NKÜ Hukuk Fakültesi Dergisi, 2021(1), 153-185
DOI 10.51562/nkuhukuk.2021217
https://dergipark.org.tr/tr/pub/nkuhukuk
Başvuru15.05.2021
Kabul:19.06.2021

NKÜ HUKUK FAKÜLTESİ DERGİSİ

ARAŞTIRMA MAKALESİ / RESEARCH ARTICLE

BİLGİSAYAR VERİLERİNDE ARAMA, KOPYALAMA, EL KOYMA TEDBİRİNİN HUKUKİ NİTELİĞİ VE BENZER KAVRAMLAR*

Burak ÇEKİÇ**

ÖZET

Bilişim sistemlerinde ve bilgisayar verilerinde, ceza yargılamasının konusunu oluşturan suçlara ilişkin deliller bulunabilmektedir. Bilgisayar verilerinde, sadece TCK'nın bilişim alanında suçlar bölümünde yer alan ve bilişim sistemlerine özgü suçlar değil, gerçek hayatta işlenebilen tüm suçlarla ilgili deliller bulunabilmektedir. Bir yargılamada bilgisayar verilerinde yer alan deliller araştırılmadığında, değerli şeyler kaçırılıyor demektir. Bilgisayar verilerinden delil elde etme süreci adli bilişim olarak adlandırılmaktadır. Elde edilen delile, sayısal delil veya elektronik delil adı verilmektedir. Sayısal delillerin kendilerine has özellikleri bulunmaktadır. Bu özellikler nedeniyle bilgisayar verilerinde arama ve el koyma tedbiri icra edilirken geleneksel arama ve el koyma yöntemlerinin yanı sıra başka adli bilişim uygulamalarının hukuka uygun olarak yerine getirilmesi gerekmektedir. Hukuka uygunluk için yasal dayanak, CMK'nın 134. maddesinde yer alan bilgisayar verilerinde arama ve el koyma düzenlemesi ile sağlanmaktadır. Bu makalenin hedefi, bilgisayar verilerinde arama ve el koymanın tanımını, işlevini ve hukuki niteliğini ve benzer kavramları araştırmaktır.

Anahtar Kelimeler Bilgisayarlarda Arama, Bilgisayarlarda El Koyma, Adli Kopyalama, Adli Bilişim, Sayısal Delil

LEGAL NATURE OF SEARCHING, COPYING AND SEIZURING OF COMPUTER DATA AND SIMILAR TERMS

Burak ÇEKİÇ *****

ABSTRACT

Evidence of crimes that are the subject of criminal proceedings can be found in information systems and computer data. In computer data, evidence can be found not only for crimes specific to informatics systems, but also for all crimes that can be committed in real life. When the evidence contained in computer data is not investigated in a trial, valuable things are being missed. The process of obtaining evidence from computer data is called computer forensics. The evidence obtained is called digital evidence or electronic evidence. Digital evidence has its own characteristics. Due to these features, while doing a search and seizure on computer data, other computer forensics applications must be executed in accordance with the law besides traditional search and seizure methods. The legal basis for compliance with the law is provided by the regulation of search and seizure of computer data in article 134 of the Turkish Criminal Procedural Code - TCPC. The aim of this article is to explore the definition, function and legal nature of computer data search and seizure, and similar concepts.

Keywords Computer search, Computer seizure, Forensic image, Computer forensics, Digital evidence.

---

* Bu makale, "Koruma Tedbiri Olarak Bilgisayarlarda, Bilgisayar Programlarında Ve Bilgisayar Kütüklerinde Arama, Kopyalama, El Koyma" isimli doktora tezinden üretilmiştir.

** Doktora Öğrencisi, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, burakcekic@marun.edu.tr, ORCID 0000-0002-7004-3677

*** PhD Candidate, Marmara University, Institute of Social Sciences, Department of Public Law, burakcekic@marun.edu.tr, ORCID 0000-0002-7004-3677

p-ISSN:2717-9621 e-ISSN: 2757-6752

Extended Summary

Searching computer data is a form of common search (Turkish Criminal Procedural Code - TCPC 116), And seizure of computer data is a form of common seizure (TCPC 123), specially arranged by considering the characteristics of digital evidence in order to obtain electronic evidence. While the subject of traditional search and seizure is tangible signs, evidence within the home or on the person, what is in question here is the abstract electronic data on various devices such as computers.

Some countries implement traditional search and seizure for computer data and do not have special regulations. It is good practice to have a special regulation for computer search and seizure in Turkey. Due to the natural characteristics of digital evidence, there is a need for regulations that are different from the provisions of traditional search and seizure measures.

One aspect of electronic documents, which do not exist in paper documents is metadata. Metadata is electronic information about other electronic data and is created by computer systems and embedded in electronic documents. Meta-data can be used to find out the author and origin of a document, the existence of any attachments, and whether the document was sent or received by any individual. Metadata would include information such as the date of creation of the document, the date sent, received and so on.

There is substantially more electronically stored information than paper documents, and electronically stored information is created and replicated at much greater rates than paper documents. Examining electronic data will of course be different from examining printed documents. The content of a hard disk may contain data that is not related to the event or that is personal, trade secret, belonging to third parties. Extracting information about the case from all data reveals the need for specialized scientific methods.

More generally, electronically stored information is more easily and more thoroughly changeable than paper documents. Electronically stored information can be modified in numerous ways that are sometimes difficult to detect without computer forensic techniques.

Digital evidence is invisible in nature. They cannot be seen directly. Appropriate hardware and software are needed to view and interpret data. A computer, word processor program, screen and printer are needed to view and understand the data produced by the word processor program. The output printed on the paper will not fully reflect the data, and metadata will not be visible.

In accordance with the mentioned characteristics of digital evidence, the search and seizure of computer data has been specially regulated, meeting this need. There is a special regulation in article 134 of the TCPC regarding the search and seizure of computer data in Turkey. There are three measures in article 134. These are search, copy and seizure of computer data. Search and seizure computer data is similar to traditional search and seizure, with some differences. Copying is a protection measure specific to computer data.

Searching and seizing computer data is a protection measure that can be applied as ultima ratio, depending on special conditions, taking into account the severity of the interventions against the private life and personal data of individuals.

The procedures regarding the search, copy and seizure of computer data should be carried out by following the scientific methods of computer forensics. The most important aspect of a scientific method is that any experiment or observation must be independently verifiable and reproducible. The same results should be achieved when the path followed in computer forensics activities is repeated by impartial persons.

Using a common terminology between the comparative law and the regulations made in our country is the most important step in determining the missing applications in the execution of the measure.

We can define computer data search as on the decision of the competent authority, to obtain numerical evidence of a committed crime, to access the data stored by the suspect in the information systems used by the suspect, by computer forensic experts. Experts, makes invisible data visible and understandable, restores deleted and lost data, recovers data from corrupted or physically damaged devices, deciphers encrypted data, with the help of appropriate hardware, software, and functions, by protecting the data integrity. Computer search is a process including extracting, searching, analyzing, interpreting, reporting data.

As the traditional search gives the right to enter (access) inside the house, the computer search also allows access to personal data in accordance with the law. The concept of search and the concept of access are used in an equivalent sense. Examination is part of search process and means analyzing of digital evidence.

There are many ways to do a forensic search. Manual browsing, find function, keyword search, regular expression search – REGEX are most common ways. But these methods are effective on clear text. Data that are not available in clear text must first be made readable, visible, indexable and understandable. Sometimes it is not enough just to find data that can be evidence. In order for the data to be efficient evidence in the investigations, it should also be interpreted by the experts in order to be clearly understood by the judges and the parties of the case.

Forensic imaging is one element of computer forensics, which is the application of computer investigation and analysis techniques to gather evidence suitable for presentation in a court of law. A forensic image (forensic copy) is a bit-to-bit, sector-by-sector direct copy of a physical storage media, including all files, folders and unallocated, free and slack space. Forensic images include all the files visible to the operating system, deleted files and pieces of files left in the slack and free space.

TCPC article 134, allows computer seizure under certain conditions for the purpose of forensic imaging. The first is that the system cannot be copied because it is encrypted. The second is that there's hidden information in the system. Third, the process will take a long time. When the conditions are met, computers can be seized with the decision of the judge. Computers must be returned immediately upon receipt of the copy.

GİRİŞ

Bilgisayar verilerinde arama, genel aramanın (CMK 116 vd.), bilgisayar verilerine el koyma ise genel el koymanın (CMK 123 vd.), elektronik delil elde etmek üzere, sayısal delile özgü nitelikler göz önüne alınarak özel düzenlenmiş şeklidir[1]. Genel arama ve el koymanın konusu bina içindeki veya kişi üzerindeki somut iz, bulgu ve şeyler iken, burada söz konusu olan bilgisayar gibi çeşitli cihazlar üzerindeki soyut elektronik verileridir[2].

Karşılaştırmalı hukukta bilgisayar verilerinde arama ve el koyma işlemleri için genel arama ve el koyma tedbirlerini uygulayan ve özel düzenlemeleri bulunmayan ülkeler mevcuttur. Ülkemizde bu işlemler için özel düzenlemenin yapılmış olması yerinde bir uygulamadır[3]. Sayısal delillerin doğal özellikleri nedeniyle genel arama ve el koyma tedbirleri hükümlerinden daha farklı düzenlemelere ihtiyaç duyulmaktadır. Bilgisayar ve akıllı telefonların kapasitelerinin gelişmesi, internet uygulamalarının, e-ticaretin ve sosyal medyanın yaygınlaşması neticesinde elektronik cihazlarda daha fazla kişisel veri metin, fotoğraf, video, ses olarak kaydedilmektedir. En temel insan haklarından biri olan kişisel verilerin korunması hakkının ihlal edilmesinin ağır ve telafi edilmesi güç sonuçları oluşmaktadır. Madde gerekçesinde, özel düzenleme yapılmasının öncelikli sebebinin temel insan haklarının kısıtlanabilmesi için yasal düzenleme zorunluluğunun olduğu vurgulanmıştır[4].

Özel düzenleme yapılmasına duyulan ihtiyacı ortaya koyabilmek için sayısal delillerin özelliklerine kısaca değinilmelidir. Sayısal verilerde, kâğıda basılı belgelerde bulunmayan çok çeşitli *üst-veriler* mevcuttur. Belgenin yazarı, oluşturulma tarihi, fotoğrafın çekildiği yerin GPS koordinatları, videoyu çeken kameranın marka-modeli gibi çok çeşitli üst-veriler mevcuttur[5]. Bu tür üst-verilerde bulunan bilgiler, soruşturmada göz ardı edilemeyecek deliller içerebilmektedir. Genel arama ve el koyma hükümlerinin yanında bu tür deliller için, özel kopyalama, arama, muhafaza etme usullerine ihtiyaç vardır.

---

[1] Olgun Değirmenci, Ceza Muhakemesinde Sayısal (Dijital) Delil (1. Baskı, Seçkin Yayınları 2014) 312; İhsan Baştürk, 'Bilgisayar Sistemleri İle Verilerinde Arama Kopyalama ve Elkoyma' (2010) 2 Fasikül İstanbul Kültür Üniversitesi Cehamer Aylık Hukuk Dergisi 23, 25; Nur Centel ve Hamide Zafer, Ceza Muhakemesi Hukuku Yenilenmiş ve Gözden Geçirilmiş (10. Baskı, Beta Yayınları 2013) 398; Özge Sırma, 'Güncel Olaylar Çerçevesinde 5271 Sayılı Ceza Muhakemesi Kanununda Arama' (2009) 34 Terazi Hukuk Dergisi 37; Veli Özer Özbek, Koray Doğan ve Pınar Bacaksız, Ceza Muhakemesi Hukuku (12. Baskı, Seçkin Yayınları 2019) 384; Hüsnü Aldemir, Adli - Önleme Arama ve Elkoyma (1. Baskı, Adalet Yayınları 2018) 179; Yusuf Yaşar ve İsmail Dursun, 'Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri' (2013) 19 Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi 3, 7

[2] Özbek, Doğan ve Bacaksız (n 1) 384

[3] Değirmenci (n 1) 313; Özbek, Doğan ve Bacaksız (n 1) 384

[4] Ceza Muhakemesi Kanunu Madde Gerekçeleri m. 110

[5] Allison Rebecca Stanfield, 'The Authentication of Electronic Evidence' (PhD Dissertation Queensland University of Technology Faculty of Law 2016) 4-5

Elektronik veriler, kâğıda basılı bilgilere göre çok daha fazladır. Sayısal veriler, daha çok üretilmekte, çoğaltılmakta, paylaşılmakta ve dağıtılmaktadır. Bir işyerinde veya bir konutta yapılan aramada birkaç dolap dolusu belge bulunabilir[6]. Görevliler bu belgeleri inceleyerek delil elde edebilirler. Ancak bir sabit diskte kütüphaneler dolusu bilgiyi saklamak mümkündür. Elektronik verilerin incelenmesi basılı belgelerin incelenmesinden elbette farklı olacaktır. Bu derece fazla elektronik verinin incelenmesi, dava konusunda delil olabileceklerin bulunması, analiz maliyetlerini artırmaktadır[7]. Bir sabit diskin içeriğinde olayla ilgili olmayan veya üçüncü şahıslara ait kişisel, ticari sır niteliğinde veriler bulunabilir. Tüm verilerden davayla ilgili bilgilerin ayıklanması, özel bilimsel yöntemlere olan ihtiyacı ortaya koymaktadır[8].

Elektronik veriler oldukça dinamiktir. Kolay bir şekilde bozulabilir, değiştirilebilir, silinebilir. Basılı belgelerin aksine insan iradesi olmadan bile elektronik veriler değişebilir. Bilişim sistemlerinde tutulan kayıtlar, otomatik olarak güncellenen günlük dosyaları, otomatik yedekleme yapılan dosyalar, insandan bağımsız olarak değiştirilmektedir. Kapalı bir bilgisayarı çalıştırmak, açık bilgisayarı kapatmak, dosyalarda tarama yapmak, başka bir yere kopyalamak gibi eylemler, birçok veriyi değiştirmektedir. Sisteme müdahale eden görevli, bilgisi ve niyeti olmadan birçok veriyi silebilir, bozabilir[9]. Bu müdahalelerle verilerin delil niteliği bozulmaktadır. Elektronik verilerin delil niteliğinin bozulmadan yargılama süresince muhafaza edilmesini sağlayacak, uygun el koyma, arama ve raporlama yöntemlerine ihtiyaç vardır.

Sayısal deliller doğası gereği gizli niteliktedir. Doğrudan gözle görülememektedirler. Verileri görmek ve anlamlandırmak için uygun donanıma ve yazılımlara ihtiyaç vardır. Kelime işlemci programı tarafından üretilen bir verinin görülüp anlaşılabilmesi için bilgisayara, kelime işlemcisi programına, ekrana ve yazıcıya ihtiyaç vardır. Veri, ancak bilgisayarda kelime işlemcisi program ile açılıp ekranda görüldüğünde veya yazıcıdan çıktısı alındığında anlaşılabilir. Kâğıda basılan çıktı veriyi tam olarak yansıtmayacak, üst-veriler görülemeyecektir. Ekran ve yazıcı çıktıları ile yetinerek değerlendirme yapmak büyük bir eksikliktir[10].

Sayısal delilerin anılan niteliklerine uygun olarak, bilgisayar verilerinde arama ve el koyma tedbirinin özel bir biçimde düzenlenmiş olması, bu ihtiyacı gidermektedir. Bilgisayar

[6] The Sedona Conference Working Group on Electronic Document Retention & Production, 'The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production Second Edition' (2007) 2
[7] Stanfield (n 5) 64
[8] Eoghan Casey, Digital Evidence And Computer Crime (2. Baskı, Academic Press 2004) 15
[9] The Sedona Conference Working Group on Electronic Document Retention & Production (n 6) 3
[10] Değirmenci (n 1) 132

verilerinde arama ve el koyma işlemleri, bu özel düzenleme kapsamında yerine getirilecek, maddede düzenlenmeyen genel arama ve el koyma çerçevesinde yürütülecek işlemler bakımından ise özel düzenlemede belirlenen hükümlere aykırı olmamak üzere genel arama ve el koyma hükümleri uygulanacaktır[11].

Doktrinde, genel bina aramaları ile bilgisayar verilerinde aramalar arasında dört temel fark bulunduğu belirtilmektedir. Bu farklılıklar, fiziksel aramalar için belirlenen kuralların, dijital aramalar için uygun olmayabileceği ihtimalini göstermektedir. Öncelikle ev aramaları fiziksel olarak haneye girilip gözlemlenerek yapılmaktadır, bilgisayar verilerinde arama ise dönen manyetik noktaların üzerinden elektrik akımının geçirilmesi, verilerin işlenmesi ve ardından ekrana veya başka bir çıkış cihazına gönderilmesi şeklinde gerçekleşmektedir. İkincisi, ev aramaları şüphelinin konutunda veya işyerinde yapılır, bilgisayar verilerinde arama genellikle, şüphelinin sabit diskinin bir kopyasının alınarak, konut dışında devlet bilgisayarında yapılmaktadır. Üçüncüsü, konut aramaları belirli miktarda mülk için söz konusudur, oysa bilgisayar verilerinde arama milyonlarca bilgi üzerinde gerçekleştirilmektedir. Dördüncüsü, konut aramalarının aksine, bilgisayar aramaları genellikle delili elde etmek için tasarlanmış özel programların kullanımıyla hem fiziksel hem de sanal ortamda gerçekleştirilmektedir[12]. Bu gibi farklar genel arama hükümlerinin yeniden yorumlanmasını ya da bilgisayar verilerine özel arama el koyma hükümlerinin tesis edilmesini gündeme getirmektedir.

I. YASAL DÜZENLEME

Düzenleme, CMK'nın "Koruma Tedbirleri" başlıklı ikinci kısmının, "Arama ve El koyma" başlıklı dördüncü bölümünün "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma" başlıklı 134. maddesinde yer almaktadır.

Madde başlığının bu kadar uzun belirlenmesi doktrinde eleştirilmektedir. Bir bütünün parçalarını ifade eden terimlerin tek tek kullanıldığı[13], düzenlemenin amacına uygun olmadığı, tedbirin uygulama alanını kısıtladığı[14] belirtilmektedir. Doktrinde alternatif olarak, *Avrupa Konseyi Siber Suç Sözleşmesinde* ifade edilen *Bilgisayar Sistemi* kavramı kullanılmaktadır[15]. Bir başka görüş ise, *Bilişim Sistemleri* kavramını tercih etmektedir[16]. Bu terimlerin hepsi somut

[11] Cengiz Tanrıkulu, Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma (1. Baskı, Adalet Yayınları 2014) 351; Aldemir (n 1) 179
[12] Orin S Kerr, 'Searches and Seizures In A Digital World' [2005] Harward Law Review 532 534
[13] Muharrem Özen ve İhsan Baştürk, Temel Hak ve Özgürlükler Bağlamında Bilişim - İnternet ve Ceza Hukuku (1. Baskı, Adalet Yayınları 2011) 142; Muharrem Çelik, 'Bilgisayarda Arama, Kopyalama Ve Elkoyma CMK m. 134' (Yüksek Lisans Tezi İstanbul Üniversitesi Sosyal Bilimler Enstitüsü 2018) 29
[14] Değirmenci (n 1) 310
[15] Özen ve Baştürk (n 13) 142
[16] Değirmenci (n 1) 310; Tanrıkulu (n 11) 348

cihazları tanımlamaktadır ve arama-el koymanın konusunu oluşturan *veriyi*, üzerinde bulunduğu donanımdan hareketle tanımlamaktadır. Ancak son 50 yıldan bugüne kadar bilgisayar teknolojilerinin kat ettiği gelişme, veri tutabilen ortamların daha da çeşitleneceğini göstermektedir. Yasal düzenlemelerdeki değişimin ve uyumun, teknolojik gelişimin hızına yetişemeyeceği ortadadır. Bu durumda sürekli olarak kavramların geniş yorumlanması suretiyle problemlerin çözümü yoluna gidilmektedir. Halbuki donanımdan, cihazdan, ortamdan bağımsız bir terime ihtiyaç vardır. Kanımızca *bilgisayar verisi* terimi bu yaklaşıma uygun bir şekilde yeterli tanıma sahiptir. *Bilgisayar verilerinde arama, Bilgisayar verilerine el koyma* ifadelerinin, düzenlemenin amacına, kapsamına, konusuna daha uygun olduğunu değerlendirmekteyiz. Nitekim uluslararası metinlerde bu kavrama sıkça rastlanmaktadır. *Bilgisayar verisi (Computer Data), Bir bilgi sisteminin bir fonksiyonu yerine getirmesine sebep olmaya uygun bir programı da içeren, bir bilgi sisteminde işlenebilmek için uygun bir forma konulan veya oluşturulan, durum, bilgi veya kavramın herhangi bir şekilde sunumu* olarak tanımlanmıştır[17]. Bu ifade ISO standart veri tanımı üzerine bina edilmiştir. Bu tanıma göre bilgisayarda yazılan bir kitap veya basılı bir kitabın bilgisayarda taranmış dosyaları da bilgisayar verisi olarak kabul edilmektedir[18]. Hangi ortamda tutulursa tutulsun elektronik veriler, her zaman, *sayısal veri, bilgisayar verisi* olarak adlandırılacaktır. Çalışmamızda *bilgisayar verileri* terimi kullanılmıştır.

ABD'de *Elektronik ortamda depolanan bilgi* (Electronically Stored Information-ESI) terimi kullanılmaktadır, Tanımlama ilk *olarak Federal Hukuk Muhakemeleri Usulü* Kural 34 (a)'da yer almıştır. Maddeye 2006 yılında yapılan değişiklikle eklenmiş olan ESI, *"bilgilerin elde edilebileceği herhangi bir ortamda depolanan yazılar, çizimler, grafikler, çizelgeler, fotoğraflar, ses kayıtları, görüntüler ve diğer veri veya veri derlemelerini"* içermektedir. Madde 34 (a) için verilen 2006 tarihli komite notunda, tanımlamayla mevcut tüm bilgisayar tabanlı bilgi türlerinin ve gelecekteki değişiklikleri ve gelişmeleri de kapsamasının amaçladığı ifade edilmektedir[19]. İngiltere'de PACE 19. maddesinde el koyma düzenlenirken *herhangi bir elektronik biçimde kaydedilen bilgi (information which is stored in any electronic form)* ifadeleri tercih edilmiştir[20]. Almanya'da kâğıda basılı ve elektronik ortamda tutulan belgelerin incelenmesini düzenleyen *StPO* 110. maddesinde *elektronik depolama ortamı (elektronischen*

[17] Council Directive 2013/40/EU - Attacks against information systems 2013 (Official Journal of the European Union, L 218) 8 Madde 2-b
[18] Proposal For A Council Framework Decision on Attacks Against Informations Systems - Explanatory Memorandum 2002
[19] 28 USC Appendix FRCP, Rule 34 Producing Documents, Electronically Stored Information, and Tangible Things or Entering onto Land for Inspection and Other Purposes
[20] Police and Criminal Evidence Act - 1984 1984 m.19/4

Speichermedien) ifadesi kullanılmıştır[21]. Fransa'da el koyma ile ilgili *CPP* 56. maddesinde *bilgisayar verileri (données informatiques)* tabirine yer verilmiştir[22].

CMK'nın 134. maddesinde yer alan düzenlemede *arama, kopyalama, el koyma* tedbirlerine yer verilmiştir. Kopyalama bilgisayar verilerine özgü bir koruma tedbiridir. Arama ve el koyma tedbirleri, genel arama ve el koyma tedbirlerine göre farklılıkları bulunan özel nitelikli tedbirlerdir[23]. Bilgisayar verilerinde arama tedbiri maddenin 1. fıkrasında yer almaktadır. Kopyalama tedbirine 1 ve 5. fıkralarda yer verilmiştir. Verilerin kaydedildiği araçlara el koyma ise 2., 3. ve 4. fıkralarda düzenlemiştir.

II. TEDBİRİN HUKUKİ NİTELİĞİ

Bilgisayarlarda, bilgisayar programlarında ve bilgisayar kütüklerinde arama ve el koyma, şahısların özel hayatına ve kişisel verilerine yönelik müdahalelerin ağırlığı dikkate alınarak *özel koşullara bağlı, son çare* olarak başvurulabilecek, bir koruma tedbiridir[24].

Bilgisayar verilerinde arama, bireylerin temel hak ve özgürlüklerine ağır bir şekilde müdahale eden bir koruma tedbiridir. Temel hak ve özgürlükler, Anayasa ile koruma altına alınmış olup ancak kanuni düzenlemelerle sınırlama yapılabilir ve müdahale edilebilir. Koruma tedbirlerinin ortak özellikleri ve koşulları, bilgisayar verilerinde arama ve el koyma için de geçerlidir[25]. Bu bağlamda kişilerin temel hak ve özgürlüklerine müdahale eden bilgisayar verilerinde arama ve el koyma, kanuni dayanağı olan, belli bir yoğunluktaki suç şüphesi üzerine geçici olarak oranlılık ilkesi çerçevesinde hâkim kararına dayanılarak başvurulan bir koruma tedbiridir.

Bilgisayar verilerinde arama ve el koyma, adli bilişimin kapsamına giren ve bilimsel metotlar çerçevesinde oluşturulan standartlara uygunluk içerisinde uygulanan bir tedbirdir[26]. Yasal kapsam ve çerçevesi, genel arama ve el koyma tedbirleri ile bağlantılı olarak CMK'nın 134. maddesinde çizilmiş, uygulama yöntem ve usulleri adli bilişimin uluslararası bilimsel standartları ile şekillendirilmiştir.

[21] Die Deutsche Strafprozessordnung StPO m. 110/3
[22] Code de Procédure Pénale m. 56
[23] Değirmenci (n 1) 315; Osman Gazi Ünal, 'Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma' (Yüksek Lisans Tezi Gazi Üniversitesi Sosyal Bilimler Ensitüsü 2011) 88; Özen ve Baştürk (n 13) 143; Çelik (n 13) 29
[24] Yaşar ve Dursun (n 1) 7; Aldemir (n 1) 179
[25] Değirmenci (n 1) 313
[26] Yaşar ve Dursun (n 1) 7

III. CMK'NIN 134. MADDESİNDE YER VERİLEN TEDBİRLER

Tedbir ile elde edilen sayısal delillere dayanarak bir yargılama yapılacak ve hüküm verilecektir. Sayısal delillerin; elde edilme ve analiz sürecinde uzmanlarca yerine getirilen tüm işlemlerin doğru yöntemlerle ve eksiksiz yapılarak, objektif ve tarafsız sonuca ulaşıldığı, şeffaf bir şekilde ortaya konmalıdır[27]. Bunu sağlamak için bilgisayar verilerinde arama, kopyalama ve el koyma tedbirine ilişkin işlemler adli bilişimin bilimsel yöntemleri izlenerek yerine getirilmelidir.

Bilimsel bir yöntemin en önemli yönü, herhangi bir deney veya gözlemin bağımsız olarak doğrulanabilir ve tekrarlanabilir olması gerektiğidir. Adli bilişim faaliyetlerinde izlenen yol, tarafsız kişilerce yinelendiğinde aynı sonuçlara ulaşılabilmelidir. Yargılanan bir kişinin özgürlüğünün kısıtlaması söz konusu olduğunda, adli bilişim yöntemleriyle elde edilen bulguların bağımsız olarak doğrulanabilmesi, özellikle önemlidir. Sayısal delilleri bulmaya ve analiz etmeye yönelik işlemlerin, başka uzmanlarca doğrulanmasını sağlayacak şekilde ayrıntılı olarak belgelenmesi gerekmektedir[28].

Mukayeseli hukukta ve ülkemizde yapılan düzenlemeler arasında ortak bir terminoloji kullanılması, tedbirin uygulanmasında eksik kalan veya fazladan yürütülen işlemlerin belirlenmesinde en önemli adımdır. Kanuni düzenlemelerde detaylı olarak bulunmayan ve adli bilişim çalışmalarında başvurulan işlemlerin, CMK'nın 134. maddesinde yer alan tedbirler bakımından dağılımını şu şekilde yapmak mümkündür.

1. *Arama tedbiri kapsamında icra edilebilecek işlemler:* verilere erişme, verilerde arama, şifre bulma, silinen verileri geri getirme, kriptolu verileri deşifre etme, veri kurtarma, veri çıkarma (Extracting), verilerin ilişkilerini, aidiyetini belirleme, analiz etme, yorumlama, raporlama ve sunum.
2. *Kopyalama tedbiri kapsamında icra edilebilecek işlemler:* adli kopya (imaj) alma, verilerin bütünlüğünü, doğruluğunu, güvenilirliğini koruma, veri bütünlüğü değeri hesaplama (HASH değerleri alma), verilere el koyma, alınan adli kopyadan bir suretini şüpheli veya müdafiine verme.
3. *El koyma tedbiri kapsamında icra edilebilecek işlemler:* donanımlara el koyma, delil toplama, koruma, delil zinciri oluşturma, delilleri uygun şekilde paketleme, nakletme ve saklama,

[27] Değirmenci (n 1) 164
[28] Eoghan Casey, Digital Evidance And Computer Crime (3. Baskı, Elsevier 2011) 25

Burada CMK'nın 134. maddesinde yer verilen tedbirlerin terim anlamlarının detaylandırılarak incelenmesinde fayda görmekteyiz. Ayrıca mukayeseli hukukta yer alan bazı terimlerin tanımlanması terminolojide birliğinin oluşturulması bakımından önem arz etmektedir.

A. ARAMA – ERİŞİM – İNCELEME

Bilgisayar verilerinde arama tedbirini, yetkili merciin verdiği karar üzerine, işlenmiş bir suça ilişkin sayısal delil elde etmek üzere, adli bilişim uzmanlarınca, şüphelinin kullandığı bilişim sistemlerinde bulunan, şüpheliye ait depolanmış verilerde, uygun donanım, yazılım ve fonksiyonlar yardımıyla, veri bütünlüğünü koruyarak, verilere erişme, görünmez verileri görünür ve anlaşılır hale getirme, silinmiş kaybolmuş verileri geri getirme, bozuk veya fiziksel olarak hasarlı cihazlardaki verileri kurtarma, gerektiğinde şifreli veya kriptolu verileri deşifre etme, soruşturmanın konusuyla ilgili daha önceden belirlenmiş, olayı aydınlatıcı harf, rakam, kelime, terim, ses, fotoğraf, video, çizim ve benzerlerini tüm veriler üzerinde arama, veri depolama üniteleri ile verileri kimliklendirme (aidiyetlerini, kime ait olduklarını, belirleme), bilgisayar verilerini tarih-zaman sıralamasıyla yeniden canlandırma, bulunan sonuçları sunma faaliyetlerinin tümü olarak tanımlayabiliriz.

CMK'da bilgisayar verilerinde arama tedbirine ilişkin bir tanımlama yapılmamıştır. Tedbir kararı verildiğinde ne tür işlemlerin gerçekleştirilebileceği hakkında bir bilgi bulunmamaktadır.

Her ikisinde de amaç suça ilişkin iz, emare, bulgu, bilgi ve delile erişmek olsa da bilgisayar verilerinde arama, genel aramadan oldukça farklıdır. Suç delili elde etmek amacıyla bina içinde veya kişi üzerinde gerçekleştirilen genel arama, somut bir şey bulmak üzere elle yoklama, gözle tarama, örtülü kapalı gizli yerlere bakma, koklama, duyma gibi beş duyu organıyla yapılan fiziksel faaliyetlerdir[29].

Genel arama tedbiri, konut içine girme (erişim) hakkı verdiği gibi, Bilgisayar verilerinde arama tedbiri de kişisel verilere hukuka uygunluk içerisinde erişim izni vermektedir. Teknik anlamda veriler üzerinde hiçbir arama yapılmasa bile verilere erişebilir olmakla temel hak ve özgürlükler, özel hayatın gizliliği, kişisel verilerin korunması hakkı ihlal edilmiş olacaktır. Doktrinde bilgisayarlarda aramanın, adli kopya alındığı zaman değil, verinin insan tarafından görülebildiği, ekrana yansıma veya yazıcıdan çıktı alınması anında gerçekleştiğini ifade

[29] Adli ve Önleme Aramaları Yönetmeliği RG. 01.06.2005, S. 25832 m 5 28/5

edilmektedir[30]. Arama kararı öncelikle verilere erişme ve sonrasında veri bütünlüğünü bozmadan veriler üzerinde çeşitli fonksiyonların çalıştırılması hakkını vermektedir. *Avrupa Konseyin Siber Suçlar Sözleşmesinde* de *arama (Search)* kavramı ile *erişim (Access)* kavramının eşdeğer anlamda kullanılmaktadır[31]. Arama kararı verilere erişime olanak veren bir karardır. Diğer bir ifade ile arama kararı yok ise hiçbir şekilde verilere erişim hakkı da bulunmamaktadır.

Bilgisayarlarda aramanın hedefi, soruşturma konusu olan suçla ilgili, delil olabilecek verilere ulaşmaktır. Bu verilere ulaşmak için icra edilmesi zorunlu olan tüm fiiller arama tedbiri içerisinde değerlendirilmelidir. Örneğin konutta yapılan bir aramada, aramaya karşı çıkılması halinde, direncin ortadan kaldırılması için durumun haklı kıldığı ölçüde *güç kullanılması,* kilitli bir kasa gibi açılması özellik isteyen bir eşyaya tesadüf edildiğinde, kolluk tarafından veya masrafları kollukça karşılanmak üzere bu konudaki meslek erbabına *açtırılması, arama kararının* kapsamında değerlendiren fiillerdir[32]. Bilgisayar verilerinde arama, anahtar kelime aramasından daha fazlasıdır. Basitçe, bir kelime işlemci programına veya bir veri tabanına girip bir kelimeyi bulma faaliyeti aramanın ifade ettiği geniş anlamın sadece küçük bir parçasını göstermektedir. Bilgisayarlarda arama kararı verildiğinde sayısal delile ulaştıracak, tüm araştırma, bulma, veriyi görünür ve anlaşılır hale getirme, şifre bulma, kripto çözme, silinmiş verileri geri getirme, kayıp dosyaları yeniden oluşturma (File Carving), sıkıştırılmış dosyaları açma gibi işlemleri de kapsam içerisinde değerlendirmek gerekmektedir. Bu işlemler, nihai hedef olan sayısal delile ulaşmak için yapılması gereken hazırlık çalışmalarıdır.

Bilgisayar verilerinde arama çeşitli yöntemlerle icra edilebilir. Birinci yöntem olarak manuel gezinti diyebileceğimiz (manual browsing), her dosyayı uygun programla tek tek açıp içeriğine göz atmak ve taramak işlemidir ki fiziki aramalara benzer bir yöntemdir[33]. Bu yöntem ile milyonlarca veriyi, analiz etmek ve delile ulaşmak çok uzun zaman alacaktır, hatta kimi zaman imkansızlaştıracaktır. O nedenle bilgisayar verilerinde bilgisayara özgü arama tekniklerine ihtiyaç vardır.

Bilgisayar verilerinde en basit arama işlemi, her ofis yazılımında yer alan ve açılan dosya içeriğinde geçen bir kelimenin aranması işlemi olan *bul* fonksiyonudur. Bul fonksiyonu

[30] Kerr (n 12) 551
[31] Explanatory Report to the Convention on Cybercrime (ETS No. 185) 2001 60 m 137 197; Sanal Ortamda İşlenen Suçlar Sözleşmesi (Convention on Cybercrime) - 2001 m. 19
[32] Adli ve Önleme Aramaları Yönetmeliği RG. 01.06.2005, S. 25832 m 30
[33] Pavel Gladyshev, 'Formalising Event Reconstruction in Digital Investigations' (PHD Dissertation, University College Dublin, Faculty of Science 2004) 22

ile anahtar kelime araması (Keyword Search) birbirinden farklı işlemlerdir. *Bul* fonksiyonu sadece o anda açılan ve görüntülenen dosya üzerinde işlem gerçekleştirirken, anahtar kelime araması tüm dosyalar üzerinde işlem yürütmektedir. Bilgisayar verilerinde arama işlemlerini hızlandırmak için en yaygın olarak kullanılan yöntem anahtar kelime aramasıdır[34].

Ancak soruşturmalarda, anahtar kelime araması yeterli olmayabilir. Anahtar kelime araması yapılırken aranan kelimeler ile birebir eşleşen kelimeler bulunmaktadır. Aslında veriler arasında yer almasına rağmen, arama için kullanılan yazılım tarafından yakalanamayan, kaçırılan kelimeler olması (False Negative), veya dava dosyasıyla ilgili olmayan verilerin bulunması (False Positive) gibi sonuçlarla karşılaşılabilmektedir[35]. Bu durum soruşturma için hatalı sonuçlara ulaşılmasına neden olabilmektedir. Soruşturma için en önemli bilgi gözden kaçırılabilmekte veya gereksiz çöp niteliğinde binlerce veriyi analiz etmeye çalışarak vakit harcanabilmektedir.

Bir takım hedef veriler için anahtar kelime araması yeterli değildir. Örneğin bir veri depolama ünitesinde yer alan kredi kartı numaralarını, banka hesap numaralarını, IBAN numaralarını, vatandaşlık numaralarını, tüm elektronik posta adreslerini, IP numaralarını anahtar kelime araması ile bulmak neredeyse imkansızdır. Bulmak için ifadeyi birebir olarak bilmek ve aramak gerekir. Bunun yerine daha profesyonelce bir yaklaşımla *belirli kalıp araması (Regular Expression Search – REGEX)* yapılmalıdır. Bu işlem için belirli düzeyde kodlama bilgisi ile bir kalıp oluşturularak kalıba uyan ifadeler veriler içerisinde aranmaktadır[36].

Yukarıda anılan arama metotları, açık metin (Clear Text) olarak ifade edilebileceğimiz, şifrelenmemiş, kriptolanmamış, sıkıştırılmamış, silinmemiş, kaybolmamış veriler üzerinde işe yaramaktadır. Açık metin halinde bulunmayan verilerin, arama kararı kapsamında öncelikle okunabilir, görülebilir, indekslenebilir, anlaşılabilir hale getirilmesi zorunludur. Bunlar adli bilişim uzmanlarınca yerine getirilebilecek, özel eğitim, bilgi, tecrübe ve dikkat isteyen işlemlerdir[37].

Kimi zaman delil olabilecek verileri sadece bulmak yeterli değildir. Verilerin soruşturmalarda verimli delil olabilmesi için mahkeme heyetince ve dava taraflarınca açık bir

[34] Joakim Kävrestad, Fundamentals of Digital Forensics_ theory, methods, and real-life applications-Springer (Springer US 2020) 117; André Årnes (ed), Digital Forensics (John Wiley & Sons, Inc 2018) 41; Casey, Digital Evidence - 2011 (n 28) 403; Bill Nelson, Amelia Phillips ve Christopher Steuart, Guide to Computer Forensics and Investigations: Processing Digital Evidence Fifth Edition (Cengage Learning 2016) 274; Hüseyin Çakır ve Mehmet Serkan Kılıç, 'The Keyword Search Method and It's Importance in Computer Forensics / Adli Bilişimde Anahtar Kelime Araması Metodu ve Önemi' (2016) 13 Journal of Human Sciences 2368, 2369-2370

[35] Gladyshev (n 33) 22-23

[36] Çakır ve Kılıç (n 34) 2370-2371; Årnes (n 34) 41; Gladyshev (n 33) 23

[37] Çakır ve Kılıç (n 34) 2375

şekilde anlaşılır hale gelmesi için arama kararı kapsamında yorumlanması da gerekir. Veriler yorumlanmadıkları takdirde anlamsız bir yığından ibaret olacaktır[38]. Örneğin banka hesaplarına ilişkin yolsuzluk soruşturmasında, kayıtlar üzerinde yasadışı değişiklik yapılıp yapılmadığını tespit etmek için banka veri tabanında bulunan günlük (log) kayıtlarında arama yapılması gerekir ve bulunan kayıtlar yorumlamadığı takdirde ne mahkeme heyetine ne savcıya ne de şüpheliye hiçbir anlam ifade etmeyecek, delil olarak kullanılamayacaktır. Böyle durumlarda veriler ancak yorumlandıkları takdirde delil niteliği kazanabilir. Burada kastedilen yorumlama, verilerin analizini yapan şahsın kişisel yorumları değil, her uzman tarafından aynı sonuca ulaştıran, bilimsel ve objektif olarak yapılan yorumlar ve anlamlandırılmalardır. Tıp biliminde kan tahlil sonuçlarının konunun uzmanı olmayan kişiler için bir anlamı olmayabilir. Ancak bir tıp doktoru tahlil sonuçlarına bakarak harfleri ve rakamları anlamlandırabilmekte ve hastalık belirtisi hakkında yorumda bulunabilmektedir.

Bilgisayar verilerinde arama, depolanan veriler bakımından uygulanan bir tedbirdir. İlgili kişinin haberi dahilinde yerine getirilmelidir. Genel arama hükümleri gereğince aramada hazır bulundurulacak kişiler hakkındaki hükümler, bilgisayar verilerinde arama tedbiri içinde geçerlidir. Bilgisayar verilerinde arama tedbirinin akışkan veriler bakımından uygulanma alanı yoktur. Akışkan veriler, iletim halinde olan verilerdir. Bilişim sistemleri arasında iletilen verilerin izlenmesi ve trafik verileri ile içeriğin elde edilmesi CMK'nın 135. maddesi kapsamında mümkündür ve ilgiliden gizli olarak icra edilmektedir[39].

B. KOPYALAMA – YEDEKLEME – VERİLERE EL KOYMA

Kopyalama tedbirini, yetkili merciin verdiği karar üzerine, işlenmiş bir suça ilişkin sayısal delil elde etmek üzere, adli bilişim uzmanlarınca, uygun donanım, yazılım ve fonksiyonlar yardımıyla, şüphelinin kullandığı bilişim sistemlerinde yer alan şüpheliye ait depolanmış verileri, el koyma anı itibariyle dondurma, veri bütünlüğünü ve güvenilirliğini sağlama, verilere ilişkin delil zincirini oluşturma ve koruma, ilk elde edildiği andan yargılamanın sonuna kadar geçen sürede el konulan verilerin değişmeden, bozulmadan, silinmeden, kaybolmadan kalmasını sağlama, verilerde soruşturmaya ilişkin arama, analiz, raporlama yapılmasına olanak sağlamak üzere, mahkemelerce verinin aslı olarak kabul edilecek şekilde, adli bilişime özel yöntemlerle verileri kopyalama, özet değer çıkarma, veri bütünlüğünü doğrulama faaliyetleri olarak tanımlayabiliriz.

[38] Årnes (n 34) 31
[39] Değirmenci (n 1) 364

CMK'nın 134. maddesinde bilgisayar kayıtlarından kopya çıkarılması zikredilmiş, ancak kopyalama tedbiri hakkında bir tanımlama yapılmamıştır. Verilerin kopyalanması soyut olan elektronik verilere has bir koruma tedbiridir[40].

Ülkemizin taraf olduğu *Avrupa Konseyi Siber Suçlar Sözleşmesinin* 19. maddesinde bilgisayar verilerinde arama ve el koyma düzenlenmiştir. Maddenin 3. fıkrasının b bendi, söz konusu bilgisayar verilerinin bir kopyasının oluşturulmasına ve bunun muhafaza edilmesine ilişkindir[41]. *Sözleşmenin* açıklayıcı raporunda, el koyma izah edilirken, verinin yahut bilginin kaydedildiği fiziksel ortamın alınıp götürülmesi veya bu verinin yahut bilginin kopyalanarak muhafaza edilmesi anlamına geldiği belirtilmektedir[42]. Buna göre sözleşmeye taraf ülkelerce *kopyalama* ile *verilere el koyma* eşdeğer olarak kabul edilmektedir. Kopyalama teriminin, teknolojinin gelişmesi karşısında hukukun uyum sağlaması amacıyla yapılan bir öneri olduğu, *arama* yerine *erişim* teriminin, *el koyma* yerine *kopyalama* teriminin kullanılmasının teknoloji odaklı terimler olarak maksadı daha doğru ifade ettiği vurgulanmaktadır[43].

Doktrinde kopyalamanın arama kararı kapsamında bir işlem olduğunu, ayrıca bir kopyalama kararı vermeye gerek olmadığı ifade edilmektedir[44]. Bir başka görüş, kopyalamanın bir *arama* olmadığını değerlendirmektedir. Kopyalama işlemleri uygun adli bilişim donanım ve yazılımları ile yerine getirilmektedir. Kopyalama yapılırken işlemi gerçekleştiren kolluk görevlisi, verilere erişmemekte, görmemekte ve gözlemlememektedir. Arama ancak erişim ve gözlemleme ile başlamaktadır. Verilere tam erişimi olan ise adli bilişim donanım ve yazılımlarıdır. Görevlinin kullandığı araçların verilere erişimi, kendisi tarafından görülmediği müddetçe *arama* anlamına gelmeyecektir. Araçların yürüttüğü işlemler, görevliye atfedilemeyecektir. Diğer taraftan geleneksel el koyma mutlak anlamda sadece somut mülkler için uygun görülmesine rağmen kopyalama *el koyma* olarak değerlendirilmektedir[45].

Amerikan hukukunda kopyalama işleminin el koyma olup olmadığı hakkında çeşitli emsal kararlar mevcuttur. *United States v. Gorshkov* kararında Mahkeme, Rusya'da bulunan verilerin kopyalanmasının el koyma olmadığını, sanığın veriler üzerindeki mülkiyet hakkına müdahale edilmediğini, verilerin bozulmamış ve değiştirilmemiş olarak bulundukları yerde

[40] ibid 314
[41] Sanal Ortamda İşlenen Suçlar Sözleşmesi (Convention on Cybercrime) - 2001 m. 19/3-b
[42] Explanatory Report to the Convention on Cybercrime m. 197
[43] ibid m. 137
[44] Servet Yetim, Ceza Muhakemesi Kapsamında Sosyal Medyadan Elektronik Delil Toplama ve Değerlendirme (1. Baskı, Seçkin Yayınları 2016) 468
[45] Susan W Brenner, 'Copying as a Seizure (Again)' (CYB3RCRIM3 Observations on Technology Law and Lawlessness 2009) <http://cyb3rcrim3.blogspot.com/2009/07/copying-as-seizure-again.html> Erişim tarihi 05 Kasım 2020

kalmaya devam ettiklerini, sanığın veya yardımcılarının verilere ulaşmaya ve kontrol etmeye devam edebildiklerini, verilerin kopyalanmasının mülkiyet hakları üzerinde kesinlikle hiçbir etkisinin olmadığını, kabul etmiştir[46].

Ancak bu karar doktrinde eleştirilere maruz kalmıştır. Geleneksel el koyma, bilgisayar verilerine el koymaya nispeten daha basit ve anlaşılabilir niteliktedir. Bir polis memuru, bir şüphelinin bilgisayar ve donanımını hukuka uygun olarak alıp giderse bu işlem bir el koymadır. Bilgisayar, poliste olduğu müddetçe şüphelide bulunmamaktadır. Somut mallara el koymada, mülkiyet üzerindeki tasarruf yetkisi şüpheliden devlete geçmektedir. Benzer uygulamanın sanal dünyada da yani somut olmayan değerler için de geçerli olma ihtimali vardır. Görevliler verileri bir bilgisayar sisteminden kopyalar ve ardından kopyalanan verileri söz konusu bilgisayar sisteminden silerlerse, veri üzerindeki tasarruf yetkisi tamamen şüpheliden işlemi gerçekleştiren görevliye geçecektir. Bu işlem geleneksel el koyma işlemi ile örtüşmektedir[47]. Elbette verilere el koyma bu durumdan biraz daha farklıdır.

Amerikan doktrininde el koymada el değiştiren tasarruf yetkisi, hırsızlık örneği üzerinden açıklanmaktadır. Oregon'da görülen 2001 tarihli *State v. Schwartz*[48] davasında, *Randal Schwartz*, işvereni Intel Corporation'a ait bir şifre dosyasını kopyalaması nedeniyle bilgisayar hırsızlığından yargılanmıştır. Schwartz, esasen suçlamanın geçersiz olduğunu çünkü hiçbir şey *çalmadığını* savunmuş, eylemin hırsızlık suçu tanımına girmediğini ileri sürmüştür. Oregon eyalet yasalarına göre geleneksel olarak hırsızlık, *sahibini mülkiyetinden ve kullanımından mahrum bırakmak amacıyla başka birinin mülkünü almak olarak* tanımlanmaktadır. *Schwartz*, şifre dosyasını kopyalamanın, mülkiyet haklarından tamamen mahrum bırakmak amacıyla yapıldığını gösteren hiçbir kanıtın olmadığını ifade etmiştir. Şifre dosyası hala işverende olduğu için hırsızlık yapmadığını, sadece bir kopyasını aldığını iddia etmiştir. Zira şifreler halihazırda *İntel'in* elinde bulunmaya devam etmektedir. Ancak *Oregon Temyiz Mahkemesi* bu iddiayı kabul edilebilir bulmamıştır. *Intel'in* parola verilerinin gizliliğini koruma yeteneğinin *Schwartz* tarafından zayıflatıldığını tespit etmiştir. Mahkemeye göre şifrelerin *ancak ne olduklarını başka hiç kimsenin bilmediği sürece* değerli olduğundan, *Intel* gerçek parola verilerine sahip olmasına rağmen *bir şeyi* kaybetmiştir[49].

[46] United States v Gorshkov, 2001 WL 1024026, 2001
[47] Susan W Brenner, 'Seizure' (CYB3RCRIM3 Observations on Technology Law and Lawlessness 2006) <http://cyb3rcrim3.blogspot.com/2006/02/seizure.html> Erişim Tarihi 06 Kasım 2020
[48] State v Schwartz, 173 Or App 301, 21 P3d 1128, 2001.
[49] Brenner (n 47)

Eğer Oregon Mahkemesi, *United States v. Gorshkov* davasının hükmüne göre hareket etmiş olsaydı *Schwartz*, davayı kazanabilirdi. Oregon mahkemesi, hırsızlık suçlamasını reddetmek zorunda kalacaktı çünkü işveren *verilere sahip olmayı bütünüyle kaybetmemişti.* Mahkeme, "*hırsızlığın, birisinin mülkünü yetkisiz bir şekilde almak* ve *mülkiyetin* de "*değerli herhangi bir şey* olarak tanımlandığını belirtmiştir. Delillerin, şifrelerin *değerli* olduğunu gösterdiğini, bunun da *mülk* oldukları anlamına geldiğini tespit etmiştir. Buna göre verileri kopyalamak eğer hırsızlık olarak değerlendirilebiliyorsa, o halde kopyalamak da el koyma olarak değerlendirilmelidir. Öyleyse izinsiz olarak bir kişiye ait veriler kopyalandığında, o kişi verileri üzerindeki mülkiyet hakkının bir kısmını kaybetmektedir. Bu durumda, kolluk kuvvetlerinin verileri kopyalayabilmesi için bir hâkim kararına ihtiyacı vardır[50].

Amerikan Yüksek Mahkemesi 1967 tarihli *Katz* kararından itibaren arama ve el koymanın somut olmayan değerler için de mümkün olduğunu kabul etmiştir[51]. Nitekim arama el koymayı düzenleyen *Federal Ceza Muhakemesi Kuralları (FRCrP)* 41. maddesine[52] 2009 yılında gerçekleştirilen değişiklik ve içtihat kararları[53] ışığında kopyalama, el koyma olarak kabul edilmektedir. *Dokuzuncu Bölge Mahkemesi*, görülen bir davada kopyalanan verileri *el konulan veri (seized data)* olarak tanımlamıştır[54].

Doktrinde el koyma, olay yerinin dondurulması, delillerin korunması işlevi açısından değerlendirilmektedir. Tıpkı el konulmasıyla fiziksel bir materyalin olay anındaki haliyle kalmasının sağlandığı gibi, dava süresince gelecekte kullanabilmek için verilerin elektronik kopyasının üretilmesi de verileri dondurmaktadır ve savcılığın kontrolü altındaki deliller arasına eklenmektedir. Verilere el konulmasıyla birlikte soruşturma yürüten görevliler veriler, üzerinde kontrol sağlamaktadırlar. Amerikan Anayasasınca koruma altında olan verilerin kopyalanması, Dördüncü Değişiklik kapsamında bir el koyma işlemi olarak kabul edilmelidir[55].

El koymanın belirleyici unsuru, zilyedinin rızası dışında malvarlığı üzerinde tasarruf yetkisinin adli makamlara geçmesi olarak tanımlanmaktadır[56]. Tasarruf yetkisinin adli makamlara geçmesinin doğal sonucu olarak, malvarlığının zilyedi tasarruf yetkisini kaybetmektedir. Doktrinde bir görüşe göre kopyalama neticesinde şüphelinin veriler üzerindeki tasarruf yetkisinin kaybolmadığı, bu nedenle el koyma olarak değerlendirilemeyeceği ifade

[50] Brenner (n 45)
[51] Katz v United States, 389 US 347, 1967
[52] Rule 41. Search and Seizure | Federal Rules of Criminal Procedure m. 41 e-2/b
[53] United States v New York Telephone Co, 434 US 159, 1977
[54] United States v Comprehensive Drug Testing Inc, 579 F3d 989, 2009
[55] Orin S Kerr, 'Fourth Amendment Seizures of Computer Data' (2010) 119 The Yale Law Journal 700, 709
[56] Ahmet Gökcen ve diğerleri, Ceza Muhakemesi Hukuku (4. Baskı, Adalet Yayınları 2020) 462

edilmektedir[57]. Kopyalama ile veriler üzerindeki tasarruf hakkının yitirilmediğini ifade edilmektedir. Kopyalama işleminden sonra asıl veriler sahibinin tasarrufunda bırakılmaktadır. Ancak, verilerin geleceğini belirleme bağlamında, kişinin verileri kiminle paylaşacağına ilişkin hakkı ortadan kaldırılmaktadır. Buna göre hukukumuzda verilerin kopyalanmasının el koyma olarak değerlendirilmesi ancak, el koymanın maddi olmayan değerleri de kapsayacak şekilde geniş yorumlanmasıyla mümkündür[58].

Kanımızca verilerin kopyalanmasıyla tasarruf yetkisi kısmen kaybedilmektedir. Verilerin tasarrufu adli makamlar ile verilerin sahibi arasında paylaşılmaktadır. Varsayalım ki verilerin sahibi, kopyalanmak suretiyle adli makamların elinde de geçen verilerinden bazılarını ebediyen yeryüzünden silmek, yok etmek veya değiştirmek istemektedir. Kendi tasarrufunda bulunan verileri silebilecek, ancak tasarrufu dışında kalan verilerin bu kopyalarını silemeyecek, yok edemeyecek, değiştiremeyecektir. Bu nedenle kopyalama neticesinde veriler üzerindeki silme, değiştirme tasarrufunu kaybetmektedir. Ancak görme, okuma tasarrufunu devam ettirmektedir. Bu ise el koymanın uygulanma gerekçesi olan delillerin yok edilmesinin ve değiştirilmesinin engellenmesi amacına uygun düşmektedir.

Somut eşyalara el koymanın, soyut veriler bakımından *birebir* olarak uygulanması, verilerin adli kopyasının alınarak adli makamlara ait elektronik ortama taşınması ve beraberinde şüphelide kalan verilerin kaldırılması ile mümkündür. Böyle bir uygulamada tasarruf yetkisi tamamen adli makamlara geçeceği gibi, şüphelinin tasarrufunda hiçbir veri bırakılmamış olacaktır. Bu uygulamaya maruz kalan şüpheli, verilerini kullanamayacak, örneğin, ticari faaliyetlerine devam edemeyecek, kişisel verilerine erişemeyecek, hayatın doğal akışını devam ettiremeyecektir. Böyle bir uygulama suç oluşturmayan veriler bakımından yersiz olacak ve temel hak ve özgürlüklere çok ağır bir müdahale ve ölçülülük ilkesine aykırılık oluşturacaktır. Yasa koyucu, verilerin şüphelinin sistemlerinden silinerek alınıp götürülmesi yerine, vatandaş lehine olan ve yargılama açısından bu tür bir uygulamayla aynı sonuçları doğuracak ve delil niteliğindeki verilerin bozulmadan, kaybolmadan korunmasını temin edecek şekilde verilerin adli kopyasının alınması suretiyle el konulması tedbirini ikame etmiştir.

Bilgisayar verilerinde arama yapılabilmesi için verilerin kopyalanması ilk olarak yapılması gereken görevdir[59]. Ceza muhakemesinde, hukuka uygun olarak elde edilen her türlü delil ispat aracı olarak kullanılabilir. Sayısal delillerde hukuka uygunluğun önemli bir unsuru

[57] Yetim (n 44) 468
[58] Değirmenci (n 1) 373
[59] Nelson, Phillips ve Steuart (n 34) 90

ise doğruluk ve güvenilirliktir[60]. Verilerin delil olarak kabul edilmesi için değiştirilmediğinden, bozulmadığından, müdahale edilmediğinden emin olunması gerekmektedir[61]. Bilgisayar verilerinde arama ve el koymayı gerçekleştiren görevliler doğruluğun sağlanması için gereken her türlü tedbiri almak zorundadır. Aksi takdirde elde edilen verilerin delil niteliği kaybolacaktır. *Yargıtay 16. Ceza Dairesi*; sayısal delillerin suistimale müsait olan verilerden oluştuğunu, kanun ile sınırları belirlenmiş teknik gerekliliklere uygun olarak toplanması ve yargılama makamlarına eksiksiz, bozulmamış halde sunulması gerektiğini, kabul etmektedir. Sayısal delillere harici müdahalenin teknik olarak mümkün olması, çoğu zaman kim tarafından hangi tarihte müdahale yapıldığının da belirlenememesi karşısında, güvenli bir şekilde el konulup incelenebilmesi için, kural olarak mahallinde adli kopya alındıktan sonra orijinal medyanın şüpheliye bırakılması gerektiğini vurgulamaktadır. Bununla beraber bu şartın soruşturma yapan kolluk personelinin teknik yetersizliği, ekipman yokluğu, ortamın incelemeye elverişli olmaması gibi nedenlerle yerine getirilemediğini de ifade etmektedir[62]. Verilerde güvenilirlik ve doğruluğu sağlamanın en kolay yolu adli kopya alınması, kopyanın bir suretinin şüpheliye verilmesi ve kopyanın yargılama sonuna kadar saklanmasıdır. Asıl olan adli kopya almak ve adli kopya üzerinde çalışmaktır. Ancak anılan kararda dile getirildiği gibi bu her zaman mümkün olmamaktadır. Adli kopya almak tedbiri amaç değil, verilerin bütünlüğünün, doğruluğunun ve güvenilirliğinin sağlanması için araçtır. Mahallinde adli kopya alınamadığı durumlarda, bu amaca ulaşmak için uygulanması gereken usul yine kararda anlatılmıştır[63].

Kopyalama tedbirinde uygulan işlem, bilgisayarlarda kullanılan yaygın kopyalama işleminden farklıdır. Bu farklılığı vurgulamak için terminolojide çeşitli terimler

[60] Nigel Jones and others, 'Electronic Evidence Guide a Basic Guide for Police Officers, Prosecutors and Judges' (2014) 13

[61] Aida Ashouri, Caleb Bowers ve Cherrie Warden, 'An Overview Of The Use Of Digital Evidence In International Criminal Courts' (International Human Rights Law Clinic Samuelson Law Technology & Public Policy Clinic at the University of California Berkeley School of Law 2013) 4 <https://www.law.berkeley.edu/files/HRC/Scholarly_articles_Salzburg_2013.pdf> Erişim Tarihi 12 Mart 2019

[62] Yar. 16 CD, E. 2015/2056, K. 2017/5023, 21.09.2017

[63] Buna göre aramayı yapan kolluk birimince sayısal delillere müdahaleyi önleyecek şekilde, veri barındıran ilgili donanımın seri numaraları tutanağa yazılmak suretiyle usulüne uygun olarak el konulup mühürlenmeli, şüpheli veya müdafiinin istemesi halinde nezaret etme ve denetleme imkanı sağlanarak inceleme mahalline kadar eşlik etmesi sağlanmalı ve bu yerde şüpheli veya müdafiinin hazır bulunmasına imkan verildikten sonra mümkün olan en kısa süre içinde mühür açılıp, veri saklanan medyanın derhal adli kopyasının alınarak ilgilisine de bir kopya verilmeli ve orijinal medya şüpheli veya müdafiine teslim edilmeli, yine sanık veya müdafiinin mühür açma işlemi sırasında hazır bulunmasının mümkün olmadığı hallerde, mühür açma işleminin arama ve el koyma kararını veren hakimin huzurunda açılarak adli kopya alma işleminin bu sırada yapılması yoluna gidilmesi gerektiği izah edilmektedir. Bu yolla elde edilmeyen delillerin de hukuka uygunluğu tartışılır hale geleceği ve yargılama makamınca hükme esas alınmasının mümkün olamayacağı vurgulanmaktadır. : Yar. 16 CD, E. 2015/2056, K. 2017/5023, 21.09.2017. Adli kopya ve veri bütünlük değeri alınmadan yapılan işlemin geçersiz olduğu hakkında bkz. Yar. 8 CD, E. 2012/21817, K. 2013/25428, 24.10.2013

kullanılmaktadır. *Ayna görüntü çıkarma*[64], *imaj alma (Forensic Image)*[65], *adli kopya alma*[66], *birebir kopyalama (bit to bit copy)*[67] bunlardan bazılarıdır. Biz çalışmamızda maksadı daha doğru ifade ettiğini düşündüğümüz *adli kopya* terimini kullanmayı tercih ediyoruz.

Bilgisayarlarda yapılan her işlem bir iz bırakır[68]. Bu prensip adli bilişim incelemeleri açısından, suç teşkil eden fiilleri ortaya çıkarmak için bu izlerin bulunması, takip edilmesi ve işlemlerin ortaya konulması hedefini göstermektedir. Ancak adli bilişim incelemeleri kapsamında bilgisayarlarda yapılacak işlemler de çeşitli izler bırakmaktadır. Diğer bir ifade ile bilgisayar verilerinde yapılacak aramalar, o verilerde kimin, ne zaman yaptığı belli olmayacak şekilde değişikliğe neden olacaktır. Adli bilişim uzmanı suça ilişkin bir veri elde etse bile, üzerinde değişiklik meydana gelmiş verilerin, doğruluğu ve güvenilirliği hakkında şüpheler ortaya çıkacaktır. Bu sorunun çözümü; adli kopya alınarak, orijinal verileri dondurmak ve doğruluğunu, bütünlüğünü, güvenilirliğini sağladıktan sonra, kopya veriler üzerinde arama ve analiz işlemleri yapmaktır[69].

Bilgisayar verilerinde en küçük bilgi birimi, BIT (Binary Digit) olarak ifade edilmektedir[70]. *Adli kopya alınması*, veri barındıran medya üzerinde bulunan tüm fiziksel sektörlerin manyetik veya optik değerlerinin *bit* düzeyinde birebir olarak yeni bir medya üzerinde yeniden üretilmesi, sıkıştırılarak dosya biçiminde saklanması ve bazı doğrulama mekanizmalarıyla üretilen verilerin tam bir kesinlikle aslının bir kopyası olduğunun belirlenmesidir[71]. Adli kopyada, veri depolama ünitesinde kayıtlı dosyalara ek olarak, dosya

[64] Mehmet Bedii Kaya, 'Hukuki Açıdan Bilişim Suçları, Siber Güvenlik ve Adli Bilişim' içinde Şeref Sağıroğlu ve Mustafa Şenol (ed), Siber Güvenlik ve Savunma Problemler ve Çözümler (1. Baskı, Grafiker Yayınları 2019) 260
[65] Ünal (n 23) 109; Murat Kızılyar, 'Ceza Yargılamasında Dijital Verilerin Delil Değeri' (2014) 50 Adalet Dergisi 72, 83; Robert C Newman, Computer Forensics Evidence Collection and Management, c 1 (Auerbach Publications 2007) 125; Leyla Keser Berber, Adli Bilişim (1. Baskı, Yetkin Yayınları 2004) 47
[66] Çelik (n 13) 109
[67] Ahmet Serhat Şirikçi ve Nergis Cantürk, 'Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi' (2012) 5 Bilişim Teknolojileri Dergisi 29, 30; Değirmenci (n 1) 245-246
[68] Yusuf Başlar, Ceza Yargılamasında Elektronik Delil (Yetkin Yayınları 2016) 197
[69] Değirmenci (n 1) 244-245
[70] Nurettin Topaloğlu, 'Bilgisayar Mimarisi' içinde Hüseyin Çakır ve Mehmet Serkan Kılıç (ed), Adli Bilişim ve Elektronik Deliller (1. Baskı, Seçkin Yayınları 2014) 65
[71] Madihah Saudi, 'An Overview of Disk Imaging Tool in Computer Forensics' (Information Security Reading Room, 2001) 3 <https://www.sans.org/reading-room/whitepapers/incident/overview-disk-imaging-tool-computer-forensics-643> Erişim Tarihi 16 Kasım 2020; Hüseyin Kiçeci, 'Bilgisayar Medyalarına İlk Müdahale' içinde Hüseyin Çakır ve Mehmet Serkan Kılıç (ed), Adli Bilişim ve Elektronik Deliller (Seçkin Yayınları 2014) 172

sistemine ilişkin veriler[72], işletim sistemi tarafından kullanılmayan alanlar[73], silinmiş dosyalar da yer alır[74]. Yedekleme ve standart disk kopyalama işlemlerinde işletim sistemi tarafından kullanılmayan alanlar ile dosya sistemine ilişkin alanlar ve silinmiş veriler kopyalanamamaktadırlar[75].

Bilgisayar verilerinde arama ve el koyma tedbirinin tüm süreçleri şeffaf ve tekrar edilebilir olmalıdır[76]. Bu ilke kopyalama tedbiri için de geçerlidir. Kopyalama tedbirinde, adli kopyanın alınması ve devamındaki süreçler açık ve anlaşılır bir şekilde belirtilmeli ve kayda alınmalıdır. Kullanılan yazılım ve donanımların tedbiri yerine getirmek için uygun olduğu belirtilmelidir. Amerika Birleşik Devletleri federal standart enstitüsü olan *Ulusal Standartlar ve Teknoloji Enstitüsü (NIST)* adli kopyalama cihazlarında olması gereken özelliklerinden bazılarını şu şekilde belirlemiştir. *"1) Araç, kendisi tarafından görülebilen her erişim arayüzü kullanan dijital kaynaktan veri elde edebilmelidir. 2) Araç, dijital bir kaynağın klonunu veya adli kopyasını oluşturabilmeli veya kullanıcıya bir dijital kaynağın klonunu veya adli kopyasını seçip daha sonra oluşturma yeteneği sağlayabilmelidir. 3) Araç, en az bir yürütme ortamında çalışabilmeli ve her yürütme ortamında dijital kaynaklardan veri elde edebilmelidir. 4) Araç, tüm görünür veri sektörlerini dijital kaynaktan tamamen alabilmelidir. 5) Araç, tüm gizli veri sektörlerini dijital kaynaktan tamamen alabilmelidir. 6) Araçla dijital kaynaktan elde edilen tüm veri sektörlerini doğru bir şekilde elde edilebilmelidir. 7) Dijital bir kaynaktan okunan çözülmemiş hatalar varsa, araç kullanıcıya hata türünü ve hata yerini bildirmelidir. 8) Dijital bir kaynaktan okunan çözülmemiş hatalar varsa, o zaman araç, erişilemez veriler yerine hedef nesnede zararsız bir dolgu kullanacaktır. 9) Adli kopya dosyasının oluşturulmasından sonra*

[72] Bir dosya sistemi, bir işletim sisteminin diskteki verilere erişimi için bir yol haritasıdır. İşletim sisteminin kullandığı dosya sistemi, verilerin diskte nasıl depolanacağını organize etmektedir. Adli bilişim uzmanlarınca şüphelinin sistemindeki verilerin değiştirilmediğinden emin olmak için, CMOS, BIOS, Extensible Firmware Interface(EFI) ve Unified Extensible Firmware Interface (UEFI) ayarlarına nasıl erişileceği bilinmelidir. Sistem BIOS'u veya EFI, donanım düzeyinde giriş ve çıkış gerçekleştiren programlar içerir. BIOS, x86 bilgisayarlar için tasarlanmıştır ve genellikle Master Boot Record (MBR) sahip disk sürücülerinde kullanılır. EFI, x64 bilgisayarlar için tasarlanmıştır ve GUID Partition Table (GPT) formatlı diskleri kullanır. Nelson, Phillips ve Steuart (n 34) 184

[73] Dosya sistemleri verileri organize etmek için kümeler (İng.: Cluster) kullanmaktadırlar. Örneğin NTFS dosya sisteminde her küme 8 sektörden oluşmaktadır ve 4096 byte veri içermektedir. Dosyalar diske kaydedilirken kümenin tamamını doldurmazsa, kalan boşluk kısım işletim sistemi tarafından kullanılmamaktadır. Örneğin 1 byte büyüklüğünde bir dosya NTFS dosya sistemine kaydedildiğinde geriye kalan 4096 byte'lık yer işgal etmektedir ve geriye kalan boş alanlar çoğu işletim sistemi tarafından kullanılmamaktadır. Bu boş alanlarda önceki dosyalara ilişkin veri artıkları kalabilmektedir. İşte bu kullanılmayan alanlar dosya artığı (İng.: file slack) olarak adlandırılmaktadır. Årnes (n 34) 161; Disk üzerinde yeni veri yazılabilecek alanlara ayrılmamış alan (İng.: Unallocated Space) denilmektedir. Bir dosya silindiğinde disk üzerinde işgal etmiş olduğu yer ayrılmamış alan olarak belirlenir. Ayrılmamış alanlar üzerinden silinmiş dosyalar tekrar kurtarılabilir. Eoghan Casey (ed), Handbook Of Digital Forensics And Investigation (2010) 37

[74] Kiçeci (n 71) 172

[75] Saudi (n 71) 3

[76] Değirmenci (n 1) 164

görüntü dosyasının (Image file) değişip değişmediğini tespit ederek bir görüntü dosyasının bütünlüğünü kontrol etmelidir. 10) Korumasız orijinal kaynakta hiçbir değişiklik yapmadan veri elde etmelidir"[77].

Veri depolama ünitelerinin fiziksel veya mantıksal olarak adli kopyaları alınabilmektedir. Adli kopya kural olarak orijinal disk üzerinde hiçbir değişiklik yapılmadan fiziksel düzeyde alınmalıdır. Birebir kopya olduğundan dolayı, orijinal diskin kriptolu olması durumunda adli kopya da kriptolu olacaktır. Bu durumda arzu edilen verilere erişilemeyecektir. Bu gibi durumlarda öncelikle kriptolanmış diskin şifresi çözülerek okunur hale getirilmesi ve bu halinin canlı olarak adli kopyasının alınması gerekecektir. Mantıksal adli kopya, bir depolama aygıtının veya bölümünün (Partition) işletim sistemi tarafından görüldüğü şekilde kopyasının alınmasıdır. Eğer bölüm kriptosu açılmış ise, mantıksal adli kopyada yer alan verilerin de kriptosu açılmış demektir. Bununla birlikte, mantıksal bir disk görüntüsü, silinen verileri geri yüklemek konusunda başarılı sonuçlar vermeyebilir, bu nedenle, fiziksel adli kopya almak mümkün olduğu sürece mantıksal adli kopya alınmamalıdır[78].

CMK'nın 134. maddesinde kopyalama tedbiri ile ilgili çeşitli terimlere yer verilmiştir. Maddenin 1. fıkrasında *"... bilgisayar kayıtlarından kopya çıkarılmasına, ..."* hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet Savcısı tarafından karar verileceği ifade edilmektedir. 2. fıkrada diğer koşullarla birlikte *"... gerekli kopyaların alınabilmesi için, ..."* ilgili araç ve gereçlere el konulabileceği, *"...gerekli kopyaları alınması halinde ..."* el konulan cihazların iade edileceği ifade edilmektedir. 3. fıkrada el koyma işlemi sırasında *"... sistemdeki bütün verilerin yedeklemesi yapılır."* ifadesi yer almaktadır. 4. fıkrada *"Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline ..."* verileceği ifade edilmektedir. 5. fıkrada *"Bilgisayar veya bilgisayar kütüklerine el koymaksızın da sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir ..."* denilmektedir.

Maddede geçen kopyalama ve yedekleme terimlerinin ifade ettiği anlam üzerinde doktrinde görüş ayrılığı bulunmaktadır. Görüş ayrılığının temel sebebi *kopyalama* ve *yedekleme* terimleri hakkında kanunda bir tanımlama bulunmamasıdır[79]. Diğer bir sebep ise kanunun hazırlandığı dönem ile arada geçen süre zarfında, bilgi teknolojilerinde ve adli bilişim bilim dalında meydana gelen gelişim ve değişimdir.

[77] National Institute of Standards and Technology, Digital Data Acquisition Tool Specification (NIST 2004) 8
[78] Kävrestad (n 34) 71
[79] Çelik (n 13) 103

Bir görüşe göre *yedekleme* terimi, birebir kopyalama işlemi değildir. Kopyalamadan farklı olarak bir terim kullanılmış ise başka bir işlem kastedilmiş olmalıdır. Yedekleme işleminde silinmiş veriler yer almamaktadır. Burada amaç sistemin malikinin veya kullanıcısının sistemde yer alan verileri kullanabilmesini sağlamaktır[80]. Diğer bir görüşe göre, sistemdeki tüm verilerin yedeklenmesi şeklinde yapılan düzenleme aslında adli kopya alma işlemidir. Maddede geçen kopyalama ve yedekleme terimleri ile kastedilen adli kopya alma işlemidir[81].

Kanımızca sistemdeki tüm verilerin yedeklenmesi, adli kopya alma işlemi ile yerine getirilmektedir. Kopyalama ve yedekleme şeklinde farklı terimlerin kullanılması neticesinde hukuki ve adli bilişim tekniğine ilişkin birbirini destekleyen anlamlardan bahsetmek mümkündür. 1. 2. ve 5. fıkrada geçen *kopyalama* ifadesi hukuki bir terim olarak, *arama, el koyma, tutuklama* gibi bir koruma tedbiri olan ve *verilere el koymayı* ifade eden *kopyalama tedbiri* anlamındadır. 1. fıkrada verilere el koyma kararının şartları, karar verecek makam, 2. fıkrada verilere el koyma tedbiri ile cihazlara el koyma tedbiri arasındaki amaç-sonuç ilişkisi, 5. fıkrada cihazlara el koymaksızın verilere el konulabileceği hususları düzenlenmiştir. *Yedekleme* ifadesi ise adli bilişime ait teknik bir terim olan *adli kopya alınması* anlamındadır[82]. 3. fıkraya göre kopyalama tedbiri, adli kopya alınmak (yedekleme) suretiyle yerine getirilmektedir. Yedekleme ifadesi hukuki değil, teknik bir terimdir ve bizatihi yapılan adli kopya alınması işlemini tarif etmektedir.

Bilgi teknolojilerinde *yedekleme (backup)* veya *veri yedekleme (data backup)*, olası bir veri kaybı olayından sonra geri yüklenerek kullanılabilmesi için orijinal bilgisayar verilerinin başka bir yerde kopyasının alınması ve saklanmasıdır[83]. Yedeklemeler, verilerin silinmesi veya bozulması nedeniyle kaybolan verileri kurtarmak veya zaman içerisinde sürekli olarak güncellenen verilerin daha önceki belirli bir zamanına döndürmek için kullanılabilmektedir. Yedeklemeler, belirli bir zamanda alınan verilerin anlık görüntü kopyalarıdır ve küresel olarak yaygın dosya biçimlerinde depolanır. Birden çok yedekleme seviyesi oluşturulabilir[84]. Veri

[80] Değirmenci (n 1) 374; Haluk Çolak ve Mustafa Taşkın, Ceza Muhakemesi Kanunu Şerhi (Seçkin Yayınları 2007) 609; Tanrıkulu (n 11) 379; Çelik (n 13) 103

[81] Ünal (n 23) 119; Ümit Bostancı ve Recep Benzer, 'Search , Copy and Seizure On The Computers In The Turkish Legal System. Türk Hukuk Sisteminde Bilgisayarlarda Arama, Kopyalama ve El Koyma' (2015) 12 International Journal of Human Sciences 1211; 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 43, 67, 68

[82] Yar. 16 CD, E. 2015/4672, K. 2016/2330, 24.04.2016

[83] 'American Heritage Dictionary Entry: Backup' (The American Heritage Dictionary of the English Language, 2020) <https://www.ahdictionary.com/word/search.html?q=backup> Erişim Tarihi 24 Kasım 2020

[84] Steven Nelson, Pro Data Backup and Recovery (Springer US 2011) 2 vd

tabanları içinden seçilen kayıtlar, veri tabanlarının tamamı, tüm belgeler, işletim sistemi seviyesi şeklinde amaca yönelik yedekleme işlemleri yapılmaktadır. Yedekleme yapılırken sıkıştırma (compression), kriptolama (encryption), tekrarlanan verilerin elenerek kopyalanması (de-duplication) gibi teknolojiler kullanılmaktadır[85].

Yedekleme işleminde tüm verilerin yedeği alınsa bile bu yedek dosyalarda, silinmiş verilerin ve işletim sistemi tarafından görülmeyen verilerin kopyası yer almamaktadır[86]. Bu nedenle bilgi teknolojilerinde yürütülen yedekleme işlemi ile adli bilişimde yerine getirilen yedekleme birbirinden farklıdır. Bu farklılığı ifade etmek için *adli kopya alma* veya *adli yedekleme (Forensic Backup)*[87] terimleri tercih edilmelidir. *Yargıtay 16. Ceza Dairesi* kararlarında yedekleme ifadesini *"imaj-adli kopya"* olarak tanımlamaktadır[88].

Bilgisayar verilerinde arama ve el koyma tedbiri uygulanırken ayrı ayrı kopyalama ve yedekleme işlemleri yapılmamaktadır. Sadece adli kopya alınmaktadır. Kopyalama benzeri başkaca bir işlemin yapılmasına gerek de yoktur. Şüpheliye de bu adli kopyadan bir nüsha verilmektedir. Sistemden alınan adli kopya aynı zamanda sistemdeki tüm verilerin yedeğini de kapsamaktadır.

C. BİLGİSAYARLARA, BİLGİSAYAR KÜTÜKLERİNE, ARAÇ GEREÇLERE EL KOYMA

CMK'nın 134. maddesinde yer alan düzenleme el koyma tedbirinin özel düzenlenmiş şeklidir[89]. Bilgisayarlara el koymayı, bir suç soruşturmasında, yetkili merciin kararı ve gerekli şartların objektif olarak varlığının kabulü halinde, adli bilişim uzmanlarınca, soruşturmalarla ilgili sayısal delil elde etmeye matuf adli kopya alınmasını ve verilere el konulmasını veya münhasıran bilişim alanında suçlardan birini işlemek amacıyla tasarlanmış veya uyarlanmış cihazların müsaderesini sağlamak amacıyla, sayısal verilere her türlü fiziksel ve elektromanyetik müdahaleyi önleyecek şekilde, üzerinde bilgisayar verilerinin kayıtlı olduğu fiziksel ortamın, paketlenmesi, mühürlenmesi, delil zinciri oluşturulması, geçici olarak

[85] ibid 48, 64, 233
[86] Değirmenci (n 1) 374
[87] Sean Goldstein, 'Two Key Differences Between Digital Forensic Imaging And Digital Forensic Clone And How They Can Affect Your Legal Case' (Digital Forensics, 2019) <https://capsicumgroup.com/2-key-differences-between-digital-forensic-imaging-and-digital-forensic-clone-and-how-they-can-affect-your-legal-case/#:~:text=Broadly speaking%2C forensic backups are,data is an unaltered state.> Erişim Tarihi 24 Kasım 2020
[88] Yar. 16 CD, E. 2015/2056, K. 2017/5023, 21.09.2017; Yar. 16. CD, E. 2015/4672, K. 2016/2330, 24.04.2016
[89] Değirmenci (n 1) 312

mahallinden alınması, adli bilişim işlemlerinin yapılacağı ortama götürülmesi faaliyetler olarak tanımlayabiliriz.

El koyma, işlenmiş suç üzerindeki maddi gerçeği ortaya çıkarmak için yürütülen yargılamada gerekli delilleri elde etmek veya yargılama sonunda müsadere edilmesi gereken eşya veya kazancı emniyet altına almak üzere gerçekleştirilen ceza muhakemesi işlemidir[90]. El koymada genel olarak amaç yargılamanın sağlıklı bir şekilde yürütülmesini temin etmek üzere delilleri elde etmek ve yargılama sonuna kadar geçici olarak muhafaza etmektir[91]. Bilgisayarlara el koyma tedbiri, genel el koyma tedbirinden çeşitli farklılıklar göstermektedir.

Bilgisayar verilerinde arama ikincillik ilkesi gereği, başka surette delil elde edilememesi halinde ikinci basamakta başvurulabilecek bir tedbirdir[92]. *Bilgisayarlara el koyma* tedbiri ise bilgisayar verilerinde aramaya olanak sağlamak üzere, adli kopya alınamadığı yani bilgisayar verilerine el konulamadığı hallerde, üçüncü basamakta başvurabilmek üzere düzenlenmiş bir tedbirdir.

Bilgisayar verilerinde arama ve el koyma tedbirlerinde asıl olan mahallinde kopyalama tedbirinin yerine getirilmesidir. Adli kopya alınması işleminin süresi, adli bilişim uzmanınca kontrol edilemeyecek birçok faktöre bağlı olarak değişmektedir. Bu faktörler, diskteki biçimlendirme türü, diskin dönme hızı, veri yoğunluğu, veri hacmi, sürücü arabirimi, sürücü yapısı, diskin sağlıklı olup olmaması, adli kopyası alınması gereken materyal sayısı ile kullanılan yazılım ve donanım gibi hususlardır. Genel uygulama, adli kopyalamaya özel olarak üretilmiş bir cihaz kullanılması ve her şeyin sağlıklı çalışması durumunda, adli kopyayı oluşturmak için dakikada 4-5 GB verinin işleme alınması şeklinde olmaktadır. Diğer bir ifade ile 320 GB'lık bir sabit diskin adli kopyasının alınması yaklaşık 70-80 dakika süreceği anlamına gelmektedir. 1 terabyte sabit diskin adli kopyasının alınması yaklaşık 3,5 ila 4,5 saat sürecektir. Bunlar sadece adli kopya alınması için gereken zamanlardır. Adli kopya alınması sürecinin hemen ardından, toplanan sayısal delillerin bütünlüğünü sağlamak için bir doğrulama işlemi gerçekleştirilmelidir. Bu işlem de kabaca adli kopya alınması aşaması kadar uzun sürmektedir ve peşi sırasında gerçekleştirilmesi gerekir[93].

[90] Gökcen and others (n 56) 461
[91] Nur Centel ve Hamide Zafer, Ceza Muhakemesi Hukuku (4. Baskı, Beta Yayınları 2006) 344
[92] Feridun Yenisey ve Ayşe Nuhoğlu, Ceza Muhakemesi Hukuku (7. Baskı, Seçkin Yayınları 2019) 426; Başlar (n 68) 164
[93] 'How Long Does A Forensic Exam Take?' (Computer Evidence Recovery, 2020) 1 <https://www.computerpi.com/resources/how-long-does-a-forensic-exam-take/> Erişim Tarihi 27 Kasım 2020

Bilgisayar verilerinde arama ve el koyma tedbirinde kural mahallinde adli kopya alınmasıdır ancak bu her zaman mümkün olmayabilir. Böyle durumlarda veri barındıran cihazların belli bir yere nakledilerek adli kopyasının alınması mümkündür[94]. Bu işlem, adli bilişim uzmanlarınca, uygun şartlarda, veri bütünlüğü, doğruluğu ve güvenilirliği hakkında şüphe oluşmasına imkân vermeyecek şekilde laboratuvara götürülerek yerine getirilmelidir.

Amerika Birleşik Devletleri'nde çeşitli bölge ve temyiz mahkemeleri, bilgisayarlardan mahallinde sayısal delil elde edilmesinin çok uzun zaman alacağını belirtilmektedir. Mahkemelere göre bilgisayarlarda arama ve el koymayı yürütmek için bu kadar zaman ayırmak, yalnızca polis kaynaklarına önemli ve haksız bir yük yüklemekle kalmayacak, aynı zamanda aramayı, temel haklara daha müdahaleci hale getirecektir. Arama ve el koyma sürerken şüphelinin binasında polisin bulunması gerekecektir ve bu durum şüphelinin evine veya işine erişimini zorunlu olarak engelleyecektir. Arama saatler veya günler sürerse, temel haklara müdahale tüm bu süre boyunca devam edecektir Mahkemelere göre, dördüncü değişikliğin, polis aramalarını olabildiğince kısa ve müdahaleci olmayan bir hale getirmeyi hedefleyen değerlerinden ödün vermek anlamına gelecektir[95].

Nitekim arama ve el koymayı düzenleyen kurallarda 2009 yılında yapılan değişiklikle bilgisayarlara el konularak mahalli dışında (off-site) bilgisayar verilerinin adli kopyasının alınması olanaklı hale getirilmiştir. Bilgisayarlar ve diğer elektronik depolama ortamları çok yoğun ve büyük miktarda bilgiler içermektedir. Arama emrini yerine getiren görevlinin aranılan yerde ve arama kararının yürütülmesi sırasında tüm bilgileri gözden geçirmesi genellikle pratik görülmemektedir. Bu değişiklikle, iki adımlı bir metoda ihtiyaç olduğu tespit edilmektedir. Bu hüküm, geleneksel arama ve el koyma sürecinin tersine, ESI için *önce el koyma, sonra arama* şeklindeki iki adımlı kuralı düzenlemektedir. Görevliler önce tüm depolama ortamına el koyacak veya kopyalayacaktır. Daha sonra elektronik ortamda depolanan bilgilerin arama emri kapsamında olup olmadığını belirlemek için inceleyecektir. Madde metninden, önce bilgisayarlara el konulabileceği sonra mahalli dışına adli kopya alınabileceği açıkça anlaşılmaktadır[96].

CMK'nın 134/2. maddesine göre bilgisayarlara el koyma tedbirine, üç durumdan birinin varlığı halinde başvurulabilmektedir. Buna göre, bilişim sistemlerinde şifre bulunması ve şifrenin çözülememesinden dolayı girilememesi halinde şifresi bulunan cihazlar hakkında el

[94] Değirmenci (n 1) 366
[95] United States v Hill, 322 F Supp 2d 1081, 2004; United States v Hill, 459 F 3d 966, 2006 1; United States v Gray, 78 F Supp 2d 524 (ED Va), 1999
[96] Rule 41: Search and Seizure m. 41-e-2-B

koyma tedbiri uygulanabilecektir. Bir diğer durum olarak, gizlenmiş bilgilere ulaşılamaması halinde ilgili aygıtlara el koyma yapılabilecektir. Son olarak işlemin uzun sürecek olması halinde bilgisayar verilerinde aramaya tabi tüm araç ve gereçlere el konulabilecektir[97].

Bilgisayarlara, bilgisayar kütüklerine, araç ve gereçlere el koyma tedbirinde, malvarlığı değerlerinden ziyade içerdikleri verilerin kıymeti daha önemlidir. Bu cihazlara çok pahalı oldukları için değil, içlerinde barındırdıkları veriler nedeniyle el konulmaktadır. Kanun koyucu, kişisel verilerin korunması hakkına müdahale edilmesini yoğun bir ihlal olarak değerlendirerek, bilgisayarlarda arama ve el koyma tedbirini daha ağır şartlara bağlamak istemiştir[98].

CMK'nın 134. maddesinde bilgisayarlara ve verilere el koyma tedbirinde somut ve soyut olmak üzere ikili bir ayrıma gidilmiştir. Bilgisayarlara el koyma tedbiri sadece cihazlar yani veri barındıran fiziksel ortamlar bakımından düzenlenmiştir Veriler ile verilere erişmek için kullanılan programlar bakımından kopyalama tedbiri ayrıca düzenlenmiştir. Maddenin 2. fıkrasında el koymaya tabi unsurlar sayılırken, yasa koyucu tarafında veri barındıran fiziksel ortamlar olarak kabul edilen somut araç ve gereçler zikredilmiştir. Maddenin 3. fıkrasında bu araç ve gereçlerin neler olduğuna ilişkin açıklık getirilmiş ve el konulanlar olarak bilgisayarlar ile bilgisayar kütükleri zikredilmiş ancak soyut verilerden teşekkül etmiş olan bilgisayar programları açıkça kapsam dışında bırakılmıştır. Somut cihaz, araç ve gereçlere el koyma, soyut verilere el koymayı yani adli kopya almayı yerine getirmeye yönelik bir tedbir olarak düzenlenmiştir.

Bilgisayarlara, bilgisayar kütüklerine, araç ve gereçlere el koymada genel el koymaya ilişkin hükümler uygulanacaktır. Bununla beraber bilişim sistemlerine özgü hususlar öncelikle dikkate alınmalıdır[99]. Örneğin genel el koymada, önce mahalde veya kişi üzerinde arama yapılmakta, arama sonucunda elde edilen delil niteliği taşıyan eşyaya el konulmaktadır. Ancak bilgisayarlar ve verileri bakımından önce verilere el koyma, kanuna belirtilen koşullar çerçevesinde mahallinde verilere el koymanın mümkün olmaması halinde, bilgisayarlara, bilgisayar kütüklerine, araç ve gereçlere el koyma, sonra veriler üzerinde arama ve analiz yapma şeklinde sıralanarak uygulanmaktadır. Bilgisayar ve verilere el koyma, verilerde aramadan önce yapılan bir uygulamadır.

[97] 5271 Sayılı Ceza Muhakemesi Kanunu m. 134/2
[98] Değirmenci (n 1) 367
[99] ibid 370

Maddenin ikinci fıkrasına göre şifrenin çözümünün yapılması ve gerekli adli kopyaların alınması halinde el konulan cihazlar, araç ve gereçler derhal ilgilisine iade edilmelidir[100]. Zira adli kopya alınmak suretiyle verile el koyma gerçekleşmiştir. Bundan sonraki adli bilişim çalışmaları adli kopya üzerinden yapılacaktır. Her türlü veri kurtarma, silinen verileri geri getirme, arama ve analiz çalışmaları için adli kopya yeterlidir. Bu işlemler çok uzun zaman alabilmektedir. Adli kopya alınması ile verilerin bütünlüğü, doğruluğu ve güvenilirliği de sağlanmaktadır. Şüpheli şahsın özel hayatına, örneğin ticari faaliyetlerine daha fazla müdahale edilmemesi için bilgisayarların, bilgisayar kütüklerinin, araç ve gereçlerin adli kopyasının alınmasını müteakip, derhal iade edilmesi gerektiği düzenlenmiştir[101].

SONUÇ

Ceza muhakemesinin amacı, hukuka uygun delillerle maddi gerçeğe ulaşıp adaletli bir karar vermektir. Maddi gerçek, ceza muhakemesinde uyuşmazlık konusu olayın ne şekilde gerçekleştiğinin deliller vasıtasıyla ortaya konmuş halini ifade etmektedir. Hukuka uygun delil elde etmek, maddi gerçeğe ulaşmak ve muhakemenin yapılmasını mümkün kılmak için, ceza muhakemesinde karar verme yetkisine sahip makamlar, koruma tedbirlerine başvurmaktadırlar. Bu koruma tedbirlerinden bir tanesi de bilgisayar verilerinde arama, kopyalama ve el koyma tedbiridir.

Bilgisayar verilerinde arama ve el koyma tedbirinin ne olduğu, hukuki niteliği, kapsamı ve etkileri incelenmiştir. Bilgisayarlarda, bilgisayar programlarında, bilgisayar kütüklerinde arama ve el koyma, CMK'nın 134. maddesiyle düzenlenen, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı halinde, geçici olarak, hükümden önce temel insan haklarına oranlılık içerisinde müdahale eden, yetkili merciin kararıyla veya emriyle uygulanabilen bir koruma tedbiridir. Bilgisayar verilerinde arama, kopyalama ve el koymanın; yasal dayanağının olması, belirli şüphe yoğunluğunun olması, hükümden önce bir hakkı sınırlaması, geçici olması, gecikmesinde tehlike olması, oranlılık içinde uygulanma zorunluluğunun bulunması, bir karara dayanması gibi koruma tedbirlerinin genel özelliklerini taşımaktadır.

Bilgisayar verilerinde arama ve el koyma tedbiri CMK'nın 134. maddesinde düzenlenmiştir. Bilgisayar verilerinde arama ve el koyma tedbiri, genel arama ve el koyma tedbirinin özel düzenlenmiş şeklidir. Bilgisayar verilerinde arama yönü itibariyle arama tedbirinin, bilgisayar verilerini kopyalama ve bilişim sistemlerine el koyma yönü itibariyle el

[100] CMK m. 134/2

[101] Değirmenci (n 1) 373; Bahri Öztürk and others, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku (13. Baskı, Seçkin Yayınları 2019) 526; Gökcen and others (n 56) 480

koyma tedbirinin özel nitelikli halidir. Bu nedenle, maddede düzenlenmeyen hususlarda genel arama ve el koyma hükümleri uygulanacaktır.

Mukayeseli hukukta ve ceza muhakemesi hukukumuzda bilgisayar verilerinde arama ve el koyma konusunda yapılan düzenlemeler ve kullanılan terminoloji karşılaştırılarak, terimlerin klasik anlamları yanı sıra ifade edilen yeni manalar belirtilerek tasnif edilmiştir. Ceza muhakemesi hukukumuzda yer verilen tedbirler kategorik olarak ele alınarak karşılaştırılmıştır. Buna göre;

Arama, erişim, inceleme terimlerinin birbirinin yerine geçecek şekilde anlamlandırılmakta ve *arama* terimi altında gruplandırılmaktadır. Arama teriminin, basit bir şekilde bilgisayarda anahtar kelime aramasından çok daha geniş bir anlamı bulunmaktadır ve bir süreci tanımlamaktadır. Bu süreç bilgisayar verilerinde arama, tüm adli bilişim süreçleri ve raporlamayı da içine almaktadır.

Kopyalama, yedekleme, verilere el koyma terimlerinin aynı anlamı ifade edecek şekilde kullanılmaktadır. Kopyalama tedbiri bir çeşit verilere el koymadır. Arama tedbirinde olduğu gibi kopyalama da tek bir işlemi değil bir süreci tanımlamaktadır. Bu süreç, verileri el koyma anı itibariyle dondurma, veri bütünlüğünü ve güvenilirliğini sağlama, verilere ilişkin delil zincirini oluşturma ve koruma, ilk elde edildiği andan yargılamanın sonuna kadar geçen sürede el konulan verilerin değişmeden, bozulmadan, silinmeden, kaybolmadan kalmasını sağlama, verilerde soruşturmaya ilişkin arama, analiz, raporlama yapılmasına olanak sağlamak üzere, mahkemelerce verinin aslı olarak kabul edilecek şekilde, adli bilişime özel biçimde verileri kopyalama, veri bütünlüğü (özet) değeri hesaplama, veri bütünlüğünü doğrulama faaliyetlerini içermektedir.

CMK'da yer verilmeyen ve fakat *Avrupa Konseyi Siber Suçlar Sözleşmesinde* yer alan tedbirler de bulunmaktadır. *Verilerin tutulması (saklanması)* tedbirine, *5651 Sayılı Kanunda* yer verilmiştir. CMK'da yer verilmeyen tedbirlerden, *verileri erişilmez kılma ve verileri kaldırma* tedbirlerine ceza muhakemesi hukukumuzda da ihtiyaç bulunduğu değerlendirilmektedir. Verilerin erişilemez hale getirilmesi, verilerin kriptolanmasını veya herhangi birinin bu verilere erişiminin teknolojik olarak engellenmesini ifade etmektedir. Veriler bulundukları ortamda varlığını sürdürmeye devam etmekte ancak adli yetkililer dışında hiç kimse tarafından erişilememektedir. Verileri kaldırma ifadesi ise bulundukları yerden başka

bir yere nakledilmesini örneğin adli kopya alınması suretiyle adli makamların elektronik ortamlarına aktarılmasını ifade etmektedir[102].

CMK'da yer verilmeyen bir diğer tedbir ise *çevrimiçi arama veya uzaktan arama,* yürütülmekte olan bir yargılamada, yetkili merciin kararı ile soruşturma makamlarının, bu amaç için üretilmiş yazılımlar marifetiyle, internet kullanımı sırasında, şüphelinin bilgisayar veya internete bağlı cihazlarının sabit diskine ve verilerine gizlice ve sahibinin veya kullanıcısının izni olmadan erişerek sayısal delil elde etme faaliyetidir[103]. Ceza muhakemesi hukukumuzda uzaktan arama tedbiri ile ilgili bir düzenleme ve uygulama alanı bulunmadığı değerlendirilmektedir[104]. Kolluk kuvvetlerinin veya üçüncü şahısların bu yöntemi kullanarak elde ettikleri verilerin sayısal delil olarak kullanılamayacağı, hukuka uygunluk sebebi bulunmadığından, TCK'nın 243. ve 244. maddelerinde düzenlenen bilişim sistemine hukuka aykırı olarak girme ve bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme suçlarının işlenmiş olacağı düşüncesindeyiz.

CMK'da yer verilmeyen bir diğer tedbir olarak *bulutta aramanın*, arama kararında belirtilen yerleşke içerisinde bulunan *özel bulut bilişim* bakımından sınırlı olarak genişletilebileceğini[105] ve uygulanabileceğini değerlendirmekteyiz. Bununla beraber, yurt içinde bulunan farklı adreslerdeki kamu ve özel bulut bilişim hizmetleri için ayrı arama ve el koyma kararları ile yerinde uygulama yapılabilecektir[106]. Yurt dışında bulunan bulut bilişim hizmetleri içinse, uluslararası adli yardımlaşma hükümlerine göre ilgili ülkeden talepte bulunulabileceğini değerlendirmekteyiz.

[102] Explanatory Report to the Convention on Cybercrime Prg. 198
[103] Tanrıkulu (n 11) 314; Christoph Keller ve Frank Braun, Telekommunikationsüberwachung und andere verdeckte Ermittlungsmaßnahmen (Richard Boorberg Verlag 2019); Jiuan-Yih Wu, 'Die Online-Durchsuchung und der Suchbegriff im Internet' içinde Hans-Jürgen Lange ve Astrid Bötticher (ed), Cyber-Sicherheit (Springer VS 2015) 281; Ahmed Ghappour, 'Searching places unknown: Law enforcement jurisdiction on the dark web' (2017) 69 Stanford Law Review 1197, 1079
[104] Özen ve Özocak (n 81) 51; Ünal (n 23) 111; Başlar (n 68) 195; Değirmenci (n 1) 365-366
[105] Başlar (n 68) 195
[106] Değirmenci (n 1) 420

KAYNAKÇA

Aldemir H, Adli - Önleme Arama ve Elkoyma (1. Baskı, Adalet Yayınları 2018)

'American Heritage Dictionary Entry: Backup' (The American Heritage Dictionary of the English Language, 2020) <https://www.ahdictionary.com/word/search.html?q=backup> Erişim tarihi 24 Kasım 2020

Årnes A (ed), Digital Forensics (John Wiley & Sons, Inc 2018)

Ashouri A, Bowers C ve Warden C, "An Overview Of The Use Of Digital Evidence In International Criminal Courts" (International Human Rights Law Clinic, Samuelson Law, Technology & Public Policy Clinic at the University of California, Berkeley, School of Law 2013) <https://www.law.berkeley.edu/files/HRC/Scholarly_articles_Salzburg_2013.pdf> Erişim Tarihi 12 Mart 2019

Başlar Y, Ceza Yargılamasında Elektronik Delil (Yetkin Yayınları 2016)

Baştürk İ, "Bilgisayar Sistemleri İle Verilerinde Arama Kopyalama ve Elkoyma" (2010) 2 Fasikül, İstanbul Kültür Üniversitesi CEHAMER Aylık Hukuk Dergisi 23

Berber LK, Adli Bilişim (1. Baskı, Yetkin Yayınları 2004)

Bostancı Ü ve Benzer R, "Search , Copy and Seizure On The Computers In The Turkish Legal System. Türk Hukuk Sisteminde Bilgisayarlarda Arama, Kopyalama ve El Koyma" (2015) 12 International Journal of Human Sciences

Brenner SW, "Seizure" (CYB3RCRIM3 Observations on Technology, Law and Lawlessness, 2006) <http://cyb3rcrim3.blogspot.com/2006/02/seizure.html> Erişim tarihi 06 Kasım 2020

——, 'Copying as a Seizure (Again)' (CYB3RCRIM3 Observations on Technology, Law and Lawlessness, 2009) <http://cyb3rcrim3.blogspot.com/2009/07/copying-as-seizure-again.html> Erişim tarihi 05 Kasım 2020

Çakır H ve Kılıç MS, "The Keyword Search Method and It's Importance in Computer Forensics / Adli Bilişimde Anahtar Kelime Araması Metodu ve Önemi" (2016) 13 Journal of Human Sciences 2368

Casey E, Digital Evidence And Computer Crime (2. Baskı, Academic Press 2004)

—— (ed), Handbook Of Digital Forensics And Investigation (2010)

——, Digital Evidance And Computer Crime (3. Baskı, Elsevier 2011)

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

Centel N ve Zafer H, Ceza Muhakemesi Hukuku (4. Baskı, Beta Yayınları 2006)

——, Ceza Muhakemesi Hukuku, Yenilenmiş ve Gözden Geçirilmiş (10. Baskı, Beta Yayınları 2013)

Çolak H ve Taşkın M, Ceza Muhakemesi Kanunu Şerhi (Seçkin Yayınları 2007)

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

Ghappour A, "Searching places unknown: Law enforcement jurisdiction on the dark web" (2017) 69 Stanford Law Review 1197

Gladyshev P, "Formalising Event Reconstruction in Digital Investigations" (PHD Dissertation, University College Dublin, Faculty of Science 2004)

Gökcen A and others, Ceza Muhakemesi Hukuku (4. Baskı, Adalet Yayınları 2020)

Goldstein S, "Two Key Differences Between Digital Forensic Imaging And Digital Forensic Clone And How They Can Affect Your Legal Case ." (Digital Forensics, 2019) <https://capsicumgroup.com/2-key-differences-between-digital-forensic-imaging-and-digital-forensic-clone-and-how-they-can-affect-your-legal-case/#:~:text=Broadly speaking%2C forensic backups are,data is an unaltered state.> Erişim tarihi 24 Kasım 2020

'How Long Does A Forensic Exam Take?' (Computer Evidence Recovery, 2020) 1 <https://www.computerpi.com/resources/how-long-does-a-forensic-exam-take/> Erişim tarihi 27 Kasım 2020

Jones N and others, 'Electronic Evidence Guide a Basic Guide for Police Officers, Prosecutors and Judges' (2014)

Kävrestad J, Fundamentals of Digital Forensics_ theory, methods, and real-life applications-Springer (Springer US 2020)

Kaya MB, 'Hukuki Açıdan Bilişim Suçları, Siber Güvenlik ve Adli Bilişim' içinde Şeref Sağıroğlu ve Mustafa Şenol (ed), Siber Güvenlik ve Savunma Problemler ve Çözümler (1. Baskı, Grafiker Yayınları 2019)

Keller C ve Braun F, Telekommunikationsüberwachung und andere verdeckte

Ermittlungsmaßnahmen (Richard Boorberg Verlag 2019)

Kerr OS, "Searches and Seizures In A Digital World" [2005] Harward Law Review 532

——, "Fourth Amendment Seizures of Computer Data" (2010) 119 The Yale Law Journal 700

Kiçeci H, "Bilgisayar Medyalarına İlk Müdahale" içinde Hüseyin Çakır ve Mehmet Serkan Kılıç (ed), Adli Bilişim ve Elektronik Deliller2 (Seçkin Yayınları 2014)

Kızılyar M, "Ceza Yargılamasında Dijital Verilerin Delil Değeri" (2014) 50 Adalet Dergisi 72

National Institute of Standards and Technology, Digital Data Acquisition Tool Specification (NIST 2004)

Nelson B, Phillips A ve Steuart C, Guide to Computer Forensics and Investigations: Processing Digital Evidence Fifth Edition (Cengage Learning 2016)

Nelson S, Pro Data Backup and Recovery (Springer US 2011)

Newman RC, Computer Forensics Evidence Collection and Management, c 1 (Auerbach Publications 2007)

Özbek VÖ, Doğan K ve Bacaksız P, Ceza Muhakemesi Hukuku (12. Baskı, Seçkin Yayınları 2019)

Özen M ve Baştürk İ, Temel Hak ve Özgürlükler Bağlamında Bilişim - İnternet ve Ceza Hukuku (1. Baskı, Adalet Yayınları 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 43

Öztürk B and others, Nazari ve Uygulamalı Ceza Muhakemesi Hukuku (13. Baskı, Seçkin Yayınları 2019)

Saudi M, "An Overview of Disk Imaging Tool in Computer Forensics" (Information Security Reading Room, 2001) <https://www.sans.org/reading-room/whitepapers/incident/overview-disk-imaging-tool-computer-forensics-643> Erişim tarihi 16 Kasım 2020

Sırma Ö, "Güncel Olaylar Çerçevesinde 5271 Sayılı Ceza Muhakemesi Kanununda Arama" (2009) 34 Terazi Hukuk Dergisi

Stanfield AR, "The Authentication of Electronic Evidence" (PHD Dissertation, Queensland University of Technology, Faculty of Law 2016)

Şirikçi AS ve Cantürk N, "Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi" (2012) 5 Bilişim Teknolojileri Dergisi 29

Tanrıkulu C, Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma (1. Baskı, Adalet Yayınları 2014)

The Sedona Conference Working Group on Electronic Document Retention & Production, "The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production Second Edition" (2007)

Topaloğlu N, "Bilgisayar Mimarisi" içinde Hüseyin Çakır ve Mehmet Serkan Kılıç (ed), Adli Bilişim ve Elektronik Deliller (1. Baskı, Seçkin Yayınları 2014)

Ünal OG, "Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma" (Yüksek Lisans Tezi, Gazi Üniversitesi, Sosyal Bilimler Ensitüsü 2011)

Wu J-Y, "Die Online-Durchsuchung und der Suchbegriff im Internet" içinde Hans-Jürgen Lange ve Astrid Bötticher (ed), Cyber-Sicherheit (Springer VS 2015)

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

Yenisey F ve Nuhoğlu A, Ceza Muhakemesi Hukuku (7. Baskı, Seçkin Yayınları 2019)

Yetim S, Ceza Muhakemesi Kapsamında Sosyal Medyadan Elektronik Delil Toplama ve Değerlendirme (1. Baskı, Seçkin Yayınları 2016)