KAMU HUKUKU/PUBLIC LAW
Araştırma Makalesi / Research Article

Bilişim Sistemlerinden Delil Elde Edilmesine Yönelik İşlemler (CMK m. 134) Hakkında Bir Değerlendirme*

An Assessment of Procedures for Obtaining Evidence from Information Systems (CPC Art. 134)

Şenel SARSIKOĞLU**

ÖZ

Bilişim sistemlerinin insanların günlük rutininde yaygın olarak kullanımı, herhangi bir bilgisayar kaydından adres, telefon ve banka hesapları gibi çok sayıda bilgiye ulaşılmasını temin etmektedir. Söz konusu elektronik verilerin kişisel veri niteliğinde olması, özel hayatın gizliliği bağlamında hukuki tartışmalara sebep olmaktadır. Bu durum, klasik koruma tedbirlerinin yanında bilişim sistemlerinden verilerin elde edilmesine yönelik yeni araştırma yöntemlerinin uygulandığı kendine has bir delil hukuku doğurmuştur. Zira elektronik devrelerden oluşan bilgisayar verilerinin, ancak elle tutulabilir ve gözle görülebilir hale getirildikten sonra ceza muhakemesinde delil olarak kullanılabilmesi mümkündür. Öte yandan anayasal hükümlere göre temel hak ve hürriyetlere müdahale oluşturan, içerisinde arama, kopyalama ve elkoyma işlemlerini barındıran bu tedbirlerin kanun ile ayrıntılı ve açık bir şekilde düzenlenmesi zorunludur. 5271 sayılı Ceza Muhakemesi Kanunu (CMK) 134. maddesine göre; "bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, hakim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine" karar verilebilir. Bununla birlikte, detaylı hükümlere yer vermesi gereken ve zikredilen koruma tedbirlerinin öngörüldüğü kanun maddesi kapsamlı olarak düzenlenmemiş ve uygulamada ortaya çıkan sorunlara cevap vermede yetersiz kalmıştır. Söz konusu maddede yapılan değişiklikler de eleştirilere maruz kalmaya devam etmektedir. Çalışmamızda bilgisayar verilerinden delil elde edilirken başvurulan

* Makale gönderim tarihi: 17.10.2024. Makale kabul tarihi: 17.03.2025. Şenel Sarsıkoğlu, "Bilişim Sistemlerinden Delil Elde Edilmesine Yönelik İşlemler (CMK m. 134) Hakkında Bir Değerlendirme", *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi,* Cilt 12, Sayı 1, 2025, ss. 283-317, DOI: https://doi.org/10.46547/imuhfd.2025.12.1.8

** Dr. Öğr. Üye., Kastamonu Üniversitesi İktisadi ve İdari Bilimler Fakültesi, 0000-0002-2204-8422, senels@kastamonu.edu.tr

Çatışma Beyanı: Yazar/lar herhangi bir çatışma beyanı bildirmemiştir.

koruma tedbirlerine ilişkin olarak doktrin ve uygulama açısından yargısal içtihatlar ışığında değerlendirmelerde ve eleştirilerde bulunulması ile kanuni düzenlemede yer verilen hükümlerin hukuk devleti ilkesi bakımından yaratabileceği muhtemel problemlere ve çözüm önerilerine yer verilmesi amaçlanmaktadır.

Anahtar Kelimeler: Siber Suçlar, bilişim sistemleri, delil, Ceza Muhakemesi Kanunu, arama kopyalama elkoyma.

ABSTRACT

The widespread use of information systems in people's daily routines allows access to a large amount of information such as addresses, telephone numbers and bank accounts from any computer record. The fact that the electronic data in question is personal data causes legal discussions in the context of privacy. This situation has given rise to a unique law of evidence where, in addition to classical protection measures, new research methods are applied to obtain data from information systems. Because it is possible for computer data consisting of electronic circuits to be used as evidence in criminal proceedings only after they are made tangible and visible. On the other hand, according to constitutional provisions, these measures, which constitute an intervention in fundamental rights and freedoms and include search, copy and seizure operations, must be regulated in detail and clearly by law. According to Article 134 of the Criminal Procedure Code No. 5271 (CPC); "In the investigation conducted for a crime, in the presence of strong suspicions based on concrete evidence and in the absence of the possibility of obtaining evidence by any other means, the judge or, in cases where there is a risk of delay, the public prosecutor may decide to search the computer and computer programs used by the suspect and the computer logs, to make copies of the computer records, to decipher these records and to convert them into text." However, the article of the law, which should include detailed provisions and envisage the mentioned protection measures, was not regulated comprehensively and was insufficient to respond to the problems arising in practice. The amendments made to the article in question continue to be subject to criticism. In our study, we aim to make evaluations and criticisms regarding the protection measures used while obtaining evidence from computer data in the light of judicial precedents in terms of doctrine and practice, and to include possible problems and solution suggestions that the provisions included in the legal regulation may create in terms of the principle of the rule of law.

Keywords: Cyber crimes, information systems, evidence, criminal procedure law, search copy seizure.

Giriş

Teknolojik gelişim beraberinde bilişim sistemleri kullanılarak ika edilen suçların sayısı ve çeşitlerinin artmasını getirmiştir[1]. Bu suçlarla mücadele etmek

1 Bilişim suçlarının "truva atı" (trojan horse), "salam tekniği" (salam techniques), "ağ solucanları"

ve cezalandırmak görevini haiz devletin klasik yöntemlerle delil etme çabasının zaman zaman yetersiz kalması daha yeni ve teknik delil elde etme prosedürlerinin kullanılmasının yolunu açmıştır. Gerçekten de ceza yargılamasının amacı olan hakikatin bulunması, adaletin sağlanması ve hukuki barışın muhafazası[2] için önemi haiz olan delillerin[3] toplanarak ve korunarak bozulmaya uğramaksızın olayı yargılayacak merciin huzuruna taşınması temel bir sorun oluşturur[4]. Bu bakımdan ceza muhakemesinde nelerin delil olarak sunulup sunulamayacağından, bunların nasıl sunulup hangi amaçlarla kullanılacağına kadar kanunilik ilkesi kapsamında birçok kural bulunur. CMK da "sanıktan delile değil, delilden sanığa ulaşılması" prensibini benimsemekte; soruşturma evresinde delil toplama yetkisini haiz Cumhuriyet savcılığı ve emri altındaki kolluk güçlerine çeşitli araştırmalar yapma ve tedbirlere başvurma hususlarında önemli yetkiler vermektedir[5]. Ceza muhakemesinde hakikatin (maddi

---

(network worms), "sırtlama" (piggybacking), "mantık bombaları" (logic bombs), "bilgisayar virüsleri" gibi çok çeşitli işlenme şekilleri ve türleri bulunmaktadır. Ayrıntılı bilgi için bkz. Tayfun Ercan, İrem Erdal, *Türk Ceza Kanununda Bilişim Sistemine Girme Suçu ve Özel Hukuk Boyutu,* Adalet Yayınevi, Ankara, 2023, s. 41. Bununla birlikte; bilişim sistemleri kullanılarak işlenebilecek suçlara dair küçük bir bakış açısı sunmak adına; *"Lübnan'da 17 Eylül 2024 tarihinde çağrı cihazlarının eş zamanlı patlatılması suretiyle ikisi çocuk 12 kişinin öldüğü, 2323 kişinin yaralandığı"* olayı hatırlatmakta fayda bulunmaktadır. Anadolu Ajansı Haber Sitesi, 19.09.2024, https://www.aa.com.tr/tr/dunya/lubnan-telsiz-ve-cagri-cihazlarinin-patlatilmasiyla-ilgili-bmgkya-sikayette-bulunmaya-hazirlaniyor/3335387 (26.09.2024).

2 Hakan Karakehya, "Ceza Muhakemesinin Amacı", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası,* Cilt 65, Sayı 2, 2007, s. 138.

3 Friedrich-Christian Schroeder (Terc. Cumhur Şahin), "Ceza Muhakemesinde 'Dürüst Yargılama' İlkesi", *Selçuk Üniversitesi Hukuk Fakültesi Dergisi,* Cilt 5, Sayı 1-2, 1996 (Özel Sayı), s. 279. Yazarın, İnsan Hakları Avrupa Sözleşmesi (İHAS) m. 6/2,3'teki asgari haklar vasıtasıyla önlendiğini ifade ettiği sanık bakımından en tehlikeli davranış biçimlerinden bir tanesi de *"delillerin kolluk tarafından tahrifi ve buna karşılık duruşmada durumun düzeltilmesi imkanının olmayışıdır."* Gerçekten de bilişim sistemleri bakımından CMK m. 134'te düzenlenen tedbirlere başvurulduğunda elektronik delillerin hassas yapısı nedeniyle bunların olay yerinden toplanırken çeşitli kurallara uyulmasını zorunlu kılar, aksi delilin kaybı yahut tahrif edilmesini sonuçlar. Dolayısıyla, ceza soruşturmalarında adli bilişimin önemi ve elektronik delillerin yönetimi için standartlaştırılmış kurallar ve prosedürler geliştirme ihtiyacı her an kendini gösterir. Ayrıntılı açıklamalar için bkz. Naeem Allah Rakha, "Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations", *Mexican Law Review,* Cilt 16, Sayı 2, 2024, s. 23.

4 Hock Lai Ho, "The Legal Concept of Evidence", Ed. Edward N. Zalta, *The Stanford Encyclopedia of Philosophy,* Aralık 2021, s. 1 vd. https://plato.stanford.edu/archives/win2021/entries/evidence-legal/ (26.09.2024). Yazar, günümüzde dahi tüm hukuk sistemleri için ortak bir delil ve ispat yaklaşımı bulunmadığını, Anglo-Amerikan ve Kıta Avrupası hukuku arasında önemli farklılıklar bulunduğunu haklı olarak ifade etmektedir. Bu bakımdan hattı zatında önemli bir husus olan delil ve değerlendirilmesi, hayatın ve hukukun her alanı açısından elektronik vasfa sahip delillerden söz edildiğinde daha da önemli bir hal almaktadır. Ayrıntılı açıklamalar için bkz. Çetin Arslan, "Dijital Delil ve İletişimin Denetlenmesi", *Ceza Hukuku ve Kriminoloji Dergisi,* Cilt 3, Sayı 2, 2015, s. 254.

5 Mahmut Koca, "Ceza Muhakemesi Hukukunda Deliller", *Ceza Hukuku Dergisi,* Cilt 1, Sayı 2, Aralık 2006, s. 208.

gerçeğin) "her ne pahasına olursa olsun" peşine düşülmesi kabul edilmez[6]. Bu makamların öncelikle delil elde etme yasağına ve kanunun öngördüğü kurallara harfiyen uymaları gerekir[7]. Nitekim, ceza muhakemesinde "kanuna aykırı" toplanmış bulguların, birer delil olarak kabul görmesi imkân dahilinde değildir. Delillerin "kanuna aykırı" olarak toplanması, bu delillerin ileri sürülmesi talebinin red gerekçesidir (AY 38/6; CMK 206/2-a). Dolayısıyla isnat edilen suç, "hukuka uygun" olarak elde edilmiş her türlü delille ispat edilebilir (CMK 217/2)[8]. Anlaşılacağı üzere, bir delilin dışlanması için herhangi bir "kanuni" koşula uyulmaması yeterliyken, bir delilin kabulü için tüm "hukuki" düzenlemelere uygun bir delil toplama sürecinin yürütülmesi elzemdir.

Ceza muhakemesinde delil, suç teşkil eden eylemin belli bir kişi tarafından işlendiği ya da işlenmediği hususunda yargı makamının kesin bir kanaate varmasını sağlamak için kullanılan, cezai uyuşmazlığı oluşturan vakıanın bir bölümünü veya tamamını temsil edebilen, duyu organlarıyla idrak edilebilecek nitelikte ve maddi bir yapıya sahip olan, hukuk düzenince kabul gören araçlara denir[9]. Başka bir ifadeyle delil, hâkimin hakikati ortaya çıkarmak için kullandığı ispat vasıtalarının bütününü ifade eder[10].

---

6 Murat Volkan Dülger, *Ceza Muhakemesi Hukukunda Dışlama Kuralı ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağacın Meyvesi Öğreti),* Seçkin Yayıncılık, Ankara, 2014, s. 36. Bununla birlikte ifade edelim ki ceza muhakemesinde hakikatin ortaya çıkarılması, bir yandan suçların cezasız kalmamasını sağlarken diğer yandan da toplumsal davranış kurallarına uyumu sağlayarak toplumsal barışın devamına hizmet etmektedir.

7 Friedrich-Christian Schroeder, Torsten Verrel (Terc. Salih Oktar), *Ceza Muhakemesi Hukuku,* Yetkin Yayınları, Ankara, 2019, s. 105.

8 Yargıtay Ceza Genel Kurulu (CGK) 12.02.2019 tarih ve 272-86 sayılı kararında; *"usulüne uygun olarak verilmiş arama kararı veya yazılı arama emri olmaksızın, sanığın kemeri çözdürülüp, pantolonunu indirmesi sağlanarak iç çamaşırından sarktığı görülen peçetenin bulunduğu yerden alınması suretiyle ele geçirilen suç konusu uyuşturucu maddenin, hukuka aykırı yöntemle elde edilen delil niteliğinde olduğu ve bu delilin hükme esas alınamayacağına"* hükmedilmiştir. Buna karşılık; CGK 24.01.2019 tarih ve 380-52 sayılı kararında; *"görevlilerce, sanık Ö.F.'nin de içerisinde olduğu araçta yapılan kontrolde, aracın dışarıdan bakıldığında görülebilen yerinde bulunan uyarıcı nitelikteki tabletlere el konulması, gizlenmiş bir şeyi bulmaya çalışma ve araştırma anlamlarına gelen arama işlemi olarak değerlendirilemeyeceğinden adli arama kararı ya da yazılı arama emri alınmasına gerek olmadığına"* hükmedilmiştir. Kararlar için bkz. Abdulhalik Yıldız, *Yargıtay Ceza Genel Kurulu Kararları (2015-2020) Cilt 2,* Türkiye Adalet Akademisi Yayınları, Ankara, 2020, s. 95 vd.

9 M. Tahir Taner, *Ceza Muhakemeleri Usulü,* İstanbul Üniversitesi Yayın No: 442, Hukuk Fakültesi No: 98, Duygu Matbaası, İstanbul, 1950, s. 156; Baha Kantar, *Ceza Muhakemeleri Usulü: Birinci Kitap: Umumi Hükümler,* Güzel Sanatlar Matbaası, Ankara, 1957, s. 259; Faruk Erem, *Ceza Usulü Hukuku,* Ankara Üniversitesi Hukuk Fakültesi Yayınları, No: 274, Sevinç Matbaası, Ankara, 1970, s. 333.

10 Cumhur Şahin, Neslihan Göktürk, *Ceza Muhakemesi Hukuku II,* Seçkin Yayıncılık, Ankara, 2020, s. 25; Bahri Öztürk, Durmuş Tezcan, Mustafa Ruhan Erdem, Özge Sırma-Gezer, Yasemin F. Saygılar-Kırıt, Esra Alan-Akcan, Özdem Özaydın, Efser Erden Tütüncü, Derya Altınok-Villemin, Mehmet Can Tok, *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* Seçkin Yayıncılık, Ankara, 2020, s. 299.

Belli bir kişinin suç oluşturan eylemi ika edip etmediğine ilişkin olarak "basit şüphe" ile yola çıkılan ceza muhakemesi sürecinde, bu kişinin suçu işlediğinin sübuta ermesi, diğer bir deyişle "belliliğe ulaşılması" halinde mahkûmiyet kararı verilerek bu süreç sona erdirilir. Ceza muhakemesinde ispat için sabit oluş (sübut) aranmakta olup bunun haricinde mahkûmiyet kararı verilememekte ve "şüpheden sanık yararlanır" prensibi işlerlik kazanmaktadır[11]. Kanun koyucu tarafından tayin edilen kurallara ve ceza muhakemesine hâkim olan prensiplere aykırı elde edilen bir delil, hukuka aykırı delil niteliğinden dolayı suçun sabit oluşuna etki edecek nitelikteki mutlak bir delil dahi olsa kullanılamaz. Ceza muhakemesi düzenimizde hukuka aykırı deliller bakımından "mutlak değerlendirme yasağı" bulunmakta ve hâkime takdir hakkı tanınmamaktadır[12]. Bu yaklaşımdan hareketle düzenleme, doktrin ve yüksek yargı içtihatları açısından "bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" koruma tedbirlerine dair çalışmamızda sistematik değerlendirmelere yer verilmiştir.

I. Kanuni Düzenleme ve İlgili Kavramlar

Şüpheli veya sanık hakkında isnat edilen suçla ilgili delil elde edilmesi için "arama" (CMK 116 vd.); "elkoyma" (CMK 123 vd.); "bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" (CMK 134) gibi tedbirlere de başvurulabilmektedir.

Arama koruma tedbiri, CMK 116. maddesi 1. fıkrasında; *"Yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe varsa; şüphelinin veya sanığın üstü, eşyası, konutu, işyeri veya ona ait diğer yerler aranabil*ir." şeklinde düzenlenmiştir.

Elkoyma koruma tedbiri, CMK 123. maddesi 1. fıkrasında; *"İspat aracı olarak yararlı görülen ya da eşya veya kazanç müsaderesinin konusunu oluşturan malvarlığı değerleri, muhafaza altına alınır."* şeklinde düzenlenmiştir.

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbiri, CMK 134. maddesi 2. fıkrasında; *"Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün ya-*

11 Nurullah Kunter, Feridun Yenisey, Ayşe Nuhoğlu, *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku,* Beta Yayıncılık, İstanbul, 2010, s. 1325; Nur Centel, Hamide Zafer, *Ceza Muhakemesi Hukuku,* Beta Yayıncılık, İstanbul, 2017, s. 233.

12 Koca, s. 223; Ahmet Gökcen, Murat Balcı, M. Emin Alşahin, Kerim Çakır, *Ceza Muhakemesi Hukuku,* Adalet Yayınevi, Ankara, 2020, s. 328.

pılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir." şeklinde düzenlenmiştir.

Hukuksal niteliği itibariyle "arama" ve "elkoyma" koruma tedbirlerinin özel bir görünüşünü oluşturan "bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" koruma tedbirleri temel hak ve hürriyetler açısından başta özel hayat, ticari ve bilimsel sırlar ile mülkiyet olmak üzere müdahale oluşturması sebebiyle sıkı koşullara bağlanmakta; kapsamı kişi ve konu yönünden sınırlandırılmakta ve kural olarak fiziki ortamda değil, yalnızca elektronik ortamda delilleri bulunan siber suçlar (işlenirken bilişim sistemlerinin kullanıldığı suçlar) bakımından uygulanabilmektedir[13]. Siber suç kavramının kullanılması hususunda doktrinde görüş birliği yoktur. Bunun yerine bilişim suçu, dijital suç, elektronik suç, e-suç, bilgi çağı suçu, yüksek teknoloji suçu, sibernetik suç, bilişim alanında suç, bilgisayar suçu, internet suçu, internet alanında suç kavramları da birbirinin yerine kullanılır[14]. Biz ise çalışmamızda uluslararası alanda genellikle kullanılan siber suç kavramını tercih etmekteyiz[15]. Bununla birlikte; siber suç kavramın içeriği hakkında da uluslararası alanda ve Türk doktrininde bir uzlaşmanın olduğunu söylemek güçtür[16]. Kolayca bir tanım yapmak gerekirse siber suç, bilişim sistemleri aleyhine ya da bunlar aracılığıyla işlenen suçlardır[17]. Bu açıklamalar karşısında CMK 134. maddesinde yer alan koruma tedbiri bakımından "bilgisayar", "bilgisayar kütüğü", "internet" ve "bilişim sistemi" gibi bazı kavramlar açıklandıktan sonra söz konusu koruma tedbirinin incelenmesi lazım gelmektedir. Bu kavramların ortaya konulması, bilişim sistemlerinin nasıl çalıştığına ve verileri nasıl depoladığına dair genel bir bakışı temin eder. Bu ise elektronik delillerin elde

13 Centel, Zafer, s. 448.

14 Regner Sabillon, Jeimy Cano, Victor Cavaller, Jordi Serra, "Cybercrime and Cybercriminals: A Comprehensive Study", *International Journal of Computer Networks and Communications Security,* Cilt 4, Sayı 6, Haziran 2016, s. 166. Yazarlar, siber suç kavramının tek bir tanımının olamayacağını, en kolay şekilde bilgisayar verilerini ya da sistemlerini etkileyen işleyiş biçimine dayanan bir dizi eylem veya davranış olarak kabul edilebileceğini belirtmektedir.

15 Durmuş Tezcan, Mustafa Ruhan Erdem, R. Murat Önok, *Teorik ve Pratik Ceza Özel Hukuku,* Seçkin Yayıncılık, Ankara, 2020, s. 1146.

16 Siber suç faaliyetlerinin genellikle üç kategoriye ayrıldığı ifade edilmektedir. Bunlar; *"teknolojinin bir suçun işlenmesinde önemli bir rol oynadığı durumlar (elektronik dolandırıcılık, kara para aklama, çocuk pornografisi); teknolojinin bir suçu işlemek için kullanıldığı durumlar (kimlik hırsızlığı, bilgisayar sabotajı, ayrıcalıklı bilgilerin çalınması) ve teknolojinin bir suçun ikincil bir yönü olarak kullanıldığı durumlar (veri ve görüntü depolama, internet ve hücresel iletişim)."* James W. Osterburg, Richard H. Ward, *Criminal Investigating: A Method for Reconstructing the Past,* 6. Bası, 2010, s. 548.

17 Peter Stephenson, Keith Gilbert, *Investigating Computer-Related Crime,* 2. Bası, 2013, s. 4; Murat Önok, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,* Cilt 19, Sayı 2, 2013 (Özel Sayı), s. 1231.

edilmesi veya silinen bilgilerin nasıl kurtarılıp incelenebileceğini anlamak bakımından önemlidir[18].

Bilgisayar, diğer bir deyişle elektronik beyin, sözlükte "birtakım bilgileri hafıza denen kısımlarına kaydedip bir program veya kurala uygun olarak değerlendiren, problemleri çabucak çözen elektronik cihaz"[19] olarak tanımlanmaktadır[20]. Bilgisayar, donanım ve yazılımdan oluşan unsurları sayesinde tek başına çalışabildiği gibi benzer cihazlardan oluşan bir ağa (network) dahil olarak da çalışabilir.

Bilgisayar kütüğü, verilerin ve işlemlerin tutulduğu yer anlamında; olay kayıtları (loglar), verilerin saklandığı yerler (veritabanları/databaseler) ve veri saklanan donanımlar (harici harddiskler, flash bellekler, hafıza katları) gibi unsurlardan meydana gelir[21]. Ayrıca internet ortamında verilerin tutulduğu yerler olarak; ücretli veya ücretsiz bulut depolama alanları (OneDrive, Dropbox, Google Drive) da bilgisayar kütüğü kavramına dahildir[22].

İnternet, inter(connetted/national) ve net(works) kelimelerinin kısaltılmış

---

18 Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, 3. Bası, 2011, s. 437. Yazar, tüm dijital verilerin temelde birler ve sıfırların, yaygın olarak bit olarak adlandırılan kombinasyonları olduğunu ifade etmektedir.

19 Kubbealtı Lugatı, https://www.lugatim.com/s/bilgisayar (26.09.2024).

20 Yargıtay 7'nci Ceza Dairesi'nin 22.02.2024 tarih ve E. 2023/18292 K. 2024/1844 sayılı kararında; *"CMK'nın 134. maddesinde geçen bilgisayar teriminden ne anlaşılması gerektiği konusunun CMK'da açık bir şekilde belirtilmediğinden, CMK'nın 134. maddesinin uygulamada; bilgisayar, akıllı telefonlar, GPS cihazları, donanım ve yan donanımlar, verileri dijital olarak kaydetme ve işleme yeteneğinde olan her türlü dijital cihazları kapsadığına"* hükmedilmiştir.

Kararın tam metni için bkz. Kazancı İçtihat Bilgi Bankası, https://lib.kazanci.com.tr/kho3/ibb/files/dsp.php?fn=7cd-2023-18292.htm&kw=%60cmk+134%60+%60bilgisayar%60&cr=yargitay#fm (27.09.2024).

21 CGK 18.10.2023 tarih ve E. 2018/16-124 K. 2023/538 sayılı kararında; *"CMK'nın 134. maddesindeki "bilgisayar kütükleri" ifadesi teknik anlamda sadece masaüstü ve dizüstü bilgisayarlarda bulunanları değil; CD, DVD, flash disk, disket, harddisk vs. tüm çıkarılabilir bellekler, telefon vb. dijital tabanlı mobil cihazlarda dahil olmak üzere herhangi bir bilgi işlem veya veri toplama araç ya da gerecinde bulunabilecek tüm dijital dosyaları kapsamaktadır. Adli Ve Önleme Aramaları Yönetmeliği'nin "bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma" kenar başlıklı 17. maddesinde el koyma sırasında zorunlu kılınan yedekleme işleminin, "bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımlar hakkında" uygulanmasının dayanağının da bu düzenlemeler olduğu anlaşılmakla, sanığın kendisine ait olmadığını savunduğu CD'lerin bilgisayar kütüğü kapsamında değerlendirilmesi gerektiğinden imajları alınmadan içeriklerinin belirleyici delil olarak kabul edilmesinin 5271 Sayılı CMK'nın 134. maddesinde düzenlenen usule aykırı olduğuna"* hükmedilmiştir. Kararın tam metni için bkz. Kazancı İçtihat Bilgi Bankası, https://lib.kazanci.com.tr/kho3/ibb/files/dsp.php?fn=cgk-2018-16-124.htm&kw=%60CMK+134%60&cr=yargitay#fm (27.09.2024).

22 Osman Yaşar, Cengiz Otacı, *Ceza Muhakemesi Kanunu Cilt 1,* Seçkin Yayıncılık, Ankara, 2022, s. 1109.

hali ve dünyadaki en yaygın bilgisayar ağının karşılığı olarak ifade edilmektedir[23]. Bilgisayarlar bu ağa, IP[24] adresleri üzerinden bağlanırken internetteki diğer bilgisayarlar da yine bu IP adresi üzerinden ilgili bilgisayara ulaşır[25]. Bilgisayar, bilgisayar benzeri veya bilgisayar dışı elektronik araçların iletişimini sağlayan bu ağ üzerinde[26] siber suç olarak isimlendirilen eylemlerin çoğu işlenmektedir. Ayrıca internet üzerinden akan veriler ele geçirilmeye, çalınmaya veya değiştirilmeye karşı hassastır. Çalınan yahut kötüye kullanılan veriler daha sonra bireysel çıkar sağlamak amacıyla kullanılabildiği gibi hırsızlık, dolandırıcılık ya da kumar ve benzeri yasadışı eylemlerde de failler tarafından kullanılabilmektedir[27].

Elektronik delil (e-delil), dijital bir cihaz üzerinde saklanan ya da bu cihazlar aracılığıyla iletilen ve ceza muhakemesi bakımından değeri olan bilgi yahut veriler olarak tanımlanabilir[28]. Elektronik ortamda muhafaza edilen bu bilgiler, muhakeme konusu maddi olayla ilgili ve güvenilir olduğu hallerde e-delil olarak kabul edilecektir. Bunların veri saklama özelliğine sahip her türlü medya, aygıt veya ortamdan elde edilebilmesi mümkündür[29].

Bilişim sistemi hakkında doktrin ve uygulamada çok sayıda tanım yapılmaktadır[30]. Bununla birlikte en kapsayıcı tanım, "Ceza Muhakemesinde Ses ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik" 3/1-b bendinde yapılmıştır. Bu bentte yer alan hükme göre; bilişim sistemi, "bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistemi" anlatmaktadır. Dolayısıyla bir iletişim şekli olarak bilişim sistemi, çok sayıda cihaz ve unsurdan meydana gelmektedir. Bu noktada ifade etmemiz gerekir ki ceza muhakemesinin amacına daha uygun olacağını düşündüğümüz "bilişim sistemi" kavramı CMK 134'üncü madde başlığında "bilgisayar" kavramı yerine kullanılmalı ve bu yönde kanuni değişikliğe gidilmelidir.

---

23 Ömer Demirci, *Bilişim Suçları ve Soruşturma Yöntemleri,* Seçkin Yayıncılık, Ankara, 2022, s. 27.

24 IP (Internet Protokol) adresleri, bilgisayarların internet trafiğine dahil olduklarında kullandığı bir nevi kimlik numarası niteliğindedir.

25 Murat Semiz, *En Güncel İçtihatlar ve Uygulamadan Örnekleriyle Bilişim Suçları ve Soruşturma Yöntemleri,* Adalet Yayınevi, Ankara, 2022, s. 21.

26 Ercan, Erdal, s. 29.

27 Nguyen The Sang, Bui Bao Trung, "Cybercrime in the Digital Age: Challenges and Implication for Prevention", *International Journal of Social Science and Human Research,* Cilt 5, Sayı 11, Kasım 2022, s. 5082.

28 Şenel Sarsıkoğlu, "Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı", *Türkiye Adalet Akademisi Dergisi,* Cilt 6, Sayı 22, 2015, s. 439.

29 Yaşar, Otacı, s. 1109.

30 Ercan, Erdal, s. 19; Demirci, s. 23.

II. Amacı

CMK 134'üncü maddesinde düzenlenen koruma tedbirlerinin amacı, soruşturma veya kovuşturma konusu cezai uyuşmazlık hakkında delil elde edilmesi ve muhafaza altına alınıp ceza muhakemesinde ikame edilerek maddi gerçeğin ortaya çıkartılmasıdır. Bu bakımdan bu tedbirlerin hâkim kararıyla olsa da bir kişinin özel hayatına ilişkin çok sayıda verinin bulunduğu bilgisayar verilerinin yalnızca cezai uyuşmazlık konusu olan suçla alakalı olan kısmına dair uygulanması esastır[31]. Bu amacın dışına çıkılması elde edilen delilleri en başından itibaren hukuka aykırı hale getirir. Nitekim maddede göze çarpan husus, çok sıkı koşullar eşliğinde bu koruma tedbirine başvurulmasıdır. Hâkim kararının, kuvvetli şüphenin varlığının, başka türlü delil elde etme imkanının bulunmamasının birer şart olarak zikredilmesi tedbire her olayda başvurulmasının önüne geçilmesinin kanun koyucu tarafından amaçlandığını göstermektedir. Bununla birlikte; düzenlemenin arama zamanı, aranacak kişinin sıfatı ve yasa yolu gibi çok önemli hususlara değinmediği ve İnsan Hakları Avrupa Mahkemesi (İHAM) tarafından aranan güvencelerin kişilere sağlanmadığı ifade edilmektedir[32]. Esasında yasal şartlara uyulmaksızın elde edilecek deliller ceza muhakemesinde kullanılamayacak olsa da yasal şartlara riayet edilerek delil elde edilmesi bir yönüyle maddi gerçeğin aydınlatılmasını sağlarken diğer yönüyle de kişilerin haksız yere suçlanmaması, kişisel verilerin gizliliğinin sağlanması ve lüzumsuz veri toplanmasının önlenmesini sonuçlayacaktır.

III. Kapsamı

A. Kişi Bakımından

CMK 134'üncü maddesi hükümlerinde düzenlenen tedbirler öncelikle şüphelinin (ya da sanığın) "kullanımında olan" bilgisayar, sistemleri veya kütükleri hakkında uygulanabilir. Her ne kadar CMK 134'üncü maddesi yalnızca şüpheliden bahsetmişse de bu tedbirlerin özel arama ve elkoyma tedbirleri olduğu düşünüldüğünde ve ceza muhakemesinde kanunda boşluk olan hallerde hakkında hüküm bulunmayan duruma en çok benzeyen durumu düzenleyen hukuk kurallarının uygulanması kabul edildiğinden[33] CMK 116'ncı ve devamı maddelerinde düzenlenen genel hükümlerin aleyhe sonuç doğurmamak ko-

31 Feridun Yenisey, Ayşe Nuhoğlu, *Ceza Muhakemesi Hukuku,* Seçkin Yayıncılık, Ankara, 2020, s. 437; Veli Özer Özbek, Koray Doğan, Pınar Bacaksız, *Ceza Muhakemesi Hukuku,* Seçkin Yayıncılık, Ankara, 2020, s. 391.

32 Yaşar, Otacı, s. 1106.

33 Centel, Zafer, s. 50. Yazarlar, kural olarak, kıyas yapılabileceğini ancak sınırlayıcı ve istisnai hükümlerin söz konusu olması halinde benzetme yoluyla boşluk doldurulamayacağını ifade etmektedir.

şuluyla (aleyhe kıyas yasağına riayet edilerek) kıyas yoluyla uygulanmasının mümkün olduğunu düşünmekteyiz. Bununla birlikte kıyasın mümkün olup olmadığı konusunda katı veya esnek yaklaşımlara rastlanmaktadır. Kıyasın mümkün olmadığını savunan görüş, koruma tedbirlerinin sıkı şekil şartlarına tabi olduğunu ve genel arama hükümleriyle genişletici kıyas yapılması halinde temel hak ve özgürlüklerin ihlalinin söz konusu olabileceğini ifade etmektedir[34]. Bu görüşün kabul edilmesi halinde CMK 116'ncı ve devamındaki madde hükümleri CMK 134'üncü maddesi için uygulanma kabiliyetine sahip olmayacak ve dolayısıyla dijital delillerin niteliği gereği yalnızca bu maddede düzenlenen istisnai koşullara uyulması gerekecektir. Kıyasın mümkün olduğunu savunan görüş ise dijital veriler üzerinde yapılacak arama, kopyalama ve elkoyma sürecinin yeterince detaylı olmadığından hareketle boşlukların CMK 116'ncı ve devamındaki madde hükümleriyle doldurulması gerektiğini; mesela arama kararının nasıl alınacağı, arama sırasında kişilerin haklarının ne olduğu ve aramanın uygulanma usulü gibi hususlarda kıyasa başvurulabileceğini belirtmektedir[35]. Ayrıca CMK 134'üncü madde hükmüne göre yapılan arama sonrasında verilecek belge yönünden genel aramaya ilişkin CMK 121'inci maddesi hükmünden istifade edilebilecektir[36]. Yine CMK 134'üncü madde hükmünün avukat bürolarında nasıl uygulanacağı ile ilgili bir düzenleme bulunmamaktadır. Bu halde avukat bürolarında bulunan bilişim sistemlerinde yapılacak arama, kopyalama ve elkoyma işlemleri hakkında CMK 130'uncu maddesi kıyasen uygulanabilecektir[37]. Kaldı ki 1412 sayılı Ceza Muhakemeleri Usulü Kanunu (CMUK) döneminde dahi telekomünikasyon yoluyla yapılan iletişimin denetlenmesi, teknik araçlarla izleme ve gizli soruşturmacı görevlendirilmesi gibi ortak özelliği yeni, yapısı gereği gizlilik içeren ve modern koruma tedbirlerinin CMUK'ta düzenlenmediği ve fakat konuyla ilgisi oldukça dolaylı olan 91'inci maddenin ilk fıkrasındaki "Maznuna gönderilen mektuplar vesair

34 Neslihan Ateş-Benek, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma", *Ceza Hukuku ve Kriminoloji Dergisi,* Cilt 10, Sayı 2, 2022, s. 388 vd.

35 Mesela, "şüpheli hakkında soruşturma süresi içinde cumhuriyet savcısınca kovuşturmaya yer olmadığına dair karar verilmesi ya da şüpheli hakkında kovuşturma sonucunda beraat kararı verilmesi halinde elde edilen kopyalar ve çözümü yapılan metinlerin yok edilip edilmeyeceği, yok edilecekse ne kadar süre içerisinde yok edileceği gibi soruların cevabının CMK 134'üncü maddesinde bulunmadığı; bu konuyla ilgili yasal düzenlemeye ihtiyaç olduğu; bununla birlikte sorunun çözümüne yönelik CMK 137'inci maddesinin 3'üncü fıkrasının kıyasen uygulanabileceği" ifade edilmektedir. Osman Gazi Ünal, *Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma,* Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, 2011, s. 127; Salih Keskin, "Bilişim Suçlarında Ceza Muhakemesi Kanununun 134. Maddesindeki Hükümlerin Uygulanmasında Yaşanan Aksaklıklar", *KÜSBD,* Cilt 11, Sayı 2, 2021, s. 663.

36 Ateş-Benek, s. 392.

37 Ateş-Benek, s. 403.

mersule ve telgrafların posta ve telgrafhanede zaptı caizdir." hükmüne kıyas yoluyla dayanılarak uygulanmış olduğu ifade edilmektedir[38]. Bu görüşün kabul edilmesi halinde ise özel hükmün önceliği ilkesine halel gelmeksizin CMK 134'üncü maddesinde açıkça düzenlenen konularda CMK 116'ncı ve devamındaki madde hükümleri uygulanmayacak ve fakat CMK 134'üncü maddesinde açıkça yer almayan hususlarda CMK 116'ncı ve devamındaki hükümleri aleyhe sonuç doğurmamak koşuluyla (aleyhe kıyas yasağına riayet edilerek) uygulanma kabiliyeti kazanacaktır[39].

Buna göre, yalnızca soruşturma aşamasında şüphelinin değil, ayrıca kovuşturma aşamasında da sanığın kullanımında olan cihazlarda da bu tedbirlere başvurulabilir[40]. Ayrıca kanun koyucu, cihazların şüphelinin (ya da sanığın) kullanımında olmasını kâfi görmüş; zilyetlik ya da mülkiyeti altında bulundurmasını aramamıştır[41]. Bu itibarla kişilerin malik (asli zilyet) veya feri zilyet ya da alelade elinde bulunduran (zilyet yardımcısı) olduğu hallerde de ilgili bilgisayar, sistemleri veya kütükleri hakkında tedbire başvurulabilir. Mesela, şüphelinin (ya da sanığın) kullandığı cihazın kendisi ya da herhangi bir kişinin elinde, üstünde, arabasında, evinde, işyerinde ele geçirilmesi mümkündür.

Ayrıca doktrinde kişilerin "özel hayat beklentilerinin azaldığı yahut ortadan kalktığının varsayıldığı" hallerde artık genel arama kararı ile bu tedbirlerin uygulanabileceği, bu kararı da CMK 134'üncü maddesine göre karar vermeye yetkili makamın vereceği belirtilmektedir. Kurum ve şirket bilgisayarları açı-

---

38 Faruk Yasin Turinay, "Ceza Muhakemesi Hukukunda Koruma Tedbirlerinin Sınıflandırılması", *Ankara Üniversitesi Hukuk Fakültesi Dergisi,* Cilt 70, Sayı 2, 2021, s. 484. Yazar, *"hukuki durumun belirtildiği şekilde olduğu dönemde doktrinde konunun açık hükümle düzenlenmesi gerektiğinin belirtilmekle olduğunu; ancak mevcut durumda postada elkoymaya ilişkin hükmün kıyas yoluyla uygulanmasının kaçınılmaz olduğunun da savunulduğunu"* söylemektedir.

39 Dilek Özge Uğraş, "Bilgisayarlarda, Bilgisayar Programlarında ve Bilgisayar Kütüklerinde Arama, Kopyalama ve Elkoyma", *TBBD,* Sayı 154, 2021, s. 111. Yazar, CMK m. 134 hükmünün, genel arama karşısında özel hüküm niteliğinde olduğundan bahisle *"arama sırasında hazır bulunması gereken kişilere ilişkin CMK m. 120 hükmünün"* kıyasen uygulanması gerektiğini ifade etmektedir.

40 Aynı yönde, Doğan Soyaslan, *Ceza Muhakemesi Hukuku,* Yetkin Yayıncılık, Ankara, 2007, s. 284; Cumhur Şahin, Neslihan Göktürk, *Ceza Muhakemesi Hukuku I,* Seçkin Yayıncılık, Ankara, 2020, s. 376; İhsan Baştürk, "Bilgisayar Sistemleri ile Verilerinde Arama, Kopyalama ve Elkoyma", *Fasikül Hukuk Dergisi,* Cilt 2, Sayı 9, Ağustos 2010, s. 25; A. Caner Yenidünya, Zafer İçer, *Ceza Muhakemesi Hukuku,* Adalet Yayınevi, Ankara, 2016, s. 449. Aksi yönde, Kunter, Yenisey, Nuhoğlu, s. 1098. Son yazarlar, bu görüşlerine gerekçe olarak; *"kanunun koruma tedbirine soruşturma aşamasında başvurulabileceğini açıkça belirtmesini"* ve *"maddede sanıktan değil, yalnızca şüpheliden bahsedilmesini"* işaret etmektedir.

41 Olgun Değirmenci, *Ceza Muhakemesinde Sayısal (Dijital) Delil,* Seçkin Yayıncılık, Ankara, 2014, s. 322. Yazar, *"bulut bilişim gibi çok kullanıcılı sistemlerde yalnızca kişinin kullanımında olan hesaba ait veriler hakkında tedbire başvurulabileceğini, hizmet veren kuruluşun tüm sunumcu bilgisayarlarında arama yapılamayacağını"* haklı olarak ifade etmektedir.

sından ise bunlarda şirket sırları veya müşterilere ait kişisel verilerin bulunması hallerinde aramayı yapanlar bakımından hukuki ve cezai sorumluluğa yol açmaması adına üçüncü kişilerin özel hayat beklentilerinin korunması ve bu hususta özenli davranılması gerekmektedir[42]. Ancak, ifade edilmelidir ki şüphelinin (ya da sanığın) "kullanımında olmayan" cihazlar hakkında bu tedbirlerin uygulanabilmesi imkân dahilinde değilken[43], "kullanımında olan" cihazların kimde yahut nerede olduğunun ise önemi bulunmamaktadır.

CMK 134'üncü maddesinde yer alan tedbirlerin muhatabı şüpheli (ya da sanık) olmakla birlikte şikayetçi veya mağdur bakımından söz konusu tedbirlerin uygulanıp uygulanmaması konusunda düzenleme bulunmamaktadır. Özellikle siber suçlar bakımından bu kişilere ait bilişim sistemlerine delil elde edilebilmesi için başvurulması zaman zaman tek alternatif olarak karşımıza çıkabilir[44]. Ancak, suç şüphesi altında olmayan kişilere ait cihazlar bu tedbirin konusu oluşturmaz[45]. Doktrinde bu hallerde şikayetçi ya da mağdurun rızasının alınması şartıyla bu kişilere karşı işlenen suçlarda hedef olarak kullanılan bilişim sisteminde Cumhuriyet savcısının yazılı kararıyla arama yapılabilmesi yönünde mevzuat değişikliğine gidilmesi önerilmiştir[46].

Cumhurbaşkanı hakkında 1982 Anayasası 105'inci maddesi uyarınca meclis tarafından karar verilmedikçe soruşturma yapılması mümkün değildir. Cumhurbaşkanı yardımcıları, bakanlar ve milletvekilleri hakkında 1982 Anayasası 83'üncü maddesine göre dokunulmazlığın kaldırılması kararı verilmedikçe herhangi bir ceza muhakemesi işlemi yapılamaz. Soruşturma ve kovuşturma engellerinin kaldırılması ile bu kişiler hakkında CMK 134'üncü maddesi uyarınca kullandıkları bilgisayara, sistemlerine veya kütüklerine ilişkin tedbir kararı verilebilir. Yüksek mahkeme başkan ve üyeleri ile hâkim ve Cumhuriyet savcıları hakkında da tedbir kararı alınabilmesi için öncelikle kendileriyle ilgili mevzuata göre açılmış bir suç soruşturması bulunmalıdır. Ancak bundan sonradır ki tedbir kararı vermeye yetkili merci tarafından bu tedbirlere başvurulabilir[47]. Biz, bu kişilerin sahip ola-

42 Gökhan Yaşar Duran, "Ceza Muhakemesi Kanunu'nda (CMK) Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" *Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi,* Cilt 14, Sayı 173-174, Ocak-Şubat 2019, s. 186.

43 Yener Ünver, Hakan Hakeri, *Ceza Muhakemesi Hukuku Cilt 2,* Adalet Yayınevi, Ankara, 2019, s. 939. Yazarlar, *"üçüncü kişilere ait bilgisayarlarda bu koruma tedbirlerinin uygulanabilmesinin şartı olarak, şüpheli tarafından bunların kullanılmış ya da kullanılıyor olmasını"* göstermiştir. Bu şartlar altında tedbire hükmedilmesi durumunda CMK 117'nci maddesindeki usul kıyasen uygulama alanı bulur. Yenidünya, İçer, s. 450.

44 Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku,* Seçkin Yayıncılık, Ankara, 2020, s. 580.

45 Baştürk, s. 28.

46 Değirmenci, s. 324.

47 Değirmenci, s. 327.

bileceği bilgi ve belgeler bakımından CMK 125'inci madde hükümlerinin uygulanabileceği düşünüldüğünde ve söz konusu maddede yer alan "devlet sırrı niteliğindeki bilgileri içeren belgeler, ancak mahkeme hâkimi veya heyeti tarafından incelenebilir" açık hükmü karşısında devlet sırrı niteliğindeki bilgi ya da belgelerin yer aldığı cihazlar hakkında soruşturma aşamasında bu tedbirlere başvurulamayacağını düşünmekteyiz[48]. Ayrıca dava şartının arandığı ancak henüz dava şartının gerçekleşmediği hallerde soruşturma yapılmasına engel bulunmamakla birlikte bu şartlar gerçekleşmeden temel hak ve hürriyetleri kısıtlayan söz konusu tedbirlere başvurulması ölçülülük ilkesinin ihlali anlamına gelebileceğinden tedbir kararının verilmesi için şartın gerçekleşmesi beklenmelidir[49].

Avukatların kişisel bilgisayarlarına ilişkin istisnai bir düzenlemeye de mevzuatta yer verilmemiştir[50]. Avukatlara ait bilgisayarlarda, sistemlerinde veya kütüklerinde tedbirlerin uygulanması gündeme geldiğinde CMK 134'üncü maddesinin CMK 130'uncu madde hükümleriyle beraber uygulanması gerekir[51]. Buna göre, tedbirlere yalnızca hâkim tarafından verilecek karar üzerine başvurulabilir olup uygulanması Cumhuriyet savcısının gözetiminde yapılır. Arama baro başkanının yahut onu temsilen bir avukatın nezaretiyle mümkündür. Nezaret deyimi, hangi arama kıstaslarının uygulandığı; hangi dosyaların kopyalandığı ve hangilerine elkonulduğunun denetlenmesi durumunu anlatmak üzere kullanılmıştır. Bununla birlikte, doktrinde avukat bürosundaki aramada hazır bulunan baro başkanı veya baro başkanını temsilen bulunan avukatın görevinin büroda tedbirlerin uygulanacağı cihazların bulunmasıyla sona ereceği ileri sürülmektedir[52]. Biz, bu aşamadan sonra da CMK 130'uncu madde hükümlerinin kıyasen uygulanmaya devam olunması gerektiğini düşünmekteyiz.

B. Konu Bakımından

Kanun koyucu tarafından bilgisayarlarda, sistemlerinde veya kütüklerinde arama, kopyalama ve elkoyma tedbirlerinin uygulanabileceği suçlar açısından herhangi bir suç kataloğuna yer verilmiş değildir[53]. Bu sebeple tedbirlerin tüm suç

48 Benzer şekilde; Duran, s. 235.

49 Duran, s. 221.

50 Baştürk, s. 28. Yazar, *"avukatlara ait bilişim araçları yönünden ayrı bir düzenleme öngörülmediğinden, CMK m.134'ün avukatlar yönünden de aynı koşullarda uygulama yeteneği olduğunu"* ileri sürmektedir.

51 Özbek, Doğan, Bacaksız s. 392. Avrupa İnsan Hakları Mahkemesi, 20 Haziran 2007 tarihli Smirnov-Rusya kararında *"yeterli şüphe sebepleri yokken avukatın bilgisayarında arama yapıldığı ve meslek sırrının saklanması hususunda kanunda bir güvence öngörülmediği"* gerekçesiyle ihlal kararı vermiştir.

52 Duran, s. 195.

53 Yaşar, Otacı, s. 1113; Baştürk, s. 26. Son yazar, *"tasarıda iki yıl ve daha fazla hürriyeti bağlayıcı ceza gerektiren suçlarda bu tedbire yer verilmişken adalet komisyonunda bu kısmın*

tipleri için uygulanabileceği şeklinde bir izlenim söz konusu olmakla birlikte kural olarak, arama ve elkoymanın özel görünüm şekillerini oluşturan bu tedbirlerin sıkı koşulları düşünüldüğünde "başka şekilde delil elde etme imkânı bulunmayan" yani klasik koruma tedbirlerinin kâfi gelmediği tek alternatif olarak bilişim sistemlerinden delil elde edilebilen suç tipleri olan siber suçlarda uygulanabilir[54]. Bunlar haricindeki suç tipleri bakımından tedbir kararı verilirken öncelikle "somut delillere dayanan kuvvetli şüphe sebeplerinin" bulunduğu; "başka şekilde delil elde etme imkanının" ise bulunmadığı dikkatle araştırılmalıdır. Dolayısıyla internetin temel bir insan hakkı olarak telakki edildiği yirmi birinci yüzyılda günlük rutinimizin merkezi bir konumuna yerleşen bilişim sistemlerinin suç olgusu içeren hemen her yerde bulunabileceği hakikati karşısında bu suçların sınırlı sayı (tahdidilik) ilkesine göre belirlenemeyeceğini ve katalog suçlar listesine kanun koyucu tarafından yer verilmemesi hususunu eleştiren görüşlere katılmadığımızı ifade etmek isteriz. Gerçekten de örneğin, tutuklama koruma tedbiri açısından CMK 100'üncü maddesinde bir kataloğa yer verilmişken uygulamada söz konusu düzenlemenin adeta bir "tutuklama mecburiyeti" olarak anlaşıldığı görülmektedir. Bu noktada kanaatimizce esas çözüm, her koruma tedbiri bakımından katalog suç listesi tutmaktansa hakimlerin tedbir kararı verirken yapacakları değerlendirmelerde ölçülülük ve akla gelen son çare olma ilkeleri ekseninde temel insan hakları ile koruma tedbirinin uygulanmasından beklenen fayda arasında bir denge tutturmasından geçmektedir[55]. Doktrinde buna uyulmamasının AY 13'üncü maddesi bağlamında ölçülülük ilkesi ve dolayısıyla hukuka aykırı olacağı ve bu yönüyle son derece sakınca doğuracağı belirtilmektedir[56].

Nitekim söz konusu tedbirler, temel hak ve hürriyetlere doğrudan müdahale içer-

---

madde metninden çıkarılmasının isabetsiz olduğunu, ceza kanunlarında suç olarak tanımlanan her fiil için bu tedbire başvurabilmesi imkanının oranlılık ilkesinin ihlali anlamı taşıyabileceğini" ifade etmektedir.

54 Kişilerin şahıs ve mal varlıklarına yönelen eylemler ile bizzat sistemin kendisini ele geçirmeyi hedefleyen bu suçlara *"hacking, bot-net/d-dos saldırıları, bilişim sistemine girme, sistemi engelleme, bozma, velileri yok etme ya da değiştirme, özel hayatın ve haberleşmenin gizliliğini ihlal, kişisel verilerin kaydedilmesi, nitelikli hırsızlık ve dolandırıcılık, banka ve kredi kartlarının kötüye kullanılması suçları ile online kumar ve çocuk pornografisi"* gibi suçları örnek gösterilebilir. Ayrıca bkz. Metin Turan, *Bilişim Hukuku,* Seçkin Yayıncılık, Ankara, 2021, s. 71 vd.

55 Gerçekten de devletin, etkin kontrolünün bulunmadığı alanlarda bilhassa "siber alanda" dahi temel hak ve hürriyetler bakımından yükümlülükleri bulunmaktadır. Bunlar; temel haklara saygı ve bunlara gerekli özeni gösterme, ülke dışındaki yükümlülükler ve uluslararası işbirliği ile şeffaflık ve hesap verebilirlik şeklinde tezahür etmektedir. Ayrıntılı açıklamalar için bkz. Berkant Akkuş, "Devletin Etkin Kontrolünün Bulunmadığı Siber Alanda İnsan Hakları Yükümlülükleri Nelerdir?", *Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi Dergisi,* Cilt 6, Sayı 1, 2024, s. 159 ve 160.

56 Yaşar, Otacı, s. 1113.

diği için "olağan dışı-istisnai-ikincil" nitelikte ve akla gelen son çare (ultima ratio) olarak uygulanır. Bunun bir neticesi olarak, her suç araştırmasında "acaba kişinin elektronik cihazlarında herhangi bir şeye rastlayabilir miyiz, bunlara da bir bakalım" şeklinde düşünülemeyecek olup tedbirlere başvurulmasını gerektiren somut olguların muhakkak karar merciine sunulması gerekir[57]. Dolayısıyla bilişim sistemlerinden elde edilecek delillerin hukuka uygun yolla elde edildiğinden bahsedebilmek için kanun koyucu tarafından kuvvetli şüphenin yanında kümülatif bir şart olarak aranan "başka bir surette delil elde edilmesi imkanının bulunmaması" koşulunun gerek savcının talebine ve gerekse karar mercii hâkimin kararına somut olgular şeklinde yansıması bu tedbirlere ultima ratio ilkesine riayet edilerek başvurulduğunu gösterir. Ancak, pratikte bu koşula özen gösterilmediği ifade edilmekle birlikte, siber suçlarda şüpheli ve sanıklar kadar vakitle de bir yarışın bulunduğundan bahsedilmektedir[58]. Bu gerekçeye ceza muhakemesinde koruma tedbirleri bakımından kabul edilen akla gelen "son çare olma" ilkesi düşünüldüğünde iştirak etmek pek mümkün gözükmemektedir. Nitekim Yargıtay Ceza Genel Kurulu'nun bir kararında; "*Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma CMK'nın 134. maddesinde düzenlenmiş olup, ... 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 şekilde ...*" hükümlere yer verildiği belirtilmektedir[59].

Söz konusu koruma tedbirleri, esasen bilgisayar verilerine ilişkin olarak uygulanır. Ancak bu verilerin içerisinde yer aldığı cihazlar olarak CMK 134'üncü maddesinde bilgisayarlar, sistemleri ve kütüklerinden bahsedilmiştir. Bilgi teknolojilerindeki gelişim, akıl almaz bir hızla devam etmekte olup neredeyse her gün veri işleyen, saklayan ve ileten birçok yeni cihaz kişilerin kullanımına sunulmaktadır. Doktrinde de bilişimin bilginin elektronik araçlarla otomatik olarak işlenmesi süreci olduğu, bilgilerin saklanması, işlenmesi, organize edilmesi, değerlendirilmesi, çoğaltılması ve iletilmesiyle ilgili işlevleri otomatik olarak gerçekleştiren sistemlerin bilişim sistemi olarak kabul edildiği ifade edilmektedir[60]. Bu özelliklere sahip tüm

57 Baştürk, s. 27.

58 Rezan Epözdemir, "Bilişim Sistemlerinde Arama ve Elkoyma Tedbirleri", *Terazi Hukuk Dergisi,* Cilt 13, Sayı 142, Haziran 2018, s. 92.

59 CGK 22.10.2019 tarih ve E. 2017/7-961 K. 2019/622 sayılı kararı. Kararın tam metni için bkz. Kazancı İçtihat Bilgi Bankası, https://lib.kazanci.com.tr/kho3/ibb/files/dsp.php?fn=cgk-2017-7-961.htm&kw=%60CMK+134%60&cr=yargitay#fm (27.09.2024).

60 Mahmut Koca, İlhan Üzülmez, *Türk Ceza Hukuku Özel Hükümler,* Adalet Yayınevi, Ankara, 2019, s. 851; Mustafa Özen, *Ceza Hukuku Özel Hükümler Dersleri,* Adalet Yayınevi, Ankara,

cihazlar bakımından CMK 134'üncü maddesinde yer alan tedbirlerin uygulanabilir[61]. Cep telefonları, cep bilgisayarları, CDler, DVDler, USBler, hafıza kartları, harici diskler, fotoğraf makineleri ve onların hafıza kartları, akıllı saatler, akıllı kartlar bu cihazlara örnek verilebilir[62]. Nitekim CMK 134'üncü maddesinde "bilgisayar kütüğü" kavramına yer verilmesi sayesinde CD, DVD, USB gibi bilgisayar olmamakla birlikte "dijital veri içeren"[63] tüm donanımlar da madde kapsamında değerlendirilir[64]. Nitekim Yargıtay Ceza Genel Kurulu'nun bir kararında; *"Sanığın kendisine ait olmadığını savunduğu CDlerin bilgisayar kütüğü kapsamında değerlendirilmesi gerektiğinden imajları alınmadan içeriklerinin belirleyici delil olarak kabul edilmesinin 5271 s. CMK'nin 134. md. düzenlenen usule aykırı olduğuna"* hükmedilmiştir[65].

2019, s. 555; Veli Özer Özbek, Koray Doğan, Pınar Bacaksız, *Türk Ceza Hukuku Özel Hükümler,* Seçkin Yayıncılık, Ankara, 2020, s. 963; Tezcan, Erdem, Önok s. 1150.

61 Ünal, s. 95; Yenidünya, İçer, s. 449.

62 Betül Gül Şarsel, *Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma,* Yaşar Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, 2017, s. 99.

63 Gerçekten de dijital delilin bir donanım aygıtında bulunması halinde, ceza yargılamasında asıl delili oluşturan donanım aygıtının kendisi değil, donanım aygıtında bulunan dijital delildir. Alaaddin Egemenoğlu, "Proving the Crime of Threat Through Digital Evidence in the Light of the Supreme Court Decisions", *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi,* Cilt 7, Sayı 2, 2024, s. 483.

64 Yaşar, Otacı, s. 1108.

65 CGK 18.10.2023 tarih ve E. 2018/16-124 K. 2023/538 sayılı kararı. Kararın tam metni için bkz. Kazancı İçtihat Bilgi Bankası, https://lib.kazanci.com.tr/kho3/ibb/files/dsp.php?fn=cgk-2018-16-124.htm&kw=%60CMK+134%60&cr=yargitay#fm (27.09.2024). Yüksek mahkeme, söz konusu kararında CMK 134'üncü ve 135'inci maddelerin ayrımına ilişkin olarak; *"Bilgisayarlarda, bilgisayar programları, bilgisayar kütükleri veya diğer araçlarda yapılacak aramanın konusu "elektronik veri"dir. Bu araçlarda arama işleminde amaç suçla bağlantılı her türlü elektronik veriye ulaşmaktır. Bu kapsamda bilgisayardaki mevcut klasördeki dokümanların tümü taranabilir. Bilgisayarda, şüpheli veya sanığın internet ortamında çeşitli programlar ya da sosyal iletişim siteleri (Msn Messenger, Facebook, Twitter vb.) vasıtasıyla gerçekleştirdiği iletişime ilişkin kayıtların aranması, CMK'nın 135. maddesine göre değil, CMK'nın 134. maddesine göre yapılabilir. Zira CMK'nın 135. maddesinde düzenlenen telekomünikasyon yoluyla iletişimin denetlenmesi koruma tedbiri, teknik araçlarla iletişimin tespitini, dinlenmesini ve kayda alınmasını kapsamaktadır. CMK'nın 135. maddesine göre yapılan iletişimin dinlenmesi ve kaydı, geçmişe dönük olarak değil geleceğe dönük olarak yapılabilir. Diğer bir ifadeyle geçmişte gerçekleşen iletişimin dinlenebilmesi, kayda alınabilmesi mümkün değildir. Ancak internet ortamında gerçekleştirilen iletişime ilişkin kayıtlar, bilgisayar kütüğünde kayıt altına alındığından bu iletişim kayıtları hakkında CMK'nın 134. maddesindeki koruma tedbiri kapsamında arama, kopyalama ve elkoyma tedbirleri uygulanabilir. Bireyin e-posta, yazışma ve haberleşmeleri CMK'nın 135. maddesi kapsamında değerlendirilirken, bireyin kendisine e-posta ile gelen bir yazı, resim, görüntü veya ek dosyayı kullandığı bilgisayara veya taşınır belleğe kaydettiğinde, artık bu belge haberleşme hürriyetinin dolayısıyla iletişimin denetlenmesinden çıkıp CMK'nın 134. maddesi kapsamında bilişim cihazına kayıtlı bilgi ve belgeye dönüşecektir. Kriptolu haberleşme sonucunda silinmiş mesajların gerek bilgisayarda gerekse sistem üzerinde ele geçirilmesi de telekomünikasyon yoluyla yapılan iletişim denetimi kapsamında olmayıp bu gibi hâllerde CMK'nın 134. maddesinde düzenlenen bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma tedbiri söz konusu olabilir."* şeklinde içtihatta bulunmuştur.

IV. Koşulları

A. En Azından Soruşturma Evresine Başlanılmış Olmalıdır[66]

CMK 134'üncü maddesi sırasıyla "soruşturma, hakim ve şüpheli" kavramlarına yer verirken "kovuşturma, mahkeme ve sanık" kavramlarından ise bahsetmemiştir. Bu durum, doktrinde uzlaşmanın sağlanamamasına ve iki değişik

66 6 Ocak 2017 tarih ve 680 sayılı Kanun Hükmünde Kararname'nin 27'nci maddesi ile 2559 sayılı Polis Vazife ve Salahiyet Kanunu 6'ncı ek maddesine eklenen; *"Polis, sanal ortamda işlenen suçlarda, yetkili Cumhuriyet başsavcılığının tespiti amacıyla, internet abonelerine ait kimlik bilgilerine ulaşmaya, sanal ortamda araştırma yapmaya yetkilidir. Erişim sağlayıcıları, yer sağlayıcıları ve içerik sağlayıcıları talep edilen bu bilgileri kolluğun bu suçlarla mücadele için oluşturduğu birimine bildirir."* hükmü sayesinde polise sanal (siber) ortamda bir "araştırma" yetkisi tanınmış idi. Ancak Anayasa Mahkemesi (AYM), 19.02.2020 tarih E. 2018/91 ve K. 2020/10 sayılı kararı ile bu hükmü iptal ederek polise tanınan sanal (siber) ortamda "araştırma" yetkisine son vermiştir. AYM kararı hakkında ayrıntılı açıklamalar için bkz. Mehmet Bedii Kaya, Polisin Sanal Devriye Yetkisini İptal Eden Anayasa Mahkemesi Kararının Değerlendirilmesi, https://mbkaya.com/hukuk/polis-sanal-devriye-siber-kolluk-aym-iptal.pdf (27.09.2024).

Yargıtay 3'üncü Ceza Dairesi'nin 07.03.2024 tarih ve E. 2022/11685 K. 2024/3488 sayılı kararında yer verilen karşı oy yazısında da vurgulandığı üzere; *"... polise siber ortamda tanınan sanal ortamda araştırma yetkisi iptal edilmiştir. Bu tarihlerden sonra ve önce Ceza Muhakemeleri Kanunu'nun genel hükümlerine göre Cumhuriyet savcısının talimatı doğrultusunda suç araştırması yapılacağı aşikardır ve hazırlık soruşturması nasıl başlayacağı kanunumuzda açıkça düzenlenmiştir. Polise sanal yetki verilen dönem dışında kalan suç tarihinde de soruşturmanın Ceza Muhakemeleri Kanunu'nun genel hükümlerine göre Cumhuriyet savcısının talimatı doğrultusunda suç araştırması yapılacağı aşikardır ve hazırlık soruşturması nasıl başlayacağı kanunumuzda açıkça düzenlenmiştir. Dolayısıyla suç tarihinde 5271 Sayılı Ceza Muhakemeleri Kanunu'na göre soruşturma ve suç delillerinin toplanması zorunludur. Cumhuriyet savcısı, ihbar veya başka bir suretle bir suçun işlendiği izlenimini veren bir hali öğrenir öğrenmez kamu davasını açmaya yer olup olmadığına karar vermek üzere hemen işin gerçeğini araştırmaya başlar (CMK. 160/1 m.). Cumhuriyet savcısı, doğrudan doğruya veya emrindeki adli kolluk görevlileri aracılığıyla her türlü araştırmayı yapabilir (CMK. 161/1 m.). Yargıtay Ceza Daireleri ve Ceza Genel Kurulu kararlarında istikrarlı bir şekilde soruşturmayı Cumhuriyet Savcısını başlatacağı ve soruşturma işlemlerini Cumhuriyet Savcısını talimatıyla yapılabileceği açıkça kabul edilmiştir. Yargıtay Ceza Genel Kurulu, 04.12.2007 tarihinde vermiş olduğu 2007/247-257 Sayılı kararında "Soruşturma evresinin asıl yetkilisi olan Cumhuriyet savcısı ihbar veya başka bir suretle bir suçun işlendiği izlenimini veren bir hali öğrenir öğrenmez ceza yargılamasının temel amacı olan maddi gerçeğin ortaya çıkartılması için soruşturmaya başlayacaktır. Cumhuriyet savcısının maddi gerçeğin ortaya çıkartılması amacına yönelik olarak hangi tür olaylarda hangi yolları takip edebileceğine ilişkin mevzuatımızda çok açıklık bulunmamakla birlikte soruşturma yöntemleri uygulamanın getirdiği benzer olaylardaki hareket tarzı yoluyla kazanılan ve mesleki birim olarak isimlendirilebilecek tecrübe, yargısal kararlar ve öğreti maddi gerçeğin ortaya çıkartılması için Cumhuriyet savcısının yolunu aydınlatmaktadır." demek suretiyle Cumhuriyet savcısının hukuk içerisinde kalarak Ceza Muhakemeleri Kanunun'daki usul işlemlerini ve (hükümleri riayet etmek suretiyle) soruşturmada yürüteceği yöntemi kendisinin belirleyeceğini benimsemiştir; ancak Cumhuriyet savcısının bu serbestliği sınırsız, hukuk düzenine ve evrensel hukuk kurallarına aykırı olamaz. Ayrıca ünlü ceza hukukçusu Rudolf Von Jhering'in değimi ile "şekil keyfiyetin düşmanı hürriyetin ikiz kardeşidir." ilkesinde belirtildiği gibi Cumhuriyet savcısı ve kolluk birimleri ceza soruşturmasında Ceza Muhakemeleri Kanunu'nda belirtilen usul kurallarına uymak zorundadır. Usul kurallarına uymadan hukuka aykırı elde edilen deliller soruşturma ve kovuşturmada kullanılamaz (CMK m. 147, 217/2, 206/2-a, 230/1-b, 289/1-i)."* Kararın tam metni için bkz. Kazancı İçtihat Bilgi Bankası, https://lib.kazanci.com.tr/kho3/ibb/files/dsp.php?fn=cgk-2018-16-124.htm&kw=%60CMK+134%60&cr=yargitay#fm (28.09.2024).

alternatifin savunulmasına sebebiyet vermiştir. Birinci alternatif, kanun koyucu tarafından bilgisayar verilerinde arama yapılması; bilgisayar verilerinin kopyalanması ve bilgisayar verilerine elkonulması tedbirlerinin yalnızca soruşturma evresine müteallik olarak düzenlendiği ve kovuşturma evresinde bu tedbirlere başvurulamayacağını öne sürer[67]. Gerekçe olarak, aleni yapılan duruşmada mahkemece bu tedbirlere karar verilmesi durumunda ilgililerin bunu öğrenerek verileri yok edeceği ve delil elde edilmesi amacına ulaşılamayacağını belirtir. İkinci alternatif, mahkemelerin re'sen (kendiliğinden) araştırma yetkisini haiz olduğu ve ceza muhakemesi sistemimizde kovuşturma evresinde delil toplanmasını yasaklayan hükümler olmadığı gerekçesiyle kovuşturmada da bu tedbirlere müracaat edilebileceğini ifade eder[68]. Bize göre, CMK 134'üncü maddesi uyarınca en azından soruşturma evresine başlanılmış olmalıdır[69]. Bu itibarla ceza soruşturması niteliğini haiz olmayan disiplin ya da idari soruşturma başlatıldığı hallerde yahut bir hukuk davasında bu tedbirlere başvurulamaz. Fakat, CMK 192'nci maddesine göre kovuşturmada mahkeme tarafından delillerin ikame edilmesinde bir sakınca bulunmamalıdır[70]. Yargıtay Ceza Ge-

67 Epözdemir, s. 91; Duran, s. 219; Yaşar, Otacı, s. 1115; Yenisey, Nuhoğlu, s. 435, yazarlar, *"maddede sadece şüpheliden söz edildiği gerekçesiyle tedbire kovuşturma aşamasında başvurulamayacağı"* kanaatindedir. Centel, Zafer, s. 449, yazarlar *"açık duruşmada tedbire karar verilmesi halinde ilgililerin kayıtları yok edeceği gerekçesiyle kovuşturmada bu tedbirin yarar sağlamayacağı"* düşüncesindedir. Bahri Öztürk, Behiye Eker-Kazancı, Sesim Soyer-Güleç, *Ceza Muhakemesi Hukukunda Koruma Tedbirleri,* Seçkin Yayıncılık, Ankara, 2019, s. 204, yazarlar, *"kanun koyucunun CMK 129'uncu ve 133'üncü maddelerinde hem soruşturma hem kovuşturma evresinden açıkça bahsederken; CMK 134'üncü maddesinde yalnızca soruşturma evresi deyimini kullanmasının bilinçli bir tercih olduğunu ve kanunilik ilkesi gereği tedbirin bu evreye münhasır olarak uygulanacağı"* görüşündedir. Mustafa Özen, *Öğreti ve Uygulama Işığında Ceza Muhakemesi Hukuku,* Adalet Yayınevi, Ankara, 2019, s. 692, yazar, *"lafzi yorum sonucunda maddede geçen hakim ibaresinin sulh ceza hakimi olarak anlaşılması halinde tedbire sadece soruşturma evresinde başvurulabileceğini"* belirtmektedir.

68 Gökcen, Balcı, Alşahin, Çakır, s. 480; Şahin, Göktürk, *Ceza Muhakemesi Hukuku I*, s. 376; Soyaslan, s. 284; Baştürk, s. 25; Yenidünya, İçer, s. 449. Son yazarlar, bu araştırma ve ispat aracı elde etme yönteminin yalnızca soruşturma evresine müteallik olarak düzenlenmesinin eksik olduğu görüşündedir. Buna göre, kanunda kovuşturma evresi için de düzenleme yapılması gerekir. Aksi bir uygulama, kanunilik ilkesi uyarınca hukuka aykırıdır.

69 Yargıtay 8'inci Ceza Dairesi'nin 14.05.2014 tarih ve 3415/12298 sayılı kararında kovuşturma aşamasında da CMK 134'üncü maddesinin uygulanabileceğine yönelik olarak; *"sanığın suçlamaları kabul etmeyerek kullandığı modemin şifreli olduğunu ve kötü niyetli kişiler tarafından şifresinin kırılıp kullanılabileceğini savunması karşısında, sanığın bilgisayarına elkonulup hard diski incelenerek suça konu siteye ait bilgisayarlar arasında bağlantı ve veri akışı olup olmadığının saptanmasına"* hükmedilmiştir.

70 Muharrem Özen, Gürkan Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirlerinin Hukuki Rejimi", *Ankara Barosu Dergisi,* Sayı 1, 2015, s. 62. Yazarlar, *"CMK 134'üncü maddesi uyarınca işlem yapılabilmesi için öncelikle bir suç soruşturmasının varlığının gerekmekte olduğunu; ancak bu şartı dar yorumlamamak gerektiğini; zira kovuşturma aşamasında eksik deliller söz konusu ise bu aşamada da CMK 134'üncü maddesi gereğince koruma tedbiri kararı verilebileceğini"* ifade etmektedir.

nel Kurulu da 2017 tarihli bir kararında bu görüşe yer vermektedir[71]. Zira ceza muhakemesinin amacı olan maddi gerçeğin (hakikatin) ortaya çıkarılmasına hizmet edebilecek delillerin CMK 134'üncü maddeye başvurulması yoluyla elde edilmesi imkânı kovuşturma evresi bakımından ortadan kaldırılmamalıdır. Nihayetinde yapılması gereken, kanun koyucu tarafından kovuşturma evresini de içine alan bir değişikliğe gidilmesidir[72]. Ancak bu noktada mevcut durum bakımından ifade etmek isteriz ki özel hükmün önceliği ilkesine halel gelmemesi için CMK 134'üncü maddesinde açıkça düzenlenen konularda CMK 116'ncı ve devamındaki madde hükümlerinin uygulanamayacağını ve fakat CMK 134'üncü maddesinde açıkça yer almayan hususlarda CMK 116'ncı ve devamındaki hükümlerinin aleyhe sonuç doğurmamak koşuluyla (aleyhe kıyas yasağına riayet edilerek) kıyas yoluyla uygulanma kabiliyetinin olduğunu düşünmekteyiz.

B. Somut Delillere Dayanan Kuvvetli Şüphe Sebepleri Bulunmalıdır

CMK 134'üncü maddesinde düzenlenen koruma tedbirleri bakımından katalog suçlara yer verilmemiştir. Bununla birlikte; söz konusu tedbirlere başvurulabilmesi için "somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı" aranmaktadır. Bu koşul, yalnızca CMK 134'üncü maddesi bağlamında bilgisayar verilerinde arama yapılması; bilgisayar verilerinin kopyalanması ve bilgisayar verilerine elkonulması tedbirlerinin uygulanabilmesi için değil, ayrıca "tutuklama; taşınmazlara, hak ve alacaklara elkoyma; şirket yönetimi için kayyım tayini; telekomünikasyon yoluyla yapılan iletişimin denetlenmesi; gizli soruşturmacı görevlendirilmesi ve teknik araçlarla izleme" tedbirlerinde öngörülen bir "ortak koşul" olarak ittihaz edilir[73]. Nitekim, ceza muhakemesinde koruma tedbirlerinin ortak özelliklerinden biri de soruşturma ya da kovuşturma konusu suçun işlendiği hususunda belli derecede şüphe bulunmasıdır[74]. Buna haklı görünüş, diğer bir deyişle görünüşte haklılık denir[75]. Gerçekten de

---

71 CGK 18.10.2023 tarih ve E. 2017/16-956 K. 2017/370 sayılı kararı. Kararın tam metni için bkz. Kazancı İçtihat Bilgi Bankası, https://lib.kazanci.com.tr/kho3/ibb/anaindex.html (27.09.2024).

72 Dülger, *Bilişim Suçları ve İnternet Hukuku*, s. 582; Ateş-Benek, s. 389. Yazarlar, temel hak ve özgürlüklere müdahale niteliğinde olan koruma tedbirlerine ilişkin sınırların kanunla düzenlenmesi gerekliliğinden hareket etmektedir.

73 Duran, s. 221.

74 Nevzat Toroslu, Metin Feyzioğlu, *Ceza Muhakemesi Hukuku,* Savaş Yayınevi, Ankara, 2008, s. 214; Centel, Zafer, s. 350. "Şüphe" kavramı, koruma tedbirleri bakımından önemli olduğu gibi ceza muhakemesi evreleri açısından da yani soruşturmanın başlayabilmesi ve kovuşturmaya geçilebilmesi için de önemli bir unsurdur.

75 Öztekin Tosun, *Türk Suç Muhakemesi Hukuku Dersleri Cilt 1 Genel Kısım,* Fakülteler Matbaası, İstanbul, 1981, s. 680; Nurullah Kunter, *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku,* Beta Yayıncılık, İstanbul, 1989, s. 661.

bir koruma tedbirine başvurulmasının haklılığı ancak muhakeme neticesinde anlaşılır. Bu itibarla görünüşte haklılıkla yetinmek gerekir. Aksi kabul, hiçbir koruma tedbirine başvurulamamasını sonuçlar. İşte, haklı görünüş için aranan şüphe derecesi çoğu koruma tedbiri gibi CMK 134'üncü maddesi bakımından da kuvvetli şüphe olarak kabul edilmiştir[76]. Kuvvetli şüphenin varlığı, kişinin isnat edilen suçu işlediği ve büyük ihtimalle hakkında mahkûmiyet kararı verileceği yönünde güçlü bir delilin bulunduğunu ve buna dayanılarak arama kararı verildiğini güvencelemektedir[77]. Yani delil o kadar kuvvetlidir ki ilk görünüşe göre bu delil, büyük ihtimalle mahkumiyete götürecektir. Söz konusu durum, doktrinde; bir soruşturmada hem kuvvetli suç şüphesini gerektiren somut delillerin olması hem de "başka şekilde delil elde etme imkânı bulunmaması" şartlarının birlikte aranmasının çelişkili ve anlam karmaşasına neden olduğu gerekçesiyle eleştirilmektedir[78]. Zira kuvvetli şüphenin varlığı, soruşturma makamının elinde iddianame düzenlenmesine yeter derece delil bulunduğu anlamına gelir[79]. Kanaatimizce kanun koyucu burada CMK 134'üncü maddesinde düzenlenen tedbirlerin arama ve elkoyma koruma tedbirlerinin özel bir görünüşünü oluşturmasından dolayı başvurulmasını sıkı şartlara bağlayarak istisnai niteliğini vurgulamakta ve karar alma mekanizmasındaki hukuk uygulayıcılarının dikkatini bu yöne çekmektedir.

Kuvvetli şüphenin her somut olayda iki yönlü olarak araştırılması gerekir[80]. İlkin, soruşturma ya da kovuşturma konusu suçu şüphelinin işlediği; ikinci olarak da bu kişiye ait bilgisayar verilerinden delil elde edilebileceğine ilişkin olarak kuvvetli şüphe bulunmalıdır. Bu itibarla kişilerin özel hayatlarına müdahale niteliğindeki bu tedbirin uygulanması bakımından sırf bir delil etme imkanının bulunması ile yetinilmemeli, bunun belli bir yoğunluğa ulaşmış olması ihtimali de barındırması ayrıca aranmalıdır. Bu bakımdan tedbir kararının gerekçesinde hangi "somut delillere" dayanılarak karar verildiğinin açıkça belirtilmesi gerekir.

6526 sayılı Kanun ile yapılan değişiklikle, CMK 134'üncü maddesi hükmüne "somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı" deyimi eklenmiştir[81]. Bu ibarenin, bilimsel ve yargısal içtihatların şüphe dereceleri bakımından

76 Öztürk, Eker-Kazancı, Soyer-Güleç, s. 203.

77 Yaşar, Otacı, s. 1113.

78 Yaşar, Otacı, s. 1114; Nurhan Soylu, *Dijital Delillere El Konulması Sürecinde CMK 134. Madde Hükümlerinde Görülen Problemler ve Çözüm Önerileri,* Üsküdar Üniversitesi Bağımlılık ve Adli Bilimler Enstitüsü Adli Bilimler Anabilim Dalı, 2021, s. 140.

79 Soylu, s. 140.

80 Değirmenci, s. 352.

81 Değirmenci, s. 347. Yazar, bu değişiklik öncesinde CMK 134'üncü maddesi bağlamında herhangi bir şüphe derecesine yer verilmemesinin sebebinin, CMK 116'ncı maddesindeki ara-

kabul ettiği "basit, yeterli ve kuvvetli şüphe" kavramları ile beraber okunduğunda hangi manaya geldiği hususunun tereddütlere yol açtığı gerekçesiyle eleştiriye maruz kalmıştır[82]. Bize göre, burada esas vurgulanması gereken, kanun koyucunun temel hak ve hürriyetler açısından ciddi bir müdahale niteliğindeki bu tedbirlerine başvurulurken şüphe sebeplerinin "somut delillerle" desteklenmesini talep etmesidir. Böylece kanun koyucu tarafından, yalnızca görünüşte haklılık ile yetinilmemiş ayrıca maddi gerçeğin bir parçası olan şüphe sebeplerinin ceza muhakemesinde delil olarak kullanılması temin edilmiştir.

C. Başka Şekilde Delil Elde Etme İmkânı Bulunmamalıdır

Ceza muhakemesinde maddi gerçek araştırılırken temel hak ve hürriyetlere en az müdahale oluşturan ve en az sınırlama getiren koruma tedbirlerine başvurulması ölçülülük ilkesinin gereğidir[83]. Her aşamada araçla amacın; yöntemle hedefin muvazene içinde olması aranır[84]. Eğer, klasik koruma tedbirlerine başvurularak delil elde edilebilecek ise bilgisayar verilerinde arama yapılması; bilgisayar verilerinin kopyalanması ve bilgisayar verilerine elkonulması tedbirlerinin uygulanması hukuka aykırılık teşkil eder. Bu itibarla, bilgisayar verilerine ilişkin koruma tedbirlerine başvuracak olan hâkimin öncelikle başka şekilde delil elde imkânı bulunmadığına dair kararına gerekçe yazması gerekir[85]. Nitekim, başka şekilde delil elde etme imkânı bulunmaması koşulu, bu düzenlemenin ikincil ya da akla gelen son çare (ultima ratio) olduğunu gösterir[86]. Ayrıca CMK 134'üncü maddesinin 2'nci fıkrasında *"gecikme olmaksızın iade edilir"*

---

maya ilişkin şüphe derecesi olan makul şüphenin bilgisayar verileri için öngörülen koruma tedbirleri açısından da uygulanması olduğunu belirtmiştir. Gerçekten de arama koruma tedbirinin özel bir görünümünü arz eden bu tedbirler bakımından genel norm niteliğindeki aramaya ilişkin CMK 116 vd. maddelerindeki hükümlerin kıyasen uygulanması söz konusu olmuştur.

82 Duran, s. 222; Özbek, Doğan, Bacaksız, s. 392. Son yazarlar, kuvvetli şüphe sebepleri kavramının kuvvetli şüphe olmadığı; basit ve yeterli şüphe arasında yeni bir dereceyi ifade ettiği; yeni bir şüphe derecesinin belirlenmesi zorunluluğu varsa bunun kanuni bir tanımlama ile yapılmasının yerinde olacağı görüşündedir. Biz de şüphe derecelerinin kanunen belirlenmesi gerektiği yönündeki görüşe iştirak etmekle birlikte, söz konusu koruma tedbirinin tedbiri uygulayanlar açısından sırf delil etme imkânı olduğu gerekçesiyle başvurulamayacak ve fakat somut delillerle makul bir ihtimal seviyesine ulaştıktan sonra başvurulabilecek bir tedbire işaret etmek amacıyla kanun koyucunun şüphe sebepleri kavramını kullandığını düşünmekteyiz.

83 Gökcen, Balcı, Alşahin, Çakır, s. 481.

84 Schroeder, Verrel, s. 97; Kunter, s. 662; Centel, Zafer, s. 351; Toroslu, Feyzioğlu, s. 215.

85 Yenisey, Nuhoğlu, s. 436; Öztürk, Tezcan, Erdem, Sırma-Gezer, Saygılar-Kırıt, Alan-Akcan, Özaydın, Erden Tütüncü, Altınok-Villemin, Tok, s. 523.

86 Özen, s. 766. Yazar, bununla birlikte yaşadığımız teknoloji çağında *"bilgisayarların en kolay delil elde etme yollarından biri olduğunu ve bu tedbirin ikincillik özelliğinin lafzi düzenlemede kaldığını"* haklı olarak belirtmiştir. Bu noktada CMK 134'üncü maddesine soruşturma evresinde cumhuriyet savcısı ve sulh ceza hakimince verilecek kararlar bakımından gerekçeli olma zorunluluğu getirilmesi önerisinde bulunmaktadır. Gerçekten de bu madde kapsamında verilecek kararların hukuka uygunluğunun denetimi açısından gerekçe kritik öneme haizdir.

ifadesine yer verilmesi tedbirlerin geçici niteliğini vurgulamaktayken son fıkrasındaki *"elkoymaksızın da ... verilerin ... kopyası alınabilir"* deyimi oranlılık ilkesine işaret etmektedir[87].

Bilgisayar verilerine ilişkin koruma tedbirleri uygulanırken esas olan, bilgisayar verilerinde arama yapılması; bunların kopyalanması ve soruşturma ya da kovuşturma konusu suça dair "verilere" elkonulmasıdır. Dolayısıyla kural olarak, bilgisayara, sistemlerine veya kütüklerine elkoyma olmaksızın uygulanmalıdır. İstisnai olarak, "şifrenin çözülememesi sebebiyle sisteme girilememesi; gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması[88] hallerinde" şifrenin çözümünün yapılması ve gerekli kopyaların alınması işlemlerinin yapılmasıyla sınırlı biçimde ve gerekçe göstermek suretiyle bu araç ve gereçlere elkonulabilir[89]. Nitekim bu işlemlerin yapılması halinde elkonulan cihazların derhal iade edilmesi gerekir[90]. Bu ölçülülük ilkesinin bir gereğidir. Fakat, bazı suçlar bakımından cihazların iade edilmesi mahzurlu sonuçlar doğurabilir. Mesela, TCK 245'inci maddesi uyarınca yapılan soruşturma ya da kovuşturmada yapılan elkoymanın konusu olan içerisinde mağdurların kredi kartı bilgilerinin olduğu bilgisayarın iade edilmesi gibi. Doktrinde bu hallerde eşya müsaderesi uygulanabileceği haklı olarak ifade edilir[91]. Bize göre, uygulamada adeta bir kural olarak uygulanan söz

87 Baştürk, s. 27.

88 İşlemin uzun sürecek olması nedeniyle bilgisayara, sistemlerine veya kütüklerine elkonulabilmesi istisnası, 7145 sayılı ve 25 Temmuz 2018 tarihli Kanun ile yapılan değişiklikten sonra CMK 134'üncü maddesine eklenmiştir. Biz, bu istisnanın dikkatle uygulanması gerektiği düşüncesindeyiz. Nitekim, içerisinde milyonlarca veri barındıran bilgisayarların aranması ve kopyalanması işlemleri belli bir zamanı alır. Neredeyse her siber suçta birden fazla cihazla muhatap olan kolluk görevlilerinin bu istisnai gerekçeye dayanarak tüm araç gereçlerle ilgili olarak elkoyma işlemi yapması mümkündür. Böylesi bir uygulama kanun koyucunun ayrıca ve açıkça sıkı şartlar öngörerek düzenlediği CMK 134'üncü maddesinin uygulanmayarak genel elkoyma hükümlerinin uygulanmasını sonuçlayacaktır. Bu bakımdan elkoyma işleminin ölçülülük ilkesine ve nihayet hukuka uygun olduğunun denetlenebilmesini sağlamak üzere kolluk görevlilerince her somut olayda; neden elkoyma işlemine başvurulduğu ayrıntılı olarak tutanaklara yazılmalı ve bu durum şüpheli ya da sanık ve işlem tanıkları ile imza altına alınmalıdır.

89 CGK 25.02.2020 tarih ve E. 2016/8-544 K. 2020/127 sayılı kararında; *"bilişim sisteminin işleyişini engelleme veya bozma suçundan yapılmakta olan soruşturmada CMK 134'üncü maddesi uyarınca verilen karar doğrultusunda yapılan aramada sabit disklerin ele geçirildiği, bu materyallerin ardından sebebi belirtilip bu husus tutanağa geçirilmeden ve mahallinde sistemdeki bütün verilerin yedeklemesi yapılmadan söz konusu sabit disklere el konularak teknik inceleme için İstanbul Emniyet Müdürlüğü, Asayiş Şube Müdürlüğü, Ar-Ge Büro Amirliği'ne getirildiği, kural olarak bulundukları mahalde incelenmeleri gereken suça konu sabit disklere hem CMK 134'üncü maddesi hem de objektif olarak kabulü gereken zorunlu sebebe bağlı bir gerekçe gösterilmeden elkonulamayacağına"* hükmedilmiştir. Kararın tam metni için bkz. Kazancı İçtihat Bilgi Bankası, https://lib.kazanci.com.tr/kho3/ibb/files/dsp.php?fn=cgk-2016-8-544.htm&kw=%602016/8-544%60+&cr=yargitay#fm (27.09.2024).

90 Özbek, Doğan, Bacaksız s. 394; Gökcen, Balcı, Alşahin, Çakır, s. 480.

91 Öztürk, Kazancı, Güleç, s. 205. Yazarlar, ayrıca bu durumlar için kanuni düzenleme yapılmasının gerekliliğine işaret etmiştir.

konusu istisnai haller olmaksızın her somut olayda bilgisayara, sistemlerine veya kütüklerine elkoyma işlemi yapılması, "hukuka aykırılık" teşkil etmekte ve ele geçirilen delillerin de "yasak delil" mahiyetinde olması nedeniyle açıkça maddi gerçeğe ulaşılmasını ve suçlulukla mücadeleyi engeller niteliktedir. Olması gereken, tedbir kararı alınırken de tedbirler uygulanırken de ölçülülük ilkesinin unsurları olan elverişlilik, gereklilik ve oranlılık hususlarının varlığının aranmasıdır. Aksi hal, elde edilen delillerin ceza muhakemesinde kullanılamamasını sonuçlar.

V. Karar Vermeye Yetkili Merci

Tedbirlere başvurulabilmesi için Cumhuriyet savcısının talebi ve hâkim kararı gereklidir. Söz konusu tedbirlerin mülkiyet gibi temel hak ve özgürlüklere kısıtlama getirmesi bakımından yalnızca hâkim kararıyla uygulanabilmesi güvenceli olmuştur. Burada hâkim ile kastedilen CMK 162'inci maddesi uyarınca sulh ceza hâkimidir[92]. Verilecek karar, CMK 134'üncü maddesi gereğince şüphelinin kullandığı bilgisayarlarda, sistemlerde ve kütüklerde "arama yapılması", bunlardan "kopya çıkarılması" ve "bu kayıtların çözülerek metin haline getirilmesi" işlemlerine yöneliktir. Hâkim kararında bu işlemlere ayrıca ve açıkça yer verilmemişse genel nitelikteki bir arama kararıyla ilgili tedbirlere başvurulması imkân dahilinde değildir.

7145 sayılı Kanun ile yapılan değişiklikle, "gecikmesinde sakınca bulunan hallerde" Cumhuriyet savcısı tarafından[93] da tedbirlere ilişkin olarak karar verilebileceği düzenlenmiştir. Söz konusu karar, yirmi dört (24) saat içinde hâkim onayına sunulur. Hâkim, kararını en geç yirmi dört (24) saat içinde açıklar. Sürenin dolması ya da hâkim tarafından aksine karar verilmesi durumlarında çıkarılan kopyalar ve çözümü yapılan metinler hemen imha edilir. Bu noktada ifade edilmelidir ki "gecikmesinde sakınca bulunan hal" olmaksızın tedbirlere başvurulması gerek tedbir kararının kendisini gerekse de tedbir uygulanarak ele geçirilen delilleri hukuka aykırı hale getirir[94]. Dolayısıyla Cumhuriyet savcısının bu istisnai yetkiyi kullanabilmesi için hâkimden karar talep etmesi halinde tedbirlerin uygulanamaz hale gelmesi ya da tedbirlerden beklenen faydanın elde edilememesi tehlikesiyle karşılaşması gerekir. Cumhuriyet savcısı, her somut olayda denetime imkân verecek şekilde hâkim kararı almasının gecikmeye sebebiyet vereceğini, bunun da sakınca doğuracağını düşündüren bilgi ve bel-

92 Duran, s. 224; Yusuf Başlar, "Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri", *UMD,* Cilt 3, Sayı 3, 2013, s. 90.

93 Baştürk, s. 28. Yazar, Cumhuriyet savcısının "gecikmesinde sakınca bulunan hallerde" tedbir uygulaması için izin vermeye yetkili kılınmasını "sınırlamanın hakim kararıyla yapılabileceği" unsuru yönünden uygun olmayacağını ifade etmektedir.

94 Schroeder, Verrel, s. 97; Centel, Zafer, s. 350.

gelere kararında yer vermelidir. Bu kararda ayrıca ve açıkça arama ve elkoyma tedbirlerine başvuracağı belirtilmelidir. Nitekim, arama ve elkoyma tedbirleri arasında tedbirin ağırlığı ile öncelik ve sonralık yönünden fark bulunur. Kanun koyucu, bu hiyerarşiyi dikkate alarak öncelikle "özel arama" hükmü nitelindeki CMK 134'üncü maddesinin 1'inci fıkrasını ihdas etmiş; bu koruma tedbiri ile amaca ulaşılamaması halinde uygulanmak üzere CMK 134'üncü maddesinin 2'nci fıkrasında "özel elkoyma" hükmünü düzenlemiştir. Bu tedrici düzenleme dikkate alınmaksızın kolluk görevlilerince uygulama yapılırsa elde edilen delillerin ceza muhakemesinde kullanılması mümkün olmaz. Çünkü, ölçülülük ilkesinin bir gereği olarak bilgisayarlarda veya programlarında ya da kütüklerinde bulunması umulan bir delilin genel bir arama kararı ile ele geçirilmesi, özel nitelikteki arama veya elkoyma tedbirlerinin uygulanma gerekliliğini ortadan kaldırır[95]. Ancak, doktrinde elkoyma ihtiyacının kanunda sayılan hallere münhasır olmadığı; mesela, terör ya da örgütlü suçlarda olay yerinin fiziksel güvenliğinin teminiyle alakalı problemler çıkabileceği veya fiziksel ortamda kesintisiz enerji temin sorunu yaşanabileceği gerekçesiyle genel bir elkoyma nedenine kanunda yer verilmesi gerektiği ileri sürülmüştür[96]. Biz, bu ihtimallerde genel elkoyma kararıyla da bu neticeye ulaşılabileceğinden dolayı zikredilen görüşe iştirak etmemekle birlikte elkoyma tedbirini uygulayan makamların hukuka aykırılık iddialarının önüne geçmek için titizlikle davranması, bilişim sistemlerinden delil elde edilmesine yönelik düzenlemenin dereceli yapısına uygun ve ölçülülük ilkesini esas alan bir pratiğin oluşturulması gerektiğini düşünmekteyiz. Ayrıca kanun değişikliği öncesinde cumhuriyet savcılarına ya da kolluk görevlilerine bu yetkinin verilmemesi ve söz konusu tedbirlere yalnızca hâkim kararıyla başvurulabilmesinin altında yatan gerekçe bilgisayar verilerinin tahrifata ve sahte delil üretimine açık yönleri olmuştur. Bununla birlikte temel hak ve özgürlükler bağlamında kanuna eklenen hüküm, cumhuriyet savcısınca verilecek tedbirlere ilişkin kararların hâkim tarafından denetime elverişliliği cihetiyle yerindedir[97].

95 Yaşar, Otacı, s. 1115. Yazarlar, arama ile bulunması umulan delilin silinmiş, dosya yolu değiştirmiş ya da çeşitli sebeplerle hemen ulaşılması mümkün bir şekilde bulunmadığı durumlarda bilgisayarın adli kopyasının alınması gerekliliğinin doğduğunu haklı olarak belirtmektedir.

96 Mehmet Bedii Kaya, "Hukuki Açıdan Bilişim Suçları, Siber Güvenlik ve Adli Bilişim", Ed. Şeref Sağıroğlu, Mustafa Şenol, *Siber Güvenlik ve Savunma Problemler ve Çözümler,* Grafiker Yayınları, Ankara, 2019, s. 267.

97 Özen, s. 764. Yazar hem hâkim kararıyla tedbire başvurulmasının hem de cumhuriyet savcısı tarafından verilecek kararların hâkim onayına sunulmasının oldukça isabetli olduğunu haklı olarak ifade etmektedir.

VI. Uygulama

Birçok temel hak ve hürriyete henüz mahkûmiyet hükmü verilmezden önce doğrudan doğruya müdahale oluşturan koruma tedbirlerinin uygulama sınırlarının çizilmesi keyfiliğin önlenmesi bakımından önemlidir[98]. CMK 134'üncü maddesinde öngörülen sistem, öncelikle suç delili olarak kullanılabilecek bilgisayar verilerinin elde edilerek bunların zarar görmemesi ve manipüle edilmemesi açısından muhafaza altına alınmasını öngörür. Söz konusu elektronik nitelikteki verilen üzerinde yapılacak inceleme, veri kayıplarının da önlenmesi adına donanımlar üzerinde değil, bunlardan alınan kopyalar (imajlar) üzerinde yapılır[99]. Buna göre, bilişim konusunda uzman kolluk görevlilerince kural olarak, bilgisayara, sistemlerine veya kütüklerine elkoyma olmaksızın sistemdeki verilerin tamamının yahut bir kısmının kopyası alınabilecek; kopyası alınan ve suçla ilgili olan veriler kâğıda yazdırılacak[100]; bu husus tutanağa kaydedilerek ilgililerce imza altına alınacaktır. Bu itibarla, arama ve kopyalama tedbirlerinin uygulanması amacıyla elektronik cihazların bulundukları yerlerden elkoyma suretiyle alınarak bir diğer yere taşınmaları gerekmez[101]. Bununla birlikte "adli bilişim" uzmanlar tarafından titizlikle yürütülmesi gereken ayrı bir alana karşılık gelmektedir. Adli bilişim uygulaması; "ön inceleme ve olay yeri tespiti", "delil toplama", "analiz" ve "raporlama" olmak üzere dört ana adımdan oluşmaktadır[102]. Bu safhaların kimi zaman saatler kimi zaman da gün boyu

98 Hakan Serdar Çöpoğlu, "Ceza Muhakemesi Hukukunda Arama Koruma Tedbirinde Belirlilik İlkesi", *ABD,* Cilt 77, Sayı 1, 2019, s. 163. İnsan hakları açısından uygulamada koruma tedbirlerine bir kontur oluşturma gayreti, "kanunilik" ilkesinin gereği olan "belirlilik" ilkesinin bir tezahürüdür. Gerçekten de çalışma konumuz CMK 134'üncü maddesi hükmünde yer alan koruma tedbirlerinin ne zaman, kimin tarafından, nerede ve ne şekilde yerine getirileceğinin açık, net ve anlaşılabilir şekilde ortaya konulması vatandaşlar nezdinde hukuk devleti ve kanunilik ilkesine işlerlik kazandıracağı gibi uygulamacılar bakımından da tereddütlerin ortadan kalkmasına hizmet edecektir.

99 Duran, s. 225.

100 Metin haline getirme unsuru bakımından günümüzde bilişim sistemlerinin hemen her yerde ve çoğu işte kullanıldığı düşünüldüğünde zamana ve maliyete mal olabilecek binlerce hatta on binlerce sayfalık çıktılarla karşılaşılacağı; harici aygıtlara yüklenilecek verilerden aranılan bilgiye ulaşmanın daha kolay olacağı ve bu yönüyle kanun maddesindeki metin haline getirme ifadesinin işlevsiz olduğu haklı olarak belirtilmektedir. Baştürk, s. 29.

101 Baştürk, s. 29; Ünver, Hakeri, s. 939. Son yazarlar, CMK 134'üncü maddesinin 5'inci fıkrasından hareketle bilgisayarlara elkoymaksızın verilere erişmenin mümkün olduğu hallerde bilgisayarların tamamına elkoyma işlemi uygulanarak kişilerin şahsi veya ticari kullanımına engel olunmamasının amaçlandığını haklı olarak ifade etmektedir.

102 Özen, Özocak, s. 51 ve 52. Yazarlar, adli bilişim sürecinde; *"delillerin bulunduğu ortamın boşaltılması ve kamera ile sürecin takip edilmeye başlanması; delillerin toplanması bağlamında, plastik eldivenler vasıtası ile gerekli bilgisayarın açılması, açılış sürecinin analizi, açılmışsa o anki durumunun tayini, var olan kablosuz bağlantıların hemen tespit edilip kapatılıp kapatılmayacağına karar verilmesi, gerekli delil toplama işlemlerinin üstün yetenekli programlar vasıtası ile yapılması ve bilgisayarın kapatılması süreçlerinin tamamının,*

sürebildiği; tedbirin muhatapları ve uygulayıcılar bakımından çeşitli zorlukları barındırdığı düşünüldüğünde bütün adımların adli bilişim uzmanları tarafından yerine getirilmesi ve bilişim sistemlerinden delil elde edilirken elektronik delillerin bütünlüğünün korunması gerekliliği daha da ön plana çıkmaktadır.

Ayrıca kopyalama işlemi cihazlardaki tüm verilere ilişkin olarak değil, ileride delil olarak kullanılabileceği umulan ve suçla alakalı olduğu düşünülen verilere ulaşmak amacıyla sınırlı olarak yapılır. Şayet, suçla alakası kesin olarak bulunmayan kişisel veriler kasten kopyalanırsa bu işlemi gerçekleştiren kişiler TCK'da düzenlenen "özel hayata ve hayatın gizli alanına karşı" suçların tipikliğini ihlal etmiş olur[103]. Zira tedbirlere ilişkin yapılan yasal düzenlemenin esas amacı, kişisel verilerin korunması olmalıdır[104]. Bu noktada ifade etmeliyiz ki tedbirlerin uygulanması esnasında bilgisayara, sistemlerine veya kütüklerini alelade elinde bulunduran (zilyet yardımcısı) veya zilyet ya da malik olan şüphelinin; bulunmaması halinde müdafi, kanuni temsilci, eş, aileden yahut komşulardan birinin; bunlar da yoksa muhtar yahut ihtiyar heyetinden birinin arama tanığı olarak işlemlere nezaret etmesi elzemdir. Bu konuda CMK 134'üncü maddesinde hüküm bulunmamakla birlikte, boşluk genel arama hükümlerine göre doldurulmalıdır[105].

Bununla birlikte, istisna olarak, bilgisayara, sistemlerine veya kütüklerine "şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması" durumlarında çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi amacıyla bunlara ilişkin elkoyma tedbiri uygulanabilir. Şifrenin çözümlenmesi ve gerekli kopyaların alınması durumunda vakit geçirilmeksizin elkonulan cihazlar iade edilir. Elkoyma tedbiri uygulanırken bilişim sistemindeki tüm verilerin yedeklemesi yapılır. Zikredilen işleme "verilerin özet-kriptografik hash değerinin çıkarılması" denmektedir. Uygulamada bu işlem bakımından açık bir hatanın yapıldığı da gözlenmektedir. Zira elkoyma işlemi sırasında yapılması gereken hash değerinin çıkarılması işlemi elkoyma gerçekleştikten sonra yapılmaktadır[106]. Elkoyma ve hash değeri çıkarma işlemlerinin eşanlı olarak yapılmaması, elde edilen elektronik delillerinin güvenirliği üzerinde etkili olmakta ve ispat sorunlarını

---

adli birimler tarafından belirlenmiş sistematiğe göre yapılıp raporlanması; elde edilen delillerin, programlar vasıtası ile incelenmesi ve gerekiyorsa şifre çözme yöntemleri kullanılması; analiz sonucu ortaya konulan raporun, adli birimlere, anlaşılır bir biçimde ve teknik terimlerden gerektiğince kaçılarak sunulması" gerektiğini ifade etmektedir.

103 Centel, Zafer, s. 449; Yenidünya, İçer, s. 454.

104 Duran, s. 226.

105 Özen, s. 768; Ünver, Hakeri, s. 981; Özbek, Doğan, Bacaksız, s. 350. Aksi takdirde deliller, hukuka aykırı yöntemle elde edilmiş olup ceza muhakemesinde kullanılamaz.

106 Baştürk, s. 30.

beraberinde getirmektedir[107]. Nitekim CMK 134'üncü maddesi 4'üncü fıkrası hükmü gereğince; CMK 134'üncü maddesi 3'üncü fıkrasına göre elkoyma işlemi sırasında alınan yedekten bir kopya çıkarılarak şüpheliye yahut müdafiine verilmesi[108] ve bu hususun tutanağa geçirilerek imza altına alınması[109] uygulamada ortaya çıkabilecek problemleri bertaraf etmek üzere kanun koyucu tarafından öngörülmüştür.

Bilgisayarda, sistemlerinde veya kütüklerinde arama, kopyalama ve elkoyma tedbirleri uygulanırken bunlara konu suç ile alakalı olmayan ve fakat başka bir suç ile alakalı "tesadüfen delil elde edilmesi" halinde nasıl davranılacağı

---

107 Yargıtay 11'inci Ceza Dairesi'nin 16.04.2007 tarih ve E. 2005/6376 K. 2007/2551 sayılı kararında; *"... gerçeğin kuşkuya yer vermeyecek şekilde belirlenmesi açısından; öncelikle e-posta yolu ile virüs göndererek sistemine zarar verilmiş bir bilgisayarda incelemenin, olayın hemen akabinde yapılması yada inceleme yapılacak bilgisayarın veya bilgisayara ait veri içeren ünitelerin, olaydan sonra inceleme yapılana kadar hiç kullanılmaması gerektiği, incelenecek bilgisayarın diskine bazı bilgilerin yazılması, değişmesi veya silinebilmesini önlemek ve söz konusu diskin bütünlüğünü sağlamak için bilgisayarda virüslü dosya üzerinde inceleme yaparken ilk işlem olarak, söz konusu dosyanın birebir (sector-by-sector) yedeğinin alınması (yani incelemenin orijinal dosya üzerinde yapılmaması), daha sonra ikinci olarak alınan birebir yedeğin değiştirilip değiştirilmediğini tespite yarayacak zaman ve bütünlük kontrolü imkanı sağlayan değerin (hash belirlenmesi)"* gerektiğine hükmedilmiştir. Kararın tam metni için bkz. Kazancı İçtihat Bilgi Bankası, https://lib.kazanci.com.tr/kho3/ibb/files/dsp.php?fn=11cd-2005-6376.htm&kw=%602005/6376%60&cr=yargitay#fm (28.09.2024).

108 6526 sayılı Kanun değişikliği öncesinde, alınan kopyadan bir örneğinin şüpheli ya da müdafiine "istemesi halinde" verilmesi söz konusuyken; değişiklik sonrasında ilgililerin istemesi şartı aranmaksızın re'sen yedekten bir kopya verilir. Bu değişiklik, ilgililerin bilgisayar verilerinin güvenilir olmadığı; manipüle edildiği; verilere ekleme ya da çıkarma yapıldığı; sahte delillerin üretildiği şikayetlerinin önlenmesi ve böylece savunma hakkının güvenceye alınması açısından yerinde olmuştur. Öztürk, Eker-Kazancı, Soyer-Güleç s. 205. Ayrıca değişiklik gerekçesinden de anlaşıldığı üzere, söz konusu iddialar gündeme geldiğinde yedekler arasında karşılaştırma imkanı sağlanmıştır. Fakat, ifade etmeliyiz ki uygulamada kolluk görevlilerinin arama mahallinde uzun süreceği istisnasına dayanarak cihazlara elkoyduğu ve günler geçtikten sonra alınan yedeklerden bir kopyanın ilgililere verildiği söylenebilir. Bu durum, halen kişilerin cihazlara müdahale edildiği yakınmalarına sebep olmaktadır. Yapılması gereken, olay mahallinde yedekleme işlemlerinin tamamlanarak ilgililere kopyadan bir örnek verilmesidir. Bununla birlikte doktrinde; uygulamaya yönelik eleştiriler dikkate alınarak değişiklik yapılacağı yerde uygulamaya uygun kanun değişikliği yapıldığı, bu durumun da CMK 134'üncü maddesinde düzenlenen kurumu etkisizleştireceği ve doğrudan elkoyma işleminin uygulanmasına yol açacağı şeklinde eleştiriler yapılmaya devam edilmektedir. Ayrıntılı bilgi için bkz. Ünver, Hakeri, s. 943 vd.

109 CGK 25.02.2020 tarih ve E. 2016/8-544 K. 2020/127 sayılı kararında; *"bilişim sisteminin işleyişini engelleme veya bozma suçundan yapılmakta olan soruşturmada CMK 134'üncü maddesi uyarınca verilen karar doğrultusunda yapılan aramada yedekleme yapılıp bir kopya çıkartılarak arama sırasında hazır bulunan sanığa verilmesi gerektiğinin gözetilmemesi suretiyle CMK 134'üncü maddesinin 3'üncü ve 4'üncü fıkralarına aykırı hareket edilmesi sebebiyle usulüne uygun olmayan elkoyma işlemi sonucu suça konu sabit disklerden elde edilen verilerin hukuka aykırı olarak elde edilen delil niteliğinde olduğuna"* hükmedilmiştir. Kararın tam metni için bkz. Kazancı İçtihat Bilgi Bankası, https://lib.kazanci.com.tr/kho3/ibb/files/dsp.php?fn=cgk-2016-8-544.htm&kw=%602016/8-544%60+&cr=yargitay#fm (28.09.2024).

hususu ayrıca değerlendirilmelidir. CMK 134'üncü maddesi, özel bir arama ve elkoyma hükmü olarak ihdas edildiği için, işlemler esnasında "tesadüfen elde edilen" deliller hakkında CMK 138'inci maddesinde öngörülen yöntem burada da uygulanabilir[110]. Buna göre, deliller muhafaza altına alınmalı ve Cumhuriyet savcısı durumdan derhal haberdar edilmelidir. Ayrıca kayıtların muhafaza altına alınmasını müteakiben bilgisayar, sistemleri veya kütükleri de CMK 127'nci maddesi uyarınca suçun işlenmesinde kullanılan araç kabul edilerek bunlar hakkında elkoyma işlemi uygulanabilir[111].

VII. İtiraz

CMK 134'üncü maddesi, sulh ceza hakimince alınan tedbir kararlarının incelenebilmesi için herhangi bir denetim mekanizması öngörmemiştir. Bu sebeple genel hükümler çerçevesinde hareket etmek gerekir. Nitekim CMK 267'nci maddesinde soruşturma aşamasında sulh ceza hakimince verilen tedbir kararları hakkında "itiraz" kanun yolunun açık olduğu belirtilmiştir[112]. Bununla birlikte, koruma tedbirlerine ilişkin kararın tebliği söz konusu olmayacağından ve ilgililer karardan ancak uygulanmasıyla haberdar olacaklarından[113] yedi (7) günlük itiraz süresi[114] de bu tarihten itibaren işlemeye başlar[115] ve bu süre içerisinde kararı veren yetkili mercie yapılır[116]. İfade etmeliyiz ki kovuşturma evresinde de bu tedbirlere başvurabileceğini kabul ettiğimizden kovuşturma aşamasında da mahkemenin ara kararlarına karşı itiraz kanun yolunun açık tutulması gerekir[117]. Gerçekten de tedbirler açısından itiraz yolunun varlığı, mesela bilgisayarına el konulduğunda ya da müdahale edilmeden yani bilişim sisteminde bulunan verilere erişilmeden karara karşı etkin bir denetleme mekanizmasının bulunması hukuk devleti ilkesinin doğal bir sonucu olarak kar-

110 Özen, s. 768; Yenidünya, İçer, s. 455.

111 Ünver, Hakeri, s. 944; Öztürk, Eker-Kazancı, Soyer-Güleç s. 206.

112 Centel, Zafer, s. 450; Özbek, Doğan, Bacaksız, s. 396; Baştürk, s. 32; Epözdemir, s. 94.

113 Ateş-Benek, s. 406.

114 02.03.2024 tarihli ve 7499 sayılı Kanun'un 37'nci maddesi ile CMK 268'inci maddesinin 1'inci fıkrasında yer alan "yedi gün" ibaresi "iki (2) hafta" şeklinde değiştirilmiştir.

115 Yenisey, Nuhoğlu, s. 435; Centel, Zafer, s. 450; Duran, s. 233.

116 Şahin, Göktürk, *Ceza Muhakemesi Hukuku II*, s. 253; Değirmenci, s. 381.

117 Yenidünya, İçer, s. 456. Doktrinde mahkeme kararlarına itirazın mümkün olmadığını ifade eden yazarlar bulunmaktadır; Özen, s. 768. Benzer bir görüş, koruma tedbirlerinin kanunilik ilkesine tabi olması nedeniyle bu hususta kanuni düzenleme yapılmasına ihtiyaç olduğunu belirtmiştir; Ünver, Hakeri, s. 948. Başka bir görüş, kanunda ister yazılı olsun ister yazılı olmasın itiraz kanun yoluna tüm "hakim kararlarına karşı" gidilebileceğini; ancak itiraz kanun yoluna "mahkeme kararlarına karşı" gidilebilmesi adına bunun kanunda mutlaka zikredilmesi gerektiğini ifade etmektedir; Ahmet Hulusi Akkaş, "Ceza Muhakemesinde İtiraz Kanun Yolunun Teorik Çerçevesi", *ERÜHFSD,* Cilt 1, Sayı 2, 2019, s. 50. Bu noktada ifade etmek isteriz ki söz konusu görüşler, CMK 267'nci ve devamı maddelerinde açıkça karşılığını bulmaktadır.

şımıza çıkar. Ne var ki kanunda bu konuda açık bir düzenleme yapılmamıştır.

Cumhuriyet savcısı tarafından da istisnai olarak, "gecikmesinde sakınca bulunan hallerde" arama, kopyalama ve elkoyma tedbirlerine karar verilebilir. Bu karar, yirmi dört (24) saat içinde hâkim onayına sunulur. Hâkim, kararını en geç yirmi dört (24) saat içinde açıklar. Sürenin dolması ya da hâkim tarafından aksine karar verilmesi durumlarında çıkarılan kopyalar ve çözümü yapılan metinler hemen imha edilir. Ayrıca elkonulan araç ve gereçlerin iadesi bakımından bunların müsadereye tabi olmayacağının anlaşılması ve muhafazasına gerek kalmaması hallerinde ilgililerin talebi yahut re'sen karar verilebilir. İade kararı kesin olmakla beraber, iadenin reddine dair karara karşı CMK 267'nci maddesine kapsamında itiraz edilebilir[118].

Sonuç

Açıkça ifade edelim ki ceza muhakemesinde bilişim sistemlerinden delil elde edilmesine ilişkin işlemlerin değerlendirilmesi söz konusu olduğunda hem teori hem de uygulama açısından zor ve önemli bir alana giriş yapılmış olmaktadır. Buradaki esas zorluk, kanaatimizce söz konusu tedbirlerin uygulanmasına ilişkin karar alan ve uygulayan makamların ispat ve delil kavramlarına yönelik geleneksel ve korumacı yaklaşımlarından kaynaklanmaktadır. Önemli olan kısmın ise belli bir süredir ülkemizde bu tedbirlerin uygulanışından kaynaklanan pratiğe ilişkin verilerin doktrin tarafından diğer ülke uygulamalarıyla karşılaştırılması ve kanuni düzenlemelerde ceza muhakemesine hâkim olan evrensel ilkeler doğrultusunda değişikliklere ve bunun neticesi olarak uygulamada iyileştirmelere gidilmesi fırsatını bünyesinde barındırması olduğunu düşünmekteyiz.

Ceza muhakemesinde hakikat (maddi gerçek) araştırılırken kişilerin temel insan haklarını kısıtlayan koruma tedbirlerine başvurulabilmektedir. Bunların en önemlilerinden birini de CMK 116'ncı ve devamı maddelerinde hüküm altına alınan arama ve elkoyma tedbirleri oluşturmaktadır. Siber suçlar hakkında neredeyse tek delil elde yöntemini oluşturan ve dijital (diğer ifadeyle sayısal veya elektronik) materyaller üzerinde gerçekleştirilen arama ve inceleme işlemleri CMK 134'üncü ve Adli ve Önleme Aramaları Yönetmeliği 17'nci maddesi hükümlerine göre yapılmaktadır. Bununla birlikte; söz konusu koruma tedbirine başvurulması, temel insan haklarına ve bilhassa özel hayata müdahale oluşturması nedeniyle biri olumlu biri olumsuz nitelikte iki sıkı koşula bağlanmıştır. Bunlar; "somut delillere dayanan kuvvetli şüphe sebeplerinin olması" ve "başka surette delil elde etme imkanının olmaması" biçiminde tezahür

118 Değirmenci, s. 381.

etmektedir. Böylece kanun bu koruma tedbirine başvurulmasını zorlaştırmak istemiştir. Tedbirin uygulandığı hallerde de titizlikle davranılması gerekmektedir. Aksi takdirde ele geçirilen deliller hukuka aykırı toplanmış olacağından ispat aracı olarak kullanılamayacaktır.

Ayrıca temel haklar bakımından doğurduğu sakıncalara rağmen kanun koyucu tarafından herhangi bir suç kataloğuna yer verilmemesi ve gerek siber suçlar gerekse diğer suçlar bakımından bu tedbirin uygulanması, özellikle mesleki uğraşları nedeniyle bilişim sistemlerini ve araçlarını kullananların maddi zarar ve mağduriyetlerine neden olacak niteliktedir. Olması gereken açısından doktrinde kanun koyucu tarafından siber alanda işlenebilecek suç kataloğunun oluşturularak kanuna dahil edilmesi gerektiği ileri sürülse de biz, esas çözümün her koruma tedbiri bakımından katalog suç listesi tutmaktansa hukuk uygulamacılarının tedbir kararı verirken yapacakları değerlendirmelerde ölçülülük ve akla gelen son çare olma ilkeleri ekseninde temel insan hakları ile koruma tedbirinin uygulanmasından beklenen fayda arasında bir denge tutturmasından geçmekte olduğunu düşünmekteyiz.

Yine elkoyma tedbiri bakımından uygulamada bunun istisnai ve geçici niteliğini bertaraf edecek bir pratiğin geliştiğini ifade etmek gerekmektedir. Uzman personel (adli bilişim uzmanı, olay yeri inceleme ekibi vs.) yetersizliği, teknik imkansızlıklar ve iş yükü gibi gerekçelerle pratikte bu tedbire çok fazla başvurulmaktadır. Dolayısıyla kanunda ayrıca ve açıkça öngörülen istisnai şartlar oluşmaksızın elkoyma tedbirine başvurulması hukuka aykırılık teşkil edecektir[119]. Bu netice bir yönüyle suç ve suçlulukla mücadeleyi engellerken diğer bir yönüyle de toplumdaki bireylerin temel hak ve özgürlükleri bakımından sakıncalar doğurmaktadır. Olması gereken, hukuk uygulamacıları ve delil

119 Yargıtay 16'ncı Ceza Dairesi 10.10.2019 tarih ve E. 2019/2637 K. 2019/5904 sayılı kararında dijital delillerin hukuka uygun yöntemlerle elde edilmesi gerekliliğinin önemi ve uygulamada meydana gelen sıkıntılar ile bunların sebeplerine ilişkin olarak; *"Ceza muhakemesinde deliller kanuna uygun olmalı ve kanuna uygun yöntemlerle elde edilmelidir. Adil yargılanmanın sağlanabilmesi, soruşturma ve kovuşturma aşamalarında toplanan bulguların delil değeri taşıyabilmesi için, şüpheli veya sanıktan elde edilen dijital verilerin, yasa ile sınırları belirlenmiş teknik gerekliliklere uygun olarak toplanması ve sonucunda yargılama makamlarına eksiksiz, bozulmamış halde sunulması gerekmektedir. Yasa koyucunun, CMK'nın 134. maddesini ayrıntılı olarak düzenlemesinin amacı da budur. Dijital delillere harici müdahalenin teknik olarak mümkün olması, çoğu zaman kim tarafından hangi tarihte müdahale yapıldığının da belirlenememesi karşısında, güvenli bir şekilde el konulup incelenebilmesi için mahallinde imaj alındıktan sonra orijinal medyanın şüpheliye bırakılması gerekmekte ise de bu şart soruşturma yapan kolluk personelinin teknik yetersizliği, ekipman yokluğu, ortamın incelemeye elverişli olmaması gibi nedenlerle yerine getirilememektedir."* şeklinde ifadelere yer vermektedir. Kararın tam metni için bkz. Kazancı İçtihat Bilgi Bankası, https://lib.kazanci.com.tr/kho3/ibb/files/dsp.php?fn=7cd-2023-18292.htm&kw=%60cmk+134%60+%60bilgisayar%60&cr=yargitay#fm (28.09.2024).

elde edilmesine yönelik işlemleri gerçekleştiren personelin ispat ve delil kavramlarına yönelik konvansiyonel ve korumacı yaklaşımların ötesine geçerek bilişim sistemlerinden delil elde edilmesine ilişkin işlemlerin düzenlendiği CMK 134'üncü madde hükümlerini doğru bir şekilde yorumlamaları ve insan hakları ihlallerine sebebiyet verebilecek yanlış bir tutumdan kaçınmalarıdır. Siber alanın ve bilişim sistemlerinin günlük hayatımızda gün geçtikçe artan kapsama alanına rağmen, buralardan delil elde edilmesine yönelik işlemlerin CMK'da tek bir madde ile karşılanması, yeterli kapsayıcılıkta bir düzenleme olmadığı gerekçesiyle haklı eleştirilere maruz kalmaktadır. Ayrıca yapılacak yasal değişiklikler için yasama organına; uygulamada yapılacak yorumlar için yargı organına ışık tutmak üzere karşılaştırmalı hukuktaki düzenlemeler ve bilhassa Avrupa Siber Suç Sözleşmesi'nin bilişim sistemlerinden delil elde edilmesi ve korunmasına ilişkin hükümlerinin yol gösterici mahiyette olduğunu düşünmekteyiz. Hızla genişlemesini sürdüren bilişim alanındaki suçlar için uzmanlık mahkemelerinin kurulması ve bu alanda bilgi sahibi hukukçu ve personellerin yetiştirilmesi gerekliliğini de ifade etmek isteriz.

KAYNAKLAR

- Akkaş, Ahmet Hulusi, "Ceza Muhakemesinde İtiraz Kanun Yolunun Teorik Çerçevesi", *Erciyes Üniversitesi Hukuk Fakültesi Sempozyum Dergisi,* Cilt 1, Sayı 2, 2019, ss. 45-70.
- Akkuş, Berkant, "Devletin Etkin Kontrolünün Bulunmadığı Siber Alanda İnsan Hakları Yükümlülükleri Nelerdir?" *Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi Dergisi,* Cilt 6, Sayı 1, 2024, ss. 159-214.
- Allah Rakha, Naeem, "Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations", *Mexican Law Review,* Cilt 16, Sayı 2, 2024, ss. 23-54.
- Arslan, Çetin, "Dijital Delil ve İletişimin Denetlenmesi", *Ceza Hukuku ve Kriminoloji Dergisi,* Cilt 3, Sayı 2, 2015, ss. 253-266.
- Ateş-Benek, Neslihan, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma", *Ceza Hukuku ve Kriminoloji Dergisi,* Cilt 10, Sayı 2, 2022, ss. 397-411.
- Başlar, Yusuf, "Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri", *Uyuşmazlık Mahkemesi Dergisi,* Cilt 3, Sayı 3, 2013, ss. 82-105.
- Baştürk, İhsan, "Bilgisayar Sistemleri ile Verilerinde Arama, Kopyalama ve Elkoyma", *Fasikül Hukuk Dergisi,* Cilt 2, Sayı 9, Ağustos 2010, ss. 23-32.
- Casey, Eoghan, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet,* 3. Bası, 2011.
- Centel, Nur; Zafer, Hamide, *Ceza Muhakemesi Hukuku,* Beta Yayıncılık, İstanbul, 2017.
- Çöpoğlu, Hakan Serdar, "Ceza Muhakemesi Hukukunda Arama Koruma Tedbirinde Belirlilik İlkesi", *Ankara Barosu Dergisi,* Cilt 77, Sayı 1, 2019, ss. 155-229.
- Değirmenci, Olgun, *Ceza Muhakemesinde Sayısal (Dijital) Delil,* Seçkin Yayıncılık, Ankara, 2014.
- Demirci, Ömer, *Bilişim Suçları ve Soruşturma Yöntemleri,* Seçkin Yayıncılık, Ankara, 2022.
- Duran, Gökhan Yaşar, "Ceza Muhakemesi Kanunu'nda (CMK) Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" *Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi,* Cilt 14, Sayı 173-174, Ocak-Şubat 2019, ss. 173-241.
- Dülger, Murat Volkan, *Ceza Muhakemesi Hukukunda Dışlama Kuralı ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağacın Meyvesi Öğreti),* Seçkin Yayıncılık, Ankara, 2014.
- Dülger, Murat Volkan, *Bilişim Suçları ve İnternet İletişim Hukuku,* Seçkin Yayıncılık, Ankara, 2020.
- Egemenoğlu, Alaaddin, "Proving the Crime of Threat Through Digital Evidence in the Light of the Supreme Court Decisions" *Necmettin Erbakan Üniversitesi Hukuk Fakültesi Dergisi,* Cilt 7, Sayı 2, 2024, ss. 481-494.
- Epözdemir, Rezan, "Bilişim Sistemlerinde Arama ve Elkoyma Tedbirleri" *Terazi Hukuk Dergisi,* Cilt 13, Sayı 142, Haziran 2018, ss. 88-98.

- Ercan, Tayfun; Erdal, İrem, *Türk Ceza Kanununda Bilişim Sistemine Girme Suçu ve Özel Hukuk Boyutu,* Adalet Yayınevi, Ankara, 2023.
- Erem, Faruk, *Ceza Usulü Hukuku,* Ankara Üniversitesi Hukuk Fakültesi Yayınları, No: 274, Sevinç Matbaası, Ankara, 1970.
- Gökcen, Ahmet; Balcı, Murat; Alşahin, M. Emin; Çakır, Kerim, *Ceza Muhakemesi Hukuku,* Adalet Yayınevi, Ankara, 2020.
- Ho, Hock Lai, "The Legal Concept of Evidence", Ed. Edward N. Zalta, *The Stanford Encyclopedia of Philosophy,* Aralık 2021, https://plato.stanford.edu/archives/win2021/entries/evidence-legal/ (26.09.2024).
- Kantar, Baha, *Ceza Muhakemeleri Usulü: Birinci Kitap: Umumi Hükümler,* Güzel Sanatlar Matbaası, Ankara, 1957.
- Karakehya, Hakan, "Ceza Muhakemesinin Amacı", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası,* Cilt 65, Sayı 2, 2007, ss. 121-143.
- Kaya, Mehmet Bedii, "Hukuki Açıdan Bilişim Suçları, Siber Güvenlik ve Adli Bilişim", Ed. Şeref Sağıroğlu, Mustafa Şenol, *Siber Güvenlik ve Savunma Problemler ve Çözümler,* Grafiker Yayınları, Ankara, 2019, ss. 213-279.
- Kaya, Mehmet Bedii, Polisin Sanal Devriye Yetkisini İptal Eden Anayasa Mahkemesi Kararının Değerlendirilmesi, https://mbkaya.com/hukuk/polis-sanal-devriye-siber-kolluk-aym-iptal.pdf (27.09.2024)
- Keskin, Salih, "Bilişim Suçlarında Ceza Muhakemesi Kanununun 134. Maddesindeki Hükümlerin Uygulanmasında Yaşanan Aksaklıklar", *Kırıkkale Üniversitesi Sosyal Bilimler Dergisi,* Cilt 11, Sayı 2, 2021, ss. 649-667.
- Koca, Mahmut, "Ceza Muhakemesi Hukukunda Deliller", *Ceza Hukuku Dergisi,* Cilt 1, Sayı 2, Aralık 2006, ss. 207-225.
- Koca Mahmut; Üzülmez, İlhan, *Türk Ceza Hukuku Özel Hükümler,* Adalet Yayınevi, Ankara, 2019.
- Kunter, Nurullah, *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku,* Beta Yayıncılık, İstanbul, 1989.
- Kunter, Nurullah; Yenisey, Feridun, Ayşe Nuhoğlu, *Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku,* Beta Yayıncılık, İstanbul, 2010.
- Osterburg, James W.; Ward, Richard H., *Criminal Investigating: A Method for Reconstructing the Past,* 6. Bası, 2010.
- Önok, Murat, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi,* Cilt 19, Sayı 2, 2013 (Özel Sayı), ss. 1229-1270.
- Özbek, Veli Özer; Doğan, Koray; Bacaksız, Pınar, *Türk Ceza Hukuku Özel Hükümler,* Seçkin Yayıncılık, Ankara, 2020.
- Özbek, Veli Özer; Doğan, Koray; Bacaksız, Pınar, *Ceza Muhakemesi Hukuku,* Seçkin Yayıncılık, Ankara, 2020.
- Özen, Muharrem; Özocak, Gürkan, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirlerinin Hukuki Rejimi", *Ankara Barosu Dergisi,* Sayı 1, 2015, ss. 41-78.
- Özen, Mustafa, *Ceza Hukuku Özel Hükümler Dersleri,* Adalet Yayınevi, Ankara, 2019.

- Özen, Mustafa, *Öğreti ve Uygulama Işığında Ceza Muhakemesi Hukuku,* Adalet Yayınevi, Ankara, 2019.
- Öztürk, Bahri; Eker-Kazancı, Behiye; Soyer-Güleç, Sesim, *Ceza Muhakemesi Hukukunda Koruma Tedbirleri,* Seçkin Yayıncılık, Ankara, 2019.
- Öztürk, Bahri; Tezcan, Durmuş; Erdem, Mustafa Ruhan; Sırma-Gezer, Özge; Saygılar-Kırıt, Yasemin F., Alan-Akcan, Esra; Özaydın, Özdem; Erden Tütüncü, Efser; Altınok-Villemin, Derya; Tok, Mehmet Can, *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* Seçkin Yayıncılık, Ankara, 2020.
- Sabillon, Regner; Cano, Jeimy; Cavaller, Victor; Serra, Jordi, "Cybercrime and Cybercriminals: A Comprehensive Study", *International Journal of Computer Networks and Communications Security,* Cilt 4, Sayı 6, Haziran 2016, ss. 165-176.
- Sarsıkoğlu, Şenel, "Ceza Muhakemesinde Delil ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı", *Türkiye Adalet Akademisi Dergisi,* Cilt 6, Sayı 22, 2015, ss. 427-454.
- Schroeder, Friedrich-Christian (Terc. Cumhur Şahin), "Ceza Muhakemesinde 'Dürüst Yargılama' İlkesi", *Selçuk Üniversitesi Hukuk Fakültesi Dergisi,* Cilt 5, Sayı 1-2, 1996 (Özel Sayı), ss. 269-283.
- Schroeder, Friedrich-Christian; Verrel, Torsten (Terc. Salih Oktar), *Ceza Muhakemesi Hukuku*, Yetkin Yayınları, Ankara, 2019.
- Semiz, Murat, *En Güncel İçtihatlar ve Uygulamadan Örnekleriyle Bilişim Suçları ve Soruşturma Yöntemleri,* Adalet Yayınevi, Ankara, 2022.
- Soyaslan, Doğan, *Ceza Muhakemesi Hukuku,* Yetkin Yayıncılık, Ankara, 2007.
- Soylu, Nurhan, *Dijital Delillere El Konulması Sürecinde CMK 134. Madde Hükümlerinde Görülen Problemler ve Çözüm Önerileri,* Üsküdar Üniversitesi Bağımlılık ve Adli Bilimler Enstitüsü Adli Bilimler Anabilim Dalı, 2021.
- Stephenson, Peter; Gilbert, Keith, *Investigating Computer-Related Crime,* 2. Bası, 2013.
- Şahin, Cumhur; Göktürk, Neslihan, *Ceza Muhakemesi Hukuku I,* Seçkin Yayıncılık, Ankara, 2020.
- Şahin, Cumhur; Göktürk, Neslihan, *Ceza Muhakemesi Hukuku II,* Seçkin Yayıncılık, Ankara, 2020.
- Şarsel, Betül Gül, *Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma,* Yaşar Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, 2017.
- Taner, M. Tahir, *Ceza Muhakemeleri Usulü,* İstanbul Üniversitesi Yayın No: 442, Hukuk Fakültesi No: 98, Duygu Matbaası, İstanbul, 1950.
- Tezcan, Durmuş; Erdem, Mustafa Ruhan; Önok, R. Murat, *Teorik ve Pratik Ceza Özel Hukuku,* Seçkin Yayıncılık, Ankara, 2020.
- The Sang, Nguyen; Trung, Bui Bao, "Cybercrime in the Digital Age: Challenges and Implication for Prevention", *International Journal of Social Science and Human Research,* Cilt 5, Sayı 11, Kasım 2022, ss. 5082-5086.
- Toroslu, Nevzat; Feyzioğlu, Metin, *Ceza Muhakemesi Hukuku,* Savaş Yayınevi, Ankara, 2008.
- Tosun, Öztekin, *Türk Suç Muhakemesi Hukuku Dersleri Cilt 1 Genel Kısım,* Fakülteler Matbaası, İstanbul, 1981.

- Turan, Metin, *Bilişim Hukuku,* Seçkin Yayıncılık, Ankara, 2021.
- Turinay, Faruk Yasin, "Ceza Muhakemesi Hukukunda Koruma Tedbirlerinin Sınıflandırılması", *Ankara Üniversitesi Hukuk Fakültesi Dergisi,* Cilt 70, Sayı 2, 2021, ss. 475-541.
- Uğraş, Dilek Özge, "Bilgisayarlarda, Bilgisayar Programlarında ve Bilgisayar Kütüklerinde Arama, Kopyalama ve Elkoyma", *Türkiye Barolar Birliği Dergisi,* Sayı 154, 2021, ss. 97-134.
- Ünal, Osman Gazi, *Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma,* Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, 2011.
- Ünver, Yener; Hakeri, Hakan, *Ceza Muhakemesi Hukuku Cilt 2,* Adalet Yayınevi, Ankara, 2019.
- Yaşar, Osman; Otacı, Cengiz, *Ceza Muhakemesi Kanunu Cilt 1,* Seçkin Yayıncılık, Ankara, 2022.
- Yenidünya, A. Caner; İçer, Zafer, *Ceza Muhakemesi Hukuku,* Adalet Yayınevi, Ankara, 2016.
- Yenisey, Feridun; Nuhoğlu, Ayşe, *Ceza Muhakemesi Hukuku,* Seçkin Yayıncılık, Ankara, 2020.
- Yıldız, Abdulhalik, *Yargıtay Ceza Genel Kurulu Kararları (2015-2020) Cilt 2,* Türkiye Adalet Akademisi Yayınları, Ankara, 2020.