T.C.

BAHÇEŞEHİR ÜNİVERSİTESİ

TÜRK CEZA MUHAKEMESİ KANUNUNDAKİ BİLİŞİM SİSTEMİNDE ARAMA, KOPYALAMA VE ELKOYMA TEDBİRİ

YÜKSEK LİSANS TEZİ

İREM COŞKUNOĞLU

İSTANBUL, 2021

T.C.

BAHÇEŞEHİR ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

KAMU HUKUKU ANABİLİM DALI

TÜRK CEZA MUHAKEMESİ KANUNUNDAKİ BİLİŞİM SİSTEMİNDE ARAMA, KOPYALAMA VE ELKOYMA TEDBİRİ

YÜKSEK LİSANS TEZİ

İREM COŞKUNOĞLU

Tez Danışmanı

Dr. Öğr. Üyesi Güner Hande ULUTÜRK

İSTANBUL, 2021

ÖZET

TÜRK CEZA MUHAKEMESİ KANUNUNDAKİ BİLİŞİM SİSTEMİNDE ARAMA, KOPYALAMA VE ELKOYMA TEDBİRİ

İrem Coşkunoğlu

Kamu Hukuku Yüksek Lisans Programı

Tez Danışmanı: Dr. Öğr. Üyesi Güner Hande Ulutürk

Haziran 2021, 145 sayfa

Günlük yaşantımızın ayrılmaz bir parçası olan bilişim sistemleri, birçok değişik suçun işlenmesinde kullanılmakta veya suça ilişkin bilgiler bu sistemler üzerinden ortaya çıkarılabilmektedir. Bu sebeple, maddi gerçeğin ortaya çıkarılmasında, klasik delil anlayışından farklı olarak, ispat vasıtası olabilecek elektronik deliller kullanılmaktadır. Bilişim sistemleri üzerinden elektronik delillerin toplanması, değerlendirilmesi ve bütünlüğünün korunmasına yönelik teknik kısım, adlî bilişim uzmanlık alanı kapsamındadır. Bu bağlamda, çalışma konumuz olan CMK m. 134, "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" başlığı altında, bilişim sistemlerinden elektronik delil elde edilmesi sürecinin hukuki rejimini düzenlemektedir. Fakat bu hükmün, sürekli gelişen teknoloji göz önünde tutulduğunda, gerek kaleme alınışına gerek uygulanışına ilişkin güncelleştirilmesi lüzum görülen bazı hususlar bulunmaktadır. Biz de tez çalışmamız kapsamında bu hususlara yer vermeye çalıştık.

Anahtar Kelimeler: Bilişim sistemi, arama, kopyalama, elkoyma.

ABSTRACT

IN THE TURKİSH CRİMİNAL PROCEDURES LAW INFORMATİON TECHNOLOGY SYSTEM

İrem Coşkunoğlu

Public Law Master Degree Program

Thesis Advisor: Lecturer Dr. Güner Hande Ulutürk

June 2021, 145 pages

Information systems, which are an inseparable part of our everyday lives, are being used for the committal of various crimes and evidence in relation to crimes are uncovered through the use of such systems. Therefore, electronic evidence that can constitute means of proof, is used to uncover material facts, unlike the traditional concept of evidence. The technical aspects aimed at the collection, evaluation and the preservation of the integrity of electronic evidence are the domain of electronic forensics. Within this context, Article 134 of the Criminal Procedures Act, which is the subject of our interest, regulates the legal framework for the process of obtaining electronic evidence from information systems under the heading “the search, copying and seizure in computers, computer programs and computer records”. However, in view of the constantly evolving technology, there are aspects that need to be updated both in its wording as well as its application. We have endeavoured to cover these aspects in our thesis.

Key Words: Information Technology (IT), search, copy, seizure

İÇİNDEKİLER

KISALTMALAR

ABD : Amerika Birleşik Devletleri

AİHM : Avrupa İnsan Hakları Mahkemesi

AİHS : Avrupa İnsan Hakları Sözleşmesi

AKSSS : Avrupa Konseyi Siber Suç Sözleşmesi

AÖAY : Adli ve Önleme AramalarıYönetmeliği

Bkz. /bkz. : Bakınız

C. : Cilt

Çev. : Çeviren

CMK : Ceza Muhakemesi Kanunu

Dr. : Doktor

E. : Esas

E.T. : Erişim Tarihi

K. : Karar

m. : Madde

No : Numara

Öğr. : Öğretim

PVSK : Polis Vazife ve Salahiyet Kanunu

s. : Sayfa

S. : Sayı

SBE : Sosyal Bilimler Enstitüsü

TBB : Türkiye Barolar Birliği

TBMM : Türkiye Büyük Millet Meclisi

TCK : Türk Ceza Kanunu

Y. : Yıl

Yarg. : Yargıtay

TÜRK CEZA MUHAKEMESİ KANUNUNDAKİ BİLİŞİM SİSTEMİNDE ARAMA, KOPYALAMA VE ELKOYMA TEDBİRİ

I. GİRİŞ

Gelişen teknolojiyle birlikte, bilgisayar ve benzeri araçların kullanımı hızla artarak hayatımızın her evresine dâhil olmuştur. Günlük yaşantımızda artık alışverişlerimizi sitelerden yapabilmekte, bankacılık işlemlerimizi tek tuşla halledebilmekteyiz. Belgelerimizi, fotoğraflarımızı bu aygıtlarda saklayabilmekte ve çeşitli uygulama programlarıyla istenildiği zaman kişilerle karşılıklı iletişim kurabilmekteyiz. Kişisel ve ekonomik pek çok faaliyeti sanal ortam aracılığı ile gerçekleştirmekteyiz. Birçok kimse günlük programlarını bilişim sistemleri üzerinden yürütmektedir. Habercilikten iletişime ve sosyal hayatımızdan iş yaşantımıza kadar dijitalleştiğimiz bu dönemde, bilişim sistemleri; hayatımızı kolaylaştırıp pratikleştirmesine karşın, ceza hukuku açısından bazı değerlerin ihlal edilmesinde ve bazı suçların işlenmesinde rol oynayabilmektedir. Zira, internet kullanımı ile fiili olarak gerçekleştirilmeyen ancak sanal ortamda işlenen suç sayısı azımsanamayacak düzeydedir. Suç olgusunun teknolojiyi bu şekilde araç olarak kullanması sonucunda, suç işleme şekilleri sürekli değişim göstermektedir. Bu doğrultuda, suçla mücadele yöntemleri de, gelişen teknolojiye uyum sağlayarak değişmektedir.

Çeşitli suçlara ilişkin delillerin bilişim sistemleri içerisinde bulunması sebebiyle, bu suçları aydınlatılabilmek ve suçlarla mücadele edebilmek adına, klasik delil anlayışından farklı olarak ispat aracı olabilecek elektronik deliller kullanılmaya başlanmıştır. Bu elektronik delillerin bilgisayar ve benzeri diğer elektronik cihazlar içerisinden elde edilmesi ihtiyacını karşılamak üzere, delil bulma yöntemlerinden olan adli bilişim ortaya çıkmıştır.

Günümüzde, adli bilişim yöntemi ile bilişim sistemleri üzerinden elektronik delillerin keşfedilmesi hususu, maddi gerçeğin ortaya çıkarılması adına önemli bir konu haline gelmiştir. Fiziksel delillerin elde edilmesi amacıyla başvurulan genel arama ve elkoyma tedbirleri, özellikle bilişim suçları söz konusu olduğunda delil elde edilmesinde yeterli

değildir. Bunun sebebi ise, elektronik delillerin niteliği ve elde edilmesi yönteminin farklı olmasıdır. Dolayısıyla bilişim sistemi üzerinden adli bilişim kurallarına uygun şekilde, elektronik delillerin elde edilmesini kapsayan düzenlemeye gereksinim duyulmaktadır. Bu bağlamda, bir koruma tedbiri olan 5271 sayılı Ceza Muhakemesi Kanunu'nun 134. maddesinde, genel arama ve elkoyma tedbirlerinin özel bir şekli olarak bilişim sistemleri üzerinden delil elde edilmesini hususu düzenlenmiştir.

Özel hayatın gizliliği, mülkiyet hakkı gibi birçok temel hak ve özgürlükler ile yakından ilişkili olan CMK m. 134 hükmünde yer alan tedbirlerin, sürekli gelişen teknolojiye paralel olarak gözden geçirilmesi gerekmektedir. Bu sebeple tez çalışmamız kapsamında; gerek mevzuata gerek uygulamaya ilişkin güncelleştirilmesi ve değiştirilmesi gereken hususlara yer vermeye çalıştık.

Çalışmamızın I. bölümünde ilk olarak konunun daha iyi anlaşılması için temel kavramlar açıklanmıştır. Sonrasında; ceza muhakemesindeki delil kavramı ve özelliklerine yer vermekle birlikte, elektronik delilin; ne olduğu, teknik yapısı, özellikleri, bulunduğu ortamlar, delil tasnifindeki yeri, taşıması gereken nitelikler ve geçerliliğine ilişkin hususlar açıklanmıştır. Son olarak ise, bilişim sistemleri üzerinden delil elde etme yöntemi olarak adli bilişim sürecine yer verilmiştir. Burada verilerin elde edilmesi yönteminde arama çeşitleri açıklanmış olmakla birlikte; hash değerinin alınması, imaj alınması, verilerin muhafazası, incelenmesi, raporlanması ve elektronik delillerin bütünlüğünün sağlanması gibi hususlar üzerinde durulmuştur. II. bölümde, öncelikle genel olarak koruma tedbirlerinin koşulları açıklanmıştır. Sonrasında ise, CMK m. 134 hükmünün; Türk hukukundaki gelişimi, Avrupa Konseyi Siber Suç Sözleşmesi bakımından değerlendirilmesi, genel arama ve elkoyma tedbiri ile ilişkisi, iletişim tespiti yöntemi ile ilişkisi, hukuki rejimini düzenleyen yasal mevzuata ve son olarak da, tedbirin muhatabı olan kişilere ilişkin açıklamalarda bulunulurken, ceza muhakemesinin hangi aşamasında başvurulabileceğine ilişkin öğretideki görüşlerden yararlanarak değerlendirmelerde bulunulmuştur.

III. bölümde ise ilk olarak, tedbirlerin konusu olan araçlar incelenmiştir. Bu araçlar açıklanırken, CMK' nun 134. maddesinde sayılan araçlar, tedbirlere ilişkin ilgili Yönetmelik olan Adli ve Önleme Aramaları Yönetmeliği(AÖAY)'nin 17. maddesinde sayılan araçlar ile CMK'nun 134. ve AÖAY'nin 17. maddesinde yer almayan, ancak

gündelik hayatta tedbirlerin konusu olabilecek araçlar olarak, ayrı başlıklarda ele alınmıştır. Sonrasında, ise CMK m. 134 hükmüne başvurulması için gerekli olan koşullar irdelenmiştir. Bu koşullar; arama, kopyalama tedbiri bakımından ve elkoyma tedbiri bakımından olacak şekilde, ayrı ayrı açıklanmıştır. Son bölüm olan IV. bölümde ise, CMK m. 134'te ki tedbirlerin uygulanmasına ilişkin bilgilere yer verilmiştir. Burada yine CMK m. 134'te yer alan tedbirlerin koşullarının açıklanmasında olduğu gibi ikili ayrımda bulunarak, önce; arama, kopyalama işleminin uygulanması, sonrasında el koyma işleminin uygulanması şeklinde izah edilmiştir. Devamında, CMK m.134 hükmünün uygulanması sonucunda bilişim sistemi üzerinden elde edilen delillerin; yok edilmesi, tesadüfen elde edilmesi hususlarına ve bu tedbirlerin uygulanması sonucunda başvurulabilecek yollar ile tazminat istemine ilişkin açıklamalarda bulunulmuştur.

II. ELEKTONİK DELİL ve ADLİ BİLİŞİM

A. TEMEL KAVRAMLAR

Çalışmamızın bu kısmında, tez konumuz olan bilişim sistemlerinde arama, kopyalama ve elkoyma tedbirinin hukuki boyutu irdelenmesi amacıyla temel kavramlar açıklanmaya çalışılacaktır.

1. Bilişim ve Bilişim Alanı

Bilişim terimi önceleri bilginin erişilmesi ve saklanması gayesini taşıyan çalışmalar için kullanılmakta iken günümüzde artık bilginin işlenmesi ve yönetilmesini amaçlayan bir bilim dalı haline gelmiştir.[1] Bilişim biliminin köklerini matematik, fizik ve elektroteknik oluşturmaktadır. Bir mühendislik alanı olarak bilişim verileri aktarabilen, depolayabilen ve algoritmalar yardımıyla verileri işleyebilen matematiksel makineler tasarlamaktadır. Bu bakımdan bilişim, özellikle gerçek süreçlerin simülasyonunu olanaklı hale getirmektedir. Bilişim, bir "yardımcı bilim" olarak düşünüldüğünde ise diğer bilimlerdeki olguları soyutlaştırıp algoritmalar yardımıyla işlemesini sağlamaktadır.[2]

Bilişim kelimesinin kaynağı, Fransızca bilgi vermek kökeninden gelen "informatique" sözcüğüdür. Bu sözcük Türkçeye öncelikle "enformasyon" şeklinde çevrilerek kullanılmış ancak daha sonra Türkçe karşılık olarak bilgi kökeninden gelmekte olan "bilişim" sözcüğü kullanılmaya başlanmıştır. [3]

Bilişim kavramı doktrinde değişik şekillerde tanımlanmıştır. YENİDÜNYA/DEĞİRMENCİ'ye göre, bilişim; *"teknik, ekonomik, sosyal hukuk ve benzeri alanlardaki verinin saklanması, saklanan bu verinin otomatik olarak işlenmesi,*

[1] AKBULUT B., Bilişim Alanında Suçlar,2. Baskı, Ankara, Adalet Yayınevi, 2017. s. 13.
[2] ERDOĞAN Y., Türk Ceza Kanunu'nda Bilişim Suçları(Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları ile), İstanbul, Legal Yayıncılık, 2013, s.6; ÖZBEK V. Ö., "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245) ," Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt: 9, Özel Sayı, 2007, s. 1019-1063 s.1023.
[3] DÜLGER M. V., Bilişim Suçları ve İnternet İletişim Hukuku,7. Baskı, Ankara, Seçkin yayıncılık, Eylül 2018. s.68

organize edilmesi, değerlendirilmesi ve aktarılması ile ilgili bir bilim dalıdır.[4]" YILMAZ'a göre "*Bilişim; bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemlerdir."* [5] DÜLGER'e göre "*İnsanların teknik, ekonomik, siyasal ve toplumsal alanlardaki iletişiminde kullandığı bilginin, özellikle bilgisayar aracılığıyla düzenli ve akılcı biçimde işlenmesi, her türden düşünsel sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarda depolanması ve kullanıcıların erişimine açık bulundurulması bilimidir.*"[6] TANRIKULU, bilişim kavramının veriyle ilgili tüm iş, işlem, ortam ve süreçleri bütüncül yaklaşımla inceleyen bir bilim dalı olduğunu ifade etmektedir.[7] ERDOĞAN, bilişim kavramını sürekli yenilenen bir bilim dalı olması sebebiyle tanım yapmayı uygun bulmamakta ancak bu kavramın temel unsurlarını belirtmektedir. ERDOĞAN' a göre bilişim kavramının ortak özellikleri; verinin işlenebilmesi, saklanabilmesi ve aktarılabilmesidir.[8] ORTA ise bilişimi; "*tanımların ortak yönlerinin şu noktalarda toplandığı görülmektedir: insanların farklı alanlardaki iletişimde kullandığı ve bilginin toplanması, saklanması ve akılcı biçimde işlenmesinin gerçekleştirildiği bilimdir*." şeklinde ifade etmiştir.[9]

Bilişim, Türk Dil Kurumunun resmi sayfasında "*İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimi*." şeklinde tanımlanmıştır.[10]

Doktrinde bir görüş, bilişim teriminin bilgisayara nazaran daha kapsamlı bir sözcük olduğunu hatta bilgisayarı da kapsayan üst bir kavram olarak tasvip etmiştir.[11] Başka bir

---

[4] YENİDÜNYA A. C./DEĞİRMENCİ O., Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, İstanbul, Legal Yayıncılık, Nisan 2003. s.27.

[5] YILMAZ S., "5237 Sayılı TCK'nın 244. maddesinde düzenlenen bilişim alanındaki suçlar", TBB Dergisi, Sayı:92, 2011. s.63.

[6] DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s.70.

[7] TANRIKULU C., 2014. Ceza muhakemesi hukukunda bilişim sistemlerinde arama ve elkoyma. Ankara: Adalet Yayınevi, s.12.

[8] ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s.8.

[9] ORTA M., 2015. Bilişim suçları ve elektronik delillerin toplanması muhafazası değerlendirilmesi sunulması(Adli bilişim). Ankara: Yetkin Yayınları s.50.

[10] http://tdk.gov.tr/index.php?option=com_bilimsanat&view=bilimsanat&kategori=terim&hng=md&kelime=bili% C5%9Fim (23.03.2019)

[11] ORTA s.50; ERDAĞ, A.İ., "Bilişim Alanında Suçlar(Türk ve Alman Hukukunda)" Gazi Üniversitesi Hukuk Fakültesi Dergisi, C.XIV, 2010, S.2, s.277; Bilişim, verilerin işlenmesini yani veri işlemi ve verilerin aktarılmasını yani veri iletişimini kapsamaktadır. YENİDÜNYA/DEĞİRMENCİ, s.31.

görüş, bu hususta, bilişimi bir bilim dalı, bilgisayar ise bu bilim dalında kullanılmakta olan araçlardan yalnızca biri olarak görmesinden dolayı karşılaştırılma yapılmasını uygun görmemektedir.[12]

Bilişim alanı ise bilgileri depoladıktan sonra otomatik işleme tabi tutan sistemlerden oluşmaktadır.[13] TCK'da kullanılan bilişim alanı kavramında, hem aynı kanunda bulunan bilişim suçlarının konusunu oluşturan alanı hem de hızla gelişmekte olan teknolojiyle birlikte ortaya çıkacak olan yeni sistemler ifade edilmek istenmektedir.[14] Bu alan, bilişim faaliyetinin gerçekleştiği yer olarak da tanımlanabilir. Ayrıca söz konusu alan somut değil, soyut bir ortamı ifade etmektedir.[15]

2. Bilişim Sistemleri

"*Sistem, ortak bir amaç için birlikte çalışan birbirine bağımlı ve birlikte hareket etme yeteneğine sahip parçaların oluşturduğu bir bütündür.*"[16] Bilgisayarlar kullanılarak, oluşturulan bilgi sistemlerine ise "bilgisayar tabanlı bilgi sistemleri" veya "bilişim sistemleri" terimleri kullanılmaktadır.[17]

ORTA' ya göre bilişim sistemi, "*verilerin belli bir düzen içinde bilgisayar ortamında saklandığı ve tanımlanan bilgi gereksinmelerini karşılamak üzere dönemsel ya da talep üzerine raporlar üreten, gereken veriye kısa sürede erişim olanağı sağlayan belli bir donanım üzerinde işletilen yazılım ve veriler bütünüdür.*"[18]

5237 sayılı TCK'nın 243. maddesinin gerekçesinde "Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir." şeklinde ifade edilmiştir. *[19]*

[12] ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s.8; YENİDÜNYA/DEĞİRMENCİ, Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, ss.30-31.
[13] APAYDIN C., Bilişim Suçları ve Bilişim Ceza Hukuku, 1. Baskı, İstanbul, Acar Matbaacılık, Mart 2017, s.151.
[14] DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s.68.
[15] ÖZBEK, "Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu" s.1023.
[16] ÖZKUL D., "Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi", Sayıştay Dergisi, Sayı: 44-45, s.11-34, s.14
[17] ÖZKUL, "Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi" s.14.
[18] ORTA, s.53.
[19] ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc [25.03.2019]

Bilişim sistemi kavramından kasıt; yazıcı, modem gibi bütün çevre birimleri dâhil olmak üzere bilgisayardan beklenen tüm amaçları gerçekleştirmeye yönelik donanım ve yazılım öğelerinin bütünü olarak anlaşılmalıdır.[20]

ERDOĞAN yine bilişim kavramında olduğu gibi bilişim sistemi kavramının da teknolojinin hızla gelişmesini esas alarak mevcut gelişmelere göre yorumlanması gerektiğini belirterek, tanım yapmaktan kaçınmakta ancak bu kavrama ilişkin temel unsurları ifade etmektedir. ERDOĞAN' a göre bir sistem ancak; verileri işleyebilmesi, saklayabilmesi ve aktarabilmesi halinde bilişim sistemi olduğu kabul edilmelidir.[21] Sayılan unsurları barındıran bilişim sistemlerinin en yaygın olanı bilgisayarlardır.[22] Ancak bilgisayar dışında, bilişim sistemi olarak nitelendirilebilecek aygıtlar mevcuttur.[23] Bilgisayar veri işleyebilmekte, depolayabilmekte fakat tek başına veri iletimini gerçekleştirememekte ve bu yönüyle bilişim sisteminden ayrılmaktadır.[24] Teknolojik gelişmeler sonucunda maddi olaya ilişkin veriler yalnızca bilgisayar üzerinden değil, diğer bilişim araçlar üzerinden de elde edilmektedir.[25] Bunlara ilaveten, bilgi teknolojileri kavramının da açıklanmasında fayda bulunmaktadır. Bilgi teknolojileri, "*bilginin toplanmasında, işlenmesinde, depolanmasında, ağ aracılığıyla bir yerden başka bir yere iletilmesinde ve kullanıcılara sunulmasında yararlanılan iletişim ve bilgisayar teknolojilerini de kapsayan bütün teknolojilere* denilmektedir. [26]"

Çalışmamızda, hem bilgisayar terimine nazaran daha kapsayıcı üst bir kavram olması sebebiyle hem de TCK'daki kullanım şeklini de dikkate alarak, bilişim sistemi kavramı kullanılacaktır.

[20] ÖZMESTİK F. Ü., "Bilişim Sistemleri Üzerinde Arama ve El Koyma Tedbirine İlişkin Mevzuat ve Uygulamada Yaşanan Sorunlar," (İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi), 2015, s.3.
[21] ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s.16.
[22] GÜNEYSU G. (Ed.). 2017. Bilişim hukuku. Eskişehir Anadolu Üniversitesi Yayınları. s.95.
[23] YILMAZ, s.63; benzer açıklama için bknz; TAŞKIN Ş. C., 2008. Bilişim suçları. 1.baskı bursa: Beta Yayınları, s.4
[24] ORTA, s.51.
[25] BAŞLAR, Y., 2016. Ceza Yargılamasında Elektronik Delil, Ankara, Yetkin Yayınları, s.70.
[26] ORTA, ss.51-52.

3. Bilgisayar

Bilgisayarın buluşundan buyana bu makineler değişik biçimlerde adlandırılmıştır.[27] Bilgisayarı icat eden Amerikalar tarafından söz konusu makineye İngilizce *computer* denilmektedir. Ülkemizde bu makineye ilişkin ilk başlarda "*ordnatör", "kompütür", "elektronik beyin*" gibi sözcükler kullanılmıştır. Günümüzde ise artık bilgisayar sözcüğünde tam bir anlaşma sağlanmıştır. Bilgisayar kelimesi söz konusu makinenin gerçek anlamına yakın olması ve bilgi işlemek kökünden gelen "*bilgi saymak, bilgi vermek*" anlamına gelmesi sebebiyle, bu sözcüğün seçimi yerinde olmuştur.[28]

Bilgisayar, çeşitli yöntemlerle dış ortamdan edindiği verileri; içerisinde barındırdığı programlar doğrultusunda depolayan, işleyen ve bu verilerden yeni sonuçlar üreten, ürettiği sonuçları da kullanıcıya sunan dolayısıyla veri iletimini sağlayan bir makinedir.[29]

Türk Dil Kurumunca bilgisayar, "*çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin*" şeklinde tanımlanmıştır.[30] Bilgisayarı benzer diğer aygıtlardan ayıran özelliği, programlanabilir bir sistem olması ve bir amaca özgülenebilmesidir. Şöyle ki gerekli programların yüklenmesiyle, bilgisayar önceden belirlemiş olan bir fonksiyonu gerçekleştirebilmektedir. Ancak bilgisayarın belirli bir işlevi yerine getirilmesine yönelik programlandırılması televizyon, fırın bulaşık makinesi, çamaşır makinesi ve diğer ev aletleri şeklinde değil, burada genel amaçlı programlanabilmesidir.[31] Yani ayırt edici özelliği genel kapsamlı olarak verileri işleyebilme ve kullanabilmesidir. Dolayısıyla bilgisayar açıkça belirtilen, önceden tanımı yapılmış karmaşık problemlere karşı yine önceden belirtilen çözüm yollarını yerine getirmektedir.[32]

---

[27] *"Sayısal makine", "matematiksel makine", "otomatik makine", "otomatik sayısal makine", "elektronik sayısal integratör ve hesap makinesi", "hassas değerli otomatik hesap makinesi", "otomatik olarak kontrol edilen sıralı hesap makinesi", "bilimsel hesap makinesi", "hesap otomatı"..* gibi kavramlarla adlandırılmıştır. IFRAH G., Bilgisayar Ne Sayar: Rakamların Evrensel Tarihi IX, (Çev.: Kurtuluş DİNÇER), 2. Baskı, Ankara, Tubitak Popüler Bilim Kitapları, 2002. s.1, aktaran DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, s.58.

[28] DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, ss.58-59.

[29] YENİDÜNYA/DEĞİRMENCİ, s.19.

[30] http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5caf03eb1102b5.68264309 [11.04.2019]

[31] YENİDÜNYA/DEĞİRMENCİ, ss.19-20; AKBULUT s.10

[32] AKBULUT, s.10

Bilgisayar, donanım(hardware) ve yazılım(software) olmak üzere iki unsurdan oluşmaktadır. Donanım bilgisayarın elle tutulabilen, gözle görülebilen fiziki parçalarıdır.[33] Bilgisayar donanımı; merkezi işlem birimi[34] ve ana bellek,[35] veri girişleri için giriş birimleri,[36] bilgi ve sonuçları göstermek için çıkış birimleri,[37] veri ve programların depolanması için depolama birimlerinden[38] ve son olarak da veri iletişimini sağlamak için iletişim birimlerinden[39] oluşmaktadır.

Yazılım (Software) bilgisayarın, elle tutulamayan gözle görülemeyen ancak sonuç almakta kullanılan soyut unsurlardan oluşmaktadır. Yazılım, programı kapsayan bir üst kavram olmaktadır.[40] Türk Dil Kurumunun resmi sayfasında yazılım, "*Bir bilgisayarda donanıma hayat veren ve bilgi işlemde kullanılan programlar, yordamlar, programlama dilleri ve belgelemelerin tümü*[41]*"* şeklide tanımlanırken program, "*bilgisayara bir işlemi yaptırmak için yazılan komutlar dizisi*[42]" olarak tanımlanmıştır. Yazılımlar, sistem yazılımları[43] ve uygulama yazılımları[44] olarak iki genel kategoriye ayrılmaktadır.[45] Sistem yazılımları, bilgisayar her açıldığında yüklenen ve kapanana kadar kullanılan

---

[33] AKBULUT, s. 11

[34] İşlem birimleri, veriler üzerinde işlem yapan birimdir. Anakart ve Chip set bu kapsamdadır. AKBULUT, Bilişim Alanında Suçlar, s.12.

[35] *"random access memory (rastgele erişimli bellek) ifadesinin kısaltması olan RAM adı verilir. Bu ad bellekte bir konuma rastgele ve hızlı bir şekilde erişebildiğimiz için verilmiştir. RAM'de sadece işlemcide çalışan program parçaları tutulur ve elektrik kesildiği anda RAM'deki bilgiler silinir."* https://tr.wikipedia.org/wiki/Bellek_(bilgisayar)[16.05.2020].

[36] AKBULUT, s.11;Giriş birimleri, bilgisayara dışarıdan veri girişine imkan sağlayan aygıtlardır. Örneğin klavye, fare, barkod okuyucu, mikrofon, dijital kameralar bu kapsamdadır. ÖZKUL, s.15;

[37] Çıkış birimleri, bilgisayarda işlenen bilgi ve sonuçları göstermeye imkan sağlayan ve manyetik alana, kâğıt üzerine veya ekrana aktaran aygıtlardır. Örneğin, monitör, yazıcı, plotter hoparlör gibi. AKBULUT, s.11.

[38] Depolama birimleri, verilerin depolanıp saklanmasında kullanılan parçalardır. Bunlara örnek olarak harddisk, disket sürücü, CD sürücü, DVD sürücü verilebilir. ÖZKUL, s.15.

[39] İletişim birimleri, bilgisayarlar arasında veri alışverişini sağlayan aygıtlardır. Ağ kabloları, modem, kızılötesi ve fax modemi bu kapsamdadır. AKBULUT, s.12.

[40] AKBULUT, s.9.

[41] http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5caf03f59a8645.30454492 [11.04.2019]

[42] http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5caf082c536ec5.72468597 [11.04.2019]

[43] Sistem yazılımları, uygulama yazılımı ile sistem donanımı arasında köprü vazifesi görmektedir. "*Uygulama yazılımlarına platform sağlayan ve program komutlarına göre donanımı kontrol eden yazılımlardır."* Bunlara Windows, Mac OS ve Linux örnek olarak verilebilir. ÇAKIR, H./KILIÇ, M. S.(Ed.). 2014. Adli bilişim ve elektronik deliller. Ankara: Seçkin yayınları, s.56

[44] "Bu yazılımlar, sistem yazılımı üzerinde kullanılmak ve belirli konulardaki problemlerin çözümüne yönelik yazılmıştır. Bu programlar hangi sistem yazılımına uygun yazılmışsa, o yazılım altında çalışırlar. Bunlara örnek olarak Microsoft Word, Microsoft Exel, Outlook Express, flash, oyunlar, antivirus programları verilebilir. AKBULUT s.12.

[45] AKBULUT s.12; ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.56.

yazılımdır.[46] Uygulama yazılımları ise "*Bilgisayar kullanıcılarının kullanımı için yazılan ve paket programlar olarak da adlandırılan bu yazılımlar, çok sayıda ve çok çeşitlidir*."[47]şeklinde tanımlanmaktadır.

Bilgisayar, verileri anlayabileceği bir dile dönüştürmektedir. Bu dönüştürme işleminde iki tabanlı sayı sistemine dayalı kodlama kullanılmaktadır. Bilgisayar, sistemine yazılan harfleri, rakamları ve diğer bir takım özel simgeler içeren verileri "1" ve/veya "0" lı hallere çevirmektedir.[48] Bilgisayarda gerçekleşen tüm işlemler aslında birçok 0 ve/veya 1 'in yan yana gelmesiyle oluşan değerlerdir.[49] Dolayısıyla bilgisayar ve medya aygıtlarında veriler, sıfır ve birden oluşan, ikili sayı sistemi yöntemiyle tutulmaktadır.[50]

4. Veri

Veri kelimesi, İngilizcedeki "data" sözcüğünün karşılığı olarak kullanılmaktadır.[51] Veri, bilişim sistemlerinin temel birimidir. Bilişim sistemlerinin amacı veriyi saklamak, işlemek ve bu verilerden sonuç çıkarmaktır.[52] Her ne kadar veri ve bilgi kavramları aynı anlamda kullanılmakta ise de birbirinden farklı kavramlardır.[53] İnternet toplu kullanım sağlayıcıları hakkında yönetmeliğin tanımlar kısmında "*Veri, Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri"* şeklinde ifade edilirken aynı Yönetmelikte, "*Bilgi, verilerin anlam kazanmış biçimini*" şeklinde belirtilmiştir.[54]

ÖZKUL' a göre "*Veri, ham haldeki olayları, rakamları ve detayları ifade ederken, bilgi organize edilmiş anlamlı ve yararlı veri çıkarsamalarını ifade eder. Örneğin, perakende satış yapan bir mağazada, bir müşterinin siparişinde yer alan müşterinin kimliği, sipariş ettiği ürün, satın almak istediği ürün miktarı ve ürün fiyatı mağaza için ham haldeki verilerdir. Ancak dönem sonunda, bütün siparişlerle ilgili detaylar bir araya getirilip toplanıp o dönem beklentileri ile karşılaştırıldığında, çıkan sonuç, mağaza*

[46] AKBULUT, s.12.
[47] ÖZKUL, s.16;
[48] AKBULUT, ss. 14-15
[49] Bu iki rakamın oluşturduğu ikili bileşenlerine "bit" adı verilmektedir. 8 bitlik bir gruba "1 byte" denmektedir. Ayrıca, verilerin (0) ve (1) sayılarına denk gelen "açık" veya "kapalı" durumlarda oluşabilen elektronik anahtarlar mevcuttur. ÖZMESTİK, s.4.
[50] ORTA, s.48.
[51] ORTA, s. 39.
[52] YENİDÜNYA/DEĞİRMENCİ, ss. 47-48.
[53] ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s.39.
[54] http://www.resmigazete.gov.tr/eskiler/2017/04/20170411-3.htm [4.04.2019]

yöneticisine, o dönemin performansının beklenen performanstan daha iyi veya kötü olduğu konusunda bilgi sunar."[55]

YENİDÜNYA/DEĞİRMENCİ'ye göre "*Veri, bilgilerin belirli bir formata dönüştürülmüş halidir.*" Bu bakımdan bir bilişim sisteminde yer alan bir program, resim veya yazı gibi saklanan her şey veridir.[56]

DÜLGER'e göre *"Veri; bilişim sistemlerinin üzerinde işlem yapabildiği, bu işlemlere dayalı sonuçlar üretebildiği, saklayabildiği, sakladıktan sonra tekrar okuyup işleyebildiği ve diğer bilişim sistemlerine iletebildiği her türlü bilgidir."*[57]

AKARSLAN' a göre veri, bilginin, iletişim, yorum ya da işlem için uygun olarak formülize edilmiş şekilde gösterilmesidir.[58]

ÇAKIR VE DİĞERLERİ'ne göre "Veri, olgu, kavram veya komutların, iletişim, yorum ve işlem için matematiksel kabul görmüş fonksiyonlar ile hesaplanarak elverişli bir biçimde gösterilen değer" şeklinde ifade etmiştir.[59]

TCK'nın 243. maddesinin gerekçesinde ise *"sistem içindeki bütün soyut unsurlar, fıkrada geçen "veri" teriminin kapsamındadır"* şeklinde belirtilmiştir. [60]

Avrupa Konseyi Siber Suç Sözleşmesi'nin birinci maddesinde bilgisayar verisini *"bilgisayar sisteminin bir işlevi yerine getirmesini mümkün kılan bir programı kapsayan, olguların, bilginin veya kavramların bir bilgisayar sisteminde işlenmeye uygun halde ki her türlü temsili ifade eder" şeklinde tanımlanmıştır.*[61] ERDOĞAN' a göre veri kavramı yalnızca bilgisayar verisi olarak anlaşılmamalıdır. Bilgisayar, yukarıda da belirtildiği gibi bir sistem dâhilinde çalışmaktadır. Bu sistemdeki bir takım araçlar, bilgisayar tanımına uymaksızın, sistemin bir parçası olarak çalışabilmektedir. Örneğin sadece bilgi yükleyen büyük sanal bilgi depoları, CD, disket, taşınabilir ana bellek gibi veri taşıyan diğer araçlar bu kapsamdadır. Ayrıca belirtmek gerekir ki

[55] ÖZKUL, s.13.
[56] YENİDÜNYA/DEĞİRMENCİ, ss. 47-48.
[57] DÜLGER M. V., Ceza Hukuku, Ceza Muhakemesi Hukuku ve Bilişim Hukuku Uygulama Çalışmaları, Ankara, Seçkin Yayıncılık, Eylül 2018, s. 414.
[58] AKARSLAN H., 2015. Bilişim suçları. 2. Baskı. Ankara: Seçkin Yayıncılık, ss.30-31.
[59] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.155
[60] www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc[4.04.2019].
[61] https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf [15.07.2020].

bilişim suçlarının büyük bir kısmı da bu veriler üzerinde işlenmektedir. Bu sebeple sadece "veri" sözcüğünün kullanılması daha uygun olmaktadır. Aksi halde bu verilerin konu olduğu suçlar yaptırımsız kalabilecektir.[62]

5. Bilgisayar Ağları

Bilgisayarın ilk kullanılmaya başlandığı zamanlarda, iki bilgisayar arasında veri aktarmak istenildiğinde, bu veriler bir diskete kopyalanarak başka bir bilgisayara aktarılması şeklinde gerçekleştirilmekteydi. Ancak geçen zaman zarfında bilgisayarlar arası veri iletişimi ve paylaşımı ihtiyacı artmıştır.[63] İşte bilişim sisteminde yer alan verilerin, paylaşılmasının istenmesi sebebiyle ağ(network) kavramı ortaya çıkmıştır. Avrupa Konseyi Siber Suç Sözleşmesi(AKSSS)' ne göre ağdan anlaşılması gereken şey iki veya daha fazla bilgisayar arasındaki ara bağlantı olmaktadır. Söz konusu bağlantı, kablolu veya kablosuz olabilir.[64] Bilgisayar ağları, bilgisayarların birbirleriyle veri alışverişi ve ortak iş yapacak biçimde bağlanmasıyla oluşmaktadır.[65] Bu ağlar kısaca veri alışverişinin işlendiği, yapıldığı ve paylaşıldığı haberleşme sistemi olarak ifade edilebilir.[66] Veri iletişimim sağlayan birçok ağ bulunmaktadır. Ağlar, yayıldıkları alan göz önüne alındığında genel olarak LAN (Local Area Network-Yerel Alan Ağı) ve WAN (Wide Area Network-Geniş Alan Ağı) olarak ikiye ayrılmaktadırlar.[67] Bilişim araçlarının birbirlerine yakın olduğu veya bir kablo ya da ağ kartı (ethernet kartı) ile bağlandıkları ağ sistemine LAN (Local Area Network-Yerel Alan Ağı) denilmektedir. Bu ağlar ile dar çerçevede, diğer ağlara sınırlı bir bağlantı kurulabilir.[68] Yerel bilgisayar ağı, aynı mekânda bulunan örneğin bir bina içerinde ya da kampüs alanındaki gibi yakın mesafede bilgisayarların birbirine bağlanması şeklinde kurulan ağlardır.[69] Uzak mesafedeki bağlantılardan oluşan ağ çeşidi ise WAN (Wide Area Network-Geniş Alan Ağı)olmaktadır.[70] Geniş alan bilgisayar ağı, şehirler, ülkeler, kıtlar arasındaki iletişimini sağlamak için kullanılmaktadır. Söz konusu ağ, küçük ağların bir araya gelmesiyle

[62] ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, ss.41-42.
[63] ORTA, s.54.
[64] YENİDÜNYA/DEĞİRMENCİ, s.34.
[65] ÖZMESTİK, s.6.
[66] 4. Ağ ve bilgi güvenliği sempozyumu. elektrik mühendisliği dergisi. 2012, s.70 http://www.emo.org.tr/ekler/ea331d3983f3898_ek.pdf?dergi=873[9.11.2019]
[67] YENİDÜNYA/DEĞİRMENCİ, s.35.
[68] BAŞLAR, Ceza Yargılamasında Elektronik Delil, s.71.
[69] AKBULUT, s.16.
[70] YENİDÜNYA/DEĞİRMENCİ, s.36.

oluşmakta ve ağlar birbirlerine telefon hattı, uydular ve radyolinkle bağlanmaktadır. Ayrıca uzak mesafeler olması sebebiyle iletişimi güçlendirmek adına modem araç olarak kullanılmaktadır.[71] Bunlar dışında PAN(Personal Area Network-Kişisel Ağ Bağlantısı),[72] MAN (Metropolitan alan ağları),[73] Intranet/Extranet[74] ve İnternet gibi ağ çeşitleri bulunmaktadır.[75]

6. İnternet

İnternet, en yaygın olan iletişim ağı olması sebebiyle ayrı bir başlıkta açıklanmasında fayda bulunmaktadır. International ve Network sözcüklerinin başlangıç kısımlarının birleştirilmesiyle oluşan[76] İnternet kavramı, dünya üzerinde bulunan ağların ya da bilgisayarların TCP/IP protokolü ile birbirine bağlanmasıyla oluşan ve insan, makine birliğini sağlayan[77] dünya çapında bir ağ olmaktadır.[78] İnternete "ağlar arası ağı" da denilmektedir. Ancak sanılanın aksine sanal alanın sadece bir parçası olup veri iletim ağlarından biridir. Sanal alan ise *"bilişim sistemleri ile bunları birbirine bağlayan her türlü veri iletişim ağından oluşan, fiziksel yapısı sayısal verilerden ibaret bir alandır."*[79]

IP adresi[80] İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelikte, "*Belirli bir ağa bağlı cihazların birbirini tanımak,*

[71] AKBULUT, ss.16-18.
[72] Kişisel ağ bağlantısı, kişisel cihazların birbirleriyle bağlanmasıyla oluşmaktadır. Bu ağ, kişisel ağın parçası olan aygıtlar(USB, yazıcı, fotoğraf makinesi ve cep telefonu gibi) ile bilgisayar arasında erişimi gerçekleştirir. AKBULUT, s.16.
[73] Metropolitan alan ağları, içerisinde birden çok LAN sistemi barındırmakta olan ve coğrafi büyüklüğü, LAN ve WAN arasında olan bir ağdır. Bir şehri kapsayacak büyüklüğe sahip olabilir. Herhangi bir kuruma veya kuruluşa ait olabileceği gibi, kamuya açık bir hizmet biçiminde de olabilir. GÖKSOY R., Ceza Muhakemesinde Dijital Delillerin Elde Edilmesi ve Güvenilirliğinin Sağlanması, 1.Baskı, Ankara, Seçkin Yayıncılık, Ocak 2019.;AKBULUT, s.17.
[74] Intranet, bir işyerinde çalışanlar arasında bilgi paylaşmak ve iletişim sağlamak amacıyla kullanılan yalnızca kuruma özgü bir iş ağıdır. Genellikle TCP/IP tabanlı olmakta ve yetkisiz kullanıcılara karşı bir güvenlik duvarı ile korunmaktadır. Extranet de ıntranete benzer nitelikte özel bir iş ağı olmakla birlikte, seçili kullanıcıların dışarıdan ağa erişimine imkân sağlanmaktadır. AKBULUT, s.17.
[75] Diğer ağ çeşitleri hakkında ayrıntılı bilgi için bkz: GÖKSOY, ss.34-41.
[76] APAYDIN, s.282.
[77] AKBULUT, s.18.
[78] ÖZMESTİK, ss.5-6.
[79] GÜNEYSU, s.96.
[80] "*İnternet Protokolü (IP) ağ sınırları boyunca datagramların geçişi için internet protokolü takımında temel iletişim protokolüdür. Yönlendirme işlevi sayesinde internetin çalışmasını sağlar ve internetin olmazsa olmazıdır. IP, paket teslim görevini paket başlıklarındaki IP adreslerine dayalı olarak kaynak adresten hedef adrese doğru gerçekleştirir. Bu amaçla, IP veri teslim edilecek kapsülleyen bir paket yapıları tanımlamaktadır. Aynı zamanda adresleme yöntemlerini tanımlayan bu method kaynak ve hedef bilgileri ile diyagramı etiketlemek için kullanılır. IP, 1974 yılında Vint Cerf ve Bob Kahn tarafından orijinal iletim kontrol programında bağlantısız bir datagram hizmeti olarak tanıtıldı. İnternet protokolü*

birbirleriyle iletişim kurmak ve birbirlerine veri yollamak için kullandıkları, İnternet Protokolü standartlarına göre verilen adres" şeklinde tanımlanmıştır.[81] Bu ağa erişim bilgisayarlar, tablet PC'ler, telefonlar ve benzeri aygıtlar üzerinden gerçekleşmektedir. İnternet kullanımı ile web sitelerinin kayıtları ve sitelerde yayınlanan bütün dosyalara ilişkin verilere ve söz konusu aygıtların depolama alanlarından elde edilebilecek olan elektronik verilere, ulaşılabilir.[82]

Bununla birlikte internet protokol standardını kullanan bir ağdaki cihazların birbirleriyle iletişim kurması ve veri alışverişinde bulunması için kullanılan IP adresi[83] ya da numarasından, suçluların takibinde yararlanılmaktadır. IP numarası ile kullanıcının bulunduğu ülkeyi, kenti, enlem, boylamı ve ISS'nı tespit edilmesi mümkündür. [84] Elektronik deliller bakımından üzerinde durulması gereken önemli bir husus olarak belirtilmelidir ki, IP numaraları tek başlarına vuku bulan suça ilişkin faili göstermez.[85] IP adresi, "*internete bağlanmak isteyen bilgisayara internet servis sağlayıcıları tarafından atanan kimlik numarasıdır*". IP numarasını internet ortamında, kolay bir biçimde temin eden programlar ve zararlı yazılımlar[86] bulunmaktadır. Bu

---

paketi bu nedenle sık sık TCP/IP gibi ifade edilir. IP'nin ilk büyük versiyonu İnternet Protokolü Sürüm 4'tür. IPv4 internette baskın olan bir protokoldür. Onun halefi İnternet Protokolü Sürüm 6 (IPv6)'dır".https://tr.wikipedia.org/wiki/IP_adresi [14.05.2020].

[81] http://resmigazete.gov.tr/eskiler/2007/11/20071130-6.htm [7.04.2019].

[82] KIZILYAR M., 2014. Ceza yargılamasında dijital verilerin delil değeri. Adalet Dergisi. (50), ss.82-83

[83] *"IP adresleri kendi içinde, statik ve dinamik olmak üzere ikiye ayrılır. Statik IP adresi; hiçbir zaman değişmeyen, kalıcı bir IP adresidir. Dinamik IP adresi ise bir cihaza, internete her bağlanışında yeniden tanımlanan yani geçici bir IP adresidir. Statik IP adresleri bilgisayara, bir admin tarafından manuel olarak atanır. Dinamik IP adresleri ise bilgisayar arayüzü ya da sunucu yazılımı tarafından, otomatik olarak atanır." h*ttps://www.chip.com.tr/ip-adresim-nedir [14.05.2020].

[84] BAŞAR, Y. "Siber Suç Soruşturmalarında Adli Bilişim İncelemeleri", Yayınlanmamış yüksek lisans tezi, Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, İnternet ve Bilişim Teknolojileri Yönetimi, Eylül 2015, ss.18-19.

[85] "Kullandığı bilgisayar üzerinde usulünce imaj alma işlemi yapılarak sonucunda çıkan veri bütünlük (hash) değerlerinin tespit edilmemiş bulunması, IP numarasının kullanılan bilgisayarı göstermeyip internetle olan bağlantıyı göstermesi, sanığın bilgisayarlarında yapılan incelemede, bu bilgisayar kütüğünden marma- riskoleji-k12.com adresine bağlantı yapıldığının tespit olunamaması "hack" programına rastlanmasının şikayetçiye ait siteye müdahale edildiğini göstermeyeceği, kesin delil bulunmadan varsayımlarla hüküm kurulamayacağı gözetilmelidir." Kararı aktaran, DULGER, M. V., Bilişim Suçları ve İnternet İletişim Hukuku, s.558; Yargıtay Sekizinci Ceza Dairesinin 24/10/2013 tarih ve E.2012/21817, K.2013/25428 sayılı kararı.

[86] *"Zombi bilgisayar, (genelde yalnızca zombi olarak kısaltılır) genel ağa (internet) bağlı, bir kırıcı (hacker) tarafından bilgisayar virüsü veya truva atı ile tehlikeye atılmış bilgisayardır. Daha geniş bir şekilde ifade etmek gerekirse Zombiler, programların içlerine gizlenmiş ya da bizzat uygulama dosyası olarak indirilir ve çalıştırılır. Program çalıştığı andan itibaren sizin internet bağlantınızı kullanarak istenilen hedeflere saldırı düzenler. Böylelikle Hacker yakalanma riskine kendisini değil Zombi Bilgisayarları atmış olur. Diğer bir avantajı ise saldırıyı güçlü hale getirmektir. Tek bir saldırı komutu ile binlerce saldırı gücüne sahip olunmuş olur."* https://tr.wikipedia.org/wiki/Zombi_bilgisayar [14.05.2020].

sebeple IP numaraları değiştirilebilmekte ve suçu işleyen kişiler kendilerini bu yöntem ile kolaylıkla gizleyebilmektedir. IP numarası soruşturma evresinde kolluk görevlileri tarafından suçlunun tespit edilebilmesi için temel delil niteliğinde görülmekte ancak adli makamlarca IP numarası tek başına delil olarak kabul edilmemektedir. Bu bağlamda IP numaraları suçlunun tespiti için yapılmakta olan çalışmada başlangıç noktası olarak kullanılmalıdır.[87] IP numarasının tespiti sonrasında şüpheli şahsın kullanmakta olduğu bilgisayar/bilgisayar kütükleri ve benzeri materyaller üzerinden inceleme işlemleri yapılmalı, inceleme sonucunda suça ilişkin delil bulunması halinde IP numarası delil olarak kabul edilmelidir. Aksi halde sadece IP numarası tespiti ile bir şahsın cezalandırılması hukuka aykırı olacaktır.[88]

B. ELEKTRONİK DELİL

1. Ceza Muhakemesinde Delil

Ceza muhakemesinde, muhakeme makamları ilk olarak uyuşmazlık konusunun maddi yönü ile ilgilenmektedir. Bu bakımdan işlendiği iddia edilen fiilin işlenip işlenmediği, işlenmişse söz konusu fiilin, kanunda bir suç teşkil edip etmediği ve suç teşkil etmesi halinde bunun sanık tarafından gerçekleştirilip, gerçekleştirilmediği tespit edilmektedir. Bu hususların tespit edilmesi ve hâkimin yapacağı değerlendirme sonucunda, suçun sabit olması halinde sanık cezalandırılmakta, suçun sübut bulunmadığı halde ise ceza verilmemektedir. Dolayısıyla ceza muhakemesinde geçmişte yaşanılan bir olayın çözümlenmesi yapılmakta neyin, nasıl gerçekleştiğini üzerinde araştırma yapılarak maddi gerçeğin ortaya çıkarılması[89] hedeflenmektedir. Hâkimin kararının oluşmasında gerçekleştirilecek olan muhakemenin temelinde, delillerin değerlendirilmesi yatmaktadır.[90]

Ceza muhakemesinde suç fiilinin sanık tarafından gerçekleştirilip gerçekleştirilmediği hususunda, hukuk düzenince kabul edilmekte olan vasıtalar ile yargılama makamlarının kuşku yer olmayacak bir biçimde tam bir kanaate varmasına yönelik faaliyetlere “ispat”

[87] DÜLGER, Bilişim Suçları ve İnternet İletişim Hukuku, ss.557-558.
[88] BAŞAR, ss. 18-19.
[89] ERCAN İ., 2014. Themıs ceza muhakemesi hukuku. 8. Baskı. İstanbul: On iki levha yayıncılık, s. 10
[90] TOROSLU, N. /FEYZİOĞLU, M., 2017. Ceza Muhakemesi Hukuku, Ankara, Savaş yayınevi, s. 172.

denilmektedir.[91] Bu bağlamda, muhakeme makamları görevlerini yerine getirirken bir ispat vasıtası olan deliller kullanılmaktadır.[92] "*Delil, cezai uyuşmazlığın konusu olan olayı temsil eden, olayın mahkeme önünde canlandırılmasına yarayan araçtır*." Dolayısıyla delillere, cezai uyuşmazlığın maddi boyutunun ispatı için ihtiyaç duyulur ve ispat gereken olguya ilişkin tüm deliller değerlendirmeden muhakeme makamı tarafından tam bir vicdani kanaate varılamaz.[93] Ceza yargılamasında mahkûmiyet hükmü muhtemel kanıya değil, kesin ve inandırıcı ispata ve her türlü şüpheden uzak bir kesinliğe dayanmalıdır. Bu noktada deliller şüpheyi yenecek, yerini kanaat alacak ve maddi gerçeğe ulaşılacaktır.[94] Ayrıca ceza muhakemesi hukukunda belirli bir konunun belirli bir delille ispat edilmesi zorunluluğu bulunmamaktadır.[95] Zira ceza hukukumuzda ispat araçları önceden hazırlanmaz. Genellikle suç gizlilik içerisinde işlenir ve delillerin yok edilmeye çalışılması da mümkündür.[96] Bu sebeple ceza muhakemesinde delilleri sınırlandırmadan, bir konunun her türlü delille ispatını mümkün kılan delil serbestisi ilkesi benimsenmiştir. Delil serbestisi ilkesi ile hâkim, sadece tarafların ileri sürdüğü delillere bağlı olmamakta ve maddi gerçeğe götüren her olguyu delil olarak değerlendirebilmektedir.[97] Hâkim yapacağı muhakeme sonucunda, akla ve mantığa uygun bir değerlendirme ile toplanan delillerin hangilerine neden inanıp inanmadığının nedenini ve hangi delilleri ne sebepten dolayı, hükme esas alıp almayacağı hususunu açıklaması gerekmektedir. Bu şekilde gerekçeleri belirtmek şartıyla hâkim, delillerin toplanmasında ve toplanan delillerin değerlendirilmesinde serbestiye sahip olmakta ve bu sisteme "vicdani delil sistemi" denmektedir.[98] Vicdani delil sisteminden, hem delil serbestliği hem de delillerin değerlendirilmesi serbestliği anlaşılmalıdır.[99]

[91] SARSIKOĞLU Ş., 2015. Ceza muhakemesinde delil ve ispat hukuku açısından elektronik delil(e-delil) Kavramı. Türkiye Adalet Akademisi Dergisi. Yıl:6, (22), Temmuz, ss.427-454. s.431.
[92] YENİSEY F./NUHOĞLU A., 2018. Ceza muhakemesi hukuku. 6. Baskı. Ankara: Seçkin, s.482; ORTA, s.237.
[93] SARSIKOĞLU, ss.428-432.
[94] ŞAHİN C./GÖKTÜRK N., 2019. Ceza muhakemesi hukuku. 2. Baskı. Ankara: Seçkin Yayınları, s 174.
[95] YENİSEY/NUHOĞLU, s.482.
[96] ŞAHİN/GÖKTÜRK, s.175.
[97] YENİSEY/NUHOĞLU, s.483; TOROSLU/ FEYZİOĞLU, s.173.
[98] ÖZEN, M./ÖZOCAK, G. "Adli Bilişim, Elektronik Deliller ve Bilgisayarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M 134)", Ankara Barosu Dergisi, Sayı:1, 2015, ss. 43-77, s. 57
[99] YENİSEY/NUHOĞLU, s.483.

2. Ceza Muhakemesinde Delillerin Özellikleri

Hâkim delilleri değerlendirmede, takdir yetkisini kullanabilmekte ise de bu serbesti sınırsız değildir. Delillerin, mahkeme tarafından hükme esas alınabilmesi için bir takım özelliklere sahip olması gerekmektedir.[100] Nitekim elektronik delillerin hukuki geçerliliğinin sağlanması için de diğer delillerde bulunması gereken özelliklere haiz olması gerekir.[101]

a.Deliller gerçek olayı temsil edici olmalıdır. Delillerin, geçmişte gerçekleşmiş olan[102] yargılama konusu olayın bütününü, ya da bir kısmını temsil etmesi gerekir.[103]

b.Deliller, mantık kurallarına uygun ve gerçekçi olmalıdır. Gerçeği akla uygun biçimde ifade edebilecek bulguların delil olarak kabul edilmesi gerekir. Dolayısıyla bu bulguların, akılcı(rasyonel) olması ve bilimce kabul edilmesi gerekmektedir.[104] Akılcılık olarak da ifade edilen bu özellik, delillerin duygusal saplantılardan ve önyargılardan arınmış bir akıl yürütmenin sonucunda ortaya konulmasıdır.[105]

c.Deliller, konu ile ilgili olmalıdır. CMK m.206/2-b gereği delil ile ispat edilmek istenen olayın, karara etkili bir olay olması gerekmektedir.[106] Elde edilen deliller, ispatına ihtiyaç duyulan hususlarla ilgili olmalı ve söz konusu hususları aydınlatmalıdır.[107]

d.Delillerin, kanuna uygun olması gerekmektedir. Deliller hem kanuna uygun olmalı, hem de kanuna uygun yollardan elde edilmiş olmalıdır.[108] Ceza Muhakemesi

---

[100] YENİSEY/NUHOĞLU, s. 489.

[101] ÖZTÜRK C., 2016. Kolluk Amaç ve Yapıları ile Veri Elde Etme Araçları Arasındaki Bağlantı Üzerine Bir Araştırma. Bitlis Eren Üniversitesi Sosyal Bilimler Dergisi. 5(1), ss. 1-24.,s.6; BAŞLAR, Ceza yargılamasında elektronik delil, s.92.; ARAALAN C., Türk Hukukunda Dijital Deliller, GSI ARTICLETTER SUMMER 2015.ss. 203-212., s.204; DEĞİRMENCİ, O, 2014. Bilgi toplumunun delil türü: sayısal deliller ve bilimselliği. Terazi Hukuk Dergisi. 9(97), ss.14-28, s.15.

[102] ÖZEN/ÖZOCAK, s. 57.

[103] BİRTEK F., Ceza muhakemesinde delil ve ispat, Ankara, 2017, Adalet yayınevi 2. Baskı, s.47.

[104] YENİSEY/NUHOĞLU, s.489.

[105] BİRTEK, s.57.

[106] YENİSEY/NUHOĞLU, s.490; CENTEL/ZAFER, Ceza muhakemesi hukuku,11. Baskı s.211. Beta: İstanbul 2014.

[107] TOROSLU / FEYZİOĞLU, s. 175.

[108] Bir takım deliller kanuna uygun yollarla elde edinilmiş olmalarına rağmen içerikleri nedeniyle delil olarak kullanılamaz. Örneğin hekimler, hekim sıfatı ile hastaları veya hasta yakınları hakkında öğrendikleri bilgileri, hukuki yollardan edinilse dahi, bu kişilerin izinleri olmadan, mahkemeye sunamazlar. Bazı deliller ise hukuka aykırı yollardan elde edinilmesinden dolayı delil olarak kullanılamaz. Buna örnek olarak CMK m. 148'de belirtildiği üzere kişinin özgür iradesini etkileyecek,

Kanunumuzda elde edilen delillerin, delil elde etme yasaklarına aykırı olması halinde değerlendirilemeyeceği belirtmiştir.[109]

e.Deliller, müşterek olmalıdır.[110] Bu bağlamda delilin içeriğini yalnız mahkeme makamının bilmesi yetmemekte, tarafların da bilmesi gerekmektedir. Ceza muhakemesinde, buna "delillerin müşterekliği ilkesi" denilmektedir. Bu ilke ile sunulan deliller muhakeme taraflarınca tartışılmalı, hâkim şahsi bilgisine dayanarak hüküm tesis etmemelidir. Aksi halde savunma hakkının zedelenmesi sonucunu doğuracaktır.[111]

Suça ilişkin emarelerin, ceza muhakemesinde kullanılabilmesi için belli kurallara uygun olması gerekir. Bunların hukuk ile ilgili olanları CMK'da yer alırken, teknik kısımlara ilişkin olanları kriminalistlik biliminin kapsamındadır. Belirti delilleri de bu tür bilimsel yöntemlerle elde edilen delillerden olup, bilimsel delillerdir. Bilişim sistemleri ile bağlantılı işlenen suçlarda bu bilim dalının kurallarına ve bilişim sisteminin özelliklerine dikkat edilerek delil elde edilmektedir. "Bilgisayar Kriminalistliği Bilimi" ya da başka bir deyişle "Adli Bilgisayar Kriminalistliği", bilimsel teknik prensiplerin uygulandığı bir inceleme sürecinin tümüdür.[112] Burada "bilimsel delil" ile "delilin bilimselliği" kavramlarını açıklamakta fayda bulunmaktadır. Bilimsel delil, delilin değerlendirme süreciyle ilgili bir kavramdır. Delilin bilimselliği ise, delilin elde edilmesi süreciyle alakalı bir kavramdır.[113]

Elektronik deliller, elde edildikleri andan hükme esas teşkil edilinceye kadarki süreçte, genel geçerli bilimsel kurallara uygun şekilde işlem görmelidir.[114] Ancak belirtmek gerekir ki her bilimsel delil objektif(nesnel) değildir. Zira bilimsel olarak adlandırılan delillerin çoğunluğu, örneğin kişinin laboratuvar deneyi yapması gibi, bilimsel bir mütalaadır. Bu anlamda yanılmalar mümkün olup, sübjektiftir(özneldir). Tam anlamıyla objektif olan bilimsel delil mevcut olması halinde hâkimin vereceği kararı etkilemesi gerekmektedir. Bu kapsamda bilimsel delil türlerinden biri olan veriler, açık ya da

---

engelleyici nitelikte kötü davranma, işkence, aldatma, ilaç verme, cebir veya tehditte bulunulması hali, bazı araçlar uygulama gibi kişinin iradesini etkileyen bedeni veya ruhi müdahalelerle veya kanuna aykırı bir menfaat vaadinde bulunulması ile elde edilen deliller verilebilir. ÖZEN/ÖZOCAK, s. 58.

[109] TOROSLU/FEYZİOĞLU, s. 175

[110] CENTEL, N. / ZAFER H.,2014. Ceza muhakemesi hukuku,11. Baskı, s.212.

[111] TOROSLU/FEYZİOĞLU, s.176

[112] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s.560.

[113] DEĞİRMENCİ, Bilgi toplumunun delil türü: sayısal deliller ve bilimselliği, s.23.

[114] DEĞİRMENCİ, Bilgi toplumunun delil türü: sayısal deliller ve bilimselliği, s.15.

kapalı elektrik devrelerini taşıyan bir cihaz yardımıyla okunduğunda anlam kazanmaktadır. Bu delillerin bir uzman tarafından değerlendirilmesinden sonra ceza muhakemesinde kullanılması, mukayeseli hukukta da kabul edilmektedir.[115]

3. Elektronik Delil

Günümüzde bilişim sistemleri ve elektronik aygıtlar yaygınlaşarak günlük yaşantımızın bir parçası haline gelmiştir. Gelişen teknolojiye paralel olarak suç tipleri ve suç işleme yöntemleri de değişim göstermektedir. Bu suç tiplerine ilişkin suç, suçluyla[116] mücadele yöntemleri ve ispat araçları da aynı doğrultuda değişmekte, gelişen teknolojiye uyum sağlamaktadır.[117] Suç soruşturmasının etkin bir şekilde yürütülebilmesi için deliller önem taşımaktadır. Bu bağlamda fiziki delillerin yanı sıra, soyut nitelikteki delillerde kullanılmaktadır.[118] Bir kişinin işlediği suç sonrası, suçla alakalı nasıl ki elinde olmadan arkasında delil niteliğinde olabilecek, herhangi bir iz veya emare bırakıyor ise bilişim sistemleri ile bağlantılı olarak işlenen suçlarda da o suç ile alakalı deliller, suç sonrasında farklı şekil ve boyutlarda, elektronik delil olarak suçun aydınlatılmasında kullanılmaktadır.[119] Dolayısıyla, bilişim sistemlerinin yaygın bir şekilde kullanılması olay yerinin, fiziksellikten; bilişim sistemlerinin oluşturduğu sanal alana doğru yönelmesine sebep olmuştur.[120]

Ceza muhakemesinde ki delillerin serbestliği ilkesi gereği[121] elde edilebilecek her izden delile ve gerçekleşen olaya ulaşılabilir. Dolayısıyla bu tür sistem veya aygıtlar

---

[115] YENİSEY/NUHOĞLU, ss.491-492.

[116] "*Günümüz suçluları fiziksel yakınlık, beceri ve cüretle sınırlıyken, gelecekteki suçluların bu tür kısıtlamarla karşılaşmayacakları ifade edilmektedir*." GÜNŞEN İÇLİ T., 2019. Kriminoloji, 10. Baskı. Ankara: Seçkin Yayıncılık., s. 573

[117] KIZILYAR, s.72.

[118] BAŞLAR Y., 2018. Elektronik delil ve ceza yargılamasında kabul edilebilirliğine ilişkin bir inceleme. *Legal Hukuk Dergisi*. 16 (184), ss. 1655-1688., s.1657.

[119] ÇAKIR H. / SERT E., Bilişim suçları ve delillendirme süreci, https://docplayer.biz.tr/1538965-Bilisim-suclari-ve-delillendirme-sureci.html s.145-146 [26.12.2020];BAŞLAR, Ceza Yargılamasında Elektronik Deliller, s.74.

[120] DEĞİRMENCİ, O, 2014. Bilgi toplumunun delil türü: sayısal deliller ve bilimselliği, s. 16.

[121] YARGITAY bir kararında "*…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 Kanununun '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*" şeklindeki ifadesiyle

üzerinden elde edilen her türlü veri, delil olarak ispat için kullanılabilmektedir. Söz konusu veriler; kişiler tarafından kaydedilen ya da transfer edilen bilgiler olabileceği gibi, kullanıcıların bu sistem veya aygıtları kullanmaları sonucunda bıraktıkları elektronik izlerden de oluşabilir. Ancak elektronik delillerin delil olarak kullanılması, yasal mevzuatta gösterilen yöntem ve koşullara uygun hareket edilmesine bağlıdır.[122] Bununla birlikte bilişim verisi şeklindeki elektronik delillerin ceza muhakemesinde kullanılabilmesi için elde edilmesinde özel hayatın gizliliğine müdahale oluşturmamasına özen gösterilmelidir.[123] Ceza muhakemesinde suçun ispatlamaya yarayan ve ikamesi mevzuat tarafından yasaklanmamış her şey delil ya da ispat vasıtası olabildiğinden, elektronik deliller de bu kapsamda değerlendirilmelidir. Dolayısıyla elektronik deliller ispat vasıtası olmakta ve bu delillerde önemli olan, muhakeme makamlarınca kabul edilebilir niteliklere haiz olmalıdır.[124]

Elektronik deliller doktrinde değişik şekillerde tanımlanmıştır.

DÜLGER' e göre elektronik deliller, *"Elektronik materyallerin içerisinde suçu ispat edebilecek nitelikteki dijital veriler "dijital delil" olarak isimlendirilir."*[125]

SARSIKOĞLU' na göre elektronik delil, elektronik bir cihaz üzerinde saklanabilen veya bu cihazlar aracılığıyla iletilebilen muhakeme bakımından değeri olan bilgi ya da verilerdir[126].

KESER BERBER' göre "*Elektronik delil, bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen soruşturma açısından değeri olan bilgi ve verilerdir.*[127]

ORTA' ya göre *"elektronik veya manyetik ortamda iletilebilen, herhangi bir şekilde saklanabilen, silinen, geri getirilen, bir suçun işlendiğini ya da işlenmediğini gösteren,*

---

delil serbestisi ilkesi çerçevesinde elektronik delillerin de ispat aracı olarak kullanılabileceğini belirtmiştir. Yargıtay CGK, 26.09.2017, E. 2017/956, K. 2017/370 Kararı aktaran BAŞLAR, Elektronik delil ve ceza yargılamasında kabul edilebilirliğine ilişkin bir inceleme, s.1679.

[122] KIZILYAR, s. 79.

[123] YENİSEY F. (Ed.). Ceza muhakemesi hukuku başvuru kitabı. 2018. Türkiye Barolar Birliği Yayını. s.134.

[124] ORTA, s.240.

[125] DÜLGER, M. V., "Adli Bilişim & Ülkemizde Uygulanması", Hukuk ve Daha Fazlası Dergisi, Sayı:1, 2017, ss.20-25, s.21.

[126] SARSIKOĞLU, ss.436-439.

[127] KESER BERBER L., 2004. Adli bilişim(Computer Forensic). Ankara: Yetkin Yayınları, s.46.

işlenmiş ise ne şekilde gerçekleştiğini açıklamaya yarayan her türlü veri şeklinde tanımlanabilir. [128]

ÇAKIR/KILIÇ' a göre ise elektronik delil*, "elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıt"* [129] şeklinde ifade edilmiştir.

Elektronik delilerin kimler tarafından toplanacağına dair mevzuatta açık bir hüküm bulunmamaktadır. CMK m. 160/2 gereği cumhuriyet savcısının adli kolluk görevlileri vasıtasıyla şüpheli hakkında lehe ve aleyhe her türlü delilli toplama imkânı bulunmakta ise de, bu delillerin üzerinde bulundukları aygıtlarda yapılacak arama işleminin özel bir uzmanlık gerektirmesi sebebiyle, adli kolluğun uzman birimlerince veya atanacak uzman bilirkişilerce elektronik delillerin toplanması gerekir.[130]

a. Elektronik-dijital kavramları

Bilişim sistemleri üzerinden elde edilen delillerin, adlandırılmasında bir standart bulunmamaktadır. Söz konusu delil çeşidini ifade etmek için; bilgisayar delili, elektronik delil,[131] sayısal delil, dijital delil[132] ve bilişim delili terimleri kullanılmaktadır. Bunlardan çoğunlukla, elektronik delil ve dijital delil kavramlarının tercih edildiği görülmektedir.

Elektronik kavramı, elektron hareketlerini esas alarak, türlü donanım yapma ilmini ifade etmektedir. Bu kavram; televizyon, radyo ve bilgisayar gibi birçok cihazın temelini meydana getirmektedir.[133] Velhasıl elektronik kavramı, maddenin elektriksel özellikleriyle güç iletiminin sağlanması ve bunu oluşturan sistemlerle ilgilenmektedir.[134] Elektronik hareketlerin matematiksel fonksiyon olarak gösterilmesine sinyal denilmektedir. Bu sinyaller, elektronik açısından veri hareketini simgelemektedir.[135]

---

[128] ORTA, s.238.
[129] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.155.
[130] ERDOĞAN, Y., 2018. Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri. İstanbul: Legal. s.222.
[131] DEĞİRMENCİ, Bilgi toplumunun delil türü: sayısal deliller ve bilimselliği, s. 16.
[132] ÖZTÜRK, M. İ., 2007. Bilişim cihazlarındaki sayısal delillerin tespiti ve değerlendirilmesinde iş akış modelleri. Yüksek Lisans Tezi Ankara: Üniversitesi SBE, s.38.
[133] KARAGÜLMEZ A., 2014. Bilişim suçları ve soruşturma kovuşturma evreleri. 5. Baskı. Ankara: Seçkin Yayıncılık., s.51.
[134] KAYNAKÇIOĞLU, U., 2015. Ceza muhakemesinde dijital deliller. Yüksek Lisans Tezi. İstanbul: Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü., s. 24.
[135] MASON, S., "Introduction", Stephen Mason (ed.), International Electronic

Söz konusu veriler ise, analog(örneksel)[136] ve dijital(sayısal) olmak üzere ikiye ayrılmaktadırlar. Bu kapsamda anlaşılacağı üzere, dijital veriler elektronik içerisinde kullanılan bir tür sinyal çeşididir.[137] Başka bir ifadeyle elektronik cihazlar, analog ve sayısal sinyalleri işleyebilmektedir.[138]

Analog sinyaller, giriş sinyalinin bazı başka sinyaller ile elektriksel işlemler geçirilerek değiştirilmesi ile elde edilir. Dolayısıyla, giriş sinyali ve çıkış sinyali arasındaki bu süreklilik bir matematiksel formül ile gösterilebilir. Ancak bu iki nokta arasındaki sinyallerin değerleri çok çabuk değişmekle birlikte, her an farklı olup bu nedenle sonsuz sayıda ara değer söz konusudur.[139]

Dijital(sayısal) kavramı, sayıları esas alan yöntemlerle çalışan[140] ve elektronik cihazlarda muhafaza edilmekte olan dijital verilerin temelini kapsamaktadır.[141] Bir şeyin sayılarla doğrudan olan bağlantısı ortaya koymaktadır.[142] Dijital sinyal, içerik olarak 0 ve 1'lerden oluşan ikili kod sisteminin kullanılmasıyla oluşturulur.[143] Dijital veriler ile analog veriler arasındaki en büyük fark, analog verilerin sürekli olan bir ölçekte ve iki nokta arasında tüm değerleri alabilecek şekilde var olmaları iken, dijital verilerin ise yalnızca belli değerlerden oluşan rakamlarla sınırlı olan, sürekli olmayan bir ölçekte ve kesikli olarak var olmalarıdır.[144]

Adli bilişim çalışmaları esasen dijital ortamdaki verilerin okunması şeklinde gerçekleşmektedir. Bu kapsamda bir suçun aydınlatılması için kolluk görevlisinin

---

Evidence, Londra: British Institute of International and Comparative Law, 2008. s. xxxv. https://www.biicl.org/files/3434_introduction_mason.pdf [21.9.2020] .aktaran KAYNAKÇIOĞLU U., s. 24.

[136] Analog devreler hakkında ayrıntılı bilgi için bkz: MANSON S., Ankara Barosu Uluslararası Hukuk Kurultayı 2008:Bilişim ve Hukuk, Ankara Barosu Yayınları, Cilt 2 Ankara, 2009.(8 Ocak - 11 Ocak 2008), ss.172-173.; Analog kavramı Benzer, eş" anlamlarına gelmektedir. https://sozluk.tdk.gov.tr/ [11.07.2020]; Bu bakımdan değişik yapılarda olmasına rağmen aynı görevi yapanlar analog olarak adlandırılmaktadır. KAYNAKÇIOĞLU, s. 25; Elektrik Elektronik Teknolojisi Analog ve Sayısal Haberleşme, http://www.megep.meb.gov.tr/mte_program_modul/moduller_pdf/Analog%20Ve%20Say%C4%B1sal%20Haberle%C5%9Fme.pdf(27.06.2019), ss.3-4.

[137] KAYNAKÇIOĞLU, s. 24.

[138] GÖKSU, M., 2010. Hukuk yargılamasında elektronik delil. Doktora Tezi. Ankara: Üniversitesi Sosyal Bilimler Enstitüsü, s.8; DEĞİRMENCİ, Bilgi toplumunun delil türü: sayısal deliller ve bilimselliği, s.17.

[139] KARAGÜLMEZ, s. 51.

[140] GÖKSOY, ss.91-93; KARAGÜLMEZ, s.51.

[141] SARSIKOĞLU, ss. 439-440.

[142] KAYNAKÇIOĞLU, s.25.

[143] Burada 1 ile akımın geçme anı, 0 ile ise geçmeme anı gösterilmektedir. KARAGÜLMEZ, s. 51.

[144] KAYNAKÇIOĞLU, ss.25-26.

edineceği deliller, dijital verileri barındıran elektronik cihazlardır. Şöyle ki, bir USB bellek söz konusu olduğunda, bellek içerisindeki yer alan dijital veriler, yapılan adli bilişim çalışmalarının temelini oluşturmakla birlikte fiziki olarak temas edilen bu USB bellek, bir elektronik delil olmaktadır. Zira suç ya da olay ile bağı araştırılacak olan araç, USB belleğin bizzat kendisidir. Bu açıklamalardan anlaşılacağı üzere "elektronik delil" kavramı, elektronik cihazı ve bu cihaz içerisinde bulunan dijital verileri kapsamaktadır.[145]

Elektronik deliller, içinde bulunduğu sistemin teknik özellikleri göz önünde tutularak isimlendirilmiştir. Bu kapsamda elektronik deliller; elektronik cihaz yoluyla işlenen, aktarılan ya da elektronik cihazlarda depo edilen delilleri belirtmektedir. [146] Ayrıca her bir dijital yapı aynı zamanda elektroniktir. Ancak her elektronik yapı aynı zamanda dijital yapı olmamaktadır.[147] Uygulamada, sayısal delil kavramı yerine elektronik kavramının kullanılmasının sebebi, analog cihazlarda tutulan delillere nadiren karşılaşılmasıdır.[148]

Doktrinde, dijital kavramını kullanmayı tercih eden yazarlar[149] bulunduğu gibi sayısal delil tabirini kullanan[150] yazarlar da bulunmaktadır.[151] Kanaatimizce, dijital(sayısal) delil ifadesini içine alan daha üst bir kavram olması sebebiyle[152] elektronik delil kavramının kullanılması daha yerinde olacaktır.

b. Elektronik delil-elektronik veri kavramları

Elektronik delil ve elektronik veri kavramları iki farklı kavramdır. Veri, daha önce belirttiğimiz üzere sistem içerisindeki bütün soyut unsurlar olup, “0” ve “1” ‘ler halinde bulunmaktadır. Elektronik delil kavramı ise elektronik bir materyal içerinde bulunan

[145] BAŞLAR, Ceza yargılamasında elektronik delil, s.66; AYDOĞAN, H., 2009. Adli bilişim’de yeni elektronik delil elde Etme yöntemleri. Yüksek Lisans Tezi. Ankara: Polis Akademisi Güvenlik Bilimleri Enstitüsü. s.30.
[146] DEĞİRMENCİ, Bilgi toplumunun delil türü: sayısal deliller ve bilimselliği, ss.16-17.
[147] KARAGÜLMEZ, ss. 51-52.
[148] DEĞİRMENCİ, Bilgi toplumunun delil türü: sayısal deliller ve bilimselliği, s. 17.
[149] AKARSLAN, s.136; HENKOĞLU T., Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi,2. Baskı, İstanbul, Pusula yayıncılık, Mart 2014, s.5; YETİM S., 2008. Dijital kanıt araştırma yöntemleri. İstanbul Barosu Dergisi. 82 (3), ss. 1201-1221, s. 1203.
[150] ORTA, s.239; KARAGÜLMEZ, s.52.
[151] ORTA, s.239.
[152] BAŞLAR, Elektronik delil ve ceza yargılamasında kabul edilebilirliğine ilişkin bir inceleme, s.1661; SARSIKOĞLU, ss. 439-440; KARAGÜLMEZ, s. 52; AYDOĞAN, s.30.

soruşturma açısından değeri olan veri ve bilgilerdir. Bu bakımdan elektronik veriler, elektronik delil kavramına dâhil olmaktadır. Elektronik deliller ise elektronik verilerin soruşturma açısından önemli olan kısmını oluşturmaktadır. Dolayısıyla adli bilişim incelemesi sonucunda hazırlanacak raporda, materyal içerisinde bulunan veriler arasından, suçla doğrudan ilgili olan verilere delil olarak yer verilmektedir.[153] DEĞİRMENCİ, veri ile elektronik delil arasındaki ilişkinin bir fonksiyon ilişkisi olduğunu, bu bağlamda elektronik delillerin veri niteliğinde bulunması gerektiğini, fakat maddi olay ile bağlantılı olan verilerin elektronik delil olabileceğini ifade etmiştir.[154]

c. Delil tasnifi bakımından elektronik deliller

Ceza muhakemesinde delillere ilişkin net bir tasnif bulunmamaktadır.[155] Deliller, doktrinde farklı şekillerde sınıflandırılmakta ve birçok delil çeşidi bulunmaktadır. Genel olarak deliller; beyan delilleri, belge delilleri ve belirti delilleri olarak üç gruba ayrılmaktadır. Beyan delillerini şüpheli-sanık, tanık ve diğer kişilerin beyanları olarak üç gruba ayırmak mümkündür.[156] Belge delilleri ise yazılı belgeler, şekil tespit eden belgeler ve ses tespit eden belgeler olarak ayrılmaktadır. Son olarak da belirti delilleri ise doğal ve suni belirti delilleri olarak ikiye ayrılmaktadır.

Bilimdeki gelişmeler sonucunda, elektronik ortamdaki birçok bilişim verisi suça ilişkin emare taşımaktadır.[157] CMK'nda bilişim sistemleri ve benzeri elektronik araçlar üzerinden edinebilecek delillere türlü hükümlerde yer verilmesine rağmen, elektronik delillerin ne tür bir delil olduğuna dair bir ibare yer almamaktadır.[158] Bu hususta öğretide, elektronik delillerin; belge delil kategorisinde değerlendirilmesi gerektiğini ifade eden görüş[159] olmakla birlikte, belirti delil kategorisi kapsamında kabul edilmesini

[153] GÖKSOY, ss. 90-91.
[154] DEĞİRMENCİ, Bilgi toplumunun delil türü: sayısal deliller ve bilimselliği. Terazi Hukuk Dergisi, s.16.
[155] GÖKSOY, s.88.
[156] YENİSEY/NUHOĞLU, ss. 492 -494.
[157] YENİSEY, Ceza muhakemesi hukuku başvuru kitabı, s.134
[158] KIZILYAR, s.75.
[159] GÖKSOY, ss.88-89.; Elektronik deliller, özellikleri gereği yazı, şekil ve ses biçimde karşımıza çıkabileceğinden dolayı, belge delil kategorisinde değerlendirilmesi gerekir. Bilişim verisi şeklindeki veriler, bir kişinin irade açıklaması içeren ve düzenleyeni bir takım yöntemlerle tespit edilebilir niteliktedir. Bu tür veriler, teknik olarak belge niteliğindedir. Ayrıca bu belgeler, özellikle bir bilgisayardan yararlanılarak word, excel gibi bilgisayar programlarının kullanılması suretiyle düzenlenmekle birlikte, bilgisayarın içerisinde saklanır. YENİSEY/NUHOĞLU, s.522; BAŞLAR, elektronik delilleri bilişim verisi şeklindeki belge olarak dördüncü bir başlıkta yer verilmesi gerektiğini ifade etmiştir. BAŞLAR, Ceza yargılamasında elektronik delil, s.40; AKARSLAN elektronik delilleri,

savunan görüşte mevcuttur.[160] Kanaatimizce, bilişim sisteminde yer alan ve diğer belgelerden farklı olarak, teknik bir çalışma ve uzman kişilerce çözümlenen[161] değişik formattaki içeriklerin oluşturduğu elektronik verilerden elde edilen bu çözüm belgelerinin, belge delil kategorisinde dördüncü bir ayrım olarak, değerlendirilmesi gerekir.

Kaynakları bakımından deliller, insan kaynaklı ve nesne kaynaklı deliller olarak ikiye ayrılmaktadır. İnsan kaynaklı deliller; tanık, sanık ve diğer kişi beyanlarıdır. Nesne kaynaklı deliller ise belge ve beyan dışında kalan nesnelerden oluşmaktadır.[162] Bu bakımdan elektronik delillerin, nesne kaynaklı deliller olduğunu kabul etmek mümkündür. İspat güçleri bakımından ise deliler, doğrudan ve dolaylı deliller olarak ikiye ayrılmaktadır. Doğrudan deliller, uyuşmazlık konusu olayı direkt aydınlatan delillerdir. Dolaylı deliller ise uyuşmazlık konusu olayın doğrudan aydınlatılmasını sağlamamakta, fakat aydınlatılmasına katkı sağlayan delillerdir. Bu ayrıma göre nasıl ki beyan delilleri somut olayın özelliklerine göre doğrudan veya dolaylı delil vasfını taşıyor ise, elektronik delillerde vuku bulan olayın özelliklerine göre doğrudan veya dolaylı delil olarak karşımıza çıkabilmektedir.[163]

Elektronik deliller senet, ikrar, tanık beyanı gibi spesifik belli bir delil tipini ifade etmemekte; uyuşmazlık konusunu aydınlatabilecek olan delilin, elektronik bir özellik

---

kâğıt üzerinde çıktı şeklinde hazırlanmasından ötürü "veri tespit eden belge" şekilde ifade etmektedir. Bununla birlikte söz konusu deliller, bilişim aygıtlarında bulunan verilerin, kâğıt üzerine basılmış halidir. AKARSLAN, s.135.

[160] KAYNAKÇIOĞLU, s.46; DEĞİRMENCİ elektronik delillerin ne tür bir delil olduğu hususunda bir ayrım yapmaktadır. Öyle ki; elektronik veri, bilişim sisteminin suçun işlenmesinde araç olarak kullanılması ya da bilişim sisteminin suçun hedefi olması durumlarında belirti delili olduğunu, ancak bilişim sisteminin başka bir suça ilişkin delili barındırıyor olması halinde ise, belge delili kategorisinde olabileceğini ifade etmektedir. DEĞİRMENCİ O., 2014. Ceza muhakemesinde sayısal (Dijital) delil. Seçkin Yayıncılık, ss.393-394; DEĞİRMENCİ, Bilgi toplumunun delil türü: sayısal deliller ve bilimselliği, s. 18; ÖZBEK'e göre elektronik ortamda "*elde edilen verilerin tespitinin bilgisayar disketi ve CD ile yapılmakta olması, hatta gerekirse bir printer ile yazılı belge haline de dönüştürülebilmesi bunları yazılı belge durumuna sokmaz. Çünkü, söz konusu gönderinin içeriğinin değiştirilebilme ve yine göndericinin adı bulunan şahıs yerine bir başkası olma ihtimali söz konusu verinin tek başına delil olma gücünü zayıflatmakta, hatta ortadan kaldırmaktadır. Bu durumda, bu şekilde elde edilmiş olan tespitler tek başına mahkûmiyet kararı verilmesi için yeterli olmayıp, bunların başka delillerle desteklenmesi gerekir*." Bu sebeple, elektronik delillerin suç fiilinin dolaylı olarak ispatına yardımcı olan emare, iz şeklinde bir belirti olabileceğini ifade etmiştir. ÖZBEK V. Ö., (2002) "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt. 4, Sayı. 1, ss.143-144.

[161] KIZILYAR, s.75

[162] BAYRAKTAR B, 2011. Muhakemelerde delillerin önemi, Sosyal Bilimler Dergisi, Sayı: 25, http://journals.manas.edu.kg/mjsr/oldarchives/Vol12_Issue25_2011/03_bayraktar.pdf [12. 10. 2020]s. 36.

[163] GÖKSOY, ss.86-89.

taşıdığını ifade etmektedir.[164] Bunların yanı sıra belirtilmelidir ki, ceza muhakemesi hukukunda delil serbestisi ilkesi gereğince hangi sınıflandırmanın esas alınacağının yargılama açısından önemi olmamakta, hâkim delilleri serbestçe değerlendirmektedir.[165] Bu bağlamda bilişim sistemi üzerinden arama ve elkoyma tedbiri ile elde edilen delillerin diğer delillerden bir farkı bulunmamaktadır. Hâkim, vicdani kanaatine göre bu delileri değerlendirecektir.[166]

d. Elektronik delillerin bulunduğu ortamlar

Günlük faaliyetlerimizi gerçekleştirirken bilerek veya farkında olmadan elektronik deliller oluşturmaktayız. Telefon görüşmeleri, banka kayıtları, elektronik posta yazışmaları, bir belgenin çıktısını alınması, GPS özelliğe sahip bir otomobil kullanma, kimlik kartlarındaki Radyo Frekansı ile Tanımlama (RFID) çipleri kullanılması ya da bir kimsenin internet ortamında oyun oynaması, video izlemesi, internetten alışveriş yapılması,[167] sosyal medyanın kullanılması,[168] elektronik belge kullanımının artması, iletişimin büyük kısmının elektronik ortamda gerçekleşmesi[169] veya şirketlerin kayıtlarını sunucu bilgisayarlarındaki uygulamalarında tutması[170] bunlara örnek olarak verilebilir.

Bunlarla birlikte bilgisayar teknolojisi, günümüzde tüm elektronik aygıtlarla entegre olmuş durumdadır. Yaşamın her alanında kullanılan araç ve aygıtlar artık bilgisayar teknolojisiyle ile çalışmaktadır.[171] Yeni çıkan buzdolabı, mikro dalga fırını[172] gibi ev aletleri bünyelerinde elektronik saklama alanları bulundurmaktadır.[173] Bu şekilde

[164] ARSLAN, Ç., "Dijital Delil ve İletişimin Denetlenmesi", Ceza Hukuku ve Kriminoloji Dergisi, Cilt: 3, Sayı: 2, 2015, ss. 253-266, s.255.; GÖKSU, ss. 37-38.
[165] GÖKSOY, s.89; ŞAHİN/GÖKTÜRK, s.177.
[166] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.529.
[167] GÖKSU, s.1.
[168] Sosyal medya ile bireyler kişisel düşüncelerini, görüntülerini ve özel yaşamlarına dair birçok veriyi bilgisayar ortamında başkaları ile paylaşmaktadır. ARAALAN, s.204. benzer açıklamalar için bkz; DEĞİRMENCİ, Bilgi toplumunun delil türü: sayısal deliller ve bilimselliği, s.20.
[169] BAŞLAR, Elektronik delil ve ceza yargılamasında kabul edilebilirliğine ilişkin bir inceleme, s.1657.
[170] DÜLGER, adli bilişim ve ülkemizdeki uygulaması, s.20.
[171] APİŞ Ö., 2018, "Bilişim Sistemine Girme Suçu Bakımından Bilgisayarda, Bilgisayar Programlarında ve kütüklerinde Arama Kopyalama ve El koyma Tedbiri", Yasama Dergisi, Sayı:37, ss. 49-86, s. 80.
[172] UZUNAY Y./BIÇAKCI K. A3D3M:Açık anahtar altyapısı destekli dijital delilleri doğrulama modeli. http://www.emo.org.tr/ekler/4843973f9b66701_ek.pdf [2.07.2019]
[173] ORTA, s.159.

bilgisayar dışındaki bilişim sistemlerinden de elektronik delil elde edilmesine karşın,[174] elektronik delilin bulunduğu ortamların başında bilgisayar gelmektedir.[175] Nitekim iç hukuk sistemimizde olduğu gibi birçok hukuk sisteminde de elektronik delil aranması veya elde edilmesi, bilgisayarda arama kavramını akla getirmektedir.[176] Bilgisayar günlük yaşamın birçok alanında işlemleri kolaylaştırması sebebiyle kullanılmaktadır. Bu aygıtlar ile birçok sektöre ilişkin veri tabanları tutulmakta, işler idare edilmekte, yapılan işlemler kaydedilmekte, iletişim sağlanmakta, veri transferleri gerçekleştirilmekte ve başka birçok faaliyet bu aygıtlar üzerinden yürütülmektedir. Tüm bu işlemler geride bir takım izler bırakmaktadır. Geriye dönük olarak yapılan işlemlerin nelerden ibaret olduğu, bu aygıtların incelenmesiyle mümkün olmaktadır.[177]

Elektronik deliller doğası gereği görsel ve işitsel olarak karşımıza çıkabilmektedir.[178] Elektronik veriler genel olarak: video görüntüleri, fotoğraflar, çeşitli bilgisayar programları, iletişim kayıtları, elektronik postalar, elektronik mesajlar, yazı dosyaları, grafik ve çizimler, tablolar gizli ve şifreli dosyalar veya klasörler; dosyaların oluşturulma, değiştirilme ve erişimine dair her türlü veri bilgileri; son ve sık kullanılan internet siteleri, internet ortamından indirilen içerik ve dosyalar, silinmiş içerikler ve dosyalar, ağlara erişim kayıtları, IP bilgileri, donanımlara ait seri veya kullanım numaraları, yazılımlara ait sürüm bilgileri gibi verilerdir.[179]

Elektronik delillerin elde edilebileceği ortamlar ise genel olarak şu şekilde sayılabilir. Bilgisayarın iç donanımları olarak, sabit disk (hard disk) ve RAM bunların başında gelmektedir. Ayrıca Floppy ve CD/DVD/BluRay,[180] hafıza kartları,[181] Taşınır Bellekler

[174] İnsanlar siber suçları yalnızca bilgisayarda gerçekleşen bir şey olarak görmemelidir. Akıllı cihazların ve internetin yaygın kullanılması, çevrimiçi pazarın milyar dolarlık bir endüstri olarak olgunlaşmasını ve siber suçların daha cazip hale gelmesini sağlamıştır. GÜNŞEN İÇLİ, s. 573.
[175] BAŞLAR Y., Ceza Yargılamasında Elektronik Delil, s.69; YENİDÜNYA/DEĞİRMENCİ s.44.
[176] DEĞİRMENCİ, Ceza Muhakemesinde Sayısal(Dijital) Delil, s.31.
[177] KIZILYAR, s.81.
[178] ÖZTÜRK, Bilişim cihazlarındaki sayısal delillerin tespiti ve değerlendirilmesinde iş akış modelleri, s.55.
[179] KIZILYAR, s. 80.
[180] Floppy disketler ve CD/DVD/BluRay, taşınabilir depolama araçlarıdır. Bu araçlara manyetik alan ya da lazer işleme yöntemi ile veri kaydedilebilir. DÜLGER, Bilişim suçları ve internet iletişim hukuku, s.568.
[181] Hafıza kartı, bellek kartı ya da flash kart, dijital bilgileri depo edilmesi amacıyla kullanılan bir elektronik veri kayıt ortamıdır. Ekseriyetle dijital kameralar, cep telefonları, tabletler, MP3 çalarlar, dizüstü bilgisayarlar ve video oyunu konsolları gibi taşınabilir elektronik aygıtlarda kullanılmaktadır. https://tr.wikipedia.org/wiki/Bellek_kart%C4%B1 [16.05.2020].

(Flash Memory),[182] Cep Telefonları, SIM Kartlar,[183] Dijital Kamera ve Fotoğraf Makineleri,[184] Mp3 Çalar/IPod,[185] Yazıcı ve Fakslar,[186] Oyun Konsolları, bilgisayar ağları, GPS (Global Positioning System) cihazları,[187] bulut bilişim ve modemler, kredi kartı kopyalama cihazları, telesekreterler[188] ve diğer teknolojik cihazlar da denilen akıllı saat, akıllı bileklik gibi cihazlardan da elektronik delil elde edilebilir.[189]

e. Elektronik delillerin özellikleri

Elektronik delillerin yapısal özellikleri, Amerika Birleşik Devletleri Adalet Bakanlığı'na bağlı Ulusal Adalet Enstitüsü[190] çıkardığı, "Elektronik Olay Yeri Soruşturması" kılavuzunda dört maddede belirtilmiştir.[191] Bunlara değinecek olursak:

i. Elektronik deliller, parmak izi veya DNA gibi gizli (latent) yapıdadır.[192]

Elektronik aygıt içerisinde saklı bulunan elektronik delilin doğrudan doğal biçimleriyle keşfedilmesi mümkün değildir.[193] Bu delillerin görünür hale getirilebilmesi için belirli

[182] Elektrik gücü kesilse bile içinde sakladığı veriyi tutan ve bu veriler üzerinde değişiklik yapılabilmesini mümkün kılan bir bellek birimidir. Bu bellekler küçük ve hafif veri depolama aygıtları olup, veri depolamaya ve saklamaya ya da bir cihazdan başka bir cihaza veri aktarmada bir araç olarak kullanılmaktadır. http://flashbellek.org/flash-bellek-nedir/ [16.05.2020].

[183] SIM kartları, bir cep telefonunun GSM şebekesinden hizmet alabilmesi için gerekli olan abone kartıdır. SIM kartlar dâhili bir belleğe sahiptir. Bu belleklerde telefon rehber bilgileri, son arama bilgileri (arayan, aranan ve cevapsız çağrı bilgileri), kısa mesajlara (SMS) ve GSM şebekesine ait bilgiler bulunmaktadır. AYDOĞAN, s. 80.

[184] Dijital kameralar ve fotoğraf makinelerinde bulunan görüntülere, video kayıtlara, ses kayıtlarına, hafızalarındaki silinmiş verilere ve bunlara ilişkin zaman damgası bilgilerine erişilebilir. BAŞLAR, Ceza yargılamasında elektronik delil, s.81.

[185] Yüksek saklama kapasitesi sayesinde yalnızca müzik/video değil, doküman/veri saklamak için de kullanılabilirler. SAMET R,, Bilgisayar Sistemleri (2-2–3) http://android.eng.ankara.edu.tr/wp-content/uploads/sites/656/2018/02/1-Giris.pdf [10.07.2020].

[186] Bu aygıtlar sınırlı da olsa, veri depolama (hafıza) üniteleri sahiptir. Yazıcı ve fakslar hafızalarında işleme tabi tutulan son belgeler, gelen giden faks kayıtları, ağ bağlantıları gibi verileri barındırabilirler. GÖKSOY, s.101; ORTA, s.208.

[187] Kiralanan araçlarda, toplu taşımalarda veya taşımacılık, nakliye vb. birçok sistemde de GPS birimi, ilgili araçlara entegre durumdadır. Bu bağlamda, GPS birimlerinin araçların ziyaret ettikleri yerleri zaman bilgisiyle tutması nedeni ile, ölümcül kazalar gibi önemli adli durumlarda ilgili aracın o anda o yerde olup olmadığı ve hareketli bir cismin takibinde önemli bir delil tespit aracı olarak kullanılabilir. ÖZEN/ÖZOACAK, s.49.

[188] BAŞLAR, Ceza yargılamasında elektronik delil ss.76-84; benzer açıklamalar için bkz HENKOĞLU, ss.5-6

[189] GÖKSOY, s.101; KARAGÜLMEZ7, s.510; ORTA, ss.190-213.

[190] ÇAKIR/SERT, Bilişim suçları ve delillendirme süreci, s.147.

[191] ASHCROFT J .(Ed.), "Electronic Crime Scene Investigation: A Guide for First Responders", Washington: PhotoDisc, Inc, 2001, https://www.ncjrs.gov/pdffiles1/nij/187736.pdf, [29.06.2019] s. 6; BAŞLAR, Ceza yargılamasında elektronik delil, ss. 86-87; AYDOĞAN, s.31; BAYRAM L.(Ed.). 2008. Ses görüntü ve data incelemeleri. Ankara: Adalet Yayınevi, s.256.

[192] KESER BERBER, s.44.

yöntemler dâhilinde nicel gözlem yapılmalı ve bir uzman tarafından değerlendirilmesi gerekmektedir.[194]

ii. Kırılgan ve kolayca değiştirilebilir, hasar görülebilir veya yok edilebilir.

Kolaylıkla değiştirilebilir, bozulabilir, kopya edilip çoğaltılabilir ve yok edilebilir niteliktedir. Elektronik deliller üzerinde gizlenmiş veya şifrelenmiş başka veriler barındırabilir.[195] Ayrıca elektronik delillerin özellikle sıcaklık, nem, manyetik alan gibi sebeplerle bozulması mümkündür.[196]

iii. Kolaylığı ve hızı ile sınırları aşabilir.

Dünya çapında bir alana dağılmış olabilir. Bilişim, iletişim teknolojilerinin gelişmesi ve küresel bir ağ haline gelen internetin kullanımıyla[197] elektronik veriler dil, ülke, milliyet ve coğrafi konum gibi kavramlarla[198] sınırlandırılamaz[199] bir hale gelmiştir. Bu sebeple elektronik ortamda gerçekleşen suçlarda, mekân ve mesafe kavramları anlamını kaybetmektedir.[200]

iv. Bazen zamana duyarlıdır.

Günümüzde bilgisayar yazılımlarının sayısı azımsanamayacak seviyededir.[201] Bazı yazılımların arka planlarında ne çeşitli işlemlerin gerçekleştirdiğinin anlaşılması pek kolay olmamaktadır. Olay yerlerinde karşılaşılan bilgisayar ekranında, rastgele bir işlem yapıyor gibi gözüken bir program aslında o anda bilgisayar sistemi içerisinde bulunan,

---

[193] "*Bu delillere ulaşmak ve gerçekliklerini sorgulamak amacıyla tarafların dinlenilmesi gerekebilir. Kayıtlar bazı hallerde üçüncü kişiler tarafından tutulduğu için (örneğin internet servis sağlayıcı veya elektronik*
imzada sertifika hizmet sağlayıcısı gibi), bu üçüncü kişilerin bilgi ve belgelerine ihtiyaç duyulabilir" GÖKSU, s.3.

[194] SAY K., 2006. Bilişim suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, yayınlanmamış yüksek lisans tezi, ss.29-30.

[195] GÖKSOY, s.95.

[196] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.146; DEĞİRMENCİ, Bilgi toplumunun delil türü: sayısal deliller ve bilimselliği, s.21; UZUNAY/BIÇAKÇI.

[197] BAYRAM, Ses görüntü ve data incelemeleri, s.257.

[198] YILDIZ S., Suçta araç olarak internetin teknik ve hukuki yönden incelenmesi, sayı:17, s. 609-623. ss.609-607, http://dergisosyalbil.selcuk.edu.tr/susbed/article/view/507/489 [28.12.2020]

[199] "*Siber alan sınırlara meydan okumuş ve coğrafyayı(yeri) ilgisiz kılmıştır*." GÜNSEN İÇLİ, s.573.

[200] KALAMIŞLIK Ö,, "Bilişim Hukukunda Delillerin Toplanması", Ankara Barosu Uluslararası Hukuk Kurultayı, Cilt. 2, Ankara, 08-11 Ocak 2008, ss. 159-160; ÖZTÜRK, Bilişim cihazlarındaki sayısal delillerin tespiti ve değerlendirilmesinde iş akış modelleri, s.40.

[201] BAYRAM, Ses görüntü ve data incelemeleri, s.257.

suça ilişkin verileri siliyor olması mümkündür. Bu durum ise elektronik delilin zamana bağlı olduğunu belirtmektedir. [202]

Bunlarla birlikte, elektronik delillerin, yargı makamlarınca kabul görmesi için bazı nitelikleri bünyesinde barındırması gerekmektedir.[203] Bu delillerin eğer doğru, güvenilir olduğu ve şüphe barındırmadığına kanaat getirilir ise, ihtiva ettiği kanıtların tutarlı olduğu kabul edilir.[204] Elektronik delillerin, ispatı sağlamaya yönelik, olayla bağlı[205] olması ve gerçeği temsil etmesi gerekir.[206] Bu bağlamda delillerin taklit olmaması, orijinallerinin kullanılması gerekmektedir. Uyuşmazlık konusuna ilişkin maddi olayı sübuta erdirecek olan en güvenilir delil şüphesiz ki delilin orijinali olsa da, elektronik ortamda bulunan e-delillerin orijinalinin aranması halinde bu delillerin hiçbir zaman kullanılamaması sonucunu da doğurabilmektedir. Ayrıca elektronik deliller tümüyle kopya edilebilme özelliğini taşımaktadır. Böylece adli bilişim uzmanlarının, elektronik verilerin kopyasını oluşturması ve bunlar üzerinden işlem yapabilmesi mümkündür. Bu sebeple elektronik deliller için kopya, suret ve nüsha gibi kavramların kullanıldığı görülmektedir. Bunların yanı sıra bir bilim tarafından kabul edilebilir yöntemle elde edilmiş deliller ceza muhakemesinde kullanılabilmektedir. Bu bakımdan bilirkişi niteliğine sahip adli bilişim uzmanının delili elde etme ve çözümleme yolu sonucunda ortaya konulan bulgular, hakim tarafından anlaşılabilir ve inanılabilir nitelikte olup, maddi gerçeği ortaya çıkarılmasında verilecek hükmü etkileyecektir.[207] Elektronik delillere bilimsel açıdan itibar edilebilmesi için tekrar edilebilme özelliğine sahip olmaları gerekir.[208] Bu bağlamda adli bilişim uzmanının uyguladığı metot ve yöntemler, farklı kişiler tarafından farklı yer ve zamanda uygulandığında; aynı sonuçların elde edilmesi, elektronik delillerin tekrar edilebilir nitelikte olmasını sağlamaktadır.

---

[202] BAŞLAR, Ceza yargılamasında elektronik delil, 87; BAYRAM, Ses görüntü ve data incelemeleri, s.258; SAY, ss 31-32.
[203] KARAGÜLMEZ, s.509; HENKOĞLU, s.6.
[204] KOZUSHKO H., http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/DigitalEvidencePaper.pdf [24.07.2020] s.3; BAŞLAR, Ceza yargılamasında elektronik delil, s. 88.
[205] BAŞLAR, Ceza yargılamasında elektronik delil, .s.88; SAY, s.43.
[206] ORTA, s.241.
[207] SARSIKOĞLU, ss.436-439; HENKOĞLU, s.7.
[208] ARAALAN, s.206.

Elektronik delillerin elde edilmesinde ve analiz aşamasında yapılan işlemler sırasında, sanık ve şüpheli ile alakalı olabilecek tüm deliller eksiksiz toplanmalı ve sunulmalıdır. Bu sunulan delillerin değiştirilmemiş, bütünlüğü bozulmamış olması gerekir.[209] Başka bir anlatımla bu deliller, suça konu fiilin işlenmesine ilişkin olarak tek bir açıdan değerlendirilmemeli, kişinin masumiyetini de ortaya çıkarabilecek şekilde; eksiksiz ve tam olmalıdır. Bu bakımdan söz konusu delillerin özellikle toplama ve analiz edilmesi sürecindeki gerçekliği ile güvenirliğine gölge düşürülmemesi gerekir.[210] Tüm bunların yanı sıra çalışmamızın ana konusunu oluşturan CMK m.134'te yer alan hususlara aykırı olarak bir bilişim sisteminde arama, kopyalama ve el koyma işlemi gerçekleşmişse, elde edilen elektronik delil yukarıda belirtilen özellikleri barındırsa dahi yasal kurallara[211] uygun olmayacaktır.[212]

f. Elektronik deliller ile fiziksel deliller arasındaki farklar

i. Fiziksel deliller somut niteliktedir. Elektronik deliller ise üzerlerinde işlem yapılmadan gözle görülemeyen soyut niteliktedir. Şöyle ki, elektronik delilleri barındıran somut bir donanım cihazı bulunmakta ise de, asıl muhakemeye konu olan bu donanım cihazı değil bu cihazın içerisinde bulunan elektronik verilerdir.[213]

ii. Elektronik ortamda verileri saklayabilmek çok kolaydır. Fiziksel deliller bakımından bu durum söz konusu değildir.[214] Nitekim kütüphane dolusu kitaba karşılık gelen elektronik veriler, küçük boyutlardaki hafıza kartlarında taşınabilmektedir.[215]

---

[209] ARAALAN, s.205
[210] HENKOĞLU, s.7.
[211] Yargıtay bir kararında da; "*Ceza muhakemesinde deliller kanuna uygun olmalı ve kanuna uygun yöntemlerle elde edilmelidir. Adil yargılanmanın sağlanabilmesi, soruşturma ve kovuşturma aşamalarında toplanan bulguların delil değeri taşıyabilmesi için, şüpheli veya sanıktan elde edilen dijital verilerin, yasa ile sınırları belirlenmiş teknik gerekliliklere uygun olarak toplanması ve sonucunda yargılama makamlarına eksiksiz, bozulmamış halde sunulması gerekmektedir. Yasa koyucunun, CMK'nın 134. maddesini ayrıntılı olarak düzenlemesinin amacı da budur*." şeklinde hüküm vererek, verilerin; yasa ile sınırları belirlenmiş teknik gerekliliklere uygun olarak ve veri bütünlüğü bozulmaksızın yargılama makamlarına sunulması gerekliliğini belirtmiştir. Yargıtay 16. CD, 21.04.2016, E. 2015/4672, K. 2016/2330 kararı aktaran BAŞLAR, Elektronik delil ve ceza yargılamasında kabul edilebilirliğine ilişkin bir inceleme, s.1679
[212] BAŞLAR, Ceza yargılamasında elektronik delil, ss. 88-89; KARAGÜLMEZ, s.509.
[213] BAŞLAR, Elektronik delil ve ceza yargılamasında kabul edilebilirliğine ilişkin bir inceleme, s.1659; ORTA, s.243; ÖZOCAK, Ceza Muhakemesinde Elektronik Delillerin tespiti ve Toplanması, İzmir 2. Uluslararası Bilişim Hukuku Kurultayı, 17-19 Kasım 2011, Bildiriler Kitabı(Editörler: Tekin Memiş, Ahmet, Ahmet Koltuksuz, Mine Akkan), s.114https://docplayer.biz.tr/811097-Izmir-2-uluslararasi-bilisim-hukuku-kurultayi-17-19-kasim-2011-bildiriler-kitabi.html [24.11.2020]; SAY, s.39.
[214] SAY, s.44.

iii. Elektronik delilin elde edilmesi, incelemesi, değerlendirilmesi ve raporlanması fiziksel delile göre daha karmaşık bir husus olup, teknik uzmanlık gerektiren bir alandır.[216]

iv. Elektronik deliller her an, özellikle de elde edilme aşamasında kasıtlı[217] veya kasıtsız olarak kolaylıkla değişikliğe uğrayabilir.[218] Buna karşın fiziksel delillerin genellikle sabit bir yapısı olmasından ötürü değiştirilmesi nispeten daha zordur. Bununla birlikte, fiziksel delilde değişiklik yapıldığında bu durumun tespiti kolaydır. Ancak elektronik deliller, yapısı gereği saptanması basit olmayan bir takım değişikliklere maruz kalabilir.[219]

v. Elektronik delil elde etmek amacıyla üzerinde inceleme yapılacak olan elektronik materyalde, suça ilişkin delilinin mevcut olup olmadığı kesin değildir.[220] Bu bakımdan söz konusu aygıtın suçu aydınlatmada aracı olup olmayacağı, fiziksel delile göre daha meçhul durumdadır.[221]

vi. Ceza yargılamasında mahkûmiyet hükmü, kesin ve açık bir ispata dayanmalıdır. Bu bakımdan fiziksel delilin, genellikle kuşkudan uzak, kesin ve inandırıcı olmasını sağlamak mümkünken, elektronik delilin sürekli olarak güvenilirliğini ve şüpheden uzak olmasını sağlamak mümkün değildir. [222]

---

[215] ERDOĞAN, Türk Ceza Kanunu'nda bilişim suçları s.405; ÖZBEK M., 2013. Adli bilişimde delillerin toplanması ve incelenmesi. Yüksek Lisans Tezi. İstanbul: Bilgi Üniversitesi SBE. s.18.

[216] ORTA, ss.242-243; ÖZBEK, Adli bilişimde delillerin toplanması ve incelenmesi, s.18.

[217] Elektronik biçimde saklanan herhangi bir veri ve bilginin somut olmayan doğası, geleneksel delili biçimlerine göre manipüle etmeyi ve değiştirmeyi daha yatkın hale getirebilir. CoE(Council of europe),(2013), Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors and judges. Data Protectionsn and Cybercrime Division. s.12.

[218] GÖKSOY, s.95; ORTA, s.242.; KARAGÜLMEZ, s.508; TANRIKULU, s.52.; DEĞİRMENCİ, Bilgi toplumunun delil türü: sayısal deliller ve bilimselliği, s.22. "*Dijital veriler, nasıl kodlandıklarına bağlı olarak anlam kazanabilirler. Günümüzde virüs, truva atı gibi zararlı kodlar sayesinde verilere değişik anlamlar yüklemek mümkündür*." UZUNAY/BIÇAKÇI.

[219] KARAGÜLMEZ, s.508; ÖZBEK, Adli bilişimde delillerin toplanması ve incelenmesi. s.18.

[220] KARAGÜLMEZ, s.508

[221] ORTA, s.244.

[222] BAŞLAR, Ceza yargılamasında elektronik delil, s.88.; DEĞİRMENCİ, Bilgi toplumunun delil türü: sayısal deliller ve bilimselliği, s. 22.;ERDOĞAN, Türk ceza Kanunu'nda bilişim suçları, s.406.;ÖZTÜRK, Bilişim cihazlarındaki sayısal delillerin tespiti ve değerlendirilmesinde iş akış modelleri, s. 41.

g. Elektronik delillerin geçerliliği

Adli inceleme sonucunda elde edilen elektronik delillerin, mahkeme huzuruna sunulduğunda ilk müdahale esnasındaki halde olduklarının, yani hiçbir değişikliğe maruz kalmadıklarının, her türlü şüpheden uzak bir şekilde doğrulanması gerekmektedir. Böylece, elektronik delillerin geçerliliği sağlanmaktadır. Bu konuda öğretide bir görüş, hassas yapıya sahip elektronik delillerin mahkemece kabul edilmeleri için bir takım doğrulama mekanizmalarına ihtiyaç duyulduğunu ifade etmektedir. Söz konusu mekanizmalar ile elde edilen delillerin hukuka uygun olup olmadığı ve delil niteliğine haiz olup olmadığı belirlenmektedir.[223] Bu görüşe göre, teknolojik gelişmelere paralel olarak değişik doğrulama mekanizmaları geliştirilecektir. Uygulamada ise en çok başvurulan doğrulama araçları; elektronik imza,[224] hash bilgisi, süreç bilgisi,[225] üst veri bilgisi[226] ve ilişki bilgisi[227] olmaktadır.

Öğretide bir başka görüş, elektronik delillerin teknolojik geçerliliğini; bütünlük, doğrulanma, inkâr edilememe, doğruluk ve daha sonra ele alınabilirlik ilkelerine bağlılığının kontrol edilmesiyle sağlandığını ifade etmektedir.[228] Bu ilkelere değinecek olursak:

Elektronik delillerin bütünlüğü ilkesi: Elektronik delilin elde edildiği andan başlayarak, fiziki olarak ve elektronik bakımdan muhafaza edilmesini ifade etmektedir. Böylece

---

[223] GÖKSOY, ss.110-111. ;ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s. 147; AYDOĞAN, s. 32.

[224] "*Sadece imza sahibinin tasarrufunda bulunan, özel bir araçla oluşturulan, nitelikli elektronik sertifikaya dayanılarak imza sahibinin kimliğinin tespitini ve imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespiti sağlayan imza*" ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s. 155.

[225] Delil zinciri de denilen süreç bilgisi; elektronik delil ile kurulan bütün temasların kaydedilmesiyle, bu süreçlerin öğrenilmesine imkân sağlanmaktadır. Bu bilgi ile, elektronik delillerin ilk elde edinildiği andan itibaren mahkeme huzuruna sunulmasına kadar geçen zaman diliminde kaç kez el değiştirdiğini ve tarihler ile kullanıcı bilgilerine ulaşılması mümkündür. GÖKSOY, s.114.

[226] GÖKSOY, ss.114-115;Üst veri bilgisi, meta data veya gömülü veri de denilmektedir. Bu bilgi, kullanıcıların veriler hakkında ek bir takım bilgiler edinilmesini sağlamaktadır. Örneğin bir fotoğrafın çekildiği tarih, fotoğraf verisine işlenmiş olan GPS bilgisi, çekim yapan makinenin markası ve modeli ve ya elektronik postanın iletilmesinde izlediği güzergâh ya da verilerin, hangi bilgisayarda oluşturulduğuna dair bilgiler üst veri bilgisidir. ÇAKIR/KILIÇ Adli bilişim ve elektronik deliller, ss.150-151.

[227] Elektronik delillerin sahibi ve suç ile ilişkisinin tespit edilmesi gerekmektedir. Bunun için suçun işlendiği yer, elektronik delili elde eden birim, delillerin üzerindeki parmak izleri, söz konusu delillerin diğer bilgisayar medyalarıyla olan ilişkisi, elektronik delillere ait üst veri bilgisi, delillerin bulunduğu ortamdaki kamera kayıtları ve gerektiğinde tanık beyanlarından dahi yararlanılmalıdır. Böylece elektronik delillerin içeriği ile mantıksal bir ilişki kurulabilecektir. GÖKSOY, s. 115; ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, ss.153-154

[228] ÖZTÜRK, Bilişim cihazlarındaki sayısal delillerin tespiti ve değerlendirilmesinde iş akış modelleri, ss. 39-40; BAŞLAR, Ceza yargılamasında elektronik delil, s.94.

delilin, değişime uğramadığı saptanmaktadır. Bu delillerin bütünlüğü için, çoğunlukla kriptografi[229] bilimi altındaki güvenlik tekniklerinden yararlanılmaktadır. Fiziki olarak korunmasından maksat ise elektronik delillerin analiz edileceği yere bozulmadan nakledilmesi, uygun ortamlarda[230] muhafaza edilerek, mahkeme huzuruna sunulmasına kadar geçen süre zarfında değişikliğe maruz kalmaması anlamına gelmektedir. [231]

Elektronik delillerin doğrulanması ilkesi: Elde edilen elektronik delilin, adli süreç kapsamında gerçekten şüpheliye[232] ve/veya iddia edilen suça ilişkin olduğu ispatlanmalıdır. Dolayısıyla, elektronik delil sahibi ile suç arasındaki bağ tespit edilmelidir. Çünkü elde edilen bu delillerin, herhangi bir kişi veya kolluk görevlileri tarafından oluşturulduğu ileri sürülebilir.[233]

Elektronik delilin inkâr edilememesi ilkesi: Elektronik delillerin ele geçirilmesi esnasında başvurulan, teknik detaylar ile metotların doğruluğu ve hatta gerekli olduğunda adli sürecin tamamı kanıtlanmalıdır.[234] CMK m. 169/2'de "*Her soruşturma işlemi tutanağa bağlanır. Tutanak, adlî kolluk görevlisi, Cumhuriyet savcısı veya sulh ceza hâkimi ile hazır bulunan zabıt kâtibi tarafından imza edilir*." şeklinde hüküm bulunmaktadır. Çalışmamızın ana konusunu oluşturan CMK m.134'e bakıldığında ise 3. fıkra uyarınca bilgisayar veya bilgisayar kütüklerinde el koyma işlemi sırasında sistemdeki bütün verilerin yedeklemesinin yapılması gerektiği[235] ve 5. fıkrada da el koyma işlemi yapılmaksızın da sistemdeki verilerin tamamının veya bir kısmının kopyasının alınabileceği, bu kopyalanan verilerin de tutanağa kaydedileceği

[229] Kriptografi ya da 'şifreleme' okunabilir durumdaki bir verinin, içerdiği bilginin istenmeyen taraflarca anlaşılamayacak bir hale dönüştürülmesinde kullanılan yöntemlerin tümüdür. Kriptografi bir matematiksel yöntemler bütünüdür. https://tr.wikipedia.org/wiki/Kriptografi [28.11.2020] ;ayrıntılı bilgi için bkz: UZUNAY/ BIÇAKCI.

[230] "*Deliller mümkün olduğunca toplandığı ortam koşullarına benzer ortamlarda taşınmalı veya saklanmalıdır."* GÖZÜŞÜRİN M., "5237 Sayılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları ile Mücadeleye İlişkin Model Önerisi", Yayınlanmamış Yüksek Lisans Tezi. Kara Harp Okulu SBE, 2011. s.95.

[231] GÖZÜŞÜRİN ss. 91-92; BAŞLAR, Ceza yargılamasında elektronik delil, ss.94-95.

[232] UZUNAY/BIÇAKÇI.

[233] GÖKSOY, s.179; ORTA, s.269; ÖZTÜRK, Bilişim cihazlarındaki sayısal delillerin tespiti ve değerlendirilmesinde iş akış modelleri, s. 39; UZUNAY/BIÇAKÇI.

[234] ÖZTÜRK, Bilişim cihazlarındaki sayısal delillerin tespiti ve değerlendirilmesinde iş akış modelleri, s. 40.

[235] BAŞLAR, Ceza yargılamasında elektronik delil, s.96.

belirtilmiştir. Bu şekilde söz konusu verilere ilişkin hazırlanan tutanağın ilgili kişilere imzalatılması, delillerin inkâr edilmemesi bakımından önem taşımaktadır.[236]

Elektronik delillin doğruluğu ilkesi: Elektronik deliler, insan müdahalesiyle veya sistem tarafından otomatik biçimde meydana getirilmiş, bir emare de olsa; aslına uygun olduğu, doğruluğu ve güvenirliği kesinlikle denetlenmelidir. Elektronik delillerin doğruluğunun ispatlanması için nasıl oluşturulduğuna bakılmalıdır. Bu bağlamda, bilişim sistemindeki kaydın kim tarafından girildiği ve sistemin kaydı işleme alırken doğru çalışıp çalışmadığına dikkat edilmelidir. Eğer kayıt, sistem tarafından oluşturulmuş ise, delili oluşturan programın doğru ve güvenilir çalıştığının tespiti gerekmektedir.[237]

Son olarak elektronik delilin sonradan ele alınabilirliği ilkesi: bir uzman tarafından yapılan inceleme sonucunda tespit edilen elektronik delillerin, istendiğinde başka bir uzman tarafından tekrar değerlendirilebileceğini ifade etmektedir.[238]

Başka bir görüş, bir bilgisayarda yapılan arama neticesinde elde edilen verilerin, delil olma özelliğini taşıması için ilk olarak sağlamlık denetiminin yapılması ve bu verinin delil olmasına yönelik 11 koşulun araştırılması gerektiğini belirtmiştir.[239]

Sağlamlık denetimi ile bilişim sisteminde yer alan elektronik kayıtların CMK m. 206 uyarınca delil olarak kabul edilebilmesi için öncelikle bilirkişi incelemesi gerekli olmakta ve sağlamlığının ortaya koyulması gerekmektedir.[240] Bilirkişi incelemesinden

---

[236] GÖZÜŞİRİN, s.92.

[237] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, ss. 138-139; Bu ilke uyarınca, elektronik delillerin değerlendirilmesi safhasında, söz konusu delilin; kişisel veya kurumsal sahibi, ele geçirildiği vakit, alındığı elektronik medya, içeriği ve bu delili ele geçiren kolluk birimi gibi faktörlerin gerçekliği ortaya koyularak belgelenmelidir. ÖZTÜRK, Bilişim cihazlarındaki sayısal delillerin tespiti ve değerlendirilmesinde iş akış modelleri, ss.39-40.

[238] ÖZTÜRK, Bilişim cihazlarındaki sayısal delillerin tespiti ve değerlendirilmesinde iş akış modelleri, s.40.

[239] YENİSEY/NUHOĞLU, ss.418-421.

[240] YENİSEY F. (Ed.)., .s.134; Özel teknik ve bilgi gerektirmesinden dolayı, adli bilişim konusunda uzman olan bilirkişi (CMK 63) veya uzman (CMK 67/6)incelemesinden geçtikten sonra "sağlam" olduğu anlaşılmaktadır. *"Özellikle, belli bir verinin kayıt öncesindeki kayda hazırlık usulleri, programdaki yapısal hatalar, veri girişinin ayrıntıları, bilgisayara verilen komutlarda yapılan hatalar, kaydedilerek saklanan verideki hasar ve bozukluklar, bilgisayarın çalıştığı sırada elektrik kesintileri olup olmadığı, bilgisayarın hata verip vermediği, veri içerisinde kelime araması veya belli bölümlerin kesilmesi, verinin başka bir karaktere çevrilmesi gibi işlemler yapılırken rutin, kişiye özgü hatalar yapılıp yapılmadığı, kullanılan bilgisayarın standart tipte bir bilgisayar olup olmadığı, bilgisayarın hassas çalıştığına güvenilip güvenilemeyeceği gibi, "teknik hususların" da bilirkişi tarafından incelenmesi ve böylece hazırlanan verinin belli bir kişinin ürünü olup olmadığının, teknik yönden bilirkişi marifetiyle*

geçerek, üzerinde oynama yapılmadığının tespit edilmesinden sonra belgenin hazırlanma süreci ile ilgili tanık dinlenmesi gerekli olabilir.[241] Bununla birlikte, bilgisayar verinin delil olmasına yönelik bir test geliştirilmiştir. Bu görüşe göre, bilişim sistemindeki verinin delil olarak kullanılmasından önce, 11 koşulun aranması gerektiği ifade edilmiştir.[242] Koşullar:

"1. Kişinin bu bilgisayarı gerçekten kullanıp kullanmadığı;

2. Bilgisayar güvenilebilir bir bilgisayar olup olmadığı;

3. Bilgisayar belli bir ofiste bulunmakta ise bu bilgisayara veri eklemek, bilgisayarda çalışmak isteyen kişilerin uyacakları belli kurallar bulunup bulunmadığı;

4.Bilgisayarın içerisinde bilgisayarın hatasız çalışmasını ve yapılabilecek hataları teşhis etmeyi sağlayacak teknik donanım bulunup bulunmadığı: Bu hususta yapılan değişikliklerin "log" olarak kayıt altına alınıp alınmadığı, yedeklemenin hangi aralıklara, nasıl yapıldığı ve bilgisayara girilen verilerin düzenli olarak denetlenip denetlenmediği gibi hususlarda tanık dinlenilmesi gerekmektedir;

5. Bilgisayarın tamirden geçip geçmediği, bozuklukları varsa, giderilip giderilmediği;

6. Tanığın bilgisayarın içinde mevcut olan belirli bir veriyi ekrandan bizzat kendisinin okuyup okumadığı;

7. Tanığın ekrandan çıktı alarak okuması halinde, bu çıktıyı almaya yetkili olup olmadığı;

8. Tanığın çıktıyı alıp okuduğu veya ekrandan okuduğu sırada bilgisayarın düzenli çalışıp çalışmadığı;

---

belirlenmesi gerekir." YENİSEY/NUHOĞLU, Ekim / 2014 , ceza muhakemesi hukuku ders kitabı, Bahçeşehir Üniversitesi Yayınları No: 111 http://www.feridunyenisey.com/Yayinlar/cezamuhakemesihukukuderskitabi.pdf ss.595-596.[13.11.2020]

[241] "*Söz konusu veri tabanına girişin denetim altında olup olmadığı, belli bir program söz konusu ise bunu kullanan kişinin tespit edilip edilmediği, inceleme konusu olan veride hangi tarihte, ne gibi değişiklikler yapıldığı, yedekleme sisteminin yapısı ve kullanımı ile veri tabanının bozulmadan varlığını sürdürebilmesi için ne gibi denetim usullerinin uygulandığı konularında, tanık dinlenmesi gereklidir."* YENİSEY/NUHOĞLU, s.419

[242] YENİSEY/NUHOĞLU, *ceza muhakemesi hukuku ders kitabı*, ss.596-597.

9. Çıktı söz konusu ise duruşma sırasında tanığa daha evvel okuduğu çıktıdan oluşan delilin gösterilip, daha önce gördüğü belge ile bunun aynı olup olmadığının sorulup sorulmadığı;

10. Tanık belgenin daha evvel okuduğu veya gördüğü belge olduğunu söylerse, evvelki belgeyi duruşma salonunda tanımasına neden olan, hatırlamasına sebebiyet veren özelliğin ne olduğu;

11. Tanık çıktıda yer alan bazı farklı işaretleri veya kelimeleri hatırladığını söylerse, tanığa bu şekil veya terimlerin ne anlama geldiğini bilip bilmediği sorularak, mahkemenin ileri sürülen bilgisayar verisini delil olarak kabul edip etmemesi konusunda bir karar vermesinin sağlanması" olarak belirtilmiştir.

Tüm bunlarla birlikte dilsiz birer tanık olan maddi suç delilleri, ceza yargılanmasında kullanılmakta[243] olup, bu delillerin elektronik ortamlardan elde edilmiş olması bu gerçeği yansıtmayacaktır. Bunun için delillerin elde edilmesi ve diğer aşamalarında usul ve esaslara uyulması gerekmektedir. Elektronik delillerin mahkemece kabul edilmesi için elde edilip muhakeme makamlarına sunulmasına kadar ki geçen süre zarfında taşıması gereken standartlar, delillerin sağlamlığını belirtmektedir. Bu delillerde öncelikle emin olunması gerekilen husus, incelenen ve muhafaza edilen verilerin orijinaliyle aynı olup olmadığıdır. Bu bakımdan delillerin asgari standartları taşıyıp taşımadığı delil zinciri ile kontrol edilmektedir. Delil zinciri, delillerin kusurlu veya değiştirilmiş olduğuna yönelik ithamları çürütmeyi sağlamaktadır.[244] Dolayısıyla elde edilen elektronik delillerin geçerli sayılabilmesi için birtakım prosedürlerin uygulanması gerekmektedir. Özellikle bu konudaki uluslararası standartların[245] yerine getirilmesi önem arz etmektedir. Bu doğrultuda olay yerinde ilk müdahaleyi gerçekleştiren ekipten, incelemenin yapıldığı uzman birime, kullanılan laboratuvarlara ve incelemeden sonra ortaya çıkan sonuçların mahkeme huzurunda ortaya konulmasına kadar süren her aşama önemlidir.[246] Ayrıca belirtilmelidir ki, elektronik delillerin ispat

[243] BAYRAM, L., 2012. Adli bilim laboratuvarında TS EN ISO/IEC 17025 standartı teknik gereklilikleri. Polis Bilimleri Dergisi. 14 (1) ss. 81-100. s. 82.
[244] ORTA, ss.163-164.
[245] "*Adli bilişim standartları, verilerin türüne, saklama birimlerindeki gelişmelere, elektronik delillerin gerek elde edilmesi gerek saklanması gibi konularda teknolojideki gelişmelere bağlı olarak sürekli güncellenmesini gerekli kılmaktadır."* ORTA, s.273
[246]ÇAKIR/SERT, Bilişim suçları ve dillendirme süreci, , s. 148.

bakımından değerli kabul edilebilmesi için bu delilleri elde edecek ve doğruluğunu teyit edecek kişilerin, bilgi birikimine sahip ve bu alana hâkim olmaları gerekmektedir.[247]

C. ADLİ BİLİŞİM

1. Adli Bilişim Kavramı

Günümüzde tesirini her geçen gün arttıran bilişim teknolojileri, bireylere sürekli yenilik ve imkânlar sağlamaktadır.[248] Teknolojideki bu gelişmeler ile birçok suç tipinin gerçekleştirilmesinde, bilişim sistemlerinin kullanılması; suç işlenmesinin kolaylaştırması, yakalanma riskinin nispeten düşük olması ve kendilerini gizleyebilme kolaylığı sağlaması[249] gibi nedenlerle suçu gerçekleştiren kişilerin, kullandıkları klasik yöntemlerden değişikliğe gitmelerine sebep olmuştur.[250] Günlük hayatımızın bir parçası haline gelen, bilgisayar ve diğer elektronik cihazlardan, sadece siber suç soruşturmalarında değil, kanunlarda belirtilen birçok suç tipinin araştırmasında adli bilişim tekniklerinden her geçen gün daha fazla faydalanılmaktadır. Bu kapsamda bilgisayarın, herhangi bir suça iştiraki üç farklı şekilde söz konusu olabilmektedir.[251] İlk olarak bilişim suçunun hedefi olabilir. Bu durum bir bilgisayarın erişilebilirliği, gizliliği ve bütünlüğüne zarar verilmesi şeklinde gerçekleşebilir. Örneğin internet web sitelerinin saldırıya uğraması gibi. İkinci olarak bilgisayarın, bilişim suçunu gerçekleştirmek için araç olarak kullanılması söz konusu olabilir. Buna örnek olarak yasadışı ürünlerin satışı, çocuk pornografisi, internet dolandırıcılığı ve fikri mülkiyet haklarının ihlal edilmesi verilebilir.[252] Üçüncü olarak ise klasik suçlardan olan cinayet, gasp, hırsızlık vb. suçların şüphelilerinden elde edilecek aygıtlarda, yapılacak incelenme ile işlenen suçla ilgili delil niteliğinde elektronik verilere ulaşmak mümkün olabilecektir.[253] Bunların yanı sıra, adli bilişim alanına yalnızca ceza yargılanmasında başvurulmamaktadır.

[247] GÖKSOY, s.178.
[248] ORAKCI M. /KÖK İ./ÇAKIR H., Adli Bilişim Eğitiminin Gereksinimi ve Genel Olarak Değerlendirilmesi, Bilişim Teknolojileri Dergisi. 9 (2), Mayıs 2016 ss.137-145, s.137.
[249] BAŞAR, "Siber Suç Soruşturmalarında Adli Bilişim İncelemeleri, ss.58-59
[250] YENİDÜNYA/DEGİRMENCİ, s.14.
[251] AKARSLAN, s.85;HENKOĞLU, s.3
[252] BAŞAR, Siber Suç Soruşturmalarında Adli Bilişim İncelemeleri, ss.58-59
[253] ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s.24.

Bilişim aygıtları, hayatın her alanına dahil olmasından dolayı uyuşmazlık durumlarında sıklıkla başvurulan, delil kaynakları haline bürünmüştür. [254]

Elektronik deliller, değerlendirmeye olanaklı hale getirilmeli yani sanal dünyadan gerçek dünyaya aktarılmalıdır.[255] Bu bağlamda, delillerin takdiri muhakeme hukukuna ilişkin bir husus iken bilişim sistemleri üzerinden delillerin toplanması, teknik bir konu olup elektronik delillerin toplanması ve değerlendirilmesine yönelik teknik kısım, adli bilişim çalışma alanı kapsamındadır.[256] Dolayısıyla yapılan incelemelerle siber suçlar veya bilişim yoluyla işlenen suçların yanı sıra klasik suçlar ile bunları işleyenlerin tespiti veya tespit edilmesi halinde elektronik delilerle desteklenmesini sağlamaktadır. Bu itibarla, adli bilişim ile bilişim sistemi üzerindeki verilerden suç soruşturmasını aydınlatacak veriler çıkartılarak, bunların delil olarak kullanılması sağlanmaktadır.[257]

Dilimize "computer forensics"(Türkçe karşılığı ile "bilgisayar adli bilimi") tanımından çevrilmiş olan[258] adli bilişim kavramı, "bilgisayar adli bilimi" olarak kullanılmak yerine kapsamının genişliği ve neredeyse teknolojik her şeye karşılık gelen sihirli kelime bilişimin baz alınması dolayısıyla "adli bilişim" olarak kullanılmıştır.[259] Dilimize tam olarak çevrildiğinde, "bilgisayar kriminalistiği" veya "bilgisayar adli bilimi" denilebilir ise de, doktrinde genel olarak adli bilişim kavramı tercih edilmektedir.[260] Adli bilişim, bir uzmanlık alanı olarak, adli bilimler çatısı altında ayrı bir disiplin alanıdır.[261] Adli tıp' da nasıl ki insanların ölüm veya yaralanma vb. nedenler tespit ediliyorsa, adli bilişimde bilgi teknolojileri kullanılarak işlenen suçların tespiti sağlanmaktadır.[262]

Adli bilişim kavramı, değişik şekillerde tanımlanmıştır. Adli bilişim, bilişim sistemleri üzerindeki suça ilişkin elde edilebilecek delillerin, bilgisayar ve diğer elektronik materyaller içerisinde bulunması, bu delillerin keşfedilmesi ihtiyacı nedeniyle ortaya

[254] BAŞLAR Y., 2020. Adli bilişim sürecinde karşılaşılan sorunlar ve çözüm önerileri. Türkiye Barolar Birliği Dergisi. (148), ss. 47-76.TBB, ss.49-50; ORTA, s.162.
[255]ARSLAN, s.261.
[256] ORTA, s.158.
[257] BAŞAR, Siber Suç Soruşturmalarında Adli Bilişim İncelemeleri, s. 60.
[258] HENKOĞLU, s.1.
[259] OĞUZ R., "Adli Bilişimde İnceleme Süreçleri" , Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, Disiplinler arası Adli Bilimler Anabilim Dalı Yayınlanmamış Yüksek Lisans Tezi, 2018 s. 5.
[260] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.38.
[261] DÜLGER, Adli Bilişim & Ülkemizde Uygulanması, ss.20-25, s.20; HENKOĞLU, s.1
[262] ARICI H. Y., 2018.Adli Bilişim, Ankara, Seçkin Yayıncılık, Ağustos, ss.23-24.

çıkan delil bulma yöntemidir.[263] Diğer bir ifadeyle *adli bilişim; Elektromanyetik-elektro optik ortam(lar)da muhafaza edilen ve/veya bu ortamlarca iletilen; ses, görüntü, veri/bilgi veya bunların birleşiminden oluşan her türlü bilişim nesnesinin, mahkemede sayısal (elektronik-dijital) delil niteliği taşıyacak şekilde: Tanımlanması, elde edilmesi, saklanması, incelenmesi ve mahkemeye sunulması çalışmalarının bütünüdür.*[264] "*Adli bilişim, kısaca potansiyel yasal delillerin elde edilmesi amacıyla bilgisayar inceleme ve analiz teknikleri kullanılarak yapılan bir uygulama şeklinde tanımlanabilir.''*[265] "*Günümüzde kullanılan ya da anlaşılması gereken şekliyle tanımlayacak olursak, adli bilişim; konusu suç oluşturan eylemlerde, bu suçlarla ilişkili kişilerin kullandıkları elektronik ortamlardan elde edilen sayısal verilerin, işledikleri suçlarla bağlantılarını ortaya çıkarmak ve suç delillerini ilgili adli makamlara sunmak amacıyla güvenlik birimleri ya da ehliyetli kişi/kurumlarca yapılan analiz işlemleri bütünüdür.''*[266] Bu bağlamda "*bilişim cihazlarından delil elde etme sürecidir. Bu süreç; delil toplama (collection), delillerin incelenmesi (examination), sonuçların değerlendirilmesi (analysis) ile raporlama ve sonuç (reporting) aşamalarından oluşur.''*[267] Dolayısıyla adli bilişim, bilişim sistemleri üzerinde herhangi bir suçu işlemede ya da yasaklanmış bir faaliyette kullanılıp kullanılmadığının tespiti amacıyla yapılan çalışmalardır.[268]

Adli bilişim incelemelerinde, elektronik materyallerin içerisindeki gözle görünmeyen, elle tutulamayan, sanal olarak nitelendirilen elektronik veriler incelenmekte ve gerçek dünya ile ilişkisi kurularak, suçu ispat edebilecek nitelikteki elektronik deliller ortaya konulmaktadır.[269] DNA ve parmak izi gibi izlerinin tespiti için nasıl ki bilimsel metotlar kullanılıyorsa, hassas yapıya sahip elektronik delillerinde bozulmadan veya yok olmadan tespit edilebilmesi için bir uzman tarafından incelenmeli, bazı donanım ve yazılımların kullanılması gerekmektedir.[270] Çünkü genellikle makine dili ile kodlanmış

[263] ÖZEN/ÖZOCAK, s. 44.
[264] AKARSLAN, s. 114.
[265] KESER BERBER, s.39; SANSAR M. Bilişim suçlarının tespiti ve dijital delillerin incelenmesi http://www.tide.org.tr/uploads/MUSTAFA%20SANSAR.pdf [10.05.2018]
[266] EMEKCİ, A./KUĞU E./ TEMİZTÜRK M., Adli bilişim ezberini bozan bir düzlem: bulut bilişim, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, Cilt:2, No:1, S:8-14, 2016; s.10.
[267] ŞİRİKÇİ, A. S./CANTÜRK N., 2012. Adli bilişim incelemelerimde birebir kopa alınmasının(imaj almak) önemi. Bilişim teknolojisi dergisi. 5, (3), ss.29-34.,s.29.
[268] HENKOĞLU, s. 1.
[269] DÜLGER, Adli Bilişim & Ülkemizde Uygulanması, s. 21.
[270] AKARSLAN, s.116.

olan veriler yine bir makine tarafından anlamlı hale getirilebilir.[271] Bu itibarla adli bilişim, yorum faaliyeti içermeyen, teknik bir inceleme yöntemidir.[272] Adli bilişim çalışmalarında veri kurtarma, veri imha etme, veri dönüştürme, veri saklama, şifre çözme, şifreleme, gizlenmiş verilerin ortaya çıkarılması vb. teknik hususlar bulunmaktadır. Bu sebeple adli bilişim sürecinde teknolojinin rolü önemlidir.[273]

Adli bilişim alanı kendi içerinde dört farklı bölüme ayrılmaktadır. Bunlar; bilgisayar adli bilişimi, ağ adli bilişimi, mobil adli bilişim ve sosyal medya adli bilişimi olarak sıralanabilir.[274] Çalışmamızın devamında konu itibariyle bilgisayardan elde edilebilecek elektronik deliller çerçevesinde bilgisayar adli bilişimi yöntemi ile devam edilecektir.

Bilgisayar adli bilişimi, "*suç işlendikten sonra, suç mahallinde bulunan ya da suçlu tarafından kullanılan masa üstü, dizüstü ve netbook tarzı bilgisayarların, adli birimlerce, teknik prosedürlere ve usul kurallarına uygun bir biçimde ön güvenliğinin sağlanması da dâhil olarak, adli bilişim laboratuvarlarına taşınması, bilgisayarlar içindeki bilgi barındıracak tüm birimlerin incelenmesi, gerekli ilişkilendirmelerin yapılması, raporlanması ve adli makamlara sunulması süreçleri yer almaktadır*."[275] Günümüzde, gerçekleştirilen pazarlama stratejileri ve algı yönetimi ile kişiler ihtiyaçları olduğu düşüncesiyle birden fazla bilgisayar donanımı kullanmaktadır. Bu bakımdan bilgisayar adli bilişimi en çok üzerinde durulan adli bilişim türüdür.[276] Bunun yanı sıra bilgisayarlar içerisinde büyük miktarda veri barındıran, e-posta işlemlerinin yapıldığı, dahili sabit diskinin bulunduğu, kendine has logları oluşturan, kullanıcı hesaplarının yönetilebildiği ayrıca en yaygın kullanılan elektronik cihazlar olması sebebi ile adli makamlar için önemli bir veri kaynağı olmaktadır. Bu disiplin, esas olarak veri kurtarma[277] projesine dayanmakta ve adli bilişim alt dalları arasında ilk olarak ortaya çıkmıştır.[278]

---

[271] ÖZEN /ÖZOCAK, s. 59.
[272] ÖZEN/ÖZOCAK, s. 45.
[273] ORTA, s.159.
[274] ARICI, s.27.
[275] ÖZEN/ÖZOCAK, s.46
[276] ARICI, s.28.
[277] "*Veri kurtarma veya Data recovery, cep telefonu, bilgisayar, notebook ve harici depolama cihazlarındaki bilgilerin, herhangi bir nedenle kaybedilen, yanlışlıkla silinen, bozulan veya erişilemez hale gelmesi, ulaşılamaması durumunda, bilgilerin yeniden ulaşılabilir hale getirilmesini, bir başka*

2. Adli Bilişim Süreci

Elektronik deliller, klasik delillerle karşılaştırıldığında delillerin elde edilmesinde farklılıklar bulunmaktadır. Adli bilişim incelemesinde elektronik bulguların, hukuki delile dönüştürebilmek için belli bir prosedür uygulanmaktadır.[279] Bu prosedüre adli bilişim süreci denmektedir.[280] Elektronik verilerin tespit edilmesi ve toplanması sırasında gerçekleşebilecek hataların telafisi pek mümkün olmamaktadır. Bu bakımdan genellikle, elektronik delillerin toplanması için tek bir fırsat bulunmaktadır.[281] Bunların yanı sıra, adli bilişim sürecinin aşamalarına yönelik net bir ayrım bulunmayıp, farklı yaklaşımlar mevcuttur. Aslında bu yaklaşımlar birbirlerine yakın olmakla birlikte, izlenecek yöntemlerin farklı aşamalarda tanımlanması söz konusudur.[282]

a. Somut olayın tespit edilmesi ve olay yerine gitmeden önce yapılması gereken hazırlıklar

Adli bilişim modellerine bakıldığında, olay yeri[283] incelemede ilk müdahale evreleri; olayın öğrenilmesi ve tespiti, olay yerine gitmeden önce yapılması gereken hazırlıklar, olay yerine ilk müdahale, elektronik delil tespiti, toplanması ve belgelenmesi ile elektronik delillerin güvenli bir şekilde taşımaya hazırlanması şeklindedir.[284]

Suç işlendiğinin öğrenilmesinden sonra olayın çerçevesinin oluşturulması, adli bilişim uzmanlarının müdahalesinin daha verimli olmasını sağlayacak ve sonraki hareketlere yön verecektir. Olayın tespit edilmesiyle birlikte olay yerine gidilmeden önce alınacak olan tedbirler şekillenir. Bu kapsamda, olay yerine götürülecek olan cihaz ve yazılımlara karar verilmelidir.[285] Olay yerine götürülecek olan bu araçlar, elektronik delil toplama, muhafaza, belgeleme aygıtları olmaktadır.[286]

---

deyişle kaybolmuş bilgilerin geri getirme işlemidir." https://www.mydisk.com.tr/tr/makale/105/veri-kurtarma-nedir/ [19.05.2020]

[278] ÖZEN/ÖZOCAK, ss.47-48

[279] KESER BERBER, s.45.

[280] SANSAR M., http://www.tide.org.tr/uploads/MUSTAFA%20SANSAR.pdf.

[281] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.162.

[282] AKARSLAN, s.124.

[283] "*Olayın işleniş tarzının, mağdur ve suç sanıklarının ilişkisinin saptanabildiği dinamik bölgeye "olay yeri" denir. Olay yeri, olayın başlangıcı, takibi ve sonucunda geçtiği mekânları kapsar*." ÖZTÜRK, Bilişim cihazlarındaki sayısal delillerin tespiti ve değerlendirilmesinde iş akış modelleri, s. 29.

[284] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s. 162.

[285] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, ss. 162- 163.

[286] Bu araçlar şu şekilde sayılabilir; "*Bilgisayar kasaları ve diğer cihazları sökmek için kullanılacak aletler, Elektronik delillerin ve olay yerinin belgelenmesi için kullanılacak kamera, fotoğraf makinası,*

b. Olay yeri incelemesinde ilk müdahale

Öncelikle bu aşamada, klasik suçlarda olduğu gibi suç mahallini korumak, soruşturmanın ilk aşamasıdır. Zira dijital suçlarda yapılacak ilk şey sistemi korumaktadır.[287] Kolluk görevlileri olay yerinin ve orada bulunan kişilerin güvenliğini sağlamalı, elektronik delillerin bütünlüğünün sağlanması için gereken önlemleri almalıdırlar.[288]Elektronik delillerin bulunduğu donanım ve yazılımlar sanal bir ortam olduğundan[289] dolayı kolayca değişikliğe maruz kalabilecekleri unutulmamalıdır.[290] Gerekli önlemler alındıktan sonra görünen delillerin dökümü yapılmalı, konum tespiti işlemleri yapılmalı ve bozulabilecek nitelikteki delillerin koruma altına alınması gerekmektedir. [291] Ayrıca biyolojik ya da görünmez izler gibi bulgular olabileceği göz önünde tutulmalıdır. Klavye, mouse, cd gibi araçlardan muhafaza edilmesi gereken parmak izleri ya da diğer fiziksel deliller söz konusu olabilir. Bu durumda parmak izlerini ortaya çıkarmak için kullanılan kimyasalların, araçlara zarar verebilmesi mümkündür. Dolayısıyla görülmeyen bu izlerin tespiti için yapılacak çalışmalar, elektronik delillerin kurtarma işleminden sonra yapılmalıdır.[292]

Olay yerinin güvenliğinin sağlanması için gerekli bir takım işlemler[293] yerine getirilmelidir. Bu aşamada olay yerindeki sistemin fotoğraflarının çekilmesi,

---

delil numaralandırma etiketleri, renkli fosforlu kalemler, kroki şablonu, elektronik delil formları, mesafe ölçüm araçları, Elektronik ve fiziki delillerin bütünlüğünü korumak için elektrostatik deşarj ekipmanları, tek kullanımlık lateks eldivenler, Elektronik delilleri usulüne uygun elde etmek için kullanılacak adli bilişim cihazları ve boot-DVD'leri, delillerin alınacağı(adli bilişim açısından steril) sabit diskler, donanımsal yazma koruma araçları, dizüstü bilgisayarlar, cross-over kablo, Elektronik delillerin güvenli taşınması için darbeye dayanıklı, antistatik ve antimanyetik çantalar, delil torbaları, radyo frekansına karşı korumalı çantalar, Olay yerinden elektronik delil toplamaya yardımcı olarak kullanılabilecek güç kaynakları, çevirici ve bağlantı aparatları, elektronik çoklama/uzatma cihazları network kabloları" ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.165.

[287] PRASAD, M.A.R. / SATİSH, Y. N. (2013). Reconstruction of Events in Dijital Forensics International Jaurnal of Engineering Trends and Technology, 4(8), syf:3460-3467 s. 3461. https://studylib.net/doc/12925458/reconstruction-of-events-in-digital-forensics[20.09.2020]

[288] ÖZMESTİK, 52; Benzer açıklamalar için bkz: KESER BERBER, s.65.

[289] DOĞU, A.H. 2017 Bilişim hukuku, Bursa, Ekin Basım Yayın Dağıtım s.100.

[290] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.164.

[291] ÖZMESTİK, s.53.

[292] KESER BERBER, ss.65-66.

[293] "*Olay yerinin bütün giriş ve çıkışının belirlenmesi, Olay yerinde bulunan şüphelilerin elektronik delillerin yanından ve çevresinden hızla uzaklaştırılması, Olay yerinin sınırlarını belirleyen şeritlerin çekilmesi, Diğer kolluk personeli ve şüphelinin elektronik delillerin bulunduğu ortamdan çıkarılması, Yetkili olmayan kimselerden gelen teknik yardım taleplerinin reddedilmesi, Kişisel ve taşınabilir cihazlar dahil tüm elektronik cihazların güvenliğinin alınması, Elektronik cihazlara yetkisiz personelin erişiminin engellenmesi, Hiçbir elektronik cihazın yerinin ve durumunun değiştirilmesine müsaade edilmemesi, Kapalı olan bilgisayar veya elektronik cihazların açılmaması, Açık olan bilgisayar veya elektronik*

bilgisayarın açık veya kapalı olması durumuna[294] göre yapılacak işlemelerin belirlenmesi gerekmektedir.[295] Özellikle olay yerinde yapılmaması gerekenleri sıralayacak olursak; bilgisayarı çalıştırmak, bilgisayar virüsleri için kontrol yapmak, delillerin nakliyesi sırasında hiçbir önlem almamak, bilgisayar sahibinden yardım istenmesidir.[296]

Olay yerinde ilk müdahale sırasında şüpheli veya şüphelilerden önceden bilgi edinmek bazı durumlarda fayda sağlayabilir. Fakat şüpheliler, yanıltıcı bilgilerde verebilir. Burada görevli personelin uzmanlığı önemli olup, şüphelilerden konuya ilişkin imkân dahilinde bir takım bilgiler[297] edinilebilir. Kısa süre içerisinde olay yerindeki araştırmacıların inceleme ve analiz yapabilmeleri için önemli bilgiler verilmesi, araştırmacı ekibine psikolojik avantaj sağlar.[298] Bununla birlikte olay mahallinde dokümantasyon yapılarak kayıt oluşturulmalı ve bu belgeleme sürecinin diğer aşamalarda da devam etmesi gerekmektedir.[299]

c. Delillerin toplanması, muhafazası ve laboratuvara nakledilmesi

Ülkemizde, elektronik delillerin nasıl elde edileceğine ilişkin kapsamlı bir yasal düzenleme bulunmadığı gibi,[300]delil toplama sürecinde kullanılması gereken ekipman ile ilgili olarak da geliştirilen ve yasa ile desteklenen bir standart henüz mevcut değildir.[301] Halbuki hem bilirkişi görevlendirilmesinde hem de adli bilişim sürecine

---

cihazların kesinlikle kapatılmaması, gerekirse çalışmaya devam edebilmeleri için gerekli elektrik gücünün sağlanması." ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s. 164.

[294] Bilgisayarın açık olması durumunda ekran görüntüsünün fotoğrafı çekilmelidir. Ekran koruyucunun devreye girmesi engellenmeli ve RAM imajı alınmalıdır. Açık haldeki sosyal paylaşım sayfaları ve anlık mesajlaşma varsa kontrol edilmelidir. Bilgisayar kapalı halde ise elektrik ve internet bağlantıları kontrol edilmelidir DÜLGER, Bilişim suçları ve internet iletişim hukuku, s.572.

[295] SANSAR, http://www.tide.org.tr/uploads/MUSTAFA%20SANSAR.pdf (10.05.2018)

[296] KESER BERBER, ss.46-47.

[297] *"Cihazların kimlere ait olduğu ve kullanıcı adları, Bilgisayar ve internet(Sosyal ağ hesapları vb) kullanıcı bilgileri, Bütün oturum açma isimleri, şifreleri ve kullanıcı hesaplarının detayları, Elektronik cihazların kullanım amacı, Yazılım, hesap veya veri erişiminde kullanılan şifreler (BIOS, oturum açma, e-posta, PGP vb şifreleri) Kullanımda olan otomatik uygulamalar, İnternet erişim tipi, Olay yeri haricinde bulunan veri depolama birimlerine ait bilgiler, İnternet servis sağlayıcı bilgileri, Olay yerinde bulunan verilerin erişimine yönelik kısıtlamalar, Kullanımda olan yok edici, zarar verici donanım ve yazılım bilgileri*." ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s. 165.

[298] DEBROTA, S.,/GOLDMAN, J./MİSLAN, R./ROGERS, M.K.,/WEDGE, T.,(2006) Computer Forenscs Field Triage Process Model. Journal of Digital Forensics, Security and Law, 1(2), s. 22. https://commons.erau.edu/cgi/viewcontent.cgi?article=1004&context, [26.11.2020]

[299] KESER BERBER, s.66.

[300] KARAGÜLMEZ, s.517.

[301] AKARSLAN, s.132; ÖZMESTİK, s.55.

ilişkin hususlar bakımdan uluslararası alanda kabul edilen adli bilişim standartlarına[302] önem gösterilmesi ve bunların yasal bir zemine kavuşturulması gerekir.[303]

Bu süreç kapsamında delillerin bozulmadan saklanması ve laboratuvara sevk edilmesi gerekmektedir.[304] Elektronik delillerin bütünlüğünü sağlamak amacıyla paketlenmesi, nakledilmesi ve muhafazasının kimler tarafından, ne şekilde yapıldığının tutanakta belirtilmesi gerekmektedir.[305] Bu doğrultuda olay yerine ilk müdahale anından itibaren tüm işlemler kaydedilmedir.[306] Olay yerinin belgelenmesi amacıyla öncelikle fotoğraflar çekilmeli ve video kaydı alınmalıdır.[307] Elektronik delillerin taşınma işlemlerine dikkat edilmelidir. Zira yapısı gereği statik elektrik ve manyetik alanlardan zarar görme olasılığı yüksektir. Bu sebeple özel toplama ve paketleme poşetleri kullanılmalıdır.[308] Elektronik delillerin toplanmasına başlamadan önce dokümantasyon ve konum tespiti işi bitmiş olmalıdır.[309] Elektronik delillerin toplanması sürecinde, delillerin bulunduğu yerin kuralları gözetilerek yasaya uygun hareket edilmelidir.[310]

Tüm bunlarla birlikte, her bir elektronik delil için form hazırlanmalıdır. Bu delil formları elektronik delilin kimliğini yansıtmaktadır. Elektronik delillere soruşturma süresinde kimlerin eriştiğini ve delilin dolaşımına dair doğru bilgiler kaydedilmelidir.[311]

---

[302] ISO tarafından 2012 yılında yayımlanan ve 2018 yılında gözden geçirilen ISO/IEC 27037:2012 bu hususlaki en temel belge olmaktadır. Bu belge, dijital verilerin tanımlama, toplama ve muhafazası için bilgiler vermektedir. KAYA M. B,, "Hukuki Açıdan Bilişim Suçları, Siber Güvenlik ve Adli Bilişim", Şeref Sağıroğlu/Mustafa Şenol (ed.), Siber Güvenlik ve Savunma Problemler ve Çözümler içinde (213-279), BGD Siber Güvenlik ve Savunma Kitap Serisi 2, Grafiker Yayınları, Ankara, 2019, s. 258. Aktaran BAŞLAR, Adli bilişim sürecinde karşılaşılan sorunlar ve çözüm önerileri, s.60.

[303] BAŞLAR, Adli bilişim sürecinde karşılaşılan sorunlar ve çözüm önerileri, s.60.

[304] SANSAR, http://www.tide.org.tr/uploads/MUSTAFA%20SANSAR.pdf (10.05.2018)

[305] Elektronik delilin toplanması ve muhafaza edilmesi, adli bilişim sürecinin başlangıç aşaması olup, delil bütünlüğünün sağlanması bakımından önemlidir. BAŞLAR Y., 2020. Elektronik delilin toplanması ve muhafazası. Hacettepe Hukuk Fakültesi Dergisi. 10(1), ss. 77-107., s.82. Benzer açıklamalar için bkz: ÖZEN /ÖZOCAK,, ss. 51-53; KARAGÜLMEZ, s.516

[306] HENKOĞLU, s.20.

[307] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller s.167.

[308] HENKOĞLU, s.25; KESER BERBER, s.67

[309] KESER BERBER, s.67.

[310] KARAGÜLMEZ, s.518.

[311] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.167; Araştırmacıların elektronik delilerin nerede, ne zaman ve nasıl bulunduğu, ne şekilde elde edildiği, delillerle kimlerin temas ettiği ve hangi şekilde değerlendirildiğine ilişkin bilgiler edinmeleri gerekir. COSİC, J /BACA m., 2010, (Im) Proving Chain of Custody and Digital Evidence Integrity with Time Stamp. Croatian Society for Information and Communication Technology, Electronics and Microelectronics(MIPRO),33rd International Convention, Opatija, Hırvatistan http://czb.foi.hr/upload/datoteke/10_400.pdf [5.08.2020], s.1. aktaran ; BAŞLAR, ceza yargılamasında elektronik delil, s. 220; BAŞLAR, Elektronik delilin toplanması ve muhafazası., s.98.

Bu kapsamda her bir elektronik delil için delil koruma ve gözetim zinciri [312] işlemleri uygulanmalıdır.[313] Koruma zinciri, elektronik delillerin sağlam delil olmasında rol oynadığı gibi, delillin geçerliliği ve bütünlüğü bakımından da adli soruşturma süresince önem taşımaktadır.[314] Güvenilir, sağlam verilere dayalı bir koruma zincirinin mevcut olmaması halinde, delilin doğru değerlendirilmediği, değiştirilmiş olabileceği, suçlayıcı delillerle değiştirilebileceği veya başka bir şekilde değişime uğramış olabileceği ileri sürülebilir.[315] Bunun yanı sıra zaman damgası, adli bilişim sürecinde önemli bir yere sahiptir. Çünkü araştırma esnasında bazı anlara ilişkin tam zamanın öğrenilmesine ihtiyaç duyulmaktadır.[316] Zaman damgası, dijital boyutta spesifik bir zamanı belirtmektedir.[317] Bu şekilde, elektronik delilin bütünlüğünü[318] sağlamaktadır.[319] Belgeleme işlemleri delillerin toplanması esnasında da devam edeceğinden bu kayıtlarda delil elde etme zamanı ve yöntemine ilişkin bilgilere de yer de verilmelidir.[320]

c.1. Verilerin elde edilmesi yöntemi (Arama)

Verilerin elde edilmesinde ilk aşama arama işlemidir. Arama işleminde, arama kararında belirtilen delile, şüpheli ya da sanığın kullandığı bilişim sistemlerinde ulaşılmaya çalışılmaktadır.[321] Bu sistemler üzerinden elde edilmek istenen veriler dört grupta değerlendirilmektedir. Bunlar; sistemde yer alan ve veri taşıma ortamına kaydedilmiş veriler, sistemde mevcut ancak veri taşıma ortamına kaydedilmemiş (uçucu) veriler, sistemde hali hazırda mevcut olmayan ancak bazı araçlarla elde

[312]Gözetim Zinciri, fiziksel veya elektronik kanıtların ne zaman, nasıl ve kimler tarafından toplandığının, işlendiğinin ve incelendiğinin kronolojik olarak belgelenmesi için kullanılır. Gözetim Zinciri Nedir? Tanım ve Örnekler, 03 Nov, 2020, https://www.greelane.com/tr/be%C5%9Feri-bilimler/sorunlar/chain-of-custody-4589132, [21.03.2021]

[313] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.167.

[314] BAŞLAR, Ceza yargılamasında elektronik delil, s.220.

[315]CASEY, Digital Evidence and Computer Crime, s. 22. https://books.google.com.tr/books/about/Digital_Evidence_and_Computer_Crime.html?id=6gCbJ4O4f-IC&printsec=frontcover&source=kp_read_button&redir_esc=y#v=onepage&q&f=false[05.08.2020] aktaran BAŞLAR, Elektronik delilin toplanması ve muhafazası, s.99.

[316] COSİC, J /BACA m., s.3; BAŞLAR, ceza yargılamasında elektronik delil s.218.

[317] BAŞLAR Elektronik delilin toplanması ve muhafazası, s.95.

[318] "*Elektronik delilin ceza yargılamasında kullanılabilmesi, veri bütünlüğünün korunmuş olmasına bağlıdır*." BAŞLAR, Elektronik delilin toplanması ve muhafazası, s.86.

[319] "*Delillerin hangi zamanlarda oluşturulduğu, erişildiği veya değiştirildiği ile ilgili bilgilerin kayıt altına alınması işlemidir*." Bu şekilde deliller üzerinde değişiklik yapması engellenmiş olacak ve elektronik delillerin doğruluğu sağlanmış olacaktır. AYDOĞAN, s.37.

[320] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.167.

[321] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.218.

edilmesi mümkün olan(silinmiş) veriler ve bilişim sisteminden elde edilemeyecek verilerdir.[322]

c.1.1. Yerinde (on-site) arama

Eşzamanlı[323] ya da mahallinde[324] arama da denilen bu arama türü, bilişim sisteminin bulunduğu mekânda suça ilişkin verilerin aranması faaliyetidir. Ancak bu yöntemin bazı sıkıntılı yönleri bulunmaktadır. Bunlar: genellikle arama işleminin uzun sürmesi, aramayı gerçekleştirecek olan uzman görevlilerin o yerde bulunmaması, arama sırasında şifrelenmiş ya da gizlenmiş verilere rastlanılması, duruma göre eldeki aletlere ek olarak bazı teknik cihazlara gereksinim duyulması[325] olarak sayılabilir. Ayrıca veri depolama birimlerinin büyüklüğü ve yapısı, yerinde arama yapılması için gerekli süre olup olmadığı düşünüldüğünde etkili olmayacaktır.[326] Eş zamanlı yerinde aramanın uygulanmasında çoğunlukla iki yönteme başvurulmaktadır. İlk metot, basit arama olarak, bilişim sisteminde bulunduğu bilinen bir verinin aranması amacıyla gerçekleştirilmesidir. Bu şekilde kolluk kuvvetleri, sisteme erişim sağlayarak denetler. Ancak bu yönteme başvurulması halinde, bilişim sisteminde bulunan dosya ya da üst verilerin değişme olasılığı bulunmasından ötürü, arama video kaydına alınmalı ve yapılan işler kayıt edilmelidir. İkinci yöntemde ise yine yerinde arama yapılmasına karşın, öncelikle bilişim sisteminin belleğinin imajının oluşturularak, arama işlemleri bu imaj üzerinden gerçekleşmektedir. Bu yöntem, veri bütünlüğünün sağlaması bakımından tercih edilmektedir.[327]

Ağ üzerinden gerçekleşen bir suçu aydınlatmak için eşzamanlı arama yöntemi kullanılmaktadır. Zira suç o anda da işlenmekte olabilir. Burada çoğunlukla amaç, ağ üzerinden gerçekleşen aktivitenin tespitidir.[328]

---

[322] BUCHHOLZ F./SPAFFORD, E. "On the Role of File System Metadata in Digital Forensics", Digital Investigation, Vol.1, 2004 s.299. aktaran DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.221.
[323] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.223; SAY, s. 19.
[324] GÖKSOY, s.127.
[325] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.222.
[326] GÖKSOY, ss.127-128.
[327] Özellikle uçucu verilerin elde edilmesinde yerinde arama yapılmaktadır. Zira güç kaynağının kesilmesiyle bu veriler kaybolabilmektedir. Bu sebeple sistemin bulunduğu yerde kopyasının alınması gerekmektedir. DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.223.
[328] SAY, s.19.

c.1.2. Off-site arama

Arama yapılacak bilişim sisteminin tamamen kontrol altına alınabildiği durumlarda gerçekleştirilen arama yöntemidir.[329] Mahallinden uzakta[330] veya eş zamansız[331] arama da denilen bu arama türü; yerinde aramanın imkan dahilinde olmadığı, müdahalede bulunan ekibin elinde birebir kopya alınması için gerekli ekipman bulunmadığı, verilerin şifrelenmiş veya gizlenmiş olması durumunda ya da sisteme erişim sağlanmasının uzun süreceği durumlarda ve birebir kopya işleminin de uzun zaman alacağı durumlarda, kolluk görevlileri tarafından bilişim sistemine el koyma işlemi yapıldığı ve aramanın laboratuvarda yapılması suretiyle gerçekleştirilen arama faaliyetidir.[332]

c.1.3. Uzaktan arama

Teknik olarak, kişinin haberi olmaksızın bilişim sistemine dışarıdan erişmek mümkündür. Bu şekilde bilişim sistemindeki kayıtlı dosyalara erişim sağlanabilir.[333] Uzaktan arama, ya internet gibi bilişim ağları üzerinden bilişim sistemine bağlanmak suretiyle, ya da bilişim sistemine bir yazılım yüklenmesiyle sistem içerisinde arama yapma yöntemidir. [334]

Bunlarla birlikte bu arama yöntemi ile web kamerası ya da bilgisayarın mikrofonu aktif hale getirilerek, ortam dinlenmesi mümkün olduğu gibi klavyeden girilen bir bilginin de elde edilmesi mümkündür.[335] Uzaktan arama yönteminde şüphelinin bilişim sisteminde arama yapılmasından haberi olmaması, deliller üzerinde şüphelinin inceleme, haklarının korunmasını isteme hakkını ortadan kaldırmakta ve bu deliller üzerinde kolluk ya da üçüncü kişiler tarafından gerçekleştirilebilecek hukuka aykırılıklara olanak

[329] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.224; SAY, s.19.
[330] GÖKSOY, s.129.
[331] SAY, s19.
[332] GÖKSOY, s.129; DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.224.
[333] YENİSEY/NUHOĞLU, Ceza muhakemesi hukuku ders kitabı, ss.602-603.
[334] RFS (Remote Forensic Software) yazılımı, şüphelinin bilgisayarına bilgisi dışında yerleştirilerek ve sistemdeki bütün verilerin analizi yapılmak üzere kolluk birimlerine kopyalanarak gönderilmektedir. Söz konusu yazılım, bir elektronik postanın eki olarak gönderilerek postanın açılmasıyla aktif hale gelebileceği gibi, şüpheli tarafından ziyaret edilen bir web sitesinden indirilen bir yazılımın parçası da olabilmektedir. Uzaktan arama, şüpheliye bilgi verilmeden gerçekleştirilmekte ve hatta duruma göre daha sonradan da bilgi verilmemektedir. ABEL W., "Agents, Trojans and Tags: The Next Generation of Investigators" International Review of Laaw, Computers & Technology, Vol. 23, No. 1, 2009, ss.100-101; DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.226
[335] GÖKSOY, s.130.

tanımaktadır.[336] Ayrıca bu arama yönteminde en çok kullanılan RFS yazılımıyla elde edilen delillerin hash değerinin alınmaması[337] ve kopyanın orijinal delil ile bütünlüğünün denetlenememesi, delilin güvenirliği hususunda kuşkuya sebep olacaktır.

c.1.4. Bulutta Arama

Dosya saklama ve dosyalara ulaşım gibi problemlerin ortadan kalkmasını sağlayan bulut bilişim hizmetleri, hardisk ve harici taşıyıcılar gibi malzeme gereksinimi olmadan, hiçbir cihaza bağımlı kalmadan, bilgilere ulaşılabilmesine imkân sağlamaktadır.[338] Geleneksel adli bilişim uygulamalarında elektronik delilin bulunduğu bir ortam vardır ve öncelikle donanım açısından elektronik aygıta ulaşılması gerekmekte, bu aşama da toplama olarak ifade edilmektedir. Daha sonraki aşama ise, elektronik aygıttaki verilerin uygun yöntemlerle kopya oluşturularak, elde edilmesidir. Bulut bilişim mimarisinde sanallaştırma uygulamaları yoğun olarak kullanıldığından, erişim çoğu zaman mümkün olmadığı gibi elektronik cihazların toplanması da pratikte mümkün değildir. Bu bakımdan delillerin elde edilmesi, sanal uygulamalar ve sanal diskler üzerinden gerçekleştirilebilmektedir. Bu bağlamda, bulut bilişime ilişkin teknik boyutta çıkmazlar bulunmaktadır.[339] Bulut bilişim hizmet sağlayıcı, kullanıcıya ait verileri farklı sunucularda, farklı bölgelerde ya da farklı ülkelerde depolayabilmektedir.[340] Bu dağınık yapı nedeniyle adli bilişim uygulamalarında değinilmeyen noktalar olabileceği gibi, işlemler için hizmet sağlayıcısı personeli ve bir başka ülkedeki kolluk kuvveti ile de işbirliği ve koordinasyon gereken durumlar söz konusu olabilir.[341] Dağınık vaziyette bulunması, ilgili verilerin farklı ülkelerdeki sunucularda depolanması, söz konusu verilerin güvenliği bakımından o ülkenin yasal düzenlemelerinin geçerli olabileceği sonucunu da doğurabilir.[342] Ayrıca örneğin bir sunucu üzerinde diğer kullanıcılara ait verilerin de depolanıyor veya işleniyor olması, adli bilişim uygulamalarını zorlaştıracağı gibi, yapılacak bir yanlış işlemle suç unsuru barındıran bir kullanıcı suçsuz, konuyla hiç

[336] GÖKSOY, s.131; ÖZEN/ÖZOCAK, s.50.
[337] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.236
[338] http://www.yazilimnet.com/tr/blog/38/bulut-bilisim-nedir- [28.07.2020].
[339] EMEKCİ/KUĞU/TEMİZTÜRK, s. 13.
[340] GÖKSOY s. 107; EMEKCİ/ KUĞU/TEMİZTÜRK, s. 13.
[341] EMEKCİ/KUĞU/TEMİZTÜRK, , s.12.
[342] YILDIZ E./ŞAHİN S., ”Bulut Bilişimde Güvenlik Riskleri ve Önlemler”, 2.Uluslararası Bilişim Hukuku Kurultayı Bildiriler Kitabı, İzmir, 17-19 Kasım 2011, s.154. aktaran GÖKSOY, s.108.

ilgisi olmayan ve verilerini yasal çerçevede bulut ortamında tutan masum bir kullanıcı ise suçlu konumuna gelebilecektir.[343]

c.2. İmaj alınması

Nasıl ki DNA Analizi orijinal kan delilleri üzerinden yapılırken 'orijinal kan delillerini korumak' gerekiyorsa, elektronik delillerde de orijinal verilerin korunması için, bu delillerin analizi kopyası üzerinden yapılmalıdır. Tabi ki koşulların bir kopya oluşturulmasını engellediği birkaç istisna dışında.[344] Bu bağlamda imaj alma yöntemine başvurulmaktadır. Bu işlem, adli bilişimde standartlaşmış bir yöntem olup, işlem sonucunda elde edilen kopyaya "forensic dublicate" (adli kopya) denilmektedir. İmaj alma işlemi, bu işlem için tasarlanmış donanım ve yazılımlarla gerçekleştirilmektedir.[345] İmaj alma işlemiyle elektronik delilde herhangi bir değişiklik meydana gelmemesi için, yazma-koruma[346] teknolojisi geliştirilmiştir.[347] Disk erişim yöntemi hukuksal delil araştırmacısı için birincil öneme sahip olmakla birlikte, gelecekte delil toplama metodolojisi ve bununla ilgili kullanılacak araçlarda önemli faktörler olacaktır.[348] Söz konusu kopyalama işlemi önemli bir husus olması sebebiyle[349] NIST(Ulusal Standart ve Teknoloji Enstitüsü), CFTT-Computer Forensic Tool Testing(Bilgisayar Adli Araç Testi),[350] projesi kapsamında kullanılan araçlarla elde edilen sonuçları doğrulamak

---

[343] EMEKCİ/KUĞU/TEMİZTÜRK, s. 13.
[344]CORNEL WALKER, Computer forensic: bringing the evidence to cout, http://www.infosecwriters.com/Papers/CWalker_Computer_Forensics_to_Court, s.2.[10.01.2020]
[345] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s. 172; AYDOĞAN, s.35.
[346] Önemli delilleri barındıran diskin tek yönlü olarak veri akışını sağlayacak şekilde, disk içerisindeki verilerin bütünlüğünün sağlanmasıdır. "*Donanımsal yazma koruma, inceleme konusu disk veya medya ile bilgisayar arasında köprü vazifesi gören bu tarz cihazlar verilerin okunmasını sağlarken diske veri yazılmasını engellemek üzere tasarlanmıştır; yazılımsal yazma koruma ise çeşitli yazılımlar yoluyla incelemede kullanılacak bilgisayarın incelenecek diske veri yazma komutlarını bloke etmek olarak tanımlanabilir."* DÜLGER, Bilişim suçları ve internet iletişim hukuku, s. 576.
[347] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s. 172.
[348] BROWN CHRISTOPHER, s. 167.
[349] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.173.
[350] Adli Bilişim Aracı Test Programı (CFTT), https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt. [29.08.2020].

adına, kesin sonuç verecek test yöntemleri geliştirilmektedir.[351] Ayrıca NIST, güvenilir bir imaj alma cihazının taşıması gereken özellikleri ortaya koymuştur.[352]

İmaj alma işlemi, orijinal medyada bulunan tüm verilerin, bit düzeyinde bire bir olarak yeni bir medyaya kopyalanmasıdır.[353] Başka bir ifadeyle imaj alınması, "*bit bazında başka bir ortamda bir örneğinin(imajının/görüntüsünün) oluşturulması suretiyle yapılır.*"[354] Bit bazında (bit-to-bit) kopya, orijinal delildeki verilerin, ikili sayı formatındaki diziliminin aynen kopyalanması anlamına gelmektedir.[355] Düşük seviye bit bazında kopyalama yapılmasının önemi, silinmiş, değiştirilmiş, deforme edilmiş verilere de incelemelerde ulaşma olanağını sağlamasıdır.[356] Bu kopya oluşturma şekli, günlük hayatımızda gerçekleştirdiğimiz kes-yapıştır veya sürükle-bırak şeklinde bir kopyalama işlemi olmamakta, zira bu işlemlerle dosya bir kaynaktan başka bir kaynağa aktarılmakta, ancak gizli dosyaların ve silinmiş verilerin elde edilmesi de mümkün kılınmamaktadır. Bu nedenle imaj alma işlemi ile boş alanların dahi kopyalanarak veri bütünlüğü ve güvenirliği sağlanır. [357]

c.3. Hash değeri

Hassas bir yapıya sahip elektronik delillerin, mahkemece kabul edilmeleri için doğrulaması gerektiğini daha önce belirtmiştik. Aksi takdirde mahkemeye sunulan veriler, delil niteliğini kaybedecektir.[358] Elektronik delillerin güvenirliği bakımından oluşturulan hash değeri, önemli bir yere sahiptir.[359] Yürütülen adli bilişim incelemeleri

---

[351] KENT K./CHEVALİER S./GRANCE T./DANG H., "Guide to Integrating Forensic Techniques into Incident Response" National Institute of Standards and Technology Special Publication 800-86, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86[20.09.2020], 800-86, s.4-7.

[352] Buna göre; orijinal disk veya bölümün bit dizisi olarak birebir kopyası alınabilmeli, orijinal diskte değişiklik yapılmamalı, alınan imajın bütünlüğü doğrulanabilmeli ve son olarak I/O(Girdi/Çıktı) hataları kaydedebilmelidir. ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.173.

[353] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s. 172; HENKOĞLU, s.30

[354] SANSAR, http://www.tide.org.tr/uploads/MUSTAFA%20SANSAR.pdf (10.05.2018)

[355] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s. 172.

[356] SANSAR, http://www.tide.org.tr/uploads/MUSTAFA%20SANSAR.pdf (10.05.2018)

[357] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s. 578; ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.149.

[358] AYDOĞAN, s. 32.

[359] DEMİRKAYA' ya göre hash değeri, aslında elkonulması hususunda mevzuatın uygulamasıyla oluşabileceği değerlendirilen sıkıntılara da çözüm olarak sunulabilir. Şöyle ki, elkoyma sırasında veri kaynağının hash numarası belirlenerek, tutanakla birlikte tespit olunursa ve imza karşılığı bilgisayarına el konulana verilirse, (medya kuruluşu ve benzerleri gibi ticari hayatları doğrudan veri kaynağı üzerinden yürütülmeyen durumlarda) en azından içerisinde suç unsuru barındırıp barındırmadığı hızlı bir şekilde incelenene kadar, veri kaynağının kopyası veya aslı yerine, hash numarası şahısta veya kuruluşta kalırsa,

sırasında uygulanan yöntemler ile elektronik delilerin değiştirilmediği "*bütünlük algoritmaları*" kullanılarak ispat edilmektedir. Söz konusu algoritmalara hash algoritmaları veya fonksiyonları, ürettikleri değerlere ise hash değeri denilmektedir.[360] Elektronik delillerin bütünlüğü, adli soruşturmaların dijital sürecinde önemli bir rol oynamaktadır.[361]

Veri özeti işlemi veya diğer bir deyişle hash algoritması değeri, adli bilişimde inceleme konusu olan depolama alanı ile kopyalanan verinin aynı olup olmadığının belirlenmesini sağlamaktadır. Hash değeri, veri bütünlüğünü kontrol etmek için kullanılan tek yönlü özetleme algoritmasıdır.[362] Veri özet değeri, değişken uzunluktaki bir mesajı girdi olarak alır ve işlem sonucunda belirli uzunlukta sayısal bir değer olarak çıkarır.[363] Hash algoritmaları, kelime dizisi, dosya, klasör, disk ya da diğer veri gruplarını belirli uzunlukta, belirsiz bir değer şeklinde oluşturur.[364] Girdideki verinin bir biti bile değiştirilmesi durumunda, üretilen çıktı değerin sayısal değeri farklı olur.[365] Dolayısıyla hash değeri değişken boyutlu bir metni, sabit boyutlu bir çıktıya dönüştüren algoritmadır.[366] Hash algoritmasının değeri, bir dijital belgenin DNA'sına benzetilmektedir. Bu değer, bir insanın parmak izi gibi ait olduğu materyale özel ve tekdir.[367] Bu bağlamda djital parmak izi görevini görmekle birlikte dijital imza olarak da kabul edilebilmektedir.[368] İşte elde edilen bu kriptografik değer, koruma zincirinin

---

suç eşyasının kişiye teslimi gibi bir durum ortaya çıkmayacaktır. DEMİRKAYA V., 2009. Delil güvenliği, Yüksek Lisans Tezi. Ankara: T.C. Polis Akademisi Güvenlik Bilimleri Enstitüsü. s.74.

[360] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.176.

[361] COSİC/ BACA, s.1.

[362] Hash değeri, "*bilgisayar medyasında bulunan tüm 0 ve 1'lerin birbirleri ile belli bir algoritma ile çarpılması"* suretiyle elde edilmektedir. Bu değer, MD5 için 32 karakter uzunluğunda 0-9 ve a-f karakterlerinden oluşan bir değerken, SHA -1 i.in aynı karakterlerden oluşan 40 karakter uzunluğunda bir değer olmaktadır. Bilgisayar medyası üzerinde yapılan en küçük bir değişiklik ile hash değeri değişecektir. ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, ss. 148-149.

[363] SANSAR, M. http://www.tide.org.tr/uploads/MUSTAFA%20SANSAR.pdf (10.05.2018)

[364] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.176.

[365] SANSAR, http://www.tide.org.tr/uploads/MUSTAFA%20SANSAR.pdf (10.05.2018);HENKOĞLU, s.56.

[366] KUMAR K., SOFAT S., JAİN S.K., AGGARWAL N., Significance of Hash Value Generation in Digital Forensic: A Case Study, International Journal of Engineering Research and Development, ss. 64-70. http://www.ijerd.com/paper/vol2-issue5/I02056470.pdf [16.02.202], s.65.

[367] DÜLGER, Bilişim suçları ve internet iletişim hukuku, ss. 578-579.

[368] Bu imzalar, elektronik delillerin mühürlenmesini sağlayarak, verilerin sonradan değiştirilip değiştirilmediğinin anlaşılmasını sağlamaktadır. ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.176.

temelini oluşturmakta ve elektronik suç mahallinden elden edilen fiziksel kanıtların bağlanmasıyla da bir bütünlük oluşturmaktadır.[369]

Hash değerinin hesaplanmasına ilişkin önemli bir husus, hard-disk üzerinde verilerin bulunduğu bazı sektörlerin sarsıntı, manyetik alan, nem gibi nedenlerle bozularak bad-sector(bozuk alan) oluşturabilmesidir. Üzerine veri kaydedilemeyen bu sektörler hash hesaplanmasında dikkate alınamayacağı için bad-sector sayısının bilinmesi önem arz etmektedir. Bu nedenle hesaplanan hash değerinin yanında bad-sector sayısı da belirtilmelidir. Böylece oluşan bad-sector'ler tespit edilerek hash değerine etkisi ölçülebilmektedir.[370]

Tüm bunlarla birlikte, adli bilişim incelemesinde imaj oluşturma işleminin doğru yapılması gerekmektedir.[371] Çünkü inceleme sonucunda mahkeme sürecinde doğru imaj olup olmadığı sorgulanmaktadır.[372] Elektronik delil olarak sunulacak olan bulgu incelemenin başında ve sonunda kontrol edilmeli, hem ait olduğu bilgisayar medyasına hem de kendisine ait hash değeri hesaplanarak raporda belirtilmelidir. Böylece elektronik delilin geçerliliği ve doğruluğu hususunda şüphe oluşmayacaktır.[373]

Yapılan inceleme sonucunda adli makama sunulacak olan raporda, incelemeye tabi olan elektronik materyallerin, hangi veri özet değerine sahip imaj dosyası üzerinden yürütüldüğü bilgilerine açıkça yer verilmelidir. Bu şekilde, başka bir adli bilişim uzmanının aynı veri özet değerine sahip imaj dosyasını incelediğinde veya yapılan işlemleri tekrarlaması halinde aynı sonuca ulaşması gerekir. Dolayısıyla inceleme işlemi sonucunda eğer farklı bir veri özet değeri hesaplanırsa, kopyası oluşturulan dosyanın farklı elektronik materyalden elde edildiği veya içerisindeki verilerin değiştirildiği anlamına gelecektir. Elde edilen materyaller toplandıktan sonra imaj dosyası olay

[369] SCHATZ, B,L(2007), Digital Evidence: Representation and Assurance, Master Thesis Queensland University of Teennology Information Security Institute, Australia, https://eprints.qut.edu.au/16507/1/Bradley_Schatz_Thesis.pdf[20.09.2020], s. 23-24.
[370] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller,s.149.
[371] İmaj alma işlemi sona erdiğinde sonuçlar doğrulanır. "*imaj alma işlemi öncesinde hesaplanan ve imaj alma işlemi sonunda raporlanan MD5 ve SHA1 checksum değerlerinin doğrulanıp doğrulanmadığı belirtilmektedir. Eğer bu iki değer arasında uyuşmazlık varsa imaj alma işlemi doğrulanmayacaktır."* Böyle bir sonuçla karşılaşılması durumunda, alınan imajın mahkemece hiçbir geçerliliği olmayacağından dolayı imaj alma işlemi tekrarlanmalıdır. AYDOĞAN, s.42
[372] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s. 578.
[373] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, ss. 149-150.

yerinde alınmaması halinde, söz konusu materyal içerisine sonradan veri eklenip eklenmediği hususunda her zaman bir şüphe söz konusu olacaktır.[374]

d. İnceleme

Toplama safhasından sonra inceleme aşamasına geçilir. Adli kolluk görevlileri tarafından olay yerinde, materyalin hash değerli bir yedeği oluşturulmalıdır. Sonrasında o yedek üzerinden tekrardan bir yedek oluşturulmalı ve tüm çalışma bu disk üzerinde gerçekleştirilmelidir. Bu şekilde inceleme sırasında diske veya içerisindeki verilere herhangi bir zarar gelmesi durumunda, yine yedek kopyadan bir örnek çıkarılarak inceleme eksiksiz gerçekleştirilebilecektir.[375] İnceleme, somut olayın şartlarına göre çeşitli yöntemlere başvurularak, delilin bütünlüğüne zarar vermeyecek şekilde yapılmalı ve güvenirliği için uluslararası standartlarda kabul edilmiş programlar kullanılmalıdır. İnceleme aşamasında, somut olaya göre ön işlem olarak şifrelenmiş verilerin geri getirilmesi,[376] şüpheli kelimelerin aranması, silinmiş verilerin disk üzerine geri getirilmesi, diskte tanımlanmış veya tanımlanmamış alanlarda bulunan gizli verilerin bulunması,[377] kriptolu dosyaların çözümlenmesi, steganografi[378] uygulanmış verilerin tespiti, geçici dosyaların analizi, swap alanının incelenmesi, log incelemeleri, sisteme nelerin kurulduğu ve hangi donanımların takıldığı, ve zararlı kodların incelenmesi gibi işlemler yapılmaktadır.[379]

Sağlıklı bir adli bilişim incelemesi için olay yerinden elde edilen deliller, gerekli cihaz ve konusunda uzman personelin bulunduğu bir laboratuvar ortamında değerlendirilmelidir.[380]Bu aşamada, kopyalanan sistemdeki her türlü veri ortaya konmuş olacaktır. Örneğin; fotoğraflar, videolar, çeşitli yazı dokümanları (Word,Excel vb.), E-postalar, ziyaret edilen web siteleri ve şifreli dosyalar, silinmiş dosyalar, bir takım dosyaların oluşturulma, değiştirilme ve erişim tarih kayıtları gibi.[381] Bu bakımdan

[374] DÜLGER, Adli Bilişim & Ülkemizde Uygulanması, s. 23.
[375] HENKOĞLU, s.57; AYDOĞAN, s.14.
[376] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s. 255.
[377] ÖZMESTİK, s.56.
[378] Steganografi tekniği, bilgiyi saklanmak için farklı formattaki dosyaların kullanılmasıyla gizlenmesidir. "*Bilginin ya da mesajın fark edilemeyecek şekilde bir yazı, resim veya ses gibi dosyaların içinde saklanmasına elektronik steganografi denilir. Burada amaç, dosyaya bakıldığında özel bir yazılım veya araç kullanılmadan gizlenen bilginin görünmemesi ve anlaşılmamasının sağlanmasıdır*." ORTA, s.214.
[379] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s.581.
[380] GÜNEYSU, s, 243.
[381] SANSAR, http://www.tide.org.tr/uploads/MUSTAFA%20SANSAR.pdf (10.05.2018); ARICI, s.24.

dağınık halde bulunan ham veriler, anlamlı verilere dönüştürülür.[382] Karşılaşılan suça ilişkin ne tür verilerin araştırılacağının belirlenmesi gerekir. Söz konusu suç ve suça ilişkin verilerin olabileceği depolama alanları[383] farklı olabilir.[384]

Adli bilişimci, inceleme sürecinde karşılaştığı tüm detayları belgelendirmelidir.[385] Belgeleme şekli, kimi zaman video kamera ile kaydetme, kimi zaman fotoğraflama şeklinde olabileceği gibi bazı durumlarda ise kayıt tutma şeklinde gerçekleşebilmektedir.[386]

e. Değerlendirme

Elde edilen verilerin analiz edilmesi ve bu verilerin birbiri ile ilişkilendirilmesiyle, muhakemede kullanılacak elektronik delillere ulaşılır.[387] Verinin incelenmesi aşamasında başvurulabilecek yollardan biri de, bir zaman dizgesine sokulmasıyla suç içeren eylemler dizesinin yeniden yapılandırılmasıdır.[388] Bu aşamada, elde edilen verilerin hangilerinin suçu aydınlatmak için rapora dâhil edileceğine karar verilir.[389] Elde edilen deliller ile orijinal veriler arasında bütünlük ve içerik doğrulanması yapılır.[390] Dolayısıyla bu safhada doğru ve öz veriler, ayrıca bütünlüğü bozulmadan, anlaşılabilir ölçüde suçu aydınlatacak olan deliller ortaya konulmalıdır. [391]

---

[382] AKARSLAN, s 128.

[383] Bu durum zaman kazanılması açısından önemli bir etkendir. ÖZEN/ÖZOCAK, s. 54. "*Çocuk pornografisi konusu ile el konulan ve imajı alınan bilgisayar depolama ortamları üzerinde öncelikli olarak resim ve video dosyalan aranırken, internet sitelerine saldın yapılması olayında bilgisayarda kurulu programlar incelenecek ve internet geçmişi araştırılmalıdır*." ÇAKIR/KILIÇ, Bilişim suçlarına ilişkin delil elde etme yöntemine genel bir bakış, s.25.

[384] http://bilisimhukuku.com.tr/adli-inceleme-nasil-yaptirilir/ [10.05.2018]

[385] ARICI, s.239.

[386] ÖZMESTİK, s.58;DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s 268.

[387] ÖZMESTİK, s.57; DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s. 266.

[388] "*Adli bilişim uzmanı maddi olayı yeniden yapılandırırken iki temel analiz sistemi kullanmaktadır. Bunlardan birisi günlük dosya analizi (log file analysis) diğeri ise dosya sistem analizi (file system analysis)'dir. Günlük dosya analizi, zaman damgalarının kontrolü, günlük kayıtlarına girdi yapan sürecin tanımlanması ve girdinin yaratılma nedenlerinin kontrolünü içermektedir.* DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, ss.266-267.

[389] AKARSLAN, s. 129.

[390] ÖZEN/ÖZOCAK, ss.54-55.

[391] EKİZER A. H., Adli Bilişim (Computer Forensics) 2 Şubat 2014 https://www.ekizer.net/adli-bilisim-computer-forensics/ [10.05.20189]

f. Raporlama

Raporlama, mahkemelerin gördüğü kısım olması ve konunun teknik olması sebebi ile önem arz etmektedir.[392] Bu aşamada, tespit edilen elektronik delillerin olayla bağlantıları ortaya çıkarılmış ve yapılan işlemlerin adli makamlara bir rapor halinde sunulması gerekmektedir. Raporun dili yalın, sade, anlaşılabilir olmalı[393] ve teknik terimler açıklanmalıdır.[394]

Bir adli bilişim raporu, adli makamlara makaledeki gibi Giriş-Gelişme-Sonuç şeklinde sunulmalıdır. Giriş bölümünde, incelemeden önceki bilgilere yer verilmelidir. Gelişme bölümünde ise toplanan materyallerde delilin nerede olduğu veri özet değeri gibi bilgilere yer verilmeli, ayrıca laboratuvardaki donanım ve yazılımlardan hangilerinin kullanılarak inceleme yapıldığı ile ulaşılan sonuca dair teknik bilgiler verilmelidir.[395] Başka bir anlatımla tespitlere nasıl ve nereden ulaşıldığı, delil inceleme sürecinin adımları, incelenen cihaz, araç ve diğer bulgular üzerinde ne gibi incelemeler yapıldığı belirtilmelidir.[396] Sonuç bölümünde ise; sorulan, talep edilen hususları özetleyecek kısa ve net bir metin[397] yazılmalıdır. Zira sonuç bölümü, hakim ve savcılara hitap etmekte ve sorulan hususa ilişkin tespitlere bakılmaktadır.[398] Raporun gelişme bölümünde belirtilen teknik kısımlar ise, daha çok tarafları ikna etmek için yazılmaktadır. Şöyle ki taraflar hazırlanan raporu başka bir adli bilişim uzmanına tekrar inceletmek isteyebilirler.[399] Bu durumda, hazırlanan raporda[400] belirtilen işlemlerin aynısı yapıldığında yine aynı sonuç ortaya çıkmalıdır.[401]

---

[392] GÜNEYSU, s.244
[393] ÖZBEK, Adli bilişimde delillerin toplanması ve incelenmesi, s.107.
[394] ARICI, s.273; AKARSLAN, s. 130.
[395] DÜLGER, Adli Bilişim & Ülkemizde Uygulanması, s. 24
[396] ÖZMESTİK, s.58; GÜNEYSU, s 234.
[397] *Örneğin" talep edilen husus, "X dosyası bu bilgisayarda var mı? Varsa ne zaman oluşturulmuştur?" şeklinde ise, "X dosyası incelenen bilgisayarda "C:\Dosyalar" klasörü altında bulunmaktadır. Dosyanın oluşturma tarihi 12.12.2016'dır" gibi kısa ve yalın bir bilgiler verilmelidir".* DÜLGER, Adli Bilişim & Ülkemizde Uygulanması, s. 25.
[398] ORTA, s.164; Raporda kullanılan ifadeler, uzmanın ulaştığı sonuçtur. Uzmanın vardığı sonuçlar her zaman kesin değildir. Ulaşılan bu sonuçlar, bir tespit, kanaat veya çeşitli eminlik derecelerindeki kesinlik düzeyleridir. Bu bağlamda, raporda kesin bir tespitin ihtimal havasında yazılması veya bir kanaat oluşturan durumun bilimsel bir tespit gibi yazılması, mahkemeyi yanıltabilir. Bu hususlara özen gösterilmelidir. BAYRAM, Ses görüntü ve data incelemeleri, s. 235.
[399] AKARSLAN, s.133.
[400] Adli bilişim raporunda "*olay tarihi, zaman, adres bilgileri, donanımların üretici, seri numarası, modeli, unsurları gibi sisteme ait bilgiler, verilerin toplanması esnasında sistemin durumuna ilişkin bilgiler, olaya ilişkin dosya numarası, şikâyetçi veya şüpheli gibi bilgiler, verinin analiz edilmesi*

Hukuk sistemimizde, bilgisayardan delil elde etmeye yönelik adli bilişim sürecinin hukuki alt yapısına, Ceza Muhakemesi Kanunun 134. maddesinde yer verilmiştir.[402]

esnasında tüm aşamalar ve özellikle kullanılan araçlar, süreçler, konular, hata mesajları gibi bilgileri, olay yerinden toplanan fotoğraflar ve fiziksel deliller varsa tanık bilgileri" gibi hususlara dikkat edilmelidir. DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s. 268.

[401] DÜLGER, Adli Bilişim & Ülkemizde Uygulanması, s. 25.

[402] DOĞU, s.130; AKARSLAN, s. 132.

III. GENEL OLARAK KORUMA TEDBİRLERİ ile ÖZEL BİR DÜZENLEME OLAN BİLGİSAYARDA ARAMA, KOPYALAMA ve ELKOYMA TEDBİRİ

A. CEZA MUHAKEMESİNDE DÜZENLENEN KORUMA TEDBİRLERİNİN KOŞULLARI

1. Kavram

Koruma tedbirleri, ceza muhakemesinin sağlıklı bir şekilde gerçekleştirilmesi, uyuşmazlık konusu somut olaya ilişkin bir karar verilmesi ve verilen kararın uygulanabilmesini sağlamak için[403] hükümden önce ve gecikmesinde sakınca bulunan hallerde, yetkili merciiler tarafından, geçici mahiyette kişilerin temel hak ve özgürlüklerine müdahale oluşturan tedbirlerdir.[404] Bu tedbirler aynı zamanda doğrudan ya da dolaylı olarak delil elde etme yöntemidir.[405] 1415 sayılı CMUK'un yürürlükte olduğu dönemde, öğretide koruma tedbirlerine ilişkin farklı terminoloji kullanılarak; usul tedbirleri, ihtiyati tedbir, ceza yargılaması önlemleri, zorlayıcı tedbir ve temel hak müdahaleleri gibi adlarla[406] anılmaktaydı. 5271 sayılı CMK bu hususu, sistematik bir biçimde "Koruma Tedbirleri" başlığında düzenlemiştir. Bu sebeple artık bir terim karışıklığı bulunmamaktadır.[407] Koruma tedbirleri ile bireyin kişi özgürlüğü, özel hayatın gizliliği, seyahat özgürlüğü, mülkiyet hakkı gibi henüz hüküm verilmeden önce, temel hak ve özgürlükleri sınırlanabilmektedir.[408]

2. Koruma Tedbirlerinin Genel Özellikleri

Koruma tedbirlerinin özellikleri; araç olma, geçici olma ve yasayla düzenlenme olarak sayılabilmektedir.[409]

---

[403] TOROSLU/FEYZİOĞLU, s. 217.
[404] ÖZTÜRK B./EKER KAZANCI B./SONER GÜLEÇ S., 2017. Ceza muhakemesi hukukunda koruma tedbirleri. 2. Baskı. Ankara: Seçkin Yayınları., s.23.
[405] ŞAHİN/GÖKTÜRK, s.113.
[406] ÖZGÜVEN A. D., "Ceza Muhakemesi Kanunu Çerçevesinde Adli Kontrol", Türkiye Barolar Birliği Dergisi, Sayı 81, 2009, s.1.
[407] ÖZTÜRK/KAZANCI/GÜLEÇ, ss.23-24.
[408] ŞAHİN/GÖKTÜRK, s.113.
[409] ÖZGÜVEN, s.2.

a. Araç olma

Koruma tedbirleri, tek başına bir mana ifade etmeyen, muhakeme boyunca eski hali yaşatmak ya da verilecek kararın yerine getirilmesini sağlamak için başvurulan araçlardır.[410] Vasıta oluş, muhakemenin usulüne uygun gerçekleştirilmesi ve amaçlarına ulaşılabilmesini sağlamayı veya bir koruma tedbirinin diğer tedbire yol açabilmesini ifade etmektedir.[411] Bu bağlamda örneğin tutuklama, şüpheli veya sanığın kaçmasını engellemek için, yakalama tedbiri ise tutuklamayı gerçekleştirmek için araç konumunda olabilmektedir.[412]

b. Geçici olma

Koruma tedbirleri, isminden anlaşılacağı üzere tedbir olmaları sebebiyle geçicidir.[413] Ulaşılmak istenen amacın gerçekleşmesi halinde tedbirin uygulanmasına son verilmelidir. Aksi takdirde, tedbir hukuka aykırı olacaktır.[414] Koruma tedbirlerinin geçici olmasından maksat, açıkça sürenin gösterilerek zamanla sınırlandırılması anlamına gelebileceği gibi, geçicilik, haklı gösterilen sebebin ortadan kalkması halinde tedbirin son bulmasını da ifade etmektedir.[415]

c. Yasayla düzenlenme

Koruma tedbirlerinin, Anayasa'nın "Temel Hak ve Hürriyetlerin Sınırlanması" başlıklı 13. maddesi gereği, kişilerin temel hak ve özgürlüklerini etkileyen önlemler olmaları sebebiyle ve kanunilik ilkesi çerçevesinde, yasayla düzenlenmesi gerekmektedir.[416]

3. Koruma Tedbirinin Ön Şartları

Koruma tedbirleri için genel olarak geçerli üç koşul sayılabilmektedir. Bu koşullar; gecikmede sakınca bulunması, görünüşte haklılık ve ölçülülük ilkesine uygunluk olarak sıralanmaktadır.[417]

---

[410] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.109;YENİSEY/NUHOĞLU, s.300.
[411] ŞAHİN/GÖKTÜRK, s.114.
[412] CENTEL/ZAFER, Ceza muhakemesi hukuku, s.321;ÖZGÜVEN, s.3.
[413] ÖZTÜRK/KAZANCI/GÜLEÇ, s.30.
[414] ŞAHİN/GÖKTÜRK, s. 114.
[415] ÖZBEK V. Ö./DOĞAN K./BACAKSIZ P., 2019. Ceza muhakemesi hukuku temel bilgiler. 10. Baskı. Ankara: Seçkin, s.173;YENİSEY/NUHOĞLU, s.300.
[416] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.99; ÖZGÜVEN, s.3.

a. Gecikmede tehlike

Ceza muhakemesinde koruma tedbirleri, uyuşmazlığın esasını çözmeye vakit olmadan başvurulan tedbirlerdir. Bu tedbirler, temel hak ve hürriyetlere karşı bir sınırlama oluşturmaktadır. Temel hak ve hürriyetlere karşı yapılan bu müdahale, ancak söz konusu tedbire gecikmeksizin başvurma zorunluluğu hali ile haklı görülebilir.[418] Tehlike, tedbire başvurulmasıyla istenilen faydanın elde edilemeyecek, ceza muhakemesinin gerektiği şekilde gerçekleşemeyecek olmasıdır.[419] Gecikmede tehlike, muhtemel ve yakın olmalıdır. Başka bir anlatımla, derhal müdahale edilmediği takdirde, korkulan zararın meydana gelme ihtimalini kabul ettiren somut olgulara dayalı bir tehlike bulunmalıdır.[420] Gecikmede tehlikenin bulunup bulunmadığı hususu, her somut olayın özelliklerine göre[421] kararı alacak makam tarafından takdir edilir.[422]

b. Haklı görünüş

Koruma tedbirlerine başvurma esnasında, haklılığının kesin olarak bilinemeyeceği muhakeme evresinde, en azından ilk değerlendirme sonucunda söz konusu tedbirin uygulaması haklı görünmelidir. Aslında koruma tedbirine gidilmesinin haklı olduğu, ancak muhakemenin sonuçlanması ile kesin olarak ortaya çıkabilecektir.[423]

c. Ölçülülük

Ölçülülük ilkesi ile kastedilen, bir koruma tedbirinin uygulanması hakkında verilecek karar ile, bu nedenle ortaya çıkacak zarar arasında makul, akla uygun bir ölçü ve denge olmasıdır. Bazen bu ölçüyü kanun koyucu açıkça kanun hükmünde belirtebildiği gibi, kanun hükmünde yazılı olmasa bile tüm koruma tedbirlerinde oranlılık ilkesine riayet edilmesi gerekir.[424]

Tüm bunlarla birlikte maddi gerçeğe ulaşılması amacıyla uygulanan birçok koruma tedbiri bulunmaktadır. Çalışmamızın ana konusu olan CMK m.134 de bunlardan biridir.

---

[417] ÖZGÜVEN, s.1.
[418] YENİSEY/NUHOĞLU, s 301
[419] CENTEL/ZAFER, Ceza muhakemesi hukuku, s.321.
[420] YENİSEY/NUHOĞLU, s 301.
[421] ŞAHİN/GÖKTÜRK, s. 114.
[422] ÖZTÜRK/KAZANCI/GÜLEÇ, s.31.
[423] ÖZGÜVEN, s.2.
[424] ÖZTÜRK/KAZANCI/GÜLEÇ, ss.32-33.

B. BİLGİSAYARDA ARAMA, KOPYALAMA ve ELKOYMA TEDBİRİ

CMK m.134 hükmü, ceza muhakemesinde kullanılacak olan elektronik delillerin bilişim sistemlerinde araştırma faaliyetini düzenlemektedir.[425] Hukukumuzdaki aramaya ilişkin hükümlerin, bilişim sisteminde uygulanmasının mümkün olmaması sebebiyle, CMK 134. maddesine ayrıca yer verilmiştir.[426]

1. Tedbirin Türk Hukukundaki Gelişimi

Bilişim sistemlerinde arama ve elkoyma tedbiri ilk olarak, 17.12.2004 tarihinde resmi gazetede yayımlanan 5271 sayılı Ceza Muhakemesi Kanun'un 134. maddesinde düzenlenmiştir.[427] Bu tedbir yürürlüğe girmesinden sonra değişikliğe uğramıştır. 6 Mart 2014 tarihinde yürürlüğe giren, 6526 sayılı yasayla iki önemli değişiklik meydana gelmiştir. Bunlardan birincisi madde metninde, daha önceden yer almayan şüphe kriterine yönelik yapılan değişiklikle tedbirin uygulanması, somut delillere dayanan kuvvetli suç şüphesinin varlığı şartına bağlanmıştır. İkinci değişiklik ise madde hükmünce elde edilen verilerin, kopyalarının talep olmaksızın şüpheliye veya vekiline verilmesi hususunun eklenmesidir. Daha sonra 25/7/2018 tarihinde kabul edilen, 7145 sayılı bazı kanun ve kanun hükmünde kararnamelerde değişiklikler yapılmasına dair Kanun ile değişikler yapılmıştır. Bu kanunun16. maddesiyle, CMK m. 134'ün ilk iki fıkrası değiştirilmiştir. Birinci fıkrada yapılan değişiklik ile, gecikmesinde sakınca bulunan hallerde, Cumhuriyet savcısı tarafından da söz konusu tedbire karar verilebilmesi düzenlenmiştir. Ayrıca bu kararın, hakim onayına sunulması ve bununla ilgili detaylara madde metninde yer verilmesi düzenlenmiştir. Bu kanunla yapılan ikinci değişiklikle, elkoyma tedbiri bakımından yeni bir şartın maddeye eklenmesi suretiyle elkoyma tedbirinin uygulama alanı genişletilmiş olup, işleminin uzun sürecek olması halinde elkoyma yapılmasına olanak sağlanmıştır.[428] CMK m. 134'e ilişkin olarak, "*Bilgisayarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma*" başlığı altında, Adli ve Önleme yönetmeliğinin 17. maddesinde düzenlenen,

[425] ŞAHİN C., PROF. Dr. Mehmet Emin Artuk'a armağan, Mahmut Koca(ed), Ankara, Seçkin 2020, s. 749.
[426] ÖZBEK/DOĞAN/BACAKSIZ, s.263.
[427] BOSTANCI Ü./BENZER R., "Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve elkoyma" Uluslararası insan Bilimleri Dergisi, s.1198.
[428] DEĞİRMENCİ, 2018. Bilgisayarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbirinde(CMK m. 134), 7145 sayılı kanunla yapılan değişikliklerin değerlendirilmesi, Terazi Hukuk Dergisi. 13(146), ss.148-150.

bilişim sistemlerinden delil elde etme yöntemine yer verilmiştir.[429] Ayrıca 668 sayılı Kanun Hükmünde, kararname ile olağanüstü halin devamı süresince; gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından da CMK m.134'e karar verilebilmesi yetkisi düzenlenmiştir. Fakat KHK'nın kabulünden sonra 7145 sayılı kanunla, CMK m.134/1'de yapılan değişiklik ile gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısına bu yetki verildiğinden, söz konusu KHK'nın bir önemi de kalmamıştır.[430]

Bunlarla birlikte, bilgisayarda arama ve elkoyma tedbiri, 5271 sayılı kanundan önceki 1412 sayılı Ceza Muhakemesi Usulü Kanununda herhangi bir düzenlemede yer almamaktaydı. Bu sebeple o dönemde bilişim sistemi üzerinde yapılan işlemlere ilişkin genel esaslar dikkate alınmaktaydı.[431]Ayrıca çalışma konumuz tedbir hükmüne benzer nitelikte, Ceza Muhakemesi Kanununun Yürürlük ve Uygulama şekli Hakkında Kanun'un 18. maddesiyle yürürlükten kaldırılan, 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu'nun 4. maddesinde "*kayıt ve verilerin incelenmesi*" başlığı altında, bilgisayarda yer alan verilerin incelenmesi söz konusuydu. Yine bu hükme benzer mahiyette, 26 Ocak 2001 tarihinde yürürlüğe giren 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunun Uygulanmasına ilişkin, Yönetmeliğin 20 ile 25'nci maddeleri arasında, "*kayıt ve verilerin*" incelenmesine yönelik düzenlemelere yer verilmektedir. Ancak bu düzenlemelere bakıldığında, suçların ve delillerin ortaya çıkarılması amacıyla bilgisayar verilerinin incelenmesinin, özel olarak yalnızca çıkar amaçlı örgütlü suçlarda söz konusu olduğu görülmektedir.[432]

2. Tedbirin Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Değerlendirilmesi

Bilişim ve iletişim sektöründeki gelişmeler neticesinde, bu alanda işlenen suç sayıları hızla artmakta ve her geçen gün farklı şekillerde çeşitli suçlar işlenmektedir. Bu suçların ülke sınırlarını aşan mahiyette olması, maddi ceza ve ceza muhakemesi hukuku

[429] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s. 545.
[430] YAŞAR G. D., 2019. Ceza Muhakemesi Kanunu'nda (CMK) bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma. Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi. 14 (173-174), ss. 173-241. s.180.
[431] YAŞAR, s.177; BOSTANCI/BENZER, s. 1198; ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.525.
[432] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.316.

mevzuatları[433] arasında uyumluluk sağlanması ve uluslararası adli iş birliği sağlanması amacıyla, ortak bir ceza politikası oluşturulmak[434] istenmiştir. Bu bağlamda, uluslararası alanda bazı adımlar atıldığı görülmektedir. Atılan adımların en önemlisi, Türkiye'nin de taraf olduğu Avrupa Siber Suçlar Sözleşmesi'dir.[435]

Avrupa Konseyi siber suç sözleşmesi, bilişim alanındaki suçlara ilişkin ilk uluslararası antlaşmadır.[436] Sözleşme, Avrupa Konseyince hazırlanarak 23 Kasım 2001 tarihinde Budapeşte'de taraf devletlerin onayına sunularak, 1 Temmuz 2004 tarihinde yürürlüğe girmiştir.[437]

Sözleşme, dört ana bölüm ve kırk sekiz maddeden oluşmaktadır. Sözleşmenin ilk bölümünde, sözleşmede kullanılan bilişim suçlarıyla alakalı terimler tanımlanmıştır. İkinci bölümde, ulusal düzeyde alınacak önlemler yer almaktadır.[438] Bu bağlamda, maddi ceza hukuku düzenlemeleri hususunda birtakım suç tipleri tanımlanmaktadır. Bununla birlikte, muhakeme hukuku kapsamında, usulü düzenlemelere yer verilmekte ve yargı yetkisi meselesine ilişkin genel ilkeler yer almaktadır. Üçüncü bölümde ise, yukarıda anılan yetkilerin kullanımı bakımından, uluslararası adli yardımlaşmanın çerçevesi oluşturulmuştur. Bu doğrultuda sözleşmeye taraf olan devletler, 2. bölümde belirtilen usulü yetkilere mevzuatlarında yer vermek zorunda oldukları gibi, 3. bölüm sayesinde, sınır aşan nitelikteki siber suçların yabancı devletler tarafından kovuşturulmasında, bu yetkilerden yaralanabilecektir.[439] Dördüncü bölümde ise,

[433] KESKİN S., 2001,"Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi." İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt:59, Sayı: 12, s.155.
[434] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, ss.22-25.
[435] USTA C. A./BENZER R., 2018. Avrupa siber suçlar sözleşmesi ve Türkiye'nin dahil olma süreci. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 4(2), ss.35-42, s. 35.
[436] ÇELİK M., 2018. Bilgisayarda arama, kopyalama ve elkoyma(CMK m.134). Yüksek Lisans Tezi. İstanbul: Üniversitesi Sosyal Bilimler Enstitüsü, s. 24; YAŞAR, s.186; ERDOĞAN, Türk ceza Kanunu'nda bilişim suçları, s.67; ÖNOK M., 2013. Avrupa konseyi siber suç sözleşmesi ışığında siber suçlarla mücadelede uluslararası işbirliği (Prof. Dr. Nur Centel'e Armağan). Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi. 19 (2), ss. 1229 – 1270, s.1241.
[437] ÖNOK, s.1241; İÇEL K., Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında "Avrupa Siber Suç Politikasının Ana İlkeleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Yıl: 2001, Cilt: 59, Sayı:1-2, s.6
[438] ERDOĞAN, Türk ceza Kanunu'nda bilişim suçları, s. 67.
[439] ÖNOK, ss.1242-1244.

sözleşmenin yürürlüğü, çekince imkânı, anlaşmazlıkların çözümü gibi özel bir takım hallere yer verilmiştir.[440]

Avrupa Konseyi Siber Suç Sözleşmesini Türkiye, 10.11.2010 tarihinde imzalamıştır.[441] 22.04.2014 tarihinde 6533 sayılı kanun ile "Sanal Ortamda İşlenen Suçlar Sözleşmesi" başlığıyla sözleşme, TBMM tarafından kabul edilmiştir. 02.05.2014 tarihli 28988 sayılı resmi gazetede yayımlanarak, yürürlüğe girmiştir.[442] Sözleşmenin ülkemizde yürürlüğe girmesiyle birlikte, başta çalışma konumuzu oluşturan CMK m. 134 olmak üzere, iç hukukumuzdaki birtakım düzenlemelerde sözleşmeye uygun biçimde değişiklikler yapılması gerekmektedir.[443] Ayrıca, soruşturma ve kovuşturma makamlarının sözleşmeye uygun bir biçimde işlemleri gerçekleştirmesi gerekmektedir.[444]

Bilişim verilerinin delil olarak kullanılabilmesi için bunların toplanması ve elde edilmesi sırasında uyulması gereken kurallara, sözleşmenin 14. ile 21. maddelerinde ve buna ilişkin açıklayıcı raporda (Explanatory Report No. 131-239) yer verilmiştir.[445] Söz konusu madde aralığındaki düzenlemelerin konuları: 16. madde; "*depolanmış bilgisayar verilerinin süratli bir biçimde korunması*", 17. madde; "*trafik verilerinin süratli bir biçimde korunması ve kısmen açıklanması*," 18. madde; "*üretim emri*", 19. madde; "*depolanmış bilgisayar verilerinin aranması ve bunlara el konulması*," 20 madde; "*trafik verilerinin gerçek zamanlı toplanması*, " 21. madde; "*içerik verilerinin yolunun kesilip ele geçirilmesi* " şeklindedir.[446] Sözleşmenin 16 ile 21. maddelerinde yer verilen tedbirlerin uygulanmasında, 14 ve 15. maddelerinde belirtilen usullere uygun olması gerekmektedir. Yani, insan haklarına ilişkin temel yükümlülüklerin göz ardı edilmemesi gerekmektedir.[447]

---

[440] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.33.
[441] ORTA, s.94; ERDOĞAN, Türk ceza Kanunu'nda bilişim suçları, s.73; ÖNOK, s, 1241; YETİM S., 2014. Siber suçlar, yargılama yetkisi ve yeni bir model önerisi. Türkiye Adalet Akademisi Dergisi. Yıl:5 (17), ss.177-232, s. 187.
[442] YAŞAR, s.186; DÜLGER, . Bilişim suçları ve internet iletişim hukuku, s.543.
[443] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.518; ERDOĞAN, Türk ceza Kanunu'nda bilişim suçları, ss.68-69.
[444] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s. 543.
[445] NUHOĞLU/YENİSEY, s.410.
[446] KESKİN, ss.156-157.
[447] BAŞTÜRK İ., Bilgisayar sistemleri ile verilerinde arama, kopyalama ve elkoyma. Fasikül Hukuk Dergisi. Yıl:2 (9) ağustos 2010 ss. 23-3, s.27.

Çalışma konumuz olan CMK m.134, sözleşmenin 19. maddesinde düzenlenen "*saklanan bilgisayar verilerinin aranması ve bunlara elkonulması*"[448] hükmünün iç hukuka uyarlanmış halidir.[449] Sözleşme, iç hukukumuzda bağlayıcı kurallar öngörmüş fakat bu kuralların küçük bir kısmı CMK m.134'e aksettirilmiştir.[450] Avrupa Siber Suç Sözleşmesindeki yeni teknolojik araştırma yöntemleri, kişinin özel hayatını kısıtlaması sebebiyle, söz konusu sözleşmedeki yöntemlerin Anayasa'nın 13. maddesi gereği kanun ile düzenlemesi gerekmektedir. Dolayısıyla, bilgisayarda delil elde etmek adına kullanılacak yetkiler, ayrıntılı bir şekilde düzenlenmelidir. Bu bağlamda CMK m. 134 hükmü ise yeterli değildir.[451]

Sözleşmeye taraf olarak, uluslararası yükümlülüklerden ötürü gerekli değişikliklerin yapılması gerekir. Aslında sözleşmenin imzaya açılma tarihi 2001 olup, süre zarfında bilişim alanında yeni teknolojik gelişmeler ortaya çıkmıştır. Bu bağlamda, yeniliklere karşı yeni soruşturma ve kovuşturma teknikleri söz konusudur. Bu sebeple CMK ve

---

[448] AK-SSS'nin "Saklanan Bilgisayar Verilerinin Aranması ve Bunlara El Konulması" başlıklı 19. maddesi;
"1. Taraflardan her biri, yetkili mercilerinin kendi ulusal sınırları içinde aşağıdakileri arama ya da bunlara benzer şekilde erişim sağlama konusunda yetkili olabilmeleri için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır:
a. bir bilgisayar sistemi ya da bu sistemin parçası ve bunlarda saklanan bilgisayar verileri; ve
2. bilgisayar verilerinin saklandığı cihazlar.
3. Tarafların her biri, yetkili mercilerinin paragraf 1 (a) uyarınca belirli bir bilgisayar sisteminde ya da bu sistemin bir parçasında arama yapması ya da bunlara erişim sağlaması söz konusu olduğunda, ayrıca, aranan verilerin kendi ulusal sınırları içindeki başka bir bilgisayar sisteminde ya da bu sistemin bir parçasında saklandığına dair gerekçeleri bulunduğunda, söz konusu mercilerin arama ya da erişim işlemlerini bu sistemi kapsayacak şekilde genişletebilmelerini sağlamak üzere gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.
4. Taraflardan her biri, yetkili mercilerinin kendi ulusal sınırları içinde paragraf 1 veya 2 uyarınca erişilen bilgisayar verilerine elkoyma ya da bunları başka şekillerde koruma altına alınması konusunda yetkili olabilmeleri için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır. Bu işlemler arasında, aşağıdakilerin yapılabilmesine yönelik yetkilerin sağlanması bulunacaktır: a. herhangi bir bilgisayar sistemine ya da bu sistemin bir parçasına veya bilgisayar verilerinin saklandığı cihazlara el konulması ya da bunların benzer şekilde koruma altına alınması;
5. bu bilgisayar verilerinin kopyalanıp alıkonulması;
6. söz konusu saklı bilgisayar verilerinin doğruluğunun muhafaza edilmesi; ve
7. erişilen bilgisayar sistemindeki söz konusu verilerin erişilemez kullanılamaz hale getirilmesi ya da silinmesi.
8. Taraflardan her biri, yetkili mercilerinin ilgili bilgisayar sisteminin işleyişi hakkında ya da bu sistem içindeki bilgisayar verilerinin korunması için kullanılan önlemler hakkında bilgi sahibi olan herhangi bir kişiye, paragraf 1 ve 2'de belirtilen işlemlerin yapılabilmesi için gerekli bilgileri makul şekilde vermesi yönünde talimat vermesi için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır.
9. İş bu maddede sözü geçen yetki ve usuller madde 14 ve 15'e tabi olacaktır." şeklindedir.
[449] ORTA, s.216; TANRIKULU, s.125; BAŞLAR, Y., 2013, Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine Ve Korunmasına İlişkin Usul Hükümleri. Uyuşmazlık Mahkemesi Dergisi, S.3, s.98.
[450] YENİSEY, s.134
[451] YENİSEY/NUHOĞLU, s.408.

ilgili yönetmelikte bir değişiklik yapılmak istendiğinde, sadece AKSSS hükümleriyle sınırlı kalınmayıp, güncel gelişmelere de yer verilmelidir.[452]

Sözleşmenin 19. maddesinin kaleme alınması amacına, açıklayıcı rapor metninin 184'ncü paragrafında yer verilmiştir. Buna göre, belli bir cezai soruşturmaya ilişkin delil elde edilebilmesi için, depolanmış bilgisayar verilerin aranmasına ve bunlara el konulmasına dair ulusal kanunların modernleştirilmesinin ve uyumlaştırılmasının sağlanması, maddi nesnelere ilişkin arama ve elkoyma hükümlerine paralel bir sistemin soyut veriler içinde kurulması olduğu belirtilmiştir.[453]

CMK 134 ile sözleşmenin 19. maddesi karşılaştırıldığında benzer hükümler içermekle birlikte, bir takım farklılıklar bulunmakta olup tam anlamda uygun değildir.[454] Sözleşmenin 19. maddesinin başlığı "*saklanan bilgisayar verilerinin aranması ve bunlara elkonulması*" şeklinde geniş bir kapsam ifade etmektedir. Ayrıca söz konusu maddenin ilk fıkrasında, "*bilgisayar sistemi ya da bu sistemin parçası ve bunlarda saklanan bilgisayar verileri"* ile ikinci fıkrasında yer alan "*bilgisayar verilenin saklandığı cihazlar*," tedbirin konusu olarak ifade edilmiştir. Buna karşılık CMK 134'ün başlığının "*bilgisayar, bilgisayar programlarında ve bilgisayar kütüklerinde arama kopyalama ve elkoyma*" şeklinde olması, tedbirin uygulama alanının dar yorumlanmasına sebep olmaktadır.[455] Bu hususta ayrıca tedbirin konusunu nispeten genişleten AÖAY'nin 17. maddesinde "*bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları*" hakkında da uygulanabileceği belirtilmiştir.[456] Dolayısıyla bazı hususlar yönetmelikle giderilmeye çalışılmış ise de, tam manada giderilememiştir. Özellikle bilişim suçları dikkate alındığında etkin bir soruşturmada, temel hak ve özgürlükleri doğrudan ilgilendiren hususların yönetmelikle giderilmeye çalışılması normlar hiyerarşisine uygun olmayıp, kanun değişikliği ile giderilmesi yerinde olacaktır.[457]

---

[452] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s.554.
[453] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.187.
[454] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.224.
[455] TANRIKULU, s.356.
[456] ÇELİK, s.27.
[457] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.224.

Bununla birlikte, sözleşmede yer alan suç unsuru ya da suç aracı olan verilerin erişilmez[458] kılınması ve kopyaları alındıktan sonra taşınması ya da silinmesine ilişkin hususlara CMK m.134'te yer verilmemiştir. Öyle ki CMK 134. madde de bu tür verilerin şüpheliye iade edilmesine ilişkin açık hüküm bulunması, sözleşme ile CMK arasında çelişkiye sebep olmaktadır.[459]

3. Bilgisayarda Arama, Kopyalama ve Elkoyma Tedbirinin, Genel Arama ve Elkoyma Tedbirleri ile İlişkisi

Bilişim sistemleriyle alakalı olarak işlenen suçlarda, klasik delil elde etme yöntemleri yetersiz kalmaktadır. Zira elde edilecek delillerin elektronik mahiyette olması, tedbirin uygulanması esnasında teknik kısmının da göz önünde bulundurulmasını gerektirmektedir. Bu sebeple, tedbirin uygulanması noktasında teknik boyut ve hukuk kurallarına riayet edilerek, disiplinler arası bir yaklaşımla tedbirin ortaya koyulması gerekmektedir.[460] Aksi halde, birçok temel hak ve özgürlüklerin ihlal edilmesi sonucu doğacaktır. Dolayısıyla bir bilişim sisteminde delil elde edilmesi farklı bir yöntem olup, genel arama ve elkoyma tedbirlerinden ayrılmaktadır.[461]

a. CMK m. 116 hükmündeki genel arama tedbiri açısından değerlendirilmesi

Arama, suç delillerinin ya da müsadereye tabi olacak eşyanın elde edilmesi amacıyla, bir kimsenin üzerinde, konutunda, işyerinde ve eşyasında yapılan araştırma yöntemidir.[462] Arama tedbirine özel hayatın gizliliği, kişi özgürlüğü, konut dokunulmazlığı gibi temel hak ve özgürlüklere müdahale oluşturan bir tedbir olması sebebiyle, Anayasa'nın 20. ve 21. maddelerinde yer verilmiş[463] olup, AİHS'nin 8. maddesinde de paralel olarak özel hayatın gizliliği güvence altına alınmıştır.[464] Arama, suç işlenmesini önlemek amacıyla yapılıyorsa, buna önleme araması (Örneğin PVSK m.9) denir. Suç işlendikten sonra yapılan aramaya ise, adli arama denilmekte ve CMK

[458] KESKİN, s. 171.
[459] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.224.
[460] BAŞLAR, Ceza yargılamasında elektronik delil, ss.154-155; DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.311.
[461] ÇELİK, ss.18-19.
[462] ÇÖPOĞLU, H. S., 2019/1, Ceza Muhakemesi Hukukunda Arama Koruma Tedbirinde Belirlilik İlkesi. Ankara Barosu Dergisi, ss. 157-229, s. 158.
[463] ŞAHİN/GÖKTÜRK, s.137-138; TOROSLU/FEYZİOĞLU, ss.244-245.
[464] ÖZTÜRK/KAZANCI/GÜLEÇ, s.126.

m. 116 ile düzenlenmektedir.[465] Söz konusu tedbir, suçun işlendiği ya da teşebbüs edildiği şüphesine istinaden başlatılan ceza soruşturması ya da kovuşturması kapsamında başvurulan bir koruma tedbiri olmaktadır.[466]

Maddi gerçeğin ortaya çıkarılması amacıyla genel arama hükmü CMK' nın 116. maddesinde, "*Şüpheli ve Sanıkla ilgili Arama" başlığı altında "Yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe varsa; şüphelinin veya sanığın üstü, eşyası, konutu, işyeri veya ona ait diğer yerler aranabilir*" şeklinde düzenlenmiştir. Adli arama, AAÖY m.5'te, "*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 yapılan araştırma işlemi*" olarak ifade edilmiştir.

Bilgisayarda arama ve elkoyma tedbirini diğer eşyalar üzerindeki aramalardan ayıran en önemli fark, bilişim sistemlerinin diğer eşyalara göre daha fazla bireylerin temel hak ve özgürlüklerine müdahale içermesiyle, kişilerin özel hayatı, haberleşme hürriyeti, kişinin kendi maddi manevi geliştirme hakkı[467] ve mülkiyet hakkı gibi değerler ile doğrudan bağının bulunmasıdır.[468]

Genel arama tedbiri ile çalışma konumuz olan CMK m134'te yer alan bilişim sistemleri üzerindeki tedbirler değerlendirildiğinde, uygulamada bir takım sorunlar meydana gelmektedir. Şöyle ki, genel bir arama kararı kapsamında şüphelinin bilişim sisteminin de bu hususa ilişkin ayrı bir arama kararı olmaksızın, aranması söz konusu olmaktadır.[469] CMK m.116 da yer alan genel arama doğrultusunda icra edilen bir arama esnasında, şüphelinin kullanmış olduğu bilgisayar üzerinde de bir arama işleminin gerçekleştirilebilmesi için, ayrıca CMK m.134 kapsamında bir kararın mevcut olması gerekmektedir.[470] Bu hususa riayet edilmeden yapılmış olan bir arama, hukuka aykırılık

[465] ŞAHİN/GÖKTÜRK, ss.137-138.
[466] ÖZTÜRK/KAZANCI/GÜLEÇ, s. 124.
[467] TANRIKULU, ss.352-353.
[468] ŞAHİN, PROF. Dr. Mehmet Emin Artuk'a armağan, s. 749.
[469] ÇELİK, s.22.
[470] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s.552; ORTA, s.221; KARAGÜLMEZ, s.505; BAŞTÜRK, ss.27-28.

teşkil edecektir.[471] Zira genel arama tedbirinin şartları gerçekleşmiş olsa da, bilgisayar üzerinde bir arama yapmak için şartlar gerçekleşmemiş olacaktır.

Bununla birlikte işlem yapılacak olan bilişim sistemi, kişinin konutunda veya işyerinde olabilir. Bu nedenle, konut veya işyeri içerisinde de arama gerçekleştirileceğinden, ayrıca 116. madde uyarınca bir arama kararı verilmesi gerekip gerekmediği sorunu ortaya çıkabilir. Başka bir deyişle, bilişim sisteminde arama, kopyalama elkoymaya (CMK m.134) yönelik bir karar genel aramayı da kapsayacak mıdır? Öğretide bir görüşe göre, şüphelinin veya sanığın kullanmakta olduğu bilgisayar ya da bilgisayarın çıkarılabilen diğer donanımlarının, şüphelinin ya da başkasının konutunda veya işyerinde bulunması, hayatın olağan akışında doğal bir durumdur. Bu bakımdan iş yerinde ya da konutta, CMK. m.134'teki tedbirin konusunu oluşturan aygıtların bulunabilmesi için, yapılacak olan arama işleminin niteliği de adli arama olmakla birlikte bu arama, CMK. m.134'teki aramanın zorunlu bir unsurunu oluşturmaktadır. Bu nedenle bilgisayarın veya diğer benzeri aygıtların bulunabilmesi için konutta ya da işyerlerinde gerçekleştirilecek aramalarda, CMK. m.116 ve devamındaki hükümlere göre ayrıca bir arama kararına gerek duyulmamalıdır.[472] Buna karşılık bir görüşe göre, iş yeri ya da konutlarda gerçekleştirilecek arama hangi amaçla ile olursa olsun, CMK m.134 bağlamında alınacak bir kararın haricinde, genel hükümlere göre fiziki bir arama kararına daha ihtiyaç vardır. Bu görüşe göre, gece arama yapılması koşulları ile gecikmesinde sakınca bulunan hallerde, savcının karar vermesi durumu gibi ön şartların birbirinden bağımsız olan ve bilişim sistemi için gidilen konutta tesadüfen başkaca suçlara ilişkin delillerin bulunması gibi durumların gerçekleşmesi mümkündür.[473]

Tüm bunlarla birlikte, bilişim sistemlerine yönelik arama ve elkoyma tedbirlerine ilişkin CMK m.134 hükmü uygulanacak, ancak bu madde kapsamına girmeyen hususlar için yine bu maddeye aykırı olmamak üzere, genel arama ve elkoyma hükümleri uygulanacaktır.[474] Böylece, CMK m.134 bakımından tereddüt oluşturabilecek birçok husus çözüme kavuşacaktır. Zira, genel arama tedbirine ilişkin mevzuatımızda

[471] ÜNVER Y./HAKERİ H., 2019. Ceza muhakemesi hukuku. 16. Baskı. Ankara: Adalet Yayınevi, s.424.
[472] YAŞAR/DURSUN, s.22.
[473] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.223.
[474] TANRIKULU, s.351; ÖLMEZ A., 2009. Bilgisayarda, bilgisayar programlarında ve kütüklerinde kopyalama ve bunlara elkoyma, Terazi hukuk dergisi. (10), ss.45-52, s.51.

açıklayıcı düzenlemeler mevcuttur. (Gece yapılacak arama(m 118), arama kararı (m.119), aramada hazır bulunabilecekler (m.120), arama sonunda verilecek belge (m.121) vb.).[475]

b. CMK m.123 hükmündeki elkoyma tedbiri açısından değerlendirilmesi

Elkoyma, müsadere edilebilecek veya ceza muhakemesinde ispat aracı olabilecek[476] eşyanın adliye eline alınmasıdır. Eşyanın ya da malvarlığı değerine ilişkin şahsın rızasına dayanan bir teslim durumu söz konusu olursa, bu durumda muhafaza altına alma durumu gerçekleşecektir.[477] Elkoyma tedbirinin uygulanması, genellikle arama tedbiri sonrasında başvurulması şeklinde karşımıza çıkmaktadır.

Elkoyma, CMK m.123'te "*İspat aracı olarak yararlı görülen ya da eşya veya kazanç müsaderesinin konusunu oluşturan malvarlığı değerleri, muhafaza altına alınır. Yanında bulunduran kişinin rızasıyla teslim etmediği bu tür eşyaya elkonulabilir*." şeklinde düzenlenmiştir. Bununla birlikte AÖAY m.4'te elkoyma, "*Suçun veya tehlikelerin önlenmesi amacıyla veya suçun delili olabileceği veya müsadereye tâbi olduğu için, bir eşya üzerinde, rızası olmamasına rağmen, zilyedin tasarruf yetkisinin kaldırılması işlemini ifade eder*" şeklinde tanımlanmıştır.

Bilişim sisteminde arama ve elkoyma tedbirinin uygulanmasında evrensel hükümler dikkate alınmalı, mağduriyete sebep olunmamalıdır. Zira, elektronik delillerin toplanmasında kişilerin özel hayatı, konutu, haberleşme dokunulmazlığı gibi kişilerin temel haklarına devlet tarafından bir müdahale öngörülmektedir. Özellikle, kişisel veriler ve özel hayatın gizliliğinin korunması ilkelerine, delillerin toplanmasında dikkat edilmelidir.[478] Bu bağlamda ölçülülük ilkesine riayet edilmelidir. Çalışma konumuz tedbir bakımından, kamu yararı ile temel hak ve özgürlükler dikkate alınarak hüküm düzenlenmiştir. Bu düzenleme bir koruma tedbiri olmasından dolayı diğer koruma tedbirleri gibi geçici ve araç olma özelliğini taşımaktadır. El konulan aracın, üzerinde çalışma bittiğinde iade edilmesi de geçici olduğunu göstermektedir. Bu doğrultuda

[475] YAŞAR, ss.193-194.
[476] ŞAHİN/GÖKTÜRK, s.143.
[477] ÖZTÜRK/KAZANCI/GÜLEÇ, s.151; TOROSLU/FEYZİOĞLU, s.249.
[478] ORTA, ss.215-216.

çözümün yapılması ve gerekli kopyaların alınmasından sonra cihazlar iade edilerek hak kayıpları önlenmelidir.[479]

Sonuç olarak, bilişim sistemleri üzerinde arama, kopyalama ve elkoyma tedbirinin uygulanması için, madde 116 ve 123'ten ayrı olarak özel bir arama ve elkoyma kararı gerekmektedir. Bu durum gerekçede, " *madde, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve geçici elkoyma konularını düzenlemektedir. Bireye ait kişisel bilgiler üzerindeki hak, temek insan haklarından olduğundan hakkın kısıtlanabilmesi için yasal düzenleme gerekeceği açıktır*." şeklinde belirtilmiştir.[480] CMK m. 134, aynı kanundaki 116 ve 123. maddeler ve devamında yer alan düzenlemelerden farklı olarak, bilişim sistemlerinde yer alan soyut veriyi konu alan bir koruma tedbiridir. Söz konusu tedbir ile bilişim sisteminde bulunan verilere ilişkin bazı koruma tedbirlerin uygulanması noktasında yasal bir zemin sağlanmıştır.[481]

4. Bilişim Sisteminde Arama, Kopyalama ve Elkoyma Tedbirinin İletişimin Tespiti Tedbiri ile İlişkisi

CMK m. 135 hükmünde, telekomünikasyon[482] yolu ile iletişimin tespiti,[483] dinlenmesi ve kayda alınması[484] hususları düzenlemektedir. Telekomünikasyon yolu ile iletişimin tespiti, dinlenmesi ve kayda alınması, *"yurt dışı çıkışlar da dâhil olmak üzere her türlü sabit veya mobil iletişim aletleri ile birlikte İnternet üzerinden yapılan her türlü iletişim detay bilgileri, yani; arayan, aranan, aranan donanım kimlik numaraları ve bilgileri,*

[479] ORTA, s.220.
[480] ŞAHİN C., 2005. Ceza muhakemesi kanunu gazi şerhi. 1. Baskı, Ankara: Seçkin Yayınları, s.371
[481] DEĞİRMENCİ, Bilgisayarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbirinde(CMK m. 134), 7145 sayılı kanunla yapılan değişikliklerin değerlendirilmesi, s. 146.
[482] Telekomünikasyon Yoluyla Yapılan İletişimin Tespiti, Dinlenmesi, Sinyal Bilgilerinin Değerlendirilmesi ve Kayda Alınmasına Dair Usul ve Esaslar ile Telekomünikasyon İletişim Başkanlığının Kuruluş, Görev ve Yetkileri Hakkında Yönetmeliğin 3. maddesinin r fıkrasında, telekomünikasyon: "*her türlü işaret, sembol, ses ve görüntünün ve elektrik sinyallerine dönüştürülebilen her türlü verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınması*" şeklinde tanımlanmıştır.
[483] İlgili yönetmelik madde 3-i'de iletişimin tespiti: "*İletişimin içeriğine müdahale etmeden iletişim araçlarının diğer iletişim araçlarıyla kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesine yönelik işlemleri.*" şeklinde ifade edilmiştir.
[484] İlgili yönetmelik madde 3-h' de iletişimin dinlenmesi ve kayda alınması: *"Telekomünikasyon yoluyla gerçekleştirilmekte olan konuşmalar ile diğer her türlü iletişimin uygun teknik araçlarla dinlenmesi ve kayda alınmasına yönelik işlemleri,"* olarak tanımlanmıştır.

kullanıcı ve yapılan İnternet bağlantı bilgileri, her türlü veri alış verişi ve metin mesajlaşma bilgileri ve abone bilgilerinin canlı olarak alınmasını" kapsamaktadır.[485]

Çalışma konumuz gereği CMK m. 135 hükmünün tüm yönleriyle değil, bilişim sistemi aracı kılınması suretiyle gerçekleştirilen iletişim kapsamındaki elektronik deliller bağlamında değerlendirilecektir. Bilişim sisteminde arama yapılması ile, elektronik ortamda kişiler arasında canlı olarak gerçekleşen iletişime ilişkin arama yapılması, farklı işlemlerdir. Bu bağlamda internet üzerinden veya kızılötesi, bluetooth, wifi, kablolu ağ gibi yollarla bilişim sistemi vasıtasıyla canlı olarak gerçekleştirilen iletişimin tespit edilmesi, CMK m. 135 çerçevesinde olacaktır. Ayrıca iletişimin dinlenmesi sadece telefon ile yapılan konuşmalar için değil, internet üzerinden yapılan konuşmalar için de geçerlidir. [486]

İletişimin tespiti ile çalışma konumuz değerlendirildiğinde, öğretide farklı görüşler bulunmaktadır. Öğretide bir görüşe göre, akış halinde bulunan verilerin elde edilmesi, CMK m. 135 düzenlemesine tabi olacaktır. Bu görüş, bilişim sisteminde iletişimin denetlenmesi ve kayda alınması, bazı yazılımlar vasıtasıyla bilişim sistemleri arasında gönderilen veri trafiğinin tespiti, veri paketlerinin toplanması ve bu veri paketlerinden bilgilerin alınması şeklinde gerçekleştiğini ifade eder. Ayrıca CMK m. 135 çerçevesinde bilişim sistemleri arasındaki iletişim denetlenirken, uzaktan bilişim sistemine erişilerek, kullanıcının bilgisi olmaksızın verilerin ele geçirilemeyeceğini ifade edilmektedir.[487] Buna karşılık öğretide bir başka görüş, CMK m. 134' ncü maddenin gerekçesinden hareketle, 135. maddede bilgisayar işlemekte iken içeri girildiğini ve ilgilinin bundan haberi olmadığını, CMK m. 134'te ise[488] bilişim sisteminde arama tedbirinin telekomünikasyon yoluyla iletişimin denetlenmesinden farklı olarak durağan haldeki araçlarda araştırma, arama yapılmakta ve ulaşılan delillere el konulmakta olduğunu

[485] TANRIKULU, s.471.
[486] GÖKSOY, ss.173-174.
[487] Bu görüş CMK 135'nci maddenin gerekçesinde bilgisayar işlemekte iken içerisine girilmesinden bahsedildiğini, akış halindeki verilere yönelik bilgisayara girmek suretiyle elde edilmesine yer verilmediğini belirtmektedir. "*CMK m. 135 nasıl ki hakkında dinleme kararı verilen taşınabilir telefonun kullanılması suretiyle ortam dinlenmesi yapılmasına olanak sağlamıyor ise bilgisayara girilerek arama yapılmasına olanak sağlamaz. Bilgisayara erişilerek içeriğinde arama yapılması yöntemi uzaktan arama tedbiridir ve Türk hukukunda uzaktan arama tedbirini düzenleyen bir hüküm bulunmamaktadır."* DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, ss.384-385.
[488] ŞAHİN, Ceza muhakemesi hukuku gazi şerhi, s.372.

ifade etmiştir.[489] Başkaca bir görüş ise CMK 135 ve CMK m.134 ile alakalı olarak, ayırt edici hususun haberleşme ile haberleşme bittikten sonra haberleşme içeriğinin saklandığı ortam olduğunu ve bu ortama göre, uygulanacak hukukun tespit edilebileceğini ileri sürmektedir. Bu görüş, iletişim kavramının tanımından yola çıkmaktadır. İletişim; "*telefon, telgraf, televizyon, radyo vb. araçlardan yararlanarak yürütülen bilgi alışverişi, bildirişim, haberleşme, muhabere, komünikasyon*" şeklinde tanımlanmaktadır.[490] Dolayısıyla söz konusu veriler, haberleşme bittikten sonra değişik şekillerde depolanarak, başkaca bir haberleşmenin konusu yapılıncaya kadar artık haberleşmenin konusu olmayacaktır.[491] Bu doğrultuda hangi aşamada olduğu fark etmeksizin, akan iletişim verisinin yakalanması ve kayıt altına alınması durumunda, CMK 135. maddede düzenlenen tedbir söz konusu olacaktır.[492] Başka bir görüşe göre ise CMK. m.135'e göre yapılan iletişimin dinlenmesi ve kaydı, geçmişe dönük olarak değil, geleceğe dönük olarak yapılabilir. İnternet ortamında gerçekleştirilen iletişime ilişkin kayıtlar bilişim sisteminde kayıt altına alındığında, bu iletişim kayıtları hakkında CMK. m.134 tedbirleri uygulanabilir.[493]

Öğretide bir başka görüşe göre, bilişim sisteminde bulunan veya internette yer alan verilerin, delil olarak ceza muhakemesinde değerlendirilmesi bakımından bir ayrım yapılması gerekmektedir. Şöyle ki, verilerin nakledildiği esnada canlı olarak dinlenmesi, algılanması ya da ele geçirilmesi halleri gerçekleşebilir. Veri nakli sırasında, her verinin bilgisayar ağı içerisinde bıraktığı akış izine sinyal bilgisi denilmektedir. Bu sinyal bilgilerinin kamu makamlarınca daha sonradan çözümlenmesi amacıyla saklanması, özel bir yetki gerektirmektedir. Bu bağlamda verilerin bir yerden başka bir yere akışını belirten veri ile gönderilen yani durağan halde ki verinin içeriği aynı değildir.[494] Bu görüşe göre, bilişim sisteminde kayıtlı bir şekilde bulunan verinin, bilgisayarda arama işlemiyle elde edilmesi esnasında yukarıda bahsettiğimiz sinyal bilgisi niteliğindeki verilerin elde edilebilmesi için, CMK m. 135 kapsamında iletişimin

[489] ŞAHİN/GÖKTÜRK, s.154; ÖLMEZ, s.46.
[490] https://sozluk.gov.tr/ [13.08.2020].
[491] TANRIKULU, s.472.
[492] Bu görüşe göre, bilişim sisteminde arama ve elkoyma tedbirinin uygulanması için telekomünikasyon yolu ile bir iletişimin varlığı gerekmemektedir. Fakat CMK 135. maddesinin uygulanabilmesi için bilgi alış verişinin gerçekleşmesi, yani bir iletişim söz konusu olmalıdır. TANRIKULU, s.475.
[493] YAŞAR/DURSUN, s.23.
[494] Bu görüşe göre, sistem de kaydedilmiş, saklanmış olan veriler söz konusu olmalıdır. Bu durumda en son yapılan kayıt tarihine bakılarak saptanmalıdır. Başka bir deyişle, failin daha önceden kaydettiği veriyi, değiştirme olanağını bulunmamalıdır. YENİSEY/NUHOĞLU, s. 411.

denetlenmesi kararı gerekirken, gönderilen verinin içeriğine erişilmesi için CMK m. 134 uyarınca ayrı bir karar verilmesi gerekmektedir. Bunların yanı sıra, şifrelenmiş ve farklı bilgisayarda bulunan verilerin bir araya getirilmesiyle bir anlam ifade eden veriler söz konusu olması durumunda ise, iki tip karar verilmesi amaca ulaşmayı zorlaştırmaktadır. Bu halde, şifrelenmiş verilere ulaşmak için ayrı bir karar verilmelidir. Bu hususa 23.11.2001 tarihli Avrupa Konseyinin siber suç sözleşmesinde ve 6.9.2001 tarihli Avrupa parlamentosu normunda yer verilmiştir.[495]

Sonuç olarak, bilişim sistemi üzerinde durağan (depolanmış) veriler söz konusu ise CMK m.134, akış halindeki(iletişim esansındaki) veriler mevzu bahis olması durumunda ise CMK m.135(telekomünikasyon araçlarına ilişkin) düzenlemesi uygulanmalıdır.[496]

5. Yasal Düzenleme

Kanun koyucu, bilişim sistemleriyle işlenen suçlarda veya klasik suçlarla ilgili delillerin elde edilmesi ve bu sistemler üzerinde yapılacak olan arama, kopyalama[497] ile, geçici elkoyma işlemlerinde uygulanmak üzere CMK m.134 hükmünü ortaya koymuştur.[498] Bu madde hükmü ile aslında klasik arama ve elkoyma tedbirlerinin elektronik ortama uyarlandığını[499] ve bilişim sistemleri üzerinde yapılacak araştırmaların ayrıca düzenlendiğini görmekteyiz.[500]

Özel nitelikli olan bu düzenleme, "*bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma*" başlığıyla kaleme alınmıştır. Buna göre; *"Madde 134(1) Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine karar verilir.*

[495] YENİSEY/NUHOĞLU, ss.411-412.
[496] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s.545.
[497] ÖZTÜRK/KAZANCI/GÜLEÇ, ss.192-193
[498] ÖLMEZ, s.47.
[499] KESKİN, 169; BAŞTÜRK, s.25.
[500] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.516.

Cumhuriyet savcısı tarafından verilen kararlar yirmi dört saat içinde hâkim onayına sunulur. Hâkim kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde çıkarılan kopyalar ve çözümü yapılan metinler derhâl imha edilir.

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.

(4) Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

(5) Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır." şeklindedir. Ayrıca Adli ve Önleme araması yönetmeliğinin 17. maddesinde aynı şekilde "*Bilgisayarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma*" başlığı altında düzenlenmeye yer verilmiştir.[501] Söz konusu yönetmeliğin

[501] *Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma*
Madde 17 – "Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması hâlinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.
Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması hâlinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması hâlinde, elkonulan cihazlar gecikme olmaksızın iade edilir.
Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır.
(Değişik ibare:RG-29/4/2016-29698) Üçüncü fıkraya göre alınan yedekten elektronik ortamda bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.
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."

ilgili maddesinde birkaç ifade haricinde CMK m.134 hükmünün tekrar edildiği görülmektedir.[502]

Suç eşyası yönetmeliğinin "Suç eşyasının muhafazası" başlıklı 8. maddesinin 3'ncü fıkrasında, "*Bilgisayar, bilgisayar kütükleri ve bu sisteme ilişkin verilerin asıl ya da kopyaları, ses ve görüntü kayıtlarının bulunduğu depolama aygıtları gibi elektronik eşya, bozulmalarını engelleyecek, nem, ısı, manyetik alan ve darbelerden korunmalarını sağlayacak müstakil uygun alanlarda muhafaza edilir."* şeklinde düzenleme yer almaktadır.[503] Hassas yapıya sahip elektronik delillerin nasıl taşınıcağına, korunacağına ve inceleneceğine dair CMK'da bir hüküm bulunmamakta, ancak anılan yönetmelikte özel bir hüküm bulunmaktadır.[504] Öğretideki bir görüşte, sözleşmenin 19. maddesinin 4. fıkrasında, "*Sözleşme'de bilişim sistemlerinin aranması ve elkonulması hususlarında özel bir bilgiye sahip herhangi bir kişinin yardımcı olmaya zorlanmasına izin verilmiştir."* ifadesi yer almasına rağmen, Türk hukukuna bakıldığında bilişim sistemlerinde arama ve elkoyma konusunda özel bir düzenlemenin bulunmadığı, delil toplanmasında genel hükümler uygulandığı ancak sözleşmeye taraf olmakla birlikte uluslararası yükümlülükler gereği iç hukukta cebri önlemlere yer verilmesi gerektiği ifade edilmiştir.[505]

CMK m.134 hükmünün unsurlarını irdelemeye başlamadan önce, madde başlığı hakkında birtakım tartışmalara değinmekte fayda bulunmaktadır. Öğretide bir görüş, başlıkta yer verilen "*bilgisayarlarda, bilgisayar programlarında ve kütüklerinde*" ibaresinin, uzun bir terim olduğunu ve tedbirin konusunu ifade etmek için sözleşmede yer alan "bilgisayar sistemi" ifadesinin kullanılması gerektiğini ifade etmektedir.[506] Başkaca bir görüş, kullanılan terminolojinin hem bilişim kavramını tam olarak kapsamaması, hem de bilgi ve verinin işleme tabi tutulduğu aşamaların tek tek zikredilmesinin mümkün olmaması sebebiyle birlikte, internet ortamını da dikkate

[502] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s.545.
[503] https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=21470&MevzuatTur=7&MevzuatTertip=5 [19.08.2020].
[504] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s. 251.
[505] ERDOĞAN Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s. 250.
[506] ÖZEN/BAŞTÜRK, 2011. Temel hak ve özgürlükler bağlamında bilişim- internet ve ceza hukuku. Ankara: Adalet Yayınevi., s.142; BAŞTÜRK, s. 25.

alarak yeniden düzenlenmesi gerektiğini ifade etmektedir.[507] Diğer bir görüş ise, başlıkta belirtilen ilgili ifadelerin uzun olması ve amacı ifade etmekten uzak olması, tedbirin uygulama alanını sınırlandırması sebebiyle yine "bilişim sistemleri" kavramının kullanılmasının yerinde olacağını belirtmiştir.[508]

Bilişim sistemi kavramının bilgisayar programlarını, kütüklerini ve hatta diğer birtakım araçları da kapsamasından dolayı, çalışmamızda söz konusu maddenin başlığında belirtilen ibare yerine, "bilişim sistemi" tabiri kullanılacaktır. Ayrıca, maddede her ne kadar "girmek" kavramı kullanılmakta ise de, bu kavram fiziki ortamlara ilişkin kullanılmasından dolayı bilişim alanına istinaden "erişmek" kavramı kullanılması daha doğru olacaktır.[509]

6. Tedbirin Muhatabı

Çalışma konumuz olan tedbirin uygulanması esnasında kapsamının net olarak belirlenmesi gerekmektedir. Veri aranacak olan bilişim sistemi, şüpheliye veya üçüncü kişilere ait de olabileceği gibi, resmi bir kuruluşa ait de olabilir. Ancak CMK m. 134 hükmünde, bu konuda bir sınırlama mevcut değildir.[510] Adli aramada şüpheli, sanık, diğer kişiler bakımından ve avukatlar nezdinde arama gibi kategoriden bahsetmek mümkündür. Bu halde, arama işlemine tabi olacak kişiye göre bilgisayarda arama kararının yanında ek olarak, aramanın yapıldığı kişilere özgü özel hükümler ve ayrıca dikkate alınması gereken hususlar bulunabilir.[511]

a. Şüpheli ve sanık açısından

Madde metninde, "şüphelinin kullandığı, bilgisayar ve bilgisayar programları ile bilgisayar kütükleri" ifade edilmiştir. Bu bakımdan, tedbirin uygulanması için kullanılan bilişim sisteminin şüpheliye[512] ait olması gerekmemektedir.[513] Öyle ki şüphelinin; kiraladığı, ödünç aldığı ya da bir şekilde ortak kullanımında olabilecek bir bilişim

[507] TANRIKULU, s.357.
[508] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.310.
[509] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s. 241.
[510] CENTEL/ZAFER ceza muhakemesi hukuku, s.410.
[511] TANRIKULU, s.352.
[512] CMK m. 2/1-a'da şüpheli "*soruşturma evresinde, suç şüphesi altında bulunan kişi"* şeklinde tanımlanmaktadır.
[513] ORTA, s.218.

sisteminin suç fiilini gerçekleştirirken yararlanılması sonucunda, tedbir uygulama alanı doğacaktır.[514] Burada ayrıca üzerinde durulması gereken husus, tedbirin uygulanmasına yönelik yapılan talepte, ilgili talep ile şüphelinin kullandığı iddia edilen bilişim sistemi arasında bir ilişkinin kurulması ve bu bağın da sulh ceza hâkimi tarafından değerlendirilmesi sonucunda tedbirin uygulanmasına karar vermesi gerektiğidir.[515]

Bunlarla birlikte, tedbirin uygulanması esnasında önemli bir başka husus ise, söz konusu tedbirin kovuşturma aşamasında sanık[516] için uygulanıp uygulanamayacağı hakkında, öğretide fikir ayrılıklarının mevcut olduğudur. Bir görüş, tedbirin kanun metnindeki açık ifade itibariyle sadece soruşturma aşamasında uygulanması gerektiğini öne sürmektedir. Çünkü kamuya açık cereyan eden bir duruşmada, söz konusu tedbire karar verilmesi halinde, bu karardan haberdar olan ilgili kişilerin sistemde bulunan kayıtları ve hatta bilgisayarı yok edebilmesi mümkündür. Böyle bir durumda ise tedbire başvurulmasının bir anlamı kalmayacak ve istenilen verilere ulaşılamayacaktır.[517] Başka bir görüş ise, yargılama esnasında delil toplanmasını engelleyen bir hüküm bulunmaması ve mahkemenin resen araştırma yetkisine sahip olmasından dolayı, kovuşturma aşamasında söz konusu tedbire başvurulabileceğini ifade etmektedir.[518] Başkaca bir görüşe göre ise ceza muhakemesinin amacı olan maddi gerçeğe ulaşılması adına, tedbir kovuşturma evresinde de uygulanabilecektir.[519] Bir diğer görüşe göre, madde metninde "kovuşturma", "mahkeme" ve "sanık" kavramlarına yer verilmemesinden ötürü, tedbirin sadece soruşturma evresinde başvurulabilecek bir tedbir olduğu kanaati oluşmaktadır.[520] Diğer bir görüşe göre, CMK m. 134/1'in hatalı düzenlemesi sebebiyle, sanığın kullandığı veya sanığa ait bilişim sisteminde bu tedbirin uygulanma olanağı bulunmamaktadır. Söz konusu hükme, sanık hakkında yani

[514] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s.545.
[515] BAŞLAR, Ceza yargılamasında elektronik delil, s.168.
[516] CMK m.2/1-b'de "*kovuşturmanın başlamasından itibaren hükmün kesinleşmesine kadar, suç şüphesi altında bulunan kişiyi ifade etmektedir."* şeklinde tanımlanmaktadır.
[517] ORTA, s.218; ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.517.
[518] ŞAHİN C., PROF. Dr. Mehmet Emin Artuk'a armağan, s. 756.
[519] Kovuşturma aşamasında maddi gerçeğe ulaşması için söz konusu tedbire başvurulması imkân dâhilindedir. Ayrıca kamu davası bitinceye kadar her aşamada da mümkün olmalıdır. TANRIKULU, ss.353-354.
[520] Bu görüşe göre, "*kovuşturma evresinde de delil toplanabilmesinin mümkün bulunması karşısında, böyle bir sınırlamanın gerekçesi ortaya konulmuş değildir*." BIÇAK, V., 2018. Ceza muhakemesi hukuku. 4. Baskı. Ankara: Seçkin Yayıncılık, s.728.

kovuşturma evresinde başvurulması kanunilik ilkesine aykırılık teşkil edecektir. Bunun çözümü için kanuni düzenlemeye ihtiyaç vardır.[521]

b. Diğer kişiler açısından

CMK m. 134'ün üçüncü kişilere karşı uygulanabilme olasılığı ise yine tartışmalı bir husus olarak karşımıza çıkmaktadır. Söz konusu maddenin lafzından yola çıkarak bir değerlendirme yapıldığında, bilgisayarın şüpheli tarafından kullanılması tedbirin uygulama alanı bulması için yeterli olup, ayrıca bilgisayarın şüpheliye ait olması aranmamaktadır.[522] Öğretide bir görüş, şüpheli tarafından kullanılan ancak bir üçüncü kişiye ait olan bilgisayarlarda, tedbir kararı verilebileceğini ileri sürülmektedir.[523] Buna karşılık, bir görüş söz konusu tedbirin şüpheli haricindeki kişilere karşı uygulanamayacağına yöneliktir.[524] Aksi yöndeki bir görüşe göre ise bazı durumlarda üçüncü kişilerin bilişim sisteminde delil elde edebilmesi için söz konusu tedbirin uygulanması gerekmektedir. Kanun koyucunun bu hususu içeren bir düzenlemede bulunmaması ciddi bir eksikliktir.[525] Diğer bir görüşe göre, üçüncü kişilere ait bir bilgisayar üzerinde söz konusu tedbirin uygulanması, şüphelinin bu üçüncü kişiye ait bilgisayarı kullanıyor[526] veya kullanmış[527] olması koşuluna bağlı olmaktadır.[528] Başkaca bir görüşe göre ise bilişim suçlarında failin kullanmadığı bilişim sistemi veya araçlar üzerinde suça ilişkin delil barınması mümkündür. Bu bağlamda, sırf o bilişim sistemini kullanmaması sebebiyle aygıtta arama yapılmaması, maddi gerçeğe ulaşılamaması sonucunu doğuracaktır. Bunun çözümü için madde metninden şüphelinin kullanması

[521] ÜNVER/HAKERİ, s.423.
[522] ÇELİK, s.33; TANRIKULU, s.393.
[523] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.220; DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, ss.318-319; ÜNAL, O. G., 2011. Bilgisayarda, bilgisayar programlarında ve kütüklerinde arama kopyalama ve elkoyma. Yüksek Lisans Tezi. Ankara: Gazi Üniversitesi SBE, s.92.
[524] KARAGÜLMEZ, s. 504; ÖZEN/BAŞTÜRK, s. 151; BAŞTÜRK, s.28.
[525] DÜLGER, Bilişim suçları ve internet iletişim hukuku, ss.545-546.
[526] YENİSEY, Ceza muhakemesi hukuku başvuru kitabı, s.116
[527] ÜNVER/HAKERİ, s. 423.
[528] "… Olay tarihinde sanıkla maktulün internet üzerinde sohbet ettikleri söylenen kafede sanığın 'Kaan' kod adıyla 21. no.lu masada ve maktulün kullandığı belirtilen bilgisayarın ve kullandıkları programın saptanarak bilgisayarda ve bilgisayar programının merkezi sisteminde sohbet kaydının mevcut olup olmadığı ve içeriğinde hakaret ve tahrik edici sözler olup olmadığı tespit edilmeden yazılı şekilde hüküm kurulması usule aykırı bulunduğundan hükmün BOZULMASINA, oybirliği ile karar verildi..." Yargıtay 1. CD'nin 14/11/2005 tarihli ve 3891/3230 sayılı kararı. Kararı aktaran ÖLMEZ, s.50

koşulu kaldırılarak, söz konusu aygıtlarda somut delille dayalı kuvvetli suç şüphesi arama için yeterli görülmelidir.[529]

Bir başka görüş ise, "*diğer kişilere ait bilgisayarlar ve diğer araçlar üzerinde arama ve kopyalama yapılabilmesi, CMK. m.117'daki şartların gerçekleşmiş olmasına bağlıdır. CMK. m.134'de tedbirin uygulanacağı araçların üçüncü bir kişiye ait olması yönünden herhangi bir hüküm bulunmamaktadır. Bu nedenle, CMK. m.134'te düzenlenen koruma tedbirinde, tedbirin konusunu oluşturan araçların şüpheli veya sanıktan başka birine ait olması durumunda, CMK. m.117 hükmü kıyasen uygulanmalıdır."*[530] şeklinde, kıyas yapılması gerektiğini ifade etmiştir.

Sonuç olarak, başkasına ait olan fakat şüphelinin kullandığı bir bilişim sisteminde CMK m. 134 hükmü uygulanabilecektir. Bu durum maddi gerçeğin ortaya çıkarılmasına yönelik bir yaklaşım olacaktır. Ancak belirtilmelidir ki, üçüncü kişilerin bilişim sistemleri üzerinde fiili kullanım durumu söz konusu değilse, tedbirin şüpheliye ait olmayan bir bilgisayarda uygulanması mümkün değildir.[531]

c. Şikayetçi ve mağdur açısından

CMK m.134 hükmünde, şikâyetçi ve mağdur açısından tedbirin uygulama alanı bulacağına ilişkin her hangi bir ibareye yer verilmemiştir. Fakat bilişim suçlarının genel özellikleri dikkate alındığı kimi durumlarda, suçun işlenmesinde kullanılan bilişim sistemlerinden delil elde edilemezken, suça maruz kalan kişinin bilişim sisteminde, suça ilişkin bir takım verilere erişilmesi mümkündür. Bu bağlamda şüpheliye ulaşılması adına, mağdura ait bilişim sistemine de gerekli incelemenin yapılması için tedbire başvurulması gerekmektedir. [532]

DEĞİRMENCİ, özellikle bilişim sistemlerine karşı işlenen suçlarda mağdur ya da şikâyetçinin bilişim sisteminde de, elektronik delil arama zorunluluğu olduğu ve bu sistemin bir nevi olay yeri olduğunu ifade etmiştir. Bu hususun çözümüne ilişkin iki

[529] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s. 220.
[530] Bu görüşe göre, "*diğer kişinin bilgisayarında arama yapılabilmesi, suçun delillerinin şüpheli veya sanığın kullanımında bulunan ancak üçüncü bir kişiye ait bilgisayarda bulunduğunun kabul edilmesine olanak sağlayan olayların varlığına bağlıdır*" YAŞAR/DURSUN, s.21.
[531] ÜNAL, s. 93.
[532] BAŞLAR, Ceza yargılamasında elektronik delil, s. 169

ayrı yaklaşımda bulunmuştur. İlk olarak, CMK m. 160/2 gereği "…*Cumhuriyet savcısı, maddî gerçeğin araştırılması ve adil bir yargılamanın yapılabilmesi için, emrindeki adlî kolluk görevlileri marifetiyle, şüphelinin lehine ve aleyhine olan delilleri toplayarak muhafaza altına almakla"* yükümlü olup, ayrıca AÖAY'nin 9/2 göre "*kamuya açık olmayan suç işlenen alanlarda "sebep ve sonuç ilişkisini ortaya koyacak delillerin aranması, bulunması ve elkonulması için geliştirilmiş bilimsel ve teknik araştırma işlemleri*"ne yönelik incelemeler, bu maddeler uyarınca yapılabileceği ve elektronik delillere ulaşılabileceğini öne sürmektedir. İkinci olarak, iletişimin denetlenmesi yönetmeliğinin 10/4 fıkrasına benzer nitelikte bir düzenleme, AÖAY'nin 17'nci maddesine eklenmesi suretiyle, mağdur ya da şikayetçinin rızası halinde, mağdurun bilişim sisteminden de delil elde edilebileceğini öne sürmektedir.[533] Başka bir görüşe göre ise mağdur veya suçtan zarar görenin rızasıyla CMK' un genel hükümleri kapsamında, elektronik delillerin elde edilmesi için bu kişilere ait bilişim sisteminde arama ve muhafaza altına alınma işlemlerinin uygulanması mümkün kılınmalıdır.[534]

Gerek Yargıtay kararı[535] gerekse uygulama dikkate alındığında ise, mağdurun rızası halinde söz konusu tedbirin, mağdura ait bilişim sistemi üzerinde de uygulandığı görülmektedir. Ayrıca, mağdurun rızası ile bilgisayar sisteminde delil aranması halinde CMK m.134 hükmünde yer alan koşullar aranmayacaktır.[536] Çünkü bu durumda kişi, mağduriyetinin giderilmesi amacıyla rıza göstermektedir.[537] Ancak mağdura ait bilişim sistemi üzerinde rızası ile arama yapılıp yapılmayacağı hususunun kaleme alınmasında fayda bulunmaktadır.[538]

---

[533] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, ss.323-324
[534] TANRIKULU, s.415.
[535] *"...virüs içeren bir e-posta veya e-postaların... İnşaat Sanayi ve Ticaret Limited Şirketi'nin bilgisayarlarına virüs bulaştırması sonucu doğacak zararın, şirketin gönderdiği e-postalar aracılığıyla başka adreslere virüs göndererek başka bilgisayarlara zarar vermesi ve kendi bilgisayarlarının sistem dosyalarını silerek çalışamaz duruma getirip iş ve zaman kaybına neden olması olduğunu... öncelikle e-posta yolu ile virüs göndererek sistemine zarar verilmiş bir bilgisayarda incelemenin, olayın hemen akabinde yapılması...";* Yarg. 11. CD. 16.04.2007, 2005/6376E, 2007/2551K. Kararı aktaran ÜNAL, s.93
[536] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.324.
[537] ÇELİK, s.35.
[538] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s. 220.

d. Özel usule tabi kişiler açısından

d.1. Avukatlar

Avukat bürolarında arama ve elkoyma, özel olarak düzenlenmiştir. Avukat ile müvekkil arasındaki ilişkinin gizlilik içerisinde yürütülmesi ve savunma hakkı ile avukatın mesleki sırlarının korunması[539] düşüncesiyle farklı bir hükme yer verilmiştir.[540] CMK m.130 hükmüne göre, "*avukat büroları ancak mahkeme kararı ile ve kararda belirtilen olayla ilgili olarak Cumhuriyet savcısının denetiminde aranabilir*."[541]

Çalışma konumuz tedbir ile bu düzenleme değerlendirildiğinde üzerinde durulması gereken husus, avukatın bilişim sistemine ilişkin bir arama söz konusu olduğunda bu işlemin, CMK m.130 hükmüne göre mi, yoksa CMK m.134 hükmüne göre mi gerçekleştirileceğidir. Doktrinde bir görüş, her iki tedbirin de birlikte uygulanması gerektiği yönündedir.[542] Bu bağlamda, avukat bürolarında şüphelinin kullandığı bilişim sisteminin aranması, CMK m.130 kapsamında yapılacaktır. Ancak, bilişim aygıtının bulunmasından sonra arama, artık CMK m.134 hükümleri uyarınca gerçekleştirilecektir.[543] YAŞAR/DURSUN, avukatların ofisinde CMK m. 134'ün nasıl tatbik edilebileceğini şu şekilde açıklamıştır; "*avukat bürolarında yer alan bilgisayarlar ve diğer araçların aranması ancak mahkeme kararı ile ve kararda belirtilen olayla ilgili olarak Cumhuriyet savcısının denetiminde yapılabilir. Baro başkanı veya onu temsil eden bir avukat aramada hazır bulundurulur (CMK. m.130/1). Arama sonucunda CMK.'nun 134 üncü maddesine göre elkonulmasına karar verilen şeyler bakımından bilgisayarında arama yapılan avukat, baro başkanı veya onu temsil eden avukat, verilerin avukat ile müvekkili arasındaki meslekî ilişkiye ait olduğunu öne sürerek karşı koyduğunda, suçla bağlantılı olduğu hususunda makul bir şüphe varsa bu veriler CMK. m.134'e göre kopyalanabilir. Kopyalanan verilerin içinde bulunduğu CD, hard disk, flaş disk gibi veri kaydedicileri, ayrı bir zarf veya paket içerisine konularak hazır*

[539] ŞAHİN/GÖKTÜRK, s.153.
[540] TOROSLU/FEYZİOĞLU, s.253.
[541] KOCAOĞLU S. S., Üst ve Büro Araması, Postada Elkoyma, İletişimin Denetlenmesi Gibi Çeşitli Koruma Tedbirlerinin Pasif Öznesi Olarak Kuram ve Uygulamada Avukatın Bağımsızlığı, Ankara Barosu Dergisi, 2012/1, ss.45-69, s.57
[542] ŞAHİN C., PROF. Dr. Mehmet Emin Artuk'a armağan, s. 756; ÖZBEK/DOĞAN/BACAKSIZ, s.264; ÇELİK, s.36; TANRIKULU, s.416; BAŞLAR, Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri, s. 94; YAŞAR/DURSUN, s.24.
[543] YAŞAR, s.195.

bulunanlarca mühürlenir ve bu konuda gerekli kararı vermesi, soruşturma evresinde sulh ceza hâkiminden, kovuşturma evresinde hâkim veya mahkemeden istenir. Arama sırasında şartları oluştuğu takdirde CMK. m.134'e göre araçlar üzerinde elkoyma kararı da verilebilir. Yetkili hâkim, suçla bağlantısı olduğu hususunda makul şüphe bulunan ve bu suretle kopyalanan verilerin, avukatla müvekkili arasındaki meslekî ilişkiye ait olduğunu saptadığında, kopyalanan veriler derhâl avukata iade edilir ve yapılan işlemi belirten tutanaklar ortadan kaldırılır. Bu kararlar, yirmidört saat içinde verilir (CMK. m.130/2). Arama sonunda verilecek belgeye ilişkin olarak da, genel aramaya ilişkin 121 inci madde hükümleri uygulanmalıdır."[544]Başka bir görüşe göre ise, "*Avukat bürolarında arama, elkoyma ve postada elkoymayı düzenleyen CMK md. 130. Avukatların kullandığı bilişim araçları yönünden ayrı bir düzenleme öngörmediğinden, CMK md. 134 avukatlar yönünden de aynı şartlarda uygulama yeteneğine sahiptir*." [545]

d.2. Yargıçlar ve savcılar

Bilişim sisteminde arama kopyalama ve elkoyma tedbirine, başvurulabilmesi için bir suç soruşturmasının varlığı aranmaktadır. Hakimler ve savcılar hakkında muhakemeler izin şartına bağlanmıştır. Hakimler bakımından soruşturma usulü, Hâkim ve Savcılar Kanunu'nun 82. Maddesinde, savcılar içinse 82, 87, 89 maddesinde düzenlenmiştir. [546] Dolayısıyla, hakim ve savcılar açısından ilgili mevzuata göre haklarında başlatılmış bir soruşturma bulunması gerekmekte olup, bu halde CMK m. 134'te belirtilen tedbirlere yetkili makamca başvurulabilir. Ayrıca, ağır cezayı gerektiren haller haricinde 2802 sayılı Yasa'nın 88. maddesi gereği, suç işlediği ileri sürülen yargıç ve savcılar yakalanamaz, üzerleri ve konutları aranamaz, sorguya çekilemezler. Bu doğrultuda CMK m. 134, özel mahiyette bir arama tedbiri olduğu göz önüne alındığında, bilişim sistemlerinde aramaya ilişkin açık bir yasak mevzu bahis olmasa da, hâkim ve savcılar açısından belirtilen makamlarca verilmiş bir karar dışında, bilişim sistemlerinde arama, kopyalama ve elkoyma işlemleri gerçekleştirilemez.[547]

---

[544] YAŞAR, ss.195-196; YAŞAR/DURSUN ss.24-25.
[545] ÖZEN/BAŞTÜRK, s. 151; BAŞTÜRK, s.28.
[546] NUHOĞLU/YENİSEY, ss.580-581.
[547] 2949 sayılı Anayasa Mahkemesinin Kuruluşu ve Yargılama Usulleri Hakkında Kanun'un 55; 2575 sayılı Danıştay Kanunu'nun 76 ila 82; 2797 sayılı Yargıtay Kanunu'nun 46; 1602 sayılı Askeri Yüksek İdare Mahkemesi Kanunu' nun 32 ve 33; 1600 sayılı Askeri Yargıtay Kanunu' nun 37 ve 38.

e. Milletvekilleri açısından

Milletvekilleri, yasama dokunulmazlığına sahiptir. Yasama dokunulmazlığı, mutlak dokunulmazlık ve geçici dokunulmazlık olarak ikiye ayrılmaktadır. Milletvekillerine ilişkin geçici dokunulmazlık kapsamında yapılamayacak ceza muhakemesi işlemleri Anayasada sınırlı olarak sayılmış olup, bunlar haricindeki muhakeme işlemleri ve tedbirlere başvurulabilecektir. Bu bağlamda, bir suç dolayısıyla başlatılmış olan soruşturmanın varlığı halinde, milletvekilleri hakkında da CMK m.134 gereği arama kararı verilebilecektir. Bununla birlikte milletvekillerinin sıklıkla kullandıkları bilişim sistemlerinde arama hususuna ilişkin bir düzenleme yapılması gerekmektedir. Zira, bu durum milletvekillerinin görevlerini yerine getirmesinde aksaklıklara neden olabilir. [548]

f. Kamu görevlileri açısından

Çalışma konumuz olan tedbirin uygulama alanı bulabilmesi için, CMK m. 134'te bilişim sisteminin kamu tüzel kişiliğine ait olması ile, özel kişilere ait olması arasında bir ayrım öngörülmemiştir. Bu bakımdan şüpheli tarafından kullanılan ve kamu tüzel kişiliğine ait bir bilişim sisteminin üzerinde de söz konusu tedbir uygulanabilecektir.[549] Bununla birlikte, kamu görevlisinin çalıştığı kurum tarafından kendisine verilen bir bilişim sisteminde, amirin veya teftişle görevli olan kişinin onayıyla söz konusu tedbirin uygulanıp uygulanamayacağı hususunun üzerinde durulması gerekir. Öğretide bir görüşe göre, yöneticilerin, kamu görevlilerin sorumluluğunda bulunan ve kullanılmak üzere kendilerine tahsis edilen bilişim sistemleri üzerinde kişisel verilerin bulunabileceği ve mahremiyet hakkı mevcut olduğu, bir suç şüphesinden hareketle sadece amirin veya teftişle görevli olan kişinin onayıyla bireyin, bilişim sisteminde bir arama veya kopyalama işlemi yapılması mümkün değildir. Aksi takdirde, yöneticiler tarafından bu delil arama faaliyetinde elde edilen delillerin hukuka aykırı olacağı ifade edilmiştir.[550] Başka bir görüşe göre ise, bilgisayarların kişiye veriliş amacına bakılması gerektiği, "*bilgisayarlar özel işlerde değil, kurum işlerinde kullanılmak üzere*

---

maddelerinde yüksek yargı organları başkan ve üyeleri hakkında hangi esaslara göre soruşturma açılacağı belirtilmiştir. DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.327.

[548] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.328.

[549] "*Bu aramalar esnasında devlet sırrı niteliğinde belgelerle karşılaşılması durumunda, bu belgeler üzerindeki inceleme CMK m. 125/2 uyarınca yapılacaktır."* DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.398.

[550] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.340; BAŞLAR, Ceza yargılamasında elektronik delil, ss.169-170.

verilmektedir, idare de verdiği veya tahsis ettiği bu bilgisayarları, yetkili merciin emri ile her zaman geri alabilir; alırken de bu bilgisayarların içinde kişiye özel bir veri bulunamayacağından, aksi durum 657 sayılı DMK'ya göre, kurum araçlarının özel işlerde kullanılması disiplin suçunu oluşturacağından, cihazın içeriğinin incelenmesi için de anılan kimsenin rızasına muhtaç olunmadığı" bu sebeple kurum tarafından, çalışana verilmiş olan ya da kullanımına tahsis edilmiş bilgisayarların, yetkili amir ya da bu kişi adına hareket eden kimsenin emriyle incelenmesinin hukuka aykırılık oluşturmayacağı ifade edilmiştir.[551] Kanaatimizce, bir suç soruşturması kapsamında delil elde etme faaliyeti olarak, arama kopyalama ve elkoyma işlemleri, CMK m. 134 uyarınca sadece görevli kişilerce yerine getirilmelidir.

C. TEDBİRİN KONUSU

Bilişim sistemlerinde arama kopyalama ve elkoyma tedbirlerinin konusunun tespiti, hükmün uygulanma alanının belirlenmesi açısından önemlidir.[552] CMK m. 134 hükmü için kanun koyucu tarafından sınırlayıcı bir yaklaşım tarzı ile hareket edilerek, tedbirin konusu olarak, madde metninde bir takım araçlar sıralanmıştır. Bu noktada, AÖAY' nin 17. maddesine bakıldığında ise CMK m. 134'te belirtilen araçların yanında, bazı başka araçlara da yer verilmesiyle tedbir konusunun nispeten genişletilmiş olduğu görülmektedir. Ancak bu tutum günümüz teknolojisiyle tam olarak uyuşmamaktadır. Zira günümüzde bilişim sistemleriyle bağlantılı suçların işlenmesinde sayılan bu araçlar, sınırlı olarak kullanılmamaktadır.

Öğretide bir görüş, kanun koyucunun CMK 134. maddeyi kabul ederken, siber suç sözleşmesinde olduğu gibi dijital verileri ele geçirmeye yönelik bir düzenle ortaya koymadığını, bunun yerine dijital delil niteliğinde verilerin bulunduğu ortamlardan hareketle bir hüküm oluşturmuş olduğunu ifade etmektedir. Bu görüşe göre madde metninde sayılan terimlerin dar yorumlanması halinde uygulamada sorun çıkabileceği gibi, birçok bilişim sisteminin CMK m. 134 kapsamında olamayacağı için bu hüküm ile getirilen hukuksal ve anayasal koruma dışında kalacak ve mağduriyetlerine sebep

[551] ERDOĞAN Y., 2012. Bilişim sistemine girme ve kalma suçu. Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi. 12, Özel S., 2010. ss.1363-1433, s. 1410.
[552] YAŞAR/DURSUN, s.15.

olacaktır.[553] Öğretide bir başka görüş, yönetmeliğin 17/3 maddesiyle belirtilen araçlara yönelik kanunda belirtilmeyen bazı cihazların, yönetmelikte zikredilmesinin hükmün kapsamını genişletmediğini ve " *134. madde kapsamına hangi cihazların girdiği ve teknolojik gelişmelere bağlı olarak ilerde gireceği, normun amacına bakılarak"* belirleneceğini ifade etmiştir. Bu görüşe göre "*bunların her birinin tek tek Yönetmelikte zikredilmesi de gerekmez. Nitekim yeni teknoloji(akıllı) telefonlar da mevzuatta bir yerde zikredilmemiştir*".[554] Öğretide bir başka görüşe göre AKSSS'nde *"Sözleşme arama ve elkoyma yetkisinin internet vb. telekomünikasyon ağları ile yasal olarak erişilebilen diğer sistemler ya da bilgisayar sistemine doğrudan bağlı bulunan veya yakınında bulunan veri depolama aygıtları için de genişletilebileceğini öngörmekte ve uygulamayı ulusal mevzuatlara bırakmaktadır. CMK 134'de bu konuda bir düzenleme bulunmamakla beraber, arama Yönetmeliğinin 17 inci maddesinde bulunan hüküm yedekleme işleminin bilgisayar ağları ve diğer uzak bilgisayar kütükleri hakkında da uygulanabileceği şeklindeki ifade, bu kapsamda değerlendirilebilir. Ancak, bilişim sistemlerinin yapısı ve bilgisayar sistemlerinin birbirine bağlanabilme özellikleri göz önüne alındığında, bilgisayar verilerinin ağa bağlı başka bir sistemde saklanabilmesi de büyük bir olasılıktır. Kanunda tek cümle ile ifade edilen bu düzenleme yetersiz olup, arama ve elkoyma işleminin genişletilmesi hususunda sınırların mümkün olduğunca net çizilmesine imkan sağlayıcı düzenlemelerin yapılması gerekmektedir."* [555]

Tüm bunlarla birlikte çalışmamızda, CMK m. 134 ile ilgili yönetmelikte belirtilen araçların yanı sıra, işlevleri itibariyle tedbirin konusunu oluşturabilecek bazı araçlara da yer verilecektir.

1. CMK m.134'te Yer Alan Araçlar

a. Bilgisayar

Bilgisayar birinci bölümde de açıklandığı üzere, bilgileri işleme tabi tutabilen, depolayan ve görüntüleyen bir aygıttır.[556] Günümüzde masaüstü bilgisayarı, dizüstü

[553] TANRIKULU, ss.355-356.
[554] ŞAHİN C., PROF. Dr. Mehmet Emin Artuk'a armağan, ss.755-756.
[555] YENİSEY/NUHOĞLU, Ceza muhakemesi hukuku ders kitabı, s.418.
[556] APİŞ, s.55.

bilgisayarı, ekran bilgisayarı, sunucu bilgisayarı ve tablet bilgisayarları vb. farklı çeşitlerde tasarlanmış birçok bilgisayar bulunmaktadır.[557]

"*Bilgisayar, çevre birimleri (bir bilgisayarın çalışması için zorunlu olmayan ancak kullanımını kolaylaştıran hoparlör, CD ROM, mouse, klavye, kulaklık, yazıcı vb), iletişim altyapısı (elektronik haberleşme, internet, intranet gibi) ve programlardan oluşan veri işleme saklama ve iletmeye yönelik sistemi ifade eder.*"[558] *"AK-SSS'de "bilgisayar sistemi" kavramına bakıldığında bilgisayarın veri işleme gibi genel özelliklerinin yanında birbirine bağlanabilen veya birbirleriyle ilişki kurabilen özellikleri de dikkate alınmıştır"* Bu bağlamda bilgisayar olarak adlandırılmamakla birlikte sahip oldukları özellikler gereği, bilgisayar olarak adlandırılmayan fakat bilgisayar gibi işlev gören (programlanabilen, veri işleyebilen, iletebilen, saklayabilen) diğer elektronik cihazlar için de bu tedbir uygulanabilir.[559]

b. Bilgisayar programı

Bilgisayar programları "*bir komut üzerine bilgisayarın çalışmasını sağlayan ve içerisindeki verilere ulaşılmasını mümkün kılan yazılımlardır*."[560] Başka bir anlatımla, "*Bilgisayar programı, genel nitelikte işlem gören bilgisayarın, belirli bazı işlemlerin yerine getirilmesi amacıyla oluşturulmuş özel bir formatlama işlemidir."*[561] Fikir ve Sanat Eserleri Kanunu'nun 1-B maddesinin g bendinde ise "*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 eder." şeklinde belirtilmiştir. Bu ifadeden anlaşılacağı üzere, bilgisayar programına yönelik hazırlık çalışmaları da bilgisayar programı kavramına dahil olmaktadır.[562]

Bilgisayar programlarının temeli veriler olup, bu programlar belli bir işlevi yerine getirmek için oluşturulmuş komutlar dizisidir. Bilgisayar programları genellikle bilişim

[557] ÖZBEK, Adli Bilişimde Delillerin Toplanması ve incelenmesi, s.19.
[558] DÜLGER M.V./MODUOĞLU G., "Türk ceza adalet sisteminin etkinliğinin geliştirilmesi" Bilişim suçları eğitim modülü. https://rayp.adalet.gov.tr/resimler/552/dosya/2-bilisim-suclari-egitimi-modulu25-08-20204-32-pm.pdf [10.08.2020] s.55.
[559] ÜNAL, s.95.
[560] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.526.
[561] YAŞAR/DURSUN, s.17.
[562] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.51.

sistemine yüklü bir halde bulunurlar. Fakat bazen bilgisayar programları veri taşıma araçlarında da bulunabilmektedir. Bu halde, CMK m 134 hükmü ile söz konusu araçlar için de uygulama alanı doğacaktır.[563]

Bilgisayar yazılımlarının programlara nazaran daha üst bir kavram olduğunu daha önce belirtmiştik. Bilgisayar programları, ilgili ve gerekli veriler ile yazılımları meydana getirirler.[564] Bu bağlamda, kötücül yazılımların bir suçun işlenmesinde araç olarak kullanılması veya bilgisayarın işleyişini bozması halinde, bu kötücül yazılımlardan suçu aydınlatmak için yararlanılabilir. Dolayısıyla, bilgisayar yazılımları da CMK m. 134 açısından tedbirin konusunu oluşturabileceklerdir.[565]

c. Bilgisayar kütüğü

Bilgisayar kütüğü kavramı İngilizcedeki "log" kelimesinin karşılığı olarak kullanılmakta ve sistemdeki bütün verilerin depolandığı yer olmaktadır.[566] CMK' nın 134. maddesine bakıldığında veri tabanı kavramına karşılık olarak, bilgisayar kütüğü ibaresi kullanıldığı görülmektedir. "*Veri tabanı, belirli bir sistem ve metot izlenerek, çeşitli veri ve bilgilerin düzenli olarak bir arada bulundurulduğu ve depolanan veri ve bilgilere erişimde kolaylık sağlayan araçlar ve ortamlara verilen addır.*" Bu araçlar CD formatında taşınabilir olabileceği gibi, internet ile erişim sağlanabilen sanal bir alan da olabilir. Söz konusu sanal alan, bulut bilişim olarak adlandırılmaktadır.[567] Bu bağlamda bilgisayar kütükleri "*sabit veya taşınabilir ya da bulut formatında her türlü veriyi taşınmasını ve depolanmasını sağlayan araç veya sistemlerdir."*[568] Diğer bir deyişle, bu ibareden kastedilen verilerin saklandığı dizinlerdir. Bu sebeple, bilgisayarlarda bulunan ve verilerin saklanması amacıyla kullanılan depolama birimleri ve dizinleri kütük kapsamına girmektedir.[569]

Bununla birlikte Adlî ve Önleme Aramaları Yönetmeliğinin 17/3 maddesinde "*Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün*

[563] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.332.
[564] TANRIKULU, s.359.
[565] TANRIKULU, s. 332.
[566] ÖZEN/BAŞTÜRK, s.153.
[567] İngilizcesi "datebase" olan veri tabanı, veri ve bilgilerin saklandığı bilgi deposu veya bilgi bankasıdır. ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.58.
[568] DÜLGER, s. 549.
[569] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.332.

verilerin yedeklemesi yapılır. Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır." şeklindeki ifade ile bilgisayar kütüğü kavramının, verilerin saklandığı ortamları ve her türlü veri taşıyıcıları kapsadığı görülmektedir. Bu bağlamda CMK m. 134 hükmünün bilgisayarlar, iç ağlar ve uzak bilgisayar sunucuları ve veri taşıyıcıları bakımından da tatbik edilmesi gerekmektedir.[570]

2. AÖAY m. 17'de Yer Alan Araçlar

CMK m. 134 hükmünün tedbir konusu araçları sınırlandırması karşısında, AÖAY' nin 17. maddesinin tedbirin kapsamını bir nebze genişletmiş olduğu görülmektedir. CMK m. 134'te bilgisayar, bilgisayar programları ve kütükleri ibarelerini belirtilirken, AÖAY 17/3'te, bilgisayar ağları, diğer uzak bilgisayar kütükleri ve çıkarılabilir donanımlarına yer verilmiştir.[571]

Burada üzerinde durulması gereken bir husus, söz konusu yönetmeliğin 17. maddesinin 3. fıkrasında belirtilen araçların, sadece elkoyma tedbiri bakımından değerlendirilmiş olmasıdır. Şöyle ki, maddenin birinci fıkrasında düzenlenen arama ve kopyalama, tedbirleri bakımından yönetmeliğin 17/3'te belirtilen araçlara yer verilmemiştir. Bu konuda öğretide bir görüş, elkoyma tedbirine ancak arama işleminden sonra başvurulabileceğini ve arama işleminin gerçekleştirilmeden elkoymaya başvurulmasının, CMK. m.134/2'deki koşullara riayet edilmemesi anlamına geleceğini ifade etmiştir. Bu bakımdan, bilgisayar ağları, uzak bilgisayar kütükleri ve çıkarılabilir

---

[570] TANRIKULU, s.360.

[571] *Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma*
Madde 17 – "Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması hâlinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.
Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması hâlinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması hâlinde, elkonulan cihazlar gecikme olmaksızın iade edilir.
Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır.
Üçüncü fıkraya göre alınan yedekten elektronik ortamda bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.
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."

donanımlar hakkında hükme göre yalnızca elkoyma söz konusu olsa da, arama ve kopyalamanın elkoyma işleminden önce gerçekleştirilen işlemler olmasından ötürü üç tedbirde uygulanabilmeli ve arama ve kopyalama işlemi gerçekleştirilmelidir.[572]

Öğretide bir görüş AÖAY' nin 17/3 hükmünde geçen "*Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır*." ifadeyi uzaktan erişim yoluyla arama olarak nitelendirmekte ve bu aramanın hukuka aykırı olduğunu öne sürmektedir. Bu görüşe göre Türk hukukunda(CMK veya başka bir kanunda) uzaktan erişimle arama yapılmasına imkân veren bir düzenleme mevcut değildir. Dolayısıyla uzaktan erişimle arama mümkün değildir. Bununla birlikte ağ üzerinden bağlanılan ve başka bir fiziki mekânda bulunan sunucu veya bilgisayar unsurlarında arama yapılmasına, ilişkin kanunda yer verilmeyip, yönetmelikte(uzak bilgisayar kütükleri ve çıkarılabilir donanımlar bakımından) imkân sağlamasını, normlar hiyerarşisi dikkate alındığında, şüpheli aleyhine bilgisayar aramasını genişleten bu hükmün hukuka aykırı olduğunu ifade etmektedir.[573] Öğretide başka bir görüşe göre, teknik olarak bilişim sistemindeki verilere uzaktan erişim mümkündür. Ancak CMK. m.134'teki koruma tedbiri kapsamında bilgisayara uzaktan erişim yoluyla arama imkân dâhilinde değildir. Bu görüşe göre "*Uzaktan erişim yoluyla bilgisayardaki verilere ulaşılması, hukuka aykırıdır. Bilgisayarda arama, fiziki olarak bilgisayardaki verilerin aranması suretiyle gerçekleştirilebilir*."[574] Kanaatimizce yönetmelik ile yasa hükmü genişletilemez. Dolayısıyla CMK m. 134 çerçevesinde, bir bilişim sisteminde uzaktan erişim yöntemiyle arama yapılması mümkün değildir.

a. Bilgisayar ağları

Bilgisayar ağı kavramını birinci bölümde ayrıntılı bir şekilde açıklamıştık. "*En az iki bilgisayarın birbirlerine bağlanıp, bilgi alış-verişinde bulunmasına bilgisayar ağı (Network) denir*.[575]

---

[572] YAŞAR/DURSUN, ss.15-16.
[573] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s. 235.
[574] YAŞAR/DURSUN, s.24.
[575] Bilgisayar Ağı Nedir? https://www.dersimiz.com/bilgisayar/bilgisayar-agi-nedir-22710.html [22.12.2018]

Bilgisayar ağlarının tedbirin konusu olabileceği Adli ve Önleme Aramaları Yönetmeliğinin 17. maddesinde belirtilmiştir.

Bilgisayar ağı, bilgisayarların ve/veya iletişim cihazını iletişim hatları aracılığıyla birbirine bağlandığı ve bilgi ve sistem kaynaklarının farklı kullanıcılar tarafından paylaşıldığı, bir yerden başka bir yere veri aktarımı gibi hizmetler sunulabilen iletişim sistemidir.[576] Ağ sistemlerinden; uygulamaların, kullanıcı işlemlerinin ve bilgi sistem ağındaki veri akışının kayıtları tutulur. Bu kayıtların türüne bağlı olarak, kullanıcıların hangi sisteme ne zaman eriştikleri, sistemlerin doluluk oranları, performans değerleri, veri tabanlarında erişilen tablolar ve yapılan değişiklikler gibi bilgiler edinilebilir.[577] Ayrıca, bilgisayar ağları üzerinden sunuculardaki her türlü bilgi, sadece belirli bir incelemeye ilişkin bilgiler (tek kullanıcının web istekleri, elektronik postaları gibi), girişim tespit cihazlarında olduğu gibi yalnızca saldırı olarak kabul edilen alarm bilgileri ve tek başına anlam ifade etmeyen ancak diğer bilgilerle beraber değerlendirildiğinde önemli olan bir takım sonuçlara erişilebilir.[578]

b. Uzak bilgisayar kütükleri

Uzak bilgisayar kütükleri ile "*bir bilgisayar aracılığıyla ağ üzerinden ulaşılabilen gerek kullanıcıya ait ve gerekse kullanıcıya ait olmayıp ancak ortak paylaşıma ve kullanıma açık diğer bilgisayarlardaki veri depolama araçlarına ulaşabilmek mümkündür*."[579] Öğretide bir görüş, uzak bilgisayar kütükleri ibaresinden anlaşılması gerekenin, iç ağ ya da internet üzerinden bağlanılan başka bir fiziki mekânda bulunan sunucu, bilişim sistemi bileşeni ya da veri taşıcısı olduğunu ifade etmektedir.[580]

c. Çıkarılabilir donanımlar

Çıkarılabilir donanımları ilk bölümde açıklamıştık. Çıkarılabilir donanımlar bilgisayara monte edilmesi halinde, bilgisayara ek özellikler sağlayan ancak bilgisayarın olmazsa

[576] Bilgisayar ağı, https://tr.wikipedia.org/wiki/Bilgisayar_a%C4%9F%C4%B1#:~:text=Bilgisayar%20a%C4%9F%C4%B1%2C%20k%C3%BC%C3%A7%C3%BCk%20bir%20alan,veri%20aktar%C4%B1m%C4%B1n%C4%B1n%20m%C3%BCmk%C3%BCn%20oldu%C4%9Fu%20ileti%C5%9Fim [06.03.2021]
[577] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, s.98;
[578] GÖKSOY, s.100; ERCAN T. / NACAK D., Kablosuz Ağlardaki Paket Trafiğine Adli Bilişim Yaklaşımı, Journal of Yasar University, 4(13), ss.1909-1921, s.1912.
[579] YAŞAR/DURSUN, s.20.
[580] TANRIKULU, s.360.

olmaz derecesinde etkisi bulunmayan donanım birimleridir.[581] Adli Arama ve Önleme Yönetmeliğinin 17. maddesinde de "*Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır*" şeklindeki ifade ile olay yerinde bulunan bilgisayarların yanı sıra CD, DVD, disket, çıkarılabilir hafıza birimleri (usb memory, SD Card vb.) gibi veri depolama aygıtlarının da yedeklenebileceği anlaşılmaktadır.[582]

Bunlarla birlikte Yargıtay kararlarında, tedbirin konusu olan bilgisayar, bilgisayar programları ve bilgisayar kütükleri, arama işlemi için dar anlamda yorumlanmakta, bilgisayar kasası ve hard diskin aranması söz konusu olduğunda CMK m. 134, CD'ler bakımından ise 116. maddenin uygulanacağı belirtilmektedir. Ancak bu durum kabul edilemez. Zira klavye, fare, harddisk gibi yazıcı, CD'ler de bilgisayarın dış donanımı niteliğinde ve bilgisayarın bir parçasıdır. Ayrıca şüphelinin herhangi bir eşyası olmamakla birlikte, bu eşyalar klasik değil elektronik delil elde edilmesini sağlayan, özel niteliği olan materyallerdir. Bu bağlamda, CMK m. 134'te yer alan işlemlerin daha sıkı şartlara bağlanmasının nedeni "özel hayatın gizliliği" ilkesi gözetilerek, CD, Flashbellek, yazıcı gibi elektronik delil kaynakları için de aynı önem gösterilmeli ve bu gibi donanımlar için de CMK 134. madde hükümleri uygulanmalıdır.[583]

3. CMK m. 134'te ve AÖAY m. 17'de Yer Almayan Araçlar

Çalışmamızın bu kısmında, CMK' nda ve AÖYA' de yer verilmeyen ancak tedbirin konusu olabilecek, günlük hayatta pek çok kişinin kullandığı ve içerisinde birçok veri barındıran bazı araçlara değinilecektir.

---

[581] YAŞAR/DURSUN, s.20.

[582] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.236; TANRIKULU, s.360; AYDOĞAN, s. 23.

[583] Nitekim Yarg. 19. Ceza. Dairesi bir kararında "Müşteki vekilinin şikayeti üzerine başlatılan soruşturmada, Yalova 1. Sulh Ceza Mahkemesi'nin 08/05/2008 Tarihli, 2008/262 D. İş Sayılı Kararında, CMK'nın 119. maddesi uyarınca sanık tarafından işletilen işyerinde arama yapılmasına karar verilmesine karşın, aynı işyerinde bulunan bilgisayarlar üzerinde arama yapılabilmesine olanak tanıyan 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 hard diskler ve CD'ler hukuka aykırı delil niteliğinde olup hükme esas alınamayacağından, sanık hakkında verilen beraat kararı usul ve yasaya uygun görülmüştür." şeklinde belirtmiştir., Yarg. 19. C. D., 2015/2163 E., 2015/2163 E., 2015/1439 K., 13.05.2015., kararı aktaran, APİŞ, s. 77

a. Cep telefonları

Gelişen teknolojiyle birlikte artık bir bilgisayar ile yapılabilecek işlemler, akıllı telefonlar aracılığıyla da gerçekleştirilmektedir. Bu sebeple, madde metninde sadece bilgisayar ifade edilmekteyse de, günümüzde en az bilgisayarlar kadar kişisel verilerin yer aldığı, temel hak ve özgürlükler açısından bilgisayar kadar önemli olan akıllı cep telefonların da maddeye dâhil edilmelidir.[584] Bugün cep telefonları sadece iletişimin sağlanması amacıyla kullanılmamaktadır. Cep telefonları, mesajlar (SMS), telefon rehberi kayıtları, son aramaların listesi gibi emarelerin yanı sıra, kapasitesine bağlı olarak, fotoğraf dosyaları, videolar, kelime işlemci program ve belgeleri, web site erişim kayıtları ve benzeri dokümanlar barındırabilmekte ve bunlar delil niteliği taşıyabilmektedir.[585] Dolayısıyla, bu aygıtlar üzerinden sesli ve görsel kayıtlara, mobil bankacılığa, sosyal medyaya[586] ve anlık paylaşımlara[587] ilişkin verilere erişilebilmektedir.

Bununla beraber, hukukumuzda bilgisayar dışındaki eşyalar genel arama ve el koyma işlemlerine tabi olmaktadır. Yani CMK m. 116 göre bilgisayar dışındaki eşyalar makul şüphe bulunması halinde aranmakta, arama kararı ise CMK 119'a göre alınmaktadır. El koyma işlemi için ise, CMK m 127'ye göre karar verilmektedir. Cep telefonlarının bugün genel arama ve el koyma tedbirlerine tabi olması, gerektiğinde kolluk emri ile el konulması, özel hayata müdahaleyi basite indirgemektedir. Başka bir ifadeyle, cep telefonları için suç şüphesinin varlığı halinde, kolluk amirinin yazılı emriyle el konulabilmekte ve hiçbir yedekleme vs. yapılmamaktadır. Bu durum özel hayatın gizliliği ve kişisel verilere müdahale oluşturabilmektedir.[588]

Öğretide, cep telefonlarında arama ve elkoyma tedbirlerine ilişkin farklı değerlendirmeler mevcuttur. Bir görüş, CMK m.134'ün gerekçesini ileri sürerek, bilgisayar hakkında belirtildiği gibi durağan bir durumda delil teşkil edilmesi halinde, cep telefonunun CMK m.134 kapsamında değerlendirilmesi gerekmektedir. Diğer bir deyişle, iletişimin sağlanması amacı dışında, verilerin saklanması ve bilişim yeteneğine

[584] ÖZEN/ÖZOCAK, s.70.
[585] ÖZOCAK, Ceza Muhakemesinde Elektronik Delillerin Tespiti ve Toplanması, http://www.ozocak.com/Dosyalar/11504e.pdf [11.07.2020].
[586] ÇELİK, s.47.
[587] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s.545.
[588] ÖZEN/ÖZOCAK, s.69.

uygun bir şekilde kullanılması gibi nedenler söz konusuysa, CMK m 134'ün konusunu oluşturabileceğini ileri sürmektedir.[589] Buna karşılık öğretide bir görüş, cep telefonunu CMK m. 134'e dayanılarak incelenemeyeceğini ileri sürmektedir.[590] Başka bir görüş, ikili bir ayrımda bulunmuştur. Bu ayrıma göre; cep telefonunda gerçekleştirilecek arama ve elkoyma işlemi, cihazın telefon özelliğine ilişkinse; konuşma ya da mesaj kayıtları incelenecekse, bu durumda genel arama tedbiri olan CMK m. 119 uygulanmalıdır. Ancak uygulanacak arama ve elkoyma işlemi, cihazın bilgisayar özelliğine ilişkinse; arama motoru, trafik kaydı, e-posta kayıtları vb. incelenecekse, bu durumda ise aramanın özel bir görünümü olan CMK m. 134 uygulanması gerekmektedir.[591] Bir başka görüşe göre ise bugün kullanılan cep telefonları hem bilişim sistemi hem de iletişim aracıdır. Bu cihazlardan iletişim kurmaya yönelik Skype, Messenger WhatsAp gibi birçok yazılım geliştirilmiştir. Bu bağlamda, bu cihazlar veya yazılımlar üzerinde arama ve elkoyma tedbirlerinin hukuka uygun bir şekilde gerçekleştirilmesi için, CMK'nın hem 135. hem de 134. maddesi doğrultusunda karar alınması gerekmektedir. Ancak 135. maddenin uygulanması için belirtilen suçlarda bilişim suçları bulunmamaktadır.[592] Kanaatimizce günümüz akıllı cep telefonlarının, bilişim sistemi özelliğine sahip olması ve bir bilgisayar kadar içerisinde kişilere ait bilgiler barındırabilmesi sebebiyle, CMK m.134 kapsamında değerlendirilmelidir. Nitekim bu hususu Yargıtay bir kararında, " *şüphe üzerinde durdurulan sanığın cep telefonunun Cumhuriyet savcısının emri ya da mahkeme kararı olmadan kolluk görevlileri tarafından incelendiği ve telefonda, müştekiye ait çalıntı motosikletin fotoğrafının telefonda K ismiyle kayıtlı bir kişiye gönderildiğinin tespiti üzerine sanık hakkında mahkûmiyet kararı verilmiş ise de; işlevi itibarıyla bilgisayar niteliğinde olan cep telefonu üzerinde inceleme yapılabilmesi için CMK 'nın 134. maddesi uyarınca hâkim kararı alınması gerektiği bu kararın alınmaması sebebiyle arama ve incelemenin*

[589] ÜNAL, s.97.
[590] CMK m.134 hükmünde bilgisayar aramasının düzenlendiği, cep telefonunun bilgisayar olmadığı ve bu sebeple tedbir kapsamında olmadığı ifade edilmiştir. Eğer cep telefonundan internete girilmesi suretiyle bir suçun işlenmesi söz konusuysa, CMK m. 134'e ek bir hüküm getirilmesi veya madde başlığının "*verileri otomatik işleme tabi tutan sistemler aracılığıyla işlenen bir suç dolayısıyla yapılacak soruşturmalarda*" şeklinde değiştirilmesi gerektiği belirtilmiştir. TAŞKIN, Bilişim suçları, ss.173-174.
[591] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.219; ÖZEN/ÖZOCAK, ss.69-70
[592] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s.557.

yasaya aykırı olduğu ve bu delilin mahkûmiyete esas alınamayacağı "nı ifade etmiştir.[593]

b. E-postalar

Elektronik posta(e-posta), kullanıcıların belirlenen bir protokol vasıtasıyla internet üzerinden yazışmalarını sağlayan bir iletişim yöntemidir.[594] Bu haberleşme yönteminde,[595] elektronik postalara ait sistemdeki gönderildi ve alındı bilgileri iletişimi göstermesi sebebiyle önem arz etmektedir. Ayrıca bu postaların, içeriği ve postaya eklenen dosyalar ile postaların sunucudan geçerek oluşturdukları kayıtlar, elektronik delil olarak kullanılabilmektedir.[596] Bu e-postaların, CMK m.134'e konu olup olamayacağı tartışmalı bir husustur.

Öğretide bir görüşe göre, postaların akış halindeki veri mi yoksa durağan veri mi olduklarına bakılmalıdır. E-postada bir iletişim hali söz konusu olması durumunda CMK m.135'in uygulanması gerekir. Çünkü bu durumda bir iletişim hali ve akış durumu mevcuttur. Bunların yanı sıra, bir e-postada bulunan verinin bilgisayarda yer alması durumunda(okunmamış olsa dahi) ise, yani kaydedilmesi halinde, CMK m.134'ün kapsamına girecektir.[597] Benzer nitelikte başka görüşe göre ise, "*Bireyin e-posta yazışma ve haberleşmeleri CMK m.135 kapsamında değerlendirilirken, kendisine e-posta ile gelen bir yazı, resim, görüntü veya ek dosyayı kullandığı bilgisayara veya taşınır belleğe kaydettiğinde, artık bu belge haberleşme hürriyetinin ve dolayısıyla iletişimin denetlenmesinden çıkıp, CMK m.134 kapsamında bilişim cihazında kayıtlı bilgi ve belgeye dönüşecektir*."[598] Buna karşılık bir görüş, e- postanın, iletişim nitelikleri

---

[593] Yargıtay 17. CD, 15.2.2017, 2015/27517-2017/1716. kararı aktaran ŞAHİN, s.754.
[594] ÇAKIR/KILIÇ, . Adli bilişim ve elektronik deliller, s.281.
[595] ŞEN E., 2014. E-Posta Takibi, Terazi hukuk dergisi, (9)97 ss.88-90, s.88.
[596] GÖKSOY, s. 103.
[597] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, ss.332-333.
[598] Bu görüşe göre ayırt edici husus, bilginin bireyin kullandığı bilgisayarda mı kayıtlı olduğu, yoksa bu cihazdan bağımsız olarak haberleşme aracı olan e-postasında mı bulunduğudur. İleti, bireyin kendisine ait ve ancak özel şifre ile açılıp kullanılabilen e-postasında durmakta ise, haberleşme hürriyeti kapsamında olacak ve CMK m.135-138 hükümlerine tabi olacaktır. "*Ne zaman bu ileti birey tarafından bilişim cihazına kayda alınır, yani elektronik posta kutusundan çıkarılır, aynı mektubun postadan veya posta kutusundan alınıp çekmeceye veya dolaba koyulmasında olduğu gibi, işte o andan itibaren CMK m.134 devreye girer. Artık bu ileti haberleşme konusu olmaktan çıkıp, bireyin arşivlemek veya kullanmak için bilişim cihazına aldığı bilgi, belge veya dosya özelliğini kazanır."* ŞEN, E., E-Posta Takibi ve CMK

üzerinden bir değerlendirme yapılması gerektiği ve bunlar üzerinden delil elde edilmesi mevzu bahis olduğunda, CMK m. 135 hükmünün uygulanma alanı bulacağını ifade etmiştir.[599] Bir başka görüşe göre, "Göndericinin bilgisayarında kayıtlı bulunan giden e-mailler, elkoyma yoluyla elde edilebilir. Burada iletişimin denetlenmesi söz konusu olmaz. Buna karşılık, e-mail internet üzerinde iken elde edilirse, iletişimin denetlenmesi söz konusudur. Alıcının bilgisayarında kayıtlı bulunan e-maillerin, bilgisayarda yapılan inceleme sırasında ortaya çıkarılmasında da elkoyma işlemi söz konusu olur."[600] Başkaca bir görüşe göre, henüz açılmamış ve bilgisayar hafızasında yer alan elektronik posta ve çevrimiçi sohbet programlarındaki görüşmeler haberleşme özgürlüğü olarak değerlendirilmeli, CMK m. 135 hükmü kapsamında ele alınmalı, fakat kişi bu bilgileri bilgisayara kaydediyor ya da kendiliğinden kaydediliyorsa, bilgisayarda kayıtlı veri olarak kabul edilmelidir. Bu görüşe göre, WhatsApp benzeri anlık mesajlaşma uygulamaları üzerinden gönderilen ileti ve SMS ler elektronik posta gibi ele alınarak; veriler eğer iletişim esnasında ise, CMK m. 135 cep telefonu ya da bilişim sistemleri üzerinde bulunan kayıtlı mesaj içerikleri bakımından, CMK m. 134 hükmü uygulama alanı bulacaktır.[601] Doktrindeki ağırlıklı olan ikili ayrım dikkate alındığında, kanaatimizce e-postanın akış halinde olması durumunda, CMK m. 135'in, durağan bir halde olması durumunda ise CMK m. 134'ün uygulanması gerekir.

E-postalara ilişkin olarak AK-SSS'ne bakılacak olursa, memorandumun 190. maddesinde sözleşme, e-postada hangi koruma tedbirinin uygulanacağı konusunda bir belirleme yapmamış, bu belirlemeyi taraf ülkelerin takdirine bırakmıştır.[602] Yargıtay Ceza Genel Kurulu e-postalara ilişkin bir kararında e-postanın bilgisayarda kayıtlı olması durumunda, CMK m. 134, internet üzerinde iken ise CMK 135'nci maddenin uygulanması gerektiğini ifade etmiştir.[603]

---

m.134'ün Kapsamı, https://www.hukukihaber.net/e-posta-takibi-ve-cmk-m134un-kapsami-makale,3524.html [2.08.2020].

[599] ÜNAL, s.99.

[600] YENİSEY/NUHOĞLU, ss.414-415.

[601] WhatsApp ve benzeri internet üzerinden canlı telefon görüşmeleri şeklinde bir iletişim söz konusu ise, CMK m. 135 uygulama alanı bulacaktır. Ayrıca, faks ve telgraftan erişilen verilere ilişkin olarak; verilerin iletim sürecinde elde edilmesi durumunda CMK m. 135, faks ve telgraftaki bilgiler elektronik olarak kaydedilmiyorsa, CMK m. 122 ve 126 hükümleri uyarınca elde edilebileceğini, elektronik olarak kayıt edilebiliyor ise de, CMK m. 134 uygulama alanı doğabileceğini belirtmektedir. GÖKSOY, ss.174-176.

[602] ÜNAL, s.98; KESKİN, s. 170.

[603] Yargıtay Ceza Genel Kurul 26.09.2017 tarih, 2017/956 E.,2017/370 K. Sayılı karar, kararı aktaran GÖKSOY, s.174.

D. TEDBİRE BAŞVURU KOŞULLARI

Bir bilişim sisteminin diğer fiziki nesnelere benzetilerek, aynı arama elkoyma hükümlerine tabi olması, bazı hak kayıplarının oluşmasına sebep olabilmektedir. Zira tedbir sonuçları itibariyle özel hayatın korunmasından ticari, mesleki ve bilimsel sırlara varıncaya kadar,[604] değişik temel hak ve hürriyetlerle yakından ilişkili olup, pek çok kişisel bilgilere ulaşılması tedbirin tatbik edilmesiyle mümkündür. Bu itibarla tedbire başvurulması, bir takım şartlara bağlanmıştır.[605]

CMK m. 134 hükmünde üç ayrı tedbir düzenlenmiştir. Bunlar; arama, kopyalama ve elkoyma tedbirleridir. Burada, özellikle kopyalama tedbiri bilişim delillerine özgüdür. Çünkü, arama ve elkoyma tedbirleri CMK da ayrıca düzenlenmiştir.[606] Doktrinde bir görüş, bilişim sisteminde arama tedbirinin usul ve esaslarının maddenin 1'nci fıkrasında, kopyalama işlemine ilişkin hususların 1 ve 5'nci fıkralarında düzenlendiğini ve bu araçlara elkoyma tedbirine ise 2, 3 ve 4'ncü fıkralarda, arama ve kopyalamadan bağımsız olarak yer verildiğini ifade etmiştir.[607] Başka bir görüş ise, arama tedbirinin unsurlarını göz önüne alarak, CMK m. 134 hükmünün 5'nci fıkrasında düzenlenen aramayı "basit arama" olarak, aynı maddenin 1'nci fıkrasındaki aramayı ise "bilgisayarda arama" şeklinde isimlendirmiştir. Bu görüşe göre, eğer önceden bilinen belirli bir unsurun aranması söz konusuysa, örneğin adı belli bir dosyanın aranması gibi hallerde, basit arama[608] hükmü uygulanacaktır. Ancak önceden bilinen veya doğrudan bulunması amaçlanan bir verinin söz konusu olmadığı soruşturma konusu, genel olarak suça ilişkin bilgisayar içerisinde delil aranması durumunda, bilgisayar araması uygulanacaktır.[609]

---

[604] ÖLMEZ, s.52.
[605] ORTA, ss.216-217.
[606] Düzenleme, kişisel bilgi ve verileri korumak amacını taşımaktadır. YENİSEY, Ceza muhakemesi hukuku başvuru kitabı, ss.25-26.
[607] YAŞAR/DURSUN, s.6.
[608] Bu görüşe göre delil olduğu düşünülen ve önceden belirlenen verinin, aslında soruşturma makamlarını yanlış yönlendirmek için hazırlanmış bir dosya olması mümkün olabileceği gibi, aranılan dosyanın adının değiştirilmiş olması veya sistem içerisinde başkaca delillerin bulunması da söz konusu olabilir. Dolayısıyla basit arama hükmünün delil güvenliğini ve güvenirliğini sağlamaması, ayrıca uygulanma güçlüğü sebebiyle kaldırılması gerekmektedir. Zira bu arama, 1. fıkra hükmü kapsamında daha güvenli bir şekilde gerçekleştirilebilir. ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, ss.233-234.
[609] ERDOĞAN Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s. 209

Çalışmamız olan bu tez kapsamında, bilişim sisteminde arama, kopyalama ve elkoyma tedbiri için öngörülen şartları iki başlık altında irdeleyeceğiz. Buna göre, birinci kısımda bilişim sisteminde arama ve kopyalama, ikinci kısımda ise elkoymaya ilişkin şartlar incelenecektir.

1. Arama ve Kopyalama Tedbiri Bakımından

a. Bir suç dolayısıyla başlatılmış bir soruşturmanın bulunması

CMK m. 134 hükmü, niteliği gereği akılda ilk olarak yalnızca bilişim suçları için uygulanabileceği kanısı uyandırsa da, diğer suçlar bakımından da başvurulabilecek bir tedbirdir.[610] Kanun koyucu tarafından bilgisayarda, bilgisayar programlarında ve bilgisayar kütüklerinde arama kopyalama ve elkoyma tedbiri, bazı suç tipleri bakımından uygulanması şeklinde bir sınırlandırmaya tabi tutulmamıştır.[611] Madde metninde açıkça "*Bir suç dolayısıyla yapılan soruşturma ...*" ifadesinin yer alması, tedbirin yalnızca bir suç olgusunu ortaya çıkarmak amacıyla[612]ve tüm suç tiplerine istinaden yürütülen soruşturmalarda başvurularak elektronik delil elde edilmesini amaçladığını açıkça ortaya koymaktadır.[613] Sözleşmede de bilgisayar araması için önceden işlenmiş bir suçun varlığı aranmaktadır. Bu bağlamda, CMK m. 134'ün birinci fıkrasının sözleşmeye uyumlu olduğu söylenebilir.[614]

CMK tasarısında, CMK m. 134'ün birinci fıkrasında "*iki yıl veya daha fazla hürriyeti bağlayıcı cezayı gerektiren cürümler*" ifadesi bulunmaktaydı. Ancak Adalet komisyonunca bu ibare metinden çıkarılmıştır.[615] Dolayısıyla, bu şekliyle tedbir tüm suçlar bakımından uygulanabilmektedir. Öğretide, bu durumun temel hak ve özgürlüklere müdahale gerçekleştirdiği düşüncesiyle, koruma tedbirlerinin ortak özelliği

[610] BAŞLAR, Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri, s. 87.
[611] ÖZBEK/DOĞAN/BACAKSIZ, s.261.
[612] AKTAŞ B., 2017. Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma Tedbiri Üzerinde Bir İnceleme. Yeditepe Üniversitesi Hukuk Fakültesi Dergisi. 14 (2), ss. 211-239, s. 221
[613] BAŞLAR, Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri, ss.87-88.
[614] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.211.
[615] ŞAHİN, s.372; ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s. 209.

olan orantılılık ilkesine aykırılık oluşturduğu ileri sürülmektedir.[616] Özellikle de ciddi bir ceza öngörülmeyen suçlarda, basit suçlarda ve şikâyete tabi suçlarda bu tedbire başvurulmasının ceza muhakemesi hukuku mantığına ters düştüğü ifade edilmektedir. Bu görüşe göre tedbirin uygulanması için katalog suçlara yer verilmesi gerekmektedir.[617] Buna karşılık olarak diğer bir görüşe göre ise söz konusu tedbire sadece belli ağırlıkta ki suçlar bakımından uygulanması[618] veya katalog suçlara yer verilmesi halinde tedbiri uygulanamaz bir hale getireceği ileri sürülmektedir.[619] Bunların yanı sıra, tedbir ceza muhakemesi hukukuna göre yürütülen soruşturmalara ilişkin suçlarda uygulama alanı bulacaktır. Bu bağlamda diğer hukuk alanlarına ilişkin soruşturmalarda, suç soruşturması kapsamında olmayan idari soruşturmalar,[620] disiplin yaptırımı ve kabahat eylemi gibi hallerde bu tedbire başvurulamayacaktır.[621]

b. Somut delillere dayanan kuvvetli suç şüphesi

Tedbire başvurulabilmesi için öngörülen diğer bir şart "somut delillere dayanan kuvvetli şüphe" sebeplerinin varlığıdır. Bu şart, düzenlemenin ilk halinde bulunmamaktaydı. Bu husus, 21.02.2014 tarih ve 6526 sayılı "Terörle Mücadele Kanunu ve Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun"un 11. maddesiyle söz konusu tedbire eklenmiştir.[622]

Şüphe, bir şeyin olup olmadığı hakkında kararsızlık, kuşku anlamına gelmektedir.[623] Delil elde etmek adına koruma tedbirlerine başvurulması için değişen derecelerde bir şüphenin bulunması gerekmektedir. 6526 sayılı kanun öncesine kadar çoğu koruma tedbirinde başvurma şartı olarak belirtilen "suç şüphesi derecesi"ne, CMK m.134 hükmünde yer verilmemiştir. Öğretide, bu hususta şüphe çeşitlerine göre değerlendirmede bulunulmuştur.[624]

---

[616] ÖZEN/BAŞTÜRK, s. 148; BAŞTÜRK, s.27.
[617] Her suç için bu tedbire başvurulması halinde temel hak ve özgürlüklere ciddi bir müdahale oluşturacaktır. YAŞAR/DURSUN, ss.10-11.
[618] CENTEL/ZAFER, Ceza muhakemesi hukuku el kitabı, s. 375; BAŞLAR, Ceza yargılamasında elektronik delil, s. 162.
[619] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.338.
[620] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s. 211; AKTAŞ, s. 221.
[621] TANRIKULU, s.389; ÖZEN/BAŞTÜRK, s.144.
[622] ÇELİK, s.60; GÖKSOY, s.160; DÜLGER, Bilişim suçları ve internet iletişim hukuku, s.546.
[623] GÖKSOY, s. 159.
[624] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, ss.348-350.

Bir görüş, basit şüphenin[625] varlığı halinde, tedbirin uygulama alanı bulabileceği yönündedir.[626] Diğer bir görüşe göre ise kanun koyucu, CMK m. 116'da makul şüphe aradığını ve CMK m. 134 hükmünün bireyin haklarına daha ağır müdahale oluşturmasından ötürü, genel arama ve elkoyma tedbirlerinden daha düşük bir şüphe derecesinin öngörülemeyeceğini belirterek, arama ve elkoyma tedbirlerinde aranan makul şüphe[627] şartının aranması gerektiğini öne sürmektedir.[628] Başka bir görüş ise, CMK m.135'te yer alan tedbir açısından "kuvvetli şüphe sebepleri"[629] şartının varlığının arandığı ve çalışma konumuz olan tedbir bakımından CMK 135/1'in kıyasen uygulanabileceğini ifade etmektedir.[630] Başka bir görüş, kıyas yapılmasa da iletişimin denetlenmesi tedbirlerinde müdahale edilen temel hak ve özgürlüklerle, söz konusu tedbire yönelik koruma tedbirlerinin uygulanmasıyla ihlale uğraması muhtemel olan temel hak ve özgürlüklerin benzer olması sebebiyle, kuvvetli şüphenin doğrudan aranması gerektiğini ifade etmiştir.[631] Kanaatimizce, söz konusu tedbire başvurulmasında şüphe derecesinin varlığının şart olarak aranmaması, ölçülülük ilkesiyle bağdaşmamaktaydı.[632] Bu haliyle, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığının aranması, CMK m. 134'te yer alan tedbirlere başvurulmasını güçleştirmiş olsa da, tedbire maruz kalacak kişinin temel hak ve özgürlüklerinin korunması bakımından yerinde olmuştur.[633]

Kuvvetli şüphe, "*şüphelinin /sanığın suçu işlediği konusunda, somut olaylarla desteklenmiş, dayanağı olan delille mahkumiyet kararı verilmesinin kuvvetle muhtemel olduğu şüphedir"*.[634] Dolayısıyla, somut olayda makul şüphenin ötesinde bir suçun

---

[625] "*Bir suçun işlendiği izlenimi veren haldir. Şüphenin en hafif derecesidir ve başlangıç şüphesi olarak da adlandırılır*." ÖZBEK/DOĞAN/BACAKSIZ, s. 174.
[626] ÖLMEZ, s. 48.
[627] AÖAY madde 6'da, "*Makul şüphe, hayatın akışına göre somut olaylar karşısında genellikle duyulan şüphedir."* şeklinde tanımlanmıştır.
[628] "*Makul şüphe, hayatın akışına göre somut olaylar karşısında genellikle duyulan şüphedir. Makul şüphede, ihbar veya şikâyeti destekleyen emarelerin var olması gerekir*." Bu görüşe göre, şüpheli veya sanığın kullandığı bilişim sistemimde suça ilişkin olarak delil niteliği taşıyacak verilerin bulunduğu hususunda bir kanaat oluşmuşsa, makul şüphenin varlığından söz edilebilir. YAŞAR/DURSUN, s.11.
[629] Kuvvetli şüphe sebeplerinden, "*Basit bir başlangıç şüphesinden daha yoğun ama yeterli ya da kuvvetli şüphe derecesine ulaşması zorunluluğu bulunmayan şüphe derecesi olarak anlaşılmalıdır."* ÖZBEK/DOĞAN/BACAKSIZ, s.174.
[630] BAŞTÜRK, s.26.
[631] ÜNAL, s.102.
[632] BAŞLAR, Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri, s. 87.
[633] ÇELİK, s.62; ÖZEN/ÖZOCAK, s.62.
[634] DÜLGER, s.547

işlendiği yönünde çok güçlü bulguların olması gerekir.[635] Kanun koyucu, bilgisayarlarda arama tedbirinin söz konusu olması halinde, en yüksek şüphe derecesinin varlığını[636] araması, bu tedbire başvurulmasını zorlaştırmak istediği söylenebileceği gibi, özel hayat kavramını korumak istediği sonucuna da varılabilir.[637] "*Somut delillere dayanan kuvvetli şüphe*" ibaresi, takdir yetkisinin kullanımı ve tedbirin uygulanmasında, keyfiyetin önlenmesi bağlamında "*somut bir ölçü norm*" meydana getirmiştir.[638] Bu hususta, somut delil ibaresinden ne anlaşılması gerektiği önem arz etmektedir. Somut delil ibaresiyle soyut delil, somut delil ayrımı gibi bir ayrımın kast edilip edilmediği sorusu akla gelebilir. Bu hususta öğretideki bir görüşe göre, CMK'da ya da öğretide bu yönde bir ayrım mevcut değildir. Bununla beraber, söz konusu ibare ulaşılabilir ve rasyonalitesi bulunan delillere ilişkin olarak kullanılmaktadır.[639]

Somut delil, soruşturma konusu suça ilişkin mi, ya da şüphelinin kullandığı bilişim sisteminde delil bulunabileceğine yönelik olması mı gerektiği sorusu da gündeme gelebilir. Kuvvetli şüphe hususu iki alanda gerekmektedir. Kuvvetli şüphenin, hem şüphelinin soruşturma konusu suçu işlediği yönünde, hem de üzerinde arama yapılacak bilgisayarda, suç delillerinin bulunabileceği yönünde olması gerekmektedir.[640] Öğretide bir görüşe göre, düzenlemede tedbire başvurulabilmesi için, bilgisayarı aranacak olan kişinin soruşturulan suçu işlediğine, ya da aranan bilgileri kendi bilgisayarında barındırdığına dair somut veri(delil) bulunması koşuluna yer verilmemesi eksikliktir.[641]

"Kuvvetli şüphe sebeplerinin varlığı" ifadesine ilişkin, "kuvvetli şüphe" ile "kuvvetli şüphe sebepleri" arasında bir farklılığının bulunup bulunmadığı noktasında DEĞİRMENCİ, "*her iki terim arasında anlam bakımından bir farklılık var olmasına rağmen terim ile ifade edilmek istenenler açısından bir farklılık bulunmamaktadır*.

---

[635] APİŞ, s.72; TANRIKULU, s.394.
[636] GÜNEYSU, s.115.
[637] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s. 547.
[638] ARSLAN, s. 259.
[639] GÖKSOY, s.160; DÜLGER, Bilişim suçları ve internet iletişim hukuku, s.546.
[640] ŞAHİN C., PROF. Dr. Mehmet Emin Artuk'a armağan, s. 752; APİŞ, s.72; ÖZEN/ÖZOCAK, s. 62; DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, ss.352-353.
[641] *Bu görüşe göre "fail olduğu tahmin edilen kişideki tahmini kriminojen özelliklerin, şüphelide veya belli kişilerde bulunup bulunmadığının tespiti ve şüpheli olanlarla olmayanların ayıklanması amacıyla şüphelinin veya üçüncü kişilerin bilgisayarındaki verilere elkonulabilmesi, ancak bazı suçların işlendiği konusunda esaslı dayanak noktaları varsa mümkün olmalıdır."* CENTEL, N./ZAFER, H., 2020. Ceza muhakemesi hukuku el kitabı. 6.Baskı. İstanbul: Beta, ss.374-375.

Başka bir anlatımla, CMK m.134 bakımından "kuvvetli şüphe" aranmaktadır." şeklinde açıklamada bulunmuştur.[642]

Bunların yanı sıra, orantılılık ve ölçülülük ilkeleri gereği, çalışma konumuz tedbir bağlamında, suç şüphesini ortaya koyan sebepler ile somut olgular gerekçede gösterilmelidir.[643]

c. Son çare prensibi

CMK m. 134 hükmü, en son çare olarak uygulanmalıdır. Son çare olmasından maksat, bu tedbirin uygulanabilmesi için başka suretle delil elde etme imkânının bulunmamasıdır. Söz konusu tedbir, her koruma tedbirinde olduğu gibi, hükümden önce bir takım temel hak ve özgürlüklere müdahale teşkil etmektedir. Kişilerin kullandığı bilişim sistemlerinde arama, kopyalama ve el koyma işlemlerinin gerçekleştirilmesinin, özel hayat ile doğrudan bağlantısı bulunmaktadır. Çünkü kişiler hakkında sistemdeki önemli veriler, tedbirin uygulanmasıyla açığa çıkarılmış olur. Bu nedenle başka suretle delil elde edilememesi koşulu, temel hak ve özgürlükler bakımından önemli bir yere sahiptir. [644]

Son çare olması nedeniyle, bilgisayarda arama, kopyalama ve elkoyma tedbirine başvurulmadan önce eğer başka bir tedbirlerle sonuç elde edilebiliyor ise, daha öncelikli olan o tedbire başvurulması gerekmektedir. Doktrinde, "ikinci derecede uygulanabilirlik" şeklinde de ifade edilmekte olan bu şart, orantılılık ilkesinin somutlaşmış hali olup, aynı amaca hizmet eden iki koruma tedbirinin bulunması halinde, bunlardan kişi hak ve özgürlüklere daha az müdahale oluşturacak olanın tercih edilmesi anlamına gelmektedir.[645] Bununla birlikte, başka suretle delil elde etme imkânının bulunmaması, her ne kadar diğer tüm tedbirlere başvurulması ve bu tedbirlerden sonuç alınamaması anlamına gelmekte ise de, karşılaşılan somut olayda eğer diğer tedbirlere başvurulmasında herhangi bir yarar bulunmadığı kuvvetle

[642] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.149.
[643] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s. 214.
[644] BAŞLAR, Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri, s. 89.
[645] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.215.

muhtemel ise, bu şart gerçekleşmiş kabul edilmelidir.[646] Bu hususta tedbire karar verecek olan hakim, somut delillere dayanan kuvvetli şüphe nedenlerini değerlendirerek, başka suretle delil elde etme imkanının bulunmadığını belirten bir gerekçe ortaya koymalıdır.[647] Başka suretle delil toplanması için imkanın neden bulunmadığı, o ana kadar süre zarfında delil toplamak için neler yapıldığına dair hususlara savcının da talep yazısında yer verilmesi gerekir.[648] Bu bakımdan, soruşturma aşamasında iddianame hazırlanabilmesi ve yeterli delillerin toplanabilmesi için, kanunda düzenlenen diğer başvurulabilecek koruma tedbirlerine başvurulmuş ve yine de sonuç alınamamış veya diğer bir tedbir uygulandığında gerekli olan delillerin toplanamayacağına dair bir kanaat oluşmuşsa, ya da kovuşturma aşamasında başvurulabileceği kabul edildiğinde eldeki deliller, mahkûmiyet hükmü kurmak için yeterli olmaması halinde suçun sübutu tedbire başvurulması için gerekliyse, söz konusu tedbir ile ilgili "başka türlü delil elde etme imkânı bulunmaması" halinin gerçekleştiği kabul edilmelidir.[649]

Uygulamada söz konusu tedbirin başvurulmasına ilişkin karar verilirken, bu şarta bağlı kalınmayarak yasa maddesi tekrar edilmesi suretiyle karar verilmektedir. Bu durum, elde edilen delillerin hukuka aykırılığını teşkil etmektedir. Ayrıca her soruşturma için ilk olarak bu tedbire başvurulması, özel hayatın gizliliği ve kişisel verilerin güvenliğini tehlikeye sokmaktadır.[650] Buna karşılık, bilişim sistemlerine karşı ya da bilişim sistemlerinin araç olarak kullanılmasıyla işlenen suçlarda, ilk olarak veri bütünlüğü sağlanarak bilişim sisteminin incelenmesi gerekmektedir. Bu durumda, başka şekilde delil elde etmeye çalışılması halinde, bilişim sistemine başvurulduğu zaman geç kalınabilir. Böylece, fail ve delil için kullanılacak verilere ulaşmak zorlaşır.[651] Bu hususa ilişkin öğretide ki bir başka görüşe göre, bilişim suçlarında ilk bakılması gereken şüphelinin kullandığı bilgisayar olması sebebiyle, CMK'un 134. hükmüne göre hareket edilmesi halinde, bilişim suçlarında elektronik delil elde edilmesi sıkıntıya sebep olabilecektir. Zira bilişim suçları doğası gereği şüphelinin bilgisayarında arama vb.

[646] AKTAŞ, s. 223
[647] YENİSEY/NUHOĞLU, s. 197; ORTA, s.219.
[648] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.216.
[649] YAŞAR/DURSUN, ss. 12-13.
[650] DÜLGER, Bilişim suçları ve internet iletişim hukuku, ss. 547- 548.
[651] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s. 548.

işlemlerin yapılması gerekmektedir.[652] Bu halde, CMK m.134'e göre delilleri araştırıp, başka delil elde etme imkânının bulunmadığının kanıtlanması ve bunun sonucunda şüphelinin bilgisayarında arama, kopyalama ve elkoyma işlemlerine ilişkin izin alınması işin doğasına aykırı olup, soruşturma evresini sıkıntıya uğratabilmektedir.[653]

Bu konuda öğretide bir görüş, gerekli hızın sağlanması amacıyla birinci fıkraya istisnai bir hüküm getirilerek, TCK'da yer alan bilişim alanında işlenen suçlar bölümünde ve aynı kanunun 135, 136, 138, 142/2-e, 158/f-1 maddelerinde yer alan suçlar için başka suretle delil elde etme imkânı bulunmaması şartı aranmaz şeklinde düzeltilmesinin yerinde olacağını ileri sürmektedir.[654] Diğer bir görüşe göre ise, yine 134. maddeye bir fıkra eklenerek, bilişim suçlarına ayrık bir hüküm getirilmesi suretiyle bilişim suçlarının soruşturma evresinde bilişim sistemlerinde arama, kopyalama ve elkoyma işlemlerine ilişkin CMK 134/1 değil, CMK m. 116 uygulanarak, suç delillerinin elde edilebileceği hususunda makul şüphenin yeterli sayılması gerektiğini ileri sürmektedir.[655]

Her ne kadar, şüphelinin kullandığı bilişim sisteminde maddede belirtilen diğer unsurlara yönelmek için başka suretle delil elde etme imkânının bulunmaması şartı, kişi hak ve özgürlükler bakımından yerinde ise de, işin niteliği bakımından problemler oluşturabilir. Zira bir suç soruşturmasında bilişim sistemine derhal el konulmaması veya arama yapılmaması durumunda, deliller kaybolabilecektir.[656] Kanaatimizce, özellikle bilişim suçları mevzu bahis olduğunda, delillerin elde edilebilmesi için hızlı davranılması gerekmektedir. Aksi halde hassas yapısı gereği elektronik delillerin ele geçirilmesi zorlaşabilir. Bu sebeple, CMK m.134 hükmünün uygulanması için, başka suretle delil elde edilmesi yoluna gidilmesi, bilişim suçları söz konusu olduğunda istisnaya tabi tutulmalıdır.

[652] KARAGÜLMEZ, s. 505; ORTA, s.219.
[653] KARAGÜLMEZ, ss.505-506; BAŞLAR, Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri, ss.89-90.
[654] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s. 548.
[655] KARAGÜLMEZ, ss.505-506; TANRIKLU, s.355; BAŞLAR, Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri, ss.89-90.
[656] Bu görüşe göre bilgisayardaki bazı deliller, zaman geçirilmeden arama ve kopyalama işlemleri yapılırsa elde edilebilir. KARAGÜLMEZ, s.504.

d. Tedbir kararını verecek merci ve kararın kapsamı

d.1. Tedbir kararını verecek merci

CMK m. 134'te belirtilen tedbirlerin uygulanmasına ilişkin cumhuriyet savcısının istemi üzerine hakim kararı olması gerektiği vurgulanmıştır. Söz konusu hakim sulh ceza hâkimi olup,[657] istisnai hal olarak gecikmesinde sakınca bulunan hal olması durumunda dahi diğer koruma tedbirlerinde olduğu gibi, örneğin arama, yakalama ve el koymada olduğu gibi cumhuriyet savcısına karar verme yetkisi verilmemekteydi.[658] Olağanüstü hal kapsamında yürürlüğe giren 668 sayılı Kanun Hükmünde Kararname ile CMK m 134 düzenlemesinde değişiklik meydana gelmiştir.[659] KHK m.3/1-j hükmü ile, CMK m.134 doğrultusunda yapılacak tüm işlemlere, gecikmesinde sakınca bulunan durumlarda cumhuriyet savcısının kararı ile başvurulabilecektir. Cumhuriyet savcısı bu kararı beş gün içerisinde hakim onayına sunacaktır. Hakim kararını, elkoyma işleminin gerçekleştiği tarihten itibaren on gün içerisinde açıklayacaktır. Ayrıca işlemlerin uzun sürmesi durumunda aygıta el konulabilecektir. [660] Öğretide bir görüşe göre, bu düzenleme olağanüstü hal süreci içerisinde ve sadece belirli suçlara ilişkindir.[661] Öğretide başka bir görüş, bu hükmün anayasa ile kurulu düzene, devletin güvenliğine karşı veya toplu olarak işlenen suçlar bakımından uygulama alanı bulacağını ifade ederek, anılan suçlar dışında işlenen suçlar bakımından yine CMK m.134 hükmünün uygulanacağını ifade etmiştir.[662]

25/7/2018 tarihinde kabul edilen 7145 sayılı Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun' nun 16. maddesi ile CMK m.

---

[657] CENTEL/ZAFER, Ceza muhakemesi hukuku el kitabı, s.372.
[658] YENİSEY/NUHOĞLU, ss. 412-413.
[659] YENİSEY, Ceza muhakemesi hukuku başvuru kitabı, ss.135-136.
[660] ŞEN E. Bilgisayarda Arama, Kopyalama ve Elkoyma, https://www.haber7.com/yazarlar/prof-dr-ersan-sen/2075545-bilgisayarda-arama-kopyalama-ve-elkoym [22.06.2020].
[661] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s. 212; ÖZTÜRK B. (Ed), 2017. Nazari ve uygulamalı ceza muhakemesi hukuku ders kitabı, 11. Baskı, s.236.
[662] "*668 sayılı KHK; olağanüstü halin devam ettiği sürece uygulanacağından, olağanüstü halin kaldırıldığı anda bilgisayara elkoyma konusunda öngörülen istisnai tedbirin tatbiki de son bulacaktır. KHK uygulandığı sürece, KHK'da özel hüküm bulunmayan hallerde CMK uygulanmaya devam eder. Bu sebeple; bilgisayarda arama, kopyalama ve elkoyma konusunda CMK m.134 ve 668 sayılı KHK m.3/1-j birlikte tatbik edilecektir. Bu tatbik sırasında KHK'da sayılan suçlar yönünden öncelik m.3/1-j'ye ait olacak, burada hüküm bulunmayan halde CMK m.134'e göre hareket edilecektir*." ŞEN E. https://www.haber7.com/yazarlar/prof-dr-ersan-sen/2075545-bilgisayarda-arama-kopyalama-ve-elkoyma [22.06.2020].

134'e ilişkin "*Cumhuriyet savcısının istemi üzerine*" ibaresi "*hakim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından*" şeklinde değiştirilmiş, fıkrada yer alan "*hakim tarafından*" ibaresi madde metninden çıkarılmıştır. Bu sebeple, bilgisayarda arama, kopya alınması ve el konulması işlemleri gecikmesinde sakınca bulunan hallerde, Cumhuriyet savcısı tarafından da karar verilebilecektir. Buna bağlı olarak kararın 24 saat içerisinde görevli hakimin onayına sunulması gerekmektedir.[663] Görevli hakiminde, kararını en geç 24 içerisinde vermesi gerekir. Belirtilen sürenin dolması halinde ya da hâkim söz konusu karardan aksi yönde karar vermesi durumunda, çıkarılan kopyalar ve çözümlenerek oluşturulan metinler derhal imha edilmelidir.[664] Belirtmek gerekir ki, gecikmesinde sakıncalı bulunan hâlin söz konusu olmadığı durumlarda, Cumhuriyet savcısı tarafından verilen ve icra edilen arama, kopyalama ve elkoyma kararı, sonradan hakim onayına sunulsa bile hukuka aykırı olacak ve bu karar ile elde edilen deliller de hukuka aykırı kabul edilecektir.[665]

Bunların yanı sıra, CMK 134'ncü maddenin birinci fıkrasında savcının arama, kopyalama ve metin haline getirme yetkisi düzenlenmiştir. Ancak, elkoyma yetkisi ikinci fıkrada yer almaktadır. Bu kapsamda, ikinci fıkrada benzer şekilde, cumhuriyet savcısına yetki verilmemesi, bazı tereddütlere neden olabilmektedir. Şöyle ki, ilk olarak elkoyma tedbiri bakımından da, savcının yetkili olduğu düşünülebilir. Dolayısıyla, gecikmesinde sakınca bulunan halin varlığında, Cumhuriyet savcısı da bilişim sistemlerinde elkoymaya karar verebilir. İkinci olarak ise, elkoyma bakımından sadece hakimin yetkili olduğu sonucuna varılabilir. Bu bağlamda, birbirinden farklı iki sonuç, madde lafzından çıkarılabilmektedir. Bu hususta DEĞİRMENCİ, "*birinci fıkrada, diğer tedbirlerin yanı sıra elkoyma tedbiri de düzenlenmeliydi. Fıkranın sonuna ise kopyaların ve çözümü yapılan metinlerin imhasının yanı sıra elkonulan eşyanın da derhal iade edileceğine veya elkoymanın derhal kalkacağına yer verilmeliydi. Bu düzenleme, ikinci fıkra ile de bir uyumsuzluk teşkil etmeyecektir. Nitekim birinci fıkrada*

[663] http://www.resmigazete.gov.tr/eskiler/2018/07/20180731-1.htm [23.12.2018].
[664] YENİSEY/NUHOĞLU, s. 413.
[665] DEĞİRMENCİ, Bilgisayarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbirinde(CMK m. 134), 7145 sayılı kanunla yapılan değişikliklerin değerlendirilmesi, s.151.

elkoyma kararı verecek makamlar düzenlenirken, ikinci fıkrada ise elkoymanın seçenek koşulları düzenlenmiş olacaktır." şeklinde çözüm önerisinde bulunmuştur.[666]

Bilgisayarda arama, kopyalama ve elkoyma tedbirine, ceza muhakemesinin hangi aşamasında başvurulacağı hususunda doktrinde farklı görüşler bulunmaktadır. Bu hususta, söz konusu tedbirin yalnızca soruşturma aşamasında uygulanabileceğini ifade eden görüş[667] bulunmaktayken, madde kapsamında suç soruşturmasının varlığı şartını dar anlamda yorumlanmaması gerektiği, eksik deliller söz konusu olması halinde, kovuşturma aşamasında da bu tedbirin uygulanması gerektiği görüşünü kabul eden yazarlar da bulunmaktadır.[668] Öğretide bir görüş, soruşturma evresinin cumhuriyet savcısı tarafından yürütülmesi ve tedbirin sadece soruşturma aşamasında uygulanabilir mahiyette bir tedbir olması sebebiyle, hakimin savcının talebi bulunmadan resen söz konusu tedbirin uygulanması yönünde bir karar vermesinin mümkün olmadığını belirtmiştir.[669] Buna karşın bir başka görüşe göre ise, CMK m. 134 hükmüne, şartları sağlaması halinde kovuşturma aşamasında da başvurulabilecektir. Bu bağlamda, kovuşturma evresinde de cumhuriyet savcısının talebiyle veya talep olmadan söz konusu tedbire resen araştırma ilkesi gereğince, hakim ya da mahkeme tarafından bilişim sisteminde arama kopyalama ve elkoyma tedbirine başvurulabileceğini öne sürmektedir.[670] Başkaca bir görüş, kovuşturma aşamasında delil toplamak için tedbire başvurulması hususunda herhangi bir engel bulunmadığını, bu sebeple başvurulabileceğini, ancak sanığın kararı duruşmada öğrenecek olması sebebiyle kendisinde bulunan bilişim delillerini yok edebilmesinin mümkün olduğunu, bu durumda da kovuşturma aşamasında, bilgisayarda arama tedbirinin uygulanması kararının istenilen sonuca ulaşmayacağını ifade etmektedir.[671] Diğer bir görüşe göre ise, maddi vakanın gerçekleşip gerçekleşmediğine vicdani kanaat getirme görevi, kovuşturma safhasında mahkemeye aittir. Bu kapsamda mahkemenin, yargılama sırasında ortaya çıkan ihtiyaca istinaden, tedbir kararı verebilmesi için bilişim

[666] DEĞİRMENCİ, Bilgisayarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbirinde(CMK m. 134), 7145 sayılı kanunla yapılan değişikliklerin değerlendirilmesi, s.152.
[667] YENİSEY/NUHOĞLU, s. 412; GÜNEYSU, s.115.
[668] ÖZEN/ÖZOCAK, s.62; BAŞTÜRK, s.25.
[669] BAŞLAR, ss.165-166.
[670] YAŞAR/DURSUN, s.13; ÜNAL, s.105.
[671] CENTEL\ZAFER, s.373; ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s. 218.

sistemlerinde yer alan verilerde arama yaptıramayacağını söylemek, ceza muhakemesini şekilsel bir süreç olduğu kanısını doğurur.[672] Bu konuda, kovuşturma aşamasında da şüphe olması halinde, şüpheyi yenmek için mahkemenin söz konusu tedbire başvurabileceği[673] kabul edilmelidir. Nitekim kovuşturma evresinde, bilgisayarda arama, kopyalama ve elkoyma tedbirine başvurma kararı verilmesine ilişkin Yargıtay kararları bulunmaktadır.[674] Sonuç itibariyle, soruşturma evresinde sulh ceza hâkimi, kovuşturma evresinde ise yargılamayı yapmakta olan mahkeme veya hakim, tedbire hükmedecektir. Eğer yargılamayı yapan mahkeme heyet halinde çalışan bir mahkemeyse, oy çokluğu ile karar verilmesi gerekir.[675] Kanaatimizce, kanunilik ilkesi gereği[676] kanun koyucunun CMK m. 134'ü yeniden kaleme alarak kovuşturma aşamasında da tedbire başvurabileceğinin, madde metnine eklenmesi yerinde olacaktır.

Bunların yanı sıra, CMK m.163'te yer alan bazı durumlarda sulh ceza hâkiminin soruşturma işlemleri de yapabileceği öngörülmüştür. Bu hükme göre, "*suçüstü hali ile gecikmesinde sakınca bulunan hallerde, cumhuriyet savcısına erişilemiyorsa veya olayın genişliği itibariyle cumhuriyet savcısının iş yükünü aşıyorsa, sulh ceza hâkimi de bütün soruşturma işlemlerini yapabilir*" şeklindedir. Böyle bir durumla karşılaşılması

---

[672] "*Bu dönemde ceza hukuku uygulamasının da kovuşturma esnasında söz konusu tedbire başvurma yönünde geliştiğini söylemek mümkündür. Özellikle kamuoyunun ilgisini çeken davalarda, mahkeme tarafından CMK m.134 tedbirine kovuşturma aşamasında başvurulduğu görülmüştür. Gerek mahkemeler tarafından kovuşturma aşamasında söz konusu tedbire başvurulurken gerek denetim muhakemesi esnasında Yargıtay tarafından konunun incelenmesi aşamasında söz konusu ayrıma hiç temas edilmemesi, kovuşturma aşamasında tedbire başvurmaya yasal metnin izin verip vermediğine ilişkin bir gerekçelendirme yapılmaması da not etmemiz gereken durumlardan birisidir".* DEĞİRMENCİ, Bilgisayarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbirinde(CMK m. 134), 7145 sayılı kanunla yapılan değişikliklerin değerlendirilmesi, s.150.

[673] *Kovuşturma aşamasında mahkemenin vereceği tedbirin kararının duruşmada aleni olması sebebiyle tedbirin muhatabının önceden haberdar olacağı bahisle söz konusu tedbirin yararlı olmayacağına ilişkin görüşlere katılmamaktadır. Ayrıca CMK m.207 uyarınca kovuşturma aşamasında da istisnai olarak elektronik delil toplanabileceğini belirtmektedir. Bu düşüncesini de Yargıtay bir kararı ile desteklemektedir "mağdurun cep telefonuna gönderilen mesajların hangi bilgisayardan gönderildiğinin tespit edilmemesini soruşturmada önemli bir eksiklik olarak görmüş ve bu tespitin kovuşturma aşamasında giderilmesi için, ilk derece mahkemesinin kararını bozarak iade etmiştir."* Yargıtay 4. CD.'nin 09.05.2006 tarihli ve 16417 E., 10607 sayılı kararı aktaran TANRIKULU, ss . 399-400.

[674]Yargıtay 1. Ceza Dairesi, 14 Kasım 2005 tarih ve 3891/3230 esas ve sayılı kararında "*olay tarihinde sanıkla maktulün internet üzerinde sohbet etikleri söylenen kafede sanığın Kaan kod adıyla 21 nolu masada ve maktulün kullandığı belirtilen bilgisayarların ve kullandıkları programın saptanarak bilgisayarlarda ve bilgisayar programının merkezi sisteminde sohbet kaydının mevcut olup olmadığı ve içeriğinde hakaret ve tahrik edici sözler olup olmadığı tespit edilmeden…*" şeklinde bozma kararı vermiştir. Aktaran ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.218.

[675] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.217.

[676] AKTAŞ, s. 222.

halinde, söz konusu tedbire ilişkin olarak sulh ceza hakiminin, savcılık sıfatına da taşıyorken hakim kararını gerekli kılan bir işleme yönelik karar verip veremeyeceği hususunda öğretide fikir ayrılığı bulunmaktadır. Bir görüşe göre, olayın genişliği cumhuriyet savcısını aşıyorsa, yani küçük bir ilçede tek bir cumhuriyet savcısının bulunuyor ve bu savcının zorunlu olarak başka bir işle meşgul olması ve aynı anda derhal harekete geçilmesi gerektiren bir durum hasıl ise, hakim CMK m.163 uyarınca resen işlemi gerçekleştirebilir.[677] Başka bir görüş, bu durumun hakimin tarafsızlığı ilkesine aykırılık oluşturacağından dolayı mümkün olamayacağı[678] ve sulh ceza hakiminin, CMK m.134' te yer alan tedbirlerine savcılık sıfatı da bulunurken karar veremeyeceğine yöneliktir. Bu şekilde bir durumun cereyan etmesi halinde, savcılık görevini yürüten sulh ceza hakimi tedbirin uygulanmasını talep etmeli, kendisini karar vermeden, başka bir sulh ceza hâkimden karar alması gerekmektedir.[679]

d.2. Tedbir kararının şekli

Anayasa'nın 20. maddesinin ikinci fıkrası gereği, tedbire ilişkin karar yazılı şekle tabidir.[680] Buna ilaveten daha önce de izah ettiğimiz üzere CMK m. 134'de yer verilmemiş bazı hususlar için, genel arama ve elkoyma hükmü dikkate alınacaktır. Bu itibarla CMK m. 119 hükmünün uygulanması gündeme gelecektir.[681] Bu bağlamda söz konusu tedbire başvurulurken düzenlenecek arama kararında, şüphelinin açık kimliği, arama nedeni, aramanın hangi eşyalar üzerinde yapılacağı ve arama kararının geçerli olacağı süre[682] gibi hususlara yer verilmelidir. Bunun yanı sıra elde edilen elektronik verilerin ne şekilde koruma altına alınacağı ve bu verilerin başka soruşturmalar için kullanılıp kullanılmayacağı hususlarının[683] kararda belirtilmesi, ileri safhalarda ortaya çıkabilecek olası hukuksal problemlerin engellenmesi bakımından önem arz edecek niteliktedir.[684] Ayrıca söz konusu tedbire ilişkin kararda başka bir tedbir ile istenen

[677] TAŞKIN, Bilişim suçları, 169.
[678] ÜNAL, s.106.
[679] BAŞLAR, Ceza yargılamasında elektronik delil, ss.166-167; ÖZEN/ÖZOCAK, s.63.
[680] Arama kararının yazılı olmasının amacı, yargılamanın ilerleyen saflarında bu kararın hukuka uygunluğunun denetlenmesine imkân sağlamaktır. TANRIKULU, ss.403-404.
[681] ÜNAL, s.105.
[682] Bilişim sisteminde yapılacak aramalarda, aramaların ne kadar süre için geçerli olduğuna dair kanunda özel bir süre sınırı söz konusu değildir. Bu şekilde arama kararının ne kadar süre içerisinde geçerli olacağına ilişkin süre sınırlamasının bulunmaması eleştirilmiştir. TANRIKULU, ss.396-397.
[683] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.224.
[684] TANRIKULU, ss.405-406.

delillerin neden elde edilemeyeceği unsurları[685] ve kuvvetli şüphe sebeplerinin de yer alması gerekmektedir.[686] Zira ilerleyen aşamalarda ileri sürülen bu sebep, verilen kararın hukuki açıdan değerlendirilmesinde yardımcı olacaktır.[687] Arama ve elkoymanın tutanağa bağlanmasında aramayı yapan görevlilerin kimlik bilgilerinin tutanağı geçirilmesi, arama sırasında bulunması gereken kişiler, arama sonunda verilecek belge gibi hususlar da tedbirin arama ve elkoymanın özel bir şekli olmasından dolayı genel hükümlerde dikkate alınır.[688]

Tüm bunlarla birlikte, tedbir kararına konu olacak bilişim sisteminin şüpheliye ait olmaması durumunda, şüpheli tarafından kullanıldığına dair kanaatin oluşma nedenlerine de istemde yer verilmelidir. Böyle bir durumla karşılaşıldığında cumhuriyet savcısının tedbir talebinde şüpheli ile kullanılmış olan bilişim sistemi arasındaki ilgiyi ortaya koyması ve sulh ceza hakiminin de bu hususu değerlendirdikten sonra tedbir kararına hükmetmesi gerekmektedir.[689]

d.3. Arama kararının kapsamı

Arama kararının kapsamının belirlenmesi, söz konusu tedbirin uygulanmasıyla gerçekleştirilecek olan müdahalelerin çerçevesinin oluşması bakımından önemlidir. [690] Tedbir kararı bilişim sistemlerinde arama yapılmasına, kopya çıkarılmasına ve buradan elde edilen kayıtların çözülerek metin haline getirilmesine yöneliktir.[691] Madde metninde arama kararının kapsamı şüphelinin kullandığı; bilgisayar, bilgisayar programları ve bilgisayar kütükleri olarak belirtilmiştir. Ancak daha önce de izah ettiğimiz üzere, tedbir kararının konusu, gündelik hayatta sıkça kullandığımız cep telefonu, tabletler, sunucular, yazıcılar, ağlar ve diğer veri depolama araçları da olabilmektedir. Bu bakımdan, arama kararında arama yapılacak olan bilişim sisteminin belirlilik ilkesi de gözetilerek, sınırlarının çizilmesi gerekmektedir.[692] Aksi bir

---

[685] ÜNAL, s.105.
[686] Arama kararı talebinde, arama kararının gerekliliğini belirten hususlara da yer verilmeli ve tedbire son çare olarak başvurulmasının nedeni ortaya konulmalıdır. DEĞİRMENCİ, Ceza muhakemesinde sayısal (Dijital) delil, ss.353-354.
[687] TANRIKULU, s.406.
[688] ÇAM A.R., 2015 Adli kolluk ve bilişim, İstanbul, On İki levha Yayıncılık. s.37.
[689] BAŞLAR, Ceza yargılamasında elektronik delil, s. 168; DEĞİRMENCİ, Ceza muhakemesinde sayısal (Dijital) delil, s.354
[690] TANRIKULU, s.404.
[691] ÖZEN/BAŞTÜRK, s.150; ÜNAL, s.105.
[692] TANRIKULU, ss.404-405

yaklaşımla hareket edilerek, arama işleminin gerçekleştirileceği bilişim sistemi olarak tüm bilgisayarlar, veri depolama araçları gibi tüm veri depolama aygıtlarının belirtilmesi durumunda hukuki sıkıntılar meydana gelebilecek[693] ve hukuka aykırılık teşkil edecektir.[694] Çünkü kararda neyin aranacağına açıkça yer verilmemesi, arama esnasında kolluğa çok geniş hareket alanı sağlamakta olup, hukuka aykırı deliller de tam da bu noktada ortaya çıkmaktadır.[695]

CMK m. 134 hükmünün uygulanacağı araçlar açısından bu şekilde sınırlandırmaya gidilmesinin sebebi, şüpheliye ait olan fakat suçla bir alakası olmayan bilişim sistemleri üzerinde, tedbire başvurulmasının engellenmek istenmesidir. DEĞİRMENCİ' ye göre, arama yapılacak bilişim sisteminin özelleştirilmesi gerekmektedir. Ancak, her somut olayda suç ile ilişkili bilişim sisteminin net olarak tespiti mümkün değildir. Bu görüş, bilişim sisteminin özelleştirilmesinin iki şekilde sağlanabileceğini ifade etmiştir. Bunun için ilk olarak, tedbirin uygulanacağı bilişim sisteminin suçun işlenmesinde, şüpheli veya sanığın kullanılıp kullanmadığı değerlendirilmeli ve bu kullanılan bilişim sistemi kararda gösterilmedir. Çünkü şüpheli veya sanık tarafından "kullanılan veya kullanılma olasılığı bulunan" şeklinde bir ifade, kolluğa geniş bir yetki sağlayacağından, temel hak ve hürriyetlere müdahale söz konusu olabilir. İkincisi ise, bilişim sisteminin suç ile bağının kurulması gerektiğidir. Yani, sistemdeki hangi suçun delilleri aranacağının açıkça belirtilmesidir. [696]

Arama tedbirine istinaden, arama kararında yer alması gereken başka bir husus ise, tedbirin konu oluşturan bilişim sistemi üzerindeki, bazı özel dosyaların ya da verilerin mi aranacağı, yoksa sistemdeki tüm dosyaların kopyasının alınarak bunlar üzerinde mi arama yapılacağının belirtilmesi gerektiğidir. Öğretide başka bir görüşe göre, özel hayat ile ilgili kişisel verilerin bulunabileceği bir bilgisayardaki tüm dosyaların açılması, özel hayatın gizli alanına müdahale oluşturabilir.[697] Avrupa İnsan Hakları Mahkemesi de, Craxi v. İtalya, Petri Sallinen v. Finlandiya ve Smirnov v. Rusya kararlarında, bilgisayarda gerçekleştirilen arama işleminde, elde edilen tüm kişisel verilerin ortaya

[693] TANRIKULU, s.405.
[694] DEĞİRMENCİ, Ceza muhakemesinde sayısal (Dijital) delil, s.354.
[695] SEVİMLİ, A. G., 2007. Bilgisayar ve bilgisayar kütüklerine el konulması ve uygulamadaki sorunlar. İstanbul Barosu Dergisi. 81(3), ss. 993-1000, s.95.
[696] DEĞİRMENCİ, Ceza muhakemesinde sayısal (Dijital) delil, s.354.
[697] YENİSEY/NUHOĞLU, s.406

çıkarılmasının 8'nci maddenin ihlali olduğunu belirtmiştir. Bu nedenle, bilgisayarlarda yapılacak inceleme ve aramalarda, belli bir arama yönteminin uygulanmasının ve bilirkişi tarafından veya uzman olarak görevlendirilen bir kişi tarafından tüm belgeleri açmayacak şekilde yapılması gerekmektedir.[698] Bu görüşe göre, "*Devlet, hakim kararı ile de olsa, bir kişiye ait bilgisayar hafızasında kayıtlı bulunan bütün dosyaları tek tek açıp okuyarak, "belki bir tanesinden bir delil elde edebilirim", düşüncesiyle inceleme yapamaz. Bunu yapması, bir şehirdeki bütün evleri bir tek karar ile aramaya veya konutta arama yapmak için karar verirken, aranacak şeyin belirtilmemesine benzer. Halbuki, CMK 119 da belirtildiği üzere, her bir arama kararı, hangi konutun aranacağını ve burada neyin aranacağını belirtmek zorundadır: "toplu arama kararları" verilemez."*[699] Öğretide bir başka görüş, bilgisayarda arama ifadesi yerine 'elektronik veri takibi' deyişini kullanmaktadır. Bu görüşe göre, "elektronik veri takibi, şüphelinin bilişim sistemindeki bütün dosyaların tek tek açılması şeklinde değil, belli dosyalar üzerinde gerçekleştirilmelidir.[700]

Sözleşmenin 19. maddesinde düzenlenen bilgisayarda arama, bilgisayar verisine girmek anlamındadır. Burada, usul kurallarına uygun bir şekilde elde edilmiş bilgisayar verisinde arama yapılması ve teknik anlamda elkonulması söz konusudur. Bir bilgisayarda arama yapılabilmesi için, üç ayrı işlem türü düzenlenmiştir. Bunlar; bilgisayar sistemine girmek, bilgisayar sisteminde kayıtlı bulunan verinin içine girmek, bilgisayar verisi saklanan ortama girmek şeklindedir. Bu kapsamda, bilgisayarda arama kararı verecek olan hakimin, hangi işlemin yapılacağını kararında göstermesi gerekir.[701]

e. Arama kararı ile elkoyma kararının ilişkisi

CMK m.134 hükmünde arama, kopyalama ve elkoyma işlemlerine ilişkin hususlar yer almaktadır. CMK m.134'te yer alan tedbirlere ilişkin ayrıca, her biri için karar verilebileceği gibi, birden fazla tedbire de aynı anda karar verilebilir.[702] Öğretide, bilişim sisteminde arama tedbirinin elkoyma tedbirini de kapsayıp kapsamadığı hususunda fikir ayrılığı bulunmaktadır. Bir görüşe göre, bir suç dolayısıyla verilmiş

[698] YENİSEY/NUHOĞLU, ss.410-411.
[699] YENİSEY/NUHOĞLU, Ceza muhakemesi hukuku ders kitabı, s.588.
[700] BIÇAK, s.727.
[701] YENİSEY/NUHOĞLU, s. 410.
[702] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.355.

olan arama tedbiri kararının elkoyma tedbirini de kapsaması gerekir. Bu görüş, arama kararının aynı genel arama ve elkoymadaki gibi elkoyma yetkisini de kapsadığını, çünkü kolluk görevlilerinin bilişim sisteminde şifre veya gizlenmiş bilgilerle karşılaşmasının olasılık dâhilinde olduğunu ve bu durumun önceden bilinemeyeceğini ifade etmiştir.[703] Buna karşılık öğretide bir görüş, bilişim sistemi üzerinde şifrelenmiş veya gizlenmiş verilerin olabileceği, ya da işlemin uzun sürecek olması durumunu kolluğun önceden tespitinin zorluğu karşısında, maddede belirtilen ön koşulları sağlaması halinde, elkoyma tedbirine de başvurulabileceğini içeren bir kararın verilmesi gerektiğini ileri sürmektedir.[704] Uygulamada hem arama kararı, hem elkoyma kararı aynı kararla birlikte verilmektedir. Elkoyma tutanağında, hangi nedenlerden dolayı CMK m.134/2 kapsamında elkoyma yapıldığı ve bu sebepleri oluşturan, kanaate vardıran olgulara yer verilmelidir. Zira CMK m.134/2'de yer alan durumdan biri gerçekleşmeden yapılan elkoyma hukuka aykırı olacaktır. [705] Bu bağlamda, iki tedbire ilişkin verilmiş tedbir kararına istinaden, öncelikle arama işlemi uygulanmalı ve eğer bu şekilde delil edilmesi mümkünse, elkoyma işlemi gerçekleştirilmemelidir.[706] Aksi halde, orantılılık ilkesine aykırılık[707] teşkil edilecek, kişilerin özel hayatlarının gizliliğine ve mülkiyet haklarına müdahale oluşturacaktır.[708]

Tüm bunlarla birlikte, birbirine bağlı olan arama ve el koyma işlemlerinde, hukuka aykırı bir arama kararı veya hukuka aykırı bir arama işlemi uygulaması söz konusu ise, buna bağlı olarak yapılacak elkoyma da hukuka aykırı olacaktır.[709]

2. Elkoyma Tedbiri Bakımından

CMK m.134 hükmünde, belirtilen bir diğer tedbir de elkoyma işlemidir. "*Bilişim verilerine elkoyma, ya da onları muhafaza altına alma, verileri kopyalamak yoluyla delil toplamak ya da verileri kopyalamak ve daha sonraki orijinal versiyonları erişilmez*

[703] ÜNAL, s.106.
[704] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.355.
[705] DEĞİRMENCİ, Bilgisayarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbirinde(CMK m. 134), 7145 sayılı kanunla yapılan değişikliklerin değerlendirilmesi, s.152.
[706] GÜNEYSU, s.115.
[707] ÖZBEK/DOĞAN/BACAKSIZ, s.261.
[708] ÖZEN/ÖZOCAK, s.66.
[709] SEVİMLİ, s. 994.

kılmak ya da taşımak yoluyla verileri müsadere etmek demektir. Bu anlamda "elkoyma", verilerin nihai olarak silinmesi anlamına gelmemektedir. (Açıklayıcı Rapor paragraf 197–199).[710]

Elkoyma işlemi arama ve kopyalama işlemlerinden daha ağır bir nitelikte olup, bu işlemlere göre temel hak ve özgürlüklere nispeten daha yoğun etkisi olmasından dolayı, bu tedbirin uygulanması için daha sıkı şartlar öngörülmüştür.[711] Öğretide bir görüşe göre, söz konusu tedbirle birçok kişisel verilere ulaşılması mümkündür. Bireyin kendisine ait kişisel bu bilgiler üzerinde karar verme ve belirleme yetkisi bulunmaktadır. Dolayısıyla bilgisayar verilerine karşılaştırma amacıyla el konulmasının sınırlandırılması gerekmektedir.[712]

Elkoyma işleminin uygulanması için CMK m.134/1'de belirtilen şartlarla birlikte, "*şifrenin çözülememesinden dolayı bilgisayara girilememesi veya gizlenmiş bilgilere ulaşılamamış olması ya da "işlemin uzun sürecek olması"* hallerinden birinin gerçekleşmesi gerekir.

a. Bilgisayarlarda, bilgisayar programlarında ve bilgisayar kütüklerinde arama, kopyalama tedbirine karar verilmiş olması

Bilgisayarlarda, bilgisayar programlarında ve bilgisayar kütüklerinde elkoyma tedbirinin uygulanabilmesi için gereken ilk şart, CMK m. 134/1'de belirtilen usule uygun olarak verilmiş bir arama ve kopyalama kararının mevcut olmasıdır.[713] Elkoyma tedbirinde, usule uygun olarak yapılan arama işlemi sonucunda, bilişim sisteminin kanun koyucunun belirttiği durumlar sebebiyle kopyalanamaması söz konusudur. Dolayısıyla, elkoyma tedbirine başvurulmadan önce arama, kopyalama tedbirinin uygulanması gerekmektedir.

Kanun koyucunun, bir bilişim sisteminde elkoyma işlemini, genel elkoyma tedbirine göre daha sıkı şartlara bağladığı görülmektedir. Zira bilişim sistemi söz konusu olduğunda, CMK m.123 hükmünde olduğu gibi, doğrudan malvarlığı değerine elkonulması öngörülmemiştir. CMK m. 134/2'deki şartların varlığı halinde, elkoymanın

[710] YENİSEY/NUHOĞLU, Ceza muhakemesi hukuku ders kitabı, s.592.
[711] ÖZEN/BAŞTÜRK, ss.150-15; BAŞTÜRK, s.28.
[712] CENTEL/ZAFER, s.374.
[713] YAŞAR/DURSUN, ss.13-14.

gerçekleşebileceği düzenlenmiştir. Bunun sebebi ise, söz konusu tedbirin diğer malvarlığı değerlerine göre daha fazla temel hak ve özgürlükler ile ilişkili olmasıdır.[714]

Öğretide bir görüş, pek çok kaynakta CMK'nın 134. maddesindeki düzenlemeyi elkoyma konusu altında değerlendirildiği, ancak bu düzenlemenin, arama koruma tedbirinin bilişim sistemleri üzerinde icra edilmesini ön gören bir hüküm olduğunu ileri sürmektedir.[715] Diğer bir görüş ise, CMK m. 134'ü "*elkoyma işlemi değil, arama ceza muhakemesi önleminin bilgisayar kütük ve programlarında icrasıyla ilgili özel bir hükümdür.*" şeklinde ifade etmiştir. Bu görüşe göre, söz konusu düzenleme bir elkoyma hükmü değil, arama hükmüdür. Sadece verilerin kopyalarının oluşturulması sağlanmakta, başka deyişle delil tespiti yapılmaktadır.[716] Buna karşı bir görüş, 134. maddede ceza muhakemesi işlemlerinden "arama", "elkoyma" ile aynı zamanda "kopyalama" türünden işlemlerin bir arada yapılabileceği bir koruma tedbirine yer verildiği, bu sebeple elkoyma hükmünü içermediğini, yalnızca aramanın özel bir işlem türü olduğu görüşüne katılmamaktadır.[717] Başka bir görüş, bilgisayarda arama, kopyalama ve elkoyma tedbirinin, arama ve elkoymanın özel bir şekli olduğunu ifade etmektedir.[718] Bir başka görüş ise aramanın, bilişime özgü özel bir türü olan yeni bir kurum olduğunu ifade etmiştir.[719] Diğer bir görüş ise, özel olarak bilişim sisteminde arama işlemine yer verilmesindeki asıl maksadın, bilişim aygıtlarına el koymaksızın verilere ulaşmanın mümkün olduğu hallerde, bilişim araçlarının tümüne el koyulmasının önüne geçilmek istenmesi olduğunu ifade etmiştir.[720] Aynı görüş, madde metninde el koyma için arama işleminin başarısız olması gerektiğini, ancak bilişim sisteminin şifrelenmiş ya da gizlenmiş veriler barındırdığının nasıl anlaşılacağı hakkında soru işareti bulunduğunu ifade etmiştir. Şöyle ki, bilişim sistemini çalıştırmadan, adli bilişim prensipleriyle incelemeden, içeriği hakkında dışarıdan fikir

[714] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.367.
[715] ORTA, s.216.
[716] ÜNVER/HAKERİ, s.422.
[717] YAŞAR/DURSUN, s. 26.
[718] CENTEL/ZAFER, Ceza muhakemesi hukuku el kitabı s.372; ÖZBEK/DOĞAN/BACAKSIZ, s. 262; YAŞAR, s.6; TANRIKULU, s.351; BAŞLAR Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri, s.93; ÇAM, s.37; ÖLMEZ, s.46.
[719] TANRIKULU, s.353
[720] Bu görüşe göre bilişim sistemine el konulduğu takdirde ve orijinal verilerin sahibine iade edilmesi durumunda dahi, soruşturma konusunun zaten bu bilişim cihazı olmadığı ve içerisindeki veriler olduğunu belirtilmektedir. ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, ss.238-239.

yürütmek mümkün olmamaktadır. Bu hüküm ile her ne kadar sözleşmeye uyum sağlanmış olsa da, bu koşul yeniden kaleme alınarak arama yapılacak, bilişim araçlarına hiçbir işlem yapılmadan doğrudan veri kopyasının oluşturulması, daha sonrasında da bu veri kopyalarına elkoyma tedbirinin uygulanması gerektiğini öne sürmektedir.[721]

Bunların yanı sıra CMK'un 134. maddesinin ikinci fıkrasında, "gecikmeksizin iade olunur" ifadesiyle elkoyma tedbirinin geçici olduğu belirtilmektedir. Öğretide bir görüşe göre, maddenin son fıkrasında "…elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir." şeklinde ki ibareyle, birinci ve ikinci fıkralarda oranlılık ilkesi vurgulanmıştır.[722] Bununla birlikte, CMK 134/2'de istisnai hallerde el konulan "cihazların" gecikme olmaksızın iade edileceği belirtilmiştir. Bu bağlamda malvarlığı hakları bakımından, mülkiyet hakkının ihlal edilmemesi için bu düzenleme önem taşımaktadır.[723] AİHM'si bir kararında, bilgisayarın uzun süre boyunca muhafazasına, AİHS'nin ihlali olarak karar vermiştir. Smirnov vs./Rusya kararında, müştekinin bilgisayarının 6 günden daha fazla bir zaman süresince alıkonulmasının bir nedeninin olmadığı, bilgisayarın müştekinin mesleğini ifa etmesi için bir araç olduğu ve elkoyma-müsadere işlemlerinin kişinin mesleki faaliyetlerini bozduğu, bu sebeple adli makamlarının toplumun genel çıkarları ve bireyin insan hakları arasındaki adil dengeye müdahalede başarısız olduğu, dolayısıyla yapılan işlemin hukuka aykırı olduğu kararını vermiştir.[724]

b. Şifrenin çözülememesinden dolayı bilgisayara girilememesi veya gizlenmiş bilgilere ulaşılamamış olması ya da işlemin uzun sürecek olması

Elkoyma tedbirine başvurulması için gerekli olan diğer bir şart, CMK m.134/2'de "*Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da*

[721] Bu görüş ilk olarak, arama işleminin nasıl yapılacağının beli olmamasını (aramada tanık bulundurulması, hash değerinin alınması, arama yapılmadan önce kopyasının alınıp kopya üzerinden arama yapılması gibi hususlara kanunda yer verilmemiştir.) ifade etmiş, ikinci olarak ise, bilgisayara müdahale edilmesi halinde bilgisayarda bulunan programlar ile delillerin yok edilmesi veya değişikliğe uğramasının mümkün olduğunu ve son olarak da aramada şifrelenmiş veya gizlenmiş verilerin olduğunun tespiti hangi kıstaslarda yapılacağının belirsiz olduğunu belirtmiştir. (Bu durumda saatlerce ve günlerce şüphelinin evinde veya işyerinde ya da aleni bir ortamda vs aramaya devam edilmesi gerekir.) ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.240.
[722] BAŞTÜRK, s.27.
[723] YENİSEY/NUHOĞLU, s.418.
[724] ÜNAL, ss.130-131.

işlemin uzun sürecek olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir" şeklinde belirtilmiştir. Bu üç durumdan birinin gerçekleşmiş olması, tedbire başvurulabilmesi için yeterli olacaktır.

b.1. Şifrenin çözülememesinden dolayı bilgisayara girilememesi

Kanun koyucu, bilişim sisteminde arama, kopyalama ve elkoyma tedbirine ilişkin, öncelikle arama ve kopyalama işlemlerinin uygulanmasını öngörmüş, fakat bazı durumlarda arama ve kopyalamanın mümkün olmaması ihtimalini de göz önünde bulundurarak, bilişim sistemi üzerinde ayrıntılı bir inceleme yapılması için elkoyma işleminin uygulanabileceğini belirtmiştir.[725]

Elkoyma tedbirinde ölçülülük ilkesi gereği, öncelikle şifreyi olay yerinde çözmek gerekmektedir.[726] Bu kapsamda, arama ve kopyalama tedbirinin uygulanması sırasında, bilişim siteminde mevcut olan bir şifrenin varlığı sebebiyle sisteme girilemeyebilir. Böyle bir durumda, öncelikle şifrenin arama ve kopyalama tedbirlerinin uygulanması esnasında çözülmeye çaba sarf edilmelidir. Eğer bu şekilde şifre çözülebiliyorsa, elkoyma işlemine başvurmak yerinde olmayacaktır. Üzerinde çalışılmasına rağmen şifre çözülemeyip sisteme giriş sağlanamamış ise, elkoyma tedbiri uygulama alanı bulacaktır.[727]

Ölçülülük ilkesi gereği her ne kadar bilişim sistemlerinde elkoyma tedbirine başvurulabilmesi için, şartların mevcut olması aranmakta ise de, elkoyma işlemi için bilişim sistemlerindeki şifrenin çözülememesi koşulunun aranması her zaman doğru bir bakış açısı değildir.[728] Şöyle ki, sistemdeki verilere ulaşmak için bilişim sistemini çalışır hale getirmek ve işletim sistemini açmak gerekmemektedir. Söz konusu bilişim sistemindeki sabit disk fiziken sökülerek, içerisinde yer alan verilerin birebir kopyası oluşturulabilir.[729] Bilişim sistemlerinde şifrelenmiş veriye iki şekilde rastlanabilmektedir. Dosya şifrelenmesi ya da tüm disk şifrelenmesi (full disk encryption) şeklinde karşılaşılabilir. Dosyanın şifreli olması, gerekli kopyaların

[725] YAŞAR/DURSUN, s. 15.
[726] ÜNAL, s.114.
[727] YAŞAR/DURSUN, ss.14-15.
[728] BAŞLAR, Ceza yargılamasında elektronik delil, s.171.
[729] BAŞLAR, Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri, s 91; AYDOĞAN, s. 112.

oluşturulmasına engel değildir. Şifreli dosyanın kopyası alınabilir ve çözüm adli bilişim laboratuvarında yapılabilir. Fakat tüm disk şifrelemesinde, kopyanın alınabilmesi için şifrenin çözülmesi gereklidir ki, bu işlem uzun süre süre alabilir. Bu sebeple, tüm disk şifrelemesinde elkoyma gereklidir.[730] Bununla birlikte, farklı işletim sistemlerinin kullanıcı şifresi ile sisteme ulaşılamadığı takdirde, belleğe erişimi engellemesi de mümkündür. Dolayısıyla, birebir kopyalamanın oluşturulamadığı, kullanıcı şifresi olmadan sistem belleğine erişilemediği ve bu şifrenin de, yetkili görevlilere verilmediği hallerde, elkoyma işlemi yapılması gerekmektedir.[731]

Elkoyma tedbirinin uygulanmasından sonra şifrenin çözümünün yapılması ve kopyalama işleminin gerçekleştirilmesi halinde elkonulan araçlar, gecikme olmaksızın iade edilmelidir. Her ne kadar kanun koyucu tarafından madde metninde sınırlayıcı bir süre belirtilmemiş ise de, işlemlerin makul bir sürede tamamlanması gerekmektedir.[732]

b.2. Gizlenmiş bilgilere ulaşılamamış olması

Elkoyma tedbirinin uygulanması için öngörülen ikinci durum ise, arama ve kopyalama tedbiri icrasında birtakım gizlenmiş bilgilere ulaşılamaması halidir. Bu bağlamda, arama işlemi sırasında, bazı verilerin bilişim sistemi içerisinde gizlenmiş olduğu kanısına varılabilir. Böyle bir durumda, yine elkoyma işlemi uygulama alanı bulacaktır. Zira sistem içerisindeki gizli bilgilere ulaşılamaması sebebiyle, sistem üzerinde detaylı bir inceleme yapılması gerekmektedir.[733] Bu bağlamda gizlenmiş olan verilere erişilmesi, uzun süre alabilir ve bu verilere ulaşılabilmesi için bazı özel programlar gerekebilir. Örneğin, bazı veri gizleme veya gömme tekniklerine (stegonagrafi gibi) başvurulması gerekebilir.[734]

Şüpheli kişinin pek tabi bilişim sistemlerindeki suçla ilgili elektronik delili, veri gizlemek için tasarlanmış bazı bilgisayar programları vasıtasıyla gizlemesi ya da silmesi muhtemeldir. Bu durumda, söz konusu gizlenmiş ya da silinmiş bilgilere olay yerinde

[730] DEĞİRMENCİ, Bilgisayarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbirinde(CMK m. 134), 7145 sayılı kanunla yapılan değişikliklerin değerlendirilmesi, s.152.
[731] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, ss. 367-368.
[732] BAŞLAR, s. 172.
[733] YAŞAR/DURSUN, s.15
[734] DEĞİRMENCİ, Bilgisayarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbirinde(CMK m. 134), 7145 sayılı kanunla yapılan değişikliklerin değerlendirilmesi, s.152.

ulaşılamaması halinde, elkoyma tedbirine başvurulabilecektir. Bu hususa ilişkin olarak, madde metninde "silinmiş" bilgilere yer verilmemiş ise de, maddede geçen "gizlenmiş" bilgiler, "silinmiş" bilgileri de içine alacak şekilde, geniş yorumlanmalıdır.[735] Gizlenmiş bilgilere ulaşılamaması durumunda ise, gizleme değişik biçimlerde olabilir. Burada önemli olan nokta, olay yerindeki imkânlar ile gizlenmiş bilgilere erişilememesidir. Görevli adli bilişim uzmanı, aslında var olmayan verilerin gizlenmiş olabileceğini düşünebilir. Böylesi bir durumda, şüphelinin verileri gizlediği veya sildiği sanılıyor ve birtakım teknik işlemlerle bu verilerin geri getirilebileceği ya da ortaya çıkartılabileceği düşünülüyorsa, el koyma işlemi gerçekleştirilmelidir.[736]

b.3. İşlemin uzun sürecek olması

CMK m.134, 31.07.2018 tarihinde Resmi Gazete'de yayımlanan 25.07.2018 tarihli ve 7145 sayılı Kanunun 16.maddesiyle değişikliğe uğramıştır. Değişiklik ile "işlemin uzun sürecek olması" ihtimali madde metnine eklenmiş olup, bu durumda çözümün yapılabilmesi ve gerekli kopyanın alınabilmesi amacıyla bilişim sistemine elkoyma imkânı tanınmıştır. Değişikliğin gerekçe kısmında, işlemin uzun sürecek olması ibaresindeki işlem kavramının, "kopyalama işlemi" olduğu belirtilmiştir. Söz konusu madde değişikliğe uğramadan önce, istisna olması gereken elkoyma işlemine uygulamada sıklıkla başvurulmaktaydı. Bu duruma gerekçe olarak ise; yeterli uzman bulunmaması, araç ve gereçlerin mevcut olmaması,[737] aranan verilerin büyüklüğü ve şifrelenmesi durumunda zaman alacak olması, arama işleminin gerçekleştiği yerdeki

[735] BAŞLAR, Ceza yargılamasında elektronik delil, s.171; DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s. 370; ORTA, s. 222; ÜNAL, s.115.
[736] AKTAŞ, s. 233.
[737] Yargıtay bir kararında bu durumu "…*CMK'nın 134. maddesi, dijital medyaların önce mahallinde incelenmesini bilgisayar programlarına veya kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde ise bilgisayarlara el konulmasını öngörmektedir. Bu hüküm uygulamada bazı sıkıntılara yol açmaktadır. Zira, bilgisayarda yerinde inceleme yapılması çoğu kez mümkün ve sıhhatli olmayıp, teknik yetersizliklerden dolayı imaj da alınamamaktadır. Dijital delillerin hukuka uygun yöntemlerle elde edildiğinin kabul edilebilmesi bakımından bu nokta önemlidir. Ceza muhakemesinde deliller kanuna uygun olmalı ve kanuna uygun yöntemlerle elde edilmelidir. Adil yargılanmanın sağlanabilmesi, soruşturma ve kovuşturma aşamalarında toplanan bulguların delil değeri taşıyabilmesi için, şüpheli veya sanıktan elde edilen dijital verilerin, yasa ile sınırları belirlenmiş teknik gerekliliklere uygun olarak toplanması ve sonucunda yargılama makamlarına eksiksiz, bozulmamış halde sunulması gerekmektedir. Yasa koyucunun, CMK'nın 134. maddesini ayrıntılı olarak düzenlemesinin amacı da budur. Dijital delillere harici müdahalenin teknik olarak mümkün olması, çoğu zaman kim tarafından hangi tarihte müdahale yapıldığının da belirlenememesi karşısında, güvenli bir şekilde el konulup incelenebilmesi için mahallinde imaj alındıktan sonra orijinal medyanın şüpheliye bırakılması gerekmekte ise de bu şart soruşturma yapan kolluk personelinin teknik yetersizliği, ekipman yokluğu, ortamın incelemeye elverişli olmaması gibi nedenlerle yerine getirilememektedir...*" şeklinde belirtmiştir. Yargıtay 16. Ceza dairesi Karar Tarihi :10.10.2019 tarihli kararı E. 2019 / 2637, K. :2019 / 5904

kişileri rahatsız etmeme isteği, veri bütünlüğünü sağlayacak olan ekipmanın arama yapılacak yerde bulunmaması ve ortamın adli bilişim uygulaması bakımından steril olmaması gibi haklı yanları bulunan nedenler ileri sürülmekteydi.[738]

Günümüzde, kişisel amaçlı kullanılan ve kolluğun olay yerine gittiğinde üzerinde tedbir uygulayacağı, 12 TB sınırına ulaşmış bir veya birden fazla disk ile karşılaşması mümkündür. Disk boyutu 12 TB olan, sabit diskin kopyalanma ortalama süresi minimum 24 saattir. Bu disklerde bozuk sektörlerin (bad sector) bulunması halinde, bozuk sektörlerin oranına bağlı olarak verilen süreler katlayarak artabilmekte ve 12 TB bir diskin adli kopyalanma süresi bir hafta bile alabilmektedir. Ayrıca, elektrik kesintisinin yaşandığı durumlarda, adli kopyalama baştan başlamakta ve kopyalama süresini artırabilmektedir. Görevliler, olay yerine birden fazla adli kopyalama cihazı (disk duplicator) götürse dahi, bir diskin adli kopyası ancak bir cihaz ile alınabilmektedir. "*Bir örnek vermek gerekirse 12 TB kapasiteli bir diskin bulunduğu olay yerine, 6 adli kopyalama cihazı ve personeli götürülse bile, adli kopyalama yine 24 saat sürecektir. Ancak 2 TB kapasiteli 6 diskin olduğu olay yerinde, 6 adli kopyalama cihazı aynı anda çalıştırılarak 4 saatte kopyalama yapılabilecektir."* Bu durumda kolluğun, adli kopyalama için gerekli yazılım ve donanımları yanlarında mevcut olsa bile, adli kopyalamanın süresi fazla uzun sürebilir.[739]

Adli kopyalamanın uzun sürmesi olasılığına dayanan elkoyma durumunda da, olay yerine giden görevliler tarafından öncelikle adli kopyalamanın uzun sürüp sürmeyeceği hususunda değerlendirme yapılmalı, kopyalama yapılacak aygıt ve kapasiteleri belirlendikten sonra elkoyma tutanağına neden adli kopya alınmasının uzun süreceği, gerekçeleriyle birlikte yazılmalıdır.[740]

İşlemin uzun süreceği kararı ölçülülük ilkesine uygun olarak verilmeli ve bu karar da cumhuriyet savcısı/mahkeme tarafından denetlenmelidir. Bu şekilde, bilişim sistemine el konulmaması, kişinin kullanımına engel oluşturmamış olur. Zira hükmün düzenleme

[738] GÖKSOY, ss.168-169.
[739] DEĞİRMENCİ, Bilgisayarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbirinde(CMK m. 134), 7145 sayılı kanunla yapılan değişikliklerin değerlendirilmesi, ss. 152-153.
[740] DEĞİRMENCİ, Bilgisayarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbirinde(CMK m. 134), 7145 sayılı kanunla yapılan değişikliklerin değerlendirilmesi, s.154.

amaçlarından biri verilere ulaşılması mümkün olması halinde elkoymayıp, kişilere mağduriyet yaşatmamaktır.[741]DEĞİRMENCİ, elkoyma tedbirine başvurulması noktasında kopyalama işlemleri için, sabit disk veya katı hal diskinde kaç GB ya da TB verinin kopyalanması ile ilgili olarak, minimum gerekli sürelerin yer verildiği bir cetvelin ilgili idari düzenleyici işlemlerde belirtilerek, bu sürelerin aşılması halinde elkoyma işleminin yapılmasına yönelik bir düzenleme hazırlanmasının olası suiistimalleri engelleyebileceğini ifade etmiştir.[742]

Bunların yanı sıra, bilişim sisteminde arama ve kopyalama tedbirlerinin uygulanması sırasında tedbiri uygulayan görevlilerin, bilişim sisteminde soruşturmaya ilişkin suçla bağlantılı veriyi saptayamaması halinde, verilen tedbir kararı konusuz kalmış olacaktır.[743]

[741] GÖKSOY, s. 167.
[742] DEĞİRMENCİ, Bilgisayarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbirinde(CMK m. 134), 7145 sayılı kanunla yapılan değişikliklerin değerlendirilmesi, s.155.
[743] YAŞAR/DURSUN, s.14.

IV. TEDBİRİN UYGULANMASI ve TEDBİR SONUCUNDA TOPLANAN DELİLLERE İLİŞKİN DEĞERLENDİRME

A. TEDBİRİN UYGULANMASI

Adli bilişim yönteminin temel amaçlarından biri, arama, kopyalama veya elkoyma tedbirlerinin uygulanması esnasında veri bütünlüğünün sağlanmasıdır. Çalışma konumuz olan CMK m.134'ün icrasında da daha önce ayrıntılı olarak açıkladığımız üzere, elektronik delillerin elde edilmesi aşamalarına uygun bir şekilde gerçekleştirilmesi, hem delilin hukuki geçerliliği hem de kabul edilebilirliği bakımından önem arz etmektedir.[744]

1. Arama ve Kopyalama

Öncelikle CMK m. 134/1 hükmü gereği, daha önce belirtmiş olduğumuz koşulların varlığı halinde, şüphelinin kullandığı araçlarda arama işlemi ile, suçla ilgili elektronik delilin varlığı araştırılacaktır. Bu hüküm çerçevesinde, bilişim sisteminde yapılacak arama işlemi adli bilişim kurallarına uygun bir şekilde gerçekleştirilmeli ve delillerin zarar görmemesi sağlanmalıdır.[745] Üzerinde arama yapılacak sistemde yazma engelleme sisteminin kurulması ile, bu şekilde verilerin değişime uğrama tehlikesinin önüne geçilebilir.[746] Arama işlemine ilişkin hukukumuzda arama faaliyetinin, gerekli aşamalarının kim tarafından, ne şekilde yerine getirileceğine ilişkin bir hüküm bulunmamaktadır.[747] Uygulamada soruşturma görevlileri, kendi iyi niyetleri ile görevini düzgün yapma isteğiyle hareket etmektedir. Fakat yapılması gereken bir işlemin yapılmaması durumunda söz konusu işlemin neden yapılmadığı sorulacak olunursa, buna ilişkin yasal bir dayanak maalesef bulunmamaktadır.[748] Bu eksikliğin giderilmesi gerekmektedir.

Maddeye göre, delil niteliğinde elektronik kayıtların tespit edilmesi halinde, bu kayıtların imajı oluşturulmalı ve bu kayıtlar çözülerek metin haline çevrilmelidir. Burada, metin haline dönüştürülen sistem kayıtları, delil mahiyetinde olduğu düşünülen

[744] GÖKSOY, s.168.
[745] BAŞLAR, Ceza yargılamasında elektronik delil, s.170.
[746] GÖKSOY, s. 169.
[747] GÖKSOY, s.168.
[748] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s.552.

ve kopyası alınan kayıtlardır. Her ne kadar maddede, kopyalama ve yedekleme ifadeleri kullanılsa da, daha öncede bahsettiğimiz gibi uygulamada buna imaj alma denir. Kural olarak, arama ve imaj alma işlemi bilgisayarın olduğu yerde yapılacak ve görevliler bilgisayar veya veri depolama aygıtlarının aslına el koymayacaklardır.[749] Arama işlemi ile bilgisayar içerisinde söz konusu suçun ispatı için "veri" araması yapılmaktadır. CMK. m.119 gereği, CMK. m.134'teki koruma tedbirinin uygulanması kararında genel nitelikteki arama kararlarında belirtilen, aramanın nedenini oluşturan fiilin, bilgisayarında veya diğer araçlarında arama yapılacak kişinin, bilgisayarın ve diğer araçların aranacağı konutun veya işyerinde aranacak aygıtların (bilgisayar, bilgisayar programları, çıkarılabilir donanımlar vb.) ve ayrıca aranan verinin ne olduğu, gibi unsurlara yer verilmesi gerekmektedir. Bu sebeple, kararda belirtilen hususların dışına çıkılarak, örneğin şüpheliye ait evrak ya da çeşitli belgelerin aranması, hukuka aykırılık teşkil edecektir.[750]

Gerçekleştirilen arama işleminde, arama konusu suçla bağlantısı olmayan, şüpheli ya da sanığın özel hayatına yönelik verilerin, bilerek ve istenerek açılması halinde, kanun hükmünün yerine getirilmesi yani hukuka uygunluk nedeni sınırı kasten aşılmış olur. Bu bakımdan, özel hayatın gizliliği suçu (TCK m. 134) veya devamı maddelerinde yer verilen verilerin ele geçirilmesine yönelik suçların oluşması söz konusu olacaktır. Ancak arama işlemi sırasında gerekli araştırma yapılmadan suçla bağlantılı olduğu düşüncesiyle hareket edilerek, şüpheli ve/veya sanığın verilerinin açılması halinde, sınır taksirle aşılmış olacaktır. Bu durumda, özel hayatın gizliliği suçu veya devamı maddelerinde yer alan verilerin ele geçirilmesine yönelik suçların taksire işlenmesine yer verilmediği için, bu suçlar oluşmayacaktır.[751] Bununla birlikte, CMK 118. maddede, genel aramalara ilişkin bir zaman sınırlaması bulunmaktadır. Fakat bilişim sisteminde arama ve elkoyma tedbirine ilişkin bu şekilde bir sınırlama mevcut değildir. Bu bakımdan, gün içerisinde herhangi bir anda gece vakti de dahil, bilişim sistemlerinde arama yapılabilir.[752]

[749] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s.549.
[750] YAŞAR/DURSUN, ss.22-23.
[751] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.221.
[752] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.222.

Tüm bunlarla birlikte, arama kopyalama işlemleri sonrası tutanak tutulur. Bu tutanakta, alınan kararda bulunması gereken hususların, yapılan çalışmaların ve incelemeyi yapan uzmanın belirtilmesi gerekmektedir. Soruşturma konusu olan suçla ilgili bilişim sisteminde herhangi bir delile ulaşılamaması halinde, bu durum tutanağa bağlanılarak tedbirin uygulanmasına son verilir. Aranılan delillere ulaşılması halindeyse kayıtlardan bir kopya çıkartılıp, metin haline dönüştürülecektir. Şifre çözümü veya gizlenmiş veriler ya da işlemin uzun sürmesi söz konusuysa, verilere ulaşılabilmesi için elkoyma işlemi geçekleştirilecektir. Soruşturma makamınca elde edilen deliller yeterli görülürse kamu davası açılacak, yeterli görülmez ise kovuşturmaya yer olmadığı kararı verilecektir. [753]

2. El Koyma

CMK m. 134'ün ikinci fıkrasında, birinci fıkranın istisnasını oluşturacak şekilde elkoyma tedbiri düzenlenmiştir. Bu hükme göre, yalnızca "*Şifrenin çözülememesinden dolayı girilememesi*" veya "*gizlenmiş bilgilere ulaşılamaması*" ve yapılan değişiklikle madde metnine eklenen üçüncü bir hal olarak "*işlemin uzun sürecek olması*" durumlarında, çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için el koyma işlemi yapılabileceği açık bir şekilde düzenlenmişken, ülkemizde bu hüküm istisnai bir hal[754] olarak değil de kuralmış gibi uygulanmaktadır.[755]

Uygulamada, CMK m. 134 hükmü uyarınca arama ve kopyalama işleminin icrasında, bilişim sisteminde bulunan verilerin değerlendirilmesi hususunda görevliler, hemen hemen her olay karşısında sistemin şifrelenmiş olması veya gizlenmiş verilerin bulunduğunu ileri sürerek, doğrudan bilgisayara elkoyma işlemini gerçekleştirmektedir. Dolayısıyla, kanunun açık hükmüne riayet edilmeyerek işlemi gerçekleştirmektedirler. Ancak bu hususa ilişkin hazırlanan tutanaklarda, hangi tür şifrelerin bulunduğu veya ne tür gizlenmiş verilerin bulunduğu ve bu engellere ilişkin uzman kişinin neden etkisiz kaldığına dair bir kayıta yer verilmemektedir. Böyle bir tutanak, gerçekle bir alakası olamadığı gibi, denetlenebilir bir yanı da bulunmamaktadır. Dolayısıyla söz konusu işlemin uygulanış şekli hukuka aykırı bir delil elde etme yöntemi olmakla beraber, bu şekilde edinilen deliller de yasak delil niteliğinde olmasından ötürü yargılama

[753] ÇAKIR/KILIÇ, Adli bilişim ve elektronik deliller, ss.527-528.
[754] YENİSEY/NUHOĞLU, s.416.
[755] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s. 550.

aşamalarında kullanılmamalıdır.[756] Bu hususta öncelikle, ölçülülük ilkesi gereğince şifre önce bilgisayarın bulunduğu yerde çözülmeye çalışılmalı, çözümlemenin başarılamaması halinde aygıtlara el konulmalıdır. Çözümün yapılması veya kopyanın alınması halinde aygıtlar hemen iade edilmelidir.

Tedbirin uygulanmasında, kolluktan kaynaklanan problemlerin çözümü için, CMK ve ilgili yönetmelikte usul kurallarına uyulmaması halinde, görevlilere caydırıcı bir takım yaptırımlar öngörülmesi gerekmektedir.[757] Ayrıca belirtmek gerekir ki, kolluk görevlileri tarafından koşullara uymadan yapılan, arama, kopyalama ve el koyma koruma tedbirinin icrası, hem hukuka aykırı delil elde edilmesi sonucu doğuracak, hem de TCK m. 243'de düzenlenen bilişim sistemine girme veya kalma suçunun hukuka uygunluk[758] nedenlerinden olan, CMK 134'ün sınırının aşılmasına sebep olacaktır. Bu halde, TCK 243. madde gereği görevlilerin cezai sorumluluğun gündeme gelmesi söz konusu olabilir. Ancak bu durumun ayrıntılı olarak irdelenmesi ve somut olaya göre değerlendirilmesi gerekir.[759]

Uygulamada karşılaşılan bir diğer durum ise, imaj alma ve arama işlemlerinin daha sonra laboratuvarda yapılmasıdır.[760] Kopyalama işleminin olay yerinde yapılmamasına gerekçe olarak, genelde personel veya teknik ekipman yetersizliği gösterilmektedir. Ancak belirtmek gerekir ki, el koyma işleminden sonra gerçekleştirilecek imaj alma işlemi, verilerin güvenliği ve bütünlüğü bakımından sakıncalı bir hal oluşturabilmektedir.[761] Bu hususta, kolluk tarafından geliştirilen ve genellikle uygulanmakta olan adımlar şu şekildedir. Tedbirin icra edileceği yere gidilerek, şüphelinin kullandığı araçların usulüne uygun olarak fişten çıkarılması ve bunların özel yapılmış torbalara konulması,[762] sonrasında torbaların mühürlenerek yapılan işlemin tutanağa geçirilmesi, merkeze götürülen aygıtlar üzerinde inceleme yapılacağı zaman ise, duruma göre şüpheli ve/veya müdafinin inceleme yapılacak ortama çağrılması ve

[756] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s. 550.
[757] ÖZEN/ÖZOCAK, s.68.
[758] CENTEL/ZAFER, Ceza muhakemesi hukuku, s.414.
[759] APİŞ, ss.79-81.
[760] GÖKSOY, s.168.
[761] Bilgisayarların başka yere transfer edilmesi sonucunda, sistemdeki bütün verilerin yedeklemesinin yapılması suretiyle elde edilen deliller, CMK.217/2. maddesi gereğince hukuka aykırı delil olabilecektir. YAŞAR/DURSUN, s. 26.
[762] CMK m.134'e göre alınan karara istinaden şüphelinin kullandığı aygıt, özel yapılmış torbalara yerleştirilmekte ve ağzı mühürlenmektedir. Bu sırada gerçekleştirilen tüm işlemler de tutanağa kaydedilmelidir. DÜLGER, Adli Bilişim & Ülkemizde Uygulanması, s.553.

kendisine ayrılmış özel bir yerden, adli bilişim uzmanlarının laboratuvarda gerçekleştirdiği işlemleri ekrandan izleme imkânı verilmesidir. Görüleceği üzere, belirtilen adımlara ilişkin elde edilen delillerin, delil gözetim zinciri bakımından bir kısmının yasal dayanağı bulunmadan gerçekleştirilmesi, elektronik delillerin hukuka uygun olarak elde edilip edilmediği hususunda şüphe oluşturmaktadır.[763]

Olay yerindeki bilişim sistemi hakkında kanun koyucu, canlı sistemler veya kapalı sistemler olması hususunda bir ayrımda bulunmamıştır. Her iki halde de, elkoyma işlemi sırasında sistemdeki verilere olay mahallinde yedekleme yapılması gerekmektedir. Canlı sistemlerin yani çalışır haldeki bilişim sistemlerinin bulunması halinde, nasıl bir yol izleneceği belirli değildir. Teknik açıdan canlı sistemler üzerindeki veriler, bilişim sisteminin kapatılması ya da enerji kaynağının kesilmesiyle yok olabilir. Böyle bir durumda adli kolluğun, elindeki malzemeyle sistem çalışır durumda iken, bir yedeğinin alınması daha doğru olacaktır.[764]

Bununla birlikte daha önce de belirttiğimiz gibi, 7145 sayılı kanun ile gelen değişikliğin uygulamada ihtiyaç olduğu düşünülse de, CMK m.134'te yer alan tedbirleri uygulayan kolluk görevlileri her durumda "*işlem uzun sürecek*" demek suretiyle elkoyma işlemine başvurmamalıdır. [765] Ancak günümüzde bir eve gidildiğinde bile bilgisayar kütüğü niteliğinde bir sürü harici bellek, DVD vb. araçlar bulunmaktadır. Hatta örgütlü suçlarda elde edilebilecek araçların sayısı çok daha fazla olabilecektir. CMK 134'ncü maddesine bakıldığında, bunların tamamının yedeklenmesi gerekir. Bu durumda, kopyalama işlemi uzun zaman alacağı gibi, bu kadar verinin incelenmesinde de güçlükler yaşanacaktır.[766]

Bilişim sisteminde arama, kopyalama ve elkoyma tedbirinin tatbik edilmesinde, kolluğun olay yerinde adli kopya alabildiği durumlarda adli kopyalama yapılmadan önce, adli kopya cihazlarının hash değeri hesaplanmalı, söz konusu rapor şüpheliye veya müdafine verilmeli, adli kopya tamamlandıktan sonra alınan adli kopyanın hash değeri de hesaplanmalı ve hash değerleri karşılaştırılmalıdır. Bu değerin aynı olması durumunda, şüphelinin veya müdafinin elindeki kopya ile bilirkişi incelemesine

[763] GÖKSOY, s.168.
[764] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s. 244.
[765] GÖKSOY, s. 167.
[766] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s. 244.

gönderilecek kopyanın da aynı olduğu hususunda şüphe giderilecektir. Ancak kopyalama işleminin uzun sürecek olması sebebiyle elkoyma yapıldığında, elkonulan bilişim sistemlerinin hash değerleri hesaplanmadan ve şüpheliye/müdafine hash değerleri verilmeden elkoymanın yapıldığı durumda, "*elkoyma işleminin Suç Eşyası Yönetmeliğinin 5'inci maddesinin dördüncü fıkrasına göre açıldığında yeniden kullanılamayacak derecede bozulan delil torbalarına konması ve şüphelinin veya müdafiinin mührünün üzerine konması gereklidir. Benzer şekilde söz konusu bilişim sistem araçlarının bilirkişiye veya kolluğa incelenmek üzere sevki için açılması gerektiğinde de, şüphelinin veya müdafiinin bulunması aranmalıdır*." [767] GÖKSOY'a göre, elektronik delillerin bütünlüğünün korunması ve güvenirliğinin sağlanması için işlemin uzun süreceğine karar verilmesi halinde dahi elkonulan materyallerdeki verilerin hash değeri oluşturulmalı, nasıl ki yedek alındığı durumda, oluşturulan yedekten bir kopya şüpheli veya müdafine verilmesi gerekiyorsa, materyale elkonulmadan da hash değeri bilgisi şüpheli veya müdafiine verilmelidir.[768]

CMK m. 134/2 gereği, olay yerinde kopyanın alınamadığı durumları tek tek açıklamak gerekirse; bunların ilki, bilişim sisteminin şifrelenmiş olması durumunda bilişim sisteminde kopyalama yapılamamasıdır. Bu durumda, delilin güvenliğini sağlamak için delil paketine konulacak ve delil paketi şüpheli ya da müdafi huzurunda mühürlenecektir. Gizlenmiş verilerin söz konusu olması durumunda, adli kopya almak mümkündür. Zaten adli kopya alınmadan gizlenmiş verinin ortaya çıkarılması neredeyse olanaksızdır. Bu ihtimalde, elkoyma işlemi aslında gereksizdir ve olay yerinde adli kopya alınarak, şüpheliye veya müdafiine verilmesi gerekmektedir. Adli kopyalamanın uzun sürmesi halinde ise elkoymada zaten adli kopya alınmamaktadır. DEĞİRMENCİ' ye göre bu durumda, CMK m.134/3 ve m.134/4 bakımından bazı sorunlar ortaya çıkmaktadır. Zira madde de134/3' te elkoyma işlemi sırasında, sistemdeki veriler

[767] DEĞİRMENCİ, Bilgisayarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbirinde(CMK m. 134), 7145 sayılı kanunla yapılan değişikliklerin değerlendirilmesi, s.153.
[768] GÖKSOY, s. 167.

yedeklenecek denmektedir; fakat zaten elkoymanın sebebi, verilerin yedeklenememesi ya da bunun uzun sürmesidir. Bu halde, iki fıkra arasında bir tutarsızlık mevcuttur.[769]

Bununla birlikte, CMK m. 134/3 gereği elkoyma işlemi esnasında, sistemdeki tüm verilerin yedeklemesi[770] yapılmalıdır. Bunun sebebi ise, sistemdeki bir takım bilgilerin kaybolmasının önüne geçilerek, şüphelinin mağdur olmamasını temin etmektir. Nitekim kanun koyucu tarafından elkoyma esnasında yedekleme yapılması, şüpheli isteğine ya da görevlilerin inisiyatifine bırakılmamış,[771] zorunlu olarak yedekleme yapılması gerektiği maddede ifade edilmiştir.[772] Ayrıca bu hüküm, bilişim sisteminde arama ve elkoyma işlemlerinin uygulanması esnasında, materyaller üzerinde gerçekleşebilecek olası bir müdahaleye karşı fayda sağlamaktadır.[773] Madde metninde geçen "elkoyma işlemi sırasında" ibaresi, "incelemeye başlamadan önce" olarak kabul edilmelidir. Çünkü inceleme esnasında verilerin; zarar görmesi, değişmesi veya yok olması söz konusu olabilir.[774] Ayrıca, ilgili hükümde sadece, "bilgisayar veya bilgisayar kütüklerinde elkoyma işlemi sırasında" yedekleme yapılacağı ifade edilerek, bilgisayar programlarının bu kapsamda yedekleme işlemine dahil edilmediği görülmektedir. Bilgisayar programları çoğunlukla sabit diskte yer aldığından için, sistemdeki bütün verilerin yedeklenmesi halinde bu işleme bilgisayar programı da dahil olacaktır.[775] Ancak bu programların bilgisayar dışındaki veri taşıma aygıtlarında da yer alabileceği gözetilerek, yaşanabilecek olası problemlerin önüne geçilmesi amacıyla, bu hususun düzenlenmesi gerekir.[776]

---

[769] DEĞİRMENCİ, Bilgisayarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbirinde(CMK m. 134), 7145 sayılı kanunla yapılan değişikliklerin değerlendirilmesi, s.153.

[770] *"İmaj alma, bilgisayarlardaki verilerin birebir kopyasının alınmasını ifade etmektedir. Yedekleme, sistemin çökmesi veya doğal afet risklerine karşı sistemi kurtarmak için verilerin kopyasının çıkarılmasıdır. Teknik detaylara inildiğinde ise ikisi arasında farklılık mevcuttur. İmaj alma adli bilişim süreci içerisinde uygulanan teknik bir işlemdir. Yedekleme ise özellikle şirketlerin, ağ sunucularının sistem çökmesi riskine karşılık bilgilerinin kaybolmaması için aldıkları bir önlemdir."* ÜNAL, s.119.

[771] 21.2.2014 tarihli 6524 sayılı yasanın 11. maddesiyle arama tedbiri doğrultusunda çıkarılan yedeğin bir kopyasının şüpheliye ya da vekiline verilmesi zorunludur. DÜLGER, Adli Bilişim & Ülkemizde Uygulanması, s.549.

[772] GÜNEYSU, s.116.

[773] BAŞLAR, Ceza yargılamasında elektronik delil, s.174; SEVİMLİ, s. 997.

[774] BAŞLAR, Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri, s.92.

[775] ÜNAL, s.119.

[776] BAŞLAR, Ceza yargılamasında elektronik delil, ss.174-175.

İmaj alma işlemi sonucunda, CMK m. 134/4 gereği bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilmesi zorunlu olup, bu hususun tutanağa bağlanarak ilgili kişilerce imzalanması gerekir. Buradaki amaç, elde edilen elektronik veriler üzerinde olası hukuka aykırılık iddialarının önüne geçilmek istenmesidir. Bu bağlamda, kopyanın şüpheliye ya da vekiline verilmesi işlemi olay yerinde yerine getirilmelidir. Bu durumun olay yerinde gerçekleştirilememesi halinde ise, adli bilişim inceleme çalışmalarından önce bu husus yerine getirilmelidir.[777] Nitekim Yargıtay bir kararında, "sanıkların ev veya iş yerlerinde yapılan aramalarda hard disk, bilgisayar kasası, CD ve DVD gibi dijital medyalara, arama mahallinde imaj alınmadan, ilgilisine bir kopyası verilmeden ve kanuna uygun gerekçesi de tutanağa yazılmadan el konulması ve bu şekilde elde edilen delillerin sanık bakımından hükme esas alınmasının CMK'nın 134 maddesine aykırı olduğunu" belirtmiştir.[778]

Ayrıca oluşturulan hash değeri de tutanağa geçirilmelidir. Bu hususa ilişkin olarak maddede açıklayıcı hüküm bulunmamasına rağmen, delil bütünlüğünün sağlanması ve daha sonra materyale herhangi bir delil eklendiğine dair iddiaların önüne geçilmesi için, hash değerinin de ilgili tutanağa geçirilerek ilgili kişiye verilmesi gerekmektedir.[779] Bunun yanı sıra, kopyalamada kullanılan diskler, temiz diskler olmalıdır. Bu diskler daha önce kullanılmış ise, mutlaka kullanım öncesi temizlenmeli ve bu hususun, tutanağa geçirilmesi gerekmektedir. Zira diskte daha önce kaydedilmiş olan verilerle, kaydedilip silinmiş ancak veri olarak disk üzerinde kalmış olan eski veriler, elektronik delillerin özgünlüğüne zarar verebilir. Kopyalama sonrasında içerisinde elektronik delil

[777] BAŞLAR, Ceza yargılamasında elektronik delil, s.175.

[778] "*…aramayı gerçekleştiren kişilerce elkoyma işlemine geçildiği sırada sistemdeki verilerin yedeklemesi (imaj-adli kopya) yapılmadan ve yedekten bir kopya alınıp şüpheli veya vekiline verilmeden, ya da yukarıda yazılı nedenlerden dolayı mahalde yedekleme ve yedekten kopya verme olanağının bulunmadığının objektif olarak kabulünde zorunluluk bulunan hallerde, aramayı yapan kolluk birimince dijital delillere müdahaleyi önleyecek şekilde, seri numaraları tutanağa yazılmak suretiyle usulüne uygun olarak zapt edilip mühürlenmeden, şüpheli veya müdafiinin istemesi halinde nezaret etme ve denetleme imkanı sağlanarak inceleme mahalline kadar eşlik etmesi sağlanmadan ve bu yerde şüpheli veya müdafiinin hazır bulunmasına imkan verildikten sonra mümkün olan en kısa süre içinde mühür açılıp, dijital medyanın derhal imajının alınarak ilgilisine de imajlardan bir kopya ve orijinal medya teslim edilmeden, 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 imaj alma işleminin bu sırada yapılması yoluna gidilmeden inceleme yapılması halinde arama ve elkoyma işleminin kanuna ve hukuka uygunluğundan bahsetmek mümkün olmadığı gibi bu yolla elde edilen delillerin de hukuka uygunluğu tartışılır hale gelecek ve yargılama makamınca hükme esas alınması mümkün olamayacaktır...*" Yargıtay 16. Ceza Dairesi, 21.09.2017 tarihli, E. 2015 / 2056, K 2017 / 5023.

[779] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s. 363.

barındıran disklerin, internete bağlı olmayan bilgisayarda tutulmasına dikkat edilmelidir. Çünkü internet aracılığı ile bilgisayara erişim sağlanması suretiyle, delillerin istenmeyen kişilerin eline geçmesi ya da tahribata uğraması mümkündür.[780]

Bununla birlikte, bilişim sisteminde arama ve elkoyma işlemlerinde, hazır bulunacaklara ilişkin herhangi bir hüküm bulunmamaktadır. Bu hususta aygıt bizzat şüpheliye ait olmasa bile, gerçekleştirilecek arama işlemi için şüphelinin, aracın sahibinin veya temsilcilerinin hazır bulundurulmasına olanak sağlanmalıdır. Bu şekilde, delillere ilişkin değişiklik yapıldığı iddiası da bertaraf edilebilir.[781] Ayrıca madde metninde geçen "vekil" ibaresinin "şüpheliyi temsil eden kişi" şeklinde geniş yorumlanması gerekmektedir. Şüpheli ve müdafiinin yanı sıra, suça sürüklenen çocuklar açısından anne-baba ya da evde bulunan diğer yasal temsilcilerin de bu kapsama dâhil olabileceği ileri sürülmektedir.[782]

CMK m. 134/5 uyarınca tedbire maruz kalan kişilerin, bilişim sistemlerini kullanmaya devam edebilmeleri sağlanmıştır. Tutanağa geçirilmiş olan ve yedeklenen verilerin değiştirilmesi, bu aşamadan sonra önem taşımamaktadır. Uygulamada, kolluk görevlileri üç kopya çıkartıp, birini şüpheliye vererek, birini incelemek, üçüncüsünü ise ileri safhada ortaya çıkabilecek uyuşmazlıkların giderilmesi için ayrı bir birimde koruma altına aldığı görülmektedir.[783] Konu ilişkin olarak, şüpheli ya da vekili tarafından herhangi bir sebeple kopyanın alınmak istenmemesi durumu söz konusu olabilir. Bu halde, elkoymayı gerçekleştiren kişilerce durum bir tutanakla tespit edilip, yedeklenen veriyi almaktan kaçınan şüpheli ya da vekiline imzalatılmalıdır. Şüpheli veya vekil tutanağı imzalamaktan kaçınır ise, bu husus tutanağa geçirilmelidir. Ardından, şüpheli veya vekilin almak istemediği kopya, istenildiği zaman alınabileceği bir şekilde adli emanete konulmalıdır.[784]

Bunların yanı sıra, CMK'nin 134/1'de belirtilen, "kopyası alınan bilgisayar kayıtların çözülerek metin haline getirilmesi" ve CMK'nin 134/5'de yer verilen, "sistemdeki

[780] TANRIKULU, ss.365-366.
[781] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.219.
[782] ÜNAL, s.123.
[783] YENİSEY/NUHOĞLU, s.417.
[784] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, ss.245-246

verilerin tamamı veya bir kısmının kopyasının alındığı hallerde kopyası alınan verilerin kâğıda yazdırılması" hususunun sebebi, elektronik delilin kaybolma tehlikesinin önüne geçilmek istenmesidir. Ancak elektronik delilin kaybolmaması için, birden fazla kopya oluşturularak, bunların zarar görmeyeceği bir şekilde koruması da sağlanabilir.[785] Her ne kadar arama esnasında kopyalanacak olan verilerin metin haline getirilmesi bir zorunluluk ise de, bu durum büyük hacimli dosyalar söz konusu olduğunda pratikte bir takım sorunlar oluşturmaktadır.[786] Zira çok sayıda sayfa çıktısı[787] tutabilecek elektronik verinin kâğıda yazdırılması pek uygulanabilir değildir. Bununla birlikte, bu miktardaki metin haline getirilmiş verinin adli makamlarca incelenebilmesi de mümkün olmamaktadır.[788] Öğretide bir görüşe göre, "kayıtların çözülerek metin haline getirilmesi" ibaresinden, aranan ve elkoyulan verilerin bilirkişi tarafından raporlanması anlaşılmalıdır.[789] Başka bir görüş, bu hususu "*Delil olabilecek veriler metin haline getirilemeyecek ölçüde büyük olduğu takdirde tıpkı adli bilişimdeki belgeleme basamağında olduğu gibi bir veri saklama birimine kaydedilmeli ve delil olabilecek verilerin özetleri metin haline getirilmelidir*." şeklinde ifade etmiştir.[790] Bir başka görüş ise, bu durumun suçla ilgili olan kısma ait veriler şeklinde anlaşılması gerektiğini ifade etmiştir.[791] Bu hususun tam olarak çözüme kavuşması için, söz konusu madde metninin uygun bir şekilde kaleme alınarak düzenlenmesi gerekmektedir.[792]

Çalışma konumuz bakımından, AÖAY'nin 17. maddesinin 1,2 ve 4'ncü fıkralarına bakıldığında, CMK m. 134 ile benzer nitelikte olduğu, 3 ve 5'nci fıkralarının ise CMK m. 134'e ilişkin eksiklikleri gidermeye yönelik düzenlemeler olduğu görülmektedir. AÖAY 17/5 düzenlemesi, CMK m 134/5 ile aynı şekilde başlamış, ancak devamı ile uygulamada tartışmalara neden olan bir hususa yer verilmiştir. Şöyle ki, CMK 134/5' te "*Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin*

[785] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s. 378.
[786] YENİSEY/NUHOĞLU, s.416; BAŞLAR, Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri, s.93; HEKİM H. ve BAŞIBÜYÜK O., 2013. Siber suçlar ve Türkiye'nin siber güvenlik politikaları. Uluslararası Güvenlik ve Terörizm Dergisi, 4(2), ss. 135-158. s. 152; AYDOĞAN, s. 22.
[787] BAŞTÜRK, s.29
[788]ÖZBEK/DOĞAN/BACAKSIZ, s.266; BALLI Y., "CMK 134. Madde Düzeltilmelidir" http://www.dijitaldeliller.com/cmk134.htm [30.06.2020].
[789] TANRIKULU, s.362.
[790] ÜNAL, s. 113.
[791] ÖZBEK/DOĞAN/BACAKSIZ, s.266.
[792] BAŞLAR, Ceza yargılamasında elektronik delil, s.177.

tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır." şeklindeki uygulamada tartışmalara yol açan bu hüküm, yönetmeliğin 17/5 te "*Kopyası alınan verilerin mahiyeti hakkında tutanak tanzim edilir ve ilgililer tarafından imza altına alınır. Bu tutanağın bir sureti de ilgiliye verilir*" şeklinde açıklanmıştır. Bu hüküm ile kopyalanan verilerin ne olduğu içerik olarak değil, liste bazında adlarının neler olduğu belirtilecektir. Bu bağlamda, kopyalanan verilerin liste olarak adlarının neler olduğu şeklinde raporlanması, yedekleme işleminde kullanılan bilgisayar programları ile listelenebilir. Böylelikle, CMK m. 134/5 doğrultusunda yığınla doküman çıktısı almaya gerek kalmamıştır.[793]

Bunlara ilaveten, uygulamada sıkıntıya sebep olabilecek bir takım önemli hususların kanun koyucu tarafından kaleme alınarak düzenlenmesi gerekmektedir. Zira içerisinde yasa dışı içerik bulunan medyanın bir kopyasının şüpheliye verilip verilmeyeceği, belirsiz konumdadır.[794] Öğretide bir görüş, içerisinde çocuk pornografisi ve başkasına ait kredi kartı bilgileri gibi, kişisel veri barındırabilecek depolama aygıtının imajının bir örneğinin şüpheliye verilmesi halinde, suç işlenmesinin önünü açabileceği, maddede bununla ilgili bir istisnaya yer verilmemesinin eksiklik olduğunu ifade etmektedir. Uygulamada böyle bir durum ile karşılaşılması halinde, bu tür içeriklere CMK m. 123 hükmüne göre suç eşyasına el koyma tedbiri doğrultusunda el konulmakta ve şüpheli ya da vekiline verilmemektedir. Bu görüşe göre, müdafi görevini yapan avukatın suç işlemeyeceği ve sır saklama yükümlülüğü göz önünde tutularak, bu görevi icra edenlere imajın yedeği verilmelidir. Bu şekilde, hem yeni suçların işlenmesinin önüne geçilmiş olacak, hem de delillerin doğruluğu hakkında şüphe oluşmayacaktır.[795] Buna karşılık başka bir görüş ise, devlet sırrı veya çocuk pornosuna ilişkin suç teşkil eden veriler aranmakta ise bunların elde tutulmasının dahi suç oluşturması sebebiyle, şüpheli veya müdafine bir kopya verilmemesini, onlara verilecek olan kopyanın da adli emanette tutulması gerektiğini öne sürmüştür.[796] Ayrıyeten bu görüş, söz konusu iade hususunun

[793] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.234.
[794] BAŞLAR, Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri, s.92; HEKİM/BAŞIBÜYÜK, s. 152.
[795] DÜLGER, Bilişim suçları ve internet iletişim hukuku, ss.550-551.
[796] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s. 241.

sözleşmeye aykırılık teşkil ettiğini ileri sürmektedir. Şöyle ki, "*sözleşmenin 19'ncu maddesinin 3'üncü fıkrasında ilk iki fıkrası kapsamında(yani arama ve uzaktan aramayla) erişilen verilere el konulması için gerekli olabilecek yasama tedbirlerinin ve diğer tedbirlerin iç hukukta düzenlenmesi zorunluluğu getirirken, bu zorunluluklardan birisi olarak da(m.19/3-d)erişim sağlanan bilgisayar sistemindeki verilerin erişilemez hale getirilmesi ya da kaldırılması olarak belirlenmiştir…. Bu durumda bulundurulması suç teşkil eden çocuk pornosu, devlet sırrı gibi veriler hakkında sözleşmenin 19'uncu maddesi kapsamında işlem yapılması halinde erişimin engellenmesi ya da bilişim sisteminden kaldırılması gerekmektedir*". Velhasıl, sözleşmeye taraf olmamız nedeniyle, CMK m. 134 hükmündeki teslim zorunluluğunun bulundurulması, suç teşkil edilen veriler yönünden değiştirilmesi gerekmektedir.[797] Belirsiz olan bir başka husus ise, imajı oluşturulan verilerin; ne şekilde, hangi aygıtlar üzerinde ve ne kadar süre ile saklanacağıdır. Bu hususların da kanun koyucu tarafından ayrıntılı bir şekilde kaleme alınması gerekmektedir.[798]

Öğretide bir görüş, yedekleme için gerekli olan depolama aygıtının şüpheliden istediği, bu durumunda hukuka aykırı olduğunu öne sürmektedir. Zira el koyma tedbirinin gerçekleştirilmesiyle, yedekleme soruşturmanın güvenilirliği ve adil yargılanma hakkı bakımından önemlidir. Adil yargılanma hakkının ihlal edilmemesi için, görünüşte ve içerikte tüm soruşturma ve yargılama işlemlerinin, tarafsız ve hukuka uygun bir şekilde gerçekleşmesi gerekir.[799] Ayrıyeten unutulmamalıdır ki, her ne kadar hash değeri delilin değişmediğini ortaya koymakta ise de, imaj alımı öncesinde, üçüncü kişiler tarafından zararlı yazılımlar kullanılarak veya doğrudan bir müdahale ile bilişim sistemine uydurma deliller konulabilir. Bu bağlamda, elde edildiği iddia edilen delillerin, sanıkla bağı ve bunların gerçekliğinin de araştırılması gerekmektedir.[800]

---

[797] Bu görüşe göre ileride delillerin değiştirildiği iddiasıyla karşılaşılmaması için, söz konusu kopyanın hash değerinin şüpheli veya müdafine tutanakla verilmeli, ancak verilmesi gereken kopyanın ise kapalı ve mühürlü bir zarf içerisinde yargılama süreci kesin hükümle bitinceye kadar adli emanette muhafaza edilmesi gerekmektedir. Şüpheli veya vekilinin delilleri incelemek istemesi halinde savunma hakkı gereği, buna imkân sağlanmalıdır. ERDOĞAN Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, ss.246-247.

[798] BAŞLAR, Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri, ss.92-93; HEKİM/BAŞIBÜYÜK, s. 152.

[799] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s.551.

[800] ERDOĞAN Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s. 244.

Bunların yanı sıra, gerçeğin ortaya çıkmasını engellemek için, suç delillerinin yok edilmesi, gizlenmesi, değiştirilmesi veya bozulması durumlarında, TCK m. 281' de düzenlenen suç işlenmiş olacaktır.[801]

B. TEDBİR SONUCUNDA TOPLANAN DELİLLERE İLİŞKİN DEĞERLENDİRME

1. Elde Edilen Verilerin Yok Edilmesi

CMK m.134 hükmünün uygulanması sonucunda elde edilen veriler, soruşturma aşamasında delil olarak kullanılacaktır. Buna ilaveten, soruşturma aşamasında şüpheli hakkında kovuşturmaya yer olmadığı kararı verilebileceği gibi, yapılan muhakeme sonucunda beraat kararı verilmesi de mümkündür. Bu bağlamda, ilk derece mahkemesince verilen kararlar veya denetim muhakemesi (temyiz ve istinaf) tarafından verilen kararlar söz konusu olabilir.[802] Bu hallerde, elde edilen verilere ne olacağı hususuna ilişkin bir bilgiye, CMK m. 134'te yer verilmemiştir. Öğretide bir görüş, söz konusu tedbirin ihlal edebileceği kişilik hakları düşünüldüğünde, ayrıca tedbir neticesinde elde edilen verilerin, kovuşturmaya yer olmadığı kararı, ya da beraat kararı verilip kesinleştiğinde, ceza dosyasından ve tüm kayıtlardan çıkartılarak yok edilmesine ilişkin hususların kaleme alınması gerektiğini ifade etmiştir.[803]

Öğretide bir başka görüş, benzer mahiyette bir düzenleme olan telekominasyon yoluyla yapılan iletişimin denetlenmesi hükmünde, yasa koyucu tarafından elde edilen verilerin yok edilmesi hususuna CMK' nun 137. maddesinin 3. fıkrasında yer verdiği ve CMK m.134'ün aynı kanunun 135. maddede yer alan; iletişimin dinleme, kayda alınması tedbirine göre temel hak ve özgürlüklere ve özel hayatın gizliliğine daha ağır müdahale oluşturduğunu ifade etmiştir.[804] Bu bağlamda, temel hak ve özgürlüklerin korunması amacıyla kanunda bu verileri yok etmeye yönelik bir hüküm bulunmamasına rağmen,

[801] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s. 252.
[802] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s.555.
[803] CENTEL/ZAFER, Ceza muhakemesi hukuku el kitabı. s.375.
[804] DEĞİRMENCİ, s.380; BAŞTÜRK, s.31.

kıyas yoluna başvurulması çözüm olarak önerilmektedir.[805] Bir diğer görüşe göre ise, CMK m. 134'ün uygulanması karar verilen veri taşıyan aygıtlarının, failin mahkûmiyeti kararı halinde iadesine veya suç unsuru barındırması halinde, TCK m. 54 gereği müsaderesine karar verilebilir. Soruşturmaya yer olmadığı ya da beraat halinde ise, şüpheli/sanığa iadesine karar verilebileceğini ifade etmiştir. Bu görüşe göre, çalışma konumuz olan tedbirin uygulanmasıyla veri taşıyan aygıtlardan alınan imajın, ne olacağı da belirsizdir. Bazı mahkemeler veya savcılıklar, emniyete veya emniyet birimlerine bunların imhasına yönelik karar veya emir göndermektedirler. Ancak bu imajlar, bir koruma tedbiri sonucunda oluşturulmuştur. İmajların alınması temel hak ve özgürlüklerin kısıtlanması ile gerçekleşmesinden dolayı, bunların imhası da adil yargılanma hakkının, temel hak ve özgürlüklerin kısıtlanması sonucunu doğurabilir. Bu bağlamda, bu imajların imhasının kim veya kimler tarafından, ne zaman, nerede, ne şekilde yapılacağını belirten teknik boyutunu içeren, ana hatlarıyla yasal bir düzenlemeye gereksinim vardır. Zira mahkemeler veya savcılıkların emirleriyle yapılması, Anayasanın 13. Ve TCK' nun 257. maddelerinin ihlal edilmesi anlamına gelmektedir.[806]

2. Tesadüfen Elde Edilen Deliller

CMK m.138/1[807] hükmünde yer verilen tesadüfen elde edilen delil hususu genel bir düzenleme olup, çalışma konumuz olan CMK m. 134 bakımından da geçerlidir.[808] Bir arama kararı kapsamında başvurulacak tedbir, iddia olunan suç şüphesiyle bağlantılı olmalıdır. Bu bağlamda, CMK m.134 çerçevesinde uygulanan tedbir de, sadece tedbire konu olan suç bakımından geçerli olacaktır.[809]

---

[805] Bu hükme göre, *"135 inci maddeye göre verilen kararın uygulanması sırasında şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi ya da aynı maddenin birinci fıkrasına göre hâkim onayının alınamaması halinde, bunun uygulanmasına Cumhuriyet savcısı tarafından derhâl son verilir. Bu durumda, yapılan tespit veya dinlemeye ilişkin kayıtlar Cumhuriyet savcısının denetimi altında en geç on gün içinde yok edilerek, durum bir tutanakla tespit edilir."* ÜNAL, s. 127.

[806] DÜLGER, Bilişim suçları ve internet iletişim hukuku, s. 556.

[807] CMK m. 138/1'e göre "*Arama veya el koyma koruma tedbirlerinin uygulanması sırasında, yapılmakta olan soruşturma veya kovuşturmayla ilgisi olmayan ancak, diğer bir suçun işlendiği şüphesini uyandırabilecek bir delil elde edilirse; bu delil muhafaza altına alınır ve durum Cumhuriyet Savcılığına derhâl bildirilir."*

[808] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.449; TANRIKULU, s.467; YAŞAR/DURSUN, ss.22-23; ÜNAL, s. 125.

[809] ÜNAL, s. 123.

Bilişim sisteminde usulüne uygun olarak yapılan arama sırasında,[810] soruşturma konusu suç dışında başka bir suçun işlendiğine dair bulgular tespit edilmesi halinde,[811] bu durumun hukuka aykırılık teşkil etmemesi için saptanan delillere dayanarak aramanın genişletilmemesi ve mevcut durumun cumhuriyet savcılığına bildirilmesi gerekmektedir.[812] Başka bir deyişle, soruşturmaya konu suç bahane edilerek, başkaca bir suçla alakalı delil araştırması yoluna gidilmesi, buna dayanılarak aramanın genişletilmesi, sınırlı ve ölçülü bir uygulama yapılmaması hukuka aykırılıklara neden oluşturabilecektir. *"Örneğin*; *uyuşturucu kaçakçılığı ile ilgili bir belge bilgisayardan elde edilmişse ve bu belge içerisinde rüşvet suçuna ilişkin deliller yer alıyorsa rüşvet suçu bakımından elde edilen delil dikkate alınabilir. Buna dayanarak arama genişletilmemeli ve derhal Cumhuriyet savcılığına bildirilmelidir*." [813] Bu bağlamda, bilişim sistemi üzerinde yapılan arama sırasında kolluk ya da adli bilişim uzmanı, yalnızca soruşturmaya konu elektronik delilleri toplamayı amaçlamalıdır. Aksi bir tutumla hareket edilerek, arama işlemi sırasında, arama kararında gösterilen suç ile ilgisi olmayan elektronik delilin elde edilmesi ve bu delilin tesadüfen elde edilen delil olarak kabul edilmesi, yapılan aramayı keşif aramasına dönüştürecektir. Bu durumda, kişilerin temel hak ve özgürlüklerine yönelik ciddi bir müdahale söz konusu olacaktır.[814]

3. Tedbire Karşı Başvuru Yolları

CMK m.134 hükmünde düzenlenen tedbir kararlarına karşı, özel bir itiraz yolu öngörülmemiştir.[815] Bu bakımdan CMK'nun 267. maddesi çerçevesinde itiraz söz konusu olacaktır.[816] Bu şekilde, bir bilişim sisteminde arama, kopyalama ve elkoyma tedbirlerine yönelik cumhuriyet savcısı tarafından verilen kararlara karşı, bir başvuru yolu mevcut değildir. Ancak CMK m 134'e karşı başvuru yolları, Cumhuriyet savcısının kararlarının hakim onayına sunulması, ya da hakim tarafından doğrudan tedbire istinaden bir karar verilmesi durumlarında söz konusu olacaktır.[817] Şöyle ki, genel bir düzenleme olan CMK m.267 hükmü ile hakim kararlarına karşı itiraz

[810] TANRIKULU, s 468.
[811] BAŞLAR, Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri, s.94
[812] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.449.
[813] ÜNAL, ss.125-126.
[814] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.450.
[815] ÖZEN/BAŞTÜRK, s. 162.
[816] TANRIKULU, ss.462-463.
[817] GÖKSOY, s. 172.

edilebilmesi mümkündür.[818] Fakat CMK m.267'de belirtilen mahkeme kararlarına karşı itiraz yolu, CMK m.134 bakımından söz konusu olmayacaktır. Zira CMK m.267'de mahkeme kararına karşı itiraza başvurulabilmek için, ilgili maddenin bu yönde bir açık düzenlemeyi barındırması gerekmektedir. CMK m.134 hükmünde ise mahkeme kararlarına karşı itiraz durumuna yer verilmediği için, CMK m.267'ye dayanarak mahkeme kararlarına itiraz edilmesi mümkün değildir. Dolayısıyla, söz konusu tedbire kovuşturma aşamasında mahkeme tarafından verilen kararlar bakımından itiraz kanun yolu kapalı olup bu karar, hükümle birlikte istinaf kanun yolunda değerlendirilecektir.[819] Bu halde, sulh ceza hakimliğince verilen tedbir kararlarına karşı CMK' nın 267'nci maddesine göre itiraz mümkündür.[820]

CMK m. 134/2 doğrultusunda, bir bilişim sistemine el koyma işleminin tatbik edilmesinde, elkoyma tedbirine ilişkin özel bir itiraz yolu olan CMK m.127/4 dikkate alınacaktır. Bu hükme göre, şüpheli ya da bilişim sisteminin zilyedi olan kişinin, hakimden her zaman elkoymanın gerekli olup olmadığına dair bir karar vermesini talep etme olanağı söz konusudur.[821]

Bilişim sisteminde elkoyma tedbiri, diğer koruma tedbirlerinde olduğu gibi geçici mahiyettedir. Bu sebeple, genel elkoymaya ilişkin olan, CMK. m.131 hükmü uygulanmalıdır. Buna göre; şüpheliye, sanığa veya üçüncü kişilere ait elkonulmuş materyallerin içerisinde yer alan verilerin incelenmesi sonucunda, soruşturma veya kovuşturma konusu suçla bağlantılı verilerin kopyalanması ile birlikte, elkonulan araçların resen veya istem üzerine geri verilmesine, Cumhuriyet savcısı, hakim veya mahkeme tarafından her zaman karar verilebilir.[822] CMK m. 131 uyarınca, el konulan aracın iadesi için talebin reddedilmesi halinde ise, CMK m. 267 kapsamında verilen karara itiraz edilebilecektir.[823] Bu durum, kanun gerekçesinde geçici elkoyma işlemine

[818] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.381; CENTEL ZAFER Ceza muhakemesi hukuku, s.413; BAŞTÜRK, s.32.
[819] DEĞİRMENCİ, Bilgisayarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbirinde(CMK m. 134), 7145 sayılı kanunla yapılan değişikliklerin değerlendirilmesi, s.154.
[820] ORTA, s.223.
[821] GÖKSOY, s.173. DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.381; TANRIKULU, s.464; ÜNAL, s.128.
[822] TANRIKULU, ss.463.464; YAŞAR/DURSUN, ss.27-28.
[823] CENTEL/ZAFER, Ceza muhakemesi hukuku el kitabı s.374; GÖKSOY, s.172. DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.381.

karşı itiraz yolunun söz konusu olabileceği şeklinde belirtmiştir.[824] İtiraz, 35. madde[825] usulüne göre yapılmaktadır.[826] Bu durumda, koruma tedbiri olmasından dolayı, CMK m.35/2 uyarınca hazır bulunmayan ilgiliye tebliğ olunmaz. Ancak itiraz kararı veren mercie, ilgili kararın öğrenildiği günden itibaren yedi gün içinde itiraz edilebilecektir.[827] Bunun yanı sıra, CMK m134/2' e göre elkoyma tedbiri kapsamında, bilişim sisteminde elkoyma işlemine ilişkin olarak aramanın kısa sürede gerçekleştirilebilecek olması veya kolay bir şekilde elde edilebilecek olan verilerin yerlerinin bilinmesine karşın bilişim sistemine elkonulması durumunda, bu elkoyma işlemine itiraz etmek mümkündür.[828]

Tüm bunlarla birlikte, arama kararlarına karşı tek başına istinaf kanun yoluna başvurma ya da temyiz edilmesi söz konusu değilse de, asıl karar ile beraberinde istinafa ya da temyize konu edilebilecektir. CMK 272/2 ve 287. maddeleri gereğince hükümden önce verilip hükme esas teşkil eden, ya da başkaca kanun yolu öngörülmemiş olan mahkeme kararları, hükümle beraber istinafa konu olabilir ya da temyiz edilebilir.[829]

4. Tedbir Nedeniyle Tazminat

CMK m.141 hükmünde açıkça belirtilmese de, çalışma konumuz olan tedbir aramanın özel bir görünümü olmasından dolayı, bu tedbir maddi ve manevi tazminat davasına konu olabilecektir.[830] Koruma tedbirlerinin uygulanması sonucunda, temel hak ve özgürlüklere karşı müdahaleler söz konusu olabilir. Bir koruma tedbiri olan, CMK m.134 hükmündeki tedbirlerin uygulanmasıyla da, kişilerin temel hak ve özgürlükler üzerinde olumsuz sonuçlar meydana gelmesi mümkündür.[831] CMK m.141/1 hükmü, bir bilişim sisteminde arama, kopyalama ve elkoyma tedbiri söz konusu olduğunda, sadece "i ve j" bentleri açısından uygulanabilecektir.[832] Bu bentlere göre; *"(i) Hakkındaki*

[824] ÖZEN/BAŞTÜRK, s.162.
[825] Madde 35 – (1) İlgili tarafın yüzüne karşı verilen karar kendisine açıklanır ve isterse kararın bir örneği de verilir.
(2) Koruma tedbirlerine ilişkin olanlar hariç, aleyhine kanun yoluna başvurulabilecek hâkim veya mahkeme kararları, hazır bulunamayan ilgilisine tebliğ olunur.
(3) İlgili taraf serbest olmayan bir kişi veya tutuklu ise tebliğ edilen karar, kendisine okunup anlatılır.
[826] GÖKSOY s.172.
[827] CENTEL/ZAFER, Ceza muhakemesi hukuku el kitabı s.374; DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.381.
[828] TANRIKULU, s.464.
[829] GÖKSOY, s. 173; TANRIKULU, s.464.
[830] GÖKSOY, s.173; ÖZBEK/DOĞAN/BACAKSIZ, s.266; ORTA, s.221; ÜNAL, ss.129-130.
[831] BAŞLAR, Ceza yargılamasında elektronik delil, s.182.
[832] YAŞAR/DURSUN, s.30.

arama kararı ölçüsüz bir şekilde gerçekleştirilen, j) Eşyasına veya diğer malvarlığı değerlerine, koşulları oluşmadığı halde elkonulan veya korunması için gerekli tedbirler alınmayan ya da eşyası veya diğer malvarlığı değerleri amaç dışı kullanılan veya zamanında geri verilmeyen, Kişiler, maddî ve manevî her türlü zararlarını, Devletten isteyebilirler" şeklinde düzenlenmesiyle arama ve elkoyma koruma tedbirlerinin uygulanması bakımından tazminat istemine yer verilmektedir. Bu nedenle, bilgisayarda, bilgisayar programlarında ve kütüklerinde, arama, kopyalama ve elkoyma koruma tedbiri, genel arama ve elkoyma tedbirinin özel bir şekli olmasından dolayı, şartların gerçekleşmesi halinde CMK m. 141 uygulanabilmektedir.

Çalışma konumuz bakımından bir bilişim sistemi üzerinde arama ve el koyma tedbiri, orantılı bir şekilde tatbik edilmelidir.[833] Arama kararında belirtilen suçla bağlantılı verilerin dışında bir takım verilerin aranması, arama kararının dışına çıkılması, aramanın sınırlandırılması mümkünken, sınırlandırılması gibi durumlarda orantısızlık söz konusu olacaktır. Ayrıca CMK m.134/2'de yer alan durumların oluşmadığı halde el koyma kararı verilmesi, tazminat sebebi olacaktır.[834] CMK m.141'de arama kararının kendisinin hukuka aykırı olması durumu yer almamaktadır. Bu bakımdan, haksız yere verilen arama kararları sebebiyle açılacak olan tazminat davaları, idare hukuku kurallarına göre idare mahkemesinde açılacaktır.[835]

CMK' nun 141. maddesi uyarınca tazminat talebi maddi olabileceği gibi, manevi tazminatta söz konusu olabilir. ÜNAL'a göre tedbir neticesinde "*elde edilen delillerin birer kişisel veri olduğu düşünülürse bunun, hukuka aykırı uygulamalarla öğrenilmesi şüpheliyi manevi olarak etkileyebilecektir. Bu tedbirin uygulanması sonucunda manevi bir zarar oluşmuşsa manevi tazminat yoluna da gidilebilecektir*."[836]

Tüm bunlarla birlikte, el konulan araçların geri verilmesine ilişkin şartlar oluşmasına rağmen bu araçların geri verilmemesi,[837] bu araçların amaç dışı kullanılması ve

[833] BAŞLAR, Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri, s.94.
[834] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, ss.381-382.
[835] ERDOĞAN, Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri, s.225.
[836] ÜNAL, s. 131.
[837] YAŞAR/DURSUN, s. 30.

korunması için gerekli tedbirler alınmaması halinde, bu maddeye göre tazminat isteminde bulunulması mümkündür.[838]

[838] DEĞİRMENCİ, Ceza muhakemesinde sayısal(Dijital) delil, s.382.

V. SONUÇ

Ceza muhakemesinin amacı maddi gerçeğin ortaya çıkarılmasıdır. Bu bağlamda meydana gelen olay ve söz konusu olayı gerçekleştiren kişi arasındaki ilişkinin ispatlanması gerekmektedir. Bu ilişkinin ispatı deliller ile sağlanmaktadır. Günümüzde bilgisayar ve benzeri elektronik aygıtlar birçok değişik suçun işlenmesinde kullanılmakta veya suça ilişkin bilgiler bu cihazlar üzerinden elde edilebilmektedir. Suç olgusunun teknolojiyi bu şekilde araç olarak kullanması sonucunda, ispat vasıtası olarak artık elektronik delillere başvurulmaktadır. Dolayısıyla yaşantımızın her alanına dâhil olan bilişim sistemleri, suçun tespitinde ve ispatında bir çeşit veri deposu haline gelmiştir. Çalışma konumuz olan CMK m. 134 hükmü, genel arama ve elkoyma tedbirlerinin özel bir şekli olarak, ceza muhakemesinde elektronik delil elde edilmesi hususunu düzenlenmektedir. Bu şekilde ayrı bir düzenlemeye yer verilmesinin sebebi, elektronik delillerin klasik delillerden farklı olarak, tespit edilmesinde, incelenmesinde, toplanmasında uzmanlık gerektiren bir alan olmasıdır. Bununla birlikte bilişim sisteminde bulunan kişisel bilgilere ilişkin genel arama ve el koyma tedbirinin uygulanması halinde, temel hak ve özgürlüklere karşı ciddi bir müdahale söz konusu olacaktır. Bunun için CMK m. 134 hükmü düzenlenerek, tedbire başvurulması noktasında genel arama ve elkoyma tedbirlerine nispeten daha ağır şartlar aranarak temel hak ve özgürlüklere müdahale edilmesi zorlaştırılmıştır.

Suçu aydınlatmak için bilişim sistemi üzerinde yapılan incelemeler sırasında gerek mevzuatımızdan kaynaklanan sebeplerle gerekse uygulamada birçok problemle karşılaşılmaktadır. Bu sorunların çözümü için kanun koyucu, Ceza Muhakemesi Kanunu'nun 134. maddesini hem gelişen teknolojinin ihtiyaçlarına cevap verebilecek şekilde hem de kişilerin özel hayatlarının gizliliğini güvence altına alarak, temel hak özgürlüklere karşı oranlılık ilkesine uygun şekilde yeniden kaleme almalıdır.

Çalışmamızda, elektronik delillerin ceza muhakemesinde kullanılması için hem fiziksel delillerde bulunması gereken özellikleri barındırması hem de elektronik delillerin niteliği, hassas yapısından ötürü geçerli sayılabilmesi açısından gerekli olan hususlara yer verilmiştir. Bu kapsamda öğretide farklı ayrım ve tanımlar olmakla birlikte adli

bilişim prensiplerine uyulmalıdır. Adli bilişime ilişkin her gün gelişen teknolojiyi göz önünde tutarak, uluslararası standartlara uygun hareket edilmeli ve işlem yapılmalıdır. Elektronik delillerin bütünlüğünün sağlanması için teknik bir takım işlemlerin yerine getirilmesi gerekir. Bu bağlamda imaj alma, hash değerinin hesaplanması, zaman damgasının tespiti ve koruma zincirinin sağlanması gerekmektedir. Çalışma konumuz tedbirler bakımından da, bu hususların yer aldığı ve adli bilişim standartlarının açıkça ortaya konulduğu bir düzenlemenin yasal zemine kavuşturulması yerinde olacaktır.

CMK m. 134 hükmünün madde başlığı ve metni, yalnızca sınırlı olarak sayılan araçların tedbirin konusu olacağı izlenimini yaratmaktadır. Oysaki bilişim sistemi özelliğine sahip, ancak uygulamada bu şekilde tanımlanmayan cep telefonları ve elektronik veri barındıran birçok aygıt CMK'nın 134'ncü hükmüne göre arama ve elkoyma tedbirine tabi tutulmalıdır. Bu yaklaşım maddi gerçeğin ortaya çıkarılması adına yerinde olacaktır. Dolayısıyla söz konusu tedbirin, bilişim sistemi ve benzeri araçları da kapsayacak şekilde yorumlanması gerekir. Aksi bir tutum temel hak ve özgürlükler bakımından ihlale sebep olabilecektir.

CMK' nun 134. hükmünde eksik düzenlenen veya hiç düzenlenmeyen bazı hususlar Adli ve Önleme Arama Yönetmeliğinin 17. maddesinde giderilmeye çalışılmış ise de yeterli olmamıştır. Özellikle bilişim suçlarının etkin şekilde soruşturulmasında, temel hak ve özgürlükleri doğrudan ilgilendiren bir yasa hükmündeki eksikliklerin, yönetmelikle giderilmeye çalışılması da doğru değildir. Ayrıca ilgili yönetmelik, tedbirin konusunu nispeten genişletse de maddenin tekrar edilmesi söz konusudur. Bunun yerine işlemlere ilişkin ayrıntılar düzenlenmelidir. Söz konusu hüküm, teknolojideki ilerlemeye uygun hale getirilmeli, şüphelinin haklarını ve soruşturmanın doğru bir şekilde gerçekleştirilmesini garanti altına alacak teknik hususlar hükmün kapsamına alınmalıdır. Bunun yanı sıra bilişim sistemlerinden elde edilen veriler çözülerek metin haline getirilip, kâğıda yazdırılması gibi uygulamada anlam ifade etmeyen yaklaşımdan vazgeçilmelidir.

Taraf olduğumuz Avrupa Konseyi Siber Suç Sözleşmesi'nin arama ve elkoymaya ilişkin 19. maddesindeki düzenlemeyle, CMK'nun 134. maddesinde düzenlenen koruma tedbirlerinin uygunluk gösterdiği söylenebilirse de, anılan Sözleşmede yer alan suç unsuru ya da suç aracı olan verilerin erişilmez kılınması ve kopyaları alındıktan sonra

taşınması ya da silinmesine ilişkin hususlara CMK m.134'te yer verilmemiştir. Öyle ki CMK'nın 134. hükmünde bu tür verilerin şüpheliye iade edilmesine ilişkin açık ifade bulunması, sözleşme ile CMK arasında çelişkiye sebep olmaktadır. Bu eksikliğin giderilmesi gerekmektedir. Ayrıca öğretide, tedbir neticesinde elde edilen verilerin kovuşturmaya yer olmadığı kararı ya da beraat kararı verilip kesinleştiğinde, ceza dosyasından ve tüm kayıtlardan çıkartılarak yok edilmesine ilişkin hususların kaleme alınması gerektiği ve alınan imajlarında imhasının kim veya kimler tarafından, ne zaman, nerede ve ne şekilde yapılacağını belirten teknik boyutunun, ana hatlarıyla yasal bir düzenlemeye gereksinimi olduğu ifade edilmiştir.

Tedbirin uygulanmasına ilişkin karar veren adli makamlar, tedbir kararının verilmesinde belirtilen kuvvetli suç şüphesi ve başka suretle delil elde etme imkânının bulunmaması hali gibi hususlara dikkat etmeli, gerekli olmadığı takdirde kişilerin bu tedbirin uygulanmasıyla özel hayatına müdahale etmemelidir. Tedbire başvurulması hususunda "başka surette delil elde etme imkânı bulunmaması" şeklinde ifade edilen son çare prensibi, bilişim suçları söz konusu olduğunda istisnaya tabi tutulması, bu suçların doğası gereği genellikle ilk olarak suça konu bilişim sisteminde inceleme yapılması gereksinimden dolayı yerinde olacaktır.

Öğretide CMK'nun 134. hükmüne soruşturma aşamasında başvurulabileceğine ilişkin bir fikir ayrılığı yokken, kovuşturma aşamasında başvurulup başvurulmayacağına dair farklı görüşler mevcuttur. Kanaatimizce maddi gerçeğe ulaşılması için kovuşturma aşamasında da gerekiyorsa tedbire başvurulabilir. Ayrıca tedbirin uygulanacağı kişi bakımından söz konusu maddede sadece "şüphelinin kullandığı" şeklinde bir ifade olsa da, özellikle bilişim suçlarında şüpheli haricindeki kişiler içinde bilişim sisteminde inceleme yapılması gerekmektedir. Bu sebeple her ne kadar mağdur veya suçtan zarar görenin rızasıyla ve tedbir için öngörülen şartlar aranmadan, bilişim sisteminde gerekli inceleme yapılsa da madde metninde bu olasılıklar değerlendirilerek, yasal bir zemine kavuşturulmalıdır.

Tüm bunlarla birlikte tedbiri uygulayan kolluk görevlileri kanun hükmünde öngörülen usul kurallarını eksiksiz yerine getirmeli, kanundan doğan yetkilerini kötüye kullanmadan ya da yasayı dolanmak suretiyle bir takım uygulamalarda bulunmamadır. Bu hususta arama işleminin gerçekleştirilmesinde, imaj alınmasında ve elkoyma

tedbirinin uygulanmasında özen gösterilmelidir. Elkoyma için CMK m. 134 hükmünde gösterilen "şifrenin çözülememesinden dolayı girilememesi" veya "gizlenmiş bilgilere ulaşılamaması" ve "işlemin uzun sürecek olması" durumlarının varlığı, tedbiri uygulayan kolluk görevlileri tarafından doğru bir şekilde değerlendirilmedir. Özellikle hemen hemen her olay karşısında sistemin şifrelenmiş olması, gizlenmiş verilerin bulunduğunu ileri sürerek doğrudan bilgisayara elkoyma işlemi gerçekleştirilmekte ve bu hususa ilişkin hazırlanan tutanaklarda, hangi tür şifrelerin bulunduğu veya ne tür gizlenmiş verilerin bulunduğu ve bu engellere ilişkin uzman kişinin neden etkisiz kaldığına dair bir kayıta yer verilmemektedir. Öncelikle ölçülülük ilkesi gereğince, şifre ilk olarak bilgisayarın bulunduğu yerde çözülmeye çalışılmalı, çözümlemenin başarılamaması halinde aygıtlara el konulmalıdır. Yine tedbirleri uygulayan kolluk görevlileri her durumda "işlem uzun sürecek" demek suretiyle elkoyma işlemine başvurmamalıdır. Adli kopyalamanın uzun sürmesi olasılığına dayanan elkoyma hallerinde de olay yerine giden görevliler tarafından öncelikle adli kopyalamanın uzun sürüp sürmeyeceği hususunda değerlendirme yapılacak, kopyalama yapılacak aygıt ve kapasiteleri belirlendikten sonra elkoyma tutanağına, neden adli kopya alınmasının uzun süreceği gerekçeleriyle birlikte yer verilmelidir. Bu bağlamda öğretide ki bir görüş, elkoyma tedbirine başvurulması noktasında kopyalama işlemlerinde sabit disk veya katı hal diskinde kaç GB ya da TB verinin kopyalanması için minimum gerekli sürelerin yer verildiği bir cetvelin ilgili idari düzenleyici işlemlerde belirtilerek, bu sürelerin aşılması halinde, elkoyma işleminin yapılmasına yönelik bir düzenleme hazırlanmasının olası suiistimalleri engelleyebileceğini ifade etmiştir.

Uygulamada karşılaşılan, imaj alma ve arama işlemlerinin laboratuvarda yapılmasıdır. Kopyalama işleminin olay yerinde yapılmamasına gerekçe olarak genelde personel veya teknik ekipman yetersizliği gösterilmektedir. Ancak şunu belirtmek gerekir ki elkoyma işleminden sonra gerçekleştirilecek imaj alma işlemi, verilerin güvenliği ve bütünlüğü bakımından sakıncalı bir hal oluşturabilmektedir. Ayrıca kolluk görevlileri tarafından koşullara uymadan yapılan arama, kopyalama ve el koyma koruma tedbirinin uygulanması, hem hukuka aykırı delil elde edilmesi sonucu doğuracak hem de TCK m. 243'de düzenlenen bilişim sistemine girme veya kalma suçunun hukuka uygunluk nedenlerinden olan CMK m.134'ün sınırının aşılması sonucunu doğurabilir. Bu halde TCK 243. madde gereği, görevlilerin cezai sorumluluğunun gündeme gelmesi söz

konusu olabilir. Ancak bu durumun ayrıntılı olarak irdelenmesi ve somut olaya göre değerlendirilmesi gerekir.

KAYNAKÇA

Kitaplar

AKARSLAN H., 2015. *Bilişim suçları*. 2. Baskı. Ankara: Seçkin Yayıncılık.

AKBULUT B., 2017. *Bilişim alanında suçlar*. 2. Baskı. Ankara: Adalet Yayınevi.

APAYDIN C., 2017. *Bilişim suçları ve bilişim ceza hukuku*. İstanbul: Acar Matbaacılık.

ARICI H. Y., 2018. *Adli bilişim*. Ankara: Seçkin Yayıncılık.

BAŞLAR Y., 2016. *Ceza yargılamasında elektronik delil.* Ankara: Yetkin Yayınları.

BAYRAM L.(Ed.). 2008. *Ses görüntü ve data incelemeleri.* Ankara: Adalet Yayınevi

BIÇAK, V., 2018. *Ceza muhakemesi hukuku*. 4. Baskı. Ankara: Seçkin Yayıncılık.

BİRTEK F., 2017. *Ceza muhakemesinde delil ve ispat*. 2. Baskı Ankara: Adalet yayınevi

CENTEL, N./ZAFER, H., 2020. *Ceza muhakemesi hukuku el kitabı*. 6.Baskı. İstanbul: Beta

CENTEL, N./ZAFER, H., 2014. *Ceza muhakemesi hukuku*. 11. Baskı. İstanbul: Beta

ÇAKIR, H./KILIÇ, M. S.(Ed.). 2014. *Adli bilişim ve elektronik deliller*. Ankara: Seçkin Yayıncılık.

ÇAM A.R., 2015. *Adli kolluk ve bilişim*. İstanbul: On İki levha Yayıncılık.

DEĞİRMENCİ O., 2014. *Ceza muhakemesinde sayısal(Dijital) delil*. Seçkin Yayıncılık.

DOĞU, A.H., 2017. *Bilişim hukuku.* Bursa: Ekin Basım Yayın Dağıtım.

DÜLGER M. V., 2018. *Bilişim suçları ve internet iletişim hukuku.* 7. Baskı. Ankara: Seçkin Yayıncılık.

DÜLGER M. V., 2018. *Ceza hukuku, ceza muhakemesi hukuku ve bilişim hukuku uygulama çalışmaları*. Ankara: Seçkin Yayıncılık.

ERCAN İ., 2014. *Themıs ceza muhakemesi hukuku.* 8. Baskı. İstanbul: On iki levha Yayıncılık.

ERDOĞAN, Y., 2018. *Avrupa konseyi siber suçlar Sözleşmesi'nde yer alan koruma tedbirleri ve bu koruma tedbirlerin Türk hukukundaki yeri*. İstanbul: Legal.

ERDOĞAN Y., 2013. *Türk Ceza Kanunu'nda bilişim suçları(Avrupa konseyi siber suç sözleşmesi ve Yargıtay kararları ile)*. İstanbul: Legal Yayıncılık.

GÖKSOY R., 2019. *Ceza muhakemesinde dijital delillerin elde edilmesi ve güvenilirliğinin sağlanması.* Ankara: Seçkin Yayıncılık.

GÜNEYSU G. (Ed.). 2017. *Bilişim hukuku*. Eskişehir Anadolu Üniversitesi Yayınları.

GÜNŞEN İÇLİ T., 2019. *Kriminoloji.* 10. Baskı. Ankara: Seçkin Yayıncılık.

HENKOĞLU T., 2014. *Adli bilişim dijital delillerin elde edilmesi ve analizi.* 2. Baskı. İstanbul: Pusula yayıncılık.

IFRAH G., 2002. *Bilgisayar ne sayar: rakamların evrensel tarihi IX.* 2. Baskı. K. Dinçer (Çev.), Ankara: Tubitak Popüler Bilim Kitapları.

KAMIŞLIK, Ö., 08-11 Ocak 2008. *Ankara Barosu Uluslararası Hukuk Kurultayı Bilişim ve hukuk, "Bilişim Hukukunda Delillerin Toplanması" Cilt. 2, Ankara* Barosu Yayınları.

KARAGÜLMEZ A., 2014. *Bilişim suçları ve soruşturma kovuşturma evreleri.* 5. Baskı. Ankara: Seçkin Yayıncılık.

KESER BERBER L., 2004. *Adli bilişim(Computer Forensic).* Ankara: Yetkin Yayınları.

MANSON S., 2009. *Ankara Barosu Uluslararası Hukuk Kurultayı 2008: Bilişim ve Hukuk. Bilişim Hukukunda Delillerin Toplanması.* Cilt 2(8 Ocak - 11 Ocak 2008), Ankara Barosu Yayınları.

ORTA M., 2015. *Bilişim suçları ve elektronik delillerin toplanması muhafazası değerlendirilmesi sunulması(adli bilişim).* Ankara: Yetkin Yayınları.

ÖZBEK V. Ö./DOĞAN K./BACAKSIZ P., 2019. *Ceza muhakemesi hukuku temel bilgiler.* 10. Baskı. Ankara: Seçkin.

ÖZEN M./BAŞTÜRK İ., 2011. *Temel hak ve özgürlükler bağlamında bilişim-internet ve ceza hukuku.* Ankara: Adalet Yayınevi.

ÖZTÜRK B. (Ed), 2017. *Nazari ve uygulamalı ceza muhakemesi hukuku ders kitabı.* 11. Baskı. Ankara: Seçkin Yayınları.

ÖZTÜRK B./EKER KAZANCI B./SONER GÜLEÇ S., 2017. *Ceza muhakemesi hukukunda koruma tedbirleri.* 2. Baskı. Ankara: Seçkin Yayınları.

ŞAHİN C., 2020. *PROF. Dr. Mehmet emin artuk'a armağan*. Mahmut KOCA(Ed), Ankara: Seçkin Yayınları.

ŞAHİN C., 2005. *Ceza muhakemesi kanunu gazi şerhi.* Ankara: Seçkin Yayınları.

ŞAHİN C./GÖKTÜRK N., 2019. *Ceza muhakemesi hukuku.* 2. Baskı. Ankara: Seçkin Yayınları.

TANRIKULU C., 2014. *Ceza muhakemesi hukukunda bilişim sistemlerinde arama ve elkoyma.* Ankara: Adalet Yayınevi.

TAŞKIN Ş. C., 2008. *Bilişim suçları.* Bursa: Beta Yayınları.

TOROSLU N./FEYZİOĞLU, M., 2017. *Ceza muhakemesi hukuku.* 17. Baskı. Ankara: Savaş yayınevi.

ÜNVER Y./HAKERİ H., 2019. *Ceza muhakemesi hukuku.* 16. Baskı. Ankara: Adalet Yayınevi.

YENİDÜNYA A. C./DEĞİRMENCİ O., 2003. *Mukayeseli hukukta ve Türk hukukunda bilişim suçları.* İstanbul: Legal Yayıncılık.

YENİSEY F. (Ed.). 2018. *Ceza muhakemesi hukuku başvuru kitabı.* Türkiye Barolar Birliği Yayını.

YENİSEY F. /NUHOĞLU A., 2018. *Ceza muhakemesi hukuku.* 6. Baskı. Ankara: Seçkin.

Süreli Yayınlar

AKTAŞ B., 2017. Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma Tedbiri Üzerinde Bir İnceleme. *Yeditepe Üniversitesi Hukuk Fakültesi Dergisi.* **14** (2), ss. 211-239

APİŞ Ö., 2018. Bilişim sistemine girme suçu bakımından bilgisayarda, bilgisayar programlarında ve kütüklerinde arama kopyalama ve el koyma tedbiri. *Yasama Dergisi*. (37), ss. 49-86.

ARAALAN C. 2015.Türk hukukunda dijital deliller, *GSI ARTICLETTE SUMMER.* (15), ss. 203-212.

ARSLAN Ç., 2015. Dijital delil ve iletişimin denetlenmesi. *Ceza Hukuku ve Kriminoloji Dergisi.* **3**(2), ss. 253-266.

BAŞLAR Y., 2020. Elektronik delilin toplanması ve muhafazası. *Hacettepe Hukuk Fakültesi Dergisi.* **10**(1), ss. 77-107.

BAŞLAR Y., 2020. Adli bilişim sürecinde karşılaşılan sorunlar ve çözüm önerileri. *Türkiye Barolar Birliği Dergisi.* (148), ss. 47-76.

BAŞLAR Y., 2018. Elektronik delil ve ceza yargılamasında kabul edilebilirliğine ilişkin bir inceleme. *Legal Hukuk Dergisi*. **16** (184), ss. 1655-1688.

BAŞLAR Y., 2013. Ceza yargılamasında elektronik delillerin elde edilmesine ve korunmasına ilişkin usul Hükümleri, *Uyuşmazlık Mahkemesi Dergisi*. (3), ss. 82 – 105.

BAŞTÜRK İ., 2010. Bilgisayar sistemleri ile verilerinde arama, kopyalama ve elkoyma. *Fasikül Hukuk Dergisi.* Yıl:2 (9), ss. 23-3.

BAYRAM, L., 2012. Adli bilim laboratuvarında TS EN ISO/IEC 17025 standartı teknik gereklilikleri. *Polis Bilimleri Dergisi*. **14** (1) ss. 81-100.

BOSTANCI Ü. /BENZER R., 2015. Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve elkoyma. *Uluslararası İnsan Bilimleri Dergisi*. (2), ss.1192-1299.

ÇÖPOĞLU H. S., 2019. Ceza muhakemesi hukukunda arama koruma tedbirinde, belirlilik ilkesi, *Ankara Barosu Dergisi*. (1), ss. 157-229.

ÇAKIR H./KILIÇ M. S., 2013. Bilişim suçlarına ilişkin delil elde etme yöntemine genel bir bakış. *Polis Bilimleri Dergisi*. **15** (3), ss.23-44

DEĞİRMENCİ, O., 2018. Bilgisayarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbirinde(CMK m. 134), 7145 sayılı kanunla yapılan değişikliklerin değerlendirilmesi. *Terazi Hukuk Dergisi.* **13** (146) ss. 146-155.

DEĞİRMENCİ, O, 2014. Bilgi toplumunun delil türü: sayısal deliller ve bilimselliği. *Terazi Hukuk Dergisi*. **9**(97), ss.14-28.

DÜLGER M. V., 2017. Adli Bilişim & Ülkemizde Uygulanması. *Hukuk ve Daha Fazlası Dergisi.* (1) ss. 20-25.

EMEKCİ, A.,/KUĞU E. /TEMİZTÜRK M., 2016. Adli bilişim ezberini bozan bir düzlem: bulut bilişim. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, **2**(1), ss. 8-14.

ERCAN, T. ve NACAK, D., 2009. Kablosuz ağlardaki paket trafiğine adli Bilişim yaklaşımı. *Journal of Yasar University*, **4**(13), ss. 1909-1921.

ERDAĞ, A. İ. 2010. Bilişim alanında suçlar(Türk ve Alman Hukukunda). *Gazi Üniversitesi Hukuk Fakültesi Dergisi.* **C. XIV** (2), ss.275-3030.

ERDOĞAN Y., 2012. Bilişim sistemine girme ve kalma suçu. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*. **12**, Özel S., 2010. ss.1363-1433.

HEKİM H. / BAŞIBÜYÜK O., 2013. Siber suçlar ve Türkiye'nin siber güvenlik politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*. **4**(2), ss. 135-158.

İÇEL K., 2001. Avrupa konseyi siber suç sözleşmesi bağlamında "Avrupa siber suç politikasının ana ilkeleri." İstanbul Üniversitesi Hukuk Fakültesi Mecmuası. **59** (Sayı:1-2), ss.3-10.

KESKİN S., 2001. Avrupa konseyi siber suç sözleşmesinde ceza muhakemesine ilişkin hükümlerin değerlendirilmesi. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, **59** (12), ss.155 – 180.

KIZILYAR M., 2014. Ceza yargılamasında dijital verilerin delil değeri. *Adalet Dergisi.* (50), ss.72-89.

KOCAOĞLU S S., 2012. Üst ve büro araması, postada elkoyma, iletişimin denetlenmesi gibi çeşitli koruma tedbirlerinin pasif öznesi olarak kuram ve uygulamada avukatın bağımsızlığı. *Ankara Barosu Dergisi*. **1**, ss.45-69.

ORAKCI M., /KÖK İ./ÇAKIR H., Adli Bilişim Eğitiminin Gereksinimi ve Genel Olarak Değerlendirilmesi, *Bilişim Teknolojileri Dergisi.* **9**(2), Mayıs 2016 ss.137-145.

ÖLMEZ A., 2009. Bilgisayarda, bilgisayar programlarında ve kütüklerinde kopyalama ve bunlara elkoyma, Terazi Hukuk Dergisi. (10), ss.45-52.

ÖNOK M., 2013. Avrupa konseyi siber suç sözleşmesi ışığında siber suçlarla mücadelede uluslararası işbirliği (Prof. Dr. Nur Centel"e Armağan). *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi.* **19** (2), ss. 1229 – 1270.

ÖZBEK V. Ö., 2002. İnternet kullanımında ortaya çıkabilecek bazı ceza hukuku sorunları. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*. **4**(1), ss. 101-158.

ÖZBEK V. Ö., 2007. Banka veya kredi kartlarının kötüye kullanılması suçu (TCK m.245). *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, **9** Özel Sayı, ss. 1019-1063.

ÖZEN M. / ÖZOCAK G., 2015. Adli Bilişim, elektronik deliller ve bilgisayarda arama ve el koyma tedbirinin hukuki rejimi (CMK M 134). *Ankara Barosu Dergisi*. (1), ss. 43-77.

ÖZGÜVEN A. D., 2009. Ceza muhakemesi kanunu çerçevesinde adli kontrol. *Türkiye Barolar Birliği Dergisi*. (81), ss.1-42.

ÖZKUL D., 2002. Bilişim sistemi kavramı ve bilişim sistemlerinin denetimi. *Sayıştay Dergisi*, (44-45), ss.11-34.

ÖZTÜRK C., 2016. Kolluk amaç ve yapıları ile veri elde etme araçları arasındaki bağlantı üzerine bir araştırma. *Bitlis Eren Üniversitesi Sosyal Bilimler Dergisi*. **5**(1), ss. 1-24.

SARSIKOĞLU Ş., 2015. Ceza muhakemesinde delil ve ispat hukuku açısından elektronik delil(e-delil) kavramı. *Türkiye Adalet Akademisi Dergisi*. Yıl:6, (22), Temmuz, ss.427-454.

SEVİMLİ, A. G., 2007. Bilgisayar ve bilgisayar kütüklerine el konulması ve uygulamadaki sorunlar. *İstanbul Barosu Dergisi*. **81**(3), ss. 993-1000.

ŞEN E., 2014. E-posta takibi, *Terazi Hukuk Dergisi*, **9**(97) ss.88-90.

ŞİRİKÇİ, A. S. /CANTÜRK N., 2012. Adli bilişim incelemelerimde birebir kopa alınmasının(imaj almak) önemi. *Bilişim Teknolojisi Dergisi*. **5**(3), ss.29-34.

USTA C. A. ve BENZER R., 2018. Avrupa siber suçlar sözleşmesi ve Türkiye'nin dahil olma süreci. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, **4**(2), ss.35-42.

YAŞAR G. D., 2019. Ceza muhakemesi kanunu'nda (CMK) bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma. *Bahçeşehir Üniversitesi Hukuk Fakültesi Dergisi.* **14**(173-174), ss. 173-241.

YAŞAR, Y. / DURSUN, İ., 2013. Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma koruma tedbiri. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırma Dergisi*. **19**(3), ss. 1-34.

YETİM S., 2008. Dijital kanıt araştırma yöntemleri. *İstanbul Barosu Dergisi*. **82**(3), ss. 1201-1221.

YETİM S., 2014. Siber suçlar, yargılama yetkisi ve yeni bir model önerisi. *Türkiye Adalet Akademisi Dergisi*. **5**(17), ss.177-232.

YILMAZ S., 2011. 5237 Sayılı TCK'nın 244. maddesinde düzenlenen bilişim alanındaki suçlar. *Türkiye Barolar Birliği Dergisi.* (92), ss.62-100.

Diğer Yayınlar

ABEL W., *"Agents, Trojans and Tags: The Next Generation of Investigators*" International Review of Laaw, Computers & Technology, Vol. 23, No. 1, 2009, https://www.tandfonline.com/doi/full/10.1080/13600860902836869?scroll=top&needAccess=true [E.T: 9.12.2020]

ASHCROFT J. (Ed.), 2001, "*Electronic Crime Scene Investigation: A Guide for First Responders"*, Washington: PhotoDisc, Inc, https://www.ncjrs.gov/pdffiles1/nij/187736.pdf [E.T: 29.06.2019]

AYDOĞAN, H., 2009. Adli bilişim'de yeni elektronik delil elde etme yöntemleri. *Yüksek Lisans Tezi*. Ankara: Polis Akademisi Güvenlik Bilimleri Enstitüsü.

BALLI Y., "CMK 134. Madde Düzeltilmelidir", http://www.dijitaldeliller.com/cmk134.htm [E.T: 30.06.2020].

BAŞAR, Y., 2015. Siber suç soruşturmalarında adli bilişim incelemeleri. *Yüksek Lisans Tezi*. Afyon: Kocatepe Üniversitesi Fen Bilimleri Enstitüsü.

BAYRAKTAR B, 2011. Muhakemelerde delillerin önemi, Sosyal Bilimler Dergisi, Sayı: 25, ss.3343. http://journals.manas.edu.kg/mjsr/oldarchives/Vol12_Issue25_2011/03_bayraktar.pdf [E.T: 12. 10. 2020]

BROWN CHRISTOPHER L. T. (2010), Computer Evindence: collectiom and preservation, Second edition (Networking& Security Series) Charles River Media, Rockland. ss.147-168. **https://silo.pub/download/computer-evidence-collection-and-preservation-second-edition.html** [E.T: 05.04.2021]

ÇAKIR H. / SERT E., Bilişim suçları ve delillendirme süreci, https://docplayer.biz.tr/1538965-Bilisim-suclari-ve-delillendirme-sureci.html [E.T: 26.12.2020]

CASEY, Digital Evidence and Computer Crime, https://books.google.com.tr/books/about/Digital_Evidence_and_Computer_Crime.html?id=6gCbJ4O4f [E.T: 16.11.2020]

CoE(Council of europe),(2013), Electronic Evidence Guide: A Basic Guide for Police Officers, Prosecutors and judges. Data Protectionsn and Cybercrime Division. https://www.dfir.training/index.php?option=com_ireviews&format=ajax&url [E.T: 14.10. 2020]

CORNEL W., Computer forensic: bringing the evidence to cout, http://www.infosecwriters.com/Papers/CWalker_Computer_Forensics_to_Court, [E.T:10.01.2020]

COSİC, J /BACA m.(2010), (Im) Proving Chain of Custody and Digital Evidence Integrity with Time Stamp. Croatian Society for Information and Communication Technology, Electronics and Microelectronics(MIPRO),33rd International Convention, Opatija, Hırvatistan http://czb.foi.hr/upload/datoteke/10_400.pdf [E.T:5.08.2020].

ÇELİK M., 2018. Bilgisayarda arama, kopyalama ve elkoyma(CMK m.134). *Yüksek Lisans Tezi*. İstanbul: Üniversitesi Sosyal Bilimler Enstitüsü.

DEBROTA, S., GOLDMAN, J., MİSLAN, R., ROGERS, M.K., & WEDGE, T.,(2006) Computer Forenscs Field Triage Process Model. Journal of Digital Forensics, Security and Law, 1(2) https://commons.erau.edu/cgi/viewcontent.cgi?article=1004&context [E.T:26. 11.2020]

DEMİRKAYA V., 2009. Delil güvenliği, *Yüksek Lisans Tezi*. Ankara: T.C. Polis Akademisi Güvenlik Bilimleri Enstitüsü.

DÜLGER, M.V. / MODUOĞLU, G., "Türk ceza adalet sisteminin etkinliğinin geliştirilmesi" Bilişim suçları eğitim modülü. https://rayp.adalet.gov.tr/resimler/552/dosya/2-bilisim-suclari-egitimi-modulu25-08-20204-32-pm.pdf [E.T:10.08.2020]

EKİZER A. H., Adli Bilişim (Computer Forensics) 2. Şubat 2014 https://www.ekizer.net/adli-bilisim-computer-forensics/ [10.05.2018]

GÖKSU, M., 2010. Hukuk yargılamasında elektronik delil. *Doktora Tezi*. Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

GÖZÜŞİRİN M., 2011. 5237 sayılı türk ceza kanununda bilişim suçları ve bilişim suçları ile mücadeleye ilişkin model önerisi. *Yüksek Lisans Tezi.* Ankara: Kara Harp Okulu SBE.

KAYA M. B., "Hukuki Açıdan Bilişim Suçları, Siber Güvenlik ve Adli Bilişim", Şeref Sağıroğlu/Mustafa Şenol (ed.), Siber Güvenlik ve Savunma Problemler ve Çözümler içinde (213-279), BGD Siber Güvenlik ve Savunma Kitap Serisi 2, Grafiker Yayınları, Ankara, 2019. https://docplayer.biz.tr/169214078-Siber-guvenlik-ve-savunma.html [E.T:12.12.2020]

KAYNAKÇIOĞLU, U., 2015. Ceza muhakemesinde dijital deliller. *Yüksek Lisans Tezi.* İstanbul: Galatasaray Üniversitesi Sosyal Bilimler Enstitüsü.

KENT K., CHEVALİER S., GRANCE T., DANG H., "Guide to Integrating Forensic Techniques into Incident Response" National Institute of Standards and Technology Special Publication 800-86, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86 [E.T:20.09.2020]

KOZUSHKO H., 2003 Digital Evidence http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/DigitalEvidencePaper.pdf [E.T:24.07.2020]

KUMAR K., SOFAT S., JAİN S.K., AGGARWAL N., Significance of Hash Value Generation in Digital Forensic: A Case Study, International Journal of Engineering Research and Development, ss. 64-70. http://www.ijerd.com/paper/vol2-issue5/I02056470.pdf [E.T:16.02.202]

MANSON, S., "Introduction", Stephen Mason (ed.), International Electronic Evidence, Londra: British Institute of International and Comparative Law, 2008. s. xxxv. https://www.biicl.org/files/3434_introduction_mason.pdf [E.T:21.9.2020]

OĞUZ R., 2018. Adli bilişimde inceleme süreçleri. Yüksek Lisans Tezi. Ankara: Üniversitesi Sağlık Bilimleri Enstitüsü.

ÖZBEK M., 2013. Adli bilişimde delillerin toplanması ve incelenmesi. *Yüksek Lisans Tezi*. İstanbul: Bilgi Üniversitesi SBE.

ÖZMESTİK, F. Ü.., 2015. Bilişim sistemleri üzerinde arama ve elkoyma tedbirine ilişkin mevzuat ve uygulamada yaşanan sorunlar. *Yüksek Lisans Tezi*. İstanbul: Bilgi Üniversitesi Sosyal Bilimler Enstitüsü.

ÖZOCAK G., Ceza muhakemesinde elektronik delillerin tespiti ve toplanması, http://www.ozocak.com/Dosyalar/11504e.pdf [E.T:11.07.2020].

ÖZOCAK G., Ceza Muhakemesinde Elektronik Delillerin tespiti ve Toplanması, İzmir 2. Uluslararası Bilişim Hukuku Kurultayı, 17-19 Kasım 2011, Bildiriler Kitabı(Editörler: Tekin Memiş, Ahmet, Ahmet Koltuksuz, Mine Akkan) https://docplayer.biz.tr/811097-Izmir-2-uluslararasi-bilisim-hukuku-kurultayi-17-19-kasim-2011-bildiriler-kitabi.html [E.T:24.11.2020]

ÖZTÜRK, M. İ., 2007. Bilişim cihazlarındaki sayısal delillerin tespiti ve değerlendirilmesinde iş akış modelleri. Yüksek Lisans Tezi Ankara: Üniversitesi SBE.

PRASAD, M.A.R. ve SATİSH, Y. N. (2013). Reconstruction of Events in Dijital Forensics International Jaurnal of Engineering Trends and Technology, 4(8), ss. 3460-3467. https://studylib.net/doc/12925458/reconstruction-of-events-in-digital-forensics [E.T:20.09.2020]

SAMET R., Bilgisayar Sistemleri (2-2–3) http://android.eng.ankara.edu.tr/wp-content/uploads/sites/656/2018/02/1-Giris.pdf [E.T:10.07.2020].

SANSAR M., Bilişim suçlarının tespiti ve dijital delillerin incelenmesi http://www.tide.org.tr/uploads/MUSTAFA%20SANSAR.pdf [E.T:10.05.2018]

SAY K., 2006. Bilişim suçlarında elde edilen delillerin olay yerinden toplanması ve laboratuvarda incelenmesi. *Yüksek Lisans Tezi*. Ankara Üniversitesi Sağlık Bilimleri Enstitüsü.

SCHATZ, B,L(2007), Digital Evidence: Representation and Assurance, Master Thesis Queensland University of Teennology Information Security Institute, Australia, https://eprints.qut.edu.au/16507/1/Bradley_Schatz_Thesis.pdf [E.T: 20.09.2020]

ŞEN E., Bilgisayarda Arama, Kopyalama ve Elkoyma https://www.haber7.com/yazarlar/prof-dr-ersan-sen/2075545-bilgisayarda-arama-kopyalama-ve-elkoyma [E.T: 22.06.2020].

ŞEN E., E-Posta Takibi, https://www.haber7.com/yazarlar/prof-dr-ersan-sen/1191018-e-posta-takibi [E.T:28.08.2020].

UZUNAY Y. / BIÇAKCI K. A3D3M:Açık anahtar altyapısı destekli dijital delilleri doğrulama modeli. http://www.emo.org.tr/ekler/4843973f9b66701_ek.pdf [E.T: 2.07.2019]

ÜNAL, O. G., 2011. Bilgisayarda, bilgisayar programlarında ve kütüklerinde arama kopyalama ve elkoyma. Yüksek Lisans Tezi. Ankara: Gazi Üniversitesi SBE.

YENİSEY F. / NUHOĞLU A., 2014, Ceza muhakemesi hukuku ders kitabı, Bahçeşehir Üniversitesi Yayınları No: 111 http://www.feridunyenisey.com/Yayinlar/cezamuhakemesihukukuderskitabi.pdf [E.T: 13.11.2020]

YILDIZ E., ŞAHİN Serap, ”Bulut Bilişimde Güvenlik Riskleri ve Önlemler”, 2.Uluslararası Bilişim Hukuku Kurultayı Bildiriler Kitabı, İzmir, 17-19 Kasım 2011. https://docplayer.biz.tr/811097-Izmir-2-uluslararasi-bilisim-hukuku-kurultayi-17-19-kasim-2011-bildiriler-kitabi.html [E.T: 17.12.2020]

YILDIZ S., Suçta araç olarak internetin teknik ve hukuki yönden incelenmesi, sayı:17, s. 609-623. ss.609-607, http://dergisosyalbil.selcuk.edu.tr/susbed/article/view/507/489 [E.T: 28.12.2020]

Adli Bilişim Aracı Test Programı (CFTT), https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt. [E.T: 29.08.2020].

Bulut Bilişim Nedir? http://www.yazilimnet.com/tr/blog/38/bulut-bilisim-nedir- [E.T:28.07.2020].

Bilgisayar Ağı Nedir? https://www.dersimiz.com/bilgisayar/bilgisayar-agi-nedir-22710.html [E.T: 22.12.2018]

Bilgisayar ağı https://tr.wikipedia.org/wiki/Bilgisayar_a%C4%9F%C4%B1#:~:text=Bilgisayar%20a%C4%9F%C4%B1%2C%20k%C3%BC%C3%A7%C3%BCk%20bir%20alan,veri%20aktar%C4%B1m%C4%B1n%C4%B1n%20m%C3%BCmk%C3%BCn%20oldu%C4%9Fu%20ileti%C5%9Fim [E.T:06.03.2021]

Elektrik Elektronik Teknolojisi Analog ve Sayısal Haberleşme, http://www.megep.meb.gov.tr/mte_program_modul/moduller_pdf/Analog%20Ve%20Say%C4%B1sal%20Haberle%C5%9Fme.pdf [E.T: 27.06.2019].

Elektrik mühendisliği dergisi, 2012, 4. Ağ ve bilgi güvenliği sempozyumu http://www.emo.org.tr/ekler/ea331d3983f3898_ek.pdf?dergi=873 [E.T: 10.11.2019]

Gözetim Zinciri Nedir? Tanım ve Örnekler, 03 Nov, 2020, https://www.greelane.com/tr/be%C5%9Feri-bilimler/sorunlar/chain-of-custody-4589132, [E.T: 21.03.2021]

IP adresi https://tr.wikipedia.org/wiki/IP_adresi [E.T: 14.05.2020].

IP Adresi Nedir? https://www.chip.com.tr/ip-adresim-nedir [E.T:14.05.2020].

Zombi bilgisayar https://tr.wikipedia.org/wiki/Zombi_bilgisayar [E.T: 14.05.2020].

Bellek kartı https://tr.wikipedia.org/wiki/Bellek_kart%C4%B1 [E.T: 16.05.2020].

Flash Bellek Nedir, Ne işe Yarar? 27 Kasım 2017 http://flashbellek.org/flash-bellek-nedir/ [E.T: 16.05.2020].

Veri Kurtarma Nedir https://www.mydisk.com.tr/tr/makale/105/veri-kurtarma-nedir/ [E.T:19.05.2020]

ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc [E.T: 4.04.2019]

http://bilisimhukuku.com.tr/adli-inceleme-nasil-yaptirilir/ [E.T: 10.05.2018]

http://resmigazete.gov.tr/eskiler/2007/11/20071130-6.htm [E.T: 7.04.2019]

http://www.resmigazete.gov.tr/eskiler/2017/04/20170411-3.htm [E.T: 4.04.2019)]

https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf [E.T: 15.07.2020].

http://tdk.gov.tr/index.php?option=com_bilimsanat&view=bilimsanat&kategori=terim&hng=md&kelime=bili%C5%9Fim [E.T: 23.03.2019]

http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5caf03eb1102b5.68264309 [E.T: 11.04.2019]

http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5caf03f59a8645.30454492 [E.T: 11.04.2019]

http://tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5caf082c536ec5.72468597 [E.T: 11.04.2019]

https://sozluk.gov.tr/ [E.T: 13.08.2020]

https://sozluk.gov.tr/ [E.T: 11.07.2020].

https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=21470&MevzuatTur=7&MevzuatTertip=5 [E.T: 19.08.2020].

http://www.resmigazete.gov.tr/eskiler/2018/07/20180731-1.htm [E.T: 23.12.2018].