Ceza Hukuku ve Kriminoloji Dergisi-Journal of Penal Law and Criminology 2022; 10(2): 367-411
ISSN: 2148-6646 / E-ISSN: 2602-3911

https://iupress.istanbul.edu.tr/en/journal/jplc/home

Research Article

DOI: 10.26650/JPLC2022-1129151

Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma

Searching, Copying and Seizing of Computers, Computer Programs and Files

Neslihan ATEŞ BENEK[1,2]

[1]Avukat, İstanbul Barosu, İstanbul, Türkiye
[2]Doktora Öğrencisi, İstanbul Üniversitesi Hukuk Fakültesi, Kamu Hukuku Anabilim Dalı, İstanbul, Türkiye

ORCID: N.A.B. 0000-0002-9927-6351

ÖZ
Teknoloji dünyasında yaşanan hızlı ilerlemenin ceza muhakemesi alanındaki en göze çarpan sonuçlarından biri, suçun ispatında dijital delillerden yararlanılmasıdır. İçinde bulunduğumuz bilgi çağında teknoloji dünyasında ortaya çıkan baş döndürücü gelişmeler, hayatın her alanında değişikliğe neden olduğu gibi hukuk alanında da etkilerini göstermiştir. Öncelikle suç işleme tarzları değişmiş ve suç dijital ortama taşınmıştır. Teknoloji alanında yaşanan bu dönüşüm karşısında, dijital deliller adeta yeni bir dünyanın kapılarını açarak ceza muhakemesi alanında klasik deliller gibi kullanılmaya başlanmıştır. Bilişim teknolojilerinin sunduğu imkanlar kullanılarak işlenen suçların her geçen gün artması karşısında gerek maddi gerçeğin ortaya çıkarılması gerekse suçlulukla mücadele kapsamında, bilimsel esaslara uygun olarak elde edilmiş dijital delillerden istifade edilmesi kaçınılmaz hale gelmiştir. Bu makalede de dijital delilleri elde edebilmek amacıyla bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbiri inceleme konusu yapılmıştır.
Anahtar Kelimeler: Dijital delil, bilgisayarlarda arama, bilgisayarlarda elkoyma

ABSTRACT
The rapid progress and stunning developments experienced in the technological world very directly impact all areas of life, including the field of law. One of the most striking impacts in the field of criminal procedures is how criminal acts transfer to the digital world and how digital evidence can be used as proof of these crimes. In the face of this transformation, digital evidence has opened the doors to a new world and started being used just like classical evidence in the field of criminal procedural law. With the increase in the number of crimes committed by using the opportunities offered by information technologies, using digital evidence that has been obtained within the scope of scientific principles has become inevitable for both revealing the truth and capturing criminals. This article deals with the issues of searching, copying, and seizing the digital evidence that is present in computers, computer programs and files.
Keywords: Digital evidence, computer search, computer seizure

Submitted: 10.06.2022 • **Accepted:** 18.10.2022 • **Published Online:** 04.11.2022

Corresponding author: Neslihan Ateş Benek, E-mail: ates.neslihan@hotmail.com

Citation: Ateş Benek, N, 'Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma' (2022) 10(2) Ceza Hukuku ve Kriminoloji Dergisi-Journal of Penal Law and Criminology, 367.
https://doi.org/10.26650/JPLC2022-1129151

EXTENDED ABSTRACT

In criminal procedural law, anything can be considered evidence provided it possesses characteristics pertaining to crime. As regards the principle of having free access to all evidence, no difference exists between digital and physical evidence. Also, due to the hierarchy of evidence being invalid with regard to criminal procedure, making a distinction between which evidence is important/strong or unimportant/weak is not possible. As a result of the tremendous developments in the field of technology also having increased the number of crimes committed regarding information systems, the need for digital evidence has gained increasingly greater importance, as well as its use as a means of proof. However, because the use of evidence obtaining measures such as the search, copy or seize of digital data belonging to individuals constitutes an infringement of many legal values, legislators have also regulated legal measures and bound these to strict conditions.

The measure on searching, copying, and seizing evidences from information systems in relation to crimes committed with use of digital technologies is listed in Criminal Procedure Code (Law No. 5271) and constitutes a special instance of the search and seizure protection measures. Article 134 of this Criminal Procedure Code covers the procedures regarding the gathering of data stored on information systems.

The topics of this study are the matters of the search, copy and seizure of digital evidence from information systems, and these matters are measures that can be applied to all criminal areas. Legislators have not limited the scope of crime in terms of the application of these measures. In this context, the relevant measures can be applied to all investigations that require the collection of digital evidence, whether for classical or cyber crimes.

In order to make a decision regarding the measures regulated in Article 134 of the Criminal Procedure Code, the conditions stipulated in the law must be fulfilled. These conditions are: the presence of strong grounds of suspicion based on concrete evidence and the absence of the possibility of obtaining evidence any other way. Evidence obtained after search, copy and seizure procedures have been made that do not adhere to these legal conditions should also be noted as being unusable as criminal evidence due to being outside the confines of the law. In addition, obtaining digital evidence in accordance with the technical requirements is also extremely important. Obtained evidence must be submitted to the judicial authorities intact and in full. Otherwise,

even if this evidence had been collected by field experts, it is neither acceptable as lawful evidence nor will it be taken as a basis for judgment.

Article 134 of the Criminal Procedure Code should be amended in accordance with the requirements of the age in the face of the rapidly developing and changing digital technologies. This regulation should also safeguard suspects' fundamental human rights and freedoms. In addition, the changes should occur rapidly and be sufficient to put an end to all the discussions regarding the doctrine. Due to digital evidence being among the most important evidence of the current day, guarantees should be introduced to ensure that this type of evidence is collected in accordance with the technical requirements and evaluated within the scope of scientific principles.

In summary, this paper aims to analyze the processes related to detecting and evaluating digital evidence within the framework of the general principles of criminal procedural law. In this context, the paper examines the search, copy and seizure measures regarding the information systems covered in Article 134 of the Criminal Procedure Code and provides explanations with respect to computers, computer programs and digital files as listed in Article 134. The paper additionally discusses the legal nature of the measures, their conditions and the way they are applied within the framework of discussions regarding the doctrine, the problems experienced in practice and the judicial decisions.

Giriş

Günümüzde teknolojik gelişmelerin hiç olmadığı kadar ivme kazanmasıyla birlikte, günlük hayattaki pek çok kişisel ve ekonomik faaliyet sanal ortama taşınmıştır. Teknolojik ilerlemeler, bilgisayarı hayatımızın bir parçası haline getirirken, bu sistemi kullanan kişiler, teknoloji alanında yaşanan bu gelişmelerden yararlanarak suç işleyebilmekte veya işledikleri suçlara ilişkin iz ve eserleri bu cihazlarda saklayabilmektedir[1]. Teknolojik gelişmelere kayıtsız kalamayan ceza yargılaması da bu gelişmelere paralel olarak suç tiplerinin değişmesi, iletişim araçlarının sıklıkla kullanılması ve yazılı belgelerin yerini dijital belgelere bırakmasıyla birlikte, ceza yargılamasının temel amaçlarından biri olan maddi gerçeğin ortaya çıkarılması amacıyla dijital delilleri elde etmek, incelemek ve hangi şartlarda delil olarak değerlendirileceğini belirlemek durumundadır[2]. Dolayısıyla bilişim sistemlerine karşı ya da bilişim sistemleri kullanılmak suretiyle bir suç işlendiği takdirde söz konusu sistem üzerinde inceleme yapılması önem arz etmektedir[3]. Klasik suçlara ilişkin delillerin bilişim sistemlerinde saklandığı hallerde de sistem üzerinde inceleme yapılması son derece önemlidir. Örneğin cinsel suçlar, çocuğun cinsel istismarı, dolandırıcılık, uyuşturucu veya uyarıcı madde ticareti dahil olmak üzere çok çeşitli suç tiplerine ilişkin soruşturmalarda, bilişim sistemlerinde delil araştırması yapılmak suretiyle dijital delillerden faydalanılmaktadır[4].

Dijital delillerin ceza muhakemesinde çok geniş bir yer tutmaya başlamasının nedenlerini ele alacak olursak, öncelikle suç, toplumun her kesiminde bilişim sistemlerinin sıklıkla kullanılıyor olmasının doğal bir sonucu olarak, bu alanda varlık göstermeye başlamıştır. Toplumdaki bu dönüşümle birlikte, suçun ispatında kullanılacak deliller de suçun yoğunlaştığı yerde, yani bilişim sistemlerinde aranmaya başlanmıştır. Esasen hem suç

1 Yusuf Yaşar ve İsmail Dursun, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri" (2013) 19 (2) Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 4.

2 Osman Yaşar ve Cengiz Otacı, *Yeni İçtihatlarla Uygulamalı ve Yorumlu Ceza Muhakemesi Kanunu I. Cilt* (10. Baskı, Seçkin Yayıncılık, 2022) 1105; Muharrem Özen ve Gürkan Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)" (2015) (1) Ankara Barosu Dergisi 44.

3 Murat Volkan Dülger, *Bilişim Suçları ve İnternet İletişim Hukuku* (9. Baskı, Seçkin Yayıncılık, 2022) 596.

4 Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd Edition, Academic Press, 2011) 6; Ayrıca bkz. Osman Gazi Ünal, *Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma* (Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, 2011) 82.

hem de suçun yoğunlaştığı yerde aranması gereken deliller dijitalleşmiştir[5]. Öyle ki, bir zamanlar yalnızca bilişim suçları kategorisinde kullanılan dijital deliller, artık her suç kategorisinde sıklıkla kullanılan bir delil haline gelmiştir. Örneğin çocuk pornografisine ilişkin suçlarda, dijital delillerin kullanılmadığı bir davaya rastlamak neredeyse imkansızdır[6]. Şu halde, Ceza Muhakemesi Kanunu'nun 134. maddesinde öngörülen *"Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma"* koruma tedbiri, yalnızca bilişim suçlarında değil, diğer suç tiplerinde de uygulanabilen bir tedbirdir. Diğer bir ifadeyle hem bilişim suçlarının hem de geleneksel suçların aydınlatılmasında dijital delillerden yararlanılmaktadır.

Belirtmek gerekir ki, teknolojinin gelişmesiyle birlikte bilgisayarlar, özellikle iş dünyasında oldukça geniş bir yer tutmaya başlamıştır. Öyle ki, işlerini yalnızca bilgisayarlarla yürüten bir şirketin bilgisayarlarında arama yapılması ve bu cihazlara elkonulması halinde, bu şirket iş yapamaz hale gelecektir. Bu nedenle, başta özel hayat ve mülkiyet gibi pek çok temel hak ve özgürlüğe müdahale eden böyle bir tedbirin Anayasa'nın *"Temel hak ve hürriyetlerin sınırlanması"* kenar başlıklı 13. maddesi uyarınca bir kanun normuna dayanması gerekmektedir[7].

Nitekim kanun koyucu da özel hayat, ticari ve bilimsel sırlar ve mülkiyet de dahil olmak üzere pek çok hukuki değere tecavüz oluşturması nedeniyle ağır sonuçlar doğuran bu tedbiri ayrıca düzenleme ihtiyacı duymuştur[8]. Hemen belirtmek gerekir ki, Ceza Muhakemesi Kanunu'ndan önceki dönemde, suç soruşturmasında gerçek veya tüzel kişilerin işyeri veya konutlarındaki bilgisayarlara fiziki olarak elkonulmaktaydı. Ancak bu uygulama hem kişi ve kuruluşların ticari faaliyetlerini ağır bir şekilde sekteye uğratmakta hem de yapılacak incelemenin güvenilirliği bakımından büyük kuşkular doğurmaktaydı. Zira CMUK'ta CMK m. 134 hükmünde düzenlenen bilişim sistemlerinde veri arama, kopyalama ve elkoymaya ilişkin bir düzenlemeye yer verilmediğinden,

5 Olgun Değirmenci, "Adli Bilişimde Önceliklendirme (Triyaj) Yönteminin Ceza Muhakemesi Açısından Değerlendirilmesi" (2020) 2 (1) Bilişim Hukuku Dergisi 56; John E. D. Larkin, "Compelled Production of Encrypted Data" (2012) 14 (2) Vanderbilt Journal of Entertainment & Technology Law 254; Aynı yönde bkz. Özge Apiş, "Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Koruma Tedbiri" (2018) (37) Yasama Dergisi 69.

6 "Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors", National Institue Of Justice <https://www.ojp.gov/pdffiles1/nij/211314.pdf> Erişim Tarihi 4 Nisan 2022.

7 Dülger (n 3) 596.

8 Nur Centel ve Hamide Zafer, *Ceza Muhakemesi Hukuku* (14. Baskı, Beta, 2017) 448; Örneğin bilişim sistemlerinin işlem hızlarında ve bilgi depolama kapasitelerinde yaşanan gelişim neticesinde, özel hayatın neredeyse tamamı bilişim sistemlerine kaydedilmekte ve dolayısıyla bu sistemlere herhangi bir müdahale halinde özel hayata müdahale söz konusu olmaktadır. Bkz. Olgun Değirmenci, *Ceza Muhakemesinde Sayısal (Dijital) Delil* (Seçkin Yayıncılık, 2014) 21.

bilişim sistemlerinde veri aramaya yönelik olarak genel arama ve elkoyma hükümlerinden istifade edilmekteydi. Ancak dijital verilerin kendilerine has niteliklerinden dolayı, genel arama ve elkoyma tedbirleriyle verilerden anlaşılabilir bir şekilde delil elde edilmesi her zaman mümkün olmuyordu. İşte CMK m.134 hükmünde yer alan özel düzenlemeye ihtiyaç duyulmasının sebeplerinden biri de bilişim sistemlerinde veri arama ve verilere elkoyma yönünden, genel arama ve elkoyma hükümlerinin yetersiz kalmasıydı[9].

Yukarıda açıklanan nedenlerle, 5271 sayılı Ceza Muhakemesi Kanunu'nun 134. maddesinde *"Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma"* kenar başlıklı düzenlemeye yer verilmiştir. Böylece bilgisayar, bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına ve bu kayıtların çözülerek metin haline getirilmesine ilişkin hükümler genel bir kanunda ilk kez öngörülmüştür. Diğer bir ifadeyle, CMK'nın 134. maddesinde yer alan bu düzenlemeyle, işlenen suçların aydınlatılması amacıyla bilişim sistemlerinde depolanan veriler üzerinde koruma tedbirlerinin uygulanması yasal bir zemine kavuşturulmuştur[10]. Bu yönüyle hükmün, ceza muhakemesinde kullanılacak olan dijital (sayısal)[11] delillerin, bilişim sistemlerinde araştırılması faaliyetine ilişkin bir düzenleme olduğunu söyleyebiliriz[12].

Öte yandan 10 Kasım 2010 tarihinde Türkiye tarafından imzalanan Avrupa Konseyi Siber Suç Sözleşmesi de 22.04.2014 tarihli ve 6533 sayılı Kanun'la onaylanarak *"Sanal Ortamda İşlenen Suçlar Sözleşmesi"* adı ile 02.05.2014 tarihinde yürürlüğe girmiştir. İşte CMK'nın 134. maddesi de Anayasa'nın 90. maddesi gereğince iç hukukumuzun bir parçası olarak kabul edilen Avrupa Konseyi Siber Suç Sözleşmesi'nin *"Saklanan bilgisayar verilerinin aranması ve bunlara el konulması"* başlıklı 19. maddesinin iç hukukumuzdaki halidir.

9 Ünal (n 4) 84-85.

10 Olgun Değirmenci, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbirinde (CMK m.134), 7145 Sayılı Kanunla Yapılan Değişikliklerin Değerlendirilmesi" (2018) 13 (146) Terazi Hukuk Dergisi 146; Adli ve Önleme Aramaları Yönetmeliği'nin 17. maddesinin kenar başlığı da "*Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma"* şeklinde düzenlenmiştir. Görüldüğü üzere, 5271 sayılı CMK'nın 134. maddesinin kenar başlığı, Yönetmelikte de aynen tekrar edilmiştir. CMK m. 134 hükmünün kanunlaşma süreci ve günümüze kadar maddede yapılan değişiklikler için bkz. Değirmenci (n 10) 146 vd.

11 Dijital kavramı sözlükte *"sayısal"* olarak tanımlanmaktadır. Bkz. Güncel Türkçe Sözlük, Türk Dil Kurumu < https://sozluk.gov.tr> Erişim Tarihi 14 Ağustos 2022; Bilişim sistemlerinden elde edilen deliller, dijital (sayısal) delil veya elektronik delil olarak adlandırılabilmektedir. Bkz. aşa. I, A; Çalışma boyunca dijital delil kavramı tercih edilecektir.

12 Cumhur Şahin, "Ceza Muhakemesinde Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" (2019) 1 (2) Yaşar Hukuk Dergisi 271.

Günümüzde iletişim, dijital verilerin iletimi yöntemiyle ve yalnızca sesli olarak değil; görsel ya da yazılı metinlerin anlık paylaşımı yoluyla da gerçekleştirilmektedir. İşte bu nedenle, bilişim sistemleri üzerinde yer alan durağan, bir diğer ifadeyle depolanmış veriler için CMK m. 134 hükmü uygulanırken; akış halindeki, yani iletişim esnasındaki veriler için CMK'nın *"Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi"* başlıklı Beşinci Bölümü'nde düzenlenen *"İletişimin tespiti, dinlenmesi ve kayda alınması"* başlıklı 135. maddesi uygulanmalıdır[13]. Çalışmamızda öncelikle CMK m.134 kapsamında durağan veriler ele alınacak olup, oldukça sınırlı bir şekilde akış halindeki verilere de temas edilecektir.

I. Dijital Deliller ve Dijital Delillere İlişkin Temel Kavramlar

A. Dijital Deliller

Ceza muhakemesinde delil serbestisi esas olup, belli delillerle belli olguların ispatı zorunlu değildir. Zira delillerin sınırlandırılması halinde, ceza muhakemesi işlemez hale gelecektir. Delil serbestisinin bir sonucu olarak, bir hususun *her türlü delille* ispatı mümkündür. Ayrıca ceza muhakemesinde ispat gücü yönünden deliller arasında bir derecelendirme yapılması da söz konusu değildir. Bu nedenle, tüm deliller ispat gücü bakımından aynı değere sahiptir[14]. Buradan anlaşılması gereken husus, ceza muhakemesinde diğer hukuk dallarından farklı olarak, delil özelliklerini taşımak kaydıyla her şeyin delil olabileceğidir. İspat araçları ve bu ispat araçlarının elde edilme yöntemleri kanunen sınırlandırılmamıştır[15]. Bu bağlamda dijital deliller ile fiziksel deliller arasında delilin değeri bakımından bir ayrım yapılması söz konusu olmadığından[16],

13 Dülger (n 3) 597; Burcu Baytemir Kontacı ve diğerleri (Editör: Cumhur Şahin ve Neslihan Göktürk), *Ceza Muhakemesi Hukuku*, (Seçkin Yayıncılık, 2018) 150; Ali Parlar ve Ahmet Çetin, *Ceza Muhakemesinde Soruşturma Evresi ve Uygulaması* (Aristo Yayınevi, 2017) 434; CMK'nın 135. maddesinin uygulanmasına ilişkin ayrıntılı açıklamalar için bkz. Seydi Kaymaz, *Ceza Muhakemesinde Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi* (4. Baskı, Seçkin Yayıncılık, 2015) 25 vd.; Cumhur Şahin, "Telekomünikasyon Yoluyla İletişimin Denetlenmesi" (2017) XI (1-2) Gazi Üniversitesi Hukuk Fakültesi Dergisi 1097 vd.; Kişinin özel hayatının ve bireysel haberleşmenin bir muhakeme tedbiri olarak denetlenmesine ilişkin olarak ayrıca bkz. Adem Sözüer, "Türkiye'de ve Karşılaştırmalı Hukukta Telefon, Teleks, Faks ve Benzeri Araçlarla Yapılan Özel Haberleşmenin Bir Ceza Yargılaması Önlemi Olarak Denetlenmesi" (1997) LV (3) İstanbul Üniversitesi Hukuk Fakültesi Mecmuası 70 vd.

14 Centel ve Zafer (n 8) 233; Mustafa Özen, *Ceza Muhakemesi Hukuku Dersleri* (2. Baskı, Adalet Yayınevi, 2017) 84.

15 Yener Ünver ve Hakan Hakeri, *Ceza Muhakemesi Hukuku* (17. Baskı, Adalet Yayınevi, 2020) 96.

16 Değirmenci (n 5) 56.

delil serbestisinin bir sonucu olarak, dijital deliller de hükme esas alınabilecektir[17].

Doktrinde dijital delil kavramına ilişkin farklı tanımlar bulunmaktadır. Bunlardan birine göre dijital delil, dijital ortamda bulunan, oluşturulan, depolanan ve iletilen her türlü veri olarak tanımlanmıştır[18]. Bir başka tanıma göre ise dijital delil, adli bilişimle ilgili bir çalışma esnasında, bilişim sistemleri (bilgisayarlar, mobil telefon, dijital fotoğraf makineleri, dijital videolar, dijital faks makineleri vb.) ve bu kapsamdaki depolama aygıtları üzerinden elde edilen adli delil şeklinde ifade edilmiştir[19]. Dijital delil yerine elektronik delil kavramını tercih eden diğer bir görüş kapsamında ise bu delil, bir elektronik araç üzerinde saklanan ya da bu araçlar aracılığıyla iletilen soruşturma açısından değeri olan bilgi ve veriler şeklinde tanımlanmıştır[20]. Bu tanımlar arasında esaslı bir farklılık olmayıp sadece dijital delil kavramı değişik cephelerden

17 Yargıtay Ceza Genel Kurulu da dijital delillerle ilgili olarak bir kararında şu ifadelere yer vermiştir: *"... istikrar kazanmış yargı kararlarında vurgulandığı ve öğretide de ifade edildiği üzere, ceza muhakemesinin amacı usul kurallarının öngördüğü ilkeler doğrultusunda maddi gerçeğin her türlü şüpheden uzak biçimde kesin olarak belirlenmesidir. Maddi gerçeğe ulaşılmasında kullanılan araç delillerdir. Ceza Muhakemesi Kanunu'nun "delilleri takdir yetkisi" başlıklı 217. maddesinin ikinci fıkrasındaki; "yüklenen suç, hukuka uygun bir şekilde elde edilmiş her türlü delille ispat edilebilir" şeklindeki hükümle, ceza muhakemesinde kullanılacak delillerin hukuka uygun bir şekilde elde edilmesi gerektiği açıkça belirtilmiş ve "delillerin serbestliği" ilkesine de vurgu yapılmıştır. Buna göre, hukuka uygun olmak kaydıyla, her türlü delil ispat aracı olarak kullanılabilir. Bu bakımdan maddi gerçeğe ulaştıracak delilin fiziki ya da elektronik olması önem arz etmemektedir."* Yargıtay Ceza Genel Kurulu, E. 2017/ 956, K. 2017/ 370, 26.09.2017 <www.lexpera.com> Erişim Tarihi 24 Ağustos 2022; "*Diğer delil türlerine göre özellik arz eden bazı yönleri olmakla birlikte dijital deliller de sonuçta, deliller hiyerarşisinin kabul edilmediği, delil serbestisinin benimsendiği ceza muhakemesi sistemimizde bir ispat aracıdır."* Yargıtay 9. CD., E. 2013/9110, K. 2013/12351, 09.10.2013 <www.kazancı.com.tr> Erişim Tarihi 20 Mayıs 2022.

18 Değirmenci (n 5) 56; Casey (n 4) 7; "Electronic Crime Scene Investigation: A Guide for First Responders", National Institue Of Justice <https://www.ojp.gov/pdffiles1/nij/219941.pdf> Erişim Tarihi 4 Temmuz 2022; <https://www.iacpcybercenter.org/officers/cyber-crime-investigations/digital-evidence/> Erişim Tarihi 4 Temmuz 2022.

19 Türkay Henkoğlu, *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi* (2. Baskı, Pusula Yayıncılık, 2014) 5.

20 Leyla Keser Berber, *Adli Bilişim* (Yetkin Yayınları, 2004) 46; Elektronik delil kavramının tercih edildiği eserler için bkz. Ali Karagülmez, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri* (5. Baskı, Seçkin Yayıncılık, 2014) 506 vd.; İsmail Ergün, *Siber Suçların Cezalandırılması ve Türkiye'de Durum* (Adalet Yayınevi, 2008) 49; Elektronik deliller, elektronik cihazlar aracılığıyla işlenen, aktarılan ya da söz konusu cihazlarda depolanan delillerdir. Elektronik cihazlar hem analog hem de dijital sinyalleri işleyebilme özelliğine sahiptir. Analog cihazlarda yer alan verilerin delil değerinden söz edilirken elektronik delil; dijital cihazlarda yer alan verilerin delil değerinden söz edilirken ise dijital delil kavramı kullanılmaktadır. Dolayısıyla elektronik delil kavramı, dijital delili de içine alan geniş bir kavramdır. Bkz. Değirmenci (n 8) 60-61; Elektronik delil ve dijital delil kavramları hakkında ayrıca bkz. Uğur Kaynakçıoğlu, *Ceza Muhakemesinde Dijital Deliller* (Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, 2015) 21 vd.; Orin S. Kerr, "Digital Evidence and The New Criminal Procedure" (2005) 105 (1) Columbia Law Review 279 vd.; Juhana Riekkinen, "Electronic Evidence in Criminal Procedure: On the Effects of ICT and the Development towards the Network Society on the Life-cycle of Evidence" (2019) 16 Digital Evidence and Electronic Signature Law Review 7 vd.; Radina Stoykova, "Digital evidence: Unadressed threats to fairness and the presumption of innocence" (2021) 42 Computer Law & Security Review 2; Martin Novak, "Digital Evidence in Criminal Cases Before the U.S. Courts of Appeal: Trends and Issues for Consideration" (2020) 14 (4) The Journal of Digital Forensics, Security and Law 1-2.

ifade edilmeye çalışılmıştır. Kanımızca dijital delili, suçun ispatına ilişkin olan ve dijital ortamda saklanan ve iletilen her türlü veri olarak tanımlayabiliriz.

Günümüzde pek çok olası dijital delil kaynağı olmasına rağmen, ceza muhakemesinde kullanılan en yaygın dijital delil türü, kişisel bilgisayarlardan elde edilen delillerdir. Bunun haricinde dijital deliller, bilgisayar programları, bilgisayar ağları ve cep telefonları gibi çeşitli elektronik cihazlarda da bulunabilir[21].

Elde edildikleri dijital ortam nedeniyle bu delillerin korunması ve güvenilirliği de önem arz eden konulardan biridir. Gözle görülemeyen ve son derece hassas bir yapıya sahip olan dijital deliller, diğer delil türlerine göre daha kolaylıkla değiştirilebilen, bozulabilen ve yok edilebilen delillerdir[22]. Bu nedenle, yapısı gereği manipülasyona açık olan dijital delillerin toplanması, muhafazası ve incelenmesi bakımından her türlü önlemin alınması gerekmektedir. Ceza muhakemesinde fiziksel delil türlerine göre özellik arz eden dijital delillerin, ispat gücü açısından diğer delillerle aynı güce sahip olabilmeleri, uygun şartlarda toplanmalarına ve muhafaza edilmelerine bağlıdır[23].

B. Temel Kavramlar

CMK'nın 134. maddesinde düzenlenen arama, kopyalama ve elkoyma tedbiri, *"bilgisayarlarda, bilgisayar programlarında ve kütüklerinde"* uygulama alanı bulmaktadır. Ancak ilgili maddede bilgisayar, bilgisayar programı ve bilgisayar kütüğü kavramlarından ne anlaşılması gerektiği hususunda bir açıklık bulunmamaktadır. Bu nedenle çalışmamızda, CMK m.134 hükmünde yer alan tedbirin konusunu oluşturan bu kavramlara ilişkin açıklama yapılması faydalı olacaktır.

1. Bilgisayar

Dijital delillerin yer aldığı başlıca ortamlardan birisi bilgisayarlardır. Şüphesiz söz konusu deliller yalnızca bilgisayarlarda bulunmayıp bilişim sisteminde yer alan farklı araçlarda da bulunabilmektedir. Ne var ki dijital delillerin aranması kavramı denildiğinde, çoğu insanın aklına ilk olarak bilgisayarlar gelmektedir. Hukukumuz dahil pek çok hukuk sisteminde de genel eğilim bu yöndedir[24].

21 Wayne Jekot, "Computer Forensics, Search Strategies, and the Particularity Requirement" (2020) 7 Pittsburgh Journal of Technology Law & Policy 6.

22 Dijital delillerin özellikleri hakkında bkz. Kaynakçıoğlu (n 20) 37 vd.

23 Dijital delillerin toplanması aşamasında uyulması gereken temel ilkeler ve yapılması gereken işlemler için bkz. Yusuf Başlar, "Elektronik Delilin Toplanması ve Muhafazası" (2020) 10 (1) Hacettepe Hukuk Fakültesi Dergisi 82 vd.

24 Değirmenci (n 8) 31; Bilişim sistemi özelliği gösteren bilgisayarlar, bilişim sistemi kavramıyla karşılaştırıldığında daha dar bir kapsamı ifade etmektedir. Bkz. Apiş (n 5) 51.

Bilgisayar kavramı sözlükte, çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin olarak tanımlanmaktadır[25]. Doktrinde ise bilgisayar kavramı yeterince kavramsallaştırılmış ve iyi tanımlanabilmiş her türlü problem üzerinde çalışabilen bir aygıt[26]; insanlar tarafından hazırlanıp yüklenen programlar yardımıyla bilgileri belirli bir düzende saklamak, işleyerek yeni sonuçlar üretmek, üretilen bilgileri başka yerlere iletmek, başka yerlerdeki bilgilere ulaşmak gibi amaçlarla kullanılan makineler[27]; bilgiyi dijital olarak işleyebilen, depolayabilen, üretebilen ve aktarabilen aygıtlar[28] ve bilgi depolayıp işleme tabi tutan ve sonucunu gösteren bir araç[29] şeklinde tanımlanmıştır.

Yargıtay Ceza Genel Kurulu da CMK'nın 134. maddesinde geçen bilgisayar teriminden ne anlaşılması gerektiği konusunun CMK'da açık bir şekilde belirtilmediğini ifade ederek bilgisayar terimini, belleğindeki programa uygun olarak aritmetik ve mantıksal işlemleri yapabilen, karar verebilen, yürüteceği programı ve işleyeceği verileri ezberinde tutabilen, çevresiyle etkileşimde bulunabilen bir araç olarak ifade etmiştir[30]. Ayrıca ilgili kararda bilgisayar, akıllı telefonlar, GPS cihazları, donanım ve yan donanımlar ile verileri dijital olarak kaydetme ve işleme yeteneğinde olan her türlü dijital cihazın CMK m. 134 hükmü kapsamında olduğu belirtilmiştir. Aynı şekilde madde kapsamına; içağlar, veri tabanları, sistem odaları, sunucular, yedek üniteler, arşivler, veri iletim hatları, yönlendiriciler vs. dâhilinde bulunan tüm dijital alanlar, veriler ve veri taşıyıcıları da girmektedir. Zira bunlar belleğindeki programa uygun olarak aritmetik ve mantıksal işlemleri yapabilen, karar verebilen, yürüteceği programı ve işleyeceği verileri ezberinde tutabilen, çevresiyle etkileşimde bulunabilen araçlar olan bilgisayarların bileşenleri olarak fonksiyon icra etmektedir.

Devamlı gelişen bilgi teknolojileri, farklı amaçlarla üretilen cihazları sahip oldukları özellikler bakımından birbirine yakın bir hale getirmiştir. Örneğin, başlıca görevi kişiler arasındaki iletişimi sağlamak olan taşınabilir telefonlar, aynı zamanda verileri

25 Bkz. Güncel Türkçe Sözlük, Türk Dil Kurumu < https://sozluk.gov.tr> Erişim Tarihi 4 Temmuz 2022.

26 Yılmaz Yazıcıoğlu, *Bilgisayar Suçları; Kriminolojik, Sosyolojik ve Hukuki Boyutları ile* (Alfa Yayınları, 1997) 25-26.

27 Berrin Akbulut, *Türk Ceza Hukukunda Bilişim Suçları* (Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Doktora Tezi, 1999) 10; Berrin Bozdoğan Akbulut, "Bilişim Suçları" (2000) 8 (1-2) Selçuk Üniversitesi Hukuk Fakültesi Dergisi Milenyum Armağanı 546.

28 Dülger (n 3) 67.

29 Yüksel Ersoy, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları" (1994) 49 (3) Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi 150.

30 Yargıtay Ceza Genel Kurulu, E. 2019/353, K. 2020/367, 18.06.2020 <www.lexpera.com> Erişim Tarihi 29 Mart 2022.

depolama, işleme ve gönderme özelliğine de sahiptir. Bu kapsamda, bir cihazın hem taşınabilir telefon hem de bilgisayar olarak kabulü mümkündür[31]. İşte bu tespit çerçevesinde, bilgisayar kavramının yalnızca bilgisayar olarak adlandırılan cihazları değil, işletim sistemi kullanan taşınabilir telefonları, tabletleri, saat gibi giyilebilir akıllı aksesuarları ve benzer diğer cihazları da kapsadığı söylenebilecektir[32].

2. Bilgisayar Programı

Bilgisayar, donanım ve yazılım olmak üzere iki temel bileşenden oluşmaktadır. Bilgisayarın somut kısmını oluşturan donanım[33], gözle görülebilen ve soyut bileşenlerin çalışacağı ortamı oluşturarak kullanıcı ile soyut bileşen arasındaki bağlantıyı sağlamaktadır[34]. Donanıma, bilgisayar kasası içinde bulunan anakart, sabit disk, ekran kartı vb. gibi parçalar ile bilgisayar kasası dışında bulunan ekran, klavye, fare ve hoparlör gibi parçalar örnek olarak verilebilir[35]. Bilgisayarın soyut bileşenini oluşturan yazılım ise program ve veri olmak üzere iki ana bileşenden oluşmaktadır[36].

Bir bilgisayarın, belirli görevleri yerine getirebilmesi için söz konusu göreve ilişkin komutların belirli bir düzen çerçevesinde sıralanması gerekir. İşte bu sıralama sonucunda oluşan komutlar dizisi bilgisayar programı olarak adlandırılır[37]. Hukukumuzda 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun *"Tanımlar"* başlıklı 1/B maddesinin (g) bendinde bilgisayar programının tanımına yer verilmiştir. Buna göre, *"Bilgisayar programı: Bir bilgisayar sisteminin özel bir işlem veya görev yapmasını sağlayacak bir şekilde düzene konulmuş bilgisayar emir dizgesini ve bu emir dizgesinin oluşum ve gelişimini sağlayacak hazırlık çalışmalarını"* ifade etmektedir. Yargıtay Ceza Genel Kurulu da yukarıdaki tanımlarla uyumlu bir tanım yaparak bilgisayar programını *"bir bilgisayar vasıtasıyla belirli bazı görevleri gerçekleştirmek için oluşturulan yazılı talimatlar dizisi olarak"*[38] tarif etmiştir.

31 Değirmenci (n 8) 35.

32 Yaşar ve Otacı (n 2) 1107.

33 Ünal (n 4) 7.

34 Değirmenci (n 8) 50.

35 Ünal (n 4) 7-8.

36 Ünal (n 4) 8.

37 Değirmenci (n 8) 51; Programlar sistem programları ve uygulama programları olmak üzere iki grupta incelenmektedir. Bu konu hakkında detaylı bilgi için bkz. Değirmenci (n 8) 51; Ünal (n 4) 9.

38 Yargıtay Ceza Genel Kurulu, E. 2019/353, K. 2020/367, 18.06.2020 <www.lexpera.com> Erişim Tarihi 29 Mart 2022.

CMK'nın 134. maddesi kapsamında tedbirin konusunu oluşturan bilgisayar programları kendi bünyelerinde veri barındırdıklarından[39], önemli bir dijital delil kaynağı olarak kabul edilmektedir. Öte yandan bilgisayar ortamında bulunan bir verinin, program olmaksızın algılanması, görüntülenmesi ya da okunması mümkün olmadığından programların, bilgisayarların adeta can damarları olarak kabul edildiğini söylemek yanlış olmayacaktır[40].

3. Bilgisayar Kütüğü

Kanun koyucu, CMK'nın 134. maddesinde aramanın yapılacağı yerleri sıralarken bilgisayar kütüklerine de yer vermiştir. Ne var ki bilgisayar kütüğü kavramı, yanlış anlaşılmaya ve tartışmaya oldukça açık bir kavramdır. Şöyle ki, doktrinde bazı yazarlar İngilizce "log" kelimesinin karşılığı olarak kütük kavramını kullanmaktadır. Ancak her ne kadar kütük kelimesinin İngilizce sözlük karşılığı olarak "log" kelimesi kullanılıyor olsa da bu karşılık kütük kavramının bilişim terminolojisindeki karşılığı değildir[41].

Dokrtinde bir görüş, kütük ve log kavramı arasındaki farkı ortaya koyarak her iki kavramı da tanımlamaya çalışmıştır. Buna göre, insan müdahalesi ile bilişim sistemi tarafından oluşturulan ve saklanan dosyalar şeklindeki tanım "kütük" kavramını; insan müdahalesi olmadan bilişim sistemi tarafından oluşturulan ve saklanan dosyalar şeklindeki tanım ise "log"ları ifade etmektedir[42].

Yargıtay Ceza Genel Kurulu da CMK m. 134 hükmünde yer verilen terimleri açıkladığı kararında, bilgisayar kütüklerinin daha çok olay kayıtları anlamında log kayıtlarının karşılığı olarak Türkçe'ye çevrildiğini, ancak CMK'nın 134. maddesinde kastedilenin esasen İngilizce *"database"* terimin karşılığı olarak kullanılan *"veri tabanı"* olduğunu belirtmiştir[43].

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 cihazlar da

39 Değirmenci (n 8) 51.

40 Cengiz Tanrıkulu, *Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma* (Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Doktora Tezi, 2014) 318.

41 Tanrıkulu (n 40) 319; Değirmenci (n 8) 51.

42 Değirmenci (n 8) 53.

43 Yargıtay Ceza Genel Kurulu, E. 2019/353, K. 2020/367, 18.06.2020 <www.lexpera.com> Erişim Tarihi 29 Mart 2022.

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 da"* uygulanmasının dayanağı budur[44].

Benzer şekilde, iç hukukumuzun bir parçası olarak kabul edilen Avrupa Konseyi Siber Suç Sözleşmesi'nde bilgisayarlarda, bilgisayar programlarında, bilgisayar kütüklerinde, bilgisayar ağları ve verilerin saklandığı depolarda ve uzak bilgisayar kütüklerinde arama, kopyalama ve el koyma tedbirlerinin uygulanabileceği kabul edilmiştir. Bu itibarla, bilgisayar kütükleri yalnızca kullanıcının kendi bilgisayarında yer alan bir bilgisayar programı aracılığıyla kullanılabilen, verilerin saklandığı depolama araçlarıyla sınırlı değildir. Bunun yanı sıra, bir bilgisayar aracılığıyla ağ üzerinden ulaşılabilen gerek kullanıcıya ait gerekse kullanıcıya ait olmayıp ancak ortak paylaşıma ve kullanıma açık diğer bilgisayarlardaki veri depolama araçlarına ulaşabilmek de mümkündür[45].

II. Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Tedbiri

A. Tedbirin Hukuki Niteliği

CMK'nın 134. maddesinde düzenlenen *"Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma"* tedbirinin hukuki niteliğini ele almadan önce, madde başlığına ilişkin olarak doktrinde yer alan görüşlere değinmek faydalı olacaktır. Doktrinde ileri sürülen bir görüşe göre, tedbiri ifade etmek üzere oldukça uzun bir terim benimsenmiş olmasına rağmen, madde başlığı tedbirin içeriğini en iyi karşılayacak

44 Bkz. Yargıtay Ceza Genel Kurulu, E. 2020/344, K. 2022/12, 13.01.2022 <www.lexpera.com> Erişim Tarihi 15 Ağustos 2022; Yargıtay Ceza Genel Kurulu, E. 2020/9-288, K. 2021/352, 08.07.2021 <www.kazancı.com.tr> Erişim Tarihi 7 Haziran 2022; Adli ve Önleme Aramaları Yönetmeliği'nin 17. maddesinde ortaya konan kavramlara değinecek olursak, bilgisayar ağı, bilgisayarlar arasında iletişim kurmaya ve paylaşım ortamı oluşturmaya yarayan bir iletim ortamıdır. Kapalı ağ ve açık ağ olmak üzere ikiye ayrılırlar. İnternet erişiminin bulunmadığı ağlar kapalı ağ, internet erişiminin bulunduğu ağlar ise açık ağ olarak adlandırılmaktadır. Bkz. Muharrem Çelik, *Bilgisayarda Arama, Kopyalama ve Elkoyma (CMK m.134)* (İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, 2018) 50; Yargıtay Ceza Genel Kurulu'nun E. 2020/344, K. 2022/12, 13.01.2022 tarihli kararında da ifade edildiği üzere bilgisayar kütükleri, yalnızca kullanıcıların kendi bilgisayarlarında yer alan bir program aracılığıyla kullanılabilen, verilerin saklandığı depolama araçlarından ibaret değildir. Bir bilgisayar aracılığıyla ağ üzerinden erişilen, ortak paylaşıma ve kullanıma açık diğer bilgisayarlardaki veri depolama araçları uzak bilgisayar kütükleri olarak kabul edilir. Son olarak çıkarılabilir donanımlar ise CD ve USB gibi bilgisayara bağlanmak suretiyle bir işleve sahip olan bilgisayar donanımlarıdır. Bkz. Çelik (n 44) 51.

45 Bkz. Yargıtay Ceza Genel Kurulu, E. 2020/344, K. 2022/12, 13.01.2022 <www.lexpera.com> Erişim Tarihi 15 Ağustos 2022.

şekilde kaleme alınmıştır[46]. Doktrinde yer alan bir başka görüş ise 134. maddenin başlığında geçen "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde" ibaresinin amaca uygun olmadığını ifade etmiştir. Bunun yerine, Avrupa Konseyi Siber Suç Sözleşmesi'nde yer alan "bilgisayar sistemi" ibaresine yer verilmesinin daha yerinde olacağı ileri sürülmüştür[47]. Doktrinde ileri sürülen ve bizim de katıldığımız diğer görüş ise konunun bilgisayarla sınırlandırılması yerine, daha kapsayıcı olacak şekilde bilişim sistemi kavramının kullanılması gerektiğini belirtmiştir[48]. Öte yandan TCK'nın *"Bilişim Sistemine Girme Suçu"* başlıklı 243. maddesinde de *"bilişim sistemi"* kavramına yer verilmiştir[49]. Biz de çalışmamızda *"bilgisayar, bilgisayar programları ve bilgisayar kütükleri"* kavramı yerine *"bilişim sistemi"* kavramını kullanmayı tercih edeceğiz.

CMK'nın 134. maddesinin hukuki niteliğine dönecek olursak, bilişim sistemlerinde arama, kopyalama ve elkoyma koruma tedbiri, CMK'nın 116 ve 123. maddeleri arasında düzenlenen *"arama"* ve *"elkoyma"* koruma tedbirinin özel bir görünümünü oluşturmaktadır[50]. CMK'nın 134. maddesinde düzenlenen bu tedbir, bilişim sistemleri üzerinde depolanan verilere yönelik arama, kopyalama ve elkoyma işlemlerini düzenleyen bir tedbirdir. Bu yönüyle söz konusu düzenleme, arama tedbirinin düzenlendiği CMK m. 116 vd. ile elkoyma tedbirinin düzenlendiği CMK m. 123 vd. hükümlerinde yer alan düzenlemelerden ayrı olarak, bilişim sistemlerinde yer alan soyut verinin konu alındığı bir koruma tedbiri niteliğindedir[51]. Kanaatimizce, CMK'nın 134. maddesinde öngörülen bu tedbirin, Kanun'da arama ve elkoyma tedbirine ilişkin bölümde ve bu tedbirlerin özel bir halini oluşturacak şekilde düzenlenmesi yerinde olmuştur.

CMK m. 134 hükmünde yer alan düzenlemenin niteliği bakımından doktrinde ileri sürülen bir görüşe[52]göre, bu hüküm bir elkoyma düzenlemesi değil, arama koruma tedbirinin bilgisayar programlarında ve kütüklerinde icrasına ilişkin özel bir hükümdür.

46 Veli Özer Özbek ve diğerleri, *Ceza Muhakemesi Hukuku* (8. Baskı, Seçkin Yayıncılık, 2016) 427.

47 Muharrem Özen ve İhsan Baştürk, *Temel Hak ve Özgürlükler Bağlamında Bilişim-İnternet ve Ceza Hukuku* (Adalet Yayınevi, 2011) 142.

48 Değirmenci (n 8) 310; Aynı yönde bkz. Çelik (n 44) 29; Dülger (n 3) 598; Karşı görüş için bkz. Apiş (n 5) 79.

49 TCK'nın 243. maddesinin gerekçesinde "bilişim sistemi", verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistem olarak ifade edilmiştir.

50 Hüsnü Aldemir, *Adli-Önleme Arama ve Elkoyma*, (4. Baskı, Adalet Yayınevi, 2021) 213; Burak Çekiç, "Bilgisayar Verilerinde Arama, Kopyalama, Elkoyma Tedbirinin Hukuki Niteliği ve Benzer Kavramlar" (2021) 2 (1) Namık Kemal Üniversitesi Hukuk Fakültesi Dergisi 156; Centel ve Zafer (n 8) 448; Şahin (n 12) 271; Apiş (n 5) 68; Yaşar ve Dursun (n 1) 6; Değirmenci (n 8) 74; Dülger (n 3) 605.

51 Değirmenci (n 10) 146.

52 Ünver ve Hakeri (n 15) 428.

Başka bir ifadeyle, CMK'nın 134. maddesi bir elkoyma hükmü değil, arama düzenlemesine ilişkin bir maddedir. Zira burada yapılan işlem bir şeye elkoyma değil, arama sonrası verilerin örnek çıktılarının ya da kopyalarının alınmasıdır. Esasen delil tespiti söz konusudur. Ancak çok istisnai olarak, bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi ya da gizlenmiş bilgilere ulaşılamaması halinde, bilgisayara elkoymak amacıyla değil de elde edilmek istenen verilere ulaşmak amacıyla ve bu amaçla sınırlı kalacak şekilde geçici bir süre bilgisayarlara, programlara ve kütüklerine elkonulmasına müsaade edilmektedir. Yine bu görüşe göre, CMK'nın 134. maddesindeki düzenleme olmasa bile, genel hükümler çerçevesinde bilgisayarlara elkonulması mümkündür. Ancak bu düzenlemeyle amaçlanan, bilgisayarlara elkoymadan da verilere ulaşılabilmesi halinde, söz konusu cihazlara elkonularak kişilerin bilgisayar kullanımına engel olunmamasıdır[53].

Dijital delilleri barındırmaları sebebiyle oldukça önemli bir delil kaynağı niteliğine sahip olan bilgisayarlar, aynı zamanda kişilere ait en mahrem ve özel verilere de ev sahipliği yapan yerlerdir[54]. İnternet uygulamaları, e-ticaret ve sosyal medya kullanımının yaygınlaşmasıyla birlikte, bilişim sistemlerinde daha fazla kişisel veri kaydedilir hale gelmiştir[55]. İşte bu nedenle söz konusu koruma tedbiri, suistimale müsait olan verilerin sıhhatini ve güvenliğini sağlamak ve ayrıca bireyin özel hayatına ve kişisel verilerine yönelik olumsuz tesirleri engellemek amacıyla *"özel koşullara bağlı"*, genel adli aramadan ayrıksı ve istisnai bir koruma tedbiri şeklinde düzenlenmiştir[56].

CMK'nın 116-133. maddeleri arasında düzenlenen "arama ve elkoyma" tedbirine ilişkin genel hükümler, uygulanabilir olduğu ve aksine bir hüküm bulunmadığı müddetçe, özel nitelikteki "bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" koruma tedbiri yönünden de uygulama alanı bulacaktır[57]. Şöyle ki, CMK'nın 134. maddesinde arama zamanı (m. 118), aramada hazır bulunabilecekler (m.120), bilgisayarı aranacak kişinin sıfatı (avukat, milletvekili), elde edilen verilerin imhası ve başka amaçlarla kullanılıp kullanılamayacağı ya da arama sırasında yapılmakta olan soruşturmayla ilgisi olmayan ancak diğer bir suçun

53 Ünver ve Hakeri (n 15) 429; Aksi görüş için bkz. Yaşar ve Dursun (n 1) 26.

54 Yaşar ve Otacı (n 2) 1105-1106.

55 Çekiç (50) 156.

56 Bkz. Yargıtay Ceza Genel Kurulu, E. 2019/353, K. 2020/367, 18.06.2020 <www.lexpera.com> Erişim Tarihi 29 Mart 2022.

57 Aldemir (n 50) 214; Aynı yönde bkz. Çekiç (n 50) 158; Batuhan Aktaş, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Tedbiri Üzerine Bir İnceleme" (2017) 14 (2) Yeditepe Üniversitesi Hukuk Fakültesi Dergisi 217; Yaşar ve Dursun (n 1) 7; Değirmenci (n 8) 74.

işlendiği şüphesini uyandırabilecek bir delil elde edilmesi gibi oldukça önemli hususlara ilişkin bir düzenlemeye yer verilmemiştir. Ancak maddede yer bulmayan bu düzenlemeler bakımından, CMK'nın ilgili hükümlerinden istifade edilmelidir. Dolayısıyla konutta, işyerinde veya diğer kapalı yerlerde gece vaktinde arama yapılamaması (m.118/f.1), hakkında arama işlemi uygulanan kimsenin belge veya kâğıtlarını inceleme yetkisinin Cumhuriyet savcısı ve hâkime ait olması (m.122/1) gibi düzenlemeler, CMK'nın 134. maddesi bakımından da uygulanmalıdır[58].

Son olarak belirtmek gerekir ki, bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirlerine ilişkin düzenlemelerin yer aldığı CMK m. 134 hükmü, önemli bir düzenleme olarak karşımıza çıksa da Türkiye'nin taraf olduğu ve hukukumuz açısından bağlayıcı olan Avrupa Konseyi Siber Suç Sözleşmesi'nde öngörülen kuralların oldukça küçük bir kısmını yansıtmaktadır[59].

B. Tedbirin Şartları

1. Somut Delillere Dayanan Kuvvetli Şüphe Sebeplerinin Varlığı

5271 sayılı CMK'nın ilk halinde 134. maddenin uygulanabilmesi için tek şart, başka surette delil elde etme imkanının bulunmamasıydı. Ancak 21 Şubat 2014 tarihli ve 6526 sayılı Kanun'un 11. maddesiyle, 134. maddenin 1. fıkrası değişikliğe uğramış ve bu fıkraya *"somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı"* ibaresi ayrı bir şart olarak eklenmiştir[60]. İfade edildiği üzere, 6526 sayılı Kanun'un 11. maddesiyle, CMK'nın 134. maddesine bir şüphe düzeyi eklenmiştir. Kanun koyucu, 6526 sayılı Kanun'la yapılan değişiklikten önce madde metninde bu tedbirin uygulanabilmesi bakımından suçun işlendiği noktasında herhangi bir şüphe düzeyine

58 Yaşar ve Otacı (n 2) 1106.

59 Rıfat Çulha ve diğerleri (Editör: Feridun Yenisey), *Ceza Muhakemesi Hukuku Başvuru Kitabı* (Bilge Yayınevi, 2017) 68.

60 6526 sayılı Kanun'un 11. maddesiyle CMK'nın 134. maddesinde yapılan değişikliğin amacı, Avrupa İnsan Hakları Sözleşmesi ile Anayasa'da yer alan temel haklar ve özellikle adil yargılanma hakkı gözetilmek suretiyle koruma tedbirlerinden beklenen fayda ile kişisel haklara verilecek zarar arasındaki dengeyi sağlamak ve orantısız müdahaleyi önlemektir. Bkz. Çulha ve diğerleri (n 59) 69.

yer vermemişti[61]. Ancak kanun değişikliğinden sonra CMK m.134/f.1 hükmüne yapılan eklemeyle, bahse konu tedbire başvurulabilmesi için kuvvetli şüphe sebeplerinin varlığı aranmıştır[62].

Şüphelinin mahkum olma ihtimalinin kuvvetle muhtemel olması halinde, kuvvetli şüphe sebeplerinin varlığından söz edilebilecektir[63]. Bu bağlamda, söz konusu tedbire karar verilebilmesi için tedbirin talep edildiği andaki deliller kapsamında, kişinin gerek fail gerekse suç ortağı olarak bir suçu işlediği konusundaki ihtimal kuvvetli olmalıdır[64].

Kanun koyucu, kamu davasının açılabilmesi için suçun işlendiği hususunda yeterli şüphe bulunmasını ararken (CMK m.170/f.2), CMK'nın 134. maddesinde yer alan tedbir söz konusu olduğunda somut delillere dayanan kuvvetli şüphe sebeplerinin varlığını aramaktadır. Öyle ki, 2014 yılında yapılan bu değişiklikle, kişilerin temel hak ve özgürlüklerine ilişkin pek çok değere müdahale eden bu tedbirin şartları zorlaştırılmak istenmiş[65], yeterli şüphenin varlığında bile bu tedbire başvurulamaması amaçlanmıştır.

Kuvvetli şüphe yalnızca soruşturma konusu suçun işlendiğine yönelik olmamalı, aynı zamanda şüphelinin kullandığı bilişim sisteminden suç soruşturmasıyla ilgili delil elde

61 Değirmenci (n 10) 148; Yaşar ve Dursun (n 1) 11; 6526 sayılı Kanun değişikliğinden önce CMK'nın 134. maddesinde herhangi bir şüphe düzeyi aranmadığından doktrindeki bazı görüşler, genel arama ve elkoyma tedbirine başvurulabilmesi için aranan makul şüphenin, özel bir arama ve elkoyma tedbiri olan CMK m. 134 için de aranması gerektiğini savunmuştur. Bkz. Ünal (n 4) 100; Aynı yönde bkz. Değirmenci (n 8) 351; Yaşar ve Dursun (n 1) 11; Bazı görüşler ise CMK m.134 hükmünde, pek çok koruma tedbirinde öngörülen tarzda bir şüphe düzeyi belirtilmediğinden, basit şüphe halinde bile bu tedbire başvurulabileceği kanaatindeydi. Diğer bir görüş ise *"İletişimin tespiti, dinlenmesi ve kayda alınması"* koruma tedbirinin düzenlendiği CMK m. 135 hükmünde yer alan kuvvetli şüphe şartının kıyasen CMK m.134 hükmü yönünden de aranması gerektiğini savunmaktaydı. Bu görüşler için bkz. Yaşar ve Dursun (n 1) 11; Çulha ve diğerleri (n 59) 69; 6526 sayılı Kanun'dan önceki durum hakkında detaylı bilgi için bkz. Değirmenci (n 8) 348 vd.

62 6526 sayılı Kanun'un 11. maddesiyle, CMK m. 134 hükmünde düzenlenen tedbirin şartlarında yapılan değişikliğin ardından *"kuvvetli şüphe sebepleri"* ibaresinin madde metnine eklenmesiyle birlikte, *"kuvvetli şüphe sebepleri"* ile *"kuvvetli şüphe"* arasında anlam açısından bir farklılığın olup olmadığı konusu doktrinde tartışılmıştır. Bu iki ifade arasında bir fark bulunduğunu savunanlar olduğu gibi iki ifade arasında herhangi bir farklılık olmadığını ileri sürenler de vardır. Doktrindeki görüşler için bkz. Ahmet Hulusi Akkaş, "Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi Koruma Tedbirinin Şartlarında 6526 Sayılı Kanun ile Yapılan Değişikliklerin Değerlendirilmesi" (2015) (21) Türkiye Adalet Akademisi Dergisi 469 vd.; Ayrıca bkz. Özbek ve diğerleri (n 46) 432-433; Kanaatimizce, her iki kavram arasında bir farklılık söz konusu olmayıp, CMK m. 134 hükmünde düzenlenen tedbire başvurulabilmesi için aranan kuvvetli şüphe sebeplerinin varlığı, kuvvetli şüpheye işaret etmektedir. Aynı yönde bkz. Değirmenci (n 8) 149; Akkaş (62) 471-472.

63 Bahri Öztürk ve diğerleri, *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku*, (14. Baskı, Seçkin Yayıncılık, 2020) 447.

64 Centel ve Zafer (n 8) 376.

65 Şahin (n 12) 274; Dülger (n 3) 600.

edilebileceğine de yönelik olmalıdır[66]. CMK m.134'teki düzenleme kişilerin temel hak ve özgürlüklerine müdahale teşkil eden bir koruma tedbiri olduğundan, şüphelinin soruşturma konusu suçu işlediğine yönelik kuvvetli şüphe bulunsa bile, şüphelinin kullandığı bilişim sisteminde delil bulunabileceğine yönelik bir beklentinin olmadığı hallerde bu tedbire başvurulması yerinde olmayacaktır[67].

2. Başka Surette Delil Elde Etme İmkanının Bulunması

CMK m. 134 hükmünde düzenlenen tedbire karar verilebilmesi için yalnızca somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı yeterli değildir. Ayrıca başka surette delil elde etme imkanının bulunmaması da gerekir. Dolayısıyla tedbire karar verilebilmesi için bu iki şartın birlikte bulunması zorunludur. Aksi takdirde, verilen karar hukuka aykırı olduğu gibi, bu karar neticesinde elde edilen deliller de hukuka aykırı delil olarak kabul edilecek ve hükme esas alınamayacaktır[68].

Başka surette delil elde etme imkanının bulunmaması, esasen bu tedbire son çare olarak başvurulmasını gerektirmektedir. Ancak başka surette delil elde etme imkanının bulunmaması şartı, temel hak ve özgürlüklere daha az müdahalede bulunan diğer tedbirlere öncelikli olarak başvurulması gerektiği anlamına gelmez. Öyle ki, diğer delil elde etme yollarına başvurulduğunda, artık delil elde edememe ihtimalinin söz konusu olduğu hallerde de başka surette delil elde etme imkanı bulunmayabilir[69].

Esasen kanun koyucu, söz konusu tedbirin temel hak ve özgürlükler açısından ciddi bir tehdit barındırdığını göz önünde bulundurarak bu tedbire son çare (ultima ratio) olarak başvurulmasını amaçlamış ve farklı bir koruma tedbirine başvurularak delil elde etme imkanının bulunduğu hallerde öncelikli olarak o tedbirin uygulanmasını yerinde görmüştür[70]. Ancak bu şartın arandığı tedbirlere konu suçlara baktığımızda

66 Ersan Şen ve Sefa Eryıldız, *Elkoyma* (Seçkin Yayıncılık, 2017) 190.

67 Değirmenci (n 8) 352-353; Bu yönde ayrıca bkz. Yaşar ve Otacı (n 2) 1113-1114.

68 Her iki şart birlikte bulunmadan tedbire karar verilmesi hukuka aykırı olduğu gibi, elde edilen deliller de hukuka aykırı delil olarak kabul edilecektir. Hukuka aykırı deliller hakkında ayrıntılı bilgi için bkz. Murat Volkan Dülger, *Ceza Muhakemesi Hukukunda Dışlama Kuralı ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağacın Meyvesi Öğretisi)* (Seçkin Yayıncılık, 2014) 33 vd.

69 Şahin (n 12) 274; Aynı yönde bkz. Şen ve Eryıldız (n 66) 191; Danıştay 10. Dairesi'nin E. 2012/1001, K. 2017/1361 ve 09.03.2017 tarihli kararı ile iptaline karar verilen Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmeliğin 4. maddesinde *"Başka suretle delil elde edilmesi imkanının bulunmaması hâli: Soruşturma veya kovuşturma sırasında diğer tedbirlere başvurulmuş olsa bile sonuç alınamayacağı hususunda bir beklentinin varlığı veya başka yöntemlerden biri veya birkaçının uygulanmasına rağmen delil elde edilememesi ve delillere ancak bu Yönetmelikte düzenlenen tedbirlerle ulaşılabilecek olmasını"* ifade eder şeklinde tanımlanmıştır.

70 Aktaş (n 57) 223.

genellikle başka surette delil elde etme imkanının bulunmadığından söz edilebilecektir[71].

CMK m. 134 hükmünün normatif yapısı gereği, soruşturmaya konu suçla ilgili delil araştırması yapılmış ancak herhangi bir delil elde edilememişse bu hususun açıkça tutanağa bağlanması gerekir. Ancak uygulamada başka surette delil elde etme imkanının neden bulunmadığı hususu hemen hemen hiç belirtilmemektedir[72]. Doktrinde bir görüşe göre, bilişim alanındaki suçlar ve bilişim sistemleri kullanılarak işlenen suçlar yönünden yapılan soruşturmalarda, başka surette delil elde etme imkanının bulunmamasına ilişkin şartın aranması hatalı bir yaklaşımdır. Zira hem bilişim suçlarında hem de bilişim sistemleri aracılığıyla işlenen suçlarda yapılması gereken ilk iş, sistem içinde yer alan verilerin ve bağlantıların tespitidir. Kaldı ki, bu suçlar hakkında yürütülen soruşturmalarda, başka surette delil elde etme imkanı çoğunlukla bulunmamaktadır. Öncelikle diğer tedbirlerin uygulanması yoluna gidildiğinde ise faillere ve delillere ulaşmak son derece güç olmaktadır. Ayrıca teknolojinin hayatın her alanına nüfuz etmesi nedeniyle, klasik suçlara ilişkin soruşturmalarda bile dijital delillere başvurulması adeta bir zorunluluk haline gelmiştir. Bu nedenle CMK m. 134 hükmünde değişiklik yapılması ve çağın gereklerine uygun hale getirilmesi gerektiği belirtilmiştir[73].

Belirtelim ki, bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirine başvurulabilmesi için öngörülen temel şartlardan biri, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığıdır. Ancak yukarıda da ifade edildiği gibi kuvvetli şüphe yalnızca soruşturma konusu suçun işlendiğine yönelik olmamalı, aynı zamanda şüphelinin kullandığı bilişim sisteminden suç soruşturmasıyla ilgili delil elde edilebileceğine de yönelik olmalıdır[74]. Dolayısıyla gerek bilişim alanındaki suçlar gerekse bilişim sistemleri kullanılarak işlenen suçlar söz konusu olduğunda, somut delillere dayanan kuvvetli suç şüphesi, şüphelinin kullandığı bilişim sistemlerinden soruşturma konusu suça ilişkin delil elde edilebileceğine de yöneliktir. Böylesine kuvvetli bir şüphenin bulunduğu hallerde, son çare olarak bu tedbire başvurulmasını aramak tedbirin şartları arasında çelişkiye neden olmaktadır. Öte yandan, bu tedbirin temel hak ve özgürlüklere ağır bir müdahale teşkil ettiğini kabul ediyor olmakla birlikte,

71 Şahin (n 12) 274.

72 Dülger (n 3) 601; Ayrıca bkz. Feridun Yenisey ve Ayşe Nuhoğlu, *Ceza Muhakemesi Hukuku* (6. Baskı, Seçkin Yayıncılık, 2018) 412.

73 Dülger (n 3) 601; Yine bu görüş, CMK m.134/f.1 hükmüne bir istisna getirilmesini ve TCK'nın bilişim alanında suçlar bölümünde ve 135, 136, 138, 148/2-e ve 158/1-f maddelerinde yer alan suçlar için başka surette delil elde etme imkanının bulunmaması şartının kaldırılması gerektiği kanaatindedir. Bkz. Dülger (n 3) 602.

74 Bkz. yuk. II, B, 1.

ister bilişim suçları isterse bilişim sistemleri kullanılarak herhangi bir suç işlendiği takdirde, suça ilişkin delillerin bulunacağı ilk yer bilişim sistemleri olacaktır. Bu nedenle biz de CMK m.134 hükmünün yeniden düzenlenmesi gerektiği kanaatindeyiz.

C. Tedbire Karar Vermeye Yetkili Olan Merci

CMK'nın 134. maddesinin ilk halinde, bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirine Cumhuriyet savcısının istemi üzerine hakim tarafından karar veriliyordu. Bahse konu tedbire karar verme yetkisi yalnızca hakime aitti. Ancak 25 Temmuz 2018 tarihli ve 7145 sayılı Kanun'un 16. maddesiyle, CMK'nın 134. maddesinin 1. fıkrası değişikliğe uğramış ve *"Cumhuriyet savcısının istemi üzerine"* ibaresi *"hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından"* şeklinde değiştirilmiştir. Ayrıca yine bu maddenin 1. fıkrasında yer alan *"hâkim tarafından"* ibaresi de madde metninden çıkarılmıştır. Buna göre, bir suç dolayısıyla yapılan soruşturmada, bu tedbire hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından karar verilebilecektir. Görüldüğü üzere, 2018 yılında yapılan bu değişiklikle, tedbire karar verme bakımından yalnızca hakim değil, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı da yetkili hale gelmiştir. Hemen belirtelim ki, burada hakim ile kastedilen, CMK m. 162 hükmü doğrultusunda sulh ceza hakimidir.

7145 sayılı Kanun'la yapılan değişiklikle, yalnızca hakime ait olan bir yetkinin, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısına da verilmesi olumlu bir düzenleme olarak karşımıza çıkmaktadır. Zira CMK'nın 134. maddesinde yer alan koruma tedbirine, gecikme olmaksızın başvurulmasını gerektiren haller söz konusu olabilir. Özellikle, bilişim sistemlerinde bulunan verilerin kolaylıkla silinebilmesi ya da bulutta[75] bulunan verilerin kolaylıkla tahrif edilebilmesi nedeniyle, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısına, bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirine karar verme yetkisi verilmesi, delillere ulaşabilmek bakımından son derece önem arz etmektedir[76]. Nitekim 7145 sayılı Kanun'un gerekçesinde de açıklandığı üzere, söz konusu düzenlemeyle, gecikmesinde sakınca bulunan hallerde 134. maddede belirtilen tedbirlere Cumhuriyet savcısı tarafından da karar verilebilmesine imkan sağlanmak suretiyle, delillerin bir an evvel elde edilebilmesi ve suçla etkin mücadele edilebilmesi amaçlanmıştır[77].

75 Bulut bilişim hakkında bkz. aşa. II, D, 2.

76 Değirmenci (n 8) 151.

77 <https://www2.tbmm.gov.tr/d27/2/2-0001.pdf> Erişim Tarihi 20 Mayıs 2022.

Düzenlemeyle, Anayasa'nın 20. maddesine uygun olarak Cumhuriyet savcısı tarafından verilen kararların hakim onayına sunulacağı öngörülmüş ve bu konuda bir teminat oluşturulmuştur. Şöyle ki, CMK'nın 134. maddesinin 1. fıkrasına, 7145 sayılı Kanun'un 16. maddesiyle eklenen cümle uyarınca, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından verilen kararlar yirmi dört saat içinde hâkim onayına sunulacaktır. Hâkim de bu konudaki kararını en geç yirmi dört saat içinde verecektir. Sürenin dolması veya hâkim tarafından onay verilmemesi hâlinde çıkarılan kopyalar ve çözümü yapılan metinler derhâl imha edilecektir. Aksi halde, TCK'nın *"Verileri yok etmeme"* başlıklı 138. maddesinde düzenlenen suç oluşacaktır.

Bundan başka, 5271 sayılı CMK'da *"gecikmesinde sakınca bulunan hal"* kavramı tanımlanmamıştır. Bu kavram, Adli ve Önleme Aramaları Yönetmeliği'nin *"Tanımlar"* başlıklı 4. maddesinde, *"Adli aramalar bakımından; derhal işlem yapılmadığı takdirde suçun iz, eser, emare ve delillerinin kaybolması veya şüphelinin kaçması veya kimliğinin tespit edilememesi ihtimalinin ortaya çıkması ve gerektiğinde hakimden karar almak için vakit bulunmaması hâli"* olarak tanımlanmıştır. Eğer Cumhuriyet savcısı, gecikmesinde sakınca bulunan bir hal mevcut olmamasına rağmen CMK m. 134 kapsamında tedbir kararı vermişse, bu karar hakim onayına sunulsa bile hukuka aykırı bir karar olarak kabul edilecektir. Dolayısıyla yasal koşullar oluşmadan verilen bir karar kapsamında icra edilen arama, kopyalama ve elkoyma işlemleri sırasında elde edilen deliller de hukuka aykırı olmaları nedeniyle suçun ispatında kullanılamayacaktır[78].

Bu başlık altında üzerinde durulması gereken konulardan biri de Cumhuriyet savcısının yetkisinin kapsamıdır. İfade edildiği üzere, 7145 sayılı Kanun'la yapılan değişiklikten önce CMK'nın 134. maddesinde düzenlenen tedbire karar verme yetkisi münhasıran hakime aitti. Ancak 7145 sayılı Kanun'un 16. maddesiyle, CMK'nın 134. maddesinin 1. fıkrası değişikliğe uğramış ve gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı, bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılması, bilgisayar kayıtlarından kopya çıkarılması ve bu kayıtların çözülerek metin hâline getirilmesi işlemleri yönünden yetkilendirilmiştir. Görüldüğü üzere, CMK m.134/f.1

78 Değirmenci (n 8) 151; Gecikmesinde sakınca bulunmayan hallerde Cumhuriyet savcısı tarafından verilen ve icra edilen kararın zaten hakim onayına sunulacağı ve dolayısıyla bu yöndeki endişelerin yersiz olduğu düşünülebilir. Ne var ki, bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirine karar verirken çok dikkat ve özenle inceleme yapan sulh ceza hakimi, aynı dikkat ve özeni Cumhuriyet savcısı tarafından verilen ve icra edilen kararların onaylanması esnasında göstermeyebilir. Bkz. Değirmenci (n 8) 151; Zira Cumhuriyet savcısı tarafından verilen ve sonradan hakim onayına sunulan kararın yasal koşulları taşıdığı düşünülebilir. Nitekim CMK'nın 134. maddesinde yer alan bu tedbirin, özel hayata ve pek çok hukuki değere müdahale oluşturan bir tedbir olması nedeniyle, Cumhuriyet savcısı tarafından verilen kararlarda gecikmede sakınca bulunduğuna ilişkin belirlemenin itinayla yapılması gerekmektedir.

hükmünde elkoyma tedbirine yer verilmemiştir. Bu tedbir m.134/f.2 hükmünde düzenlenmiştir. Bu nedenle, savcının yalnızca CMK'nın 134. maddesinin 1. fıkrasında yer alan tedbirler bakımından yetkili olduğu; 2. fıkrada düzenlenen elkoyma tedbiri bakımından ise münhasıran hakimin yetkili olduğu düşünülebilir[79]. Her ne kadar elkoyma tedbiri CMK m.134/f.2 hükmünde düzenlenmiş olsa da 134. maddenin kenar başlığı *"Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma"* şeklinde düzenlenmiştir. Dolayısıyla tedbire karar vermeye yetkili olan mercilerin, elkoyma tedbiri bakımından da yetkili olduklarının kabulü gerekir. Bir başka ifadeyle, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da elkoyma tedbirine karar verilebilecektir. Kanaatimizce tüm bu tereddütlerin giderilmesi adına, CMK'nın 134. maddesinin 1. fıkrasında arama, kopyalama ve kayıtların çözülerek metin haline getirilmesi tedbirinin yanı sıra, elkoyma tedbirine de yer verilmelidir.

Yine bu başlık altında değinilmesi gereken bir başka konu ise CMK m.134 hükmünde düzenlenen tedbire, kovuşturma evresinde başvurmanın mümkün olup olmadığıdır. Doktrinde CMK m. 134 hükmünün yalnızca soruşturma evresinde uygulanacak bir düzenleme olduğunu savunanlar olduğu gibi, bu tedbirin kovuşturma evresinde uygulanabileceğini ileri sürenler de vardır. Dolayısıyla doktrinde tedbire kovuşturma evresinde de başvurulabileceğine ilişkin bir uzlaşı mevcut değildir.

Bu konuda doktrinde ileri sürülen bir görüş, Kanun'da "bir suç dolayısıyla yapılan soruşturmada", "şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde/dosyalarında arama"dan ve ayrıca "hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından" karar verilmesinden söz edilmesi sebebiyle, bu kavramların düzenlemenin soruşturma evresine ait olduğunu ortaya koyduğu kanaatindedir. Ayrıca bu görüşe göre, Kanun'da söz konusu tedbire kovuşturma evresinde de başvurulabileceğine ilişkin bir düzenlemeye yer verilmemiştir. Öte yandan, aleni bir duruşmada mahkemenin CMK m.134 hükmünde düzenlenen tedbire karar vermesi halinde, bu tedbirden haberdar olan ilgili kişiler söz konusu kayıtları yok edebilecek ve dolayısıyla kovuşturma evresinde bu tedbire başvurulması hiçbir fayda sağlamayacaktır[80].

79 Değirmenci (n 8) 151.

80 Centel ve Zafer (n 8) 449; Tedbire yalnızca soruşturma evresinde başvurulabileceğine ilişkin görüşler için bkz. bkz. Mustafa Artuç, *Pratik Ceza Muhakemesi Kanunu* (2. Baskı, Adalet Yayınevi, 2018) 134; Apiş (n 5) 71; Ünver ve Hakeri (n 15) 429; Yaşar ve Otacı (n 2) 1115; Özde Dereboylular, "Bulut Bilişim Bakımından Arama ve Elkoymaya İlişkin Hükümlerin Uygulanabilirliği" (2019) 14 (19) Ceza Hukuku Dergisi 182; Hakan Karakehya, *Ceza Muhakemesi Hukuku* (2. Baskı, Savaş Yayınevi, 2016) 349; Yenisey ve Nuhoğlu (n 72) 412.

Doktrinde, yargılama sırasında delil toplanmasını engelleyen bir düzenleme olmadığını, mahkemenin re'sen araştırma yetkisine sahip olduğunu ve dolayısıyla kovuşturma evresinde bu tedbire başvurulmasının önünde bir engel bulunmaması gerektiğini ileri süren görüşler de bulunmaktadır[81]. Yargıtay kararları da söz konusu tedbire kovuşturma evresinde başvurulabileceği yönündedir[82].

Biz bu konuda gerek yukarıda yer verilen gerekçeler gerekse temel haklara müdahale niteliğinde olan koruma tedbirlerine ilişkin sınırların kanunla düzenlenmesi gerektiğinden hareketle, CMK'nın 134. maddesindeki düzenlemenin, soruşturma evresine ilişkin olduğu yönündeki görüşe katılmaktayız. Ancak yine de doktrindeki tartışmaların ve bu alandaki belirsizliğin önlenmesi amacıyla, bu hususta bir düzenleme yapılması yerinde olacaktır.

Son olarak, CMK'nın 134. maddesinde *"Bir suç dolayısıyla yapılan soruşturmada"* ibaresine yer verildiğinden, bu tedbire yalnızca CMK kapsamında bir suçu ortaya çıkarmak amacıyla yürütülen soruşturma kapsamında başvurulabilecektir. Buna göre, burada soruşturma ile ifade edilmek istenen adli soruşturmalar olduğundan, idari ya da disiplin soruşturması gibi hukukun diğer alanlarında yürütülen soruşturmalar bakımından bu tedbire başvurulamayacaktır[83].

D. Tedbirin Uygulanma Şekli

1. Genel Olarak

Çalışma konumuz olan bilişim sistemlerinde arama, kopyalama ve elkoyma tedbiri, tüm suçlarla ilgili uygulanabilen bir tedbirdir. Kanun koyucu, bu tedbirin uygulanması

81 Bkz. Şahin (n 12) 278; Ünal (n 4) 99-100; Aktaş (n 57) 222; Yaşar ve Dursun (n 1) 9; Değirmenci (n 8) 318.

82 *"Mümkün olduğu takdirde katılanın ve sanığın suç tarihinde kullandıkları bilgisayarlara el konulup teknik bilirkişi tarafından hard disklerinin, suç tarihine ilişkin LOG kayıtları bakımından karşılıklı olarak incelenmesi, suç tarihinde bilişim sistemindeki verilerin bozulup bozulmadığı, yok edilip edilmediği, değiştirilip değiştirilmediği veya erişilmez kılınıp kılınmadığı, sisteme veri yerleştirilip yerleştirilmediği, var olan verilerin başka bir yere gönderilip gönderilmediği, nereye gönderildiği saptanıp, sonucuna göre, toplanan deliller değerlendirilerek sanığın hukuki durumunun takdir ve tayini gerekirken, eksik incelemeye dayanarak yazılı şekilde hüküm kurulması…"* Yargıtay 8. CD., E. 2018/10160, K. 2019/15726, 25.12.2019 <www.kazancı.com.tr>Erişim Tarihi 21 Mayıs 2022; Yargıtay Ceza Genel Kurulu, E. 2017/956, K. 2017/370, 26.09.2017; <www.lexpera.com> Erişim Tarihi 24 Ağustos 2022.

83 Ünal (n 4) 100; Yaşar ve Dursun (n 1) 8.

bakımından suç sınırlaması yapmamıştır[84]. Bu bağlamda, dijital delillerin toplanması amacıyla oldukça sık başvurulan bir koruma tedbiri olan CMK m. 134 hükmünde yer alan düzenlemenin, yalnızca bilişim suçlarına ilişkin soruşturmalarda başvurulabilecek bir tedbir olduğunu düşünmek hatalı bir yaklaşım olacaktır. Gerek klasik suçlar gerekse bilişim suçları olmak üzere, dijital delillerin toplanmasını gerektiren tüm soruşturmalarda ilgili koruma tedbirine başvurulabilecektir[85]. Madde metninde geçen *"bir suç dolayısıyla yapılan soruşturma"* ibaresi de tedbirin her türlü suç yönünden tatbik edilebileceğini ortaya koymaktadır.

CMK m.134 hükmü bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma işlemine yöneliktir. Tedbirin genel şartlarının düzenlendiği CMK m.134/f.1 hükmüne göre bu tedbir kural olarak, bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına ve bu kayıtların çözülerek metin hâline getirilmesine olanak sağlamaktadır. Görüldüğü üzere, bu fıkrada elkoyma işlemine yer verilmemiştir. Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama tedbirine ilişkin usul ve esaslara maddenin 1. fıkrasında; kopyalama işlemine 1. ve 5. fıkralarda; elkoyma tedbirine ilişkin düzenlemelere ise 2, 3 ve 5. fıkralarda yer verilmiştir[86]. Bahse konu tedbirler, aşağıda ayrı alt başlıklar halinde incelenerek açıklanacaktır.

2. Arama

Bu başlık altında öncelikle genel arama ile bilişim sistemlerinde arama arasındaki temel farka değinecek olursak, genel aramanın konusu maddi niteliği bulunan bir mal iken, CMK m.134 hükmünde yer alan arama tedbirinin konusu gayri maddi niteliğe

84 Artuç (n 80) 465; Parlar ve Çetin (n 13) 436; Doktrinde ileri sürülen bir görüşe göre, CMK m.134'te düzenlenen koruma tedbiri, ceza üst sınırı ya da katalog suç öngörmemesi nedeniyle hatalı bir düzenlemedir. Zira CMK'nın 134. maddesinde düzenlenen "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" tedbiri ile CMK'nın 135. maddesinde düzenlenen "İletişimin tespiti, dinlenmesi ve kayda alınması" tedbiri, teknolojik gelişmelerden istifade edilerek uygulanan ve kişilerin temel hak ve özgürlüklerine müdahale oluşturan koruma tedbirleridir. İletişimin tespiti, dinlenmesi ve kayda alınması koruma tedbiri, haberleşme hakkına, haberleşmenin ve özel hayatın gizliliğine ağır müdahale oluştururken; bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbiri, kişilerin özel hayatıyla birlikte ticari ve bilimsel sırlarına, dahası kişisel verilerine müdahale teşkil etmektedir. Oysa Anayasa ile güvence altına alınmış bu haklar arasında bir hiyerarşiden söz etmek mümkün değildir. Dolayısıyla CMK m. 135'te düzenlenen koruma tedbiri yönünden katalogda yer alan suçların varlığı aranırken, CMK m. 134'teki tedbirin uygulanması yönünden herhangi bir suç sınırlaması yapılmaması koruma tedbirlerinin orantılılığı ilkesiyle uyuşmamaktadır. Bkz. Yaşar ve Dursun (n 1) 10-11; Bu konuda doktrinde ileri sürülen bir başka görüş de CMK m.134'te düzenlenen tedbirin kişilik haklarına tecavüz oluşturduğunu belirterek söz konusu tedbirin yalnızca belli ağırlıktaki suçlar yönünden uygulanmasını ifade etmiştir. Bkz. Centel ve Zafer (n 8) 450; Aynı yönde bkz. Yaşar ve Otacı (n 2) 1113.

85 Değirmenci (n 8) 310.

86 Yaşar ve Dursun (n 1) 6.

sahip veridir[87]. Gelişen teknoloji ve bilişim sistemlerinin yaşamın her alanına nüfuz etmesi neticesinde, arama ve elkoyma tedbirine konu olan şeylerin niteliğinde de bir değişim meydana gelmiştir[88]. Bu bakımdan, bilişim sistemlerinde veri arama, genel arama tedbirinin verilere uyarlanmış halidir. Şüpheli tarafından kullanılan bilişim sistemleri üzerinde arama yapılmasındaki amaç ise suçun ispatına yarayan delilleri elde etmektir.

Bilişim sistemlerinde yapılacak aramanın hukuki niteliği adli aramadır[89]. Arama tedbirine, bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin ortaya çıkması ve başka surette delil elde etme imkanının bulunmaması halinde hakim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından karar verilebilecektir. Arama kararının verilmesinin ardından, kolluk güçleri aracılığıyla söz konusu tedbirin konusunu oluşturan araç ve gereçlerde arama faaliyetine başlanacaktır. Her ne kadar CMK'nın 134. maddesinde arama faaliyetinin kim tarafından yapılacağına ilişkin bir düzenlemeye yer verilmemiş olsa da uzmanlık gerektiren bu faaliyetin adli kolluğun uzman birimleri ya da CMK'nın 63. maddesi uyarınca atanacak bilirkişiler tarafından –kolluk güçleri ve diğer kişilerin huzurunda- yapılacağını söyleyebiliriz[90]. Ayrıca ifade etmemiz gerekir ki, üzerinde arama yapılacak araçların bulundukları yerden başka bir yere götürülmelerine gerek yoktur. Tedbire konu araçların bulunduğu yerde arama faaliyeti gerçekleştirilebilecektir.

Belirtelim ki, üzerinde veri aranacak sistem şüpheliye ait olabileceği gibi üçüncü bir kişiye ya da resmi bir kuruluşa da ait olabilir[91]. CMK m.134/f.1 hükmünde *"şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde"* ibaresine yer verilmiş olduğundan, bu sistemin şüpheliye ait olması aranmamış, şüpheli tarafından

87 Değirmenci (n 8) 76.

88 Özbek ve diğerleri (n 46) 427.

89 Adli ve Önleme Aramaları Yönetmeliği'nin *"Adli arama ve kapsamı"* kenar başlıklı 5. maddesinde adli arama, *"bir suç işlemek veya buna iştirak veyahut yataklık etmek makul şüphesi altında bulunan kimsenin, saklananın, şüphelinin, sanığın veya hükümlünün yakalanması ve suçun iz, eser, emare veya delillerinin elde edilmesi için bir kimsenin özel hayatının ve aile hayatının gizliliğinin sınırlandırılarak konutunda, işyerinde, kendisine ait diğer yerlerde, üzerinde, özel kâğıtlarında, eşyasında, aracında 5271 sayılı Ceza Muhakemesi Kanunu ile diğer kanunlara göre yapılan araştırma işlemi"* şeklinde ifade edilmiştir. Bilişim sistemlerinde önleme aramasının uygulanıp uygulanamayacağı hususuna da değinecek olursak, kanun koyucu yalnızca adli aramalar yönünden bir düzenleme getirmiş olduğundan, CMK m.134'te yer alan tedbirin önleme aramalarında uygulanması kişi hak ve özgürlüklerine orantısız bir müdahale teşkil edecektir. Detaylı bilgi için bkz. Değirmenci (n 8) 336.

90 Yaşar ve Dursun (n 1) 21-22.

91 Centel ve Zafer (n 8) 448.

kullanılması yeterli görülmüştür[92]. Dolayısıyla üçüncü bir kişiye ait olmasına rağmen, şüpheli tarafından kullanılan sistem üzerinde arama, kopyalama ve elkoyma tedbirine başvurulabilecektir[93].

CMK'nın 134. maddesinde arama kararının hangi hususları içermesi gerektiğine ilişkin bir düzenlemeye yer verilmemiştir. Ancak ceza muhakemesi hukukunda kanunda boşluk olan hallerde, hakkında hüküm bulunmayan duruma en çok benzeyen durumu düzenleyen hukuk kurallarının uygulanması kabul edildiğinden[94], kıyas yoluyla genel aramaya ilişkin CMK m. 119/f.2 hükmü uygulanabilecektir. Buna göre, CMK m.134 hükmü uyarınca verilmiş bir arama kararında, CMK m.119/f.2 hükmünde yer alan hususlar açıkça gösterilmelidir. Bu bağlamda, bilişim sistemlerinde aramanın nedenini oluşturan fiil, şüphelinin kimliği, aramanın yapılacağı eşya[95], arama kararının geçerli olacağı zaman süresi kararda belirtilmelidir[96]. Öte yandan, bilişim sistemlerinde arama, kopyalama ve elkoyma tedbiri bakımından, somut delillere dayanan kuvvetli şüphe sebepleri ve başka surette delil elde etme imkanının neden bulunmadığı da kararda gösterilmelidir[97].

92 Aktaş (n 57) 220; Yaşar ve Dursun (n 1) 21; *"CMK'nın 134/1. maddesinde "şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde" arama ve kopyalama işleminin yapılabileceği belirtilmiştir. Kanun koyucu, söz konusu maddede arama ve kopyalama işlemlerinin yapılacağı araçların şüpheliye ait olmasını aramamış, şüphelinin fiilen bu araçları kullanıyor olmasını yeterli görmüştür. Maddede özellikle "şüphelinin kullandığı" ifadesine yer verilmiştir; zira üzerinde arama ve kopyalama işlemi yapılacak bilişim sisteminin şüpheliye ait olması gerekmez. Şüphelinin maliki olduğu, kiraladığı, ödünç aldığı ya da ortak kullanıma açık bir bilgisayarı eylemini gerçekleştirirken kullanması bu tedbirin uygulanması için yeterlidir."* Yargıtay Ceza Genel Kurulu, E. 2022/9-51, K. 2022/141, 03.03.2022 <www.kazancı.com.tr> Erişim Tarihi 22 Mayıs 2022; Yargıtay Ceza Genel Kurulu, E. 2019/ 295, K. 2021/ 545, 11.11.2021 <www.lexpera.com> Erişim Tarihi 24 Ağustos 2022.

93 Ünver ve Hakeri (n 15) 428; Karakehya (n 80) 350; Dülger (n 3) 599; CMK m. 134 hükmünde, diğer kişilere ait bilişim sistemleri üzerinde tedbirin ne şekilde uygulanacağı yönünde bir açıklık bulunmamaktadır. Bu konuda doktrinde ileri sürülen bir görüşe göre, tedbirin konusunu oluşturan araçların üçüncü bir kişiye ait olması halinde CMK'nın *"Diğer kişilerle ilgili arama"* başlıklı 117. maddesi kıyasen uygulanmalıdır. Bkz. Yaşar ve Dursun (n 1) 21; CMK m. 134'te düzenlenen tedbirin mağdurun bilişim sistemlerinde uygulanıp uygulanamayacağı hakkında bkz. Değirmenci (n 8) 322 vd.; Ünal (n 4) 93; Çelik (n 44) 34; Tanrıkulu (n 40) 367.

94 Centel ve Zafer (n 8) 50.

95 Arama kararında, hangi bilişim sistemlerinde arama yapılacağı özelleştirilmelidir. Aksi takdirde tüm bilişim sistemlerinde veri araması yapılması rasyonel olmayacaktır. Bilişim sistemlerinin özelleştirilmesine ilişkin öneriler için bkz. Değirmenci (n 8) 354.

96 CMK'nın 134. maddesinde aramada hazır bulunabileceklerle ilgili bir düzenlemeye de yer verilmemiştir. Ancak ceza muhakemesinde mevcut hukuki boşluk kıyas yoluyla doldurulabilecektir. Bu durumda genel aramaya ilişkin olarak CMK'nın *"Aramada hazır bulunabilecekler"* başlıklı 120. maddesi kıyasen uygulanabilecektir. Yine CMK m.134 hükmüne göre yapılan arama sonrasında verilecek belge yönünden de genel aramaya ilişkin CMK m.121 hükmünden istifade edilebilecektir.

97 Değirmenci (n 8) 354.

Bilişim sistemlerinde, şüphelinin internet ortamında veya sosyal ağlar üzerinde gerçekleştirdiği iletişime ilişkin kayıtların aranması da bu başlık altında üzerinde durulması gereken konulardan biridir. Acaba söz konusu kayıtların aranması CMK m.134 hükmüne göre mi yoksa iletişimin tespiti, dinlenmesi ve kayda alınması koruma tedbirinin düzenlendiği CMK m.135 hükmüne göre mi yapılacaktır? Belirtmek gerekir ki, CMK m. 135 uyarınca iletişimin tespiti, dinlenmesi ve kayda alınması koruma tedbirine geçmişe değil, geleceğe dönük olarak başvurulabilir. Başka bir ifadeyle, geçmişte yapılan iletişimin dinlenmesi ve kayda alınması mümkün değildir. Fakat internet ortamında gerçekleştirilen iletişime ilişkin kayıtlar, bilgisayar kütüklerinde kaydedildiğinden, bu iletişim kayıtları hakkında CMK m. 134 hükmü kapsamında arama, kopyalama ve elkoyma tedbirine başvurulabilecektir[98].

Yine bu başlık altında ele alınması gereken hususlardan biri de bulutta[99] aramadır. Zira failler, suç delillerini saklamak veya bilişim sistemlerine karşı gerçekleştirecekleri saldırıları planlamak amacıyla yerel bilişim sistemleri yerine bulut ortamını kullanmaktadırlar[100]. Bu nedenle, bulut bilişimde saklanan veriler bakımından CMK m.134 hükmünün uygulanıp uygulanamayacağını değerlendirmemiz gerekecektir. İlk olarak, bulut hizmetinin özel ve dar bir ağda verilmesi haline ilişkin bir değerlendirme yapmamız gerekirse, bu ihtimalde şüpheliye ait hesap bilgilerinin CMK m.134 kapsamında alınacak bir arama kararıyla elde edilmesi mümkündür. Böylece şüphelinin hesap bilgilerine ait olan veriler elde edilebilecek ve kopyalanabilecektir[101].

98 Yaşar ve Dursun (n 1) 23; *"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."* Yargıtay Ceza Genel Kurulu, E. 2022/9-51, K. 2022/141, 03.03.2022 <www.kazancı.com.tr> Erişim Tarihi 22 Mayıs 2022; CMK m.134 hükmünün elektronik postalar yönünden uygulanıp uygulanamayacağına ilişkin olarak bkz. Değirmenci (n 8) 332-333.

99 Bulut bilişim (cloud computing), tüm veri, bilgi, belge, yazılım ve uygulamaların internet bulutu üzerinde bulunan sanal bir depoda depolanmasını ve internet üzerinden ulaşılmasını sağlayan bir teknolojidir. Bkz. Kamil Çelik, "Bulut Bilişim Teknolojileri" (2021) 12 (24) Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi 438; Bulut bilişim hakkında ayrıca bkz. Won Kim, "Cloud Computing: Today and Tomorrow" (2009) 8 (1) Journal of Object Technology 65; Dereboylular (n 80) 164 vd.

100 Değirmenci (n 8) 237.

101 Değirmenci (n 8) 242.

Kamusal hizmet bakımından ise kamusal bulut hizmet sağlayıcısının yurt içinde ya da yurt dışında bulunmasına göre ikili bir ayrım yapılması gerekecektir. Kamusal bulut hizmetini sunan hizmet sağlayıcısının yurt içinde bulunması durumunda, CMK m.134 hükmü uyarınca verilen bir arama kararıyla bulutta arama yapılabileceği kabul edilmelidir. Zira kullanıcıya ait olan bir verinin kişinin bilgisayarında saklanması ile bulutta saklanması arasında bir farklılık yoktur[102]. Buna göre, bilgisayarlarda arama için gerekli olan arama kararı ile bulut ortamında da arama yapılabilmelidir. Kamusal bulut hizmetini sunan hizmet sağlayıcısının yurt dışında bulunması halinde ise bulut bilişimde arama yapılması ve verilere elkonulması adli yardımlaşma hükümleri kapsamında yerine getirilmelidir[103].

Burada son olarak, dijital haberleşme uygulaması olan Bylock iletişim sistemine değinmekte yarar görüyoruz. Yargıtay Ceza Genel Kurulu'nun 24.01.2019 tarihli ve 417-44 sayılı ve 20.12.2018 tarihli ve 419-661 sayılı kararlarında da ayrıntılarıyla belirtildiği üzere şifreli haberleşme uygulaması olan Bylock iletişim sistemi, global bir uygulama görüntüsü altında belli bir tarihten sonra yenilenen ve geliştirilen haliyle münhasıran silahlı terör örgütü mensuplarının kullanımına sunulmuş bir programdır[104]. İşte bu noktada, Bylock bilgilerinin CMK'nın *"Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma"* başlıklı 134. maddesi kapsamında mı yoksa *"İletişimin tespiti, dinlenmesi ve kayda alınması"* başlıklı 135. maddesi kapsamında mı elde edilebileceği değerlendirilmelidir. Bu konuda doktrinde ileri sürülen bir görüşe göre, haberleşme hakkına ilişkin Bylock bilgileri yalnızca CMK m. 135 kapsamında elde edilebilir. Öyle ki, haberleşmeye ilişkin yazışma içerikleri kişinin kullandığı bilgisayarda kayıtlı olsa da bu içeriklere ulaşılması CMK m. 135

102 Değirmenci (n 8) 243; Benzer yönde bkz. Dilek Özge Uğraş, "Bilgisayarlarda, Bilgisayar Programlarında ve Bilgisayar Kütüklerinde Arama, Kopyalama ve Elkoyma" (2021) 34 (154) Türkiye Barolar Birliği Dergisi 116.

103 Değirmenci (n 8) 243; Uğraş (n 102) 116.

104 Bylock uygulamasının bir örgüt faaliyetiyle ilişkilendirilebilecek özel bir iletişim aracı olup olmadığı hususuna ilişkin olarak bkz. Burcu Baytemir Kontacı, "Avrupa İnsan Hakları Mahkemesi ve Anayasa Mahkemesi Kararlarında Özel İletişim Araçlarının Kullanılmasının Ceza Sorumluluğu Üzerindeki Etkisi", *Anayasa Mahkemesi Kararları Işığında Hak ve Özgürlüklerin Sınırlandırılması Rejimleri Sempozyumu* (Seçkin Yayıncılık, 2022) 558 vd.; Ayrıca bkz. İzzet Özgenç, *Suç Örgütleri* (Seçkin Yayıncılık, 2022) 115 vd.; Bylock programının genel özelliklerine ilişkin tespit ve değerlendirmeler için bkz. AYM, *Aydın Yavuz ve diğerleri*, Başvuru No: 2016/22169, 20.06.2017, para. 106; Bylock programına ilişkin açıklamalar hakkında ayrıca bkz. AYM, *M.T.*, Başvuru No: 2018/10424, 04.06.2020; AYM, *Ferhat Kara*, Başvuru No: 2018/15231, 04.06.2020; Bir bireyin, bir suç örgütü tarafından özel olarak tasarlanmış ve münhasıran bu örgütün iç iletişimi amacıyla kullanılan şifreli bir mesajlaşmayı kullandığını doğrulayan elektronik delil kullanımının, örgütlü suçla mücadelede oldukça önemli bir araç olabileceğine ilişkin değerlendirme hakkında bkz. AİHM, *Akgün v. Türkiye*, Başvuru No: 19699/18, 20.07.2021, para.167.

hükmüne göre verilmiş bir hakim kararına bağlıdır[105]. Kanaatimizce, Bylock uygulamasına ait sunucular üzerindeki verilerin elde edilmesi, Bylock verilerini içeren hard disk ve flash belleğin incelenmesi CMK'nın 134. maddesi gereğince yapılmalıdır. Bylock uygulamasının haberleşmeyi sağlayan bir sistem olması, doğrudan CMK'nın 135. maddesinin uygulanması sonucunu doğurmaz. Söz konusu iletişime ilişkin bilgiler, bir sunucu bilgisayardan elde edildiğinden Bylock iletişim sisteminin kullanımı sonucu oluşan verilerin tespitinin CMK'nın 134. maddesinde belirlenen esas ve usuller çerçevesinde yapılması gerektiği kanaatindeyiz. Bir diğer ifadeyle, internet ortamında gerçekleştirilen iletişime ilişkin kayıtlar, bilgisayar kütüğünde kaydedildiğinden, bu iletişim kayıtları hakkında CMK'nın 134. maddesindeki koruma tedbiri uygulanmalıdır. Yargıtay'ın konuya ilişkin görüşü de bu yöndedir[106].

3. Elkoyma

Kanun koyucu, bilişim sistemlerinde veri arama bakımından öncelikle yerinde aramayı öngörmüştür. Ancak yerinde arama işlemi her zaman mümkün olmamaktadır. İşte bu nedenle, CMK m.134/f.2 hükmünde bilişim sistemlerine elkoyma tedbiri özel olarak düzenlenmiştir. İlgili hüküm incelendiğinde görülecektir ki, kanun koyucu elkoyma tedbirine başvurulabilmesi için birtakım şartların varlığını aramıştır. CMK m.134/f.2 düzenlemesine göre bilişim sistemlerine *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. Görüldüğü üzere, CMK m.134/f.2 hükmü bağlamında elkoyma tedbirinin amacı, dijital delillere ilişkin çözümün yapılması ve gerekli kopyaların alınmasıdır.

Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde elkonulan cihazlar gecikme olmaksızın iade edilmelidir[107]. Madde metninde yer alan *"gecikme olmaksızın"* ibaresinden anlaşılması gereken husus, incelemenin makul sürede bitirilmesidir. Dijital deliller üzerinde yapılacak incelemeler alınan kopya üzerinde yapılacağından, elkonulmak

105 Uğur Yeşil, *Hukuk ve İnsan Hakları Bağlamında Bylock Bilgilerinin Delil Değeri* (Alternatif Düşünce ve Medya Yayıncılık, 2018) 113.

106 Bkz. Yargıtay Ceza Genel Kurulu, E. 2017/956, K. 2017/370, 26.09.2017 <www.lexpera.com> Erişim Tarihi 24 Ağustos 2022; Yargıtay Ceza Genel Kurulu, E. 2019/ 295, K. 2021/ 545, 11.11.2021 <www.lexpera.com> Erişim Tarihi 24 Ağustos 2022.

107 CMK m.134 kapsamında elkonulan cihazların iadesi yönünden, genel elkoymaya ilişkin CMK'nın *"Elkonulan eşyanın iadesi"* başlıklı 131. madde hükmü uygulanmalıdır. Buna göre, şüpheliye, sanığa veya üçüncü kişilere ait elkonulmuş cihazların, soruşturma ve kovuşturma bakımından muhafazasına gerek kalmaması halinde, re'sen veya istem üzerine geri verilmesine Cumhuriyet savcısı, hakim veya mahkeme tarafından karar verilir. İstemin reddi kararlarına itiraz edilebilir.

suretiyle kopyası alınan cihazın derhal iadesi gerekmektedir[108]. Zira burada elkoyma bakımından önemli olan eşyalara elkonulması değil verilere elkonulmasıdır[109]. Ayrıca bilgisayar donanım ve yazılımlarına elkonulması, ilgili kişilerin anayasa tarafından koruma altına alınan haberleşme, kendini geliştirme ve mülkiyet hakkı gibi temel hak ve özgürlüklerinin sınırlandırılması anlamına geldiğinden, elkonulan araçların iadesi yasal bir zorunluluk olarak Kanun'da öngörülmüştür[110].

Doktrinde, gerekli kopyaların alınması halinde, elkonulan cihazların gecikme olmaksızın iade edileceğine ilişkin düzenlemenin ciddi sorunlar doğurabileceği ifade edilmiştir. Bu düzenlemenin şüphelinin haklarını teminat altına alma amacını güttüğü açıktır. Ancak suçun konusunu oluşturan verilerin cihazın içinde yer alması ciddi sonuçlar doğurabilecektir. Örneğin iade edilen cihazın içinde çocuk pornografisi içeren görüntülerin ya da mağdurun kredi kartı bilgileri gibi verilerin bulunması, suçun işlenmesine devam edilmesine kanun tarafından cevaz verildiği anlamına gelecektir[111]. Ne var ki, CMK m.134/f.2 hükmünde, iadesi gereken cihazlarda bulunan suç unsuru içeren veriler yönünden ne şekilde işlem yapılacağı düzenlenmemiştir. Bu konuda doktrinde ileri sürülen bir görüşe göre, suç unsuru içeren bu verilerin delil olarak kullanılacağı hallerde veya kamu davasının açılmış olduğu hallerde, söz konusu veriler delil olarak muhafaza edilmelidir. Kovuşturmaya yer olmadığı kararı ve beraat kararı verilmesi ya da suça konu verilerle ilgili işlem yapılmasının gerekli olmadığı hallerde[112] ise bu verilerin tamamen imhası yoluna gidilmelidir. Zira Avrupa Konseyi Siber Suç Sözleşmesi'nin m.19/f.3 (d) hükmü uyarınca, elde edilen veri veya programların suç unsuru teşkil etmesi halinde, bu verilere erişilememesi, kullanılamaz hale getirilmesi ve silinmesi öngörülmüştür[113]. Benzer şekilde, CMK düzenlemesinde de Sözleşme'nin ilgili maddesi göz önünde bulundurularak konusu suç oluşturan verilere ilişkin ne şekilde işlem yapılacağına ilişkin belirsizlik giderilmelidir. Bu gibi hallerde TCK'nın 54. maddesi gereğince eşya müsaderesine ilişkin hükümden istifade edilebilecekse de kanun koyucunun CMK m.134 hükmünde bu hususa ilişkin bir düzenlemeye yer vermemesi önemli bir eksiklik olarak karşımıza çıkmaktadır[114].

108 Özen ve Özocak (n 2) 63.

109 Şahin (n 12) 278.

110 Tanrıkulu (n 40) 407.

111 Özen ve Özocak (n 2) 70.

112 Bu hallere örnek olarak, verilerin ele geçirildiği şüphelinin ölümü ve CMK'nın 223. maddesi uyarınca ceza verilmesine yer olmadığı kararı verilmesi örnek olarak gösterilebilir. Bkz. Tanrıkulu (n 40) 408.

113 Tanrıkulu (n 40) 408.

114 Özen ve Özocak (n 2) 70.

7145 sayılı Kanun'la CMK'nın 134. maddesinin 2. fıkrası değişikliğe uğramadan önce elkoyma tedbirine başvurulabilmesi için bilişim sistemlerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması gerekiyordu. Ancak 7145 sayılı Kanun'un 16. maddesiyle, CMK m.134/f.2 hükmüne *"bilgilere ulaşılamaması"* ibaresinden sonra gelmek üzere *"ya da işlemin uzun sürecek olması"* ibaresiyle yeni bir şart eklenmiştir. Madde metnine, kopyalama işleminin uzun sürecek olması halinde araç ve gereçlere elkonulabilmesine olanak sağlayan bu yeni şartın eklenmesiyle, elkoyma tedbirinin uygulama alanı genişletilmiştir[115].

CMK m.123 gereğince genel elkoymadan farklı olarak bilişim sistemlerine elkoyma tedbiri, daha ağır şartlara tabi tutulmuştur. CMK m.123 hükmündeki düzenlemeye bakıldığında, malvarlığı değerlerine elkonulabilmesi için herhangi bir şart öngörülmemektedir. Ancak CMK m.134/f.2 hükmüne baktığımızda, elkoyma tedbirine başvurulabilmesi için yukarıda yer verilen üç şarttan birinin gerçekleşmesi zorunludur. Belirtelim ki, bilişim sistemlerine elkoyma tedbiri, genel elkoyma tedbirine kıyasen temel hak ve özgürlüklere daha fazla müdahaleyi gerektirdiğinden, kanun koyucu CMK m. 134 hükmünde öngörülen elkoyma tedbiri bakımından daha ağır şartlar öngörmüştür[116].

CMK m.134 kapsamında elkoyma tedbirine başvurulabilmesi için gerekli olan şartlara değinecek olursak, bu şartlardan ilki *şifrenin çözülememesinden dolayı bilişim sistemine girilememesidir.* Ancak gerekli kopyaların alınabilmesi için bu şifrenin çözülmesi gerekmektedir[117]. Şifreleme, sistemde yer alan verilerin karışık matematiksel algoritmalarla korunması olarak tanımlanmaktadır[118]. Bilgisayarın bulunduğu yerde şifrenin çözülememesi halinde, çözümün yapılması ve gerekli kopyaların alınması amacıyla elkoyma tedbirine başvurulabilecektir.

Elkoyma tedbiri için gerekli olan şartlardan bir diğeri ise *bilişim sistemlerinde gizlenmiş bilgilere ulaşılamamasıdır.* Bu ihtimalde ise sistemde herhangi bir şifre bulunmamasına ya da şifre bulunsa bile çözümü yapılmış olmasına rağmen, sistem içinde gizli bilgilere

115 Değirmenci (n 8) 150.

116 Değirmenci (n 8) 367.

117 Bilişim sistemlerinde şifrelenmiş veri, dosya şifrelenmesi ya da tüm disk şifrelenmesi şeklinde karşımıza çıkmaktadır. Dosyanın şifrelenmesi halinde, gerekli kopyaların alınabilmesi mümkündür. Söz konusu şifrelenmiş dosyanın kopyası alınarak adli bilişim laboratuvarında çözümü yapılabilecektir. Fakat tüm disk şifrelenmesi halinde, gerekli kopyaların alınabilmesi için şifrenin çözülmesi gerekecektir. Şifrenin makul bir sürede çözülmesinin olanaksız olduğu hallerde ise elkoyma ihtiyacı doğacaktır. Ancak şifre çözüldükten sonra kopyalama yapılabilecektir. Bkz. Değirmenci (n 8) 152.

118 Aktaş (n 57) 233.

ulaşılamıyor olabilir. Bu durumda, sistem üzerinde detaylı bir arama yapılması ihtiyacı doğabileceğinden, elkoyma tedbirine başvurulması zorunluluk arz edebilir[119]. Ancak bilgiler gizlenmiş olmasına rağmen, diskin kopyası alınabiliyorsa, elkoyma tedbirine başvurulması gerekmeyecektir. Ancak uygulamada 7145 sayılı Kanun'la yapılan değişiklikten önce, diskin kopyalanması işleminin uzun zaman alabilecek olması nedeniyle, elkoyma yapılabilmekteydi[120].

Son olarak, *işlemin uzun sürecek olması* halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için elkoyma tedbirine başvurulabilecektir. Olay yerine giden kolluk görevlileri, hangi nedenden ötürü elkoyma tedbirine başvurduklarını elkoyma tutanağına yazmalıdır. Örneğin, kopyalama işleminin uzun sürecek olması nedeniyle elkoyma durumunda, kopyalama işleminin neden uzun süreceğine ilişkin değerlendirme de tutanağa yazılmalıdır[121].

Kanunun açık ifadesi karşısında, bilişim sistemlerine elkoyma ancak 134. maddenin 2. fıkrasında sayılan hallerde mümkündür. Buna göre, şifrenin çözülememesi, gizlenmiş bilgilere ulaşılamaması ve işlemin uzun sürecek olması halleriyle sınırlı olmak üzere, çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi amacıyla bu araç ve gereçlere elkonulabilir. Bunun dışındaki hallerde elkoyma işlemi yapılamaz[122]. CMK m.134/f.2 hükmünde öngörülen şartlar gerçekleşmeden elkoyma yapılması halinde, hukuka aykırı bir elkoyma işleminden bahsedilecektir[123].

Düzenleme bu şekilde olmakla birlikte, ne yazık ki uygulama bu yönde değildir. Kural olan, yerinde arama yapılması ve yine sistemin bulunduğu yerde kopyalama işlemi yapılarak öncelikle bu tedbirlerin işletilmesidir. Ancak uygulamada kolluk güçleri tarafından CMK m.134/f.2 hükmünde yer alan istisna hükmü kural haline getirilerek sistemde şifre olduğu ya da gizli verinin bulunduğu gibi sözde gerekçelerle tutanak tutularak elkoyma tedbirine başvurulmaktadır[124]. Kanaatimizce, bu yolla elde edilen deliller hukuka aykırı delil olarak kabul edilmeli ve CMK m.217/f.2 hükmü uyarınca ceza yargılamasında hükme esas alınmamalıdır.

119 Yaşar ve Dursun (n 1) 15.
120 Değirmenci (n 8) 152.
121 Değirmenci (n 8) 154; Yaşar ve Otacı (n 2) 1119.
122 Artuç (n 80) 467.
123 Aldemir (n 50) 222.
124 Dülger (n 3) 602-603.

Yukarıda yapılan açıklamalardan anlaşılacağı üzere, bilişim sistemlerine elkonulabilmesi için her şeyden önce bu araç ve gereçler hakkında hukuka uygun şekilde verilmiş arama ve kopyalama kararı bulunması gerekir. Şunu ifade etmeliyiz ki, CMK m.134/f.2 hükmünde düzenlenen elkoyma tedbiri, CMK m.123 vd. hükümlerinde düzenlenen elkoyma tedbirinin özel bir görünümünü oluşturmaktadır. Ancak CMK m.123 hükmünde yer alan elkoyma tedbirinden farklı olarak, CMK m.134 kapsamında elkoyma işlemi yapılabilmesi için öncelikle elkonulacak araç ve gereçler hakkında verilmiş bir arama ve kopyalama kararı bulunmalıdır. Zira CMK m.134/f.2 hükmünde öngörülen elkoyma koruma tedbirine başvurulabilmesi için bilişim sistemlerine "şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması" şartlarından birinin gerçekleşmesi, öncelikle söz konusu araçlar üzerinde hukuka uygun olarak verilmiş bir arama ve kopyalama kararını zorunlu kılmaktadır[125].

CMK m.134/f.3 hükmünde ise bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesinin yapılacağı düzenlenmiştir. Böylece bir istisna hükmü olan CMK m.134/f.2 hükmünün işletilmesi halinde neler yapılması gerektiği hususuna yer verilmiştir[126]. Ne var ki, CMK m.134/f.3 hükmü bağlamında sistemdeki bütün verilerin yedeklemesinin yapılarak tüm verilerin denetlenmesine olanak sağlayan bu düzenleme, özel hayatın gizliliğini ihlal eder nitelikte bir düzenlemedir[127]. Bu nedenle, kişisel bir bilgisayar üzerinde yapılan inceleme sırasında gelişigüzel bütün dosyaların açılması, bu dosyalarda kişilerin özel hayatına ilişkin kişisel veriler bulunabileceğinden, Anayasa'nın 20. maddesinde ve Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde düzenlenen "özel hayatın gizli alanına" müdahale teşkil edebilecektir[128]. Dolayısıyla ölçülülük ilkesi açısından, bireye ait kişisel bilgilerin de yer aldığı verilerin tamamının yedeklenmesi yerine yalnızca soruşturmayla ilgisi bulunan verilerin yedeklenmesi yoluna gidilmelidir.

Öte yandan, Adli ve Önleme Aramaları Yönetmeliği m.17/f.3 hükmünde ise yedekleme işleminin, *"bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları"*[129] hakkında da uygulanacağı ifade edilmiştir. Bu konuda

125 Yaşar ve Dursun (n 1) 13-14; Şen ve Eryıldız (n 66) 188; Doktrinde ileri sürülen bir başka görüş ise bilişim sistemlerinde elkoyma tedbirine başvurulabilmesi için arama kararının varlığının zorunlu olmadığı yönündedir. Bkz. Değirmenci (n 8) 355.

126 Sistemdeki verilerin yedeklenmesiyle kastedilenin fiziksel kopyalama mı yoksa mantıksal kopyalama mı olduğu hakkında bkz. Değirmenci (n 8) 149.

127 Centel ve Zafer (n 8) 449.

128 Yenisey ve Nuhoğlu (n 72) 406; Ayrıca bkz. Şen ve Eryıldız (n 66) 213.

129 Bu kavramlar hakkında bkz. yuk. I, B, 3

doktrinde ileri sürülen bir görüşe göre Yönetmelikte, CMK'nın 134. maddesinde yer almayan bir düzenlemeye yer verilerek tedbirin sınırları genişletilmiştir[130]. Doktrinde ileri sürülen ve bizim de katıldığımız diğer görüş ise CMK'nın 134. maddesinde yer almayan *"bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları"* ibaresinin, maddede yer alan kavramların daha iyi anlaşılabilmesi için yapılan bir ekleme niteliğinde olduğu yönündedir[131]. Dolayısıyla Yönetmelik aracılığıyla CMK m.134 hükmünün kapsamı genişletilmemiş, aksine amaca uygun bir düzenleme yapılmıştır. Ancak bu konuda yaşanan tereddütlerin önüne geçmek adına, kapsamlı bir yasal düzenleme yapılmasının isabetli olacağı kanaatindeyiz.

Sistemdeki verilerin yedeklenmesi CMK m.134/f.3 hükmü uyarınca elkoyma işlemi sırasında yapılmalıdır. Zira verilerin güvenliğini tehlikeye sokabilecek olması nedeniyle, elkoyma işleminden sonra yedekleme yapılmamasına dikkat edilmelidir. Öyle ki, personel ya da teknik ekipman yetersizliği gibi gerekçelerle olay yerinde değil de elkoyma işleminden sonra sistemdeki verilerin yedeklemesinin yapılması halinde, elde edilen delillerin CMK m.217/f.2 hükmü bağlamında hukuka aykırı yöntemle elde edildiği ve delil olarak değerlendirilemeyeceği sorunu gündeme gelebilir[132].

6526 sayılı Kanun'la CMK'nın 134. maddesinde yapılan ikinci değişiklik maddenin 4. fıkrasında yapılmıştır. Kanun değişikliğinden önce 4. fıkra *"İstemesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır."* şeklinde düzenlenmişti. Ancak 6526 sayılı Kanun'un 11. maddesiyle, 134. maddenin 4. fıkrasında yer alan *"İstemesi halinde, bu"* ibaresi *"Üçüncü fıkraya göre alınan"* şeklinde değiştirilmiştir. Buna göre, üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline[133] verilecek ve bu husus tutanağa geçirilerek imza altına alınacaktır. İfade edildiği üzere, bu değişiklikten önce, CMK m.134/f.3 kapsamında sistemdeki bütün verilerin yedeklemesi yapıldıktan sonra, istemesi halinde bu yedekten bir kopya çıkarılarak şüpheliye veya müdafiine

130 Çelik (n 44) 38; Benzer yönde bkz. Şen ve Eryıldız (n 66) 199.

131 Tanrıkulu (n 40) 337; Benzer yöndeki görüşler için bkz. Değirmenci (n 8) 331; Yaşar ve Dursun (n 1) 16; Başlar (n 23) 100.

132 Yaşar ve Dursun (n 1) 26; Ayrıca bkz. Dülger (n 3) 604; Özen ve Özocak (n 2) 68.

133 Doktrinde bir görüş, CMK m.134/f.4 hükmünde "müdafii" yerine, hatalı olarak "vekil" ibaresi kullanıldığını ileri sürmektedir. Bkz. Centel ve Zafer (n 8) 449 dn. 245; Benzer yönde bkz. Değirmenci (n 8) 377; Ancak başka bir görüş ise buradaki "vekil" ibaresi ile bir hukukçunun değil, şüpheliyi temsil eden kişinin, esasen aileden birisinin kastedildiğini ileri sürmektedir. Bkz. Şahin (n 12) 278.

veriliyordu. Ancak 6526 sayılı Kanun'la yapılan değişiklikle, istem olmasa dahi bu yedeklerin verilmesi yönünde bir düzenleme yapılmıştır. İstem aranmaksızın, elkoyma tedbiri sonucu çıkarılan yedeğin bir kopyasının şüpheliye ya da savunma makamına verilmesindeki amaç, alınan yedek üzerinde sonradan yapılabilecek müdahalelere engel olmaktır[134]. 6526 sayılı Kanun'un gerekçesinde de haklı olarak ifade edildiği üzere söz konusu düzenlemeyle, yedeklemesi yapılan sistemdeki verilerde değişiklik yapıldığı iddiasının gündeme gelmesi durumunda, şüpheli veya vekiline verilen yedek ile ekleme yapıldığı iddia edilen kopya arasında karşılaştırma yapılabilmesi imkanı sağlanmaktadır[135].

Öte yandan, bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verildiğine dair bir tutanağın bulunmaması, CMK m.134 hükmüne riayet edilmediği anlamına gelecektir. Dolayısıyla hukuka aykırı yapılan bu arama ve elkoyma sonucu elde edilen deliller de hukuka aykırı yöntemlerle elde edilmiş delil niteliğinde olacak ve hükme esas alınamayacaktır[136].

Arama ve elkoyma kararı doğrudan CMK'nın 134. maddesi kapsamında olabileceği gibi, CMK m.119 ve m.127 kapsamında verilen genel arama ve elkoyma kararı üzerine yapılan aramalarda da bilgisayarlara elkonulabilir. Ancak elkonulan bilgisayarlarda aramaya ihtiyaç duyulması halinde, CMK'nın 134. maddesine göre verilmiş bir arama kararı bulunmalıdır. Örneğin genel arama ve elkoyma hükümlerine göre verilmiş bir kararla konut ya da işyerinde arama yapılması halinde, arama yapılan yerde bulunan bilgisayar gibi CMK m.134 hükmüne tabi dijital materyallerde arama yapılamaz. Söz

134 Şahin (n 12) 277; Öztürk ve diğerleri (n 63) 523; Karakehya (n 80) 351; Yedekten çıkarılan kopyanın isteğe bağlı olarak şüpheli veya vekiline verildiği dönemde yaşanan tartışmalar için bkz. Ünal (n 4) 121 vd.

135 <https://www2.tbmm.gov.tr/d24/2/2-1981.pdf> Erişim Tarihi 20 Mayıs 2022.

136 Yargıtay'ın bu yöndeki kararları için bkz. Yargıtay 4. CD., E. 2020/15324, K. 2021/ 7827, 04.03.2021 2022; Yargıtay 4. CD., E. 2021/16706, K. 2021/23109, 30.09.2021; Yargıtay 18. CD., E. 2016/ 8680, K. 2018/5914, 24.04.2018 <www.lexpera.com> Erişim Tarihi 19 Ağustos 2022.

konusu sistemlerde arama yapılmasına ihtiyaç duyuluyorsa CMK m. 134 hükmüne göre karar alınmalıdır[137].

Yukarıda yapılan değerlendirmeler gerek telefon gerekse gelişen teknolojiyle birlikte bilgisayar işlevi gören akıllı telefonlar yönünden de geçerlidir. Bu nedenle, arama ve elkoyma işlemi, konuşma veya mesaj kayıtlarının incelenmesi gibi cihazın telefon işlevine yönelik ise CMK m. 119 ve m. 127 hükümlerine göre verilmiş kararlar yeterli olurken; arama ve elkoyma işleminin, cihazın bilgisayar işlevine yönelik olduğu hallerde CMK m. 134 uyarınca verilen bir kararın varlığı aranacaktır[138].

CMK m.134 hükmünün avukat bürolarında nasıl uygulanacağına da değinmemiz yerinde olacaktır. Öncelikle CMK'nın 134. maddesinde bu konuyla ilgili bir düzenleme bulunmamaktadır. Bu durumda, avukat bürolarında bulunan bilişim sistemlerinde

137 Şahin (n 12) 275; Aynı yönde bkz. Aktaş (n 57) 227; Dülger (n 3) 605; Artuç (n 80) 466; Ünver ve Hakeri (n 15) 430; Aldemir (n 50) 219; Yaşar ve Otacı (n 2) 1114; *"Soruşturma dosyası kapsamında emanete alınan bilgisayar ve CD'ler üzerinde CMK'nın 134. maddesi uyarınca inceleme yapılması ve imaj alınmasına ilişkin bir kararın bulunmadığı, bilgisayarın yedeklemesinin yapılıp sanığa ve/veya müdafisine verildiğine dair bir tutanağa da yer verilmediği, bu suretle CMK'nın 134. maddesi hükümlerine riayet edilmeyerek bilgisayar kütüklerinde bilirkişi incelemesi yaptırıldığı, bunun sonucu elde edilen delillerin de hukuka uygun elde edilmiş delil niteliğinde olmadığı, delil değerlendirme yasağı kapsamında kaldığı gözetilmeyerek yazılı şekilde hüküm kurulması…"* Yargıtay 4. CD., E. 2021/16706, K. 2021/23109, 30.09.2021 <www.kazancı.com.tr> Erişim Tarihi 22 Mayıs 2022; *"…yapılan denetim sırasında sanık tarafından rıza ile teslim edilen ve iş yerinde görünür vaziyette bulunan 85 adet film ve oyun CD/DVD'sinin muhafaza altına alınması sebebiyle bu materyallerin hukuka uygun yöntemlerle elde edilen delillerden olduğu ancak sanığın iş yerinde bulunan bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılması, bilgisayar kayıtlarından kopya çıkarılması, bu kayıtların çözülerek metin hâline getirilmesi için sanık tarafından gösterilen rızanın yeterli olmayacağı ve mutlaka "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" başlıklı CMK'nın 134. maddesine göre hâkim kararı alınması gerektiği, hâkim kararı olmaksızın bilgisayar ve hard disklerde yapılan arama sonucunda elde edilen delillerin hukuka aykırı yöntemlerle elde edilen delil niteliğinde olduğunun anlaşılması karşısında…"* Yargıtay Ceza Genel Kurulu, 7-961/622, 22.10.2019 <www.kazancı.com.tr> Erişim Tarihi 21 Mayıs 2022; *"CMK'nın 134. maddesine göre verilmiş bir arama kararı bulunmadığı anlaşılmakla, işyerinde bulunan bilgisayarlar üzerinde yapılan arama sonucunda elkonulan ve içerisinde müşteki firmaya ait lisanssız yazılımların olduğu belirtilen harddiskler ve CD'ler hukuka aykırı delil niteliğinde olup hükme esas alınamayacağından, sanık hakkında verilen beraat kararı usul ve yasaya uygun görülmekle…"* Yargıtay 19 CD., E. 2015/2092, K. 2015/1175, 06.05.2015 <www.lexpera.com> Erişim Tarihi 19 Mayıs 2022; Bu yöndeki kararlar için bkz. Yargıtay 18. CD., E. 2019/11460, K. 2020/ 829, 15.01.2022; Yargıtay 19. CD., E. 2019/ 30045, K. 2020/ 2782, 11.03.2020; Yargıtay 19. CD., E. 2015/ 11396, K. 2016/ 1087, 02.02.2016 <www.lexpera.com> Erişim Tarihi 19 Ağustos 2022.

138 Şahin (n 12) 275; Özen ve Özocak (n 2) 69; Uygulamada bilgisayarlardan farklı olarak cep telefonlarına kolluk amirinin yazılı emriyle elkonulabilmekte ve bu elkoyma işlemi sırasında yedekleme vb. önlemlere başvurulmamaktadır. Uygulamadaki bu durum, kişilerin temel hak ve özgürlüklerine zarar vermekte olup, kişisel verilere ve özel hayatın gizliliğine hukuka aykırı şekilde müdahale edilmesi anlamına gelmektedir. Bu nedenle, yukarıda da bahsedildiği üzere, yapılan arama ve elkoyma işlemi cihazın telefon özelliğiyle ilgiliyse, örneğin konuşma veya mesaj kayıtlarının incelenmesi gerekiyorsa genel arama ve elkoyma hükümlerine başvurulmalıdır. Ancak cep telefonunda yapılan arama ve elkoyma işleminin trafik kaydı, e-posta kayıtlarının incelenmesi gibi cihazın bilgisayar özelliğine yönelik olduğu hallerde özel hüküm niteliğinde olan CMK m. 134 hükmü uygulanmalıdır. Bkz. Özen ve Özocak (n 2) 69-70; Cep telefonlarında arama için ayrıca bkz. Yenisey ve Nuhoğlu (n 72) 415.

yapılacak arama, kopyalama ve elkoyma işlemleri hakkında CMK'nın 130. maddesi kıyasen uygulanabilecektir. Buna göre, CMK m.130/f.1 hükmü uyarınca, avukat bürolarında bulunan bilişim sistemleri ancak mahkeme kararı ile ve kararda belirtilen olayla ilgili olarak Cumhuriyet savcısının denetiminde aranabilir. Ayrıca Baro başkanı veya onu temsil eden bir avukat aramada hazır bulundurulur. Arama sonucunda CMK'nın 134. maddesinde yer alan gerekçelerle elkonulmasına karar verilen şeyler bakımından bilgisayar ve diğer araçlarında arama yapılan avukat, baro başkanı veya onu temsil eden avukat, elkonulmak istenen verilerin avukat ile müvekkili arasındaki mesleki ilişkiye ait olduğunu öne sürerek karşı koyduğunda, söz konusu veriler kopyalanabilir. Kopyalanan bu veriler, ayrı bir zarf veya paket içerisine konularak hazır bulunanlarca mühürlenir ve bu konuda gerekli kararı vermesi, soruşturma evresinde sulh ceza hâkiminden, kovuşturma evresinde hâkim veya mahkemeden istenir. Yetkili hâkim elkonulan şeyin avukatla müvekkili arasındaki mesleki ilişkiye ait olduğunu saptadığında, elkonulan şey derhâl avukata iade edilir ve yapılan işlemi belirten tutanaklar ortadan kaldırılır. Son olarak, CMK m.130/f.2 hükmünde öngörülen kararların, yirmi dört saat içinde verilmesi gerekir.

Avrupa İnsan Hakları Mahkemesi (AİHM) *Wieser and Bicos Beteiligungen GmbH v. Avusturya* kararında, bir avukat bürosunda aramanın söz konusu olduğu hallerde, mesleki sır saklama yükümlülüğü kapsamında olan dijital verilerin güvenliğini temin amacıyla, yazılı belgelerin incelenmesi ve bu tür belgelere el konulmasına ilişkin kuralların kıyasen, dijital verilerin incelenmesi ve bu tür verilere elkonulması halinde de uygulanması gerektiğine işaret etmiştir[139]. Mahkeme, başvuruya konu olayda avukatların mesleki sır saklama yükümlülüğüne ilişkin hükümlerin dijital deliller yönünden dikkate alınmaması[140], bilişim sistemlerinin aranması sırasında hangi kriterlerin uygulandığı, hangi dosyaların kopyalandığı ve hangileri yönünden elkoyma tedbirine başvurulduğunu gösteren arama ve elkoyma tutanağının elkoyma işleminin sonunda değil de aynı günün ilerleyen saatlerinde düzenlenmesi, arama sonrasında Baro temsilcisinin bilgilendirilmemesi[141] ve avukatın mesleki sır saklama yükümlülüğünü korumayı amaçlayan usuli güvencelere uygun hareket edilmemesi[142] nedenleriyle Sözleşme'nin 8. maddesinin ihlal edildiğine karar vermiştir.

139 AİHM, *Wieser ve Bicos Beteiligungen GmbH v. Avusturya*, Başvuru No: 74336/01, 16.10.2007, para. 34.
140 *Wieser and Bicos Beteiligungen GmbH v. Avusturya*, para. 48.
141 *Wieser and Bicos Beteiligungen GmbH v. Avusturya*, para. 63.
142 *Wieser and Bicos Beteiligungen GmbH v. Avusturya*, para. 66.

Mahkeme, Kırdök ve Diğerleri v. Türkiye davasında da bir avukatlık bürosunda yapılan elkoyma işlemiyle ilgili olarak, avukat olan başvuruculların dijital verilerine elkonulmasının avukat ve müvekkili arasında bulunan güven ilişkisinin dayanağı olan meslek sırrını ihlal ettiği gerekçesiyle Sözleşme'nin 8. maddesinin ihlal edildiğine karar vermiştir[143].

Burada son olarak tesadüfen elde edilen delillere de kısaca değinmek istiyoruz. Bilişim sistemlerinde arama ve elkoyma tedbirinin uygulanması sırasında, yapılmakta olan soruşturmayla ilgisi olmayan ancak, diğer bir suçun işlendiği şüphesini uyandırabilecek bir delil elde edilirse, CMK'nın tesadüfen elde edilen delillere ilişkin 138. madde hükmü uygulanacaktır. Buna göre, tesadüfen elde edilen delil muhafaza altına alınacak ve bu durum Cumhuriyet Savcılığına derhal bildirilecektir[144].

4. Kopyalama

CMK m.134 hükmünde yer alan bir diğer tedbir ise kopyalamadır. Kanun koyucu, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde yapılacak incelemelerin, bu araçların bizzat kendi üzerinde değil, bunlardan elde edilecek kopyalar üzerinde yapılmasını öngörmüştür[145].

CMK m.134/f.5 hükmü uyarınca, bilgisayar veya bilgisayar kütüklerine elkoymaksızın da sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Bu itibarla, üzerinde arama ve kopyalama işlemi yapılacak cihazların bulundukları yerden başka bir yere götürülmelerine ihtiyaç yoktur. Cihazın fiziki olarak bulunduğu yerde arama ve kopyalama işlemi yapılabilecektir[146]. Bu durumda, CMK m.134/f.2 hükmünde öngörülen şartların gerçekleşmesi halinde, derhal elkoyma tedbirine başvurulmamalıdır. Öncelikle CMK m.134/f.5 hükmü gereğince, bilgisayarın bulunduğu yerde delil elde etme imkanının bulunup bulunmadığı değerlendirilmelidir. Buna göre, sistemdeki verilerin kopyasının alınabildiği hallerde, elkoyma tedbirine başvurulmasına yer olmayacaktır. Bir başka ifadeyle, CMK m.134/f.5 hükmünün uygulanamadığı hallerde elkoyma işlemine başvurulabilecektir[147].

143 AİHM, *Kırdök ve diğerleri v. Türkiye*, Başvuru No: 14704/12, 03.12.2019, para. 55-58; Benzer yöndeki AİHM içtihatları için bkz. *Petri Sallinen ve Diğerleri v. Finlandiya*, Başvuru No: 50882/99, 27.09.2005; *Smirnov v. Rusya,* Başvuru No: 71362/01, 07.06.2007; *Robathin v. Avusturya*, Başvuru No: 30457/06, 03.07.2012.

144 Tesadüfen elde edilen delillerin şikayete bağlı bir suça ilişkin olması halinde nasıl hareket edileceği hakkında bkz. Yaşar ve Dursun (n 1) 29.

145 Şen ve Eryıldız (n 66) 205.

146 Şahin (n 12) 279.

147 Ünal (n 4) 113.

Kopyalama işleminde dikkat edilmesi gereken husus, sistemdeki verilerin teknik gerekliliklere uygun olarak kopyalanması ve *hash değerlerinin* alınmasıdır[148]. Hash değeri ise dosyaların adeta parmak izi olarak kabul edilen ve dosya üzerinde herhangi bir değişiklik yapıldığında tamamen değişen, bu itibarla yedeklenen verinin bütünlüğünü güvence altına alan sayısal değerdir[149]. Birebir kopyalama işlemine imaj adı verilmekte olup, alınan imajların bütünlüğü hash değerleri hesaplanarak sağlanmaktadır[150]. Doktrinde isabetli olarak, *hash* değeri alınması gibi teknik zorunlulukların yasada da öngörülmesi gerektiği ileri sürülmüştür[151].

Son olarak, CMK m. 134/f.5 hükmünün ikinci cümlesi uyarınca, kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilmeli ve ilgililer tarafından imza altına alınmalıdır[152]. Ne var ki doktrinde kopyalanan verilerin kağıda dökülmesi şeklindeki hüküm hem gereksiz olması hem de kimi zaman tele baytlarca verinin kağıda dökülmesi gibi maddi olarak imkansız bir kural olması nedeniyle haklı olarak eleştirilmiştir[153].

Buraya kadar yapılan açıklamalar ışığında konuyu kısaca özetlersek, öncelikle yerinde aramanın mümkün olduğu hallerde elkoyma tedbiri işletilmemelidir. Bilişim sistemlerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması halinde elkoyma tedbirine başvurulmalıdır. Ancak elkoyma tedbirinin şartları oluşsa bile, bilişim sistemlerindeki verinin kopyasının alınabildiği hallerde öncelikle bu yola başvurulmalıdır[154]. Şu halde, maddi gerçeğe ulaşma ile temel hak ve özgürlükler arasındaki dengenin bozulmaması amacıyla, CMK m.134 hükmünün kademeli olarak uygulanmasına özen gösterilmelidir[155].

148 Özen ve Özocak (n 2) 53.

149 Tanrıkulu (n 40) 324; Özen ve Özocak (n 2) 53; Hash değeri, İnternetin Güvenli Kullanımına İlişkin Usul ve Esaslara Dair Kararın *"Tanım ve kısaltmalar"* kenar başlıklı 4. maddesinin 1. fıkrasının (ç) bendinde *"Bir bilgisayar dosyasının içindeki verilerin matematiksel bir işlemden geçirilmesi sonucu elde edilen ve dosyanın içerisindeki verilerde bir değişiklik yapılıp yapılmadığını kontrol için kullanılan dosyanın özünü belirten değer"* şeklinde tanımlanmıştır.

150 Özen ve Özocak (n 2) 66; Ayrıca bkz. Kaynakçıoğlu (n 20) 57.

151 Özen ve Özocak (n 2) 70.

152 Ayrıca bkz. Adli ve Önleme Aramaları Yönetmeliği m.17/f.5 *"Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan verilerin mahiyeti hakkında tutanak tanzim edilir ve ilgililer tarafından imza altına alınır. Bu tutanağın bir sureti de ilgiliye verilir."*.

153 Özen ve Özocak (n 2) 70; Tanrıkulu (n 40) 378; Ayrıca bkz. Özbek ve diğerleri (n 46) 434.

154 Ünal (n 4) 107; Doktrinde bir görüşe göre, CMK m.134 hükmü teknik olarak hatalıdır. Şöyle ki, bilişim sistemlerinde yerinde inceleme yapılması çoğu zaman mümkün olmadığından, delillerin korunması ve şüphelinin mağduriyetini önleyen tüm önlemlerin alınması için bilişim sistemlerine elkonulmalı ve laboratuvar ortamında teknik uzmanlar tarafından inceleme yapılmalıdır. Bkz. Özen ve Özocak (n 2) 63.

155 Ünal (n 4) 108.

Çalışmamızda öncelikle CMK'nın 134. maddesinde öngörülen arama, kopyalama ve elkoyma tedbiri üzerinde yoğunlaşılmış olmakla birlikte, bilişim sistemlerindeki verinin tanımlanması, elde edilmesi, korunması ve raporlanması gibi hususları kapsayan adli bilişim kavramına[156] son derece sınırlı olacak şekilde değinmemiz faydalı olacaktır. Adli bilişimi, toplumsal hayata hızlı bir şekilde entegre olan bilişim sistemleri üzerinde yer alan suç delillerinin ortaya çıkarılması faaliyeti şeklinde tanımlayabiliriz[157]. Dijital delillerin delil değerine sahip olabilmesi için hukuka ve teknik gerekliliklere uygun olarak elde edilmeleri son derece önem arz etmektedir. İşte bu nedenle, söz konusu delillerin bütünlük ve doğruluğunun sağlanmasında görevli memurlar, kolluk güçleri ve adli bilişim uzmanları önemli bir role sahiptir[158]. Bu bağlamda, elde edilen dijital delillerin yargılama makamlarına eksiksiz ve bozulmamış olarak sunulması da önem taşıyan konulardan biridir[159]. Ayrıca CMK m.134 kapsamında delil toplandığı hallerde, soruşturmanın sağlıklı bir şekilde yürüdüğünü gösteren en önemli hususlardan biri de mevzuata eksiksiz uyulmasıdır. Aksi takdirde, elde edilen deliller alanında uzman kişiler tarafından toplanmış olsa bile, hukuka aykırı delil olarak kabul edilecek ve hükme esas alınamayacaktır[160].

E. Tedbir Kararına İtiraz

CMK m.267 kapsamında, soruşturma evresinde sulh ceza hakimi tarafından verilen tedbir kararına karşı itiraz yoluna gidilebilir. Hemen burada ifade etmemiz gerekir ki, CMK m.35/f.2 hükmü uyarınca, koruma tedbirlerine ilişkin olan kararlar, hazır bulunamayan ilgiliye tebliğ olunmaz. Ancak ilgili, söz konusu tedbirin kendisine uygulanmasıyla bu tedbirden haberdar olacağından, itiraz süresi de bu tarihten itibaren işlemeye başlayacaktır[161].

Sonuç

Günümüzde bilişim teknolojileri alanında yaşanan hızlı ilerleme siyasal, toplumsal ve ekonomik alanda göze çarpan sonuçlar doğurmuştur. Hayatın her alanına nüfuz eden

156 Değirmenci (n 8) 68.

157 Değirmenci (n 8) 66; Özen ve Özocak (n 2) 44; Adli bilişimin amacı, dijital delillerin eksiksiz ve tarafsız bir şekilde adli birimlere aktarılmasıdır. Bu nedenle, adli bilişim, bir yorum faaliyeti olmayıp teknik bir delil inceleme faaliyetidir. Bkz. Özen ve Özocak (n 2) 45; Adli bilişim kavramı ve evreleri hakkında bkz. Dülger (n 3) 620 vd.; Kaynakçıoğlu (n 20) 52 vd.; Özen ve Özocak (n 2) s. 45 vd.

158 Dülger (n 3) 640.

159 Aldemir (n 50) 225; Dülger (n 3) 626.

160 Dülger (n 3) 649.

161 Centel ve Zafer (n 8) 450.

teknolojinin ceza muhakemesi alanındaki dikkat çeken sonuçlarından biri de suçun ispatında dijital delillerden istifade edilmesi olmuştur. Dijital delillerin ceza muhakemesi alanında klasik deliller gibi kullanılmaya başlamasının temel nedeni, teknoloji alanındaki hızlı ilerleme neticesinde suçun işlenme şekillerinin değişikliğe uğraması ve suçun dijital ortama taşınmasıdır. Özellikle bilişim teknolojisi alanında yaşanan gelişme, bilişim alanındaki suçların her geçen gün artmasına neden olduğu gibi, klasik suçları da bilişim sistemleri kullanılmak suretiyle işlenebilir hale getirmiştir.

İşte bu nedenle, bilişim sistemleri kullanılarak bir suç işlendiği takdirde, bu suçlara ilişkin delillerin toplanması amacıyla söz konusu sistem üzerinde inceleme yapılması ve elde edilen dijital delillerden yararlanılması kaçınılmaz hale gelmiştir. Ancak kişilere ait bilişim sistemleri üzerinde inceleme yapılması özel hayat, kişisel veri ve mülkiyet hakkı da dahil olmak üzere pek çok hukuki değere müdahale teşkil ettiğinden, kanun koyucu bu işlemi bir kanun normuna dayandırmış ve CMK'nın 134. maddesinde bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirini düzenlemiştir.

Her ne kadar CMK'nın 134. maddesinin kenar başlığı *"Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma"* olarak düzenlenmişse de yukarıda temas edilen açıklamalar çerçevesinde, konunun bilgisayarla sınırlandırılması yerine, daha kapsayıcı olacak şekilde bilişim sistemi kavramının kullanılmasının daha isabetli olacağı kanaatindeyiz. Öyle ki, TCK'nın *"Bilişim Sistemine Girme Suçu"* başlıklı 243. maddesinde de *"bilişim sistemi"* kavramına yer verilmiştir.

Bilişim sistemleri üzerinde depolanan verilere ilişkin arama, kopyalama ve elkoyma işlemlerini düzenleyen bu tedbir, CMK'nın 116 ve 123. maddeleri arasında yer alan arama ve elkoyma koruma tedbirinin özel bir görünümünü oluşturmaktadır. CMK'nın 134. maddesi özel bir norm olarak karşımıza çıkmakla birlikte, genel arama ve elkoymaya ilişkin hükümler, uygulanabilir olduğu ve aksine bir hüküm bulunmadığı müddetçe, bilişim sistemlerinde arama, kopyalama ve elkoyma tedbiri yönünden de uygulanabilecektir.

Kanun koyucu, CMK m.134 hükmünde düzenlenen koruma tedbirine başvurulabilmesi için birtakım şartların varlığını aramıştır. Bunlar somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkanının bulunmamasıdır. Kanun koyucu, kişilerin temel hak ve özgürlüklerine ilişkin pek çok değere ağır bir müdahale teşkil eden bu tedbir yönünden kuvvetli şüphe sebeplerinin varlığını arayarak, söz konusu tedbirin şartlarını ağırlaştırmak istemiştir. Ancak kuvvetli şüphe yalnızca

soruşturma konusu suçun işlendiğine yönelik olmamalı, aynı zamanda şüphelinin kullandığı bilişim sisteminden suç soruşturmasıyla ilgili delil elde edilebileceğine de yönelik olmalıdır.

Başka surette delil elde etme imkanının bulunmaması şartı ise bu tedbire son çare olarak başvurulmasını gerektirir. Ne var ki, temel hak ve özgürlüklere daha az müdahale teşkil eden koruma tedbirlerine öncelikli olarak başvurulduğu hallerde artık delil elde edememe ihtimali söz konusu olabilecektir. İşte bu gibi hallerde, başka surette delil elde etme imkanının bulunmadığı rahatlıkla söylenebilir.

Öte yandan doktrinde, bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirine kovuşturma evresinde de başvurulabileceği yönünde bir uzlaşı mevcut değildir. Söz konusu tedbire yalnızca soruşturma evresinde karar verilebileceğine ilişkin görüşü benimsiyor olmakla birlikte, bu hususta açık düzenleme yapılmasının yerinde olacağı kanaatindeyiz.

Kanun koyucu, bilişim sistemlerinde veri arama bakımından öncelikle yerinde aramayı öngörmüştür. Ancak CMK m.134/f.2 hükmü gereğince, bilişim sistemlerine 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 elkonulabilecektir. Bununla birlikte, CMK m.134/f.2 hükmünde yer alan koşullar oluşsa bile, derhal elkoyma tedbirine başvurulmamalıdır. Öncelikle CMK m.134/f.5 hükmü kapsamında, sistemdeki verilerin kopyasının alınıp alınamayacağı hususu değerlendirilmelidir.

Bundan başka, bilişim sistemleri üzerinde arama yapılabilmesi için CMK m.134 uyarınca verilen bir kararın varlığı zorunludur. Genel arama ve elkoyma hükümlerine göre verilmiş bir kararla, CMK m. 134 hükmüne tabi dijital materyaller üzerinde arama yapılamayacaktır. CMK m.134 hükmüne göre verilmiş bir karar olmadan bilişim sistemlerinde arama yapılması halinde, elde edilen deliller hukuka aykırı delil niteliğinde olup hükme esas alınamayacaktır.

Son olarak, bilişim sistemleri üzerinde yer alan durağan, yani depolanmış veriler için CMK'nın 134. maddesi uygulanırken; akış halindeki, bir diğer ifadeyle iletişim esnasındaki veriler için CMK'nın 135. maddesi uygulanmaktadır. Bu bağlamda, şifreli haberleşme uygulaması olan Bylock iletişim sisteminin kullanımı sonucunda oluşan verilerin tespiti CMK'nın 135. maddesi kapsamında olmayıp, *"Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma"* başlıklı 134. madde kapsamındadır. Zira CMK'nın 135. maddesine göre, geçmişte gerçekleşen

iletişimin dinlenebilmesi ya da kayda alınabilmesi mümkün değildir. Başka bir ifadeyle, CMK'nın 135. maddesi kapsamında iletişimin dinlenmesi ve kayda alınması geçmişe değil, yalnızca geleceğe dönük olarak yapılabilir. Ancak internet ortamında gerçekleştirilen iletişime ilişkin kayıtlar, bilgisayar kütüğünde kaydedildiğinden, bu iletişim kayıtları hakkında CMK'nın 134. maddesindeki koruma tedbiri uygulanabilecektir.

Hakem Değerlendirmesi: Dış bağımsız.
Çıkar Çatışması: Yazar çıkar çatışması bildirmemiştir.
Finansal Destek: Yazar bu çalışma için finansal destek almadığını beyan etmiştir.

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

Kaynakça/References

Akbulut B, *Türk Ceza Hukukunda Bilişim Suçları* (Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Doktora Tezi, 1999).

Akkaş A H, "Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi Koruma Tedbirinin Şartlarında 6526 Sayılı Kanun ile Yapılan Değişikliklerin Değerlendirilmesi" (2015) (21) Türkiye Adalet Akademisi Dergisi 467-488.

Aktaş B, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Tedbiri Üzerine Bir İnceleme" (2017) 14 (2) Yeditepe Üniversitesi Hukuk Fakültesi Dergisi 211-239.

Aldemir H, *Adli-Önleme Arama ve Elkoyma*, (4. Baskı, Adalet Yayınevi, 2021).

Apiş Ö, "Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Koruma Tedbiri" (2018) (37) Yasama Dergisi 49-86.

Artuç M, *Pratik Ceza Muhakemesi Kanunu* (2. Baskı, Adalet Yayınevi, 2018).

Başlar Y, "Elektronik Delilin Toplanması ve Muhafazası" (2020) 10 (1) Hacettepe Hukuk Fakültesi Dergisi 77-107.

Baytemir Kontacı B ve diğerleri (Editör: Cumhur Şahin ve Neslihan Göktürk), *Ceza Muhakemesi Hukuku*, (Seçkin Yayıncılık, 2018).

Baytemir Kontacı B, "Avrupa İnsan Hakları Mahkemesi ve Anayasa Mahkemesi Kararlarında Özel İletişim Araçlarının Kullanılmasının Ceza Sorumluluğu Üzerindeki Etkisi", *Anayasa Mahkemesi Kararları Işığında Hak ve Özgürlüklerin Sınırlandırılması Rejimleri Sempozyumu* (Seçkin Yayıncılık, 2022) 553-573.

Bozdoğan Akbulut B, "Bilişim Suçları" (2000) 8 (1-2) Selçuk Üniversitesi Hukuk Fakültesi Dergisi Milenyum Armağanı 545-555.

Casey E, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (3rd Edition, Academic Press, 2011).

Centel N ve Zafer H, *Ceza Muhakemesi Hukuku* (14. Baskı, Beta, 2017).

Çekiç B, "Bilgisayar Verilerinde Arama, Kopyalama, Elkoyma Tedbirinin Hukuki Niteliği ve Benzer Kavramlar" (2021) 2 (1) Namık Kemal Üniversitesi Hukuk Fakültesi Dergisi 153-185.

Çelik K, "Bulut Bilişim Teknolojileri" (2021) 12 (24) Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi 436-450.

Çelik M, *Bilgisayarda Arama, Kopyalama ve Elkoyma (CMK m.134)* (İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, 2018).

Çulha R ve diğerleri (Editör: Feridun Yenisey), *Ceza Muhakemesi Hukuku Başvuru Kitabı* (Bilge Yayınevi, 2017).

Değirmenci O, *Ceza Muhakemesinde Sayısal (Dijital) Delil* (Seçkin Yayıncılık, 2014).

Değirmenci O, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbirinde (CMK m.134), 7145 Sayılı Kanunla Yapılan Değişikliklerin Değerlendirilmesi" (2018) 13 (146) Terazi Hukuk Dergisi 146-155.

Değirmenci O, "Adli Bilişimde Önceliklendirme (Triyaj) Yönteminin Ceza Muhakemesi Açısından Değerlendirilmesi" (2020) 2 (1) Bilişim Hukuku Dergisi 47-79.

Dereboylular Ö, "Bulut Bilişim Bakımından Arama ve Elkoymaya İlişkin Hükümlerin Uygulanabilirliği" (2019) 14 (19) Ceza Hukuku Dergisi 161-202.

Dülger M V, *Ceza Muhakemesi Hukukunda Dışlama Kuralı ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağacın Meyvesi Öğretisi)* (Seçkin Yayıncılık, 2014).

Dülger M V, *Bilişim Suçları ve İnternet İletişim Hukuku* (9. Baskı, Seçkin Yayıncılık, 2022).

Ergün İ, *Siber Suçların Cezalandırılması ve Türkiye'de Durum* (Adalet Yayınevi, 2008).

Ersoy Y, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları" (1994) 49 (3) Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi 149-184.

Henkoğlu T, *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi* (2. Baskı, Pusula Yayıncılık, 2014).

Jekot W, "Computer Forensics, Search Strategies, and the Particularity Requirement" (2020) 7 Pittsburgh Journal of Technology Law & Policy.

Karagülmez A, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri* (5. Baskı, Seçkin Yayıncılık, 2014).

Karakehya H, *Ceza Muhakemesi Hukuku* (2. Baskı, Savaş Yayınevi, 2016).

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

Kaynakçıoğlu U, *Ceza Muhakemesinde Dijital Deliller* (Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, 2015).

Kerr Orin S., "Digital Evidence and The New Criminal Procedure" (2005) 105 (1) Columbia Law Review 278-318.

Keser Berber L, *Adli Bilişim* (Yetkin Yayınları, 2004).

Kim W, "Cloud Computing: Today and Tomorrow" (2009) 8 (1) Journal of Object Technology 65-72.

Larkin J E D, "Compelled Production of Encrypted Data" (2012) 14 (2) Vanderbilt Journal of Entertainment & Technology Law 253-278.

Novak M, "Digital Evidence in Criminal Cases Before the U.S. Courts of Appeal: Trends and Issues for Consideration" (2020) 14 (4) The Journal of Digital Forensics, Security and Law 1-42.

Özbek V Ö ve diğerleri, *Ceza Muhakemesi Hukuku* (8. Baskı, Seçkin Yayıncılık, 2016).

Özen M ve Baştürk İ, *Temel Hak ve Özgürlükler Bağlamında Bilişim-İnternet ve Ceza Hukuku* (Adalet Yayınevi, 2011).

Özen M ve Özocak G, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)" (2015) (1) Ankara Barosu Dergisi 41-77.

Özen M, *Ceza Muhakemesi Hukuku Dersleri* (2. Baskı, Adalet Yayınevi, 2017).

Özgenç İ, *Suç Örgütleri* (Seçkin Yayıncılık, 2022).

Öztürk B ve diğerleri, *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku*, (14. Baskı, Seçkin Yayıncılık, 2020).

Parlar A ve Çetin A, *Ceza Muhakemesinde Soruşturma Evresi ve Uygulaması* (Aristo Yayınevi, 2017).

Radina Stoykova, "Digital evidence: Unadressed threats to fairness and the presumption of innocence" (2021) 42 Computer Law & Security Review 1-20.

Riekkinen J, "Electronic Evidence in Criminal Procedure: On the Effects of ICT and The Development towards the Network Society on the Life-cycle of Evidence" (2019) 16 Digital Evidence and Electronic Signature Law Review 6-10.

Sözüer A, "Türkiye'de ve Karşılaştırmalı Hukukta Telefon, Teleks, Faks ve Benzeri Araçlarla Yapılan Özel Haberleşmenin Bir Ceza Yargılaması Önlemi Olarak Denetlenmesi" (1997) LV (3) İstanbul Üniversitesi Hukuk Fakültesi Mecmuası 65- 110.

Şahin C, "Telekomünikasyon Yoluyla İletişimin Denetlenmesi" (2017) XI (1-2) Gazi Üniversitesi Hukuk Fakültesi Dergisi 1095-1112.

Şahin C, "Ceza Muhakemesinde Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" (2019) 1 (2) Yaşar Hukuk Dergisi 271-286.

Şen E ve Eryıldız S, *Elkoyma* (Seçkin Yayıncılık, 2017).

Tanrıkulu C, *Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma* (Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Doktora Tezi, 2014).

Uğraş D Ö, "Bilgisayarlarda, Bilgisayar Programlarında ve Bilgisayar Kütüklerinde Arama, Kopyalama ve Elkoyma" (2021) 34 (154) Türkiye Barolar Birliği Dergisi 97-134.

Ünal O G, *Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma* (Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, 2011).

Ünver Y ve Hakeri H, *Ceza Muhakemesi Hukuku*, (17. Baskı, Adalet Yayınevi, 2020).

Yaşar O ve Otacı C, *Yeni İçtihatlarla Uygulamalı ve Yorumlu Ceza Muhakemesi Kanunu I. Cilt* (10. Baskı, Seçkin Yayıncılık, 2022).

Yaşar Y ve Dursun İ, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri" (2013) 19 (2) Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 3-34.

Yazıcıoğlu Y, *Bilgisayar Suçları; Kriminolojik, Sosyolojik ve Hukuki Boyutları ile* (Alfa Yayınları, 1997).

Yenisey F ve Nuhoğlu A, *Ceza Muhakemesi Hukuku* (6. Baskı, Seçkin Yayıncılık, 2018).

Yeşil U*, Hukuk ve İnsan Hakları Bağlamında Bylock Bilgilerinin Delil Değeri* (Alternatif Düşünce ve Medya Yayıncılık, 2018).