktı tarihi, fiziki çıktı üzerinde yazmaktadır. Fakat bu bilgilerin fiziki çıktı üzerinde yer alması yeterli değildir; ek deliller ile URL linkinin ve URL linkine bağlı adreste bulunan görüntünün doğrulanması gerekmektedir.[42]

B. Ekran Görüntü Çıktısının İspat Değeri

Uygulamada, başta hakaret, tehdit, şantaj veya özel yaşamın ihlali suçları olmak üzere çok sayıda suç son yıllarda yoğun bir şekilde Facebook, Youtube, Twitter gibi sosyal paylaşım siteleri üzerinden veya WhatsApp, Messenger gibi mesajlaşma/konuşma uygulamaları veyahut elektronik postalar aracılığıyla işlenmekte,[43] suçun mağduru da şikayet dilekçesine genellikle buna dair (örneğin Facebooktaki hesabın ekran görüntüsünü içeren) bir çıktıyı eklemekte, bu çıktı esas alınarak hesap sahibi görünen kişi şüpheli olarak soruşturmaya dahil edilmekte, hakkında dava açılabilmektedir.[44]

---

41 Özkan, "Ekran Görüntüsü," 271.

42 Özkan, "Ekran Görüntüsü," 271.

43 Sosyal medya aracılığı ile işlenen bilişim suçları, örnek dava ve kararlar için, bkz. Çubukçu ve Atiker, "Sosyal Medya ve Bilişim Suçları," 3*ff*.

44 "… soruşturma aşamasında dosyaya sunulan facebook çıktısı örnekleri esas alınmak suretiyle, internet servis sağlayıcısı ve IP adresinin tespit edilip edilemeyeceği hususunda, bilişim alanında uzman bilirkişilerden rapor aldırılması ayrıca sözkonusu hesabın üzerindeki bilgilerden yola çıkarak açık kaynak araştırması yapılmak suretiyle ve sonucuna göre sanığın hukuki durumunun belirlenmesinin gerektiği" Yar. 4. CD, E. 2014/44927, K. 2019/2543, 20.02.2019, (UYAP).

Dijital deliller, parmak izi veya DNA delili gibi çoğu kez ilk bakışta fark edilemeyen, gizli ve görünmeyen bir yapıya sahiptir. Bu nedenle dijital delillerin bazı araçlar veya yöntemlerle somut, yani insanların duyu organlarıyla algılayabilecekleri, bir hale getirilmelerine ihtiyaç olacaktır. Donanım ve yazılımdan oluşan bu vasıtalar sayesinde elektronik ortamda yer alan bilgiler bilgisayar çıktısı ya da ekran çıktısı şeklinde beş duyu organımızla algılanabilecek niteliğe kavuşmakta ve muhakeme makamı tarafından temas edilebilir hale gelmektedir.[45] Ancak belirtmemiz gerekir ki, dijital delillerde delil niteliğinde olan ekrandan veya yazıcıdan alınabilen çıktı değil, bizzat dijital ortamdaki verinin kendisidir.[46]

Dijital verilerin kendilerine özgü özellikleri ve kolay zarar görebilen, değiştirilebilen ve yok edilebilen yapıları sebebiyle doğrulanmaları son derece önemlidir. Ancak *dijital delillerin doğrulanması*[47] konusu, dijital delillere ilişkin en tartışmalı konulardan birini oluşturmaktadır. Dijital delillerin doğrulanması, delillin iddia edilen "şey" olup olmadığını ispat etmektir. Dijital delillerin doğrulanamaması halinde delillin hukuka uygunluğu şüpheye düşebilecektir. Özellikle son yıllarda dijital delillere dayanarak sürdürülmekte olan birçok ceza yargılaması bulunmasına karşın hukukumuzda, diğer bazı hukuk sistemlerine kıyasla, dijital delillerin doğruluğunu tayin etmeye ilişkin geliştirilmiş bir kurallar bütünü bulunmamaktadır.[48]

Amerikan hukukunda genel olarak dijital deliller, özel olarak da ekran çıktılarının delil niteliğini haiz olduğunu söyleyebilmek için hem "*kabul edilebilir"* hem de "*doğrulanabilir"* olması aranmaktadır. Çünkü

---

[45] Gökşen, "Dijital Verilerin Delil Değeri," 57, 62; Uğur Kaynakçıoğlu, "Ceza Muhakemesinde Dijital Deliller" (yayımlanmamış yüksek lisans tezi, Galatasaray Üniversitesi, 2015), 38-39; Şenel Sarsıkoğlu, "Ceza Muhakemesinde Delil Ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı," *Türkiye Adalet Akademisi Dergisi*, no. 22 (Temmuz 2015): 520; Değirmenci, *Sayısal (Dijital) Delil*, 132; Özkan, "Ekran Görüntüsü," 268.

[46] Değirmenci, *Sayısal (Dijital) Delil*, 132; Sarsıkoğlu, "(E-Delil) Kavramı," 520.

[47] Dijital delillerin teknik olarak doğrulanması kavramı ve modelleri için, bkz. Yusuf Uzunay ve Mustafa Koçak, "Bilişim Suçları Kapsamında Dijital Deliller," Akademik Bilişim Konferansları http://ab.org.tr/ab05/ tammetin/134.pdf.

[48] Gökşen, "Dijital Verilerin Delil Değeri," 93-94.

ekran görüntüsü çıktıları orjinalinden türetilen delil (türev) niteliğinde olup, mutlak şekilde doğrulanması ve kabul edilebilirliğinin ispatlanması gerekmektedir. Daha doğrusu delilin kabul edilebilir olması için doğrulanabilir olması, doğrulanabilirlik için de; 1) ekranda o an için aslında ne vardı? 2) ekran görüntüsünü doğrulayan doğrudan bir delil veya tanık ifadesi var mı? 3) ekran görüntüsü internet ortamında ise web site sahibi/ içerik, yer, servis veya erişim sağlayıcısı tarafından o andaki görüntü doğrulanıyor mu?, şeklinde kıstaslara ve duruma göre ek kıstaslara başvurulmaktadır. Diğer taraftan ekran görüntüsü sayısal veya fiziki değerlendirilmesi uzman kişilerce yapılmaktadır. Böylelikle dava daha jüri önüne gelmeden önce dijital delilin bilimselliği ve akılcılığı kısmen de olsa değerlendirilmiş olur. Şayet dava jüri önüne taşınırsa, ekran görüntüsü hakkında çalışmış olan taraf bilirkişi ya da mahkeme tarafından atanan bilirkişi mahkemede dinlenir, çapraz sorguya tabi tutulur.[49]

Öğretide *Gökşen'e* göre, dijital verilerin delil olarak değerlendirilmesi için içlerinde bulundukları dijital sistemin bütün olarak incelenmesi ve dijital delillerin değiştirilmesinin görece kolay olması sebebiyle mutlaka uzmanlar tarafından doğrulanması gerekmektedir. Dijital delillerin adli bilişim prosedürüne aykırı olarak incelenmesi ve bu belgelerin doğrulanamaması halinde hükme esas alınmaması gerekir.

Özkan ise, dijital verilerin sadece dijital ortamdaki şekillerinin orijinal delil kabul edilmesi ve ekran görüntüsü çıktıları doğrulanması mümkün olan "suret" olarak kabul edilmesi gerektiği görüşündedir. Yazara göre, en nihayetinde başka delillerle desteklenmediği müddetçe ekran görüntüsü çıktıları "delil başlangıcı/ dolaylı delil" kabul edilmelidir. Çünkü siber ortamdaki dijital delillerin bir yazıcı ile yazılı belge haline dönüştürülmesi, bu çıktıları doğrudan delil niteliğinde "belge" haline dönüştürmeyecektir. Ekran görüntüsü çıktıları manipülasyona açıktır ve %100 güvenilir değildir. Bu nedenle ekran görüntüsü dijital/ fiziki çıktıları, başka delillerle desteklenmediği ve dijital doğrulama yapılmadığı müddetçe, tek başına

[49] Özkan, "Ekran Görüntüsü," 273*ff*.

hükme esas alınmamalıdır. Bu çıktıların delil kabul edilebilmesi için hem doğrulanabilir hem de kabul edilebilir olması gerekir.[50]

*Sarsıkoğlu'*na göre ise dijital delillerin hukuka uygun olarak elde edildiği ve içeriklerinin de gerçeği yansıttığı dolayısıyla taklit ve tahrif edilmediği kesin olarak muhakeme makamları tarafından anlaşıldıktan sonra tek başına delil olarak kullanılmaları ve hükme esas alınmalarında bir sakınca bulunmamaktadır.[51]

Uygulamamızda ise, ekran görüntüsünün sayısal çıktısından ziyade fiziki çıktılarının sıklıkla soruşturma veya dava dosyasına dahil edildiğini görmekteyiz. Sunulan bu çıktılar üzerinden soruşturmaya yön verilmekte; ikrar, tanık ve olayın gelişimi gibi tüm delillerin değerlendirilmesi sonucunda ve diğer delillerle birlikte hükme esas alınabilmektedir.

Ekran görüntülerinin delil niteliği ve ispat değeri konusunda, konuyu açık bir şekilde tartışarak sonuca varan Yargıtay içtihadına rastlamadık. Bununla birlikte, örneğin Antalya 10. Asliye Ceza Mahkemesi, yargılamasını yaptığı bir davanın gerekçeli kararında, "Katılan son duruşmadan önce dosyaya sunduğu yazılı beyanları ve ekindeki facebook sayfasından çıkmakla bastırılmış bulunan fotoğraf, yakınan ve sanığın facebook sosyal paylaşım sitelerinde yer alan çıktılarla ilgili belgeler dosyada bulunmaktadır" diyerek *çıktıları* da deliller içerisinde saymış ve tehdit ile özel yaşamın ihlali suçundan sanığın mahkumiyetine karar vermiştir.[52] Bu kararın temyizi üzerine Yargıtay 12. Ceza Dairesi de "Dosya içeriği, sanığın ikrar içeren savunmaları, katılanın tutarlı beyanları, tanık anlatımları ve mesaj tespit tutanağına göre; ev arkadaşı ve aynı okulda öğrenci olan sanık ile mağdurun, aralarındaki anlaşmazlık nedeniyle evlerini ayırdıkları, olayın akabinde, sanığın, makyajsız hali ile uyurken çekilen fotoğrafının, mağdur tarafından internetteki facebook profil hesabında yayımlanarak, fotoğrafa olumsuz yorumlar yapılması üzerine sanığın, bu olayın meydana getirdiği haksız tahrik altında, mağdurun,

---

50 Özkan, "Ekran Görüntüsü," 272, 282.

51 Sarsıkoğlu, "(E-Delil) Kavramı," 520.

52 Antalya 10. Asliye Ceza Mahkemesi, E.2013/130, K.2013/575, 24.10.2013, (UYAP).

evde erkek arkadaşı ile öpüştüğü sırada çekilen özel fotoğrafını facebook profil hesabında yayımladığı ve mağdura, iki gün ara ile cep telefonuna mesajlar çekerek "ağzını yüzünü şişirecem, celladın olucam, anan kapıları iyi kilitlesin bu sefer kezzap yiyecek, mezarını hazırlat" gibi sözlerle tehdit ettiği, atılı suçların bu şekilde sübut bulduğu" şeklindeki içtihadıyla, ikrar, tanık anlatımı gibi diğer delillerle desteklenmiş *çıktıların* da esas alındığı yerel mahkeme hükmünü onamıştır.[53]

Yine bir başka olayda, Facebook hesabı üzerinden gerçekleştirilen hakaret ve tehdit suçlarından açılan davada, adına olan hesabın sahte olduğunu beyan ederek suçlamayı kabul etmeyen sanık savunması ile "facebook.com" adli hizmet sağlayıcı kuruluşun Türkiye temsilciliğinin bulunmaması ve Facebook'ta işlem yapan bilgisayarların IP adreslerini hizmet sağlayıcı kuruluş tarafından doğrulanmıyor olması gerekçeleri verilen beraat kararının istinaf edilmesi üzerine Gaziantep BAM 9. Ceza Dairesi, "yorum yapılan facebook sosyal paylaşım sitesinin sayfa çıktılarının dosya içerisinde mevcut olduğu ve paylaşım altında sanık adına olan hesap üzerinden yazılan hakaret ve tehdit içerikli yorumun bulunduğu, yorum içeriğinin hakaret ve sair bir kötülük yapacağına dair tehdit suçlarını oluşturacak nitelikte olduğu, sanığın kendisine ait tek bir hesabın olduğu ve yorum yapılan hesabın kendisine ait olmayıp adına sahte olarak açılmış bir hesap olduğunu ileri sürdüğü, ancak sanığın kendisine ait olmadığını ileri sürdüğü hesaptaki profil fotoğrafının yeğenine ait fotoğraf olduğunu kabul ettiği, yine bu hesap üzerinden yapılan bir paylaşımda görülmekte olan aracın da kendisine ait araç olduğunu ve bu paylaşımın altına yorum ekleyen kişilerin de kendi arkadaşları olduğunu, ancak kendisinin ne yeğeninin fotoğrafını ne de aracına ait fotoğraf paylaşımı yapmadığını ileri sürdüğü, sanığın bu paylaşımlarına ilişkin fotoğrafların özelinde kendisine ait ve sadece kendisinin paylaşıma atabileceği türden fotoğraflar olduğu, bu fotoğrafları kendisi dışında birilerinin haksız yere elde ederek adına açılan hesapta profil resmi olarak ya da paylaşım olarak kullanılmış olmasının hayatın olağan akışına uygun olmadığı, kaldı ki araç fo-

[53] Yar. 12. CD, E.2014/10722, K.2014/25542, 15.12.2014, (UYAP).

toğrafına ilişkin paylaşım altında sanığın arkadaşlarının yorumlarının bulunduğu, bir başkasının sırf suç teşkil edecek yorumlarda bulunmak üzere sanığın sosyal medya hesabını ele geçirmiş olduğu iddiasının da tek başına inandırıcı olmadığı, sanığın, sosyal medya hesabının birileri tarafından ele geçirildiğine ve kendisine ait bilgilerin bu hesap üzerinden izinsiz olarak paylaşıldığına yönelik bir başvuruda bulunduğunu da ileri sürmediği, bu hali ile sanığın bu hesabın kendisine ait olmadığına yönelik savunmasının soyut nitelikte ve kendisini suçtan kurtarmaya yönelik bir savunma olduğu ve itibar edilecek nitelikte bulunmadığı" gerekçesiyle sanığın cezalandırılmasına karar vermiştir.[54]

Ceza Dairelerinden farklı olarak Yargıtay Hukuk Dairelerinin, konuyu daha açık bir şekilde tartıştıklarına ve ekran görüntüsü çıktılarının ispat değerine ilişkin ölçütler geliştirdiklerini görmekteyiz. Nitekim Yargıtay 2. Hukuk Dairesi, davacı tarafından dosyaya sunulan elektronik ortamdan elde edilen resimler ve elektronik ortamda (sosyal paylaşım sitesi kullanılarak) yapılan görüşmelere ilişkin çıktılar esas alınmak suretiyle kocanın güven sarsıcı davranışlarda bulunduğu kabul edilerek boşanma kararı verilen bir davaya ilişkin "Elektronik ortamdaki fotoğraf, film, görüntü veya ses kaydı gibi veriler ve bunlara benzer bilgi taşıyıcılar, diğer delillerle desteklendikleri takdirde "delil" olarak hükme esas alınabilir. Bu veriler tek başına vakıaların ispatına yeterli değildir. Hükme esas alınan elektronik ortamdan elde edilen görüntülerdeki şahısların kocanın yakınları olduğu anlaşılmaktadır. "Facebook" isimli sosyal paylaşım sitesi kullanılarak kocanın, dayısıyla görüşmelerine ilişkin iletişim kayıtlarının da; davacının, sosyal paylaşım sitesinde kendisini "kocanın dayısı" yerine koymak suretiyle "dayısı ile koca" yazışıyormuş görüntüsü verilerek davacı tarafından oluşturulduğu, davacının da bunu kabul ettiği anlaşılmaktadır. Bu halde, sosyal paylaşım sitesi üzerinden yapılan görüşme kayıtları da vakıaların ispatında dikkate alınamaz (HMK md. 189/2)" şeklinde ekran görüntü çıktılarının hükme esas alınma ölçütünü ortaya koymuştur.[55]

---

[54] Gaziantep BAM, E.2017/2691, K.2018/2260, 22.11.2018, (UYAP).

[55] Yar. 2. HD, E.2013/19577, K.2014/19269, 05.02.2014, (UYAP).

Benzer şekilde ilk derece mahkemesi kararında dayanak yapılan; davacı nafaka yükümlüsü tarafından (Facebook ve WhatsApp'tan alındığı iddia olunan) görüntü kayıtlarından ibaret olan delilinin hukuken geçerli ve hükme esas alınabilecek bir delil niteliğinde olup olmadığına ilişkin olarak Yargıtay 3. Hukuk Dairesi de; Anayasa, CMK ve 6100 sayılı HMK'nın ilgili hükümlerine değinerek hukuka aykırı (yaratılmış veya elde edilmiş) delillerin hiçbir şekilde ispat aracı olarak kullanılmayacağını[56] belirttikten sonra "Somut olayda, toplanan delillerin birlikte değerlendirilmesinden; nafaka alacaklısı olan davalının, tanık olarak dinlenen şarkıcıya ait şarkının klip çekimi sebebiyle ... isimli oyuncu ile birlikte yer aldığı çekim görüntülerinin, (klibin yayınlanmasından vazgeçilmesi üzerine) davacı nafaka yükümlüsü tarafından hukuka aykırı olarak elde edildiği sabittir. Diğer taraftan, hukuka aykırı olarak elde edilen klip görüntülerinin, paylaşımlarının yapıldığı sosyal medya hesaplarının kendisine ait olduğu hususu da davalı tarafından kabul edilmediği gibi, davacı taraf sosyal medya hesaplarının (Facebook/ WhatsApp) ve bu hesaplardaki paylaşımlarında davalı tarafından yapıldığı hususunu da ispatlayamamıştır. Ayrıca, sosyal medya hesaplarında yapılan paylaşımların, ancak hesabın sahibi veya aynı paylaşım ortamında (Facebook/ WhatsApp) bulunan kişilerce delil olarak kullanımının mümkün olduğu düşünülebilecektir. Diğer bir anlatımla, sahte profil oluşturup paylaşımlarda bulunmak veya kişi profillerinde hesap sahibinin bilgisi, muvafakatı ve izni olmaksızın yapılan

[56] Yargıtay Hukuk Genel Kurulu 2012 tarihli içtihadında: "Bir delilin mahkemece kabul edilebilmesi için, gerek öğretide yer alan ağırlıklı görüş, gerekse de Hukuk Genel Kurulu Kararlarında ortaya konulan ölçüt; o delilin usulsüz olarak yaratılmamış olması ve hukuka aykırı biçimde elde edilmemesidir. Vurgulanmalıdır ki, bir delilin usulsüz olarak elde edilmesi ayrı, usulsüz olarak yaratılması ayrı bir olaydır. Usulsüz olarak elde edilen bir delil somut olayın özelliğine göre değerlendirilebilirse de; usulsüz olarak yaratılan bir delilin hiçbir şekilde delil olarak kabulü olanaklı değildir" Yar. HGK, E.2011/2-703, K.2012/70, 15.02.2012, (UYAP). Bu şekilde Yargıtay Hukuk Genel Kurulu, usulsüz yaratılan delilin hiçbir şekilde kullanılmayacağını, buna karşılık usulsüz elde edilen delilin bazı durumlarda kullanılabileceğini belirtmiştir. Bize göre, Anayasa m. 38/6 karşısında, böyle bir ayrıma gidilmeksizin hiçbir şekilde hükme esas alınmaması gerekir.

paylaşımların delil olarak sunulması halinde, bunların 6100 Sayılı HMK'nun 189/2. maddesi kapsamında hukuka aykırı delil kabul edilmesi gerekir. Hal böyle olunca, mahkemece; davacı nafaka yükümlüsü tarafından sunulan delillerin bir bölümünün hukuka aykırı olarak elde edilmiş olduğu, diğer delillerin ise hukuka aykırı bir şekilde yaratılmış olduğu gözetilerek, dosya kapsamındaki diğer delillerle de ispat edilemeyen nafakanın kaldırılması davasının reddine karar verilmesi gerekirken, yanılgılı değerlendirme ile davanın kabulüne karar verilmiş olması usul ve yasaya aykırıdır", demiştir.[57]

Bu açıklamalardan sonra sayısal veya fiziki çıktıların ispat bakımından değeri için şunları söyleyebiliriz: Öncelikle bu tür çıktılara ihtiyatla yaklaşmak gerekmektedir; zira çıktının kendisi üzerinde ekleme, çıkarma şeklinde tahrifat yapmak mümkün olduğu gibi çıktının alındığı örneğin (A) adına olan hesabın da sahte olma veya var olan bir hesabın başkası tarafından ele geçirilme ihtimali bulunmaktadır. Nitekim uygulamada bir başkası adına ve hatta bir yerden fotoğrafını bulup kullanarak sosyal paylaşım sitelerinde hesap (profil) açmak[58] veya başkasının hesabını ele geçirip bu hesap üzerinden suç işlemek[59] sıklıkla görülen yöntemlerdir. Diğer taraf-

[57] Yar. 3. HD, E.2016/14742, K.2017/2577, 7.3.2017, (UYAP).

[58] Örneğin, bkz. "…facebook oturumunu açık bırakmasından faydalanan sanık S.., tanık E.. habersiz, onun arkadaş listesinde yer alan katılan S.. sayfasına girip, katılana ait 20 adet fotoğrafı, kendi elektronik posta hesabına gönderdikten sonra, aynı sitede, katılan adına ve onun bilgisi dışında oluşturduğu sahte profile, ele geçirdiği katılana ait fotoğrafları koymak suretiyle verileri hukuka aykırı olarak verme veya ele geçirme suçunu işlediği" Yar. 12. CD, E.2013/7765, K.2014/3758, 17.2.2014, (UYAP).

[59] Örneğin bkz. "…Oluşa, katılanın aşamalardaki anlatımlarına, sanığın da çalıştığı aile şirketine ait telefona bağlı internet hesabından katılana ait elektronik posta hesabına girildiğine ilişkin Microsoft şirketinden gelen yazı yanıtları ve kolluk araştırması sonuçlarına, katılanın 22.12.2010 tarihli dilekçesi ekinde ibraz ettiği fotoğraflara ve tüm dosya kapsamına göre; katılana ait elektronik posta ve facebook hesaplarının şifresini ele geçirerek bu adreslere giren, facebook hesabında yazışmalar yapan … " Yar. 8. CD, E.2012/33557, K.2013/25987, 01.11.2013, (UYAP).

"Sanığın, katılanın Facebook hesabını kullandığı sırada, katılanın arkadaşı olan B. H. E.'in Facebook hesabını bir şekilde ele geçirerek katılana mesaj gönderdiğini, internet banka hesabı kullanıp kullanmadığını sorduğu, kullandığını öğrenince de kendisinden iade etmek şartıyla 450,00 TL para istediği, katılanın Akbank internet bankacılığı aracılığıyla sanığın vermiş olduğu … hattına 450,00 TL para gönderdiğini" Yar. 15. CD, E.2013/14846, K.2013/12178, 01.07.2013, (UYAP).

tan yine başkası adına (örneğin Facebooka kayıt edilerek değil de) bilgisayar program ve teknikleri kullanılarak yapay bir Facebook profili görüntüsü oluşturulabilir ve bilahare bunun çıktısı da sunulabilir. Dolayısıyla bu yönlü olası savunmaları/ itirazları göz önünde bulundurmak gerekmektedir. Bu nedenle sayısal veya fiziki çıktı savcılığa veya kolluğa sunulduğunda, ilk etapta bir tutanakla çıktı ile çıktının ait olduğu söylenen görüntünün aynı olup olmadığını belirlemeye yönelik tespit işlemi yapılmasının yararlı olacağını düşünüyoruz. Yine duruma göre hemen bilirkişiye de (adli bilişim uzmanına) başvurulabilir.[60] Bu aşamada hızlı hareket edilmesi önemlidir; zira, örneğin şikayetin dayanağını oluşturan profil her an kapatılabilir veya örneğin internet üzerinden yapılan dolandırıcılığa konu ilan kaldırılabilir veya site kapatılabilir. Bu tür bir tehlikeyi bertaraf etmek ve iddiasını güçlendirmek adına mağdur olan kişi, şikayette bulunmadan önce 1512 sayılı Noterlik Kanunu'nun 198/A maddesi uyarınca elektronik tespitte[61] bulunabileceği[62] gibi adli bilişim uzmanı yardımıyla[63] da ekran görüntüsünü alabilir.

---

60 Ekran görüntüsü yazıcı çıktılarının bilirkişiye incelettirilmesi ancak orijinal görüntünün siber ortamdaki versiyonun bilirkişiye tevdii ile gerçekleştirilebilir. Çünkü bir ekran görüntüsü yazıcı çıktısı üzerinden sahihliğin tespiti teknik olarak mümkün değildir. Ekran görüntüsünün yazıcı çıktısı olması durumunda, siber ortamda yer alan ekran görüntüsünün ile beraber saklanan verinin verisi olarak tanımlanan üst verileri görmek artık mümkün olmayacaktır. Bilirkişi ancak ekran görüntüsü sayısal çıktısını inceleyerek bir raporlama yapabilecektir. Ekran görüntüsü sayısal çıktısına ulaşılamadığı hallerde pek tabi yazıcı çıktısı üzerindeki delil başlangıcı olabilecek verilerin tespiti, bilirkişi tarafından yapılabilecektir. Örneğin yazıcı çıktısında URL linkinin bulunması veya sistem bilgilerinin bir pencerede açık unutulması sırasında ekran görüntüsünün alınmış olması gibi, bkz. Özkan, "Ekran Görüntüsü," 281.

61 Noterlik Kanunu'nun 198/A maddesinin ikinci fıkrasının üçüncü cümlesinde, noterlerin, Noterlik Kanunu'nun 61. maddesi çerçevesinde yapacağı işlem grupları arasında yer alan tespit işlemleri ile elektronik ortamdaki durum, görüntü, işlem veya benzeri her türlü verinin tespiti işlemlerinin, yine, elektronik ortamda da noterliklerce gerçekleştirilebileceğine açıkça işaret edilmiştir. Elektronik ortamda yapılabilecek işlemlerin gerçekleştirilmesi sırasında uyulacak olan usûl ve esasları belirlemek amacıyla, *"Noterlik İşlemlerinin Elektronik Ortamda Yapılması Hakkında Yönetmelik"* (RG: 11.7.2015, S. 29413) çıkartılmıştır. Noterlerin, Noterlik Kanunu'nun 61. maddesi çerçevesinde yapacakları tespit işlemleri, ilke (olarak, fizikî ortamda gerçekleştirilir. Ancak, ilgilinin talep etmesi halinde sözü

Savcılıkça, sunulan çıktının türev olduğu dikkate alınarak ilgili web sitesi veya erişim sağlayıcısından görüntünün *doğrulanmasına* çalışılmalıdır. Çünkü dijital delil olan "çıktı"nın kendisi değil, dijital ortamdaki orijinal halidir.[64] Dijital delillerin kendine has yapıları

edilen işlem grubunun da elektronik ortamda, noterliklerce gerçekleştirilmeleri mümkündür (Yön. m. 5, V; m. 2). Burada özellik arz eden husus, elektronik ortamdaki durum, görüntü veya benzeri verilerin, tespitidir. Yönetmeliğin 6. maddesinde, elektronik ortamdaki bir verinin, tespiti işleminin nasıl gerçekleştirileceğine ilişkin olarak özel bazı belirlemelerde bulunulmuştur. Her şeyden önce, burada sözü edilen, elektronik ortamdaki bir verinin tespiti işleminden, bir donanımdaki veya internet ortamındaki verinin, tespiti işlemi ile o verinin belirli bir anda ya da zaman aralığında, o anki veya zaman aralığındaki halinin değişmez olarak belirlenmesi, tekrar edilebilir bir halde tutulması ve saklanması anlaşılır. Tespit edilecek veri, bir donanımda ise tespit, malikin ya da zilyetin rızasıyla, noterlikte veya mahallinde yapılabilir. Tespit edilecek veri, internet ortamındaysa, tespit işlemi, ancak, bu durumda, Türkiye Noterler Birliği Bilişim Sistemi kullanılmak suretiyle gerçekleştirilebilir (Yön. m. 5, VI/a,b,c). Bu konuda ayrıntılı bilgi için, bkz. Süha Tanrıver, "Noterler Tarafından Elektronik Ortamda Yapılabilecek Olan İşlemler Ve Bu İşlemlerin Gerçekleştirilmesi Usûlü," *Ankara Üniversitesi Hukuk Fakültesi Dergisi* 65, no. 4 (2016): 3677*ff*.

62 Türkiye Noterler Birliği Başkanı Yunus Tutar: "Artık sosyal medyada veya internet sitelerinde gördüğünüz ya da okuduğunuz bir yayını, haberi kayıt altına aldırabileceksiniz. Bu yenilikle TNB portala girerek tespit edilmesini istediğiniz yeri online belirleyebileceksiniz. Sistem arka planda her adımı kaydediyor, hangi sayfayı açtınız, nereyi tıkladınız gibi tüm bilgiler kaydediliyor. Bu veriler ve iz kayıtları özet bilgileri alınarak zaman damgası ile damgalandıktan sonra değiştirilemez bir şekilde TNB Bilgi Sistemleri'ne kaydediliyor ve size bir başvuru numarası veriliyor. Ertesi gün size verilen başvuru numarasıyla ya da TNB web sayfasındaki e-başvuru bölümünden istediğiniz noteri seçip başvuru yaparak noterden tespit tutanağınızı alıyorsunuz." "Elektronik Ortamda Tespit," Profelis, erişim tarihi Şubat 02, 2019, https://www.profelis.com.tr/tr/hakkimizda/basari-oykuleri/e-tespit/.

63 Adli bilişim uzmanı tarafından adli bilişim standartlarına uygun olarak (örneğin zaman damgası, dosyaların hash değeri, işleme ilişkin video kaydı gibi teknik bilgiler içeren) ekran görüntüsü alınmış olmasının, ileride manipülasyon olup olmadığına dair ortaya çıkabilecek tereddütleri gidermek bakımından yararlı olacağı kuşkusuzdur.

64 Değirmenci, *Sayısal (Dijital) Delil*, 132. Diğer taraftan dijital ortamdaki veriler, çıktılara yansımayan unsurları da içerebilirler. Bu konuda *Gökşen'in* Örneğin bir e-posta metni ekranda görüntülenebildiği gibi bir yazıcı vasıtasıyla da bu metnin basılmış hali edinilebilir. Ancak yazı aracılığıyla basılmış bir e-posta metni dijital belgenin kim tarafından, ne şekilde yazıldığına ilişkin sağlıklı bilgi ver-

nedeniyle ortaya çıkan doğru (sahih) olması ve doğruluğunun sağlanması[65] meselesi, inceleme konumuz bakımından daha önem arz etmektedir. Ülkemizde yayın yapan ve kayıtlı olan internet sitelerinin sahibi olan firmalardan, içerik ve yer sağlayıcı firmalardan her türlü bilgi ve belge talebinde bulunulabilir. Örneğin dolandırıcılık şikâyetine konu "sahibinden.com" isimli platform üzerinden yapılan bir ilana ilişkin fiziki çıktı sunulmuşsa, zikredilen platformla yazışma yapılarak (üye bilgileri, IP gibi bilgilerin temini yanı sıra) ilan görüntüsünün doğrulama işlemi yapılmalıdır. Ancak muhatap yurt dışı merkezli (Youtube, Facebook, Twitter, WhatsApp gibi) ise uluslararası istinabe kuralları gereğince yazışma gerekmekte olup, bu yola başvurulduğunda da çoğu zaman sonuç alınamamaktadır.[66]

Belirtelim ki, fiziki çıktıların manipülasyona açık yönlerine rağmen dosyaya sunulduğunda, hukuka aykırı olmamak kaydıyla her şeyin delil kabul edildiği vicdani delil sistemi içerisinde elbette ki delil olarak kabul edilecektir.[67] Bunun için hukuka uygun şekilde elde edilmesi gerektiği izahtan varestedir. Zira ceza muhakemesinde bir ispat aracının delil olarak kullanılabilmesi için bazı özelliklere

meyebilir. Bu takdirde söz konusu e-posta metninin bulunduğu bilgisayar içinde incelenmesi halinde bu belgeyi destekleyen farklı verilere de ulaşılabilecektir. Çıktısı alınmış bir e-postada bu metnin kimin e-posta adresinden, kime, hangi tarihte ve hangi saatte yazıldığında genellikle ulaşılabilmektedir. Ancak bu bilgilerin doğruluğu yine de sorgulanmalıdır. Zira e-postanın çıktısından bulunan bilgiler epostanın ait olduğu zannedilen kişi dışında kişilerce de yazılmış olabilir, bkz. Gökşen, "Dijital Verilerin Delil Değeri," 58.

65 Dijital delillerin sahihliği ve doğrulanabilir olması konusunda ayrıntılı bilgi için, bkz. Özkan, "Ekran Görüntüsü," 289*ff.*; Gökşen, "Dijital Verilerin Delil Değeri," 93*ff.*; Uzunay ve Koçak, "Bilişim Suçları Kapsamında," 3*ff.*

66 Sosyal medya üzerinden işlenen suçlarda uluslararası istinabe konusunda, bkz. Özocak, "Sosyal Medyada İşlenen."

67 Ceza muhakemesi maddi gerçeği ortaya çıkarmayı amaçladığından vicdani delil sistemini benimsemiş olup bununla ifade edilmek istenen, hem delil serbestisi hem de delillerin serbestçe değerlendirilmesidir. Delil serbestisi, hukuka uygun olmak kaydıyla ceza yargılamasında her şeyin delil olabileceği esasına dayanmaktadır. Bu konuda ayrıntılı bilgi için, bkz. Doğan Gedik, *Ceza Muhakemesinde İspat ve Şüphenin Sanık Lehine Yorumlanması* (Ankara: Adalet Yayınevi, 2016), 42*ff.*

sahip olması gerekir. Bir delilde bulunması gereken en önemli özelliklerden biri de onun hukuka uygun olmasıdır.[68] Anayasamızın 38/6. maddesi hükmü ile 5271 sayılı CMK'nın 206/2-a, 217/2 ve 289/1-i maddelerindeki düzenlemeler gereğince hukuka aykırı şekilde elde edilen deliller hükme esas alınamaz. Bu bilgiler ışığında, örneğin soruşturma dosyasına sunulan çıktının ilişkin olduğu Facebook hesabı başkasına ait olup da şifresi kırılarak girilmiş veya sahte oluşturulmuş bir hesap ise, söz konusu olan hukuka aykırı delil elde etme yöntemidir ve dolayısıyla fiziki çıktıların delil olarak değerlendirilmesi mümkün değildir. Sonuç olarak bize göre, hukuka aykırı elde edildiğine dair bir belirleme yoksa ve olayla ilgili ise üzerinde durulması gereken konu; fiziki çıktıların delil olarak kabul edilip edilmemesinden ziyade, her şeyin delil olarak kabul edildiği ve hâkimin de bunları değerlendirmekte serbest olduğu vicdanı delil sisteminde, bu çıktıların ispat gücünün ne olduğudur. Bu noktada biz de, çıktıları "belirti"/ "dolaylı delil"[69] niteliğinde kabul et-

---

[68] Genel olarak bir delilde bulunması gereken özellikleri için, bkz. Gedik, *Ceza Muhakemesinde İspat*, 45*ff*.; dijital delillerde bulunması gereken özellikler için, bkz. Değirmenci, *Sayısal (Dijital) Delil*, 114*ff*., 132*ff*.; Özkan, "Ekran Görüntüsü," 267*ff*.; Gökşen, "Dijital Verilerin Delil Değeri," 58*ff*.; Kaynakçıoğlu, "Ceza Muhakemesinde Dijital Deliller," 37*ff*.

[69] Öğretide, delillerin çeşitli tasniflere tabi tutularak incelendiği görülmekle birlikte, yaygın olarak "beyan", "belge" ve "belirti" şeklinde bir ayrıma tutulduğunu görmekteyiz. Yine öğretide bu delillerin, *somut olaya münhasır deliller* ve *genel mahiyette temsili deliller şeklinde* tasnifi de yapılmaktadır. Bunlardan beyan ve belge şeklindeki deliller, örneğin olayı gören tanığın beyanında olduğu gibi geçmişte kalan olayı doğrudan doğruya ispat edebilme niteliğine sahip olduğundan *somut olaya münhasır deliller*; buna karşılık belirtiler, maktulün gömleğinde bir başkasına ait saç teli bulunması örneğinde olduğu üzere somut olayın da dahil olduğu geniş bir gerçekliğin ispatına yaradığı için genel mahiyette temsili delil olarak kabul edilmektedir. Bu bağlamda ispat edilecek olayın dolaylı olarak ispatına yardımcı olan vakıalara ve izlere *belirti* denmektedir. Belirti, ispat edilmeye muhtaç olaydan geriye kalan her türlü iz ve eserlerdir. Vicdani delil sisteminde, hukuka uygun ve olayı temsil etme, akla vs. uygun olma gibi diğer özellikleri taşımak kaydıyla belirti de bir ispat aracıdır ve diğer deliller gibi hâkim tarafından değerlendirmeye tabi tutulacağı kuşkusuzdur. Ancak olayı doğrudan doğruya ispat etmediklerinden, tek başına her zaman yeterli olmayabilir, başka delillerle desteklenmesi çoğunlukla gerekebilir. Belirtinin önemli bir işlevi de, somut olaya münhasır delillerin değerlendirmesinde kendini göstermesidir.

mek;[70] ikrar, tanık beyanı veya dijital doğrulama gibi destekleyici başka delil bulunmadığı sürece soyut olarak tek başına hükme esas almamak gerektiği düşüncesindeyiz.

IV. SONUÇ

Bilişim teknolojilerindeki baş döndürücü gelişmeler, gerek maddi hukuka gerekse muhakeme hukukuna ilişkin yeni sorunları da beraberinde getirmekte; bu da yeni tartışmalara ve çözüm arayışlarına neden olmaktadır. Biz bu çalışmada; bilişim suçlarında uygulaması oldukça çok olan IP adresi (numarası) tespiti ile ekran görüntüleri fiziksel çıktılarının, ceza muhakemesinde ispat değerini inceleme gayretinde olduk.

Ulaştığımız sonuçları şu şekilde toparlayabiliriz: Bilişim suçlarında soruşturmanın yönlendirilmesi ve nihayetinde faile ulaşılması bakımından IP numarasının tespiti oldukça önemlidir. Ancak hem IP numarasının tespiti hem de bundan yola çıkarak failin tespiti, suçun sanal ortamda işlenmesinden kaynaklı kendine özgü zorlukları ihtiva etmekte ve adli makamları daha ihtiyatlı olmaya zorlamaktadır. Bu bağlamda öncelikle soruşturma konusu fiilin ilişkilendirildiği IP tespitinin doğru şekilde yapılması gerekmektedir. Yanlış bildirilen bir IP numarası, soruşturmanın seyrini değiştirebildiği gibi olayla ilgisi olmayan kişi/kişilerin şüpheli veya sanık olmasını da sonuçlayabilmektedir. Bu nedenle IP numarasının tespiti kadar, IP numarasının tahsis edildiği internet abonesinin belirlenmesi aşamasında da dikkatli olunmalıdır.

Hâkim, maddi sorunu çözerken doğrudan deliller gibi belirtilerden de yararlanarak bir sonuca ulaşacaktır. Belirtiler ve ispat güçleri hakkında, bkz. Gedik, *Ceza Muhakemesinde İspat*, 93*ff*.

[70] Öğretide *Kaynakçıoğlu'na* göre de dijital delilleri, belirti delilleri içerisinde sınıflandırmak gerekir. Dijital delil içeren elektronik aygıtların da bir kan ya da DNA örneği gibi gerek elde edilmesi gerekse incelenmesi sırasında uzmanlık gerekmektedir. Dijital deliller yapısal özellikleri nedeniyle kolaylıkla değiştirilebilir, bozulabilir ve yok edilebilirler. Bu nedenle dijital delillerin uzmanlarca incelenmeden delil olarak kabulü son derece tehlikelidir. Bkz. Kaynakçıoğlu, "Ceza Muhakemesinde Dijital Deliller," 46.

IP numarasının tespiti, ilişkin olduğu soruşturma bakımından sonuç değil, başlangıç noktası olabileceğini unutmamak gerekir. IP adresi kullananına işaret ediyor gibi görünse de teknik açıdan çoğu zaman doğrudan bir bilgisayarı veya bir kişiyi göstermekten ziyade, yalnızca bir internet aboneliğini gösterebilir. Bu nedenle IP adresinin tespiti, adres sahibinin suçun faili olduğunu doğrudan göstermez. IP numarası kullanılarak tespit edilen adreste sadece internet abonesi yaşasa dahi o kişi ikrarda bulunmadıkça veya diğer delillerle desteklenmedikçe, sadece IP numarası esas alınarak o kişi hakkında mahkumiyet hükmü verilmesi doğru değildir. Dolayısıyla IP adresi, tek başına mahkumiyeti gerektiren bir delil niteliği taşımayacak**,** ancak ikrar veya başkaca destekleyici deliller de varsa kişiler mahkum edilebilecektir. Yargıtay'ın da yaklaşımı bu yöndedir.

Uygulamada, başta hakaret, tehdit, şantaj veya özel yaşamın ihlali suçları olmak üzere çok sayıda suç son yıllarda yoğunlukla Facebook, Youtube, Twitter gibi sosyal paylaşım siteleri üzerinden veya WhatsApp, Messenger gibi mesajlaşma/konuşma uygulamaları veyahut elektronik postalar aracılığıyla işlenmekte, suçun mağduru da şikayet dilekçesine genellikle buna dair (örneğin Facebooktaki hesabın ekran görüntüsünü içeren) bir çıktıyı eklemekte, sunulan bu çıktılar üzerinden soruşturmaya yön verilmekte; ikrar, tanık ve olayın gelişimi gibi tüm delillerin değerlendirilmesi sonucunda ve diğer delillerle birlikte hükme esas alınabilmektedir. Gerçekten de fiziki çıktıların manipülasyona açık yönlerine rağmen dosyaya sunulduğunda, hukuka aykırı olmamak kaydıyla her şeyin delil kabul edildiği vicdani delil sistemi içerisinde elbette ki delil olarak kabul edilecektir. Hukuka aykırı elde edildiğine dair bir belirleme yoksa üzerinde durulması gereken konu; fiziki çıktıların delil olarak kabul edilip edilmemesinden ziyade, her şeyin delil olarak kabul edildiği ve hâkimin de bunları değerlendirmekte serbest olduğu vicdanı delil sisteminde, bu çıktıların ispat gücünün ne olduğudur. Bu noktada biz de, çıktıları "belirti"/ "dolaylı delil" niteliğinde kabul etmek, başka delillerle desteklenmediği ve dijital doğrulama yapılmadığı müddetçe, soyut olarak tek başına hükme esas almamak gerektiği düşüncesindeyiz.

KAYNAKÇA

Balı, Yunus. "IP Numarası Tespiti." Dijitaldeliller. Erişim tarihi Aralık 1, 2018. http://www.dijitaldeliller.com/ip_tespiti.html.

Cebecioğlu, Gülçin ve İpek Beyza Altıparmak**.** "Dijital Şiddet: Sosyal Paylaşım Ağları Üzerine Bir Araştırma." *Sakarya University Journal of Education* 7, no. 2 (Ağustos 2017): 423-431.

CHIP Online. "IP Adresim Nedir." Erişim tarihi Mayıs 25, 2019. https://www.chip.com.tr/ip-adresim-nedir.

Çubukçu, Ceren ve Berrin Atiker. "Sosyal Medya ve Bilişim Suçları." Academia. Erişim tarihi Mayıs 5, 2019. https://www.academia.edu/31785425/Sosyal_Medya_ve_Bilişim_Suçları.

Değirmenci, Olgun. *Ceza Muhakemesinde Sayısal (Dijital) Delil*. Ankara: Seçkin Yayıncılık, 2014.

Doğan**,** Koray. *Kuşkudan Sanık Yararlanır İlkesi*. Ankara: Seçkin Yayıncılık, 2016.

Durnagöl, Yasemin. "5651 Sayılı Kanun Kapsamında İnternet Aktörlerine Getirilen Yükümlülükler İle İdari Ve Cezai Yaptırımlar." *Türkiye Adalet Akademisi Dergisi* 2, no. 4 (2011): 375 – 416.

Dülger, Murat Volkan ve Gözde Modoğlu, *Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri ile İnternet İletişim Hukuku (Uygulama Rehberi)*. Ankara: Türk Ceza Adalet Sisteminin Etkinleştirilmesi Avrupa Birliği/Avrupa Konseyi Ortak Programı, 2014.

Dülger, Murat Volkan. *Bilişim Suçları ve İnternet İletişim Hukuku*. Ankara: Seçkin Yayıncılık, 2014.

Erdoğan, Burcu. "Bir Kişiyi Suçlamak İçin IP Adresi Yeterli midir?." *digiSophia*. Erişim tarihi Ekim 1, 2018. http://www.digisophia.com/Article/Details/61.

Gedik, Doğan. *Ceza Muhakemesinde İspat ve Şüphenin Sanık Lehine Yorumlanması*. Ankara: Adalet Yayınevi, 2016.

Gökşen, Elif. "Türk Ceza Muhakemesinde Dijital Verilerin Delil Değeri." Yayımlanmamış yüksek lisans tezi, Galatasaray Üniversitesi, 2014.

Gülseren, Fehmi Şener. "İnternet Ortamında İşlenen Hakaret Suçları." *LAÜ Sosyal Bilimler Dergisi* 4, no. 1 (Nisan 2013): 15-33.

Kaya, Mehmet Bedii. "İnternet Hukuku, Mevzuat & İçtihat." Mehmet Bedii Kaya. Erişim tarihi Mayıs 25, 2019. https://www.mbkaya.com/hukuk/internetmevzuat.pdf.

Kaynakçıoğlu, Uğur. "Ceza Muhakemesinde Dijital Deliller." Yayımlanmamış yüksek lisans tezi, Galatasaray Üniversitesi, 2015.

Özçelik, Gülsel Öykü. "IP Adresleri Tek Başına Delil Olabilir Mi? IP Adreslerine Yargılamada Ne Kadar Güvenilir?." TAG Hukuk Bürosu. Erişim tarihi Ekim 1, 2018. taghukuk.com/wp-content/uploads/2018/04/ip_adreslerinin_delil_niteliği.pdf.

Özkan, Halid. "Ceza Muhakemesinde Ekran Görüntüsü Çıktılarının Delil Niteliği." İç. *Ceza Muhakemesi Hukukunda Delil ve İspat*, editör Yener Ünver, 265-288. Ankara: Seçkin Yayıncılık, 2014.

Özocak, Gürkan. "Sosyal Medyada İşlenen Suç Tipleri Ve Suçluların Tespiti." Özocak Hukuk & Danışmanlık. Erişim tarihi Mart 11, 2019. http://www.ozocak.com/Dosyalar/a104b3.pdf.

Sarsıkoğlu, Şenel. "Ceza Muhakemesinde Delil Ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı." *Türkiye Adalet Akademisi Dergisi*, no. 22 (Temmuz 2015): 507-534.

Süha Tanrıver, "Noterler Tarafından Elektronik Ortamda Yapılabilecek Olan İşlemler Ve Bu İşlemlerin Gerçekleştirilmesi Usûlü," *Ankara Üniversitesi Hukuk Fakültesi Dergisi* 65, no. 4 (2016): 3677*ff*.

Şıracı, Sertel. "İnternet Kanununa Göre Log Tutma." Av. Sertel Şıracı. Erişim tarihi Şubat 02, 2019. https://www.sertels.av.tr/avukat/ hukuk/bilisim-hukuku/internet-kanununa-gore-log-tutma.html.

Taşçı, Ufuk ve Ali Can. "Türkiye'de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014." *Fırat Üniversitesi Sosyal Bilimler Dergisi* 25, no. 2 (2015): 229-248.

Uzunay, Yusuf ve Mustafa Koçak. "Bilişim Suçları Kapsamında Dijital Deliller." Akademik Bilişim Konferansları. http://ab.org.tr/ab05/tammetin/134.pdf.

Yegen, Ceren. "Demokratik Ve Yeni Bir Kamusal Alan Olarak Sosyal Medya." *Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi* 1, no. 2 (Aralık 2013): 119-135.

Yetim, Servet. "Bilişim Suçları ve Etkin Mücadele Yöntemleri." *Terazi Hukuk Dergisi* 9, no. 95 (Temmuz 2014): 80-86.