T.C.
GAZİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
CEZA VE CEZA USUL HUKUKU
ANABİLİM DALI

BİLGİSAYARLARDA BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA KOPYALAMA VE ELKOYMA

YÜKSEK LİSANS TEZİ

HAZIRLAYAN

OSMAN GAZİ ÜNAL

098258101

TEZ DANIŞMANI

PROF. DR. FATİH S. MAHMUTOĞLU

ANKARA-2011

T.C.
GAZİ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
CEZA VE CEZA USUL HUKUKU
ANABİLİM DALI

BİLGİSAYARLARDA BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA KOPYALAMA VE ELKOYMA

YÜKSEK LİSANS TEZİ

HAZIRLAYAN

OSMAN GAZİ ÜNAL

098258101

TEZ DANIŞMANI

PROF. DR. FATİH S. MAHMUTOĞLU

ANKARA-2011

ONAY

Osman Gazi ÜNAL tarafından hazırlanan *"Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma"* başlıklı bu çalışma, 07/04/2011 tarihinde yapılan savunma sınavı sonucunda *(oybirliği/oyçokluğu)* ile başarılı bulunarak jürimiz tarafından Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı Yüksek Lisans tezi olarak kabul edilmiştir.

Prof Dr. Cumhur ŞAHİN (Başkan)

Prof Dr. Fatih S. MAHMUTOĞLU

Doç. Dr. İlhan ÜZÜLMEZ

ÖNSÖZ

Bilgisayarlar bilgi toplumunun en önemli cihazıdır. Bilgisayar kullanımının yaygınlaşmasıyla içindeki verilerin muhakeme sürecinde delil olarak kabul edilip kabul edilemeyeceği sorunu ortaya çıkmıştır. Ceza muhakemesinin amacı göz önünde bulundurulduğunda bu hususun önemi daha iyi anlaşılacaktır. Bu nedenle kanun koyucu ortaya çıkan bu yeni duruma kayıtsız kalmamış, 5271 sayılı Ceza Muhakemesi Kanunu'nun 134. maddesinde bir koruma tedbiri olarak "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma"'yı düzenlemiştir.

Adli bilişim ABD, Kanada, Finlandiya, İsrail ve İngiltere gibi ülkelerde gelişmiş bir adli bilim dalıdır. Bilgisayardan delil elde edilmesi, adli bilişim alanı içerisinde yer aldığından bu konuya çalışmamızda yer verilmiştir. Avrupa dışından ülkelerin katılımıyla adeta uluslararası bir sözleşmeye dönüşen Avrupa Konseyi Siber Suç Sözleşmesi'nde, bilgisayarlara yönelik koruma tedbirlerine ilişkin hükümler ele alınmıştır. Bu hükümlerle beraber söz konusu koruma tedbirinin karşılaştırmalı hukuktaki yansımalarına değinilmiştir. Bu alanda kullandığımız internet kaynakları daha önce yayınlanmış akademik dergilerden oluşmaktadır.

Bugüne kadar bu koruma tedbirleri hakkında yeterli bir çalışma yapılmamıştır. Ayrıca bu alanda yapılan çalışmalarda konuya, bilişim suçları ve adli bilişim açılarından yaklaşılmıştır. Ancak bu düzenleme bir koruma tedbiri olduğu için ceza muhakemesi hukuku içerisinde değerlendirilmesi gerekmektedir.

Bu konuda çalışma yapma konusunda bizleri cesaretlendiren, tavsiyeleriyle çalışmamızda bizlere yol gösteren tez danışmanım değerli hocam Prof. Dr. Fatih Selâmi MAHMUTOĞLU'na, çalışmamızda bilgisiyle, gösterdiği farklı bakış açılarıyla kanunu yorumlamam konusunda bizlere yardımcı olan, saygı değer hocam Prof. Dr. Cumhur ŞAHİN'e, görüşlerinden faydalandığım değerli hocalarım Prof. Dr. İzzet ÖZGENÇ'e ve Doç Dr. İlhan ÜZÜLMEZ'e, çalışma arkadaşlarım Arş. Gör. Mehmet MADEN'e ve Arş. Gör. Ahmet Hulusi AKKAŞ'a teşekkürlerimi sunuyorum.

Desteklerinden ötürü babam Prof. Dr. Mehmet Ali ÜNAL'a, bilgisayar alanında yardımlarda bulunan kardeşim Hasan Şahin ÜNAL'a ve Hakan TARIM'a, adli bilişim alanındaki gelişmeler ve teknik konularda bilgi sağlayan Ankara Kriminal Polis Laboratuvarı Müdürlüğü'ndeki Data İncelemeleri Ekibi'ne ayrıca teşekkür ediyorum.

Bu özgün koruma tedbiri yeni bir düzenleme olduğundan çalışmamız bir ilk adımı oluşturmaktadır. Diğer adımların atılmasında çalışmamızın katkıda bulunması bize mutluluk sağlayacaktır.

Arş. Gör. Osman Gazi Ünal
Gazi Üniversitesi Hukuk Fakültesi
Ceza ve Ceza Muhakemesi Hukuku Anabilim Dalı
Demirlibahçe / ANKARA 2010

İÇİNDEKİLER

KISALTMALAR

AB: Avrupa Birliği

ABD: Amerika Birleşik Devletleri

AFP: Avustralya Federal Polisi

AİHM: Avrupa İnsan Hakları Mahkemesi

AİHS: Avrupa İnsan Hakları Sözleşmesi

AK-SSS: Avrupa Konseyi Siber Suç Sözleşmesi

AÖAY: Adli ve Önleme Aramaları Yönetmeliği

AYM: Anayasa Mahkemesi

Bkz: Bakınız

BM: Birleşmiş Milletler

BverfG: Bundesverfassungsgerıcht

CD: Compact Disk

CD: Ceza Dairesi

CHD: Ceza Hukuku Derneği

CIA: Central Intelligence Agency

CMA: Computer Misuse Act

CMK: Ceza Muhakemesi Kanunu

CMUK: Ceza Muhakemeleri Usulü Kanunu

CPU: Central Processing Unit

CTOSE: Cyber Tools On-line Search for Evidence

ECPA: Electronic Communications Privacy Act

FBI: Federal Bureau Investigation

FSEK: Fikir ve Sanat Eserleri Kanunu

HTML: Hyper Text Markup Language

HUMK: Hukuk Usulü Muhakemeleri Kanunu

IP: İnternet Protokolü

IT: Information Technology

İBD: İstanbul Barosu Dergisi

İÜHFM: İstanbul Üniversitesi Hukuk Fakültesi Mecmuası

Md.: Madde

MSN: Messenger

NJW: Neue Juristische Wochenschrift

PDA: Personal Digital Assistant

RAM: Random Access Memory

RFS: Remote Forensic Software

RIPA: Regulation of Investigatory Powers Act

ROM: Read Only Memory

SEY: Suç Eşyası Yönetmeliği

SOP: Standart Operating Proceedures

SWGDE: Scientific Working Group On Digital Evidence

TCK: Türk Ceza Kanunu

TCKÖ: Türk Ceza Kanunu Öntasarısı.

TCP: Transmission Control Protocol

TDK: Türk Dil Kurumu

USB: Universal Serial Bus

USC: United States Code

UYAP: Ulusal Yargı Ağı Projesi

Vb: ve bunun

Vd: ve devamı

Yarg: Yargıtay

GİRİŞ

Bilgisayarlar sayesinde dünya artık iyice küçülmektedir. İnsanlar bilgisayar sistemlerinin sunduğu internet ortamıyla birbirleriyle iletişim kurabilmekte, ticaret yapabilmekte, bankaya gitmeden banka işlerini yürütebilmekte ve bunun gibi birçok işlemi icra edebilmektedirler. İnsanların bilgisayar kullanımı sadece yetişkinlerle sınırlı kalmamıştır. Günümüzde ilkokul öğrencileri ödevlerini hazırlamada bilgisayarlardan yararlanmaktadır. Teknolojik olarak sürekli gelişen bu cihaz hayatımızı baş döndürücü bir şekilde değiştirmiştir. Bu nedenlerle yaşadığımız çağı bilgisayar veya bilişim çağı olarak adlandırmak mümkündür.

"Işığın olduğu yerde gölge de vardır." düsturundan hareketle bilgisayar hem olumlu yanlarıyla hem de olumsuz yanlarıyla insan hayatını değiştirmekle kalmamış, toplumun yapısını da değiştirmeye başlamıştır. İnsanlar bilgisayarın sunduğu internet ortamı sayesinde sosyalleşebilmektedir. Başka bir açıdan bakıldığında ise insanların bilgisayar başında daha çok vakit harcamaları, onları toplumdan uzaklaştırmakta ve asosyal bir varlık haline getirmektedir. Bunun sonucunda aile içerisindeki iletişim azalmakta, eşler arasında anlaşmazlıklar artmakta ve boşanmalar vukubulmaktadır.

Eskiden odalar kaplayan bilgisayarların transistorün ve mikroçiplerin keşfi ile avuç içine sığabilecek hale gelmesi, bilgisayar teknolojisinin hızla geliştiğini göstermektedir. Bilgisayar teknolojisinin hızlı gelişmesi kendisini bilgisayar piyasasında da göstermiştir. Bu zamanda en üst özelliklere sahip olan bilgisayarlar birkaç ay sonra eskiyecek ve sonunda kullanılmayan bir cihaz olup elektronik alet çöplüğü yaratacaktır.

Bilgisayarın yükselişiyle beraber bilgisayarla işlenebilen haksızlıklarda da bir artış gözlemlenmiştir. Özellikle internetin bilgiye ulaşmadaki bizlere sağladığı geniş özgürlük alanı suistimal edilebilmekte ve suç işlenmesini kolaylaştırmaktadır. Bilgisayar korsanları (Hacker) güvenlik duvarlarını kolayca etkisiz hale getirmekte, banka hesaplarını boşaltabilmekte, haberleşme araçlarını dinleyebilmektedirler. Bu sebeple devletler hukuk

düzeni içerisinde hem kendilerini hem de bireyi korumak amacıyla bu tür haksızlıkları birer suç olarak düzenlemişlerdir. Bilgisayarla işlenebilen suçların etkisinden korunabilmek için bilgisayar sahipleri, bankalar, ticaret şirketleri, ordu ve kamu kurumları kendi güvenliklerini sağlayabilmek amacıyla donanım ve yazılımlara ihtiyaç duymaktadır. Bu ihtiyaç doğrultusunda yeni iş alanları doğmuştur. Donanım ve yazılım üreten ve bunların tamiri ile ilgilenen şirketler kurulmuştur.

Ceza Muhakemesinin amacının maddi gerçeğe ulaşmak olduğundan elektronik biçimdeki verilerin delil olarak anlaşılır bir biçimde mahkemeye sunulması ihtiyacı doğmuştur. Bilgisayarla işlenebilen örneğin Türk Ceza Kanunu "Bilişim Alanında Suçlar" başlığı altında (md. 243, 244, ve 245) düzenlenen bilişim suçlarının delilleri genellikle bilgisayarda olmaktadır. Bunun yanında bilgisayarla işlenmeyen klasik tipteki suçların delilleri de bilgisayarda bulunabilmektedir. Bilgisayardan delil elde etmek için 5271 sayılı Ceza Muhakemesi Kanunu'nun "Bilgisayarlarda ve Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma" başlığı altında 134. maddesi düzenlenmiştir. Bu madde arama ve elkoyma koruma tedbirlerinin özel bir düzenlemesini oluşturmaktadır. Söz konusu tedbirlerin uygulanması ticari, mesleki ve bilimsel alanlarda saklanan sırları ortaya çıkarabilecek nitelikte olduğundan anayasada bulunan temel hak ve özgürlüklere müdahale teşkil edecektir. İfade edilen bu nedenlerle özel koruma tedbirlerinin düzenlenmesi gerekmiştir.

Çalışmamızın ilk bölümünde öncelikle bilgisayarlarla ilgili temel kavramlardan bahsedilecektir. Bilgisayardan delil elde edilmesi bir adli bilim alanı olan adli bilişim alanına girmektedir. Adli bilişim kısaca otopsinin bilgisayar üzerinde yapılmasıdır. İlk bölümde adli bilişim ve süreci, elektronik deliller, adli bilişim alanındaki dünyada kabul edilen ilkeler, adli bilişimin inceleme alanları olan bilgisayar ve veri saklama birimleri ile ilgili konular incelenecektir. Teknik kavramlara ilk bölümde yer vermemiz, önem arzetmektedir. Bilgisayarlara yönelik tedbirlerin içeriğini belirlememizde ve

bilgisayardaki delillerin doğru ve hukuka uygun bir şekilde toplanıp toplanmadığı hususundaki bu bilgiler yön gösterici olacaktır.

İkinci bölümde bilgisayarlara yönelik arama ve elkoyma tedbirlerinin Avrupa Konseyi Siber Suç Sözleşmesi'ndeki düzenlenişine ve anlaşmaya taraf olan veya taraf olmayan ülkelerde bu tedbirin nasıl düzenlendiğine yer verilecektir. Bu bölümde özellikle ABD'deki temel hak ve özgürlüklerin söz konusu tedbirlerin uygulanmasıyla maruz kaldığı müdahalelere ayrı başlıklar içerisinde değinilmiştir. Böylelikle konuya temel hak ve özgürlükler bakımından da yaklaşılmaya çalışılmıştır.

Çalışmamızın üçüncü bölümünde bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbiri incelenmiştir. Tebirin hukuki niteliği, genel arama ve elkoyma tedbirlerinden farkları ve uygulanması bu bölümde yer almaktadır. Kanunun uygun ölçüde yorumlanmasıyla varılan neticelerden ve diğer koruma tedbirlerindeki özel durumlardan karşılaştırmalı bir şekilde bahsedilecektir. Bilgisayarlara yönelik özel tedbirin uygulama alanındaki yarattığı sorunlara ve ayrıca adli bilişim penceresinden görünen durumlara da değinilecektir. Tedbirlerin bilişim suçları ve 5651 sayılı kanun bakımlarından uygulanması ayrı bir başlık altında ele alınmıştır.

Değerlendirme ve sonuç kısmında karşılatırmalı hukuktaki gelişmeleri gözlemleyerek söz konusu özel koruma tedbirlerinin olumlu-olumsuz yönlerini fikirlerimiz doğrultusunda belirteceğiz.

BİRİNCİ BÖLÜM

BİLGİSAYARLA İLGİLİ TEMEL KAVRAMLAR, ELEKTRONİK DELİL VE ADLİ BİLİŞİM

I- BİLGİSAYARLA İLGİLİ TEMEL KAVRAMLAR

A- BİLGİSAYAR VE BİLGİSAYARIN ÖZELLİKLERİ

İngilizce'de hesaplama anlamına gelen "compute" kelimesinden türetilen ve kelime anlamı hesaplayıcı olan "computer" kelimesi Türkçemize bilgisayar olarak çevrilmiştir[1]. TDK'nın sözlüğüne göre bilgisayarla ilgili şu şekilde bir tanımlama kullanılmıştır:

"*Çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin."*[2].

Sözlükteki tanımdan ayrı olarak bilgisayar, "*aritmetik ve mantıksal işlemler yapabilmesi yanında, bir problemin çözümünde gerekli işlemler, kendisine tanıtılarak (programlanarak) veriyi işleyebilen elektronik makinalardır*." olarak da tanımlanabilir[3].

765 sayılı TCK'ya bilişim suçlarını getiren 3756 sayılı "Türk Ceza Kanunu'nda Değişiklik Yapılmasına Dair Kanun'un gerekçesinde parantez içersinde "bilgisayar" kelimesinin bulunması bilgisayarın bir bilişim alanı olarak anlaşılmasına yol açmıştır[4]. Öğretideki bir görüş kanunun gerekçesinde bilişim alanı tarif edilirken parantez içerisinde "bilgisayar" kelimesini içermesi nedeniyle bu kavramdan bilgisayarın anlaşılacağı ileri

---

[1] Levent Kurt, **Açıklamalı ve Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunu'ndaki Uygulaması,** Ankara, Seçkin Yayınevi, Eylül 2005, s. 29.

[2] TDK, **Türkçe Sözlük**, 10. baskı, Ankara, 2005, s. 268.

[3] Aslan Gülcü, M. Ali Alan, **Bilgisayarın Temelleri Ve İnternet Rehberi**, Ankara, Detay Yayıncılık, Ekim 2003, s. 3.

[4] "*bilgileri toplayıp depo ettikten sonra bunları otomatik işleme tabi tutma sistemlerinden (bilgisayar) oluşan alan"*. (14.06.1991 tarihli 20901 s. Resmi Gazete).

sürmüştür[5]. Bir diğer görüş ise bu kavramın bilgisayarla birlikte bilgisayar gibi çalışabilen yeni elektronik cihazları da kapsadığını belirtmiştir[6]. 2003 tarihli TCKÖ'de ise *verileri toplayıp yerleştirdikten sonra bunları otomatik olarak işleme tabi tutma imkanı veren manyetik sistemlerin oluşturduğu alan*" olarak ifade edilen bilişim alanı kavramı çıkarılmış yerine "bilişim sistemi" kavramı metne dahil edilerek "*verileri toplayıp yerleştirdikten sonra bunları otomatik olarak işleme tabi tutma olanağı veren manyetik sistemler*" şeklinde bir tanım yapılmıştır[7]. 5237 sayılı TCK'da ise 10. bölüm "Bilişim Alanında Suçlar" başlığı altında düzenlenen 243. maddesinin gerekçesinde bu tanım değişikliğe uğramamış, sadece "*Bilişim sisteminden maksat"* ibaresi getirilmiştir[8].

Bilgisayarın uluslararası sözleşmelerde de bir tanımı mevcuttur. Avrupa Konseyi Siber Suç Sözleşmesi, bilgisayarı bir sistem olarak ele almıştır. Buna göre bilgisayar sistemi; "*bir veya birden fazlası belirli bir yazılım çerçevesinde otomatik olarak veri işleyebilen bir cihazı veya birbirine bağlı veya birbiriyle ilişkili bir dizi cihaz*" olarak madde 1-a'da tanımlanmıştır[9].

Tanımlardan anlaşılacağı üzere bilgisayar öncelikle elektronik tarzda tasarlanmış bir cihazdır. İçerisine elektronik olarak yerleştirilen mikroçipler ve devreler sayesinde bilgisayarlar veriyi işleyebilme görevlerini yerine getirirler. Veri işleme bilgisayarı diğer elektronik cihazlardan ayıran en önemli özelliklerden biridir. Başka bir ifadeyle bilgisayarın diğer elektronik cihazlardan farklı olarak kendine özgü bir "bilişim yeteneği" vardır[10]. Bilişim yeteneği olan bilgisayarın veriyi otomatik olarak işlemesi insan etkisinin uzak

---

[5] R. Yılmaz Yazıcıoğlu, **Bilgisayar Suçları**, İstanbul, Alfa Yayınevi, 1997, s. 224.
[6] Şaban Cankat Taşkın, **Bilişim Suçları**, Bursa, Beta Yayınevi, Kasım 2008, s. 6, 7.
[7] Kurt **a.g.e.** s. 25.
[8] TCK 243. maddesinin gerekçesi aynen, "*Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir*." şeklindedir. (İzzet Özgenç, **Türk Ceza Kanunu Gazi Şerhi**: **Genel Hükümler**, 3. Bası, Ankara, Adalet Bakanlığı Eğitim Dairesi Başkanlığı, 2006. s. 987).
[9] Avrupa Konseyi Siber Suç Sözleşmesi, (Erişim) http://www.binbilen.org/belgeler/Siber_Suclar_Sozlesmesi.pdf, 25 Haziran 2009. s. 3.
[10] Kurt, **a.g.e.**, s. 29.

olduğunu göstermektedir[11]. Bilgisayar aynı zamanda belli bir program doğrultusunda işlem yapar. Bilgisayardan ayrı olarak diğer elektronik cihazlar da (örneğin bulaşık makinesi) programlanabilirler. Ancak bu cihazların veri işleme fonksiyonları yani bilişim yetenekleri yoktur. Mevzuattaki düzenlemelere bakıldığında bilgisayarın bilişim yeteneğine sahip olması ile 5237 sayılı TCK'daki bilişim sistemi tanımı birbirleriyle örtüşmektedir.

Bilgisayarların programlar vasıtasıyla aynı anda çok hızlı bir şekilde ve (1 saniyede 1 milyar değişik toplama işlemi yapabilirler.) çok çeşitli işlem yapmaları mümkündür. İnsanların aylarca belki de yıllarca uğraşacakları işlemler bilgisayarların yardımı ile çok kısa bir süre içerisinde ve hatasız bir şekilde yapılabilmektedir[12]. Bu açıdan bilgisayarlar güvenilir cihazlardır. Ayrıca, bilgisayarlar işlenmiş olan verileri bizlere sunabileceği gibi hafızalarında da saklayabilirler. Taşıdıkları bu özellik; sözlükte de belirtildiği üzere, bilgisayarın bir "elektronik beyin" olduğunu göstermektedir.

Bugünkü elektronik yapıdaki modern bilgisayarlar ikili sayı (0-1) sistemine göre çalışırlar. Bu türde olanlara sayısal bilgisayar da denilmektedir. Dünya üzerinde kullanımı en yaygın olan bilgisayarlar aynı zamanda bir sayısal bilgisayar olan kişisel bilgisayarlardır (PC- Personal Computer). Kişisel bilgisayarlardan başka internet ağını yöneten büyük çaptaki bilgisayarlar ve avuç içine sığabilecek kadar küçük, bilgisayar işlevine sahip çok çeşitli cihazlar üretilmiştir.

Tanımlarda bulunan aritmetik ve mantıksal işlemlerin yanında otomatik olarak bilgisayarlar girdi (input), çıktı (output), saklama ve programlanma işlemleri de yapabilmektedir[13]. Verinin bilgisayara aktarılması, programın yüklemeye alınması ve işlemlerle ilgili komutların girilmesi işlemlerine girdi

---

[11] Aslı Deniz Helvacıoğlu, "Avrupa Konseyi Siber Suç Sözleşmesi-Temel Hükümlerinin İncelenmesi", **İnternet ve Hukuk**, Der: Yeşim M. Atamer, İstanbul, İstanbul Bilgi Üniversitesi Yayınları 51, Hukuk 2, Ocak 2004, s. 280.

[12] Nilgün Tosun, Aytaç Karamanlıoğlu, Tarık Yerlikaya, **Bilgisayara Giriş**, Ed: Nilgün Tosun, y.y. Kriter Yayınları, Ekim 2007, s. 4.

[13] Mustafa Balay, Neşe Erses, **Bilgisayar Kullanımı ve İnternet**, Ed: Aysan Şentürk, 2. Baskı, Bursa, Ekin Kitabevi, Kasım 2005, s. 8.

işlemi adı verilmektedir[14]. Girdi işlemlerinin yapılması, bilgisayara bağlanabilen klavye, fare (Mouse), mikrofon, disket, CD, DVD, tarayıcı vb. gibi girdi birimlerine (input unit) bağlıdır. Girilen verilerin dış ortama geri gönderilmesi işlemleri çıktı işlemi olarak adlandırılır[15]. Girilen bilgilerin birer çıktı olarak görünebilmesi için ekran, yazıcı, çizici, ses çıkışı, hoparlör vb. gibi çıktı birimlerine (output) ihtiyaç duyulur.

Bilgisayarlar verileri işlemekle kalmaz aynı zamanda onları saklayabilme veya kayıt altına alma işlemlerini yapabilmektedir. Bu sayede veriler birçok kez kullanılabilirler. Belleğin (Memory) kapasitesi ne kadar yüksek olursa o kadar kapasitede veri saklanabilir. Veri saklama işlemi, bilgisayar komutlarıyla veri saklama birimlerine yönelik yapılır.

Bir program bilgisayarın belleğine bir kez yüklendiyse tekrar yüklenmesine gerek olmayıp yeniden çalıştırılabilir. Bilgisayarlar programlar sayesinde işlemler yapabilirler. Programlarla ilgili bilgiler bilgisayar programları başlığı altında daha ayrıntılı olarak ele alınacaktır.

B- BİLGİSAYARIN TEMEL BİLEŞENLERİ (DONANIM VE YAZILIM)

Bilgisayarın fiziki ve elektronik temelini oluşturan parçaların bütününe "Donanım" (Hardware) denilmektedir[16]. Donanım bilgisayarın somut kısmını oluşturmaktadır. Donanım merkezi işlem birimi (Central Processing Unit-CPU) ve buna bağlanan diğer parçalardan meydana gelmektedir. Merkezi işlem birimi ise bir bilgisayar sisteminin beynidir ve "mikro işlemci" olarak da adlandırılmaktadır[17]. Donanıma anakart, merkezi işlem birimi, bellek türleri, (RAM, ROM ve önbellekler) yonga, sabit disk, işlemci fanı, ekran kartı, ses kartı vb. gibi bilgisayar kasası içinde bulunan parçalardan başka bilgisayar

[14] Tosun, Karamanlıoğlu, Yerlikaya, **a.g.e.**, s. 3.
[15] Tosun, Karamanlıoğlu, Yerlikaya, **a.g.e.**, s. 4.
[16] Balay, Erses, **a.g.e.**, s. 10.
[17] Balay, Erses, **a.g.e.**, s. 15.

kasası dışında bulunan monitör, fare, klavye, hoparlör gibi parçalar da dahildir[18].

Bilgisayarın çalışmasını sağlayan soyut kısmına "Yazılım" (software) adı verilmektedir[19]. Yazılım donanım gibi somut olmasa da donanımla kullanıcı arasında bir bağ kurar. Yazılım olmadan donanım tek başına bir anlam ifade etmez. Aynı şekilde donanım olmadan da yazılımın bir hükmü yoktur. İkisi birlikte olduğu sürece bir bilgisayarı oluştururlar.

Yazılım aynı zamanda program olarak da adlandırılmaktadır[20]. Lâkin yazılım programın üst bir kavramıdır. Yazılım bilgisayar programlarının toplamından oluşmaktadır. Donanımın çalışmasına ve bilgisayarın işlem yapmasına olanak sağlayan komutlar, bilgisayarın programlama dilleri, tasarımlar, işletim sistemleri ve ekranda görülen her unsur yazılım içerisindedir[21]. Yazılımları kendi içerisinde işletim sistemleri, uygulama yazılımları ve programlama dilleri olarak 3'lü bir gruplandırmaya tabi tutabilmek mümkündür[22]. Bu gruplar birer bilgisayar programı olduğundan söz konusu gruplar bilgisayar programı başlığı altında incelenecektir.

C- BİLGİSAYAR PROGRAMLARI

Yazılım, program ve veri olmak üzere iki temel bileşenden oluşmaktadır. Programdan, yerine getirilmesi bir sıra çerçevesi içerisinde istenen işlemleri belirlemek üzere tasarlanan komutlar dizisi anlaşılır[23]. Bilgisayar programları sayesinde kullanıcılar bilgisayara işlem yaptırabilmektedirler. İşlemlerin yapılabilmesi için girilen komutların bir arada ve bir dizi şeklinde olması gerekir. Bu komutlar ve diziler belli bir kurala göre yazılmıştır ve bu kurallar "programlama dili" olarak adlandırılır[24].

---

[18] Yazıcıoğlu, **a.g.e.**, s. 31.
[19] Yazıcıoğlu, **a.g.e.**, s. 31.
[20] Balay, Erses, **a.g.e.**, s. 10.
[21] Gülcü, Alan, **a.g.e.**, s. 24.
[22] Tosun, Karamanlıoğlu, Yerlikaya, **a.g.e.**, s. 53.
[23] Gülcü, Alan, **a.g.e.** s. 24.
[24] Balay, Erses, **a.g.e.**, s. 40.

Bilgisayarın açılmasını ve çalışmasını düzenleyen en temel program, işletim sistemi programıdır. İşletim sistemi işlemlerin ne şekilde yerine getirileceğini idare eden bir sistemdir. Dünyada en yaygın kullanımıyla Windows ve Linux, işletim sistemlerine birer örnektirler.

Programlar birçok alanda kullanıcıların ihtiyacı doğrultusunda işlem yaparlar. Kullanıcıların amaçlarına göre disket, CD ve DVD gibi veri saklama birimlerine kaydedilerek tasarlanan, yazılım veya bilgisayar şirketlerince piyasaya sürülen programlara paket programlar denilmektedir[25]. Bu programların kullanılmasıyla grafik, sunum, istatistik, mühendislik, oyun, animasyon, hesaplama ve tablo programları sayesinde eğitim, iş istatistik, pazarlama vb. gibi birçok alanda kolaylıklar sağlanmıştır. Kullanım amaçlarına göre birçok program türü vardır. Örneğin; kelime işlemci programıyla isteklerimiz doğrultusunda metin yazabilir, sayfa düzeni sağlayabilir, yazdıklarımız kâğıda yazdırılabilir ve yazım kontrolü yapabiliriz[26]. Örneğin; Microsoft Word gibi kelime işlem programlarında metin yazılabilmektedir. Microsoft Excel gibi elektronik tablolama programları ile elektronik hesaplamalar yapılabilir ve yapılan hesaplamalar tablo şeklinde sınıflandırılabilir. Sunma hazırlama programları ile bir konferans veya toplantıda slayt gösterileri yapılması mümkündür. Web sayfası hazırlama programlarıyla bilgisayar kullanıcısına ait bilgiler internet ortamına aktarılabilirler.

Uygulama programları genellikle şirket içi çalışmalarda basit ve etkili işlem yapabilmek amacıyla kullanıcılar tarafından meydana getirilen ve genellikle ücret-maaş bordrosu, faturalama gibi alanlarda kullanılan programlardır[27].

Bilgisayar programının ne olduğu Fikir ve Sanat Eserleri Kanunu'nun 1-B maddesinin g bendinde "*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*

[25] Gülcü, Alan, **a.g.e.**, s. 28.
[26] Gülcü, Alan, **a.g.e.**, s. 28.
[27] Balay, Erses, **a.g.e.**, s. 41.

çalışmalarını... ifade eder." denilmek suretiyle açıklanmıştır. Buradaki tanım yukarıda verdiğimiz program tanımıyla uyumlu bir tanımdır. Ek olarak "*hazırlık çalışmaları"* da bir bilgisayar programı olarak nitelendirilmiştir. Bununla birlikte FSEK md. 2/1-1'e göre bilgisayar programları ve bir sonraki evrede program sonucu doğma şartıyla yapılan hazırlık çalışmaları ilim ve edebiyat eseri sayılırlar[28].

D- VERİ

İngilizce'den "data" kelimesinin karşılığı olarak dilimize aktarılmış olan veri, "*Bilgi taşıyan herhangi bir simge, damga ya da analog bir büyüklük*" şeklinde tanımlanabileceği gibi "*Olgu, kavram ya da komutların iletişim, yorum ve işlem için elverişli biçimsel ve uzlaşımsal bir gösterimi*" denilmek suretiyle de tanımlanabilir[29]. Veri, bilgisayarın programları çalıştırabilme durumuna bağlı olarak kullandığı önbilgilerdir[30]. Bilgisayara girilen bilgiler bilgisayarın işlem yapabilmesi, yapılan işlemlerin kaydedilmesi ve kaydedilen işlemlerin yeniden değerlendirilmesi için sayısal varlıklara çevrilmektedirler. Sayısal varlıklara çevrilen bu bilgiler veriyi oluştururlar. Veriler programlarla birlikte bir bilişim sisteminin, soyut yani yazılım kısmında yer almaktadır. Verinin soyut alanda bulunması TCK'nın 243. maddesinin gerekçesinde de belirtilmiştir[31].

Veriler sayısal, alfabetik ve işaret özellikli olabilirler. Bir değer ifade etseler de ilk bakışta ne anlama geldiği anlaşılmayıp ancak bir bilişim sistemi tarafından anlaşılabilirler[32].

---

[28] İlim ve Edebiyat Eserleri başlıklı FSEK'in 2. maddesinin 1. fıkrası aynen,
"İlim ve edebiyat eserleri şunlardır:
1. Herhangi bir şekilde dil ve yazı ile ifade olunan eserler ve her biçim altında ifade edilen bilgisayar programları ve bir sonraki aşamada program sonucu doğurması koşuluyla bunların hazırlık tasarımları." şeklindedir.

[29] Emin Doğan Aydın, **Bilgisayar, Bilgi İşlem ve Telekomünikasyon Terimleri Sözlüğü**, Cilt 1, 6. Basım, İstanbul, Yalın Yayıncılık, 2007, s. 264.

[30] Gülcü, Alan, **a.g.e.**, s. 24.

[31] TCK 243. maddesinin gerekçesi aynen, *"Sistem içindeki bütün soyut unsurlar, fıkrada geçen "veri" teriminin kapsamındadır."* şeklindedir. (Özgenç, **a.g.e.**, s. 988).

[32] Kurt, **a.g.e.**, s. 39.

Ceza mevzuatındaki 2005 yılı değişiklikleri öncesinde verinin ne olduğuna ilişkin bir düzenleme bulunmamaktaydı. 4422 sayılı Çıkar Amaçlı Suç Örgütüyle Mücadele Kanunun Uygulanmasına İlişkin Yönetmelik'in 4. maddesinde tanımlanan "veri taşıyıcısı" kavramı ise bizlere verinin ne olduğuna ilişkin sadece bir ipucu vermekteydi[33]. Buna göre veri taşıyıcısı *"İletişim dinlenmesi ve tespiti ile gizleme tedbirinin uygulanması neticesinde elde edilebilecek ses ve görüntü bilgilerinin kaydedileceği disket, CD ve kaset gibi araçlardır*." şeklinde düzenlenmişti. Burada verinin tanımından ziyade nerelerde bulunabileceğinden bahsedilmekte ve veriler telekomünikasyon yoluyla iletişimin tespiti, dinlenmesi ve kayda alınması tedbirleri açısından ele alınmaktaydı[34]. Bilişimle veya bilgisayarla ilgili bir veri tanımı yapılmamıştı. Veri taşıyıcısını düzenleyen bu kanun 5320 sayılı "Ceza Muhakemesi Kanununun Yürürlük Ve Uygulama Şekli Hakkında Kanun"'un 18. maddesiyle yürürlülükten kaldırılmıştır[35].

04.05.2005 kabul tarihli 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un" tanımlar balığı altında düzenlenen 2. maddesinin "k" bendinde "*Veri: Bilgisayar tarafından üzerinde işlem yapılabilen her türlü değeri ...ifade eder.*" denilmek suretiyle verinin tanımı bilgisayarla ilişkili bir biçimde hukukumuza yerleşmiştir. Aynı durum AK-SSS'nin 1. maddesinin b bendinde; "*Bilgisayar verisi terimi bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlarda dahil olmak üzere bir bilgisayar sisteminde işlenmeye uygun nitelikteki her türlü bilgi ve konspeti ifade edecektir."* şeklinde belirtilerek veri-bilgisayar ilişkisi vurgulanmıştır[36]. Buradaki "*işlenmeye uygun*" ibaresinden verinin bilgisayar

---

[33] Veli Özer Özbek, "Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi", **İÜHFM**, Cilt LIX, Sayı 1-2, İstanbul, Beta Basım Dağıtım, 2001, s. 183.

[34] Özbek, **a.g.m.**, s. 184.

[35] 23.03.2005 Kabul Tarihli, 5320 sayılı Ceza Muhakemesi Kanununun Yürürlük Ve Uygulama Şekli Hakkında Kanun'un 18. maddesi aynen, *"d) 30.7.1999 tarihli ve 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu, bütün ek ve değişiklikleriyle birlikte yürürlükten kaldırılmıştır."* şeklindedir. (31 Mart 2005 RG).

[36] Avrupa Konseyi Siber Suç Sözleşmesi , Çev: İnternet ve Hukuk Platformu: İVHP, http://www.binbilen.org/belgeler/Siber_Suclar_Sozlesmesi.pdf (Erişim), 25 Haziran 2009. s. 3.

sistemince doğrudan işlenebilir bir biçimde olması anlaşılmaktadır[37]. Bununla birlikte sözleşme programları da bir bilgisayar verisi şeklinde ele almıştır.

Veriler yukarıda bahsedildiği gibi sadece bilgisayar verisi olarak anlaşılmamalı ve konuya daha geniş bir açıdan bakılmalıdır. Veriler elbette bilgisayarla ilişkilidir ve bilgisayarlar tarafından işlenirler. Lâkin bilgisayarlar kendi başlarına çalışabilirse de büyük sanal bilgi depolarında, CD, disket, USB flash bellekler gibi çeşitli birimlerde de veriler saklanabilir. Adli bilişimin çalışma alanı olan veri araştırması sadece bilgisayar üzerinde yapılmamakta, veri saklama birimlerine de uygulanmaktadır. Dar bir yorum elektronik yapıdaki delillerin elde edilmesini yalnızca bilgisayarla sınırlayacaktır. Bu bakış açısı veri saklama birimlerinin araştırılmasını engelleyecektir.

II- ADLİ BİLİŞİM VE ELEKTRONİK DELİL

A- ADLİ BİLİŞİM

1- Genel Olarak

Dilimize İngilizce'den çevrilen "Bilgisayar Kriminalistiği-*Computer Forensic*" kavramı "*Adli Bilişim*" olarak adlandırılmıştır. Her ne kadar yapılan bu adlandırma farklı olsa da adli bilişim kriminalistik[38] incelemelerinden ayrı bir alan oluşturmamaktadır[39].

Adli bilişim bir adli bilim dalıdır. Adli bilim, tıp, sosyal, fen, mühendislik, vb. gibi mesleki bilginin adli görev ve hizmetlerde kullanılmasını amaç edinmiştir. Adli bilimler kendi içerisinde fen bölümleri, tıp-sağlık bölümleri, sosyal bölümler, kriminalistik bölümler olmak üzere çeşitli bölümlerden oluşmaktadır. Adli bilişim alanı ise kriminalistik bölümü içerisinde yer alır.

---

[37] Helvacıoğlu, **a.g.m.**, s. 281.

[38] *"Kriminalistik; suç ve suçlunun bilimsel yöntem ve araçlar kullanılarak tesipit edilmesi, belirlenmesi, suçun aydınlatılması ve suç analizinin yapılmasıdır."* (Mustafa Kaygısız, **Adli Bilimler Suç Analizi**, Ankara, Adalet Yayınevi, 2008, s. 9).

[39] Ahmet Hakan Ekizer, **Adli Bilişim (Computer Forensics-Bilgisayar Kriminalistiği)**, (Erişim) http://www.bilgisayarpolisi.com/index.php?sayfa=makaleoku&kategori=11&135, 10 Temmuz 2009, s. 1.

Başka bir açıdan adli bilişim kendine özgü ilkeleriyle bilişim teknolojisinin gelişimi sonucunda ve her zaman yenilenen standartlarıyla çoklu-disiplinli yeni bir bilim dalı olarak da nitelendirilmiştir[40].

Adli bilişim bir suç dolayısıyla yapılan soruşturmada, maddi gerçeğe ulaşabilmek için elektronik birimlerde bulunabilecek suçla ilgili delillerin bozulmadan veya yok edilmeden anlaşılabilir ölçüde adli mercilere sunulmasını uygun hale getiren, belirli bilimsel-teknik prensiplerin uygulamaya konulduğu, delillerin incelenmesi sürecine verilen addır[41]. Adli bilişim, elektronik cihazlarda bulunabilecek davacı veya davalının iddialarını kuvvetlendiren veya çürüten bilgilerin mahkeme önüne konulması için yapılan bir inceleme faaliyeti olarak da tanımlanmaktadır[42]. Adli bilişim erişilen bilişim sistemlerinde, ağlarda, uygulamalarda ve diğer bilişim özellikli kaynaklarda bulunan bilginin toplanması, işlenmesi, sunumu ve analizi veya bilişim sistemlerine saldırının kaynağının tespiti ile ilgilenmektedir[43]. Suçun önlenmesiyle ilgili çalışmalardan ziyade suçun işlenmesinden sonraki aşamalarda delillerin toplanmasını göz önüne alır[44]. Adli bilişim olayın ispatlanmasında yararlı olabilecek elektronik delillerin incelenmesine imkân sağlayan laboratuar çalışmalarını da kapsamaktadır.

Verilerin kurtarılması, imha edilmesi, saklanması, dönüştürülmesi, şifreleme, şifreleri çözme, gizli dosya bulma vb. gibi birçok işlemler adli bilişimin çalışma alanı olarak kabul edilir[45]. Bu çalışma alanlarındaki faaliyetler adli bilişimin hem olay yeri incelemesi hem de laboratuar kısmında yer alan veri inceleme ve veri kurtarma servislerinde yürütülmektedir.

Adli bilişimin incelemeye konu olabilecek kaynakları çok çeşitlidir. İnternet kullanımları, bilişim suçları, fikri hakların konumu, şirket stratejisi

---

[40] Gökhan Ahi, "Adli Bilişim Nedir ?" **Güncel Hukuk Dergisi**, Mart 2009, (Erişim), http://www.ahi-gurler-taygun.av.tr/?adli-bilisim-nedir-av.-m.gokhan-ahi,52, 11 Temmuz 2009. s. 1.

[41] Ekizer, **a.g.m.**, s. 1.

[42] Leyla Keser Berber, **Adli Bilişim**, Ankara, Yetkin Yayınları, 2004, s. 39.

[43] Joel Weise, Brad Powel, "Using Computer Forensics When Investigating System Attacks", April 2005, (Erişim), www.sun.com/blueprints/0405/819-2262.pdf, 09 Temmuz 2009, s. 3.

[44] Semih Dokurer, "Adli Bilişim"**, Ses Görüntü ve Data İncelemeleri**, Ed: Levent Bayram, Ankara, Adalet Yayınevi, 2008. s. 245.

[45] Aydoğan Tan, "Adli Bilişim", 26 Haziran 2009, (Erişim) http://www.hukuksokagi.com/makale/adli-bilisim-computer-forensic.html, 09 Temmuz 2009, s. 2.

ihlali, internet kullanılarak şeref ve haysiyete karşı fiiller, kurumsal yaşama müdahaleler, sistem suiistimalleri gibi durumlar adli bilişimin birer inceleme kaynağı olarak görülmektedir[46]. İşletilen süreç sonunda elde edilen deliller, suç şüphesiyle başlatılan ceza muhakemesinde, (kasten adam öldürme, örgütlü suçlar, uyuşturucu madde ticareti, şantaj, zimmet, dolandırıcılık, çocuk pornografisi vb. gibi.) özel hukuka ilişkin uyuşmazlıklarda, (boşanma, ayrımcılık, kişiliğin korunması vb. gibi.), ticari alanda yaşanabilecek hukuka aykırılıklarda (zimmete para geçirme, ihaleye fesat karıştırma, ticari sırların ve şirketiçi bilgilerin sızdırılmış olup olmadığını belirlemek amacıyla) veya davada tarafların kendi iddialarını kuvvetlendirme amacıyla kullanılabilmektedir[47].

2- Adli Bilişim Uzmanı

Bu alanda çalışma yapabilmek ve bilgi saklayan veya ileten birimlerdeki delillere ulaşabilmek için bir takım aletlere ve tekniklere ihtiyaç duyulmuştur[48]. Bu aletleri ve teknikleri ancak iyi eğitimli adli bilişim uzmanları kullanabilirler.

Bilişim teknolojisinin ilerlemesi doğal olarak özel bir dil doğurmuştur. Bu nedenle adli bilişim uzmanları, çalıştıkları aşamaları ve elde ettikleri bilgileri bu özel dili bilmeyen veya çok az bilen kişilere özel dili kullanmadan yazılı bir şekilde sunmakla görevlidir[49]. Bir bilgisayardan veya elektronik cihazlardan bir delilin nasıl elde edileceği ve mahkemeye nasıl sunulacağı konusunda adli bilişim uzmanlarının yapacağı çalışmalar çok önemlidir. Bu uzmanlar bilişim teknolojisi üzerine iyi bir bilgi birikimine sahip olup bilgisayar

---

[46] Berber, **a.g.e.**, s. 40.
[47] Berber, **a.g.e.**, s. 76, 77.
[48] Erin Kenneally, "Computer Forensics" **Login**, Berkeley, The Magazines of Usenix&Sage, August 2002, (Erişim), http://www.usenix.org/publications/login/2002-08/pdfs/kenneally.pdf, 11Temmuz 2009, s. 8.
[49] Yunus Balı, "Adli Bilişim Rapor Metinlerinin Yargılama Sürecinde Kullanımı Ve Anlamlandırabilirliği", **Ses Görüntü ve Data İncelemeleri**, Ed: Levent Bayram, Ankara, Adalet Yayınevi, 2008. s. 231.

ve diğer elektronik cihazlardan delil elde etme konusunda eğitimlidirler ve bunun yanında hukuki bilgilere de sahiptirler[50].

Adli bilişim uzmanları inceleyeceği bilgisayarın veya veri saklama birimlerinin özelliklerini, elektronik verileri elde etmede veya verilerin kurtarılmasında kullanacağı programları, adli bilişim alanında kabul edilen bir takım standart ve protokolleri iyi bilmeli; Hukuk Usulü Muhakemeleri Kanunu ve CMK'daki bilirkişilik kurumuna ve delil konusuna hakim olmalıdırlar[51].

Bilişim Ağı Hizmetlerinin Düzenlenmesi Ve Bilişim Suçları Hakkında Kanun Tasarısı'nda adli bilişim uzmanlarının ancak yetki belgesi alarak bilirkişilik yapabileceği; adli bilişim uzmanlığının ve yetki belgesiyle ilgili hususların yönetmelikle düzenleneceği ve 5271 sayılı CMK'daki bilirkişilik düzenlemelerinin bu konuda genel bir norm olduğu vurgulanmıştı[52]. Ancak tasarının sonraki metinlerinde adli bilişim uzmanlarıyla ilgili düzenlemeler tasarıdan çıkarılmıştır. Şu anda adli bilişim uzmanıyla ilgili ceza mevzuatında veya başka bir mevzuatta mevcut bir düzenleme bulunmamaktadır.

İyi bir adli bilişim uzmanı bu alanda geçerli kabul edilen bir takım sertifikalara sahip olmalıdır. Adli bilişim uzmanları aldıkları eğitim sonucu ENCE (Encase Certified Examiner), CCE (Certified Computer Examiner), CCCI (Certified Computer Crime Investigator), CFCE (Computer Forensic Computer Examiner) vb. gibi sertifikalar edinirler[53]. Bu sertifikalar onları diğer bilişim sistemi uzmanlarından ayıracak ve davalarda bilirkişilik yapmalarını kolaylaştıracaktır.

Bilgisayar ve elektronik cihazlardan adli bilişim uzmanlarının uygulayacakları adli bilişim yöntemleriyle veya diğer teknik incelemelerle delil elde edilebilir. Adli bilişimde bilgisayardan delil elde etme basit bir yöntem

---

[50] Bu bakımdan adli bilişim uzmanları IT (Information Technology) uzmanlarından farklıdır. IT uzmanları zarar görmüş bilgisayar bileşenlerini düzeltme ve sistemlerin çökmeyle tehlikesi karşısında yeniden yükleme işlemlerini delilin zarar görmesi veya kaybolma risklerini gözönüne almadan yaparlar. Bunun yanında IT uzmanları hukukçu bir bakış açısına sahip değildirler ve meselelere faydacı bir şekilde yaklaşırlar. Bkz. Berber, **a.g.e.**, s. 41.

[51] Leyla Keser Berber, "Adli Bilişim Uzmanı Kimdir? -1" (Erişim) http://turk.internet.com/haber/yazigoster.php3?yaziid=16731, 12 Temmuz 2009. s. 1.

[52] Berber, "Adli Bilişim Uzmanı Kimdir? -1" s. 1.

[53] Ahmet Hakan Ekizer, "Adli Bilişim Uzmanlığı Sertifikasyonları", 16 Ekim 2008, (Erişim) http://www.bilgisayarpolisi.com/index.php?sayfa=makaleoku&kategori=11&id=136, 30 Temmuz 2009. s. 1.

olmayıp üzerinde dikkatle durulması gereken bir takım süreçlerden oluşmaktadır. Söz konusu bu sürecin incelenmesinden önce elektronik verilerin delil olup olamayacağı hususuna bakılacaktır. Bu hususa değinilmesi süreçte yer alan prosedürlerin daha iyi anlaşılmasını sağlayacaktır.

B- ELEKTRONİK DELİL

1- Genel Olarak

Elektronik delil, elektronik bir cihaz üzerinde saklanabilen veya bu cihazlar aracılığıyla iletibilen muhakeme bakımından değeri olan bilgi ve verilerdir[54]. Söz konusu tanımda, elektronik delillerin bulunabileceği yerler ile iletimde ve muhakeme sürecinde kullanılabilme özelliklerine işaret edilmiştir.

Elektronik delil ve dijital delil kavramları genellikle birbirlerinin yerine kullanılmaktadır. Bu iki kavramın, bilişim sistemlerindeki donanım ve yazılım ayrımı nedeniyle ayrı durumları ifade ettiği ileri sürülmüştür[55]. Özellikle Amerika Birleşik Devletleri'nde hukukçular ve adli bilişim uzmanları ağırlıklı olarak dijital delil (digital evidence) terimini kullanmaktadırlar.

Dijital delliler veya diğer bir ismiyle sayısal deliller sayıyı temel almaktadır. Bu nedenle dijital deliller elektronik delillerden farklıdır. Bunun kökenine bakıldığında bilimsel manada elektronik, elektronların hareketleriyle bu hareketlere uygun devreler yapmasıyla ilgilenmektedir[56]. Dijital, sayı ile ilgilenen bir terimdir. Elektronik alanında, analog (örneksel) elektronik ve dijital (sayısal) elektronik olmak üzere ikili bir gruplandırma yapılması mümkündür[57]. Böylelikle dijital kavramı, elektronik kavramının alt bir başlığı olmaktadır. Dolayısıyla elektronik teriminin dijital terimine kıyasla daha üst bir kavramı karşılamakta olduğunu belirten görüşe[58] katılmaktayız. Buna ek

---

[54] Berber, **Adli Bilişim**, s. 46.

[55] Kubilay Say, "Bilişim Suçlarında Olay Yeri İncelemesinin Hukuki Boyutu", **Ses Görüntü ve Data İncelemeleri**, Ed: Levent Bayram, Ankara, Adalet Yayınevi, 2008, s. 255.

[56] Ali Karagülmez, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, 2. Bası, Ankara, Seçkin Yayıncılık, 2009, s. 32.

[57] Karagülmez, **a.g.e.**, s. 32.

[58] "*Elektronik"; 1- Analog (örneksel) 2-Dijital (sayısal) olarak iki kısımda ele alınmaktadır. ... Görülüyor ki "dijital" yapı, "elektronik" yapının kapsamı içerisinde kalmaktadır. Her dijital*

olarak TCK'nın 6. maddesinin 1 fıkrasının g bendinde, CMK'nın 43. maddesinin 2. fıkrasında (elektronik posta) ve 4077 sayılı Tüketicilerin Korunması Hakkındaki Kanunun 3/c ve 9/A maddelerinde (elektronik ortam) "elektronik" terimine yer verilmiştir. Çalışmamızda terim birliğini sağlamak için E-imza, e-ticaret, e-posta, e-devlet, e-keşif terimlerinden ilham alarak e-delil yani elektronik delil terimi dijital delilleri içerecek bir biçimde kullanılacaktır. Ayrıca yayınlanan birçok makalede "elektronik delil" terimine rastlanılmaktadır.

Elektronik delilin temelini; bilgisayar ve bilgisayar sistemlerinde bulunan, suç veya uyuşmazlıkla ilgili olan, veriyi ifade eden her türlü bilgi veya değer oluşturmaktadır. Bilişim sistemlerinde veya veri saklama birimlerinde, suçun ispatına yarayan ve çok değişik biçimlerde saklanabilen veriler ve buna bağlı olarak da deliller bulunabilir. Elektronik deliller her çeşit veri kaydıyla, dosya kaynak şifreleriyle, yazılımlarıyla veri saklama birimleriyle ve bu türdeki birçok birimle ilişkilidir[59].

Elektronik deliller DNA incelemesinden elde edilen delillere benzer şekilde görünmez ve gizli niteliktedir. Elektronik delillerin elle tutulamaması, gözle görülememesi daha geniş bir anlatımla duyularla algılanmasının mümkün olmaması nedeniyle incelenmesi, ancak uygun teçhizat ve aletlerin yardımıyla olabilecektir[60]. Yanlızca teçhizat ve alet yeterli olmayıp delil araştırmasına özel olarak hazırlanmış bir takım yazılımlara da ihtiyaç vardır.

Elektronik deliller hassas bir yapıya sahiptir. Hatalı bir işlem veya hatalı bir hareket sonucunda zarar görebilme veya yok edilebilme risklerinden dolayı toplanması, muhafazası ve incelenmesi için bir takım özel önlemler öngörülmüştür[61]. Bilgisayardaki elektronik deliller üzerinde çalışma yapılması mümkündür. Ancak inceleme yapılırken delilin bozulması, hata ile silinmesi

---

yapı, aynı zamanda elektroniktir; fakat her elektronik yapı aynı zamanda dijital değildir. Bu açıdan "elektronik" kelimesi "dijital"e göre, daha üst bir nitelik taşımaktadır." (Karagülmez, **a.g.e.**, s. 33).

[59] Basri Aktepe, "Emniyet Personelinin Bilgisayar ve Bilgisayarla İlintili Suçlarla Mücadelede Dikkat Edilmesi Gereken Hususlar", **1. Polis Sempozyumu**, Ankara, EGM Bilgi-İşlem Daire Başkanlığı, 2003, s. 67.

[60] Say, **a.g.m.**, s. 256.

[61] Berber, **a.g.e.**, s. 44.

virüs kapması gibi çeşitli tehlikelerin potansiyel varlığı elektronik delilin bir imaj yöntemiyle[62] kopyasının alınmasını ve bu alınan kopya üzerinden çalışma yapılmasını gerektirebilir[63]. Elektronik veri, elektrik akımıyla ortaya çıkan elektrik akımının kesilmesiyle ortadan kaybolan bir bilgi olduğundan, delil olarak mahkemeye taşınmasında güçlükler yaşanabilmektedir[64]. Bu nedenle elektrik enerjisinin kesilmesi riskine bağlı olarak veriler, dijital bir biçimde veri saklama birimlerine manyetik saklama teknolojisiyle kaydedilmelidir[65]. Doğası gereği değişken, maddi olmayan ve geçici olabilen elektronik delillerin elde edilme yöntemleri, fiziksel delillerin elde edilmesinde kullanılan yöntemlerden ayrı bir nitelik taşımaktadır[66].

Elektronik deliller yukarıda bahsedilen risklere rağmen fiziksel delillerle karşılaştırıldığında bir takım avantajları bünyesinde barındırmaktadır. Elektronik delillerin kolaylıkla kopyalanabilmesi; kopya üzerinden inceleme yapılabilmesi; doğru alet ve programlar yardımıyla kopya-orijinal karşılaştırılması yapılarak elektronik delilin değiştirilip değiştirilmediğinin anlaşılabilmesi; silinmesi kolay gözükse bile silinen dosyaların geri getirilebilmesi; şüphelilerin veya sanıkların elektronik delili yok etmeye çalıştıklarında bir kopyasının görünmeyen yerlerde saklanabilmesi bu avantajlara birer örnektir[67].

2- Elektronik Delilin Ceza Muhakemesindeki Yeri

Ceza muhakemesinde maddi gerçeğe ulaşabilmek için elde edilen her şeyin delil olabilmesi, delillerin serbestliği ilkesiyle açıklanır. Delillerin

---

[62] *"İnceleme için alınan birebir kopyaya bilgisayar kriminalistiği'de İmaj (Forensic Image) adı verilmektedir."* (Ekizer, **Adli Bilişim (Computer Forensics-Bilgisayar Kriminalistiği).**, s. 10).
[63] Dokurer, **a.g.m.**, s. 244.
[64] Dokurer, **a.g.m.**, s. 241.
[65] Say, **a.g.m.**, s. 256.
[66] Kenneally, **a.g.m.**, s. 9.
[67] Eoghan Casey, **Digital Evidence and Computer Crime**, y.y. Academic Press, 2000, s. 5.

serbestliği ilkesi ile delillerin serbestçe değerlendirilmesi ilkesi ceza muhakemesinde vicdani delil sistemini oluştururlar[68].

Ceza muhakemesinde elektronik deliller nitelikleri gereği bilimsel delil türü olarak kabul edilirler. Vicdani delil sistemi bugün ceza muhakemesinde yürürlülüktedir ve bilimsel delil sistemine tam olarak geçilememiştir. Kriminalistik bilimlerin gelişmesi halinde bilimsel delil sistemine geçiş kolaylaşacaktır. Bilimsel delil sistemi, vicdani delil sistemini zayıflatmakta ve giderek onun yerini almaktadır[69]. Bununla birlikte vicdani delil sistemi bilimsel metodların kullanılmasına engel değildir. Vicdani delil sistemiyle hakim her türlü delili değerlendirebilir ve bilimsel metodlara yardım için başvuruda bulunabilir[70]. Vicdani delil sisteminde hakimin hüküm verirken keyfi durumların ortaya çıkabileceği ve bilimsel delillerin bu durumlara engel oluşturacağı ifade edilmektedir[71].

Bilimsel delillerin konusunu belirti delilleri oluşturur. Kendi içerisinde bir tutarlılığı olsa da bilimsel delillere daima şüpheyle yaklaşılmalıdır. Şüphe yenilinceye kadar delil üzerinde bilimsel metodlar tekrar tekrar uygulanmalı ve ulaşılan sonuç hep aynı ise bu sonuç esas alınmalıdır[72].

Elektronik cihazlardan elde edilen deliller, ilk bakışta anlaşılır olmasa da çözümleme yapıldıktan sonra ceza muhakemesindeki delilin özelliklerini taşımalıdır. Elektronik delil olayı yansıtmalı, akla ve mantığa uygun olmalıdır. Aynı zamanda gerçekçiliğe önem verilmeli, önceden düzenlenen prosedürlere uygun şekilde elde edilmeli ve hukuka aykırılık taşımamalıdır.

Bir görüşe göre bilgisayardan elde edilen veriler muhakemede; bilgisayar verilerin değiştirilebilir nitelikte olması ve irade açıklamasını tam olarak yansıtmaması nedeniyle delil olarak kullanılmamalıdır[73]. Başka

---

[68] Ayrıntılı bilgi için bkz. Cumhur ŞAHİN, **Ceza Muhakemesinde İspat (Delillerin Doğrudan Doğruyalığı İlkesi)**, Ankara, Yetkin Yayınları, 2001.

[69] Mahmut Koca, "Ceza Muhakemesi Hukukunda Delilller", **CHD,** Yıl: 1, Sayı: 2, Seçkin Yayınevi, 2006, s. 209.

[70] Nurullah Kunter, Feridun Yensisey, Ayşe Nuhoğlu, **Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku**, 16. Bası, İstanbul, Beta yayınevi, Ocak 2008, s. 624.

[71] Kunter, Yenisey, Nuhoğlu, **a.g.e.**, s. 624.

[72] Kunter, Yenisey, Nuhoğlu, **a.g.e.**, s. 625.

[73] Özbek, **a.g.m.**, .s. 186.; Aynı yönde bkz. İsmail Ergün, **Siber Suçların Cezalandırılması ve Türkiye'de Durum**, Ankara, Adalet Yayınevi, 2008, s. 44.

delillerle desteklenmelidir. Bu görüşe göre bilgisayardan elde edilen veriler sadece belirti şeklinde tanımlanabilir. Şüphelinin veya sanığın bu delillerin başkası tarafından konulmuş olabileceğini (örneğin polis tarafından) ileri sürebilmeleri ihtimal dahilindedir. Bu husus dijital delillerin doğrulanması problemini gündeme getirmektedir[74].

Günümüzde yaşanan teknolojik ilerleme sayesinde bir bant kaydındaki ses üzerinde bir bozulma meydana gelip gelmediği ve sesin kime ait olduğu belirlenebilmektedir[75]. Bu cihazların hukuka uygun bir şekilde elde edildikleri, cihazlar üzerinde herhangi bir tahrifatın bulunmadığı ve içeriğinin doğru olduğu saptanabiliyorsa muhakemede tek başına delil olarak kullanılmaları için herhangi bir engel yoktur[76]. Aynı şekilde bilgisayardaki verilerin değiştirilebilir olmasına karşılık verilerin değiştirilip değiştirilmediği son yıllarda buna bağlı olarak gelişen yazılımlar sayesinde anlaşılmaktadır. Kanımızca veriler, adli bilişim sürecinin uygulanmasıyla veya bu süreç uygulanmadan elde edilen verilerin bütünlüğü ve güvenliği teknik bir inceleme sonucunda ispat edilebiliyorsa delil olarak kabul edilebilirler. Lâkin teknik inceleme yapılırken elektronik veriler üzerinde hangi işlemlerin yapıldığı ayrıntılı bir şekilde kaydedilmelidir. Adli bilişim süreci ve teknik incelemeler uygulanmadan elde edilen veriler sadece belirti hükmünde kalacaktır. Diğer delillerle desteklenmeden sadece buna dayanarak mahkumiyet hükmü verilmemelidir. Elde edilenler üzerinde hukuka aykırılık veya bir bozma şüphesi varsa belirti delili olarak da kabul edilmeleri mümkün değildir. Buna karşılık vicdani delil sisteminin unsurlarından biri olan delillerin serbest değerlendirilmesi ilkesi gereği; hakim tarafından yapılacak değerlendirmenin, hem belirtiler hem de elektronik deliller bakımından saklı olduğu unutulmamalıdır.

---

[74] Yusuf Uzunay, Mustafa Koçak, "Bilişim Suçları Kapsamında Dijital Deliller", **Akademik Bilişim Konferansı**, Gaziantep, Şubat 2005, (Erişim), http://www.ii.metu.edu.tr/~yuzunay/Download/ab05.pdf, 12 Haziran 2009, s.3. ; (zikreden; Chet Hosmer, "Providing The Integrity of Digital Evidence With Time", International Journal of Digital Evidence, Volume I, Spring 2002).

[75] Koca, **a.g.m.**, s. 218.

[76] Koca, **a.g.m.**, s. 218.

3- Elektronik Delil Elde Etmede Uygulanan Süreçler

Elektronik delil elde etme süreci yani adli bilişim süreci, olay yeri inceleme esaslarına benzemektedir. Bu süreç sonunda görünmez nitelikte olan elektronik deliller görünür hale gelmekte ve anlaşılabilir olmaktadır. Süreç içerisinde elektronik delilin değiştirilip değiştirilmediği veya tahribata uğrayıp uğramadığı da saptanabilmektedir.

Elektronik verinin olay yerinden mahkeme önüne anlaşılabilir bir şekilde delil olarak gelebilmesi için uygulanan adli bilişim süreci beş basamaktan oluşmaktadır. Bunlar: toplama, inceleme, analiz, belgeleme ve raporlama basamaklarıdır. Bu basamaklar bir sıra halinde takip edilmelidir.

Toplama basamağı olay yerinden elektronik verilerin toplanmasını konu edinmektedir. Olay yerinden elektronik verilerin toplanması bu basamağın en önemli bölümüdür. Bu bölüm üzerinde iyi bir şekilde ve titizlikle durulursa diğer basamakların işletilmesindeki başarı oranı artacaktır[77]. Delillerin toplanmasında hukuka aykırılık iddiasıyla karşılaşmamak için kanunda öngörülen şartlara uyulmalıdır. Olay yeri incelemede nasıl olay yeri koruma altına alınıyorsa adli bilişimin toplama basamağında da bilgisayar, bilgisayara bağlı olan birimler ve veri saklama birimleri koruma altına alınmalıdır. Adli bilişim uzmanlarından ayrı olarak bilgisayara ve veri saklama birimlerine olayla ilgisi olan veya olmayan üçüncü bir kişi yaklaştırılmamalıdır[78]. Delil elde etmek için bilgisayarda yapılacak olan incelemeler teknik bilgi gerektirdiği için sadece bu teknik bilgiyi bilenler iş başında olmalıdır. Bu tür önlemlerin alınmasındaki amaç, sistem akışının sürdürülmesi; araştırma boyunca sistemin (bilişim sistemi) bozulmasının engellenmesi; olabilecek yanlışlıkların azaltılması; sistemin birebir kopyasının korunmasıdır[79].

Toplama basamağında elektronik delillerin yeri tespit edilirken olay yerinin fotoğrafının çekilmesine başvurulmalı, gerekirse kamera kaydı

---

[77] Dokurer, **a.g.m.**, s. 243.
[78] Mustafa Kaygısız, **Suç Yeri Ve Delil Güvenliği**, Hukuk Yayınları Dizisi-295, y.y., Adalet Yayınevi, Ekim 2007, s. 294.
[79] Weise, Powel, **a.g.m.**, s. 18.

kullanılmalı, diğer bulgularla karışmasını önlemek için tanımlayıcı bilgiler yazılmalı, bilgisayarlara ve veri saklayabilen bütün elektronik cihazlara bakılmalıdır[80]. Bilgisayar ve veri saklama birimleri toplanırken paketleme ve nakliyesine çok dikkat edilmeli ve bunun için özel teçhizat edinilmelidir. Elektronik deliller statik elektrikli bir yapıda olduğundan, bir bilgisayar ve manyetik tarzdaki veri saklama birimleri statik elektrikten etkilenmeyecek paketler içerisine yerleştirilmeli veya plastik çantalar içerisine konulmalıdır[81]. Bu paketler çantalar veya özel kutular toz, nem ve ısı geçirmemeli ve fiziksel zararlara karşı koruyucu olma niteliklerini taşımalıdır. Bilgisayar ve veri saklama birimleri bu paketlere, çantalara veya özel kutulara konuluyorsa birbirleriyle karışmaması için üzerlerine tanımlayıcı bilgiler içeren etiketler yapıştırılabilir. Paketlerin izinsiz açılmaması için mühürleme yapılacaktır.

Toplama basamağı imaj yönteminin uygulanmasından sonra bitmiş olur ve bir sonraki basamak olan inceleme basamağı başlar. İnceleme basamağı delilin gözle görülebilir hale gelmesini ve delil odaklarının açıklanmasıyla ilgilidir. İleride açılacak soruşturmada delil olarak bozulmuş, saldırıya uğramış bilgisayarların asıl durumuna erişilmesi ve bunun yanında aranabilen, soruşturulabilen ve analize tabi tutulan sistem kopyasının ayrılması bu basamağın önemli amaçları arasındadır[82]. Gizlenmiş bilgiler de dahil olmak üzere tüm bilgilerin görünebilir duruma getirilmesi bu basamakta ele alınmaktadır[83].

İnceleme asıl birimlerin kendisinde değil; imaj yöntemiyle alınan kopyalar üzerinde yapılmalıdır. Yukarıda ifade edildiği gibi elektronik deliller hassas bir yapıya sahip olup kolaylıkla bozulabilir ve değiştirilebilir. İnceleme ve analiz basamaklarında bilgisayardan elde edilen elektronik verinin

---

[80] Osman Nihat Şen, "Adli Bilişim Bilimi ve Diğer Bilimlerle Olan İlişkisi", 01 Mayıs 2007, (Erişim) http://www.bilgisayarpolisi.com/index.php?sayfa=makaleoku&kategori=11&id=121, 29 Temmuz 2009, s. 4.

[81] Servet Yetim, "Dijital Kanıt Araştırma Yöntemleri", **İstanbul Barosu Dergisi**, Cilt: 82, Sayı: 3, 2008, (Erişim) http://www.istanbulbarosu.org.tr/yayinlar/BaroDergileri/ibd/20083/ibd2008312.pdf, 24 Haziran 2009, s. 1207.

[82] Weise, Powel, **a.g.m.**, s. 19.

[83] Berber, **a.g.e**., s. 45.

değişime uğrayıp uğramadığını tespiti için dilimize İngilizce'den özetleme işlemi olarak çevrilen "hashing"[84] yapılacaktır[85].

Asıl birimlerde (örneğin sabit disk) yapılan araştırmalar, veri sayısını değiştirebilme ihtimalini taşımaktadır. Veri sayısının değişmesi halinde müdafi, sonradan buna delil eklendiğini ileri sürebilme imkanını elde etmiş olacaktır. Bu durum delilin ispat gücünü ve dolayısıyla muhakemede savcının iddiasını zayıflatacaktır. En küçük tek bir veri parçasının değişmesiyle birimin önceki özetiyle sonradan çıkarılan özeti arasındaki matematiksel değer birbirinden farklılık arz edecektir. Bu farklılığın meydana gelmemesi için analiz basamağına varmadan önce birim üzerinde kesinlikle bir özetleme (hashing)[86] işlemi yapılmalı ve asıl birim, veri değişmesine engel olunacak ortamlarda tutulmalıdır. Sonradan yapılan bir özetleme işlemi sonucunda elde edilen matematiksel değer, önceki değerle aynı ise verinin sonradan eklenmemiş ve değişmemiş olduğu sonucuna ulaşılır[87]. Öte yandan adli bilişim uygulanmadan delil elde edilmesi söz konusu olursa bu durum veri sayısını değiştirse bile sadece arama işlemi yapıldığı ve hangi verilerin kopyalandığı kaydedilmişse bu işlemler sonucunda elde edilen veriler de delil hükmünde olabilir. Çünkü bilgisayarlara sonradan veri konulsa bile hangi tarihte ve nasıl yapıldığı teknik bir inceleme sonucu ispat edilebilmektedir.

İnceleme basamağında bir takım aksaklıklar söz konusu olursa veya kötü bir ihtimalle incelenecek kopya birim bozulsa dahi aslından imaj yöntemiyle yeni bir kopya alınabilir[88]. İnceleme basamağında delil

---

[84] "*Basitçe "hash" gönderilecek verinin (bilginin yada mesajın) belili bir fonksiyona sokulup, matematiksel olarak tek bir sonuç elde edilmesidir.*". ; (Evren Şen, "Kriptografi ve Kullanım Alanları I", (Erişim), http://www.scribd.com/doc/2581535/Kriptografi-ve-Kull-Alan-I, 17 Eylül 2009, s. 7); "*Hashing işlemi de öyle bir işlemdir ki, bununla sıkıştırdığınız veriler (hash value), yani evraka yazdıklarınız, adeta bir sürü yerinden yırtılıp bir küçük boyuta (***message…** *mesaj özeti) indirilmekte, bir tür yığın teşkil etmektedir."* (H. Vedat Gürer, "Hukukçu Gözüyle Sayısal İmza, Sayısal Kimlik, Sayısal Evrak ve Sayısal Sözleşme", (Erişim) http://www.bilisimrehber.com.tr/arastirma/tr_arastirma_vedat_gurer_1.phtml, 18 Eylül 2009, s. 6).

[85] Dokurer, **a.g.m.**, s. 244.

[86] Harun Şeker, "Adli Analiz İşlemlerine Başlamak", (Erişim) http://www.cehturkiye.com/adli_analiz_islemleri.pdf, 27 Temmuz 2009. s. 1 ve 2; Özetleme "Hashing" işlemlerinde MDI5 ve SHA1 gibi algoritmalar kullanılmaktadır. Bu iki algoritmatik fonksiyonlar sayesinde başarılı bir özetleme işlemi yapılabilecektir.

[87] Dokurer, **a.g.m.**, s. 244.

[88] Şeker, "Adli Analiz İşlemlerine Başlamak", s. 1.

bütünlüğünün korunması ve laboratuar çalışmalarındaki delil olabilecek verilerin başka verilerle karıştırılmaması ve delillerin değişikliğe uğramaması amaçlanmaktadır.

Analiz basamağında bir araştırma ekibinin rolü söz konusudur. Elektronik delilin davada neyi ispat edip neyi etmeyeceği sorularına cevap aranır ki bu açıdan analiz basamağı, inceleme basamağından farklıdır. Analiz basamağındaki en büyük sorunlardan birisi incelenen verilerin sınırlandırılması konusudur[89]. İncelenecek verilerin sınırlandırılması dava ile ilgisi olmayan verilerin elenmesi anlamına gelmektedir[90]. Örneğin bir veri olayı desteklemiyorsa veya başka bir olayla ilgiliyse araştırma planının tekrar gözden geçirilmesi gerekecektir[91].

Analiz basamağında gerekli olan yazılımlar ve teçhizatlar kullanılır. Delilin soruşturma bakımından uygun olup olmadığını saptayabilme bakımından delilin özelliklerine veya bulunduğu ortamlara göre ardışıklı ve farklı modelleme örneklerine rastlamak mümkündür. Öte yandan modelleme örnekleri sadece analiz basamağında değil tüm adli bilişim süreci bakımından (tüm basamakları içerecek şekilde) elektronik delillendirme döngü modeli olarak da gösterilmektedir[92]. Kısaca hem analiz basamağı için hem de bütün adli bilişim süreci için modelleme örnekleri oluşturulmuştur. Bu modelleme örneklerinin çeşitliliği elektronik delil türlerinin sürekli bir şekilde genişlemesi nedeniyledir. Sonuç olarak farklı yazılımlardan yararlanmak; işletim sistemlerinin ve bilgisayarın özelliklerine göre farklı yazılımlar kullanmak, analiz basamağındaki çalışmaların etkin ve hızlı bir şekilde olmasını sağlayacaktır[93].

Belgeleme basamağında elektronik delillerle ilgili davada kullanılacak belgelerin tespit edilmesi, oluşturulması ve hazır hale getirilmesi işlemleri

---

[89] Joseph C. Sremack, "Formalizing Computer Forensic Analysis: A Proof-Based Technology", **Department of Computer Science**, Raleigh, 2004, (Erişim), http://www.lib.ncsu.edu/theses/available/etd-03312004-230130/unrestricted/etd.pdf, 28 Temmuz 2009. s. 24.
[90] Sremack, **a.g.m.**, s. 23.
[91] Sremack, **a.g.m.**, s. 23.
[92] Uzunay, Koçak, **a.g.m.**, s. 4. ;
[93] Aktepe, **a.g.m.**, s. 69.

uygulanır. Bu basamak raporlama basamağının alt yapısını oluşturur. Belgeleme basamağı aslında adli bilişimin bütün basamakları bakımından uygulanacaktır[94]. Yapılan bütün adli bilişim işlemleri kayıt altına alınacaktır.

Belgeler genellikle bir yazıcıdan alınan çıktı şeklinde olur. Lâkin büyük yer kaplayan dosyalar ve görüntüler CD ve DVD gibi veri saklama birimlerine kaydedilebilirler[95]. Delillerin ve uygulanan sürecin belgelenmesi belgelendirme işi ile uğraşan uzmanlar tarafından yerine getirilmelidir.

Adli bilişim sürecinin son basamağı olan raporlama basamağında işletilen tüm süreç bir rapor olarak mahkemeye sunulur. Raporlama veya diğer adıyla sunum (presentation) basamağında hazırlanacak olan adli bilişim raporunda teknik terimler ve kavramlar hakkında ayrıntılı bir açıklamaya yer verilmeli, delil niteliğini haiz veriler için kesin ve somut göstergeler bulunmalı, kullanılan adli bilişim yöntemleri gösterilmeli, delil bütünlüğünün bozulmadığı ispatlanmalı ve inceleme basamağındaki yer alan tüm işlemler genel rapora bağlı bir şekilde ek bir rapor altında düzenlenmelidir[96]. Belgeleme basamağında dava için hazırlanan belgeler de rapora eklenmelidir. Rapor, belgeleme basamağında belgelenen bilgilere dayalı olacaktır. Belge büyük boyutlardaki dosya veya görüntülerden de oluşabilir. Bunun için kaydedilen CD ve DVD gibi birimler raporda ek olarak belirtilebilir.

Rapor hazırlanmasındaki amaç yalnızca delilleri sunmak değildir. Raporda incelenen konular, en basit yöntemlere başvurularak anlatılmalı ve buna ait sorulara karşı cevaplar eksiksiz bir biçimde açık, doğru ve eleştiriye yer vermeyecek şekilde raporda bulunmalıdır[97]. Teknik bir anlatımla elektronik delilin doğruluğu ispatlanmalı ve elektronik delillerin inkar edilmemesi sağlanmalıdır[98].

---

[94] Yusuf Uzunay, "Dijital Delil Araştırma Süreci", **2. Polis Bilişim Sempozyumu**, Ankara, EGM Bilgi-İşlem Daire Başkanlığı, Nisan 2005, s. 6.
[95] Balı, **a.g.m.**, s. 237.
[96] Ekizer, **a.g.m.**, s. 15.
[97] Yetim, **a.g.m.**, s. 1218. ; (zikreden; "Guidelines For Best Practise In The Forensic Examination Of Digital Technology", www.ensfi.org.).
[98] Uzunay, Koçak, **a.g.m.**, s. 3. ; (zikreden; Chet Hosmer, "Providing The Integrity of Digital Evidence With Time", International Journal of Digital Evidence, Volume I, Spring 2002).

Raporda incelenen veri saklama birimleri karışıklığa yer vermeyecek şekilde ayrıca değerlendirilmeli; hangi birimlerde hangi delillerin keşfedildiği gibi önemli konuların, anlaşılması kolay bir şekilde rapora kaydedilmesi sağlanmalıdır[99].

Raporda hangi basamakların hangi tarihte başlatıldığı ve hangi tarihte son bulunduğu hususlarına yer verilmelidir. Tarihlerin belirlenememesi raporun sağlamlığını sakatlayacaktır.

Raporda adli bilişim sürecinde farklı birimlerle birlikte yapılan çalışmalarda elektronik delilin el değiştirilme işlemlerinin kaydedilmesi yani delil güvenlik zincirinin (chain of custody) belgelenmesi gerekir[100]. Delille ilgilenen her bir kimsenin kaydı ile delilin belgelenmesini, detayını, soruşturma safhalarını, toplamayı, elde etmeyi, sunumunu ve bunların da belgelenmesini kapsayan sürece delil güvenlik zinciri denilmektedir[101]. Delil güvenlik zinciri delil bütünlüğünün bozulmadığının kanıtlanmasında bir araçtır.

Raporun mahkemeye sunulmasıyla bu basamak sona ermektedir. Bundan sonra mahkeme bu rapora dayanarak hüküm verebilir veya delillerin serbestçe değerlendirilmesi ilkesi kapsamında sunulan rapora dayanmaksızın karar verebilir.

Bu beş basamak, belirtilen sıra halinde uygulama alanı bulacaktır. Basamaklar arasında boşluk olmamasına veya sıranın karışmamasına dikkat edilmelidir. Mahkemede bu işlem sırasının doğru yapılıp yapılmadığına ilişkin bir denetleme söz konusu olabilir[102].

4- Elektronik Delil Elde Etmede Başlıca İlkeler ve Standartlar

Elektronik delilin karmaşık yapısı, gözle görünmemesi ve diğer özellikleri onu diğer delillerden ayırır. Hangi verilerin elektronik delil

---

[99] Balı, **a.g.m.**, s. 234.
[100] Say, **a.g.m.**, s. 259.
[101] Weise, Powel, **a.g.m.**, s. 6.
[102] Aktepe, **a.g.m.**, s. 67.

olabileceği tartışılmasının yanında yeni veri türlerinin ortaya çıkması, bu tartışmayı ileri boyutlara taşımaktadır.

Elektronik delilin toplanması, muhakemede etkin bir şekilde kullanılması, güvenirliliğinin sarsılmaması için elektronik delilde bulunması gereken bir takım özellikler vardır. Bu özellikler ulusal veya uluslararası olarak çeşitli sempozyum, konferans, toplantı ve panellerde tartışılmış olup belirli ilkelere ve ilkelere bağlı olarak belirli standartlara dönüştürülmüştür. Bunun yanında kabul edilen bu ilkelere ek olarak adli birimler ve adli bilişim servisleri ve adli birimler de gelişen teknoloji karşısında bir takım ilkeler geliştirmişlerdir.

Elektronik delillerde bulunması gereken bir takım standartlara ek olarak elektronik delilleri elde etmede yani adli bilişim sürecinde uygulanabilecek bir takım ilkeler öngörülmüştür. Örneğin İngiltere Polis Başkanlığı Birliği'nin yayınladığı "Bilgisayar Temelli Elektronik Deliller İçin İyi Pratik Rehberi" 'nde (Good Practice Guide For Computer Based Electronic Evidence) 4 temel ilkeye önem verilmiştir. Bu ilkeler şunlardır:

1- Adli bilişim birimleri veya adli birimler mahkemede delil olarak kullanılabilecek bilgisayar veya veri saklama birimlerindeki elektronik verilerin değişikliğine neden olacak girişimlerden kaçınmalıdırlar.

2- İncelenecek bilgisayar veya veri saklama birimlerindeki orjinal verilere erişimin gerekli olduğu istisnai durumlarda, bu erişimi mümkün kılabilecek kişinin işlem yapmaya yetkili, tecrübe sahibi ve uzman olması aranacaktır. Bu kişi aynı zamanda uyguladığı işlemleri ve bunların arka planını ispatlamaya muktedir olacaktır.

3- Bilgisayar temelli elektronik delillere uygulanan bütün işlemler bir denetimden geçirilmeli ve deliller muhafaza edilmelidir. Taraf olmayan bir üçüncü kişi de bu süreçleri izleyerek aynı sonucu elde etmeli; farklı bir sonuca varmamalıdır.

4- Elektronik delilleri incelemede sorumlu olan görevlilerin; uygulamaya konulan işlemlerin hukuka uygun olup olmadığını ve öngörülen ilkelere aykırı olup olmadığını denetlemede sorumlulukları vardır[103].

Amerika Birleşik Devletleri'nde elektronik delilin elde edilmesinde bir takım standartlara ulaşılması amacıyla 1998 yılında Federal Suç Laboratuvarı yöntecilerinin yardımlarıyla Dijital Delil Bilimsel Çalışma Grubu (Scientific Working Group On Digital Evidence-SWGDE) oluşturulmuştur. Bu grupla ABD temelli standartlaşma bakımından Uluslararası Bilgisayar Delili Organizasyon arasında (International Organization On Computer Evidence-IOCE) bir bağlantı kurulmuştur[104]. Bu çalışma grubu Standart Yönetim Prosedürleri (Standart Operating Proceedures-SOP) denilen bir takım usullere uymaktadır. Bu usuller hem adli bilişim alanında hem de hukuki alanda ilgili hususlar içerdiğinden bütün adli bilişim birimlerinde kullanılır.

Söz konusu belgeye göre elektronik delilin (dijital delil) toplanmasını, incelenmesini, sunulmasını, sağlayabilmek ve delilin güvenirliliğini sağlam kılabilmek için adli bilişim ve hukuk alanında gerekli birimler kurulmalıdır. Kalite kontrol politikaları içerisinde belgelenen SOP; doğru dava kayıtlarıyla desteklenmeli ve kabul edilen prosedürler, aletler ve diğer teçhizatlar kullanılabilir durumda olmalıdır. Söz konusu standartlar şunlardır:

- Adli bilişimle uğraşan bütün birimler kabul gören bir SOP belgesindeki hususları izlemelidir. Elektonik delillerle ilgili bu konu üzerine uzmanlaşan bütün birimlerin politikaları ve prosedürleri birim yönetimi altında yayınlanan SOP belgesininde açıkça yer almalıdır.

- Bu birimler SOP dökümanını, en temel olarak çalışmaların etkinliğini ve uygunluğunu saptayabilmek adına gözden geçireceklerdir.

- Kullanılan prosedürler, bilimsel alanlar veya veri toplamdaki sınıflandırılan durumlar üzerinde bir mutabakat sağlanmalıdır.

---

[103] Uzunay, **a.g.m.**, s. 6; (zikreden; United Kingdom Association Of Police Officers The Good Practices Guide For Computer Based Electronic Evidence", National High-Tech Crime Unit, 2003).

[104] "Proposed Standarts For The Exchange Of Digital Evidence", **Digital Evidence: Standarts and Principles**, Forensic Science Communications, April 2000 Volume 2 Number 2, (Erişim) http://www.fbi.gov.tr/hq/lab/fsc/backissu/april2000/swgde.htm, 17 Mart 2009, s. 1.

- Birimler teknik prosedürlerin yazılmış kopyalarını muhafaza etmek zorundadırlar.

- Birimler elkoyma ve inceleme prosedürleri için etkin ve uygun niteliklere sahip donanım ve yazılım kullanmalıdır.

- Delillerin elkonması, saklaması, incelenmesi ve iletimi ile ilgili bütün hareketler yazılı olarak kaydedilmeli; gözden geçirilmeye ve ispatlanmaya elverişli olmalıdır.

- Potansiyel olarak elektronik delilleri bozacak, hasar verecek ve yok edecek ya da orjinal delile zarar verecek herhangi bir hareketin bu alanda uzman olmuş kişilerce yapılması zorunluluk arzeder[105].

Dijital Deliller Bilimsel Çalışma Grubu'nun çalışmalarında bağlantılı olduğu Uluslararası Bilgisayar Delili Organizasyonu, 1995 yılında, uluslararası hukuk uygulama birimlerinin bilişim suçu soruşturmasıyla ilgili bilgilerin ve diğer bilgisayarla ilgili kriminalistik yayınların değişimi için bir forum oluşturulmasını sağlama amaçlı kurulmuştur[106]. Bu organizasyon, bilgileri kurumsallaştırarak ve onların yayılmasını kolaylaştırarak faaliyetleri, yayınları ve tavsiyeleri ile üye olan hukuk birimlerine yardımcı olmaktadır. Organizasyon elektronik delillerin kurtarılması ve değişimi için uluslararası standartlar geliştirmekle görevlendirilmiştir. ABD'de, Kanada'da ve Avrupa'da bu organizasyonun çalışma grupları mevcuttur.

Bu organizasyonun ilkelerinde her ne kadar elektronik delil kavramı kullanılasa da kanımızca dijital delilleri de kapsayabilme bakımından bilgisayar delilli (computer evidence) veya bilgisayar temelli delil (computer based evidence) kavramları baskın bir şekilde kullanılmaktadır.

Organizasyonun belirlediği bilgisayar temelli delillerle ilgili uluslararası ilkeler şunlardır:

- Bütün hukuk sistemleriyle bağlı ve tutarlı olma
- Delille ilgili yaygın bir dil kullanımı tavsiyesi
- Dayanıklı ve uzun ömürlü olma
- Uluslararası sınırları aşabilme yetisi

[105] Proposed Standarts For The Exchange Of Digital Evidence, s. 4.
[106] Proposed Standarts For The Exchange Of Digital Evidence, s. 5.

- Delilin doğruluğu konusunda güven telkin edebilme
- Bütün adli bilişim delillerine erişebilirlik
- Bireysel, birimsel düzeyde ve ülke çapını içerecek şekilde her bölüme erişebilirliğin sağlanması[107].

Bu organizasyonun daha sonraki yıllarda düzenlendiği konferanslarda hem elektronik delillere hem de adli bilişim sürencindeki kullanılan yöntemlere ilişkin bir takım ilkeler eklenmiş var olan ilkeler değiştirilmiştir. Bu ekleme ve değişikliklerin en önemli nedeni teknolojinin ilerlemesi ve elektronik delillerle ilgili daha fazla bilginin ortaya konulmasıdır. Lâkin ana esaslar yukarıdaki gibidir.

Bunun gibi elektronik delillerin mahkemeye sunulması ve muhakemede değerlendirilmesiyle ilgili bir başka ilkeler bütünlüğü de vardır. Örneğin medeni yargılama hukukundaki keşif (e-keşif) konusu ile ilgili olan Sedona İlkeleri (Sedona Principles) daha çok elektronik verilerin, elektronik belgelerin korunması ve yargılamada kullanılmasını ele almaktadır[108]. Her ne kadar medeni muhakeme hukukundaki keşif ceza yargılamasındaki keşifle farklı olsa da bir takım benzerlikler göstermektedir. Bu açıdan ceza muhakemesinde e-keşifin yürürlülüğe girmesi ihtimaline karşılık özellikle e-keşfin uygulanmasında bu ilkelerin dikkate alınması yararlı olabilecektir.

III- ELEKTRONİK DELİL SAKLAYAN İLGİLİ BİRİMLER

A- BİLGİSAYARDA BULUNAN VERİ SAKLAMA BİRİMLERİ

Rastgele Erişimli Bellek (Random Access Memory-RAM), Sadece Okunabilir Bellek (Read Only Memory-ROM), Ön Bellek (Cache Memory) ve Sabit Disk (Hard Disk) bilgisayarın içerisinde bulunan veri saklama birimleridir. Bu veri saklama birimlerinden ilk üçü bilgisayarın çalışmasını, hızını, veri işleyebilmesini ve veri okuyabilmesini düzenlerler. Bu bellek türleri

[107] Orjinali için bkz. Proposed Standarts For The Exchange Of Digital Evidence, s. 5.
[108] Berber, **a.g.e.**, s. 168, 169, 170.

kurucu ve birincil niteliktedirler. Küçük çaptaki verileri sakladıklarından bu bellek türlerinden doğrudan delil elde edilmesi pek mümkün olmamaktadır.

Sabit disk ise bilgisayar içerisinde de olsa ikincil bellek birimi olarak nitelendirilir[109]. Bilgisayara haricen bağlanabilen veya USB girişleri olan sabit diskler de bu nitelemeyi desteklemektedir. Sabit diskler bilgisayarların belki de en önemli veri saklama birimdir. RAM'lerde ve ROM'larda bulunan geçici veriler buraya kaydedilip kalıcı hale getirilirler.

Katı ve metalik yapısının olması nedeniyle İngilizce'de sabit diske "harddisk" denilmiştir[110]. Sabit diskte dokümanlar, ses-görüntü-video dosyaları, veri tabanı dosyaları, internet geçmişi, sohbet kayıtları, şifrelenmiş dosyalar, dosyanın oluşum-erişim-silme tarihleri, silinmiş dosyalar, silinmiş disk alanları, kayıt bilgileri, erişim şifreleri, kullanıcı adları, sistem hizmetleri gibi delil olabilecek veriler bulunabilir[111]. Bununla beraber bilgisayara zarar veren virüsler ve zararlı programlar, sistem bilgisi taşıyan programlar, sanal disk alanları ve RAM'le ilgili bilgiler sabit diskte saklanabilirler[112].

B- VERİ SAKLAMA BİRİMLERİ

Bilgisayardan kendisine veya kendisinden bilgisayara veri aktarabilen bu birimler her türlü veri çeşidini saklama kapasitelerine göre içerisinde bulundurabilirler. Veri saklama birimleri çok çeşitlidir. Teknolojinin ilerlemesiyle boyut olarak daha küçük ancak saklama kapasitelerine göre daha büyük birimler üretilmektedir.

Elektronik altyapı ve devreler, modem, uzaktan kumanda ve kamerada (dijital kamera hariç) mevcut olduğundan her ne kadar görünüşte elektronik delil içermese de elektronik delil saklayabilirler[113]. Sabit diskten ayrı olarak disket, CD (Compact Disc), DVD, (Digital Versalit Disc), BD (Blue Ray Disc), USB Bellek, MP3, MP4 ve diğer çalıcılar, Hafıza Kartları, Akıllı Kartlar, Yazıcı

---

[109] Balay, Erses, **a.g.e.**, s. 21.
[110] Gülcü, Alan, **a.g.e.**, s. 15.
[111] Kaygısız, **a.g.e.**, s. 300.
[112] Ekizer, **a.g.m.**, s. 3.
[113] Dokurer, **a.g.m.**, s. 242.

ve Faks Cihazları, Dijital Kameralar ve Dijital Fotoğraf Makineleri, Cep Telefonları ve El Bilgisayarları, Oyun Konsolları, Jaz ve Zip Kartuşları, Ağ (Network) Cihazları birer veri saklama birimidir. Her veri saklama biriminin kendisini diğer veri saklama birimlerinden ayıran özellikleri vardır. Boyutu, şekli, yapısı, veri saklama kapasiteleri vb. gibi özellikler bir veri saklama birimini diğer birimlerden ayırmaya yardımcı olur. Ancak kendi içerisinde bile bir çok türe rastlamak mümkündür. Örneğin; CD'lerin bazılarında tek yazılabilme; (CD-Recordable) bazılarında ise (CD Rewritable) birden fazla yazılabilme özelliği vardır[114]. CD'lerin markaları aynı olsa dahi seri numaraları aynı değildir. Bu bakımdan adli bilişim uzmanı bu özelliklere (kendi içerisindeki farklılıklara), markalarına ve seri numaralarına da dikkat etmelidir. Aksi takdirde veri saklama birimleri birbirine karışabilir ve zarar görebilir.

Bu birimler içerisinde dokümanlar, kelime işlemci dosyaları, resimler, ses ve video dosyaları, veri tabanı dosyaları, veri tabanı erişim kayıtları, şifrelenmiş veya dosyalar, silinmiş dosyalar ile disk alanları, mevcut dosyaların tarihleri, adres ve telefon bilgileri, Virus, Trojan, SpyWare vs gibi zararlı yazılımlar, SMS kayıtları, erişim şifreleri ve kullanıcı adları vb. gibi ceza muhakemesinde delil olabilecek bir çok bilgi bulunabilmektedir[115]. Böylelikle veri kavramının bilgisayar verisiyle sınırlandırılmaması gerektiği sonucuna bir kez daha ulaşılmaktadır. Adli bilişim sürecinin ve bilgisayardan delil elde edilmesinin koşulları veri saklama birimleri için de uygulanmalıdır.

C- İNTERNET ORTAMINDA BULUNAN VERİLER

İnternet ortamında bulunan verileri incelemeye geçmeden önce internetin ne olduğunu belirtmemiz gerekir. "İnternet" kelimesi "International" (Uluslararası) ve "Network" kelimelerinin ilk hecelerinin birleştirilmesi sonucu türetilmiştir[116]. İnternet kelimesinin sonunda olan "net" hecesi temel olarak bir

---

[114] Balay, Erses, **a.g.e.**, s. 27.
[115] Ekizer, **a.g.m.**, s. 3, 4, 5, 6, ve 7.
[116] Hakan Karakehya, "Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu", **TBBD**, Sayı 81, Mart-Nisan, 2009, s. 197.

"ağ"'ı ifade eder[117]. Bununla birlikte "Network" kelimesinin dilimizeki karşılığı "ağ"dır. İnternet birden çok "network" yani haberleşme ağının bir araya gelerek oluşturdukları çok büyük bir bilgi ve iletişim alanıdır[118]. Dünya üzerindeki milyonlarca bilgisayar bir araya gelerek veri paylaşımlarını bu alan üzerinden yapmaktadır. Herhangi bir sahibinin bulunmadığı başka bir ifadeyle bir kişinin veya kurumun mülkiyetinde olmadığı için herkes internet hizmetinden serbestçe yararlanabilmektedir[119].

Serbestçe girilen bu bilgi ve iletişim alanı sınırsız gibi görünebilirse de sınırsız değildir. TCP (Transmission Control Protocol-İletim Kontrolü Protokolü) ve IP (Internet Protocol-Internet Protokolü) gibi bir takım kurallar rol oynar. TCP dosya akışını sağlar ve ortaya çıkan hata durumlarını çözer. IP ise internette adresleyici ve yönlendirici bir işlev görmektedir[120].

İnternetin hukukumuzda tek başına bir tanımı bulunmamaktadır. Ancak 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"'un 2. maddesinde "*Haberleşme ile kişisel veya kurumsal bilgisayar sistemleri dışında kalan ve kamuya açık olan internet üzerinde oluşturulan ortamı... ifade eder."* şeklinde "internet ortamı" tanımına yer verilmiştir.

İnternet sayesinde her geçen gün daha fazla bilgi üretilmekte ve üretilen bu bilgi daha hızlı bir şekilde paylaşılmaktadır. Veri paylaşımı yapılabildiğine göre internet ortamında bulunan veriler bir suçun delili olabilmektedir.

İnternet ortamında veriler devamlı olarak akışkan bir yapıda bulunurlar[121]. Bu akışkanlık incelemeyi, farklı modelleme örneklerine götürecektir. Örneğin internet ortamından delil elde edebilmek için bilgisayar mümkün olduğunca açık kalmalı ve kapatılmamalıdır. Aksi halde veri akışı duracağından istenilen verilere ulaşılamayabilir. Açık duran bilgisayardan bir kopya çıkartılarak bu kopya üzerinden delil incelemesi yapılacaktır.

---

[117] Hasan Sınar, **İnternet ve Ceza Hukuku**, İstanbul, Beta Yaynevi, 2001, s. 21.
[118] Ergün, **a.g.e.**, s. 7.
[119] Sınar, **a.g.e.**, s. 30.
[120] Gülcü, Aslan, **a.g.e.**, s. 251.
[121] Kaygısız, **a.g.e.**, s. 305.

D- HİZMET VEREN BİLGİSAYARLARDA BULUNAN VERİLER

5651 sayılı kanunun 2. maddesinde internet süjelerine yer verilmiştir. Bu süjelerden biri olan erişim sağlayıcı 2. maddenin 1. fıkrasının e bendinde "*Kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri … ifade eder.*" denilmek suretiyle tanımlanmıştır. İçerik sağlayıcılarla ilgili olarak fıkranın f bendinde "*İnternet ortamı üzerinden kullanıcılara sunulan her türlü bilgi veya veriyi üreten, değiştiren ve sağlayan gerçek veya tüzel kişileri … ifade eder.*" şeklinde bir tanım yer almaktadır. Fıkranın m bendinde ise yer sağlayıcı hakkında bir tanım yapılmıştır. Buna göre yer sağlayıcı: "*Hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri … ifade eder.*"

İçerik sağlayıcılar bir web sayfasının içeriğini hazırlama işlemleriyle ilgilenirler[122]. Erişim sağlayıcıları bilgi akışını ve ağa erişimi sağlarlar. Erişim sağlaycılar, verileri kısa süreli saklayabilirler; ancak onların kural olarak böyle bir nitelikleri yoktur[123]. Yer sağlayıcıların diğer bir adıyla hizmet sağlayıcıların içerik sağlayıcılarda üretilen içeriği, kendi sunucularında saklayabilme ve kendi bağlantılarını kullanarak doğrudan internet ortamında erişilebilir hale getirebilme gibi niteliklere sahip olması sebebiyle diğer internet süjelerinden farklılaşmaktadır[124].

Yer sağlayıcılar internet ortamına yönelik hizmetlerini bilgisayarlar ve büyük çaptaki veri saklama birimleri ile gerçekleştirirler. Hizmet, bir ağ (Network) ortamında gerçekleşir. Her türlü bilgisayar hatta bir diz üstü bilgisayar da sunucu olarak diğer bilgisayarlara kaynak hizmeti verebilir[125]. Ağ bakımından dosya saklama, web sayfası, internet erişimi, e-posta hizmetleri bu tür bilgisayarlarca görülür.

Hizmet veren bilgisayarlardaki veriler örneğin bir bilişim suçunun delili olabilmektedir. Bu bilgisayarlar üzerinde koruma tedbirleri uygulanıp uygulanmayacağı hususu ayrıca incelenecektir.

---

[122] Sınar, **a.g.e.**, s. 41.
[123] Fatih Selami Mahmutoğlu, "Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu" **İÜHFM**, Cilt LIX, Sayı 1-2, İstanbul, Beta Basım Dağıtım, 2001, s. 44.
[124] Sınar, **a.g.e.**, s. 42.
[125] Berber, **a.g.e.**, s. 59.

E- ELEKTRONİK POSTA (E-POSTA)

Elektronik Posta, kısaca "e-posta" insanların birbirleriyle mektupla iletişim isteklerinin internet ortamında gerçekleşmesini sağlayan bir hizmettir[126]. İletişim mektup gibi yazılı bir biçimde olmaktadır. Buradaki fark yazının kağıt üzerinde değil; "HTML" (Hyper Text Markup Language), biçimindeki elektronik belge üzerinde olmasıdır.

E-posta çok hızlı bir şekilde iletilebilme, iletişimde güvenirlilik ve ucuz olması gibi özelliklerinden dolayı posta, telefon ve diğer iletişim araçlarına nazaran üstün tarafları vardır[127]. E-posta veri saklama kapasitesinin yüksek olduğu sanal bir posta kutusudur. Birden fazla mesaj aynı anda alınabilir ve gönderilebilir. Gönderilen veya alınan mesajlar saklanabilir ve istenildiği zaman kullanılabilir. Özellikle iş yazışmalarında büyük önemi vardır. Zira bu yazışmalar ileride delil olacak bilgileri taşıyabilirler. Bu bahisle e-postalar, e-keşfin inceleme alanı arasında gösterilirler[128].

E-posta "@" işareti ile gösterilir. Kişinin kullanacağı isim, numara e-posta adresin alındığı sistem adresi @ işaretiyle ikiye ayrılır[129]. E-posta adresi internet servis sağlayıcıların sunduğu internet paketleriyle, kamu veya özel kurumlarda görev yapan personelin çalıştıkları kurumdan veya en yaygın kullanımıyla ücretsiz e-posta hizmeti sunan (hotmail, yahoo, gmail vs...) internet adreslerinden alınabilir[130].

E-posta adresine ses kaydı, görüntü, resim, belge, program ve videolar "ekle" (attach) yöntemiyle eklenerek bir başka e-posta adresine gönderilebilir. Bunun tersi de mümkün olup alınan dosyalar bilgisayara indirilebilir veya "forward" yani bir başka adrese yönlendirilebilir. Bir e-posta gönderildiğinde öncelikle mail sunucusuna ulaşır. Alıcının alma işlemleri tamamlandıktan sonra mail sunucusunun veri tabanındaki mesaj yok olur. E-posta programlarını tamamına yakını bu özelliklere sahiptir. Eklenen dosyalar e-posta adresinin taslak veya gönderilen klasörlerinde kaydedilebilir. Şayet

[126] Tosun, Karamanlıoğlu, Yerlikaya, **a.g.e.**,, s. 4.
[127] Sınar, **a.g.e.**, s. 34.
[128] Berber, **a.g.e.**, s. 115.
[129] Balay, Erses, **a.g.e.**, s. 308.
[130] Balay, Erses, **a.g.e.**, s. 308.

eklenen dosyaların birer delil olabilme özelliği varsa bu halde e-posta klasörlerine dikkatli bir şekilde yaklaşılmalıdır. En küçük bir yanlış müdahale verileri silebilir. Lâkin silinseler bile geri getirilmesi imkansız da değildir[131]. Fakat bu durum, adli bilişim sürecinde vakit kaybına neden olacaktır.

E-postalara erişimin diğer bir yolu ise internet servis sağlayıcılardır. E-postalar internet servis sağlayıcılar üzerinden gönderilebilmelerinden dolayı e- postalar internet servis sağlayıcılarının tuttukları rutin yedeklemeleri içerisinde saklanmış olabilirler[132].

E-posta internetin bizlere sunduğu bir hizmettir. İnternetten elde edilen veriler başlığı altında ele alınabilirse de kendine özgü özelliklerinden dolayı delil araştırmasında ayrı bir yaklaşımla incelenmesi daha yararlıdır. Ayrıca şüphelinin veya sanığın e-posta adresi biliniyorsa şifresi kırılarak delil olabilecek verilere ulaşılması daha kolay bir yöntem olarak gözükmektedir.

E-postalar bazı sohbet programlarının olmazsa olmazıdır. Örneğin en yaygın olan MSN sohbet programı Hotmail adresli e-postaları temel almaktadır ve bu programı kullanabilmek için Hotmail sitesinden bir e-posta hesabı açtırmak gereklidir[133]. Sohbet siteleri ve programlarıyla yapılan yazışmaların bir örneği bilgisayarda kayıt altına alınabilir. Kaydedilmeseler de bunlara bazı programlar aracılığıyla ulaşılabilir. Özellikle şüphelinin veya sanığın yaptığı yazışmalara dikkat edilmelidir.

Sohbet siteleri ve programlarından başka internet üzerinde “youtube”, “facebook” gibi en yaygın siteler, forumlar, haber grupları adli bilişimin inceleme alanına girerler. Bu siteler belge, ses, görüntü, resim, video dosyalarını içermektedirler. Dolayısıyla delil araştırması bunlar üzerinde de yapılabilir.

---

[131] Berber, **a.g.e.**, s. 121.
[132] Berber, **a.g.e.**, s. 124.
[133] Balay, Erses, **a.g.e.**, s. 322.

İKİNCİ BÖLÜM

AVRUPA KONSEYİ SİBER SUÇ SÖZLEŞMESİ VE SÖZLEŞMEYE TARAF OLAN-TARAF OLMAYAN ÜLKELERDE BİLGİSAYARLARA YÖNELİK ARAMA KOPYALAMA VE ELKOYMA TEDBİRLERİ

I- AVRUPA KONSEYİ SİBER SUÇ SÖZLEŞMESİ VE KAPSAMI

A- SÖZLEŞMENİN GENEL DURUMU

Bilgisayarın ve internetin getirdiği yenilikler ve kolaylıklara karşılık suç işlemek için kullanılması; bu suçun ülke sınırlarını aşan boyutta olması; (terör ve pornografik yayınlarla mücadele); devletleri, bilişim alanındaki suçlarla mücadelede bir işbirliği yapma noktasına getirmiştir. 1996 yılında Avrupa Suç Sorunları Komitesi internet ortamında işlenen suçları gözlemleyebilen, uzmanlardan oluşan bir komitenin kurulması konusunda çalışmalar yapmıştır[134]. Oluşturulan bu komite 2001 yılının Haziran ayında Avrupa Konseyi Siber Suç[135] Sözleşmesini (The Council of Europe Convention on Cybercrime) kaleme almıştır. 8 Kasım 2001 tarihinde Avrupa Konseyi Bakanlar Komitesince bu sözleşme onaylanmış 23 Kasım 2001 tarihinde

---

[134] Mahmutoğlu, **a.g.m.**, s. 40.

[135] "*Siber suçun ne olduğunu tanımlamak zordur. Siber suç, siber uzay ortamında işlenen suç olarak tanımlanmaktadır. Ancak bu tanımlama, siber suçların tasnifine ilişkin lup, siber suçun niteliğini ortaya koyamamaktadır. "Siber suç kavramı, esasen, bilgisayar sistemlerine karşı veya bilgisayarlarla işlenen suç anlamına gelmektedir. Bu yönüyle "siber suç" kavramı ile "bilgisayar suçu" kavramı arasında bir fark yoktur*." (Mahmut Koca, "Avrupa Konseyi Siber Suç Sözleşmesin'nin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku", **Bilgi Toplumunda Hukuk**, **Ünal Tekinalp' Armağan**, Cilt III, İstanbul, Beta Yayınevi, 2003, s. 788).

imzaya sunulmuştur. Macaristan'ın başkenti Budapeşte'de imzaya sunulan bu sözleşmeye 43 Avrupa Konseyi üyesi devlet ve konseye üye olmayan 4 devletle (Kanada, Japonya, Güney Afrika ve ABD) beraber 47 ülke imza koymuştur[136]. Sözleşmenin yürürlülük kazanması Avrupa Konseyi'nden üç ve toplamda beş ülkenin onaylaması şartına bağlanmıştır[137].

Sözleşme, dili itibariyle bilişim teknolojileri kaynaklı suçları ifade etmede tarafsız bir tutum takınmış; kullanılan dilin mevcut ve ileride mevcut olabilecek teknolojilerle uyumlu olmasını hedeflemiştir[138]. Şekil bakımından sözleşme 48 maddeden müteşekkil olup 6 bölüme ayrılmıştır. Son kısmında

---

[136] (Erişim) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG, 08 Eylül 2009, Güncelleme tarihi 01 Aralık 2010.
Sözleşmeye Avrupa Konseyi Üyeleri olan Almanya, Arnavutluk, Avusturya, Belçika, Bosna-Hersek, Bulgaristan, Çek Cumhuriyeti, Danimarka, Ermenistan, Estonya, Finlandiya, Fransa, Hollanda, Hırvatistan, Macaristan, İngiltere, İrlanda, İspanya, İsveç, İsviçre, İtalya, İzlanda, Karabağ, Kıbrıs Rum Cumhuriyeti, Lüksemburg, Makedonya, Malta, Moldovya, Norveç, Polonya, Portekiz, Romanya, Sırbistan, Slovakya, Slovenya, Ukrayna ve Yunanistan, imza koymuştur.
Sözleşmeye en son imza koyan ülkeler: Azerbaycan (30.6.2008), Gürcistan (1.4.2008), Liechtenstein (17.11.2008) ve Türkiye'dir (10.11.2010).
Sözleşmeyi iç hukuk uyarınca yürürlülüğe sokan ülkeler: Almanya (01.07.2009), ABD (01.01.2007), Arnavutluk (01.07.2004), Azerbaycan (01.07.2010), Bosna-Hersek (01.09.2006), Bulgaristan (01.08.2005), Danimarka (01.10.2005), Ermenistan (01.02.2007), Estonya (01.07.2004), Hırvatistan (01.07.2004), Finlandiya (01.09.2007), Fransa (01.05.2006), Hollanda (01.03.2007), İspanya (01.10.2010), İtalya (01.10.2008), İzlanda (01.05.2007), Karabağ (01.07.2010), Kıbrıs Rum Cumhuriyeti (01.05.2005), Macaristan (01.07.2007), Makedonya (01.01. 2005), Moldovya (01.09.2009), Norveç (01.10 2006), Portekiz (01.07.2010), Romanya (01.09.2004), Sırbistan (01.08.2009), Slovakya (01.05.2008) Slovenya (01.01.2005) ve Ukrayna (01.07.2006).

[137] Helvacıoğlu, **a.g.m.**, s. 279.;
İmza ve yürürlük başlıklı Avrupa Konseyi Siber Suç Sözleşmesi'nin 36. maddesi aynen,
1. İşbu Konvansiyon, Avrupa Konseyine üye Ülkelerin ve bu belgenin hazırlanmasında payı bulunan üye olmayan Ülkelerin imzasına açık olacaktır.
2. İşbu Konvansiyon, tasdik edildikten, kabul edildikten ve onaylandıktan sonra yürürlüğe girecektir. Tasdik, kabul ve onay evrakı Avrupa Konseyi Genel Sekreterine teslim edilecektir.
3. İşbu Konvansiyon, en az üçü Avrupa Konseyi üyesi olan beş Ülkenin, işbu Konvansiyonun kendileri açısından paragraf 1 ve 2 hükümlerine uygun olarak bağlayıcı olduğunu beyan ettikleri tarihten sonraki üç aylık sürenin bitiminin ardından gelen ayın ilk gününde yürürlük kazanacaktır.
4. İşbu Konvansiyon, Konvansiyonun bağlayıcılığını kabul eden Ülkelere ilişkin olarak, söz konusu Ülkelerin işbu Konvansiyonun kendileri açısından paragraf 1 ve 2 hükümlerine uygun olarak bağlayıcı olduğunu beyan ettikleri tarihten sonraki üç aylık sürenin bitiminin ardından gelen ayın ilk gününde yürürlük kazanacaktır." şeklindedir. (Bkz. Avrupa Konseyi Siber Suç Sözleşmesi, (Erişim) http://www.binbilen.org/belgeler/Siber_Suclar_Sozlesmesi.pdf, 25 Haziran 2009. s.17).

[138] Helvacıoğlu, **a.g.m.** s. 283.

(ekler) açıklayıcı memorandum vardır. Açıklayıcı memorandum sözleşmenin gerekçesidir.

Açıklayıcı memorandumun son bölümünde (16. kısmında) sözleşmenin amacı belirtilmiştir. Buna göre siber suçlarla ilgili, taraf ülkelerdeki maddi ceza mevzuatlarının birbirleriyle uyumlu olmasına yönelik düzenlemeler yapılacak; bilişim alanındaki suçların ve bilgisayar aracılığı ile işlenen diğer suçların soruşturma ve kovuşturulmasını kolaylaştıran ceza muhakemesi içerisindeki tedbirler tanınacak; hızlılık ve etkinlik esaslarını içeren uluslararası bir işbirliği sağlanacaktır[139]. Sözleşmenin düzenlenmesindeki en önemli etkenlerden biri de taraf ülkeler arasında bir işbirliği gözetilerek siber suçlarla mücadelede ortak bir ceza politikası oluşturmaktır[140].

Sözleşmenin giriş kısmında Avrupa Konseyi İnsan Hakları ve Temel Özgürlükler Konvansiyonu'na (1950) BM Siyasal ve Sivil Haklar Sözleşmesi'ne (1996), Çocukları Korumayı Amaçlayan BM Çocuk Haklarına Dair Sözleşmesi'ne (1989), Uluslararası Çalışma Örgütü Çocuk İşçilerin Kötü Durumları Konvansiyonunu'na (1999) atıfta bulunulmuştur. Sözleşmelere atıf yapılarak siber suç sözleşmesinin uygulanma ve yorumlanma bakımından işlerlik kazandırılması istenmiştir[141]. Bu sözleşmeye ek olarak "Bilişim Sistemlerinin Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Eylemlerin Suç Haline Getirilmesi İçin Avrupa Siber Suç Sözleşemesine Ek Protokol" 28.01.2003 tarihinde imzaya sunulmakla beraber, 20 ülke bu protokole imza koymuştur[142].

---

[139] Avrupa Konseyi Siber Suç Sözleşmesi, http://www.binbilen.org/belgeler/Siber_Suclar_Sozlesmesi.pdf, 25 Haziran 2009. s. 24.

[140] Koca, **a.g.m.**, s. 786.

[141] İnci Biçkin, "Siber Suç Sözleşmesi, 5237 sayılı Türk Ceza Kanunu, Bilişim Suçları", **Bilişim ve Hukuk**, Sayı: 1, Yıl: 1, Ankara, Ankara Barosu, 2006.

[142] Bilişim Sistemlerinin Aracılığıyla İşlenen Irkçı ve Yabancı Düşmanı Eylemlerin Suç Haline Getirilmesi İçin Avrupa Siber Suç Sözleşemesine Ek Protokol, (Erişim) http://conventions.coe.int/Treaty/EN/Treaties/html/189.htm, 16 Nisan 2011.

B- SÖZLEŞMEYE TARAF OLAN ÜLKELERE YÜKLENEN YÜKÜMLÜLÜKLER

Sözleşmeye taraf olan ülkelere bir takım yükümlülükler yüklenmiştir. Sözleşmenin maddi ceza hukuku kısmında bilişim suçlarıyla ilgili yasama işlemlerinin yapılması bir yükümlülük olarak öngörülmüştür[143]. Bunu müteakiben taraf ülkeler mevzuatlarındaki bilişim suçlarının soruşturma ve kovuşturma aşamalarını sözleşmeye uygun olarak değiştirecek; eksiklikler varsa uygun eklemeler yapacaklardır.

Sözleşmenin usul hukuku kısmında (Bölüm II) başlık 1'de (genel hükümler) usul hükümlerinin kapsamı (md. 14.), şartlar ve önlemler (md. 15.) düzenlenmiştir. Başlık 2'de (Saklanan Bilgisayar Verilerinin Korunmasının Kolaylaştırılması) saklanan bilgisayar verilerinin korunmasının kolaylaştırılması (md. 16), trafik bilgilerinin korunmasının kolaylaştırılması ve kısmen açıklanması (md. 17) konuları yer almaktadır. Başlık 3'te üretim talimatı (md. 18), başlık 4'te saklanan bilgisayar verilerin aranması ve bunlara el konulması (md. 19), başlık 5'te (Bilgisayar verilerinin gerçek zamanlı olarak toplanması), trafik bilgilerinin gerçek zamanlı olarak toplanması (md. 20), içerikle ilgili bilgilere müdahale edilmesi (md. 21) hususlarını düzenleyen ilgili hükümler bulunmaktadır. Sözleşmedeki maddi ceza hukuku ile ilgili yasama işlemlerine başvurma yükümlülüğü, sözleşmenin usul hukuku bakımından da geçerlidir.

Sözleşmeye taraf olan ülkelerarası bir yardım antlaşması varsa; taraflar, aralarındaki yardım antlaşmasını dikkate alıp sözleşme hükümlerinin tamamının veya bir kısmının uygulanmamasını kararlaştırabilirler (AK-SSS md. 27/1). Şayet böyle bir antlaşma yoksa sözleşmenin 27. maddesindeki hükümler uygulanacaktır.

Yukarıda bahsettiğimiz iki kısımda sözleşmeye taraf devletlerin yargı yetkisinin düzenlenmesi (Kısım 3 – md. 22), uluslararası alanda işbirliği (Bölüm II-Kısım 1-Başlık-1-md. 23) yapmaları öngörülmüştür. Ayrıca diğer

---

[143] Avrupa Konseyi Siber Suç Sözleşmesi, (Erişim) http://www.binbilen.org/belgeler/Siber_Suclar_Sozlesmesi.pdf, 25 Haziran 2009. s. 3.

bölüm ve kısımlarda, işbirliği ile ilgili özel hükümlere, özel yardım taleplerine ve bu yönelik taraf devletlerin yükümlülüklerine yer verilmiştir.

C- TÜRKİYE'NİN SÖZLEŞME KARŞISINDA DURUMU

Ulusal sınırların dışında bilişim suçlarının takibi veya diğer suçların delillerinin elektronik ortam aracılığı ile toplanmasında bu sözleşme hızlı, etkin ve özel bir adli yardımı düzenlemiştir. Türkiye, bu sözleşmeye taraf olmadığı için bu özel adli yardım taleplerine cevap verilememekteydi. Türkiye'nin de bu sözleşmeye; bilişim suçlarının takip edilmesinde uluslararası işbirliği sağlamak ve Avrupa siber suç politikasının ana ilkelerinin benimsenmesi amacıyla taraf olması gerektiği görüşü ileri sürülmüştü[144].

Sözleşmeye taraf olunmasa da bu sözleşmedeki bilişim suçları tanımları 5237 sayılı TCK'daki bilişim suçlarının hazırlanmasında esas alınmıştır[145]. Nihayetinde Türkiye 10.11.2010 tarihinde sözleşmeye imza koymuştur[146]. Ancak sözleşme, iç hukuk uyarınca yürürlülüğe henüz girmemiştir.

D- SAKLANAN BİLGİSAYAR VERİLERİNİN ARANMASI VE BUNLARA EL KONULMASI

Bilgisayarlarda arama yapılması sözleşmede "üretim emri" (production order) olarak anlaşılan bir karar tipidir[147]. Üretim emri hangi konuyla ilgili verilmişse o konuyla ilgili yasama işlemlerinin gerçekleştirilmesini yükümlü kılmaktadır. Bu itibarla taraf devletler üretim emrine uygun ölçüde yasama işlemlerini yapacaktır. Bir üretim emri olarak Sözleşmenin II. Bölüm, 2. kısım,

---

[144] Ayrıntılı bilgi için bkz. Ankara Barosu Uluslararası Hukuk Kurultayı, Cilt 2, Ankara, 2008, s. 94.
[145] Biçkin, **a.g.m.**, s. 66.
[146] (Erişim) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG, 01 Aralık 2010.
[147] Kunter, Yenisey, Nuhoğlu, **a.g.e.**, s. 1022.

başlık 4, madde 19'da "Saklanan Bilgisayar Verilerinin Aranması ve Bunlara El Konulması" düzenlenmiştir[148].

19. maddede düzenlenen bu tedbirlerin sözleşmenin memorandum kısmının başlık 4'ün 184 ve 204. maddeleri arasında gerekçeleri verilmiştir. Bu tedbirler hakkında yapılan açıklamalar oldukça geniş mahiyettedir. Memorandumun 184. maddesinde bilgisayarlara yönelik bu özel tedbirlerin düzenlenerek taraf ülkelerdeki mevzuatlar arasındaki uyumluluğun kurulması amaçlandığı belirtilmiştir. Diğer bir ifadeyle buradaki amaç, birbirine paralel ve yakın mevzuatlar oluşturmaktır[149].

Maddenin ilk iki paragrafında vurgulandığı üzere bilgisayar sistemi, bu sistemin parçası ve bunlarda saklanan bilgisayar verileri veya bu verileri saklayan birimler bu özel tedbirlerin konusudur. Bu maddeyi açıklayan

---

[148] AK-SSS'nin "Saklanan Bilgisayar Verilerinin Aranması ve Bunlara El Konulması" başlıklı AK-SSS'nin 19. maddesi aynen,
"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 el koyma 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. İşbu maddede sözü geçen yetki ve usuller Madde 14 ve 15'e tabi olacaktır." şeklindedir.

[149] Avrupa Konseyi Siber Suç Sözleşmesi, (Erişim) http://www.binbilen.org/belgeler/Siber_Suclar_Sozlesmesi.pdf, 25 Haziran 2009. s. 53.

memorandumun 187. maddesi arama ve elkoymadaki genel usullerin yanında bir takım özel usullerin eklenmesi gerektiğini vurgulamıştır. Bunun nedenleri olarak elektronik verilerin elektromanyetik ortamda olduğu; nesne gibi götürülemeyeceği; anlaşılabilmesinin bilgisayar teçhizatı yardımıyla olabileceği; verilerin saklı tutulduğu birimlere elkonulmasına ve bu birimlerin bir kopyasının çıkartılmasına ihtiyaç duyulması; kopya çıkartılmasının taraf ülkelerin mevzuatınca kanuni olarak tanınması gerektiği ve bilgisayarın birbirine bağlanabilmesi imkânından dolayı delillerin aranılan bilgisayar olmamakla beraber başka bir bilgisayar üzerinde bulunabilmesi; gösterilmiştir[150]. Memorandum ayrıntıya girerek bu tedbirlerin sadece bilgisayarı kapsamayıp tanımdaki "bilgisayar sistemi" kavramınındaki "*birbirine bağlı veya birbiriyle ilişkili cihaz*" ibaresinin geniş şekilde anlaşılmasını tavsiye etmektedir. Başka bir ifadeyle veri saklama birimleri üzerinde ve yerel ağdaki bilgisayarlarda da bu tedbirlerin söz konusu olabileceğini ve bunların yapılabilmesi için kanuni düzenlemelerin yapılması gerektiği konusuna önem atfetmiştir.

Maddedeki 3. paragraf, arama veya erişim konusunun sadece aranılan yerde değil; kendi ulusal sınırları içindeki başka bir bilgisayar sisteminde ya da bu sistemin bir parçasında saklandığına dair belirtiler varsa bu tedbirlerin başka sistemleri de kapsayacak şekilde genişletilmesini ve bunun için kanuni bir zeminin oluşturulmasını hükmetmektedir. Memorandumun 192. ve 195. maddeleri, 3. paragrafı açıklayarak arama ve elkoymanın ulusal sınırlar dışında uygulanmasının mümkün olmadığını, taraf ülkelerin işbirliğine gitmesiyle bunun işletilebileceğini belirtmiştir.

Memorandumun 191. maddesi, aramanın neyi ifade ettiğini ve bilgisayarla ilgili aramada erişim kelimesinin teknik terimlere daha yakın durduğunu ifade etmiştir[151]. 194. maddesi ise arama alanlarının nasıl

---

[150] Avrupa Konseyi Siber Suç Sözleşmesi, (Erişim) http://www.binbilen.org/belgeler/Siber_Suclar_Sozlesmesi.pdf, 25 Haziran 2009. s. 54.

[151] Memorandumun 191. maddesi aynen,
"*Arama ya da benzer şekilde erişim" ifadesi kullanılmıştır. Geleneksel "arama" kelimesinin kullanımı,*
Devlet tarafından cebri yetkilerin kullanılması fikrine işaret etmekte ve bu Maddede söz edilen yetkinin geleneksel aramaya karşılık düştüğünü göstermektedir. "Arama", verileri bulmaya

genişletileceği hususunu ulusal düzenlemelere bırakmıştır. Elkoyma tedbiri ise sözleşmenin 19. maddesinin 4. paragrafında ve memorandumun 196. maddesinde öngörülmüş olup genel bir çerçevede ele alınmıştır. 4. paragraf, 1. ve 2. paragrafa atıfta bulunarak, aynı arama tedbirinde olduğu gibi elkoyma tedbirinde de kanuni düzenlemelerin yapılması gerektiğinin altını çizmiştir. Söz konusu 19. maddenin 4. paragrafın a bendinde gösterildiği üzere aramanın konusu ile elkoymanın konusu aynıdır. Aramada hangi yerler aranacaksa ve hangi birimlere bakılacaksa, elkoyma tedbirinde de o yerlere ve birimlere ilgili işlemler yapılacaktır.

Maddedeki 4. paragrafın devamında bilgisayar verileriyle ilgili elkoymanın bir türü olan "başka şekillerde koruma altına alma" konusu ele alınmıştır. Elkoyma teriminin çeşitli anlamlarından (örneğin maddi olmayan bilgisayar ortamında taşınan verileri için "benzer şekilde güven altına alma" memorandumun 197. maddesinde bahsedilmiştir[152]. Elkoyma veya güven altına alma tedbirleri memorandumun 199. maddesi gereği öncelikle verilerin kopyalanmasıyla delil elde edilmesi; verilerin kopyalanıp aslının erişilmez kılınması veya taşınmada elde edilecek verilere izin verilmesi amacıyla işletilir.

çalışma, okuma, denetleme ve inceleme anlamındadır. Veriyi arama ve araştırma (inceleme) kavramlarını içine almaktadır. Diğer taraftan "erişim" kelimesi, bilgisayar terminolojisini daha iyi yansıtan, belli bir yargı bildirmeyen bir kelimedir. Geleneksel kavramlarla modern terminolojiyi uzlaştırmak için her iki terim birlikte kullanılmıştır." şeklindedir. (Avrupa Konseyi Siber Suç Sözleşmesi, (Erişim) http://www.binbilen.org/belgeler/Siber_Suclar_Sozlesmesi.pdf, 25 Haziran 2009. s. 55).

[152] Memorandumun 192. maddesi aynen,
"*İşbu Konvansiyonda, "el koymak", üzerinde veri ya da bilgilerin kayıtlı olduğu fiziksel ortamı alıp götürmek ya da bu verilerin ya da bilgilerin bir kopyasını üretmek ve tutmak anlamına gelmektedir. "El koymak", el konan verilere erişmek için gereken programların kullanımını ve bu programlara el konmasını da kapsamaktadır. Geleneksel "el koymak" teriminin yanı sıra, maddi olmayan verilerin bilgisayar ortamında taşındığı, erişilmez kılındığı ya da kontrolünün başka bir şekilde ele geçirildiği diğer yolları yansıtmak için benzer şekilde güven altına almak" terimi de kullanılmıştır. Önlemler saklı durumdaki maddi olmayan verilerle ilgili olduğu için yetkili mercilerin verileri güven altına alması için, kopyalanan ya da taşınan verilerin el koyma anında bulundukları durumda tutulmaları ve cezai takibatlar sırasında değişmemiş durumda kalmaları anlamına gelen "verilerin bütünlüğünün korunması" ya da verilerin "koruyuculuk zincirinin" korunması gibi ek önlemler gereklidir. Terim verilerin kontrolünü ele geçirmeyi ya da verileri alıp götürmeyi ifade etmektedir."* şeklindedir. (Avrupa Konseyi Siber Suç Sözleşmesi, (Erişim) http://www.binbilen.org/belgeler/Siber_Suclar_Sozlesmesi.pdf, 25 Haziran 2009. s. 55, 56).

Maddenin 5. paragrafında bilgisayar verilerinin kaybolabilme riskinden dolayı kopyalanarak alıkonulmasını belirtmiştir. 6. paragraf, koruma altına alma ile ilgilidir. 7. paragraf ise erişilen bilgisayar sistemindeki ilgili verilerin başkaları tarafından erişimin engellenmesini, kullanılamayacak hale getirilmesini ve silinmesini düzenlemiştir. Bu üç paragraftaki teknik ayrıntılar bile sözleşmeye taraf ülkelerin hukukuna dahil edilmek zorundadır.

Maddenin 8. paragrafında bilirkişilik kurumuna başvurulmasını belirten ibareler mevcuttur. Bu paragrafta aramanın teknik boyutunun iyi derecede işletilebilmesi için bilgisayar sistemlerine yönelik özel bilgileri haiz olan sistem yöneticilerine ve diğer ilgili kişilere arama ve bilgisayar verilerinin saklandığı cihazlar konusunda danışma ve emir verebilmeyle ilgili düzenlemeler yapılması hususu incelenmiştir.

9. paragrafta ise söz konusu 19. maddenin, sözleşmenin 14. ve 15. maddelerinde yer alan usul hükümlerinin kapsamı, şartları ve alınacak önlemlerle ilgili esaslara tabi olduğu belirtilmiştir. 14. maddenin 4. paragrafında "cezai bir suça ilişkin olarak elektronik ortamda delil toplanması" konusunda düzenlemeler yapılması hususu genel bir düzenleme olarak yer almıştır. Bahsedilen koruma tedbirleri, sözleşmenin atıfta bulunduğu (Avrupa Konseyi İnsan Hakları ve Temel Özgürlükler Konvansiyonu, BM Siyasal ve Sivil Haklar Sözleşmesi vb. gibi) temel hak ve özgürlükleri düzenleyen ilgili sözleşmelerdeki hükümlere uygun olarak işletileceği sözleşmenin 15. maddesinde belirtilmiştir.

Sözleşmede saklanan bilgisayar verilerinin aranması ve bunlara elkonulması tedbirinden başka bilgisayar verileriyle ilgili "Saklanan Bilgisayar Verilerinin Korunmasının Kolaylaştırılması" (md. 16), "Trafik Verilerinin Gerçek Zamanlı Olarak Toplanması" (md. 20) ve "Trafik Bilgilerinin Korunmasının Kolaylaştırılması ve Kısmen Açıklanması" (md. 17) konularına yer verilmiştir. Memorandumda da bu konuların lafzi açıklaması ve teknik boyutu ile ilgili bilgiler verilmiştir.

"Trafik Verilerinin Gerçek Zamanlı Olarak Toplanması" tedbiri bilgisayarlar vasıtasıyla yapılan iletişimle ilgili verilerin elde edilmesini konu

edinmektedir. Trafik verilerinin ne olduğu sözleşmenin 1. maddesindeki tanımlar kısmında gösterilmiştir[153]. Kısaca trafik verisi sözleşmede tanımlanan bir bilgisayar verisi çeşididir. Bu bilgisayar verisi çeşidinin toplanması ve elde edilmesi sözleşmeye taraf olan ülkenin sınırları dâhilinde belirtilen bir iletişimin varlığına bağlıdır[154]. Trafik verileri ve bununla ilgili tedbirler sözleşmenin 20. maddesi uyarınca taraf ülkelerce kendi mevzuatlarına dâhil edilecektir.

Sözleşmede bilgisayar ve bilgisayar verileriyle ilgili ayrıntılı düzenlemeler yapılması ve memorandumda bunlara açıklık getirilmesi, sözleşmeye taraf ülkelerdeki uygulamaların; her ne kadar birbirinin aynısı olmasa da birbirine paralel olması içindir. Ayrıntıya bu kadar önem verilmesinin bir diğer nedeni kanımızca zamanın geçmesiyle kanuni ve uygulamada oluşacak olan farklılığın önüne geçilebilmesidir. Farklılık bakımından sözleşme, fedaral ülkelerdeki uygulanma hususlarını bile ihitva etmektedir. Bir diğer ayrıntı ise teknik terim konusundadır. Bir terim birliği veya bir terim paralelliği yaratılmak istenmiştir. Zengin bir ayrıntıya (bunu açıklayan 331 maddelik memoranduma) sahip olan bu sözleşme devletlere birçok yükümlülük getirdiğinden bazı devletler sözleşmeyi yalnızca imzalamış olup kendi iç hukuklarında yürürlülüğe sokmamışlardır.

Avrupa Birliği çalışma raporlarında bilgisayarlardaki verilerin bilişim suçlarında delil olarak kullanılabileceğini ve bu delillerle işlenen suçun soruşturulmasının mümkün olduğunu ileri sürmektedir[155]. Bununla ilgili olarak "Delillerin Online Araştırılmasında Kullanılacak Siber Araçlar" (Cyber Tools On-line Search for Evidence) projesi AB komisyonu tarafından başlatılmıştır.

---

153 AK-SSS'nin tanımlar başlığı altında 1. maddesinin d fıkrası aynen,
"trafik bilgileri" terimi, bir bilgisayar sistemi kullanılarak yapılan bir iletişime ilişkin olarak, söz konusu iletişim zincirinin bir halkası konumunda bulunan bir bilgisayar sistemi tarafından üretilen ve iletişimin başlangıç noktasını, varış noktasını, izlediği yolu, saatini, tarihini, boyutlarını, süresini veya bu iletişimde kullanılan hizmetin tipini gösteren herhangi bir bilgisayar verisini ifade edecektir." şeklindedir. (Avrupa Konseyi Siber Suç Sözleşmesi, (Erişim) http://www.binbilen.org/belgeler/Siber_Suclar_Sozlesmesi.pdf, 25 Haziran 2009. s. 3).

154 Helvacıoğlu, **a.g.m.**, s. 293.

155 Leyla Keser Berber, "Adli Bilişimle İlgili Olarak AB ve ABD'deki Yasal Düzenlemeler ve Kişisel Verilerin Korunması", **Bilişim Hukuku Konferansı-YARGITAY**, Ankara, 09-10 Ekim 2008, s. 29.

Proje elektronik delillerin tespitini, korunmasını, bütünlüğünün sağlanmasını, sunulmasını ve hukuken geçerli olmalarını hedeflemiştir[156]. Aynı zamanda proje, bu kapsamda geliştirilen araçlar sayesinde sistem yöneticilerine, bilgi güvenliği uzmanlarına, bilgisayar olayları soruşturmacılarına polis ve diğer kolluk birimlerine; bilgisayarla ilgili olayları soruşturmada yararlanabilecekleri uygun ve standart ölçülere bağlı metodlar getirmektedir[157].

II- SÖZLEŞMEYE TARAF OLAN ÜLKELERDE BİLGİSAYARLARA YÖNELİK ARAMA KOPYALAMA VE ELKOYMA TEDBİRLERİ

A- İNGİLTERE

İngiltere AK-SSS'ye 23 Kasım 2001 tarihinde imza koymuştur. Sözleşme, iç hukuk uyarınca bir yasama işleminden geçmemiş olup, yürürlüğe girmemiştir[158].

İngiliz Adli Polis ve Suç Delili Kanunu'nda (Police and Criminal Evidence Act 1984) genel olarak arama ve elkoyma tedbirlerine yer verilmiştir. Kısım 1'in 1. maddesinde polisin kişileri ve araçları arama yetkisini; 2. maddesi arama yetkisine ait düzenlemeleri; Kısım 2'nin 8. maddesi arama iznini, 17. maddesi arama izni olmaksızın bir binaya (kapalı yere, konuta) girme ve arama hallerini; 19. maddede ise genel elkoyma yetkileri düzenlenmiştir[159]. Bu düzenlemelerin yanında Adli Polis ve Delil Kanunu'na tabi olan "Evde Arama ve Kişilerin Üzerinde veya Evde Bulunan Eşyaya Elkoyma Yönetmeliği" vardır. Yönetmelikteki arama ve elkoyma

---

[156] Berber, **a.g.m.**, s. 29.
[157] Berber, **a.g.m.**, s. 30.
[158] (Erişim), http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG, 01 Aralık 2010.
[159] (Erişim), http://www.statutelaw.gov.uk, Police and Criminal Evidence Act, 8 Eylül 2009.

tedbirlerinin Adli Polis ve Delil Kanunu'na tabi olduğu 1.3. maddesinin a ve b bendlerinde belirtilmiştir[160].

Adli Polis ve Suç Delili Kanunu'nun 8. maddesi binalara girme ve arama yapma izni verme yetkisinin sulh hakimine (justice of the peace) ait olduğunu göstermektedir. Binada tutuklanabilir bir suçun işlendiğine veya binada suçun soruşturulmasında çok önemli bir değere sahip bir şeyin bulunduğuna inanmayı haklı gösterecek makul sebepler varsa; aranılan şey delil niteliğini haiz ise veya arama özel nitelikteki bazı durumlar dışında ise (örneğin polis acil olarak binaya girmediği için arama tedbirinin amacının tehlike altına girmesi veya aranılan şeyin ciddi bir şekilde zarar görme olasılıkları) polis arama kararı (search warrant) için sulh hâkimine başvurabilir. Arama kararı için bir talep gerekir. İlgili talepte arama kararının dayanacağı kanun; arama yapılacak olan bina (veya ev) ve arama sonucunda bulunacak olan eşyanın ne olduğu belirtilmelidir. Ayrıca aranılan şeyin kanuni ayrıcalığa tabi olmaması, ayrık tutulmuş veya özel bir prosedürle ilgili bulunmaması gerekir. Bu maddenin 2. fıkrasında polisin arama kararı uyarınca yaptığı aramada soruşturma için gerekli gördüğü her şeye elkoyma yetkisinden bahsedilmiştir.

Kanunun 19. maddesinde elkoymanın genel hükümlerine yer verilmiştir. Buna göre el koyma yapabilmek için polisin binada kanuni bir yetkiyle bulunması şart koşulmuştur. Kanuni yetki sulh hakimi tarafından verilir. Maddenin 2. ve 3. fıkraları makul sebeplerin varlığı durumunda suçla ilgili olan, suç işlenerek elde edilen bir eşya ile eşyanın değiştirilmesinin, kaybedilmesinin ve zarara uğratılmasının önlenmesi için uygulanan elkoyma tedbiriyle ilgilidir.

Maddenin 4. fıkrası polise, soruşturulan suçla ilgili olması veya suç sonucunda elde edilmesi nedeniyle bozulmasını, kaybedilmesini, zarar görmesini engellemek amacıyla saklanan elektronik yapılı erişilmesi mümkün olan bilgileri elde etme yetkisini vermektedir. Buna ek olarak verilerin

[160] (Erişim) http://www.epysportal.com/Mevzuat/Yabanc%C4%B1PolisMevzuat%C4%B1/tabid/285/language/tr-TR/Default.aspx, 21.05.2009.

görünebilmeleri ve okunabilmeleri için metin haline getirilmesini öngören düzenleme 2001'deki kanuni değişikliklerle getirilmiştir[161].

Genel elkoymanın sulh hakimi tarafından alınan bir arama kararına dayanması gerektiği, bu fıkranın uygulanmasında da söz konusu olacaktır. Söz konusu yönetmeliğin el koymayı düzenleyen 6. maddesinin 5. bendinde polis memuru, bilgisayardaki verilerin delil olarak kullanılmasının mümkün olduğunu gördüğü zaman bilgisayardaki verilerin görünebilir veya okunabilir hale getirilmesini isteyebilmektedir. Yönetmeliğin bu maddesi kanun hükmüne dayanmakta ve binada bulunanların rızalarıyla yapılan arama hallerinde de polisin eşyaya elkoymasını ifade etmektedir.

Kanunun 20. maddesinde bilgisayar kaynaklı verilerin elde edilmesi yetkisinin genişletilmiş bir düzenlemesi bulunmaktadır. Polis memuru kanunun verdiği yetkiye dayanarak sadece bilgisayardaki verileri değil; bilgisayara bağlanabilen birimlerin de araştırılmasını isteyebilir. Bundan ayrı olarak maddenin 2. fıkrası bu maddeyle birlikte uygulanacak olan diğer maddeleri ve düzenlemeleri göstermektedir. Bunların arasında 8. maddedeki sulh hâkimince verilen arama kararı da vardır.

İngiltere'de bilişim suçlarıyla ilgili Bilgisayarı Kötüye Kullanma Kanunu (Computer Misuse Act) 1990 yılından beri yürürlülüktedir. Bu kanunun 14. maddesinde bilişim suçlarına ilişkin arama kararı düzenlenmişti. Lâkin bu madde Polis ve Adalet Kanunu'nun (Police and Justice Act-(2006)-Commencement No:9, Order 2008) getirdiği cetvel 14'le (shcedule 14) ilga edilmiştir[162].

2000 yılında iletişimin denetlenmesi ve teknik takibi kolaylaştıran "Soruşturma Yetkilerini Düzenleyen Kanun" (Regulation of Investigatory Powers Act) yürürlülüğe girmiştir. Kanun, polis ve adli birimlere yargı kararı

---

161 (Erişim), http://www.statutelaw.gov.uk, The Criminal Justice and Police Act 2001 (Commencement No. 9) Order 2003 (No. 708 (C.34)), 08 Eylül 2009.

162 *The following provisions of the Police and Justice Act 2006 shall come into force on 1st October 2008 ;*
(d) in Part 4 of Schedule 15 (repeals and revocations) the entries relating to—
(i) sections 11, 12, 14, 16 and 17 of the Computer Misuse Act 1990(4) ((Erişim), http://www.opsi.gov.uk/si/si2008/uksi_20082503_en_1, 10 Eylül 2009;
(Erişim) http://www.davros.org/legal/cma.html#s14, 10 Eylül 2009.)

olmadan soruşturmaya ait bazı yetkilerin kullanılmasına imkân vermiştir[163]. Ancak hakim kararının arandığı hususlar da yok değildir. Yer verilen tedbirlere ek olarak trafik verilerinin gerçek zamanlı olarak toplanması tedbiri de bu kanunda karşılık bulmuştur. Kanunun kısım 3'ün 49., 50., 51., 52., 53., 54., 55. ve 56. maddelerinde şifre ve diğer yöntemlerle korunan elektronik verilerin araştırılmaya konu olması düzenlenmiştir[164]. Bu maddelerde gizlenmiş veya şifrelenmiş verinin, kişinin mülkiyetinde bulunan yerlerde aranması, tutulması, araştırılması ve elkonulması yetkileri öngörülmüştür. Aynı zamanda gizli izleme tedbiri sonucu bilgilerin elkonulması yetkilerine de bu madde içerisinde atıf yapılmıştır. Sıraladığımız maddelerin hiç birinde terim olarak ne bilgisayar, ne de veri saklayabilen herhangi bir birim kullanılmıştır ki; verinin herhangi bir yerde olduğunun kabulüyle bir yerde aranması bakımından sınırlanmaması amacı güdülmüş olabilir. Buna benzer şekilde Bilgisayarı Kötüye Kullanma Kanunu'nda da bilgisayar, program ve veri kavramlarına tanım olarak yer verilmemiştir. Tanımın yapılması durumunda, eskiyeceği ve yeni gelişmeler söz konusu olduğunda kanunun uygulanmasının kısıtlanacağı görüşü hâkimiyet kazanmıştır[165].

Soruşturma Yetkilerini Düzenleyen Kanun'un 49. maddesinde korunan bilgilerin ifşa edilmesi veya ortaya konması için bildirim gereken durumları öngörmektedir. Bu madde çerçevesinde verilerin araştırılması için bir görevliye bölge hâkimi tarafından "uygun izin" (appropriate permission) verilmelidir[166]. Uygun izin makul sebepler çerçevesinde verilir. Bunun için korunan bilgi, tedbire muhatab olan kişinin mülkiyeti altında olmalıdır. Korunan bilgiyle kastedilen şifre olmadan ona ulaşılması, hâlihazırda erişilmesi veya anlaşılabilir bir biçime dönüştürülmesi mümkün olmayan

---

[163] Emmanuel Gross, "The Struggle of a Democracy Against Terrorism-Protection of Human Rights: The Right to Versus The National Interest – The Proper Balance, **Cornell International Law Journal**, Volume 37, 2004, (Erişim) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=683942, 27 Ekim 2009, s. 155.

[164] (Erişim), http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_8#pt3-pb1, 23 Eylül 2009.

[165] Karagülmez, **a.g.e.**, s. 107.

[166] (Erişim), http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_12#sch2, 23 Eylül 2009. Bu durum kanunun son kısmında yer alan cetvel 2'de (schedule 2) öngörülmüştür.

herhangi bir elektronik veridir[167]. Uygun izne sahip kişi, korunan bilgiye sahip olan bir kimseye bu korunan bilgiyi açabilecek şifreyi açıklama yükümlülüğünü (disclosure requirement) öngören bir bildirimde bulunur. Bu şifrenin ne olduğunu açıklama sadece uygun izne sahip olan veya uygun izin kararında belirtilen kimselere karşı yapılır. Söz konusu kanunun 50. maddesinde bu bildirimle ilgili olarak elde edilen şifrenin korunan bilgiyle ilgili olup olmadığının tespiti ve bunun sonuçları üzerinde eğilirken tedbirlerin ulusal güvenlik, suçun belirlenmesi, önlenmesi ve İngiltere'nin ekonomik çıkarlarını korunması amaçlandığı gözlemlenmektedir. Bu maddedeki hükümlerin gerekli ve makul sebepler içerisinde uygulanmasına 49. maddenin 3. fıkrası cevaz vermiştir.

Kanunun yukarıda sıralanan bu maddelerinde şifrelenmiş elektronik verinin elde edilmesi çok ayrıntılı bir şekilde düzenlemiştir. O kadar ki bu tedbirlerin maliyetinden teminatına ve kimler tarafından uygulanacağına ilişkin bir çok konulara değinilmiştir. Adli Polis ve Suç Delili Kanunu'ndaki bilgisayarlara uygulanan tedbirlerle karşılaştırıldığında bu tedbirin özel bir düzenleme olduğu kolaylıkla anlaşılmaktadır. Bu özel düzenleme şifrelerin çözümüyle ilgili olduğundan elektronik yapıdaki iletişim araçlarında da bu tedbirin uygulanması söz konusu olabilmektedir.

İngiltere'deki polis ve adli birimler elektronik delil elde etmede daha önce ifade edilen "Bilgisayar Temelli Elektronik Deliller İçin İyi Pratik Rehberi"'ndeki esasları dikkate alırlar.

İngiltere'de kıta avrupası sisteminden farklı olarak mevzuattan çok mahkeme kararları rol oynamaktadır. İngiltere'de delillerin ceza muhakemesinde kabul edilebilirliği istisnalar haricinde genel kurallara (The Legal Rules of Evidence) tabidir. Kural olarak ceza muhakemesinde bütün

---

[167] "*protected information" means any electronic data which, without the key to the data—(a) cannot, or cannot readily, be accessed, or (b) cannot, or cannot readily, be put into an intelligible form;"* ((Erişim) http://www.statutelaw.gov.uk/SearchResults.aspx?TYPE=QS&Title=Regulation+of+Investigatory+Powers+A, 08 Eylül 2009).

ilgili deliller mahkemece kabul edilebilirler[168]. Tutukluluk ve cezalandırmayla ilgili kararlar için bütün delillere başvurulabileceği gibi bu delillerin kullanılması ve kabul edilebilmesi mümkündür. Bu durum bazı hukuka aykırı olarak elde edilen delilleri içerse de suçu ispat etme bakımından bazı istisnalar öngörülmüştür[169]. Delil kurallarının ihlali halinde, ihtilaf halindeki bulgulardan üretilen bir suçlamaya bir engel yoktur. Ancak bu durumda mahkeme hukuka aykırı delillere başvuru veya reddetme haklarını saklı tutacaktır[170]. Buna ek olarak delil kurallarına göre kabul edilebilirliği olmayan deliller yok edilmez ancak değerlendirilmelerine cevaz verilmemektedir. Ceza muhakemesinde delilin kullanılabilirliği konusunda mahkeme, delili şüpheye yer bırakmayacak şekilde (beyond reasonable doubt) ispat edilmesini dikkate alarak mahkumiyet hükmü kuracaktır[171].

Bilgisayardan elde edilen delillerin kabul edilebilirliğini 2000'li yıllara kadar Adli Polis ve Suç Delili Kanunu'nun 69. maddesi düzenlemekteydi. Bu madde bilgisayar delillerini bir ispat yüküne tabi tutmaktaydı[172]. Söz konusu 69. maddenin yürürlülüğü ortadan kaldırılmıştır[173]. Delilin sağlam olup olmadığı yargılama sırasında tartışılmakta ve delile şüpheci bir şekilde yaklaşılmasına bugün de devam edilmektedir[174].

Bilişim suçları çerçevesinde (CMA'daki düzenlemeler) elektronik olarak saklanmış verilerden oluşturulan belgeler, İngiliz mahkemelerinin çeşitli yorumlarına bağlı kalarak delil olarak kabul edilebilmektedirler[175].

---

[168] Oliver Leroux, "Legal Admissibility of Electronic Evidence", **International Review of Law, Computers and Technology**, 01 July 2004, Volume 19, Number 2, (Erişim) http://dx.doi.org/10.1080/1360086042000223508, 17 Eylül 2009, s. 211.

[169] Leroux, **a.gm.**, s. 203, 212.; Örneğin "Hearsay Evidence" yani kulaktan dolma bilgilere dayanan bulguların değerlendirme dışı olmasının en önemli nedeni bilginin kendi gözlemlerinden ziyade başkalarından öğrenilmiş olmasıdır.

[170] Leroux, **a.g.m.**, s. 212.

[171] Leroux, **a.g.m.**, s. 214.

[172] Wieke Abel, "Agent, Trojans and Tags: The Next Generation of Investigators**"**, **International Review of Law, Computers & Technology**, March 2009, Volume 23, Issue 1&2, s. 101. (Erişim) http://www.informaworld.com/smpp/section?content=a910308496&fulltext=7132409, 15 Eylül 2009. s. 105.

[173] Abel, **a.g.m.**, s. 101.

[174] Abel, **a.gm.**, s. 101.

[175] Leroux, **a.g.m.**, s. 213.

B- ALMANYA

Almanya AK-SSS'ne 23.11.2001 tarihinde imza koymuş olup 09.03. 2009 tarihinde onaylamıştır. Sözleşme, 01.07.2009 tarihinde iç hukukta yürürülülük kazanmıştır[176].

Almanya AK-SSS'nin ortaya koyduğu hükümleri kendi mevzuatına uyumsallaştırmak için bir takım çalışmalarda bulunmaktadır. Sözleşmedeki düzenlemeleri karşılamak amacıyla Alman Ceza Kanunu'na (Strafgesetzbuch, StGB) ve Alman Ceza Muhakemesi Kanunu'na (Strafprozeßordnung, StPO) bir takım eklemeler yapılmıştır. Örneğin; sözleşmenin 1. maddesinde geçen "bilgisayar verisi" kavramı Alman Ceza Kanunu'nun veri casusluğunu düzenleyen 202a. maddesine yansımıştır[177]. Maddedeki tanımdan verinin, elektronik, manyetik, gözle görülemeyen, saklanması mümkün olan ve iletilebilen bir şey olduğu anlaşılmaktadır[178].

Arama ve elkoyma tedbirleri Alman Ceza Muhakemesi Kanunu'nun 8. bölümünde, 94. ve 111. maddeleri arasında yer almaktadır. Genel arama ve elkoyma hükümlerinin yanında iletişimin denetlenmesi, gizli soruşturmacı, kişisel verilerin kullanımı ve bilgisayar destekli arama vb. gibi diğer tedbirler de bu bölümde mevcuttur.

AK-SSS'nin 19. maddesinde düzenlenen bilgisayarlara yönelik arama ve elkoyma tedbirlerinin ceza muhakemesinde çeşitli görünümleri vardır. Maddenin 1. fıkrasındaki arama ve erişim sağlama yetkileri Alman Ceza Muhakemesi Kanunu'nun 8. bölümündeki 94., 95., 102., 103., 105., 110.,

---

[176] (Erişim), http://conventions.coe.int/Treaty/Commun, 12 Eylül 2009.

[177] 202a; Strafgesetzbuch, StGB;
(1) "Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.
(2) Within the meaning of subsection (1), data shall only be those which stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner.".
((Erişim), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/567-LEG-country%20profile%20Germany%20_1%20June%2007_En.pdf, 08 Eylül 2009.; http://www.iuscomp.org/gla/statutes/StGB.htm#202a).

[178] Karagülmez, **a.g.e.**, s. 115.

161. ve 163. maddeleri karşılamaktadır[179]. Ancak bu maddelerde bilgisayarlara yönelik bir arama ve erişim sağlama yetkileri bulunmamaktadır. Başka bir deyişle Alman Ceza Muhakemesi Kanunu'nda özgün bir biçimde bilgisayarlara ve veri saklama birimlerine yönelik arama, kopyalama ve elkoyma hükümleri yoktur. Kanunda bilgisayarla ilgili; kişilere ait verilerin bilgisayar verileriyle karşılaştırılması (StPO md. 98a), bilgisayar verilerini karşılaştırmaya karar veren merci ve verilerin geri verilmesi ve silinmesi (StPO md. 98b), kişisel verilerin bilgisayarda kayıt altına alınması ve bilgisayar destekli arama (StPO md. 163d) konuları hüküm altına alınmıştır. Bilgisayar destekli arama tedbirinde şüphelinin bilgisayarında arama ve elkoyma yapılması söz konusu değildir. Bilgisayar burada adli işlemlerin yapılmasında bir yardımcı olarak öngörülmüştür. Henüz AK-SSS'ndeki 19. maddesindeki özel düzenleme Alman ceza mevuzatına yansımamıştır. İş bu nedenlerle genel hükümlerdeki esaslara bakılacaktır. Bilgisayarlar hakkında birer genel hüküm olan kanunun 102., 94. ve 110. maddeleri bir arada uygulanacaktır[180]. Verilerin elkonulması, orijinaline uygun kopyasının çıkarılması işlemleri kanunun 98. maddesindeki esaslara göre gerçekleştirilecektir[181].

Arama ve elkoymanın genel hükümlerine bakıldığında 94. maddede muhakeme sürecinde kullanılabilecek delillere elkonulmasından bahsedilmiştir. 98. madde yukarıda genel olarak değinildiği üzere elkoyma emrini düzenlemiştir. Buna göre arama ve elkoyma tedbirleri hakim kararına bağlanmıştır. Zorlayıcı hallerde savcı ve diğer adli görevliler arama veya elkoyma kararı verebilmektedir (Basımevleri, matbaalar ve yazım ofisler ve bunların eklentilerinde elkoyma sadece hakim kararıyla olmaktadır.). Hakim kararı olmadan yapılan elkoyma 3 gün içinde hakim onayına sunulmaktadır. Hakim elkoymadan itibaren 3 gün içinde karar vermek durumundadır. Elkoyma ile ilgili olan kişiler bu kararlara karşı hehangi bir zamanda bir karar

---

[179] (Erişim), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/567-LEG-country%20profile%20Germany%20_1%20June%2007_En.pdf, 08 Eylül 2009.
[180] Abel, **a.g.m.**, s. 101.
[181] Abel, **a.g.m.**, s. 101.

verilmesini talep edebilmek için başvuru yapabilirler (StPO md. 98). Her iki tedbirde de ilgili kişiler veya bu tedbirlere maruz kalan kişilerin yetişkin yakınları hazır bulunabilir. 102. maddede şüpheli kişiler için arama yapılabileceği; 103. madde ise şüpheli dışındaki diğer kişiler için uygulanacak arama tedbirini konu edinmiştir. Böylelikle bilgisayarlara yönelik arama ve elkoyma tedbirleri sadece şüpheli ile sınırlı olmayıp diğer kişilere karşı da işletilebilecektir. 105. maddede aramanın uygulanma esasları; 107. maddede elkonulan eşyaların, delillerin veya nesnelerin liste halinde bu tedbirlere maruz kalan kişilerce talep üzerine verilmesi konularına yer verilmiştir. Şüpheliye veya sanığa ve diğer kişilere ait elkonulan bilgisayarın iadesi bu maddeye dayanılarak talep edilebilecektir. Şüpheliye ait belgelerin aranması 110. maddede belirtilmiştir. Belgelerin bilgisayarda da bulunabileceği mantığı ile belgelere ilişkin bu madde, bilgisayarların aranması ve elkonulmasında da uygulanacaktır.

Kanunun 161. maddesi savcılığın bilgi toplaması ve araştırma yapması konularını ele almıştır. Buna göre savcı, bilgi toplayabilmek için kamu makamlarıyla yazışabilir ve kendisi bizzat veya polis aracılığı ile bilgi toplayabilir. Kanunun 163. maddesinde ise polisin görevlerinden söz edilmiş olup suçlarla ilgili bütün delillerin elde edilmesi ve delillerin karartılmasını engellenmesi yükümlülüğü gösterilmiştir. Bu iki madde bilgisayarlara yönelik arama, kopyalama ve elkoyma tedbirleri bakımından uygulanabilir niteliktedir[182].

Avrupa Konseyi bilgisayarlara yönelik yeni bir arama ve kopyalama tedbirinin siber suçlarla etkin mücadelede kullanılması amacıyla yasal düzenleme altına alınmasını tavsiye etmiştir[183]. Bu yeni arama ve kopyalama tedbiri ile şüphelinin bilgisayarı gizli bir şekilde uzaktan aranacak ve depoladığı bilgileri kopyalanacaktır. Bu amaçla RFS (Remote Forensic Software) yani uzaktan adli arama programları tasarlanmıştır. Bir programa dayanan bu yeni tedbir hakkında "uzaktan arama", "online arama" ve "federal

[182] (Erişim), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/567-LEG-country%20profile%20Germany%20_1%20June%2007_En.pdf, 08 Eylül 2009.
[183] Abel, **a.g.m.**, s. 99.

trojan" gibi çeşitli adlandırmalar yapılmıştır[184]. Bu program türleri ile şüphelinin haberi olmaksızın bilgisayarına internet ortamından bir virüs yerleştirilmektedir[185]. Bu yerleştirilen virüs sayesinde şüphelinin bilgisayarında bulunan sabit diskteki ve çalışmakta olan hafızadaki (RAM ve ROM'daki) veriler araştırılabilir, e-posta trafiği denetlenebilir, gizli bir şekilde web sayfaları gözetlenebilir ve geçici mesajlar takip altına alınabilmektedir.

Almanya'da bu yöntem 20 Aralık 2006 tarihli Kuzey Rhine Vestfalya'daki Anayasa'yı Koruma Kanunu'nun 5. maddesi (Article 5.2 no.11) değişikliği ile hukuki bir zemine kavuşturulmuştur[186]. Bu değişiklik ile polis ve adli birimler, gizli izleme-internet üzerindeki keşif ve bilgi teknolojisi sistemlerine gizli erişim olmak üzere iki önemli tedbirle yetkilendirilmişlerdir. Söz konusu kanun değişikliğinin bazı maddeleri Alman Federal Anayasa Mahkemesi tarafından 27.02.2008 tarihli kararıyla iptal edilmiş ve hükümsüzlükle sonuçlandırılmıştır[187]. Mahkeme, kararının gerekçesinde Alman Anayasası'nın (Grundgesetz GG) 1. maddesindeki insanlık onuruna (1.1. GG) ve 2. maddesindeki kişi özgürlüklerine (2.1 GG) atıf yaparak "*Bilgi teknolojisi sistemlerinde mahremiyet ve doğruluk (bütünlük) hakkı*" olmak üzere anayasada olmayan, yeni bir hak ihdas etmiştir[188]. Bu yeni tedbiri düzenleyen kanunun bazı maddeleri anayasaya aykırıdır. Mahkeme kişisel bilgisayarların internet aracılığla yüklenen gizli ve uzaktan arama programlarıyla delil elde edilmesine yalnızca insan hayatını, devletin varlığını ve kamu güvenliğini tehdit eden durumlarda izin vermektedir. Buna ek olarak mahkeme, söz konusu tedbirin somut bir tehlikenin varlığı ve hâkim kararının olması halinde uygulanabileceğini vurgulamaktadır[189]. Böylelikle hâkim kararı olmadan soruşturma ve istihbarat amaçlı olarak uzaktan arama imkanı veren maddeler Anayasa Mahkemesi'nce iptal edilmiştir. Buna rağmen tedbirin

---

[184] Wieke Abel, Burkhard Schafer, "The German Constitutional Court on the Right Confidentially and Integrity of Information Technology Systems – A Case Report on BverfG, NJW 2008, 822." **SCRIPTed - A Journal of Law, Technology & Society**, April 2009, Volume I, Issue I, (Erişim), http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/abel.asp, 14 Eylül 2009**.**, s. 108.

[185] Abel, Schafer, **a.g.m.**, s. 108.

[186] Abel, Schafer, **a.g.m.**, s. 107.

[187] Abel, Schafer, **a.g.m.**, s. 110.; BverfG, NJW 2008, 822.

[188] Abel, Schafer, **a.g.m.**, s. 119.

[189] Abel, Schafer, **a.g.m.**, s. 109.

ileride tekrar gündeme gelebilmesi hakkında bir tartışma devam etmektedir[190].

Ceza muhakemesinde kıta avrupası sistemleri delil serbestisi ve hakimin delilleri serbestçe değerlendirmesi ilkelerini benimsemiştir[191]. Hakim delilleri değerlendirecek ve vicdani kanaatine göre hüküm verecektir. Kural olarak hakime delilleri değerlendirmede büyük bir serbesti tanınmıştır. Hakim kararını oluştururken bütün delil çeşitlerini kullanmada serbesttir. Bu itibarla Kıta Avrupası sistemlerinde bilgisayardan ve veri saklama birimlerinden elde edilen elektronik veriler yargılamada delil olarak kullanılabilecektir[192]. Kıta Avrupası hukuk sisteminin sacayaklarından biri olan Almanya'nın Ceza Muhakmesi Hukuku düzenlemelerinde elektronik delillerin diğer delillerle aynı vasıfları taşımakta olduğu kabul edilmekte ve yargılamada delil olarak kullanılmaktadır[193].

C- FRANSA

Fransa AK-SSS'ni 23.11.2001 tarihinde imzalamıştır. Sözleşme 10.01.2006 tarihinde onaylanmış, 01.05.2006 tarihinde de yürürlülük kazanmıştır[194]. Sözleşmeye uygun olarak ceza mevzuatında son yıllarda değişiklikler yapılmıştır.

Fransız Ceza Muhakemesi Kanunu'nun (Code de Procedure Penal) 94. maddesi 1991 ve 2004 yıllarında değişikliğe uğramış olup maddi gerçeğe ulaşmada işe yarayan herhangi bir yerdeki nesnelerin aranmasını

---

[190] Abel, Schafer, **a.g.m.**, s. 119.
[191] Leroux, **a.g.m.**, s. 205.
[192] Leroux, **a.g.m.**, s. 206.
[193] "Update to the Handbook of Legal Procedures of Computer and Network Misuse In Eu Countires For Assiting CSIRT, D: 15 Final Report", Ed: Lorenzo Valeri, **RAND EUROPE & LAWFORT**, December 2005, (Erişim) ftp://ftp.cordis.europa.eu/pub/ist/docs/directorate_d/trust-security/ec-csirt-d15.pdf, 26 Eylül 2009, s. 115.
[194] (Erişim) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG, 01 Aralık 2010.

düzenlemektedir. Bu genel hükmün elektronik verilere de uygulanacağı ifade edilmektedir[195].

Söz konusu kanunun 56. ve 97. maddeleri AK-SSS'nin 19. maddesiyle tutarlılık arzetmektedir[196]. Bahsedilen bu maddeler kağıtlara ve belgelere yapılan arama ve el koymayı düzenlemektedir. Düzenlemeler her ne kadar kağıtlara ve belgelere uygulansa da bilgisayarlara da uygulanması mümkün gözükmektedir[197]. Belgelerin bilgisayarda kayıtlı olduğu düşünüldüğünde bu iki hükmün bir arada uygulama alanı bulacağı ileri sürülebilir. Maddede öngörülen elkonulan nesnenin veya belgelerin bir liste altında tutulması, mühürlenmesi elektronik veri için de söz konusu olacaktır. Elektronik verinin elkonulması ya elektronik veriyi saklayan birimin elkonulmasıyla, ya da bir kopyasının alınmasıyla yapılabilecektir[198].

Genel olarak arama ve elkoymada hakim kararı esastır ve bu kararda makul şüphenin varlığı aranır. Bu kararı soruşturma hakimi vermektedir ki karar verildikten sonra uygulanan tedbirler soruşturma hakiminin denetimine tabidir[199]. Kararda verilen yetkiler çok geniş bir şekilde düzenlenmeyecek ve öngörülen meşru amaca orantılı bir şekilde yaklaşılacaktır[200]. Söz konusu kararların uygulanması adli polis (De la police judiciaire) başka bir ifade ile adli kolluk tarafından yapılacaktır.

---

195 "Update to the Handbook of Legal Procedures of Computer and Network Misuse In Eu Countires For Assiting CSIRT, D: 15 Final Report", Ed: Lorenzo Valeri, s. 108.

196 Lorenzo Picotti, Ivan Salvodori, "National Legsitation Implementing The Convention On Cybercrime-Comparative Analysis and Good Practises", **(Discussion Paper)**, 12.03.2008, Strasbourg,,., (Erişim), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/DOC%20567%20study2-d-version8%20provisional%20(12%20march%2008).PDF, 26 Eylül 2009, s. 50.

197 Picotti, Salvodori, **a.g.m.**, s. 50.

198 "Update to the Handbook of Legal Procedures of Computer and Network Misuse In Eu Countires For Assiting CSIRT", D: 15 Final Report", Ed: Lorenzo Valeri, s. 108.

199 "Update to the Handbook of Legal Procedures of Computer and Network Misuse In Eu Countires For Assiting CSIRT", D: 15 Final Report", Ed: Lorenzo Valeri, s. 106.

200 Funke vs. Fransa davasında mahkeme, arama emrinin alınmasını şart koşmuş ancak arama kararındaki yetkilerin orantısız ve yetkilerin genişçe ve gevşek olduğunu vurgulayarak Fransa'yı mahkum etmiştir. Bkz. Kenan Özdemir, "Türk Hukukunda ve Avrupa İnsan Hakları Sözleşmesi ile AİHM Kararlarında Özel Hayatın Gizliliği", (Erişim) http://www.hukuki.net/hukuk/index.php?article=515, 05.06.2009.;
(Kararın orijinali için bkz. Funke vs. Fransa davası, 25 Şubat 1993. http://cmiskp.echr.coe.int, Application no. 10828/84).

Ceza Muhakemesi Kanununun 57-1[201] maddesi bilgisayarlara ve veri saklama birimlerine yönelik özel bir düzenlemedir. Kanuni şartlar çerçevesinde uygulanan elkoyma sırasında adli kolluk görevlileri soruşturma için önemli görülen bilgisayar eklentilerinde ya da başka bir bilgisayar sistemi içerisinde kurulan bir bilgisayar sisteminde saklanan verilere erişmede yetkili kılınmışlardır. Elkoymanın kanundaki şartlara uygun ölçüde yapılması sırasında bu özel tedbir gündeme gelebilecektir. Maddedeki ifadelerden genel hükümlerdeki gibi bir elkoyma kararına ihtiyaç olduğu anlaşılmaktadır. Benzer şekilde kanunun bir önceki düzenlemesinde (md. 57) arama işleminin şüphelinin huzurunda yapılabileceğini şayet huzurda bulunamıyorsa onu temsil edebilecek bir kişi, temsil edebilecek bir kişi de yoksa iki kişinin şahitliği altında yapılabileceği belirtilmiştir. İlgili hüküm bilgisayarların aranması ve elkonulmasında da uygulanacaktır.

Kanunun 57. maddesinin ikinci fıkrası hâkimiyet alanın dışındaki verilerin elde edilmesiyle ilgilidir. İlk aranılan bilgisayar sistemindeki erişilebilen veya bilgisayar sistemi için erişilmesi mümkün görünen verilerin Fransa'nın hâkimiyet alanının sınırları dışında bir bilgisayarda olduğu öncelikle tespit edildiği takdirde adli kolluk birimleri ancak taraf olunan ikili sözleşmelerdeki hükümler ışığında veri toplayabilir[202]. Maddenin 3. ve son fıkrası da herhangi bir şekilde erişilen verinin bir veri saklama birimine kopyalanabileceğini ve veri saklama birimlerinin de elkoymaya veya koruma altına alınmaya konu olabileceğini belirtmiştir. Kanunun 2007 yılında getirilen 99-3. maddesi bilirkişiye başvuruyu düzenlemiştir[203]. Bahsedilen hüküm gereğince soruşturma hâkimi soruşturmayla ilgili olabilecek saklanan

---

[201] Fransız Ceza Muhakemesi Kanunu için bkz. Inserted by Law n° 2003-239 of 18 March 2003 Article 17 °1 Official Journal of 19 March 2003, (Erişim). http://www.legislationline.org/download/action/download/id/1674/file/848f4569851e2ea7eabfb2ffcd70.htm/preview, 24 Eylül 2009.

[202] Inserted by Law n° 2003-239 of 18 March 2003 Article 17 °1 Official Journal of 19 March 2003, (Erişim). http://www.legislationline.org/download/action/download/id/1674/file/848f4569851e2ea7eabfb2ffcd70.htm/preview, 24 Eylül 2009.

[203] Update to the Handbook of Legal Procedures of Computer and Network Misuse In Eu Countires For Assiting CSIRT", D: 15 Final Report", Ed: Lorenzo Valeri, s. 108.

elektronik verilerin ortaya çıkarılması için bir kimseye veya bir kuruma emir verebilmektedir.

Kıta Avrupası hukuk sisteminin diğer bir önemli ayağı olan Fransız Ceza Muhakemesi Hukuku sistemi delil serbestisi ve delillerin hâkim tarafından serbestçe değerlendirmesi ilkelerini esas almaktadır. Bu husus kanunun 427. maddesinde vurgulanmıştır. Hakim duruşma sırasında sunulan mevcut veya tartışılmış olan delilleri temel alarak vicdani kanaatine göre karar verecektir. Buna karşılık her delil yargılamada kullanılmaz. Ceza muhakemesinde deliller, bir takım koşullara sahip olmalıdır. Buna göre deliller hukuka uygun olarak elde edilecek, temel insan haklarını derinden ihlal edecek şekilde kullanılamayacak ve hukukun genel ilkelerine aykırılık teşkil etmeyecektir[204].

Sonuç olarak ceza muhakemesi sistemine göre elektronik delilin kabul edilebilirliği durumu genel hükümlerdeki duruma göre çözülecektir[205]. Kısaca elektronik delil, ceza muhakemesindeki bir delilin temel özelliklerini taşımalıdır.

Şifrelenmiş bilgilere ulaşma tedbiri 15 Kasım 2001'de kabul edilen Güvenlik Kanunu'nun (Loi sur la sécurité quotidienne-The Daily Security Act) 30. ve 31. maddeleriyle Fransız Ceza Muhakemesi Kanunu'nun 230. maddesine (230-1 ve 230-5 arası) özel olarak dahil edilmiştir[206]. Buna göre bölge savcısı soruşturmayla ilgilenen mahkeme veya esasa ilişkin ilk derece mahkemesi bu bilgilere erişimin önlenmesi durumunda erişimin sağlanabilmesi çözülebilmesi, okunabilmesi için yasal veya uzman bir kişiyi atayabilir. Atanan bu kişiler gerekli durumlarda şifre kırıcı yöntemlere de başvurabilirler. En az iki yıl ve daha fazla hapis cezasını gerektiren suçlarda ve kanunda öngörülen diğer hallerde bu tedbir uygulanabilecektir. Atama yetkisine sahip olan muhakeme süjeleri madde 230-2'de (bir önceki madde olan 230-1'e uygun olarak) ulusal adli kolluğa veri saklama birimlerindeki çözümün yapılabilmesi ve kopyasının alınması, bilgi sistemlerine sızan

---

[204] Leroux, **a.g.m.**, s. 208.

[205] "Update to the Handbook of Legal Procedures of Computer and Network Misuse In Eu Countires For Assiting CSIRT, D: 15 Final Report", Ed: Lorenzo Valeri, s. 108.

[206] Leroux, **a.g.m.**, s. 209.

suçların soruşturulmasına ait yetkileri yazılı bir izinle kullanacaktır. Madde 230-2'de belirtildiği üzere izin, bir süre ile sınırlıdır ve bu süre aynı koşullar altında uzatılabilir. Sürenin ne kadar olduğu konusunda herhangi bir belirlemeye gidilmese de verilecek sürenin makul olan bir süre olduğu anlaşılmaktadır. Tedbirin uygulanması tamamlanırsa; çözümün yapılmasının mümkün olmadığı anlaşılırsa; belirlenen sürede bir aşım söz konusuysa veya yargısal süjeler tarafından tedbirin sona ermesine ilişkin bir emir verilirse; toplanan deliller ve elde edilen çözümler adli kolluğun talebi üzerine resmi bir belgeye dönüştürülür. Bu husus madde 230-3'te yer almıştır. Madde 230-4 gereği, söz konusu koruma tedbirleriyle ilgili olarak alınan kararlara karşı temyiz kanun yoluna başvurulamaz.

Fransız Ceza Muhakemesi Kanunu'nda veya diğer özel kanunlarda trafik verileriyle ilgili herhangi özel bir koruma tedbiri mevcut olmadığı için genel hükümlerdeki arama ve elkoyma tedbirlerine başvurulmaktadır[207]. Trafik verilerinin gerçek zamanlı olarak toplanması tedbirinin ancak Fransız Ceza Muhakemesi Kanunu'nun 60. ve devamı maddelerindeki genel hükümler çerçevesinde uygulama alanı bulacağı belirtilmektedir[208]. Buradaki hukuki boşluk genel hükümlere yollama yapılarak doldurulmuştur. Söz konusu madde kriminal, bilimsel ve teknik incelemeler konusunu ele almaktadır.

D- AMERİKA BİRLEŞİK DEVLETLERİ

1- Genel Olarak

Amerika'da elektronik ortamda yapılan ticaret (kısaca e-ticaretin) hayati bir önem taşıdığından bunun korunması için bilişim sistemleri güvenliği konusu üzerinde özellikle durulmuştur. E-ticaret, internet ve bilişim alanındaki diğer gelişmeler, bilişim suçları olarak adlandırılan yeni suç tiplerini ortaya çıkarmıştır. Bilişim suçlarının ilk örnekleri bu ülkede işlenmiştir[209].

---

[207] Leroux, **a.g.m.**, s. 209.
[208] Picotti, Salvodori, **a.g.m.**, s. 73 vd 77.
[209] Karagülmez, **a.g.e.**, s. 83.

Bilişim suçlarıyla mücadelede en ileri ülke ABD'dir. Böyle olmasına rağmen bilişim suçları istatistiklere göre yine en fazla bu ülkede işlenmektedir. Bilişim suçları nedeniyle ekonomik zararlar söz konusu olmakta ve bilişim suçlarını önleyebilmek adına gerek CIA (Central Intelligence Agency) ve FBI'a (Federal Bureau of Investigation) gerek yerel adli birimler içerisinde veya bunlara bağlı çeşitli birimler ve gruplar oluşturulmuştur[210].

ABD bilişim suçlarında mücadele etmede olduğu kadar bilgisayar üzerinden elektronik delil elde etmede de ileri ülke konumundadır. Teknolojik alanda ilerleme hukuk alanına da yansımış ve bütün eyaletlerde uygulanabilecek kanunlar çıkarılmıştır. Bunun yanında her eyalet kendi suç tanımlamalarını içeren ayrıntılı kanuni düzenlemeler gerçekleştirmiştir[211]. Bilişim mevzuatı bakımından ABD'de federal alanda ilk olarak Bilgisayar Sahtekarlığı ve Bilgisayarların Kötüye Kullanılması Kanunu (Counterfeit Access Device and Computer Fraud and Abuse Act) 1984 yılında düzenlenmiştir. Bu kanun, 1986 yılında aynı isimle çıkarılan kanunla (Computer Fraud and Abuse Act of 1986) ve 1988, 1989 ve 1990 yıllarında bir takım değişikliklere uğramıştır[212]. Bu kanundan başka 1986 yılında Elektronik Fonların Transferi Kanunu[213] (Electronic Fund Transfers Act), Elektronik Haberleşme Gizlilik Kanunu (Electronic Communications Privacy Act - ECPA), 1997 yılında İnternette Kumarın Önlenmesi Kanunu (Internet Gambling Prohibition Online Prevention Act), 1998 yılındai Çocukların Online Yayınlardan Korunması Kanunu, (Child Online Prevention Act) ve 2001

---

[210] *"Amerika Birleşik Devletleri'nde teknolojik suçlar ve siber terörizmle mücadele eden pek çok kuruluş ve bu kuruluşlara ait özel birimler bulunmaktadır:*
1-FBI National Infrastructure Protection Center
2-FBI Computer Crime Squad
3-Information Technology Association of America
4-Trap and Trace Center Authority
5-Carnegie Mellon's Emergency Response Team
6-Commision of Critical Infrastructure Protection
7-CIA Information Warfare Center". (Bünyamin Atıcı, Çetin Gümüş, "Sanal Ortamda Gerçek Tehditler: Siber Terör", **Polis Dergisi**, Sayı 37, y.y., (Erişim) http://www.egm.gov.tr/egitim/dergi/eskisayi/index.htm, 01 Ekim 2009).

[211] Kurt, **a.g.e.**, s. 101.

[212] Casey, **a.g.e.**, s. 208, 209.

[213] Karagülmez, **a.g.e.**, s. 85.

yılında Anti Terörizm Kanunu (USA- Patriot Anti-Terrorism Act) çıkarılmıştır[214].

Bilişim suçları bakımından zengin bir mevzuata sahip olan bu ülke AK-SSS'ni 23.11.2001 tarihinde imzalamıştır. Sözleşmeye 29.09.2006 tarihinde onay verilmiş 01.01.2007 tarihinde de yürürlülük kazandırılmıştır[215].

2- Arama Tedbiri ve Özel Hayatın Gizliliği

Özel hayatın gizliliği konusu ABD anaysasının temel metninde ve Haklar Bildirisi'nde (Bill of Rights) açıkça ifade edilmemiş olup mahkemelerin kararlarında esas aldığı anayasaya eklenen Dördüncü Değişiklik'te (The Fourth Amendment) gösterilmiştir[216].

ABD Anayasası'ndaki Dördüncü Değişiklik; (U.S. Consitiution-The Fourth Amendment) kişilerin kendilerini, evlerini, belgelerini ve diğer nesnelerini makul olmayan aramalara karşı korumakta ve arama için bir arama kararını (search warrant) şart koşmaktadır[217]. Makul olmayacak aramalar için arama kararı düzenlenmeyecektir. Arama yetkisini veren karar, mutlaka makul bir sebebe dayanmalı (probable cause)[218] yemin veya bir beyanla desteklemeli ve aranılacak yer, tutulacak kişi ve elkonulacak eşya özellikle belirlenmelidir. Yüksek mahkeme (The Supreme Court) arama

---

[214] Kurt, **a.g.e.**, s. 99.

[215] (Erişim) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG, 01 Aralık 2010.

[216] Jonathan Rosenoer, **Cyberlaw: The Law of Internet**, New York, Springer, 1997, s. 130.

[217] "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons ot things to be seized.*". (Amerikan Anayasasındaki Dördüncü Değişiklik (U.S.-The Fourth Amendment) (Erişim) http://caselaw.lp.findlaw.com/data/constitution/amendment04/, 03 Ekim 2009).

[218] Joanne Banker Hames, Yvonne Ekern, **Constitutional Law: Principles and Practice**, The West Legal Studies Series, Clifton Park-New York, Thomson Delmar Learning, s. 435; Probable Cause; "Muhtemel Neden" veya "Makul Sebep" olarak çevrilse bile makul şüpheden daha kuvvetli bir şüpheyi ifade eder. Polis memurunca şüphelinin aranmadan veya yakalanmadan önce bilinen olaylar ve durumlar değerlendirerek kararlaştırılır. Bireyin suç işlediğine dair bir kanaat, bu makul şüpheye kaynaklık eder. Başka bir tanım için bkz. "*The most well-known definition of probable cause is "a reasonable belief that a person has committed a crime. ... "Probable cause" is a stronger standard of evidence than a reasonable suspicion, but weaker than what is required to secure a criminal conviction.*" ((Erişim) 03 Ekim 2009 http://en.wikipedia.org/wiki/Probable_cause).

kararında aranılan nesnelerin belirtilecek olmasının genel bir şekilde yapılan aramaları imkânsız hale getireceğini ve arama kararında olmayan başka bir şeye el konulmasını önleyeceğini vurgulayarak anayasayı yorumlamıştır.[219] Özetle anayasadaki Dördüncü Değişiklik arama ve elkoymada makul olanı teşvik etmekte ve bireylere devletin müdahalelerine karşı anayasal bir güvence sağlamaktadır. Buna karşılık Dördüncü Değişiklik özel müdahalelere karşı bir güvence oluşturmamaktadır[220].

Katz vs. ABD davasında Yüksek Mahkeme dava konusu elektronik haberleşme ile ilgili olsa da arama ve elkoyma bakımından emsal sayılacak bir karar vermiştir. Karar, "Katz Testi" olarak Amerikan hukuk sisteminde yer edinmiş olup arama ve elkoymalarda önemli bir bakış açısı getirmiştir[221]. Bu teste göre mahkeme, bireyin mevcut özel hayatın gizliliğine ilişkin beklentisine (expectation of privacy) müdahale teşkil edecek bir ihlalin olup olmadığını ve bu beklentinin kamuoyunca makuliyet içerisinde görülüp görülmediğini saptamak zorundadır[222]. Test sonucunda müdahale ihlal niteliği taşımıyorsa ve makuliyet içerisinde görülüyorsa yapılacak aramalar hukuka uygun olacaktır[223].

3- Bilgisayarda Uygulanan Arama ve Elkoyma Tedbirleri

Bilgisayarlardan elektronik delil elde etmeye ilişkin tedbirler, kaynağını Dördüncü Değişiklik'ten almaktadır. 18 USC (United States Code) § 2510-22 (ECPA), 18 USC §§ 2701-12 ve 18 USC §§ 3121-27 sayılı kanunlarda bilgisayarlardan elektronik delil elde etmeye yönelik hükümler mevcuttur[224]. Bu kanunlar esasen elektronik haberleşmede hukuka aykırı erişim, transit ve

---

[219] Marron vs . United States, 275 U.S. 192, 196 (1927); (David J. S. Ziff, "Fourth Amenment Limitations On The Execution Of Computer Searches Conducted Pursuant To A Warrant", **Columbia Law Review**, Vol 105, Issue 3, April 2005, (Erişim), http://web.ebscohost.com/ehost/pdf?vid=3&hid=5&sid=916b04fe-ccb4-4635-bb13-60b508d6615b%40sessionmgr7, 03 Ekim 2009, s. 843).

[220] Rosenoer, **a.g.e.**, s. 131.

[221] Katz vs. United States, 389 U.S. 347, 362 (1967); (Orin S. Kerr, "Searches and Seizures In a Digital World", **Harward Law Review**, Vol 116, 531, December 2005 - 2006, (Erişim) http://web.si.umich.edu/tprc/papers/2005/495/orinkerrhlr.pdf, 03 Ekim 2009, s. 585).

[222] Ziff, **a.g.m.**, s. 843.

[223] Ziff, **a.g.m.**, s. 844.

[224] Karagülmez, **a.g.e.**, s. 91.

veri saklama birimlerinde kaydedilmiş olan haberleşmenin ortaya çıkarılması ve teknik takibin yapılmasıyla ilgilidir[225]. Dördüncü Değişiklik'teki genel arama ve elkoyma tedbirleri ise yeni yürürlülük kazanan Federal Ceza Muhekemesi Kuralları'nın (The Federal Rules of Criminal Procedure 2009) 41. maddesinde[226] ve 18 USC § 3101-18 sayılı kanunda ayrıntılı bir biçimde düzenlenmiştir[227]. Amerika'da 11 Eylül olayları yüzünden ekim ayında yürürlülüğe giren Anti-Terörizm Kanunu (The USA Patriot Act 2001) internet ve haberleşme özgürlüğünü önemli ölçüde kısıtlamıştır[228]. Bu kanunun 220. maddesi yukarıda bahsettiğimiz § 2701 ve § 3127 sayılı kanunlarda bulunan terimleri değiştirerek ve yeni terimler ekleyerek elektronik delil için arama kararına dayanılan aramanın ülke çapında uygulanmasını sevk etmektedir[229]. 220. madde FBI aramalarını kolaylaştırmış ancak zaman içinde bu maddenin yürürlülüğü sona ermiştir[230].

Bilgisayarlardan elektronik delil elde edilmesini gerektiren bir suç şüphesi söz konusu olduğunda, Dördüncü Değişiklikğe veya ECPA'ya başvurulabilirlik imkânının bulunup bulunmadığı, adli birimlerin olay yerinde ne kadar durabileceği ve olay yerine tekrar giriş yapılabilmesi için hangi hukuki araçlara ihtiyaç duyulacağı gibi bir takım sorunlar vukubulmaktadır[231].

---

[225] Rosenoer, **a.g.e.**, s. 132, 133; Ayrıca kanuna erişmek için bkz. U.S. Code, Title 18, Chapter: 119, Wire And Electronic Communications Interception and Interception Of Oral Communications, (Erişim) http://www.law.cornell.edu/uscode/html/uscode18/usc_sup_01_18_10_I_20_119.html; U.S. Code, Title 18, Chapter: 121, Stored Wire and Electronic Communications and Transactional Record Access, (Erişim) http://www.law.cornell.edu/uscode/html/uscode18/usc_sup_01_18_10_I_20_121.html, 03 Ekim 2009.

[226] Fedaral Rules of Criminal Procedure 2009, (Erişim) http://www.law.cornell.edu/rules/frcrmp/, 03 Ekim 2009.; Yeni düzenlemeler içeren bu kanunda elektronik olarak cihazların izlenmesi tedbirine de verilmiştir.

[227] U.S. Code: Title: 18, Chapter 205, Searches and Seizures, (Erişim) http://www.law.cornell.edu/uscode/html/uscode18/usc_sup_01_18_10_II_20_205.html, 03 Ekim 2009.

[228] Gerald R. Ferrera, Stephen D. Lichtenstein, Margo E. K. Reder vd... **CyberLaw: Text and Cases**, Second Edition, Ohio, Thomson\South-Western\West, 2004, s. 386.

[229] The USA Patriot Act of 2001, Nationwide Service of Search Warrants For Electronic Evidence (Erişim) http://epic.org/privacy/terrorism/hr3162.html, 19 Ekim 2009.

[230] The USA Patriot Act Sunset, Expiring Sections, (Erişim) http://epic.org/privacy/terrorism/usapatriot/sunset.html#intro, 20 Ekim 2009.

[231] Casey, **a.g.e.**, s. 215.

Bu sorunların çözümü Dördüncü Değişiklik kapsamında, mahkeme kararları penceresinden aranacaktır.

Bu konudaki ana kaynak olan Dördüncü Değişikliğe uygun bir biçimde arama ve elkoyma tedbirlerini uygulayabilmek için mutlaka bir arama kararı gereklidir. Başlıca elektronik haberleşme, bilişim, çocukların online yayınlardan korunması ve anti terörizm kanundaki suç tanımlarına bağlı olarak suç şüphesi altındaki kişilerin bilgisayarlarını aramada karar, hakim (magistrate) tarafından verilir. Polis veya adli birimler bir yerde arama yapabilmek için makul sebepleri mahkemeye sunmalıdır. Makul sebepler bir beyanın zapta geçirilmesiyle veya bir dilekçe ile mahkemeye sunulur[232]. Dilekçede arama ve elkoymanın hangi araçlar üzerinde yapılabileceği veya bu araçlar üzerinde hangi tür verilere bakılacağı belirtilecektir. Hâkim bu hususları değerlendirmek suretiyle arama kararı verebilir. Arama Federal Ceza Muhakemesi Kuralları'nın 41. maddesinin 2. fıkrasının "e" bendinin A paragrafına göre kural olarak gündüz zamanı yapılır. Hâkim gerekçe göstererek gece vakti için de arama kararı verebilmektedir. Maddenin B paragrafında ise karar, veri saklayan birimlerine elkoymayı ya da bunların içindeki verilerin kopyalanmasını içerebilecektir[233]. Arama kararı bilgisayarların aranmasından ziyade elkoyma ve kopyalamaya yönelik olduğundan arama tedbiri çıkartılacak kopya üzerinden işletilecektir. Arama kararı verildikten sonra polis kararda bahsedilen verilere elkoyabilir. Elkonulan veriler arama kararında önceden bahsedilmişse uygulanan tedbir makuliyet içerisindedir[234]. Hal böyle iken arama kararında belirtilen soruşturma ile ilgili suç dışında tüm verilerin elkonulduktan sonra yargılamada kullanılması Dördüncü Değişikliği ihlal eden bir tedbir

---

[232] Hames, Ekern, **a.g.e.**, s. 435.

[233] Warrant Seeking Electronically Stored Information. *A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review."* (Fedaral Rules of Criminal Procedure 2009, (Erişim) http://www.law.cornell.edu/rules/frcrmp/,.03 Ekim 2009).

[234] Kerr, **a.g.m.**, s. 537.

olacaktır[235]. Somut olayda makul bir sebebin olmadığı ispat edildiği takdirde arama sonucunda elde edilen deliller kullanılmayacaktır[236].

Bilgisayarlara yönelik aramalar ile evlere ilişkin aramalar arasında kapalı bir konteynırdaki delillere ulaşma ve onları elde etme açısından bir benzerlik olduğu vurgulanabilir[237]. Buna karşılık adli bilişim süreci ayrı bir süreç içerdiği için aralarında farklılıkların olması da doğaldır. Kapalı bir konteynırdaki bilgileri açmayı engelleyen bir durum varsa bilgisayardaki bilgilere erişme ve onları elde etmede de bu engelleyici durumdan bahsedilecektir[238]. Aynı perspektiften bakıldığında veri saklama birimlerinin kapalı bir konteynır gibi algılanması mümkündür. Böylece tedbirlere konu olan veri saklama birimlerine sahip olan kişiler için özel hayatın gizliliğine ilişkin beklentileri gündeme gelecektir. Sonuç olarak bu husus Dördüncü Değişiklik çerçevesinde ele alınacak ve delil elde etmede arama kararına ihtiyaç duyulacaktır[239].

Arama kararı olmadan da başka bir ifadeyle Dördüncü Değişiklik kapsamı dışında da arama ve elkoyma tedbirlerine başvurulabilir. Rızanın varlığı, aciliyet içeren durumlar, makul sebepler içerisinde arabada yapılacak aramalar, havaalanı ve sınır aramaları, kamuya açık alanlardaki aramalar, Çıplak Gözle Görme Doktrini'ne (Plain View Doctrine) istinaden yapılan aramalar ve terkedilmiş mülkiyette yapılacak aramalar genel kuralın istisnasını oluşturmaktadır[240]. Bu istisnaların bir kısmı bilgisayarlara yönelik arama ve elkoyma tedbirleri için de uygulanabilmektedir.

Rıza söz konusu olduğunda bir arama kararına ihtiyaç duyulmayacaktır. Şüpheli rızaen kendi bilgisayarında elektronik delil

---

[235] Telefon konuşmalarıyla ilgili bir suç soruşturması sırasında mahkeme bütün verilerin elkonulmasını, aranılan dosyanın belirlenmediği gerekçesiyle Dördüncü Değişikliğe aykırı olduğunu hükmetmiştir. United States v. Riccardi, 405 F.3d 852, 862 (10th Cir. 2005); ((Erişim), http://www.cybercrime.gov/ssmanual/02ssma.html#A., 15 Kasım 2009).

[236] Fred Galves, Christine Galves, "Ensuring Admissibility of Electronic Forensic and Enhancing Its Probative Value At Trial", **Criminal Justice Magazine,** Vol: 19, Number 1, Spring 2004, (Erişim) http://www.abanet.org/crimjust/cjmag/19-1/electronic.html, 13 Ekim 2009.

[237] Kerr, **a.g.m.**, s. 532.

[238] Karagülmez, **a.g.e.**, s. 91.

[239] Karagülmez, **a.g.e.**, s. 91.

[240] Hames, Ekern, **a.g.e.**, s. 436.

aramasına izin verebilmektedir[241]. Rızanın varlığını ispat çok önemli bir konudur. Adli birimler, geçerli rızanın alındığını mahkemede kanıtlamak zorundadır. Bu nedenle rızanın yazılı olarak alınmasının uygulamada faydası vardır. Arama ve elkoymada rızanın sadece rızayı veren kişinin kendisini bağlayacak şekilde verilebileceğine ilişkin bir hüküm öngörülmemiştir. Rıza diğer kişilere etki edecek şekilde de verilebilir. Fakat rızayı verenle tedbirlere maruz kalan arasında hukuki bir ilişki mevcut olmalıdır. Örneğin; ailedeki diğer kimselere ait bilgisayarlardaki elektronik verilerin elde edilmesinde rıza verilebilir[242]. Aynı şekilde rıza, işveren veya sistem yöneticisi tarafından verilirse arama kararı talep edilmeksizin çalışanların bilgisayarlarından da elektronik delil elde edilebilecektir[243].

Çıplak Gözle Görme Doktrini'ne göre (Plain View Doctrine)[244] eşya suçun delili ise veya bulundurulması suç olan bir eşyanın varlığı konusunda kolluk görevlilerinin makul sebeplere dayalı bir kanaati varsa; eşyanın suç karakteri hemen farkedilmişse; hakim kararına başvurulmadan elkoyma tedbiri işletilebilir[245]. Lâkin bu yola gidebilmek için polisin elkonulacak eşyayı gözlemlemede hukuka uygun bir konumda olması gerekir.

Bu doktrin dâhilinde elektronik delil elde edebilmek için bir yerde fiziksel delil arandığı sırada suç delili olabilecek veya bulundurulması suç olacak bir veri bilgisayar ekranına yansımışsa ve açıkça gözle görülebiliyorsa arama kararı olmadan elkonulması mümkündür[246]. Ancak mahkemeler buna istisnai hallerde cevaz vermişlerdir[247].

---

[241] Galves, Galves, **a.g.m.**, s. 2.
[242] Galves, Galves, **a.g.m.**, s. 2.
[243] Galves, Galves, **a.g.m.,** s. 3.
[244] *"Mesela müsade edilen hız limitinin üzerine çıktığı için polis tarafından durdurulan bir aracın içerisinde "bulundurulması suç teşkil eden bir eşya gözüküyorsa, söz gelimi arka koltuğpun üzerinde bir tabanca duruyorsa, polis bu eşyaya hakim kararı olmadan elkoyabilir. (plain view doctirine)".* Kunter, Yenisey, Nuhoğlu, **a.g.e.**, s. 1060.
[245] Ziff, **a.g.m.**, s. 844, 866.
[246] Robert Moore, "Plain View and Digital Evidence", **American Journal of Criminal Justice**, Volume 29, Number 1, 2004, (Erişim) http://www.springerlink.com/content/rj8x868346127281/, 05 Ekim 2009., s. 64.
[247] Soruşturma daha çok uyuşturucu trafiği ile ilgili ise de soruşturma esnasında bir tane çocuk pornosu görüntüsü fark edilmiş ve soruşturmayla ilgili arama terkedilerek şüphelinin disketlerinde söz konusu görüntülerin yüzlercesi bulunmuştur. Mahkeme Carey hakkında aramanın hukuka uygun olmadığını belirterek beraat kararına hükmetmiştir. Kararı değerlendiren bir görüşe göre bu doktirin adli memurların gözüne çarpan sadece tek bir çocuk

Adli bilişim süreciyle birlikte bilgisayarlara yönelik Dördüncü Değişikliğe ve Çıplak Gözle Görme Doktirini'ne göre arama ve elkoyma tedbirlerini işletmek sorunlar doğuracaktır[248]. Örneğin suç delili veya bulundurulması suç teşkil eden eşya bir bilişim suçu verisi olabileceği gibi bir organize suç örgütü kayıtları da olabilmektedir. Genellikle bu tür bilgiler şifrelenmiş bir şekilde saklanmış olduğundan farkedilebilmeleri zordur ve çözülmeleri de zaman alacaktır[249]. Arama ve elkoyma tedbirleri sınırlılık içerisinde kalmaktadır. Bazı yerel mahkemeler arama kararında öngörülen sınırın belirli istisnalar haricinde çıkılmasının mümkün olamayacağına hükmetmişlerdir[250]. Bu nedenle bir bilgisayar kopyasında yapılacak arama, makul bir sebebe dayalı olarak bir başka bilgisayara veya bir veri saklama birimine karşı genişletilemeyecektir[251]. Arama kararının kapsamının genişletilmesinde ortaya çıkan zorluklar; yeni bir arama kararının gündeme gelmesine, aramanın yetkisiz olmasına ve arama işlemine derhal son verilip geri dönülmesi sorunlarına yol açmaktadır[252]. Sorunlarla karşılaşmamak için polis, hakime sunduğu beyanında bu tür durumların ortaya çıkabileceğini göstermeli ve buna uygun arama kararı almalıdır.

Bir mahkeme kararında acil durum istisnası dâhilinde hâkim kararı olmadan bilgisayarlarda veya veri saklama birimlerinde (disket ve PDA chiazlarına) arama ve elkoyma tedbiri işletilmesinin hukuka aykırı olmadığı sonucuna ulaşılmıştır[253].

---

pornografisi görüntüsüne dayanarak uygulanabilecektir. Kararda tartışılmasa da devam eden görüntüler için mutlaka bir arama kararı veya diğer istisnaların gerçekleşmesi gerekmektedir. United States vs. Carey, 172 F. 3d 1268, 1999; (Moore, **a.g.m.**, s. 65.).

248 Jerry Wegman, "Computer Forensics: Admissibility of Evidence In Criminal Cases", **Journal of Legal, Ethical and Regulatory Issues,** Volume 8, Number 1, 2005, (Erişim) http://www.cbe.uidaho.edu/wegman/Computer%20Forensics%20AA%202004.htm, 05 Ekim 2009, s. 3.

249 Wegman, **a.g.m.**, s. 3.

250 Horton vs. California davasında polisin ve ilgili memurların arama kararında saptanan sınırların dışına çıkılmaması gerektiğine hükmetmiştir. 496 US 128, 128 88-7164, (Ziff, **a.g.m**., 854 ve 855).

251 Wegman, **a.g.m.**, s. 3.

252 Karagülmez, **a.g.e.**, s. 90.

253 Yalnızca bir mahkeme kararında bu durum mevcuttur. Acil durum istisnası altında bilgisayarlara elkoymanın bir karar olmadan işletilmesine izin vermiştir. Mahkeme kararından arama kararı için başvurulmasının zaman kaybına yol açacağı ve tespit edilen yerdeki dosyaların silinebileceği endişesiyle derhal elkonulduğu anlaşılmaktadır. Acil durum istisnası

Akışkan verilerin başka bir ifadeyle internet-online ortamdaki verilerin elkonulmasıyla ilgili herhangi bir mahkeme kararı da bulunmadığından fiziksel olarak veri saklama birimlerine ve verinin kendisine bu tedbirler uygulanmakta ise de içeriğinin incelenmesi için uygun ölçekteki bir arama kararına gerek duyulmaktadır[254].

Polis bilgisayara arama ve elkoyma tedbirlerini kural olarak arama kararının yayımlanmasından itibaren Federal Ceza Muhakemesi Kuralları'na göre (41. maddesi [b] [1]) kararda belirtilen süre içinde yerine getirecektir. Arama kararında bu süre 14 günü aşamaz. Polisin bilgisayara elkoyduktan sonra ne kadar sürede inceleme yapacağı kanun veya kurallarda yer almasa da bir mahkeme kararında belirlemeye gidilmiştir[255]. İlgili davada öngörülen süre (30 gün) dava ile sınırlı olup genel bir düzenleme teşkil etmemektedir. Buna ek olarak adli birimler gecikmeksizin tedbirlere konu birimler üzerinde incelemelerini tamamlayacaklardır[256].

Dördüncü Değişiklik çerçevesindeki özel hayatın gizliliğine ilişkin beklentiler bilgisayarlara yönelik arama ve elkoyma tedbirleri için de gündeme gelecektir. Örneğin bir mahkeme kararına göre; Hava Kuvvetleri Askeri Yüksek Mahkemesi çocuk pornografisi suçunda sanığın oluşturduğu e-posta iletimlerinin Amerika Online Bilgisayarı'nda (America Online Computer) depolandığı sürece özel hayatın gizliliğine saygı duyulmasına hükmedilmiştir[257]. Kararın gerekçesinde; bireyin bilgisayarda depolanan bu e-postalara kendi oluşturduğu şifre ile girebildiği; kendi şifreleriyle kendi hesaplarına bağlanabilen abonelerin özel hayatın gizliliğine ilişkin bir beklentisinin olduğunu vurgulamıştır[258]. Öte yandan her arama ve elkoyma tedbiri bireyin özel hayatın gizliliğine ilişkin beklentisine aykırırlık oluşturmaz.

---

altında bilgisayarlara elkoymanın bir karar olmadan işletilmesine izin vermiştir. Mahkeme kararından arama kararı için başvurulmasının zaman kaybına yol açacağı ve tespit edilen yerdeki dosyaların silinebileceği endişesiyle derhal elkonulduğu anlaşılmaktadır. *United States v. Gorshkov,* 2001 WL 1024026 (2001). (Arrest Doctirine); (Moore, **a.g.m.**, s. 60).

[254] Moore, **a.g.m.**, s. 60.

[255] İlgili davada polisin elkonulan bilgisayar üzerinde inceleme yapabilmesi 30 günlük bir süre ile kısıtlanmıştır. United States vs. Brunette, 76 F. Supp. 2d 30, 1999, (Wegman, **a.g.m.**, s. 4).

[256] Wegman, **a.g.m.**, s. 4.

[257] Rosenoer, **a.g.e.**, s. 131.

[258] United States vs. Maxwell, 42 M.J. 568. (Rosenoer, **a.g.e.**, s. 131).

Örneğin ABD-Simons davasında CIA adına çalışan bir memurun işyerindeki kendi çalışma bilgisayarına çocuk pornografisi ile ilgili dosya indirdiğine dair bir şüphe doğmuştur. Buna dayanarak CIA herhangi bir arama kararı elde etmeksizin bilgisayarı, uzaktan erişimli olarak aramış ve çocuk pornografisi fotoğraflarını bulmuştur. Sanık bu aramanın özel hayatın gizliliğine ilişkin beklentisini ihlal ettiğini savunmuştur. CIA ise kendilerinin bir internet kullanım politikası olduğunu ve buna göre periyodik olarak internet erişiminin denetlendiğini ileri sürmüştür. Mahkeme bu resmi politikayı esas alarak çalışanın özel hayatın gizliliğine ilişkin beklentisinin olay içerisinde varolmadığını ve arama kararı alınmadan da arama yapılabileceğini hükmetmiştir[259].

Son yıllarda ABD'de ve dünya üzerinde, etkisi çığ gibi büyüyen "Facebook" ve "MySpace" gibi internet sitelerindeki kişilere ait profillerin özel hayatın gizlilik beklentisi kapsamına girip girmediği tartışılmaktadır[260]. Bununla ilgili birçok davanın ortaya çıkacağına kesin gözüyle bakılmaktadır.

Elektronik deliller önceleri ABD'de diğer suçlarda kullanılan deliller gibi algılanmakta ve mahkemelerce kullanılmaktayken teknoloji alanındaki yeni gelişmeler bu delilleri şüpheli ve tartışmaya açık duruma düşürmüştür[261]. Elektronik delil, Federal Delil Kuralları'na (The Federal Rules of Evidence)[262] bağlı olarak mahkemeye sunulacaktır. Bu kuralların 1001. maddesinde elektronik delilin ikinci bir kopya ve en önemlisi orijinali ile eşdeğer olması gerektiğinin altı çizilmiştir[263]. Elektronik delilin mahkemede kabul edilmesi; elde edilmesinde herhangi bir hukuka aykırılığın olmadığına ve bozulmaya uğramadığına bağlıdır. Mahkemede bu hususlar ispat edilecektir. Yukarıda belirtildiği üzere elektronik deliller bilimsel delil sistemine dâhildir. Özünde

---

[259] United States vs. Simons, 206 F. 3d 392, 2000, (Wegman, **a.g.m.**, s. 5).

[260] Matthew J. Hodge, **"**The Fourth Amendment and Privacy Issues On The "New" Internet: Facebook.com, and MySpace.com", **Sourthern Illinois University Law Journal**, 31, 95, 2006-2007 (Erişim) www.law.siu.edu/research/31fallpdf/**fourthamendment**.pdf., 20 Ekim 2009.

[261] Karagülmez, **a.g.e.** s. 367.

[262] The Federal Rules of Evidence (Erişim) http://www.law.cornell.edu/rules/fre/rules.htm#Rule1001, 20 Ekim 2009.

[263] Karagülmez, **a.g.e.**, s. 367.

bilimsellik taşıdığından doğruluğunu ispatlamada "Daubert Testi" gibi bilimsel testler uygulanabilir[264].

Özetle Dördüncü Değişikliğe aykırı olarak yapılan bir arama, istisnalar haricinde kişilerin özel hayatın gizliliğine ilişkin beklentilerini ihlal edecektir. Böylece makul olmayan arama ve elkoymalar yüzünden elde edilen deliller hukuka aykırı sayılacak ve mahkemece kabul edilmeyecektir[265]. Hakim bu delili kullanmayacak ve diğer delillerle davayı sonuçlandıracaktır.

Adli bilişim alanında en ileri ülkelerden biri olan ABD, ceza muhakemesinde bilgisayarlara yönelik arama ve elkoyma tedbirlerini uygularken adli bilişim sürecini yukarıda bahsettiğimiz belirli kriterler dahilinde uygulamaktadır. Ayrıca ABD'deki adli bilişim birimleri bu kriterleri her zaman gözden geçirerek gelişen teknoloji ve yeni suç tiplerine göre güncellemekte ve bu kriterleri düzenlediği sempozyum ve konferanslara ev sahipliği yaparak duyurmaktadır. Adli bilişim sürecinde, elektronik delilin güvenilirliği ve kabul edilebilirliği konularında yaygın ve etkin olabilecek standartları belirleme yönündeki çalışmalar ABD'de devam etmektedir.

III- SÖZLEŞMEYE TARAF OLMAYAN ÜLKELERDE BİLGİSAYARLARA YÖNELİK ARAMA KOPYALAMA VE ELKOYMA TEDBİRLERİ

A- AVUSTRALYA

İngiliz uluslar topluluğu içerisinde yer alan bu ülke (British Commonwealth) AK-SSS'ne taraf değildir. 2001 tarihli Siber Suç Kanunu ile

---

[264] ABD'de Yüksek Mahkemenin 1993 yılında Daubert vs. Merrel Dow Pharmacuticals davasında ileri sürülen delillerin doğruluğunu bilimsel olarak ispata yarayan bir testtir. Bu test diğer bir bilimsel delilin doğruluğunu ispatlamaya yarayan Fyre testi gibi bir ön duruşmada uygulanır. Burada bilimsel delilin doğruluğu ispatlanmaya çalışılır. Aynı zamanda bu husus Federal Delil Kurallarının 702. maddesine dayanmaktadır. Buna göre bir delil bilimsel teknik veya uzmanlık bilgisi dahilindeyse o delilin doğruluğu, kanıtlama özellikleri, niteliği bir uzmanca bilimsel yöntemlerle test edilecektir. Bkz. Karagülmez, **a.g.e.**, s. 369, 373.

[265] Ferrera, Lichtenstein, Reder vd.. **a.g.e.**, , s. 386.

(The Cybercrime Act 2001) Avustralya Ceza Kanunu'na (Ciriminal Code Act 1995) bilişim suçlarıyla ilgili eklemeler yapılmıştır. Bu kanun 11 Eylül olaylarının neticesinde terörizmle savaş anlayışı içerisinde siber terörizmin (cyberterrorism) önlenmesi amacıyla çıkarılmıştır[266]. Kanun düzenlenirken AK-SSS'nin hazırlık taslakları ve İngiltere'deki Bilgisayarı Kötüye Kullanma Kanunu (CMA 1990) örnek alınmıştır[267]. Öte yandan her eyaletin kendine özgü kanunları olsa da ülkedeki genel kanunlara tabidirler. Örneğin Yeni Güney Galler (New South Wales) eyaletinde Siber Suç Kanunu esas alınarak getirilen Suçlar Kanunu değişikliği ile 1900 tarihli yerel Suçlar Kanunu'na siber suçlar ile ilgili eklemeler yapılmıştır[268].

Bilişim suçlarında bilgisayarlara yönelik arama ve elkoyma tedbirlerini öngören iki kanun vardır. Bunlar: 1914 tarihli Suçlar Kanunu (The Crimes Act 1914)[269] ve 1901 tarihli Gümrükler Kanunudur (The Customs Act 1901). Elektronik delil elde etmede ağırlıklı olarak Suçlar Kanunu'ndaki düzenlemeler kullanılmaktadır. Avustralya Parlamentosu'ndaki hukuk ve anayasa komisyonunca çıkarılan siber suçları açıklayan memoranduma göre (Inquiry into Provisions of The Cybercirme Bill 2001) Gümrükler Kanunu'ndaki ilgili hükümler ihracat-ithalat kayıtlarının bilgisayarlarda olması ve bilgisayardaki bu kayıtların aranmasında veya elkonulmasınıda uygulanacaktır[270]. Burada konuya ilişkin bir ayrımın yapıldığı göze çarpmaktadır. Arama ve elkoyma yetkilerini düzenleyen kanunlar sadece bunlarla sınırlı değildir. Telekomünikasyon Kanunu ve (Telecommunnications Act 1997) Spam Kanunu (Spam Consequential Amenments Act 2003) arama ve elkoymanın özel kısmını oluşturan hükümler içerirler. Bu

---

[266] Simon Bronitt, Miriam Gani, "Shifting Boundaries of Cybercrime: From Computer Hacking to CyberTerrorism", **Crime Law Journal**, Number 27, (Erişim) http://law.anu.edu.au/UnitUploads/LAWS8164-2581-Bronitt%20and%20Gani.pdf, 24 Ekim 2009 s. 303.

[267] David Teisserie, "Cybercrime Legistation – The Kangaroo Perspective", (Erişim) http://www.scribd.com/doc/7545925/Cyber-Crime-Legislation-The-Kangaroo-Perspective, 23 Ekim 2009. s. 1.

[268] The Crimes Amendment (Computer Offences) Bill 2001, (Teisserie **a.g.m.**, s. 2).

[269] The Crimes Act 1914, (Erişim) http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/, 19 Ekim 2009.

[270] Inquiry into Provisions of The Cybercrime Bill 2001 – August 2001, (Erişim) http://www.aph.gov.au/senate/Committee/legcon_ctte/completed_inquiries/1999-02/cybercrimebill01/report/report.pdf, 24 Ekim 2009. s. 34.

kanunlardaki hükümlere karşı bir ihlal şüphesi varsa delil elde edilmesi amacıyla arama ve elkoyma tedbirlerine başvurulacaktır[271].

Suçlar Kanunu'nun tanımlar başlığı altında düzenlenen 3C maddesinde verinin ne olduğuna ilişkin bir tanımlama yapılmıştır. Buna göre veri, herhangi bir biçimdeki bilgiyi ve bir programı veya bir program parçasını ifade etmektedir. Sadece verinin tanımı yapılmamış olup "bilgisayarda saklanan veri" (data held in a computer) ve "veri saklama birimleri" terimlerinin (data storage device) tanımlarına da yer verilmiştir[272].

Suçlar Kanunu'nun 3E maddesinde bir suç şüphesi altında, makul sebepler (reasonable grounds) çerçevesinde aramaya konu olabilecek yerdeki bir delilin var olduğuna yönelik bir kanaate ulaşılmışsa bina ve eklentilerinde delil elde edebilmek için arama kararını düzenlemeye yetkili kişiler (issuing officer) arama kararı verebilmektedirler. 3C maddesinde "arama kararını düzenlemeye yetkili kişiler" deyiminden (issuing officer) bir hâkim (magistrate) veya sulh hâkimi (justice of peace) veyahut da Avustralya'nın başkent eyaleti (Capital Territory) ve diğer eyaletlerinin adli mercilerinde görev yapan tutuklama için arama, bina ve eklentileri için arama ve diğer soruşturmalar için arama kararlarını vermeye yetkili kişiler anlaşılır[273]. Arama kararı, talep edilirken soruşturulmakta olan suç, olay yeri adresi, delil ile bulunması beklenen delillerin çeşitleri ve idda edilen suçla

---

[271] Gergor Urbas, Kim-Kwang Raymond Choo, "Resource Materials Technology - Enabled Crime", **Australian Institute of Criminology,** Technical and Backround Paper, No: 28, (Erişim) http://aic.gov.au/documents/E/7/8/%7BE78191C1-5833-4658-BD07-DEA35DAC184A%7Dtbp028.pdf, 21 Ekim 2009, s. 55.

[272] " data" includes: (a) *information* in any form; or(b) any program (or part of a program)
data held in a computer" includes:
"(a) data held in any removable data storage device for the time being held in a computer; or (b) data held in a data storage device on a computer network of which the computer forms a part. "data storage device" means a thing containing, or designed to contain, data for use by a computer"
Bilgisayarda saklanan veri (data held in a computer) çıkarılabilen herhangi bir veri saklama biriminde olabilenn verinin geçici olarak bilgisayarda bulunması veya bilgisayarın bir parçası olarak bilgisayar ağında bulunan veri saklama birimindeki birimler olarak özetlenebilir. Veri saklama birimleri (data storage device) ise saklayan veya bilgisayarların kullanması için veri saklamak üzere tasarlanan bir alet anlamına gelmektedir. (Erişim) http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/s3c.html, 19 Ekim 2009.

[273] (Erişim) http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/s3c.html, 19 Ekim 2009.;

arasındaki ilişkileri talepnamede bulunacaktır[274]. Nitekim Suçlar Kanunu'nun 3E maddesinin 5. fıkrasında arama kararında bulunması gereken durumlar gösterilmiştir. Buna göre iddia edilen suç; arama yapılacak bina ve eklentilerinin özellikleri; bu bina ve eklentileriyle ilgili olan kişilerin isimleri ve bu kişilerin bilinen özellikleri; kararda bahsi geçen elde edilebilecek delile ilişkin materyaller (Evidential Material)[275], aramayı yapacak polis memurlarının isimleri ve aramanın biteceği süre ve aramanın hangi saatlerde yapılacağı arama kararında belirtilir. Arama kararı verilirken delile ilişkin materyallerin bir suçla ilgili olduğu konusunda hâkimlerde makul sebeplere dayanan bir kanaatin oluşması gerekir. Ayrıca tanımlar kısmında da belirtildiği üzere elektronik yapıdaki bilgiler delile ilişkin materyaller arasındadır. Bu bakımdan bilgisayar içerikleri ve veri saklama birimleri arama kararı kapsamında aranabilecektir[276].

3K maddesinde delile ilişkin materyalleri incelemek amacıyla aranılan yere alet ve techizatın getirilmesinden bahsedilmiştir. Ancak bu yöntemin işletilmesi için makul sebeplerin var olup olmadığı adli birimlerce değerlendirilecektir. Bu maddenin 2. fıkrasına göre delil inceleme açısından bir zorluk varsa bulunan nesne veya delile ilişkin materyal başka bir yere nakledilebilir. Yapılacak inceleme 72 saat süre ile sınırlıdır. Süre sınırının aşılması hali mevcutsa polis veya ilgili memurlar (executing officer) makul sebeplere dayalı olarak arama kararını vermeye yetkili kişilerden ek süre talebinde bulunabilirler.

Elektronik aletlerin kullanımları hakkında ayrıntılı düzenlemeler kanunun 3K maddesine yansımıştır. 3L maddesi ile 3K maddesi beraber düşünüldüğünde 3L maddesinin 3K maddesine göre özel hüküm olduğu sonucuna ulaşılmaktadır. Madde, polisleri ve adli birimleri bilgisayardaki ve veri saklama birimlerindeki verilere erişme ve bunları veri saklama birimlerine

---

[274] Urbas, Choo, s. 56.

[275] *"evidential material" means a thing relevant to an indictable offence or a thing relevant to a summary offence, including such a thing in electronic form.";*
Delile ilişkin materyal res'en takibi suçlar veya basit suçlarla ilgili olarak elektronik biçimdeki bilgileri ifade etmektedir. (Erişim) http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/s3c.html, 19 Ekim 2009.

[276] Urbas, Choo, s. 53.

kopyalamada yetkili kılmaktadır[277]. Verileri kopyalamak için gerekli elektronik aletler ve veri saklama birimleri olay yerine getirilebilir. Getirilen bu alet ve birimlerle adli bilişim işlemleri veya diğer teknik incelemeler yapılacaktır.

Söz konusu 3C maddesinin 1A fıkrasının b bendinin gereği olarak verilerin kopyası bir diskete veya bir veri saklama birimine kaydedebilecek veya verilerin bulunduğu birime elkonulacaktır. Bu hüküm tedbirlere maruz kalan kişinin yazılı kabulüyle de uygulanabilmektedir. Yani yazılı bir rıza söz konusudur. 1B fıkrasında ise Avustralya Federal Polis Teşkilatı'nın (Australian Federal Police – AFP) elkoymadaki rolünden bahsedilmiştir. Söz konusu maddenin 2. fıkrası delile ilişkin materyallerin elkonulmasını ve bunların mümkünse belge biçimine dönüştürülmesini ele almaktadır. Belgeye dönüştürülme işleminin sadece delile ilişkin materyal olduğu inanılan kopya birimler üzerinde yapılacağı konusunda yargı, polis ve uzman çevreleri hemfikirdirler[278]. 3. fıkra ise kopyalamanın ve belgeye dönüştürülmesinin pratik olmaması durumunda elkoymaya gidileceğini hüküm altına almıştır. 3N maddesinde bahsedildiği üzere polis tarafından karara uygun bir biçimde elkoyma tedbiri uygulanmışsa belgelerin, görüntülerin, bilgisayar veriler bir kopyası sahibine veya olay yerinde hali hazırda onu temsil eden herhangi bir kimsenin talep etmesi halinde mümkün olduğunca kısa sürede verilecektir. Bu ilk fıkranın 3L1/A, 3L/2/ b ve 3LAA/4/ b bendlerinde uygulama alanı yoktur. Bu hükümler ise AFP'nin daha etkin olduğu alanları vurgulamaktadır ki burada federal meseleleri ilgilendiren durumların varlığı söz konusudur[279]. Dolayısıyla 3N maddesi yerel polis ve yerel adli birimler için uygulanabilecektir. AFP'nin görev kapsamına giren durumlarda şüpheliye veya onu olay yerinde temsil eden kimseye karşı arama veya elkoymaya konu olan birimlerden kopya verilmesi işlemleri icra edilmeyecektir[280].

Maddenin 4. fıkrası ise polisin veya adli görevlilerin delile ilişkin materyallere elektronik aletlerin yardımıyla ulaşmasını ve incelemeyi yapacak

---

[277] Teisserie **a.g.m.**, s. 6.
[278] Bronitt, Gani, **a.g.m.**, s. 314.
[279] Ayrıntılı bilgi için bkz. (Erişim) http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/s3n.html, 19 Ekim 2009.
[280] (Erişim) http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/s3n.html, 19 Ekim 2009.

uzmanın yardıma çağırılmasını öngörmüştür. Bununla birlikte herhangi bir şekilde bir önlem alınmamışsa verinin kaybolma ve yok edilme riski karşısında elektonik aletlerin derhal koruma altına alınacağı maddenin devamında belirtilmiştir. Bu koruma altına alma işlemlerine olay yeri inceleme için getirilen elektronik aletler de dâhildir. 3L maddesinde belirtildiği üzere inceleme süresi 24 saatten fazla olamaz. 24 saatten önce inceleme bitirilmişse bu tedbirin muhatabı olan kişiye koruma altına alma ile ilgili düşüncelerini ve uygulanan tedbirle ilgili belirten bir belge verilecektir. Şayet bu 24 saatte delilin elde edilemeyeceğine ilişkin makul sebeplerin olduğuna polis ve adli birimler kanaat getirmişlerse arama süresinin uzatılması için arama kararını düzenlemeye yetkili kişilere başvuru yapmak zorundadırlar. Aksi halde bu tedbirler hukuka aykırı olacaktır.

3LA maddesi elektronik delil elde etmede uzman veya diğer kişilerden yardım almayı öngörmüştür. Mahkeme bu hükme dayanarak kişilerin (arama yapılacak yerin sahibi veya kiracısı veya çalışanları sistem yöneticileri, aranılacak birimleri daha önce kullanmış kişiler) yardımcı olması için makuliyet ve gereklilik çerçevesinde görev yükleyebilmektedir. Bu kişi kararda bulunan bilgisayardaki verilere erişmede veya erişilebilir kılmada; bunları bir veri saklama birimine kopyalamada veya bu verilerin belge biçimine dönüştürülmesinde yardımcı olacaktır. Son olarak 3LB maddesi verilerin aranılan yer dışında, farklı bir yerde bulunması koşullarına; 3M maddesi ise zarara uğrayan elektronik aletlerin tazmini konularına yer vermiştir.

Bilgisayarlara yönelik arama ve elkoyma şartlarının geniş kapsamı ve başvurabilirlik hali hukuk ve bilgisayar uzmanları arasında ihtilaflara neden olmuştur[281]. Hakim olan bir görüşe göre söz konusu tedbirler, ayrıntılı bir biçimde düzenlendiyse de teknolojinin ilerlemesi karşısında geri kalmıştır[282]. Özellikle şifrelenmiş verilerin aranması konusunda herhangi bir yetki Suçlar

[281] Urbas, Choo, **a.gm.**, s. 54.
[282] Bronitt, Gani, **a.g.m.**, s. 314.

Kanunu'na yansımamıştır[283]. Bu konuda AK-SSS'deki hükümlerin takip edilmesi gerektiği ifade edilmektedir[284].

B- İSRAİL

İsrail Anayasası'nın İnsan Onuru ve Özgürlük (Human Dignity and Liberty) başlığı altındaki 7. maddesi özel yaşamın gizliliğini korumaktadır.[285] Buna göre hiç kimsensin üstü, eşyası, onuru, özgürlüğü, ülkeden ayrılma ve ülkeye giriş hakkı ihlal edilmeyecektir. İhlalin ancak hukuki bir durum çerçevesinde ve İsrail devletinin değerlerine uygun bir şekilde yapılması gerektiği ifade edilmektedir[286]. Anayasa'daki bu hükümlerin yanında Özel Hayatın Gizliliğini Koruma Kanunu 1981 (5741-1981) yılında yürürlülüğe girmiştir. Bu kanun özel hayatın gizliliğinin ihlalini suç saymakta ve buna ilişkin cezai hükümler öngörmektedir. Elektronik veri toplanmasıyla ilgili hususlar bu kanunda düzenlememiştir. Hatta kanunun sadece 2. maddesi kişisel veri bankalarının korumasından bahsetmiştir[287].

"Bilgisayar", "bilgisayar materyali" (computer material), "çıktı" (output) gibi terimler Ceza Muhakemesi Düzenlemelerine (Criminal Procedure Ordinance) Bilgisayar Kanunu (The Computers Law of 1995) ile girmiştir[288]. Bu tanımlar bilgisayarlara yönelik arama ve elkoyma tedbirlerinin konusunu oluşturmaktadır.

2002 yılının haziran ayında Kudüs yerel mahkemesinin bir kararına göre bilgisayara erişim ve bilgisayar çıktılarının edinimi arama tedbirinin

---

[283] Bronitt, Gani, **a.g.m.**, s. 314.
[284] Inquiry into Provisions of The Cybercrime Bill 2001 – August 2001, (Erişim) http://www.aph.gov.au/senate/Committee/legcon_ctte/completed_inquiries/1999-02/cybercrimebill01/report/report.pdf, 24 Ekim 2009. s. 9.
[285] Basic Law: Human Dignity and Liberty, (Erişim) http://www.mfa.gov.il/MFA/MFAArchive/1990_1999/1992/3/Basic%20Law-%20Human%20Dignity%20and%20Liberty-, 19 Ekim 2009.
[286] Martin C. Golumbic, "The Legal Framework in Israel", **Fighting Terror Online**, Newyork, 2008, Springer, (Erişim) http://www.springerlink.com/content/u61n05j928p62476/fulltext.pdf, 24 Kasım 2008, s. 107.
[287] Golumbic, **a.g.m.**, s. 108.
[288] Criminal Procedure Ordinance (Arrest and Searches) 5729-1969., (Erişim) https://www.imolin.org/doc/amlid/Israel/Israel_Criminal_Procedure_Ordinance.pdf; 09.04.2010.

işletilmesiyle mümkün olabilecektir[289]. Bu karardan sonra iş ve kamu yönetimindeki uyuşmazlıkları önlemek için bir kuruma ait bilgisayar bulgularına elkonulması ve bu tedbirin mahkeme kararına bağlanması Ceza Muhakemesi Düzenlemeleri'nin 32. maddesine getirilen bir ek paragraf (32 (b)) ile mümkün olmuştur. Bundan ayrı olarak bir suç şüphesi altında bilgisayar verilerine giriş ve arama söz konusu düzenlemelerin 23., ve 23a maddelerine göre hakim tarafından verilen bir arama kararına dayanacaktır[290]. Bu özel tedbirlerin uygulamasında bilgisayar konusunda bilgi sahibi uzmanlardan yardım istenebilecektir. Bilgisayarlara yönelik yapılan arama tedbirinde iki şahidin olay yerinde durması gerekmektedir[291]. Bu iki şahidin olay yerinde durmasının asıl sebebi polisin veya adli memurların bilgisayara sonradan delil yerleştirmesinin önlenmesi ve kamu güvenirliliğinin tesis edilmesidir[292]. Bilgisayarda veya veri saklama birimlerindeki veriler elde edildikten sonra şüphelinin talebi üzerine uzmanın huzurunda kopyası çıkarılmalıdır. Sahibinin önceden rızası varsa orjinal birim, sonradan gösterilebilir ve talep halinde kişiye geri bırakılabilir[293].

Bilgisayarlara yönelik arama ve elkoyma tedbirleri bu düzenlemelerle sınırlı değildir. Mevzuat bakımından konusuna göre ayrı ayrı alanlarda düzenleme getirilmiştir. Terörü Önleme Düzenlenmesi'nin (Prevention of Terror Ordinance) 5. maddesindeki koşullara göre internet sitesi kapatılabilir ve bu terör örgütünün amaçlarına hizmet eden site içerisindeki materyallere elkonulabilir[294]. Burada internet verilerinin elkonulmaya konu olmasından ve müsadere durumundan bahsedilmiştir. Acil Savunma Düzenlemeleri'ne (Emergency Defense Regulations) göre bir suç teşkil eden yazılar veya bir suça delil olabilecek yazılar 99. madde gereği elkonulabilir. 100. ve 101. maddeleri ise basın ve yayında kullanılan bilgisayar sabit diskinin

---

[289] Ruth Levush, "Law Library of Congress Israel: Computer Security and Protection of Computer Information", (Erişim) http://www.mafhoum.com/press4/236.pdf, 28 Kasım 2009, s. 16.
[290] Golumbic, **a.g.m**, s. 109.; "*(Search Warrants Penetration of Computer Material, and Order to Obtain Article, respectively)"*.
[291] Golumbic, **a.g.m**, s. 109.
[292] Levush, **a.g.m.**, s. 16.
[293] Levush, **a.g.m.**, s. 16.
[294] Golumbic, **a.g.m.**, s. 110.

aranabilmesine izin vermiştir. İlgili düzenleme bina ve eklentilerin aranabileceğini ve delil teşkil edecek nesnelerin elkonulabileceğini göstermiştir ki bilgisayar bulguları buna dâhildir[295].

Bilgisayardan elde edilen delillerin kabul edilebilirliği konusunda Bilgisayar Kanunu'nun getridiği bir takım değişiklikler Delil Düzenlemelerine (Evidence Ordinance 5731-1971) yansımıştır. Bu değişiklikler sonrası kurumsal belgeler diğer bir deyişle bilgisayar çıktıları delil olarak kabul edilecektir[296]. Bilgisayar çıktılarının delil olarak kabul edilebilmesi için bir takım şartlar aranacaktır. Delil Düzenlemelerindeki söz konusu şartlar delilin doğruluğunu kanıtlamaya yöneliktir. Öncelikle normal olarak hemen hemen vuku bulan zamanda belgedeki olay konusunun kayıt altına alınması sağlamalı; ikinci olarak veri toplama yöntemleri ve belgenin hazırlanması belge içeriğinin doğruluğunu ispat etmelidir[297]. Son olarak bir davada, belge bir bilgisayar çıktısı ise çıktının oluşturulma yöntemi, oluşturulan belgenin doğru bir şekilde hazırlandığı ve tedbiri uygulayan adli birimin düzenli olarak bilgisayar çalışmalarına karşı sabotajı önleyecek makul korumacı ölçüler kullandığı kanıtlanmalıdır[298]. Bilgisayar çıktısı bir bilimsel konuda, araştıma sanat, mesleki bilgi veya sağlık alanında bir görüşü ifade ediyorsa uzman görüşlerine uygunluk içerisinde sunulmadıkça delil olarak kabul edilmeyecektir[299]. Burada bilgisayardan elde edilen delillerin konu bakımından ayrılması söz konusudur. Kural olarak hukuka aykırı bir şekilde elde edilen elektronik deliller diğer klasik tipteki deliller gibi muhakemede kullanılamazlar. Bazı davalarda ise mahkeme aramanın sonradan hukuka aykırı olduğunu belirlemesine rağmen bilgisayara elkonulmasını hukuka uygun olduğu yönünde bir karar vermiştir[300]. Ayrıca bu karar şüpheli olmayan

---

[295] Golumbic, **a.g.m.**, s. 110.
[296] Levush, **a.g.m.**, s. 14.
[297] Levush, **a.g.m.**, s. 15.
[298] Levush, **a.g.m.**, s. 15.
[299] Levsuh, **a.g.m.**, s. 16.
[300] Davada servis sağlayıcısının şüpheli kişilerin e-posta haberleşmesinin kayıtları tutulmaktadır. Üçüncü kişilerin bilgisayar kayıtlarına yönelik arama ve elkoyma uygulanmaktadır. Mahkemede e-posta haberleşmesinin iletişimin denetlenmnesine tabi tutulacağı ve buna ilişkin arama kararı alınması gerektiği ileri sürülmüştür. Ancak burada Ceza Muhakemesi Düzenlemelerinin 23. ve 43. maddelerine göre arama kararı yapılmıştır. Yerel mahkeme

diğer kişilerin bilgisayarlarında arama ve elkoyma yapılmasının mümkün olduğunu belirtmektedir.

hukuka aykırı olan arama neticesinde el konulan bir yazı hala delil olarak kabul edilmektedir. Mahkeme Nahmias davasında Yüksek Mahkemenin verdiği karara dayanarak bu sonuca ulaşmıştır. Netvision Ltd vs. Israel Defence Forces (MC 090868/00) (Golumbic, **a.g.m.**, s. 110).

ÜÇÜNCÜ BÖLÜM

CEZA MUHAKEMESİ KANUNUNA GÖRE BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA, KOPYALAMA VE ELKOYMA (CMK md. 134)

I- BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA, KOPYALAMA VE ELKOYMANIN HUKUKİ NİTELİĞİ

A- GENEL OLARAK

Bilgisayarlar getirdikleri kolaylıklara karşılık bir suçun işlenmesinde kullanılabilirler. Bilgisayar korsanı olarak adlandırılan "hacker"lar bilgisayarları kullanarak bilişim sistemlerini bozabilir, mali zararlara neden olabilir, şirketlerin kasalarını boşaltabilir, özel yaşamın gizliliğini ihlal edebilir ve devletin ulusal güvenliğini dahi etkisiz hale getirebilirler.

Bilgisayarlar suç işlenmesinde kullanılmasalar da bir suçun ispatına yarayan bir araç olabilir. Örneğin; bir seri katil günlüğünü bilgisayarda tutabilir. Uyuşturucu kaçakçılığı ile ilgili bilgiler bu suçu işleyen kişilerin bilgisayarlarında bulunabilir. FSEK kapsamına giren fikri hak ihlalleri veya Bankacılık Kanunu'ndaki suç tiplerine ilişkin deliller bilgisayarların sabit disklerinde veya veri saklama birimlerinde olabilir. Bu nedenle ceza muhakemesinin amaçlarından biri olan maddi gerçeğe ulaşma bakımından bilgisayarlar üzerinde de delil araştırması yapılabilmelidir. Nitekim CMK'nın 134. maddesinin gerekçesinde "*Ancak bilgisayarlardaki kayıtların gerçeğin*

açığa çıkarılması yönünden, ceza davasında delil, … oluşturacağı ortadır." ifadesi yer almaktadır[301].

Günümüzde, ticaretin ve haberleşmenin çok hızlı bir şekilde yapıldığı göz önüne alındığında, bilgisayarlar olmadan bankaların, şirketlerin ve ticari işletmelerin işlerini yürütebilmeleri mümkün görünmemektedir. Ancak bilgisayarlar sadece iş yaşamımızda değil; günlük özel yaşamımızda da büyük rol oynamaktadır. İnsanlar birbirleriyle bilgisayarlar sayesinde iletişim kurabilmekte, birbirlerine fotoğraflar gönderebilmekte ve hatıralarını paylaşabilmektedirler. Bu nedenle bilgisayarlar ticari ve mesleki sırlarımızın yanı sıra kişisel verilerimizin de saklandığı bir cihaz olmuştur.

Bilgisayarlar üzerindeki herhangi bir geçici müdahale iş yaşamını sekteye uğratabilmekte, ticari ve mesleki sırların gizliliğini sona erdirmekte ve haberleşmeyi engelleyebilmektedir. Örneğin; elkoyma uygulanmaksızın bilgisayarlarda arama yapmak bile bilgisayarları birkaç saat iş yapamaz hale getirmekte ve mali kayıplara yol açmaktadır. Şirketin bilgisayarları üzerinde elkoyma tedbiri icra ediliyorsa, şirketin ticari güveni sarsılabilmektedir. Bunun sonucunda şirket iflas etme riskiyle karşı karşıya kalabilmektedir.

Bilgisayarlarında arama ve elkoymanın uygulanması sonucunda kişilerin mahremiyetleri ihlal edilmekte ve sakladıkları bütün sırlar açık hale gelmektedir. Bu sırların başkaları tarafından öğrenilmesi kişilere manevi bir ızdırap verebilmektedir. Bilgisayarlara elkonulmasıyla kişilerin kendi bilgilerine erişmeleri engellenmektedir. Ayrıca bilgisayarlara elkoyma durumunda kişilere ait olan bütün bilgilerin veya çalışmaların silinmesi riski de ortaya çıkmaktadır. Özellikle kişilere ait çalışmaların istenmeden yok edilmesi durumunda telafisi mümkün olmayan zararlar meydana gelmektedir. Öte yandan, avukatlara ait bilgisayarların söz konusu tedbirlere maruz kalması, avukat ve müvekkil ilişkisinin gizliliğini zedeleyebilmekte ve dolayısıyla savunma hakkı ihlal edilmiş olmaktadır.

Özetle genel arama ve elkoyma tedbirlerinin bilgisayar üzerinde uygulanmasıyla anayasada belirtilen özel hayatın gizliliği, haberleşme

---

[301] Cumhur Şahin, **Ceza Muhakemesi Kanunu: Gazi Şerhi,** Ankara, Seçkin Yayınevi, 2005, s. 372.

hürriyeti, düşünceyi açıklama ve yayma hürriyeti, bilim ve sanat hürriyeti, çalışma ve sözleşme hürriyeti, mülkiyet hakkı, hak arama hürriyeti gibi temel hak ve hürriyetler ihlale uğramaktadır. Koruma tedbirleri özellikleri gereği geçicidir. Tedbirlerin geçici olarak bilgisayarlara uygulanması bile müdahalede bulunduğu temel hak ve özgürlükler bakımından ağır sonuçlara yol açmaktadır.

Bilgisayarlar üzerinde genel arama ve elkoymanın uygulanması durumunda yukarıda belirtilen sakıncalar doğmaktadır. Bu sakıncaların vukubulmaması için ölçülü bir şekilde tedbirlere başvurmak gerekmektedir. Koruma tedbirlerinin genel özelliklerinden bir olan ölçülülük ilkesi araçla amacın, uygulanan yöntemle gayenin dengeli olmasını ifade eder[302]. Tedbire başvurularak müdahale edilen temel hak ve özgürlükler ile ulaşılmak istenen maddi gerçek arasındaki dengeye dikkat edilmelidir. Bu nedenlerle bilgisayarlara yönelik genel arama ve elkoymadan ayrı bir koruma tedbirinin düzenlenmesi; müdahalede bulunulan temel hak ve özgürlüklerin korunması ve koruma tedbirlerindeki ölçülülük ilkesi bakımlarından son derece önemlidir.

Bilgisayarlara yönelik bu koruma tedbirleri CMUK'da bulunmamaktaydı. Yanlızca Ceza Muhakemesi Kanununun Yürürlük ve Uygulama Şeklinde Kanun'un 18. maddesiyle ilga edilen 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu'nun 4. maddesinde kayıt ve verilerin incelenmesi başlığı altında bilgisayar verilerinin incelemeye tabi olacağına dair bir hüküm mevcuttu[303] [304]. CMUK'ta böyle bir düzenleme olmadığından bilgisayarlar üzerinde genel arama ve elkoyma (CMK md. 116, 117 ve 127) hükümleri uygulanmaktaydı. Elektronik ortamda yani bilgisayarı

---

[302] Cumhur Şahin, **Ceza Muhakemesi Hukuku I**, Ankara, Seçkin Yayınevi, 2007, s. 202.

[303] Yazar, ÇASÖMK'nun 4. maddesinin CMK'nın 134. maddesine nazaran daha geniş bir içeriğe sahip olduğunu ve CMK'nın 134. maddesinin bunu karşılamadığını ileri sürmektedir. Bkz. Veli Özer Özbek, **CMK İzmir Şerhi**: **Yeni Ceza Muhakemesi Kanunun Anlamı**, Ankara, Seçkin Yayınevi, 2005, s. 499.

[304] Kayıt ve Verilerin İncelenmesi başlıklı (MÜLGA) 4422 sayılı Çıkar Amaçlı Suç Örgütleriyle Mücadele Kanunu'nun 4. maddesi aynen,
"Bu Kanunda öngörülen suçların veya delillerinin ortaya çıkarılması için, suçların işleniş biçimlerine benzer tutum ve davranışlarda bulunan kişilere ilişkin yer, kuruluş, çevre ve kurumdaki, Devletin ulusal güvenliği bakımından gizli kalması zorunlu olanlar hariç her türlü resmi ve özel kayıtlarla bilgisayar verileri incelenebilir." şeklindedir.

oluşturan donanım ve yazılım alanlarında bu tedbirin uygulanması genel arama ve elkoymaya benzerlik gösterse de kendi içerisinde farklılıkların olması doğaldır. Bu farklılıkların nedeni olarak elektronik ortamın veya elektronik delillerin kendilerine özgü nitelikleri gösterilebilir. Verinin bilgisayarın soyut tarafında yer alması düşünüldüğünde genel arama ve elkoyma tedbirleriyle verilerden anlaşılabilir bir şekilde delil elde edilmesi her durumda mümkün olamamaktadır. Hem tedbirlerin elektronik ortamda uygulanması hem de müdahalede bulunulan temel hak ve özgürlüklerin etkin bir şekilde korunması amacıyla bilgisayarlara yönelik özel koruma tedbirlerine ihtiyaç duyulmuştur.

5271 sayılı CMK'nın 134. maddesinde ise bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirleri özel bir biçimde yer almıştır. Söz konusu bu madde esasen genel arama ve elkoymanın elektronik ortamda gerçekleştirilmesini düzenlemektedir. Bu tedbirler yalnızca CMK'nın 134. maddesinde düzenlenmiş değildir. Hükmün uygulanmasına ilişkin ayrıntılara yönetmelikte yer verilmiştir. Adli ve Önleme Aramaları Yönetmeliği'nin 17. maddesi (Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma) CMK'nın 134. maddesi temelinde düzenlenmiştir[305].

---

[305] AÖAY'in Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma başlığını taşıyan 17. maddesi aynen,
"1-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.
2- 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.
3-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.
4- İstemesi hâlinde, bu yedekten elektronik ortamda 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 verilerin mahiyeti hakkında tutanak tanzim edilir ve ilgililer tarafından imza altına alınır. Bu tutanağın bir sureti de ilgiliye verilir." şeklindedir.

B- BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA VE ELKOYMANIN GENEL ARAMA VE ELKOYMA HÜKÜMLERİYLE İLİŞKİSİ

Ceza muhakemesinin süreci zorunlu olarak bir takım tedbirlerin uygulanmasını gerektirmektedir. Zira koruma tedbirlerine başvurmadan bazen muhakemenin yapılabilmesi mümkün olmamakta, verilecek kararlar kağıt üzerinde kalmakta, deliller elde edilememektedir. Koruma tedbirleri hükmün verilmesinden önce ve muhakeme sürecinde gündeme gelecektir. Yapısında zorlayıcılık vardır. Tedbirlerin uygulanmasıyla bir takım temel hak ve özgürlüklere geçici surette müdahalede bulunulacaktır. Bireyin bu geçici müdahalelere yönelik bir katlanma yükümlülüğü vardır.

Arama tedbiri ile konut dokunulmazlığı, vücut bütünlüğü, özel hayatın gizliliği ve kişi özgürlüğü gibi anayasal haklara müdahale edilmektedir. Bu temel hak ve özgürlükler anayasanın 20. ve 21. maddelerinde güvence altına alınmıştır. Arama, adli ve önleme araması olarak ikiye ayrılır. AÖAY'nin 5. maddesinde tanımlandığı üzere; adli arama suç şüphesi altında 5271 sayılı CMK ve diğer kanunlara göre işletilen bir tedbirdir[306]. Başka bir deyişle arama bir ceza muhakemesi işlemidir (CMK md. 116). Önleme araması ise her ne kadar adli ve önleme aramaları yönetmeliğinde yer almışsa da kamu düzenini ve kamu güvenliğini korumak amacıyla kolluk tarafından uygulanan bir idari işlemdir (AÖAY md. 19)[307]. Amaç suç işlenmesini önlemek olsa da önleme aramasında idare hukuku boyutu yoğundur.

Arama işleminin amacı şüpheli veya sanığın yakalanması ve suç delillerinin elde edilmesidir (CMK md. 116). Şüpheli veya sanığın yakalanması ve suç delillerin elde edilebilmesi kanunda düzenenlenen bir

---

[306] Adli Arama ve Önleme Arama Yönetmeliğinin 5. Maddesi aynen,
"*Adlî arama, bir suç işlemek veya buna iştirak veyahut yataklık etmek makul şüphesi altında bulunan kimsenin, saklananın, şüphelinin, sanığın veya hükümlünün yakalanması ve suçun iz, eser, emare veya delillerinin elde edilmesi için bir kimsenin özel hayatının ve aile hayatının gizliliğinin sınırlandırılarak konutunda, işyerinde, kendisine ait diğer yerlerde, üzerinde, özel kâğıtlarında, eşyasında, aracında 5271 sayılı Ceza Muhakemesi Kanunu ile diğer kanunlara göre yapılan araştırma işlemidir*." şeklindedir.

[307] İsmail Malkoç, Mert Yüksektepe, **Açıklamalar ve Yorumlarıyla 5271 Sayılı Yeni Ceza Muhakemesi Kanunu**, 1. Cilt, Ankara, Malkoç Kitabevi, 2008, s. 306.

takım şartların varlığına bağlıdır. İlgili şartlar, temel kaynağını anayasanın incelenen bu iki maddesinden almaktadır.

Anayasa'nın 20. ve 21. maddelerinde arama tedbirine ek olarak elkoyma tedbirine yer verilmiştir. Elkoyma (CMK md. 123) ile delil niteliğini haiz; müsadere altına alınabilecek bir malvarlığı değeri üzerinde zilyedin tasarruf yetkisi kaldırılmaktadır[308]. İlgilinin rızasının varlığına veya yokluğuna bakılmaksızın devlet zora başvurarak mala elkoymaktadır. Şayet rıza ile mal teslim edilmişse burada elkoyma değil; muhafaza altına almadan bahsedilir. Elkoyma genellikle arama tedbirini takiben uygulanan bir koruma tedbiridir. Bu husus koruma tedbirlerinin birbirlerinin aracı olduğunu (araç oluş) göstermektedir. Arama kararı olmadan elkoyma kararı verilebilir. Buna karşılık salt arama kararına dayanılarak elkoyma tedbirine başvurulamaz. Arama kararı ile elkoyma kararı birlikte verilmelidir. Lâkin arama kararına ihtiyaç olmadan da örneğin açıkta bulunan bir eşyaya doğrudan elkoyma tedbiri uygulanacaksa bir karara veya yazılı emre gerek duyulur[309].

Arama ve elkoyma tedbirlerinin yanında CMK, belge veya kâğıtları inceleme yetkisi, postada elkoyma, avukat bürolarında arama, elkoyma ve postada elkoyma gibi arama ve elkoymaya benzer özel koruma tedbirleri öngörmüştür. Özel koruma tedbirlerinin düzenlenmesinde amaçlanan hedef, maddi gerçeğe ulaşılırken müdahale edilen hak ve özgürlüklerin makul ölçüde korunmasıdır. Örneğin; postada elkoymayı düzenleyen CMK'nın 129. maddesinin gerekçesinde: "*Madde postada elkoyma konusunu, haberleşme özgürlüğünün demokratik hayat biçimindeki çok üstün değeri dolayısıyla ayrıca düzenlenmiş bulunmaktadır.*"[310] ifadesi ile bu duruma işaret edilmiştir. Keza aynı durum avukat bürolarında arama, elkoyma ve postada elkoymayı düzenleyen CMK'nın 130. maddesinde vurgulanmıştır[311].

---

[308] Şahin, **a.g.e.**,, s. 248.
[309] Şahin, **Ceza Muhakemesi Kanunu: Gazi Şerhi,** s. 339.
[310] Şahin, **a.g.e.**, s. 359.
[311] "*Madde, avukat bürolarında arama, elkoyma ve avukatlarla ilişkili postada yapılacak belge ve varakalara elkoyma ile ilgili ve suç nedeniyle yapılacak işlemleri ayrı ve genel hükümlere göre farklı usullere ve özel hükümlere bağlamış bulunmaktadır. Böylece ayrı ve istisnai usuller getirilmesinin temel nedeni, savunma hakkını sağlam tutmaktır.*" (Şahin, **a.g.e.**, s. 361).

Söz konusu 134. maddenin gerekçesinde: "*Madde, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve geçici elkoyma konularını düzenlemektedir. Bireye ait kişisel bilgiler üzerindeki hak, temel insan haklarından olduğundan hakkın kısıtlanabilmesi için yasal düzenleme gerekeceği açıktır.* "[312] ifadesi, tedbirin düzenlenmesindeki temel amacı ortaya koymaktadır. Buna ek olarak bireyin kişisel veriler üzerindeki hakkı, 5982 sayılı kanunla yapılan 03.10.2010 tarihinde yürürlüğe giren anayasa değişikliği ile özel hayatın gizliliğini düzenleyen 20. maddeye getirilen ek bir fıkra ile düzenlenmiştir[313].

Temel hak ve özgürlüklerin sınırlandırılması yalnızca kanunla mümkün olduğundan, bilgisayarlara yönelik özel bir koruma tedbirinin CMK'da yer alması, anayasaya uygundur (Anayasa md. 13).

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma, genel normlar olan arama ve elkoyma tedbirlerinin yanında aynen postada elkoyma veya avukat bürolarında arama ve elkoyma gibi özel bir normdur. Zira bu tedbirleri düzenleyen CMK'nın 134. maddesi koruma tedbirlerinin düzenlendiği birinci kitap dördüncü kısmının arama ve elkoyma başlıklı dördüncü bölümünde yer almaktadır. Madde özel koruma tedbirlerini düzenlediğine göre koruma tedbirlerindeki kanunilik, geçicilik, araç oluş, gecikmede tehlikelilik, görünüşte haklılık, ölçülülük, bir karara dayanma ve zorlama ilkeleri burada uygulama alanı bulacaktır.

Genel norm-özel norm ilişkisi gereği özel norm niteliğindeki bu koruma tedbirinde yer almayan hususlar gündeme geldiğinde genel hükümlere başvurulacaktır. Örneğin; bilgisayarlarda yapılan arama sonucunda arama sonunda verilecek belge CMK'nın 121. maddesine göre düzenlenecektir.

---

[312] Şahin; **a.g.e.**, s. 371.

[313] Anayasa'nın 20. maddesinin 3. fıkrası aynen,
"*Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.*" şeklindedir.

Aynı şekilde CMK'nın 121. maddesi 3. fıkrası gereği koruma altına alınan veya elkonulan eşyanın tam bir defteri yapılacaktır. Böylelikle bilgisayarlara ve veri saklama birimlerine elkoyma uygulandığı takdirde elkonulan bilgisayarların ve veri saklama birimlerinin tam bir defteri yapılmalıdır.

C- BENZER KORUMA TEDBİRLERİ İLE ARASINDAKİ FARKLAR

CMK'nın getirdiği yeni düzenlemeler sadece bilgisayarlara yönelik tedbirle sınırlı değildir. "Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi" başlığı altında iletişimin tespiti, dinlenmesi ve kayda alınması tedbirleri CMK'nın 135. maddesinde yer almıştır. Bilgisayarlara yönelik bu özel koruma tedbirleri ile iletişimin tespiti, dinlenmesi ve kayda alınması (CMK md. 135) tedbirleri karşılaştırıldığında her ne kadar teknolojik olarak benzerlikler olsa da, bu iki tedbir arasında farklılıkların bulunduğu görülmektedir. CMK'nın 134. maddesinin gerekçesinde de belirtildiği üzere bu tedbirler durağan pozisyondaki bilgisayarlara uygulanırken; iletişimin tespiti, dinlenmesi ve kayda alınması tedbirlerinde ise iletişimde bilgisayar kullanılsa dahi, bilgisayar çalışır vaziyette iken içeri girilmekte ve tedbire maruz kalan kişinin bu durumdan haberi olmamaktadır[314].

Bu özel koruma tedbirleri bilgisayarın maddi varlığıyla ilgili olurken telekomünikasyon yoluyla iletişimin denetlenmesi tedbirleri ise bilgisayarın maddi varlığı ile ilgili olma şartına bağlı değildir ve başka bilgisayarlar kullanılarak da tedbirler uygulanabilir[315]. Telekomünikasyon yoluya iletişimin denetlenmesi kapsamı altında bulunan koruma tedbirlerinde öncelikle iletişimin varlığının belirlenmesi söz konusu olsa da bilgisayar alanındaki bu tedbirlerde iletişimin varlığı aranmaz[316].

CMK'nın 135. maddesinde katalog suç sınırlaması vardır. CMK'nın 134. maddesinde böyle bir suç sınırlaması yoktur. Buna ek olarak adalet komisyonunun raporunda CMK'nın 134. maddesinin 1. fıkrasının önceki

[314] Şahin, **Ceza Muhakemesi Kanunu: Gazi Şerhi**, s. 372.
[315] Özbek, **a.g.e.**, s. 499.
[316] Özbek, **a.g.e.**, s. 499.

halinde bulunan "*iki yıl veya daha fazla hürriyeti bağlayıcı cezayı gerektiren cürümler*" ibaresi kaldırılmıştır[317]. Böylece suç sınırlamasının yapılmaması amaçlanmıştır.

İletişimin tespiti, kayda alınması ve dinlenmesi tedbirleri belirli sürelerle sınırlandırılmıştır (CMK md. 135/3). Şartları varsa bu sürelerin uzatılması mümkündür. Bilgisayarlara yönelik koruma tedbirinde ise böyle bir süre sınırlandırılması yapılmamıştır. Genel arama ve elkoyma hükümleri uyarınca karar veya emrin geçerli olacağı zaman süresi, kararda açıkça gösterilecektir. (CMK md. 119/2-c). Bilgisayarlara yönelik bu tedbirler genel arama ve elkoyma tedbirlerinin özel bir türü olduğundan süreye ilişkin hususlar burada da geçerli olacaktır. Başka bir ifadeyle bilgisayara yönelik arama kararında süre, açık bir şekilde belirtilecektir.

Belge veya kağıtları inceleme yetkisi Cumhuriyet savcısı ve hakime verilmiştir (CMK md. 122). Kolluk sadece arama sırasında elde edilen belge veya kâğıtlara soruşturulan suçla ilgili olup olmadığını belirleyebilmek adına inceleme yapmadan bakabilir[318]. Bununla birlikte bilirkişi incelemesi gerektiriyorsa belgelerin listelerden seçilen veya alanında uzman olanlar arasından atanan bilirkişilerce veyahut da görevlendirilmek koşulu ile kolluğun konusunda uzman personeli tarafından incelenmesi mümkündür[319]. Belge veya kâğıtların bir örneği bilgisayarlarda bulunabilmektedir. Ancak burada belge somut bir şekilde değildir; soyut bir haldedir. Kanaatimizce bu belge veya kâğıtların incelenmesi hükmü ile bilgisayarlara yönelik koruma tedbirleri birlikte değerlendirilmelidir. Bilgisayarlara yönelik bu tedbirler uygulandığında belge örneklerine rastlayan kolluk görevlileri belgenin suçla ilgili veri içerip içermediğini saptadıktan sonra çıktısını alıp durumu Cumhuriyet savcısına veya hakime bildirmelidir. Hakim veya Cumhuriyet savcısı bu çıktıların soruşturmada veya kovuşturmada delil olarak değerlendirilip değerlendirilmeyeceğini belirleyecektir.

---

[317] Şahin, **a.g.e.**, s. 372.
[318] Ünver, Hakeri, **a.g.e.**, s. 406.
[319] Çolak, Taşkın, **a.g.e.**, s. 551.

Postada elkoyma (CMK md. 129) ile bilgisayarlardaki elektronik postaların (e-posta) aranması, kopyalanması ve elkonulması tedbirleri birbirlerinden farklıdır. Farklılık, somut bir posta ile elektornik veri arasındadır. Bu nedenle ayrı şartlara tabi olması doğaldır. E-postanın iletişim aracı olarak kullanılması, incelenmesi gereken ayrı bir konudur. Dolayısıyla CMK'nın 134. maddesinin mi veya CMK'nın 135. maddesinin uygulanıp uygulanmayacağı hususu gündeme gelmektedir. Bu tartışmaya ileride değinilecektir.

II- BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA, KOPYALAMA VE ELKOYMAYANIN KAPSAMI VE ŞARTLARI

A- KAPSAMI

1- Kişi Bakımından

CMK'nın 134. maddesinde "*şüphelinin kullandığı bilgisayar*" ibaresine yer verilmiştir. Şüpheliden başka üçüncü kişilerin bilgisayarları hakkında bu tedbir uygulanamaz[320]. Başka bir ifadeyle genel hükümlere yollama yapılarak şüphelinin bilgisayarına uygulanacak olan bu tedbir, üçüncü kişilere karşı genişletilemez. Bunun nedeni, maddenin sınırlayıcı bir şekilde tedbirin uygulanmasını öngörmüş olmasıdır. Zira kamu kurumu ve kuruluşlarının, özel hukuk gerçek ve tüzel kişilerin bilgisayar sistemlerinden aramayı, taramayı ve kopya çıkarılmasını düzenleyen, "Bilgisayar Sistemlerinde Veri Taraması ve Karşılaştırılması" başlıklı tasarının 135. maddesi 26.11.2004 tarihinde kanun

[320] Şahin, **Ceza Muhakemesi Hukuku I.**, s. 248.; Aynı görüş bkz. Çolak, Taşkın, **a.g.e.**, s. 608.; *"İddianameye konu olan eylemin kanıtı olarak gösterilen ve bir kısım sanıkların yetkilisi ve çalışanı olan Uzanlara ait şirket ve evlerde yapılan aramalar sırasında elde edilen bilgisayarların nerede ve hangi yöntemle elde edildiği, sanıkların kullanımında olup olmadığı, kimler arasında yapıldığı, başkaları tarafından oluşturulma ya da içeriklerine müdahale olanağı bulunup bulunmadığı…"* Yarg. 5. CD., 11.06.2007 3700/4661K. (Aslan Ölmez, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Kopyalama ve Bunlara Elkoyma", **Terazi Aylık Hukuk Dergisi**, Sayı: 30, Şubat, 2009, s. 50).
Karşı görüş için bkz.: "*Veri aranacak olan bilgisayar, şüpheliye ait olabileceği gibi; üçüncü kişilerin veya resmi kuruluşun da olabilir."* (Centel, Zafer, **a.g.e.**, s. 398).

metninden çıkarılmıştır[321]. Tartışmalarda şüpheli veya sanıkla ilgili olmamasından; özel hayatın gizliliği, ticari sırlar gibi birçok temel hak ve özgürlüğe müdahalede bulunmasının birçok soruna neden olabileceğinden bahisle bu durumun ayrı bir kanunla düzenlenmesi gerektiği kanaatine ulaşılmıştır[322]. Kanuni bir düzenleme bulunmadığından üçüncü kişilerin bilgisayarları bu tedbirler açısından konu dışında kalacaktır.

Buna karşılık söz konusu ibareden fiili bir kullanım anlaşılmaktadır. Bilgisayarın şüpheliye ait olması gerekmez. Kaldı ki şüpheliler kendi adlarına kayıtlı ya da kendi adlarına fatura edilmemiş bilgisayarlar üzerinden de işlem yapabilirler[323]. Bu nedenle üçüncü kişilere ait olup da şüphelinin fiili kullanımında bulunan bilgisayarlar da tedbirin kapsamına dâhil olacaktır[324].

---

[321] Tasarıdan çıkarılan "Bilgisayar Sistemlerinde Veri Taraması ve Karşılaştırılması" başlıklı 135. madde aynen,
(1) Bir suç dolayısıyla yapılan soruşturmada, başka surette failin belirlenememesi veya delil elde etme imkanının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine, kamu kurum ve kuruluşları veya özel hukuk gerçek veya tüzel kişilerine ait bilgisayar sistemlerinde kayıtlı verilerin taramasının ve karşılaştırmasının yapılmasına, bu kayıtlardan kopya çıkarılmasına, kayıtların çözülerek metin haline getirilmesine, hakim tarafından karar verilebilir.
(2) Birinci fıkra hükmü ancak aşağıda sayılan suçlarla ilgili olarak uygulanabilir.
a) Türk Ceza Kanununda yer alan, 1. Göçmen kaçakçılığı ve insan ticareti (madde 79, 80), 2. Çevrenin kasten kirletilmesi (birinci fıkra hariç, madde 181), 3. Uyuşturucu veya uyarıcı madde imal ve ticareti (madde 188),4. Suç işlemek amacıyla örgüt kurma (iki, yedi ve sekizinci fıkralar hariç, madde 220) ,5. Suçtan kaynaklanan malvarlığı değerlerini aklama (madde 282), 6. Silahlı örgüt (madde 314) veya bu örgütlere silah sağlama (madde 315), suçları b) Ateşli Silahlar ve Bıçaklar İle Diğer Aletler Hakkında Kanunda tanımlanan silah kaçakçılığı (madde 12) suçlarıc) Kaçakçılıkla Mücadele Kanununda tanımlanan ve hürriyeti bağlayıcı cezayı gerektiren suçlar, d) Kültür ve Tabiat Varlıklarını Koruma Kanununun 68 ve 74 üncü maddelerinde *tanımlanan suçlar.*
(3) Birinci fıkra hükmü, a) Devlet sırrı niteliğindeki bilgiler, b) Tanıklıktan çekinebilecek kişilere ait bilgisayar sistemlerindeki bilgiler,hakkında uygulanmaz.
(4) Tarama ve karşılaştırma işlemleri sonucunda elde edilen veriler, soruşturma bakımından ihtiyaç duyulmadığının anlaşılması halinde, Cumhuriyet savcısının denetiminde derhal yok edilir ve bu husus, dosya içerisinde muhafaza edilmek üzere bir tutanağa bağlanır." şeklindedir. (**Tutanaklarla Ceza Muhakemesi Kanunu**, Ankara, Adalet Bakanlığı Yayın İşleri Dairesi Başkanlığı, 2005. s. 580, 581).

[322] Ayrıntılı bilgi için bkz. **Tutanaklarla Ceza Muhakemesi Kanunu**, Ankara, Adalet Bakanlığı Yayın İşleri Dairesi Başkanlığı, 2005. s. 580, 581, 582.

[323] Çolak, Taşkın, **a.g.e.**, s. 608.

[324] "*...Olay tarihinde sanıkla maktulün internet üzerinde sohbet ettikleri söylenen kafede sanığın 'Kaan' kod adıyla 21 no.lu 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 yazılı şekilde hüküm kurulması..."* Yarg. 1. CD. 14.11.2005. (Ölmez, **a.g.m.**, s. 50.).

Üçüncü kişilerin bilgisayarı üzerinde şüphelinin fiili bir kullanımı yoksa bu tedbirler uygulanamayacaktır.

Madde, tedbirlerin sadece şüphelinin kullandığı bilgisayarlara uygulanacağını belirtmiş, mağdurun bilgisayarlarına yönelik olarak uygulanıp uygulanmayacağı hususuna değinmemiştir. Örneğin; bir bilişim suçunun delilleri mağdurun bilgisayarında bulunabilir. Mağdurun savcılığa veya mahkemeye delilleri sunabilme imkânı vardır. Burada mağdur kendi bilgisayarına bu tedbirlerin uygulanmasını mahkemeden talep edip edemeyeceği sorusu akla gelmektedir. Kanuni bir düzenleme bulunmasa da Yargıtay, suçtan zarar gören bir tüzel kişinin bilgisayarında delil arama yapılmasının mümkün olduğuna hükmetmiştir[325]. Mağdur kavramı da suçtan zarar gören kapsamına dâhil olduğundan mağdurun bilgisayarında ve veri saklama birimlerinde delil araştırılması mümkündür. Ancak CMK'nın 134. maddesindeki şartlar mağdur bakımından aranmaz. Zira suç şüphesi altında olmayan mağdurun, şikâyetçinin veya tanığın bilgisayar sistemleri ve verileri söz konusu tedbirin konusunu oluşturmamaktadır[326]. Bu açıdan yaklaşıldığında mağdurun bilgisayarındaki arama ve elkoyma sadece bir delil incelemesi mahiyeti taşımaktadır. Nitekim CMK'nın 134. maddesindeki söz konusu şartlar sadece şüpheli veya sanık için öngörülmüştür.

Kişiler bakımından tartışılması gereken bir husus daha vardır. Günümüzde avukatların bilgisayar kullandıkları göz önüne alınırsa bir soruşturmada şüpheli olan avukatın bilgisayarına yönelik hangi koruma tedbirinin işletileceği sorunu karşımıza çıkmaktadır. Çünkü ceza muhakemesinde suç şüphesi altında bulunan avukatlara özgü bir koruma tedbiri mevcuttur. Avukat bürolarında arama, elkoyma ve postada elkoyma tedbirlerine yer veren CMK'nın 130. maddesi, genel arama ve elkoymanın

---

[325] *"...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 dosylarını 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. (Malkoç, Yüksektepe, **a.g.e.**, s. 643).

[326] İhsan Baştürk, "Bilgisayar Sistemleri ile Verilerinde Arama, Kopyalama ve Elkoyma", **Fasikül Aylık Hukuk Dergisi**, CEHAMER, Sayı: 9, Ağustos 2010 s. 28.

özel bir düzenlemesini oluşturmaktadır. Avukatlara yönelik özel bir düzenleme getirilmesinin asıl gayesi müdafilik mesleğini korumaktır[327]. Düzenlemeye göre avukatın bürosunda arama yapabilmek için mahkeme kararına ihtiyaç vardır. Avukat bürolarında arama ve elkoyma ise savcının denetiminde mümkün olacaktır (CMK md. 130/1). Buna ek olarak baro başkanı veya onu temsil eden bir avukat, arama yapılan avukat bürsounda hazır bulunabilecektir. Madde hükmü, avukat ile müvekkil arasındaki mesleki ilişkinin gizliliğini zedelemeden arama ve elkoyma yapılmasını ele almaktadır. Aranan deliller avukatın bilgisayarında olabilmektedir. Dolayısıyla CMK'nın 130. maddesine istinaden avukatın bilgisayarları aranabilecek midir sorusu akla gelmektedir. Kanaatimizce CMK'nın 130. maddesi avukatın bilgisayarlarını kapsamamaktadır. Tedbirlerin ilişkili olduğu temel hak ve özgürlükler açısından yaklaşılırsa CMK'nın 130. maddesi avukat-müvekkil arasındaki gizliliğe ve savunma hakkına müdahalede bulunmaktadır. CMK'nın 134. maddesi ise burada sadece avukat-müvekkil gizliliğine dokunmamakta; özel yaşamın gizliliği, mülkiyet hakkı vb. gibi diğer hak ve özgürlüklere müdahale etmektedir. Yani bilgisayarlara yönelik bu tedbir, avukat bürolarında arama, elkoyma ve postada elkoymaya oranla daha ağır sonuçlara neden olacaktır. Bu nedenle ölçülülük ilkesi gereği CMK'nın 130. maddesi öncelikle uygulanabilir. Ancak CMK'nın 130. maddesi bakımından bir sonuca varılamayacağı arama sırasında veya arama öncesinde anlaşılmışsa, şartlar sağlandığı takdirde CMK md. 134'teki hükümler avukatların bilgisayarları hakkında da uygulanabilecektir. Fikrimizce ölçülülük ilkesine riayet edilerek avukatın bilgisayarına yönelik bu tedbirler CMK'nın 130. maddesindeki hükümlerle birlikte işletilmelidir. Bu açıdan yaklaşıldığında CMK md. 134'e göre sadece şüphelinin bilgisayarına yönelik arama yapılacağı için avukat şüpheli sıfatını taşımadığı müddetçe, onun bilgisayarı aranamayacaktır. Ancak avukat şüpheli sıfatını taşıyorsa, bilgisayarında arama yapılırken baro başkanı veya onu temsil eden avukat, avukatın

[327] Doğan Soyaslan, **Ceza Muhakemesi Hukuku**, 3. Baskı, Ankara, Yetkin Yayınları, 2007, s. 287.

bürosunda bulunabilmeli ve avukat-müvekkil ilişkisinin gizliliğine ait hususlarda görüşlerini ileri sürebilmelidir.

2- Bilgisayarlar, Bilgisayar Programları, Kütükleri ve Diğer Cihazlar Bakımından

Bilgisayarlar ilk bölümde bahsedilen esaslar çerçevesinde ele alınmalıdır. Öncelikle bilgisayarlar TCK'daki bilişim alanındaki suçlar başlığı altında düzenlenen 243. maddenin gerekçesinde vurgulandığı üzere verileri otomatik işlemlere tabi tutan manyetik sistemlerdir. Verileri işleme fonksiyonuna, yani bilişim yeteneğine sahip olan bilgisayardan bir bilişim sistemi anlaşılmalıdır. Bu itibarla bilgisayar olarak adlandırılmayan fakat bilgisayar gibi işlev gören (programlanabilen, veri işleyebilen, iletebilen, saklayabilen) diğer elektronik cihazlar için de bu tedbir işletilebilir.

AK-SSS'de "bilgisayar sistemi" kavramına bakıldığında bilgisayarın veri işleme gibi genel özelliklerinin yanında birbirine bağlanabilen veya birbirleriyle ilişki kurabilen özellikleri de dikkate alınmıştır. İster bir bilişim sistemi olarak ister birbirlerine bağlanabilen veya ilişkili olabilen cihaz olarak düşünülsün buradan anlaşılması gereken; hizmet veren bilgisayarlar da dahil her türlü bilgisayarın (masaüstü, dizüstü, el bilgisayarları vb.) bu tedbirin konusunu oluşturduğudur. Her türlü bilgisayarda delil aranması söz konusu olunca elektronik delil elde edebilmek amacıyla bilgisayarın türü, işletim sistemi ve özellikleri hakkında bilgi edinilmeli ve bir ön inceleme yapılmalıdır[328].

CMK'nın 134. maddesindeki hükümler gereğince arama ve kopyalama bilgisayar programlarında da yapılabilmektedir. Birinci bölümde belirtilen; FSEK md. 1-B-g'deki tanım gereğince bilgisayar programından bilgisayarın özel işlem ve görev yapmasını sağlayacak bir emir dizgesi anlaşılmalıdır. Bu emir dizgeleri sayesinde bilgisayarlar çalışmakta ve bilgi içeren dosyalar

[328] Berber, **Adli Bilişim**, s. 64.

açığa çıkabilmektedir. Veri kavramını tanımlarken belirttiğimiz üzere AK-SSS'ye göre veri kavramına programlar da dâhildir (AK-SSS md. 1-b).

Bilgisayar programlarının bilgisayarda bulunması doğal olduğundan bilgisayar programlarında yapılacak arama ile bilgisayarda yapılacak arama aynı olmaktadır. Bilgisayar programları bilgisayar dışında örneğin veri saklama birimlerinde (paket programlar) de bulunabilmektedir. Dolayısıya programlarda delil araması söz konusu olursa, bu tedbirlerin uygulanması veri saklama birimlerine de yansıyacaktır.

Kullanıcının işlerini kolaylaştıran uygulama yazılımlarının yanında zararlı programlara da birer delil olabilme gözüyle bakılabilir. Örneğin bilişim sistemini bozarak bilişim suçunu işlenmesine olanak sağlayan virüs gibi zararlı programlar şüphelinin bilgisayarında saklanabilir. İster işletim sistemleri veya uygulama yazılımları olsun isterse programlama dilleri olsun bazen programın kendisi de illegal olabilmektedir[329]. FSEK'e aykırı lisanssız yazılımların bir veri saklama biriminde bulunması buna örnek oluşturur. Sayılan bu örneklerin yanında bilgisayar programları yalnızca arama, kopyalama ve elkoymanın konusu olmazlar; adli bilişim incelemesinde ve elektronik delil elde etmede birer araç olarak da kullanılabilirler.

Bilgisayar kütükleri İngilizce'de "log" olarak geçmekte ve internet hizmet sağlayıcılarının internet erişimini gerçekleştirdikleri kullanıcılara ait olan IP (Internet Protocol) numaralarını ve diğer erişim bilgilerini sakladıkları veri tabanlarını ifade etmektedir[330]. Bunun dışında büyük kapasitedeki verileri saklayan veri tabanları veya arşiv amaçlı saklanan büyük çaptaki veri saklama birimleri de bilgisayar kütüğü olarak nitelendirilebilir.

2007 yılında yürürlüğe giren 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun uyarınca düzenlenen 01/11/2007 tarihli Resmi Gazetede yayımlanan İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmeliğin 3/1(e) maddesinde "*İç IP Dağıtım Logları; Kendi iç ağlarında*

---

[329] Osman Nihat Şen, "Ceza Hukukunda Bilgisayar Araştırmaları", **CHD**, Sayı:1, Ekim 2006, s. 376.

[330] Özbek, **a.g.e.**, s. 502.

dağıtılan IP adres bilgilerini, kullanıma başlama ve bitiş tarih ve saatini ve bu IP adreslerini kullanan bilgisayarların tekil ağ cihaz numarasını (MAC adresi) gösteren bilgileri … ifade eder" şeklinde bir tanım yapılmıştır. Bu tanım bilgisayar kütüklerinde arama ve elkoymanın uygulanmasının daha iyi anlaşılmasına hizmet etmektedir.

AK-SSS'deki memorandumda "*birbirine bağlı veya birbiriyle ilişkili cihaz*" ibaresinin geniş yorumlanmasıyla veri saklama birimlerinin de bu tedbirin konusunu oluşturduğu yukarıda ifade edilmişti. CMK'nın 134. maddesinde veri saklama birimleri hakkında bu tedbirlerin uygulanmasına ilişkin bir bilgi yoktur. Lâkin AÖAY'nin elkoymaya ilişkin 17. maddesinin 3. fıkrası şu şekildedir: "*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."*. Bu suretle "*çıkarılabilir donanımlar*" ibaresinden veri saklama birimleri anlaşılmalı ve bunlar üzerinde de arama, kopyalama ve elkoyma yapılmalıdır. Kaldı ki, maddi gerçeğe götüren deliller bilgisayarlarda olmasa bile bilgisayara bağlanabilen veri saklama birimlerinin içinde bulunabilir.

İletişimde kullanılan cihazlar bakımından örneğin; bazı cep telefonu modelleri günümüzde bir bilgisayar gibi işlev görebildiğine göre cep telefonu üzerinde telekomünikasyon yoluyla iletişimin denetlenmesi tedbirlerinin mi, yoksa bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirlerinin mi, uygulanacağı sorusu akla gelmektedir. CMK'nın 134. maddesinin gerekçesinde bahsedilen cihazın durağan olma hali, bilgisayar işlevi gören diğer cihazlar için de yorumlanabilir. Yine maddenin gerekçesinden hareket edilerek iletişimin denetlenmesi tedbirlerinde bilgisayar kullanılsa dahi tedbire maruz kalan kişinin haberinin olmaması burada dikkate alınmalıdır. Buna göre, cep telefonu iletişimde kullanılıyorsa iletişimin tespiti, dinlenmesi ve kayda alınması tedbirleri uygulanacaktır. Ancak cep telefonu durağan bir cihaz olarak kullanılıyorsa başka bir ifadeyle elektronik verileri saklamada veya bilişim yeteneğine uygun şekilde kullanılıyorsa CMK'nın 134. maddesi uygulanacaktır. Kısaca

hangi alanda daha fazla veya kim tarafından kullanıldığı tespit edilebiliyorsa ya da hangi alanda delil elde edilebileceği anlaşılıyorsa o alanda etkin olan koruma tedbirine başvurulmalıdır. Buradan hareketle cep telefonu ile bir bilişim suçunun işlenmesi halinde bu suçun delillerinin elde edilmesi bakımından CMK'nın 134. maddesinin uygulanamacağı görüşüne katılamamaktayız[331].

İnternet yardımıyla iletişimin ses ve görüntülü bir şekilde veya e-posta yardımıyla yapılması münkündür. E-posta CMK'nın 134. maddesinin gerekçesinde belirtilen durağan olma niteliğini taşısa da iletişimde kullanılan bir hizmettir. E-postalar üzerinde aynı cep telefonlarında olduğu gibi hangi koruma tedbirinin uygulama alanı bulacağı sorusuna cevap aramamız gerekmektedir. Bu sorun AK-SSS'deki memorandumun 190. maddesinde de tartışılmıştır[332].

Sözleşme e-postada hangi koruma tedbirinin uygulanacağı konusunda bir belirleme yapmamış, bu belirlemeyi taraf ülkelerin takdirine bırakmıştır. E-postalar hakkında doğru bir değerlendirme yapabilmek için telekomünikasyon yoluyla iletişimin denetlenmesi tedbirlerinden iletişimin tespiti, dinlenmesi ve kayda alınması tedbirlerine kısaca değinmek gerekmektedir. İletişimin tespiti, belli bir telefon numarasından kimlerin ne zaman arandığı, konuşmanın ne kadar süreyle yapıldığı, e-posta yoluyla kimlerle iletişimin sağlandığı

---

[331] "*Cep telefonundan doğrudan doğruya internete girilerek bir bilişim suçu işlendiğinde bu suçun CMK 134'teki soruşturma yöntemine göre soruşturulmasının mümkün olmadığı kanaatindeyiz. Çünkü CMK 134, bilgisayarların aranmasını düzenlemektedir. Oysa cep telefonu bilgisayar değildir. Ancak internete girmek yoluyla bilişim suçu cep telefonu aracılığıyla da işlenebilir.*" (Taşkın, **a.g.e.**, s. 173).

[332] AK-SSS memorandumun 190. maddesi aynen,
"*Madde 19 saklı bilgisayar verileri için geçerlidir. Bu açıdan, alıcı kendi bilgisayar sistemine indirinceye kadar bir İnternet hizmet sağlayıcının posta kutusunda bekleyen e-posta mesajlarının saklı bilgisayar verisi olarak mı yoksa aktarım halindeki veri olarak mı değerlendirilmesi gerektiği sorusu ortaya çıkmaktadır. Bazı Taraf Ülkelerin mevzuatında bu e-posta mesajları iletişimin bir parçasıdır ve dolayısıyla içerikleri ancak müdahale yetkisini uygulayarak temin edilebilir. Bazı hukuk sistemlerinde ise bu mesajlar Madde 19'un kapsamına giren saklı veriler olarak görülür. Bu nedenle, Taraflar hangisinin kendi ulusal hukuk sistemlerine uygun olduğunu belirlemek için yasalarını incelemelidir.*" şeklindedir. (Avrupa Konseyi Siber Suç Sözleşmesi, Çev: İnternet ve Hukuk Platformu: İVHP, (Erişim) http://www.binbilen.org/belgeler/Siber_Suclar_Sozlesmesi.pdf, 25 Haziran 2009. s. 55).

hususlarının belirlenmesiyle ilgilidir[333]. İletişimin dinlenmesi, telli veya telsiz telefonla ya da internet ortamı içerisinde yapılan konuşmalarla ilgili olurken, kayda alınması ise bu konuşmalardaki sesleri görüntüleri ve e-posta yoluyla yapılan iletişim içeriklerini kapsamaktadır[334]. Ayrıca e-postada, kişinin haberi olmadan da delil elde etmek mümkündür. Başka bilgisayarlar veya cihazlar kullanılarak hangi e-posta adresleriyle iletişim kurulduğu ve bu iletişimin içeriği hakkındaki bilgilere ulaşılabilir. Bununla birlikte e-postalar internet yer sağlayıcılarının sakladıkları yedeklerinde de olabilir. Netice itibariyle e-postanın iletişim nitelikleri üzerinden bir değerlendirme yapılmalıdır. Bu bakımdan e-posta üzerinden delil elde edilmesi söz konusu olduğunda telekomünikasyon yoluyla iletişimin denetlenmesi tedbirlerine başvurulması gerekecektir.

B- ŞARTLARI

1- Suç Soruşturmasının Varlığı

Maddenin ilk fıkrasından bu tedbirlerin sadece soruşturma aşamasında uygulanabileceği anlaşılmaktadır. Madde metninde soruşturmadan, şüpheliden ve hâkim kararından bahsedilmekte, kovuşturma, mahkeme kararı ve sanıkla ilgili herhangi bir bilgi bulunmamaktadır. Buna istinaden maddenin kovuşturma aşamasında uygulanmayacağı görüşü ileri sürülmektedir[335]. Fakat maddede kovuşturma aşamasında bu tedbirin uygulanmamasına ilişkin sınırlayıcı bir hüküm bulunmadığı dikkate alınırsa,

---

[333] Cumhur Şahin, "Telekomünikasyon Yoluyla İletişimin Denetlenmesi-Yargıtay Kararları Çerçevesinde Bir Değerlendirme" **Bilişim Hukuku Konferansı-YARGITAY**, Ankara, 09-10 Ekim 2008, s.124.

[334] Şahin, **a.g.m.**, s. 125.

[335] "*Bu tedbire kovuşturma evresinde başvurulması açıkça öngörülmemiştir. Belirtelim ki aleni bir duruşmada mahkemenin bu tedbire karar vermei halinde tedbirden haberdar olan ilgililerin söz konusu kayıtları yok etmesi söz konusu olacaktır. Kovuşturma evresinde bu tedbire başvurulması yarar sağlamayacaktır."* (Centel, Zafer, **a.g.e.**, s. 399); "*Ayrıca, CMK 134/1'in hatalı düzenlemesi nedeniyle, sanığın kullandığı veya sanığa ait bilgisayar veya bilgisayar kütüklerinde arama yapılması olanağı bulunmamaktadır.Bu hükmün kovuşturma evresi için, yani sanık hakkında da kullanılması, koruma tedbirlerinin kanunilik ilkesine aykırı olup; bunun yapılabilmesi için kanuni düzenlemeye ihtiyaç bulunmaktadır."* (Ünver, Hakeri, **a.g.e.**, s. 425).

tedbirlerin kovuşturma aşamasında da uygulanabileceği sonucuna ulaşabilecektir. Mahkeme re'sen araştırma ilkesine dayanarak bu tedbirlere hükmedebilecektir[336]. Kovuşturma aşamasında, kovuşturmayı gerektirecek belirli delillerin toplanmış olması "*başka surette delil elde edilme imkânının bulunmaması* " şartını uygulanmaz hale getirse de; elde edilen deliller maddi gerçeğin ortaya çıkarılmasına, sanığın mahkûmiyetine hükmedecek nitelikte olmayabilir. Şüphe hala yenilmemiş olabileceğinden bahisle mahkeme, ihtiyari olarak ve re'sen araştırma ilkesini de esas alarak bu tedbirin uygulanmasına kovuşturma aşamasında karar verebilir.

Bu tedbirlere sadece CMK kapsamında yürütülen bir "suç" soruşturmasında imkân tanınmış olması nedeniyle hukukun diğer alanlarında (örneğin; idari soruşturma ve disiplin soruşturması gib) yürütülen soruşturmalarda bilgisayarlara başvurulması söz konusu olmayacaktır[337]. Aksi kabul temel hak ve özgürlüklere derin bir müdahale teşkil eder. Aynı husus kabahatler bakımından da geçerlidir.

CMK'nın 134 maddesinde arama koruma tedbirinde olduğu gibi bir şüphe derecesi belirtilmemiştir. Şüphe derecesinin belirtilmemiş olmasıyla basit şüphenin yeterli olduğunu ileri süren görüşler mevcuttur[338]. Madde metnindeki "*başka surette delil elde etme imkânının bulunmaması"* deyiminden ilk olarak diğer koruma tedbirlerinin uygulanması sonucunda herhangi bir delil bulunamamış olduğu anlaşılmaktadır. Buna rağmen bu tedbire başvurulması, şüphenin hala yenilmediğini göstermektedir. Suç şüphesi bakımından burada basit şüpheden ziyade temel olarak makul şüphe gündeme gelmektedir.

CMK'nın 117. maddesinin 2. fıkrasında ise, üçüncü kişilere ait aramalarda belirli olayların varlığı sözkonusu olduğundan makul şüpheye nazaran daha yoğun olan bir şüphe aranmıştır. Üçüncü kişilere ait bilgisayarlar üzerinde şüphelinin fiili kullanımı mevcut olabilir. Fakat madde düzenlemesi şüphelinin kullandığı bilgisayarı esas aldığından makul

---

[336] Şahin, **Ceza Muhakemesi Hukuku I.**, s. 248, 261.; Aynı görüş bkz. Soyaslan, **a.g.e.**, s. 284.
[337] Baştürk, **a.g.m.**, s. 25.
[338] Özbek, **a.g.e.**, s. 503; Aynı görüş için bkz. Centel, Zafer, **a.g.e.**, s. 398.

şüphenin daha yoğun hali bu madde bakımından aranmayacaktır. CMK'nın 135. maddesinde ise kuvvetli şüphe belirtilmiştir. Bu itibarla kuvvetli şüphenin bilgisayarlara yönelik tedbirlerin uygulanmasında aranması gereken bir unsur olduğu ifade edilmiştir[339]. Bu görüş, bilgisayara yönelik tedbirlerin uygulanmasında, CMK'nın 135. maddesinden hareketle kıyas yaparak bu sonuca varmaktadır.

Kuvvetli şüphe CMK'nın çeşitli maddelerinde özel olarak belirtilmiştir. Kuvvetli şüphe gözlem altına alınma, tutuklama, taşınmazlara hak ve alacaklara elkoyma, az önce bahsedilen telekomünikasyon yoluyla iletişimin denetlenmesi tedbileri gibi temel hak özgürlükleri derinden etkileyen koruma tedbirleri için aranmaktadır. Başka bir ifadeyle kuvvetli şüphenin belirtilmediği koruma tedbirlerinde temel hak ve özgürlüklere müdahale; belirtildiği koruma tedbirlerine oranla daha az niteliktedir. Örneğin; telekomünikasyon yoluyla iletişimin denetlenmesi özel hayatın gizliliğine ve haberleşme hürriyetine ağır bir müdahale olarak anlaşıldığından basit bir şüphe yeterli sayılmamış, şüphenin nitelikli bir yoğunluğa erişmiş olması amaçlanmıştır[340]. Kuvvetli şüphe, belirtildiği tedbirlerle sınırlılık arz eder ve CMK'nın düzenleniş sistemi bunu öngörmektedir. Toplanan delillere bakıldığında yapılan bir duruşmada sanığın mahkum olması kuvvetle muhtemel ise kuvvetli şüphenin varlığından bahsedilir[341]. Kuvvetli şüphe denildiği vakit bu şüpheye kaynaklık eden kuvvetli belirtilerin varlığı gerekmektedir. Kuvvetli belirtiler olmadığı takdirde somut olgular varsa ortaya çıkan şüphe makul şüphedir.

Söz konusu tedbirlerin arama ve elkoymanın genel hükümlerine tabi olması göz önüne alındığında bu tedbirlerin icrasında makul şüphe aranabileceği ileri sürülebilir. Böylelikle madde metninde şüphe derecesine yer verilmemesi basit şüphenin aranacağını göstermeyecektir. Kanımızca bir bilgisayar kişinin tüm hayatını içerebilecek detayları saklayabileceğinden bu

---

[339] "*Nasıl ki bir kimsenin cep telefonunun dinlenmesi için CMK 135 gereğince kuvvetli suç şüphesinin varlığı aranmaktaysa, cep telefonunu kadar mahrem verileri içerebilecek dizüstü bilgisayarın aranmasında da kuvvetli suç şüphesinini varlığı kabul edilmelidir.*" (Taşkın, **a.g.e.**, s. 171).

[340] Şahin, **Ceza Muhakemesi Hukuku I**, s. 268.

[341] Öztürk, Erdem, **a.g.e.**, s. 540.

madde içerisinde kuvvetli şüphenin özellikle belirtilmesi gerekirdi. Koruma tedbirlerinde kıyas yapılmasa da iletişimin denetlenmesi tedbirlerinde müdahale edilen temel hak ve özgürlüklerle bilgisayara yönelik koruma tedbirlerinin uygulanmasıyla ihlale uğrayan temel hak ve özgürlükler hemen hemen aynıdır. Her ne kadar CMK'nın 135. maddesinden hareketle kıyas yapılabileceğine ilişkin görüşle aynı sonuca ulaşılsa da kanaatimizce sanığın lehine olan durumlar dikkate alınarak ve temel hak özgürlüklerle de bağlantılı olarak kıyasa gerek olmadan kuvvetli şüphe doğrudan aranmalıdır. Fakat maddeye kuvvetli şüphenin konulması CMK'nın sistemiyle tutarlılık açısından yararlı olacaktır[342].

2- Başka Surette Delil Elde Etme İmkânının Bulunmaması

Maddedeki "*başka surette delil elde etme imkânının bulunmaması*" ibaresi maddenin gerekçesinde son çare ilkesi (ultima ratio) olarak yer almıştır. Buna göre ilgili tedbirlere başvurabilmek için durumun zorunluluk arzetmesi yani en son uygulanması gerekmektedir. Koruma tedbirlerinde ölçülülük ilkesi önemli bir role sahip olduğundan diğer koruma tedbirlerinin uygulanması ve bu yolla sonuç alınabilmesi mümkünse, bu özel tedbirlere gidilemeyecektir[343]. Telekomünikasyon yoluyla iletişimin denetlenmesi tedbirlerinde ve diğer gizli koruma tedbirlerinde de yer alan bu şart, bu tedbirin diğer tedbirlere göre ikincil olduğunu belirtmektedir[344]. Ölçülülük ilkesi gereği işlenen fiili ortaya koymak amacıyla birden fazla tedbirin işletilmesi söz konusu olursa, öncelikle temel hak ve özgürlüklere en az müdahale oluşturan tedbire başvurulacaktır (Öncelik-sonralık ilişkisi)[345]. Tedbirlerin ağır sonuçlara neden olabilmesi ihtimali karşısında bu şartın varlığı temel hak ve özgürlükler açısından bir güvence teşkil etmektedir.

Başka surette delil elde etme imkanınının bulunmaması şartından yalnızca diğer tedbirlere başvurulmuş ve bundan sonuç alınamadığı değil;

---

[342] Aynı yönde bkz. Baştürk, **a.g.m.**, s. 26.
[343] Özbek, **a.g.e.**, s. 504.
[344] Öztürk, Erdem, **a.g.e.**, s. 640.
[345] Şahin, **a.g.e.**, s. 268.

diğer koruma tedbirlerine başvurulduğunda amaca ulaşılamayacağına ilişkin bir öngörünün varlığı da anlaşılmalıdır[346]. Lakin bu öngörünün somut noktalara dayanması gerekmektedir ki, aksine tutum uygulanan tedbirin hukuka aykırılığına neden olacaktır.

Bilgisayarlara yönelik koruma tedbirlerinde aranan bu şart, tedbirin arama ve elkoymaya nazaran ikincil nitelikte olduğunu göstermektedir. Tedbirlerin ikincil nitelikte olması, tedbirlerin mutlaka diğer tedbirlerden sonra uygulanacağı anlamına gelmez. Somut olayın durumuna göre, diğer koruma tedbirlerine başvurulması halinde amacın hâsıl olmayacağı en başından itibaren anlaşılmaktaysa; doğrudan bilgisayarlara yönelik tedbirlere başvurulabilir. Örneğin; TCK'nın 226. maddesindeki müstehcenlik suçuna ait deliller şüphelinin bilgisayarlarında saklanabilir. Başka koruma tedbirleri ile delil elde edilemeyeceği anlaşılmışsa, sadece bilgisayarlarda arama yapılarak bu delillerin elde edilmesi mümkünse ve bu delillerin bilgisayarlarda bulunduğuna dair somut belirtiler varsa şüphelinin bilgisayarları üzerinde CMK'nın 134. maddesi öncelikli olarak uygulanacaktır.

Bilgisayarlara yönelik özel koruma tedbirleri, başka surette delil elde etme imkânının bulunmaması şartını ihtiva eden diğer koruma tedbirleri ile birlikte uygulanabilir mi sorusu akla gelmektedir. Örneğin; hem şüphelinin bilgisayarları hakkında arama, kopyalama veya elkoyma kararı verilmiş hem de kişi hakkında iletişimin denetlenmesi tedbirlerine veya teknik araçlarla izleme tedbirine yer verilmiştir (CMK md. 140). Bu ikincil nitelikteki koruma tedbirleri arasında öncelik-sonralık ilişkisinin uygulanması ayrı bir sorundur. Özellikle organize suçlarda aynı zaman diliminde bu ikincil nitelikteki tedbirlerin hepsinin uygulanmasını gerektiğini ileri süren görüşler vardır[347]. Ölçülülük ilkesine riayet edilerek somut olayda bu tedbirlerden hangisi aynı neticeye varma bakımından temel hak ve özgürlüklere daha az oranda müdahale ediyorsa o tedbir öncelikli bir şekilde işletilebilir; fakat bu durum

[346] Öztürk, Erdem, **a.g.e.**, s. 640.
[347] Ünver, Hakeri, **a.g.e.**, s. 439.

gerekli koşulların varlığı durumunda her iki veya üç tedbirin birlikte uygulanmasına engel oluşturmamaktadır[348]. .

CMK'nın 134. maddesi, başka surette delil elde etme imkânının bulunmaması şartını öngörse de uygulamada bu hususun dikkate alınmadığı gözlemlenmektedir. Arama tedbirinin uygulanması sonucunda bilgisayar üzerinde elkoyma söz konusu olursa, son çare ilkesi değerlendirme dışı kalacaktır[349]. Genel arama ve elkoymanın şartları bilgisayara yönelik tedbirlere nazaran daha hafif olduğundan, uygulamaya yansıyan bu durumun eleştiriye maruz kalması aşikârdır. Genel arama ve elkoyma tedbirlerinin uygulanması sırasında bilgisayara elkonulması CMK'nın 134. maddesini işlevsiz hale getirecektir. Ayrıca eleştiriye maruz kalan bu durum, söz konusu tedbirin ikincil olma özelliğinin anlaşılamadığının göstergesidir. Başka surette delil elde etme imkânının gözetilmeden bu tedbire başvurulması halinde elde edilen deliller, hukuka aykırılık iddiasına maruz kalacaktır.

Elkonulma sonucunda soruşturma dosyasına giren bilgisayarların araştırılmasının savcı tarafından görmezden gelinmesi ve değerlendirmenin savcı tarafından yapılmaması konuları da eleştirilmiştir[350]. Kanaatimizce savcı bu durumda bilgisayarlar üzerinden elde edilen delilleri de değerlendirmelidir. Bilirkişinin veya kolluğun buradaki inceleme görevi belge ve kağıtları inceleme yetkisindeki gibi sınırlıdır (CMK md. 122/1). Savcı çözülererek metin haline getirilen veri özetlerinin delil niteliğinde olup olmadığını hazırlayacağı iddianamede belirtebilecektir.

3- Hâkim Kararına Dayanması

Bilgisayarlara yönelik arama ve kopyalama tedbiri ancak hâkim tarafından karar verilir. Gecikmesinde sakınca bulunan hal meydana gelse dahi Cumhuriyet savcısının veya savcıya ulaşılamayan hallerde kolluk amirinin yazılı emriyle bu tedbirler uygulanamaz. Buna karşılık maddenin 1.

---

[348] Öztürk, Erdem, **a.g.e.**, s. 640.
[349] Bkz. Güçlü Sevim, "Bilgisayar ve Bilgisayar Kütüklerine El Konulması ve Uygulamadaki Sorunlar", **İBD**, Cilt 81, Sayı 3, 2007, s. 997.
[350] Sevim **a.g.m.**, s. 997.

fıkrası hakimin kararının söz konusu olabilmesi için savcının talebini aramaktadır. Soruşturma aşamasında savcının etkinliğini arttırması CMK'nın en göze çarpan özelliğidir[351]. Bu itibarla maddede savcının talebine yer verilmesi, ceza muhakemesinin genel işleyişiyle uyumludur.

Maddenin gerekçesinde soruşturma evresinde tedbire sulh ceza hakiminin karar vereceği belirtilmiştir. Kovuşturma aşamasında ise mahkeme bu tedbirlere savcının talebiyle veya talep olmadan re'sen araştırma ilkesini dikkate alarak hükmedebilir.

Söz konusu tedbirlerin soruşturma aşamasında Cumhuriyet savcısının talebiyle hâkim kararına bağlanması; maddede gecikmesinde sakınca bulunan hal ve bu halde söz konusu olabilecek yazılı emirlere yer verilmemesi; tedbirin sıkı koşullara bağlı bir şekilde düzenlendiğini göstermektedir. Hâkim kararı, burada başka surette delil elde etme imkanının bulunmaması koşulu gibi temel hak özgürlüklerin korunmasında bir güvence sağlamaktadır.

CMK'nın 119. maddesinin 2. fıkrasında yer alan arama kararında olması gereken unsurlar söz konusu bu tedbirlerin uygulanması açısından da dikkate alınacaktır. Bilgisayarlar, bilgisayar programları ve kütüklerinde arama ve kopyalama kararında; şüphelinin açık kimliği, hangi suçtan ötürü soruşturma yapıldığı, süresi, suçun işlendiğine yönelik belirtilerin varolduğu ve başka bir tedbir ile istenen delillerin elde edilemeyeceği unsurlarına yer verilmelidir[352]. Uygulamada bazı somut olaylar açısından hâkim kararının olmaması değil; hâkim kararında olması gereken unsurların yer almaması eleştirilmiştir[353].

Hâkim kararı şüphelinin kullandığı bilgisayar, bilgisayar programları ve kütüklerinde arama yapılmasına, kayıt altında tutulan bilgilerden kopya elde edilmesine ve kayıtlardan bir çözümleme işlemi yapılarak metin haline çevrilmesine yöneliktir[354]. Hâkim kararının arama, kopyalama ve elkoymanın her birini içerebileceğini veya bu tedbirlerden sadece birinin ya da ikisinin

[351] Şahin, **a.g.e.**, s. 113.
[352] Malkoç, Yüksektepe, **a.g.e.**, s. 640.
[353] Ayrıntılı bilgi için bkz. Sevim, **a.g.m.** , s. 997.
[354] Kunter, Yenisey, Nuhoğlu, **a.g.e.**, s. 1023.

kararda bulunabileceğini ileri süren bir görüş vardır[355]. Kanaatimizce elkoyma gizlenmiş bilgileri bulma ve şifrelerin kırılması hallerinde uygulandığından arama kararı aynı genel arama ve elkoymadaki gibi elkoyma yetkisini de kapsamalıdır. Çünkü kolluk görevlilerinin bilgisayar başında şifre veya gizlenmiş bilgilerle karşılaşması muhtemeldir ve bu durum önceden bilinmeyebilir.

CMK'nın 163. maddesinde sulh ceza hâkiminin yapabileceği soruşturma işlemlerinden bahsedilmiştir[356]. Sulh ceza hâkimi suçüstü hali ile gecikmesinde sakınca bulunan hallerde savcıya ulaşılamadığı veya olayın içeriğinden savcının iş yükünü aşan bir durumun varlığı anlaşılıyorsa sulh ceza hâkimi savcının soruşturma işlemlerindeki yetkilerini kullanabilecektir. Ancak sulh ceza hakimi savcılık sıfatı altında soruşturma yürütüyorsa, soruşturma evresinde CMK'nın 162. maddesince hakim kararını gerekli kılan bir işlem gündeme gelirse, bu kararı hükmedemeyecektir[357]. Aksi kabul hakim tarafsızlığını gölgeler niteliktedir. Bu itibarla sulh ceza hakimi, bilgisayarlarda arama, kopyalama ve elkoyma tedbirlerine savcılık sıfatı altında hükmedemez. Bu durumda sulh ceza hakimi, hakim kararı için diğer bir sulh ceza hakiminden talep de bulunacaktır. Ancak karar düzenlenirken savcıya ulaşılamama nedenlerine veya olay içeriği itibariyle savcının iş yükünü aştığını gösteren hususlara kesinlikle değinilmelidir.

---

[355] Vahit Bıçak, **Suç Muhakemesi Hukuku,** Ankara, Seçkin Yayınevi, 2010, s. 584.

[356] CMK'nın 163. maddesi aynen,
1- Suçüstü hâli ile gecikmesinde sakınca bulunan hâllerde, Cumhuriyet savcısına erişilemiyorsa veya olay genişliği itibariyla Cumhuriyet savcınsın iş gücünü aşıyorsa,sulh ceza hakimi de bütün soruşturma işlemlerini yapabilir.
2- Kolluk amir ve memurları, sulh ceza hakimi tarafından emredilen tedbirleri alır ve araştırmaları yerine getirirler." şeklindedir.

[357] Şahin, **a.g.e.**, s. 124.

III- BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA, KOPYALAMA VE ELKOYMANIN UYGULANMASI

A- GENEL OLARAK

Bilgisayarlara yönelik arama, kopyalama ve elkoymanın uygulanmasındaki asıl amaç delillerin anlaşılabilir ve bütünlüğünün bozulmamış bir şekilde elde edilmesidir. Ancak tedbirlerin müdahalede bulunduğu temel hak ve özgürlükler bakımından sonucunun ağır olması, bu tedbirlere dikkatli bir şekilde yaklaşmayı gerekli kılmaktadır. Kaldı ki yapılan müdahale ile kişiye aşırı yük getirilmemeli ve kişi üzerindeki etkisi makul bir seviyede olmalıdır[358]. Özellikle bilgisayarlara uygulanacak koruma tedbirlerinde bu husus daima göz önünde bulundurulmalıdır. Şüphelinin hak ve özgürlüklerine ağır müdahaleye yol açmayan tedbirlerden başlanmalıdır. Yeterli delile ulaşıldığı takdirde bu kapsamdaki diğer tedbirlere başvurulmayacaktır. Delile ulaşılamaması nedeniyle bilgisayarlar üzerinde diğer tedbirlerin uygulanması gündeme geldiğinde ölçülülük ilkesine en uygun tedbirden devam edilmelidir. Her tedbir olay itibariyle ölçülü olmayabilir. Bunun için tedbirler arasında ölçülülük bakımından bir değerlendirme yapılmalıdır. Temel hak ve özgürlüklere ağır müdahaleyi öngören tedbir en son olarak uygulanmalıdır.

CMK'nın 134. maddesi şüphelinin kullandığı bilgisayarı mümkün olduğunca az meşgul ederek arama yapılmasını öngörmektedir. Şüphelinin bilgisayarı şüphelide kalacak şekilde tedbirler işletilmelidir. Delile ulaşılırsa çıktısının alınması veya kayıtlardan kopyanın çıkarılması yeterlidir. Bilgisayara elkoymanın şartları ortaya çıksa bile bilgisayardaki verilerin bir kısmının veya tamamının kopyasının alınması mümkünse bu yola başvurulmalıdır. Nitekin kanun bu duruma cevaz vermiştir (CMK md. 134/5). Kanaatimizce elkoymaya başvurmadan önce bilgisayardaki verilerin bir

[358] Centel, Zafer, **a.g.e.**, s. 315.

kısmının veya tamamının kopyası alınmalıdır. Bu tedbir kullanılamıyorsa ve şartları varsa elkoyma tedbiri icra edilmelidir. Elkoyma, niteliği itibariyle arama ve kopyalamadan daha ağır bir tedbir olduğundan CMK'nın 134. maddesine TBMM Genel Kurulu'ndaki yapılan görüşmeler sonucunda elkoyma ile ilgili son üç fıkra konulmuştur. Değişiklik gerekçesinde, bilgisayara veya bilgisayar verilerine elkoymanın uygulama alanında meydana gelebilecek sorunların önüne geçilmesi istendiği ifade edilmiştir[359]. Bilgisayarlara elkoyma şifrenin çözülememesi veya gizlenmiş bilgilere ulaşılamaması hallerinde söz konusu olmaktadır.

Öte yandan karmaşık veya organize suçlarda delillerin kaybolma riskiyle karşılaşılmaması için bilgsayardaki verilerin tamamının adli bilişim süreci doğrultusunda imajı alınabilir. Lakin bu yöntem basit bir şekilde delil elde etmenin mümkün olmaması durumunda uygulanmalıdır. Şüphelinin kullandığı bilgisayarın gereksiz yere meşgul edileceği anlaşılmışsa bu süreç işletilmemelidir. Çünkü imaj alma işlemi, yani yedekleme yapılması uzun sürebilmektedir[360]. Bu süreçle amaçlanan, elektronik delillerin tutarlılığını, bütünlüğünü, bozulmadığını ispatlamaktır. Bir diğer amaç da şüphelinin, bilgisayarına veri eklendiğine ve eklenen veri üzerinden hakkında soruşturma ve kovuşturma yürütüldüğüne ilişkin iddiasının önüne geçmektir. Alınan imaj üzerinden arama yapılması mümkündür. Böylelikle CMK md. 134/5'in adli bilişim yöntemleriyle uyumlu bir şekilde yorumlanabileceği sonucuna ulaşmaktayız.

Sonuç olarak CMK'nın 134. maddesi hükümleri terditli bir şekilde uygulanmalıdır. Aksi halde maddi gerçeğe ulaşma ile temel hak ve özgürlükler arasındaki denge maddi gerçeğe ulaşma lehine bozulmuş olacaktır.

---

[359] Şahin, **Ceza Muhakemesi Kanunu: Gazi Şerhi**, s. 372.

[360] *"...elkoyma işlemi sırasında tüm verilerin yedeklemesinin yapılabilmesi için, şüphelinin Polisleri evinde veya işyerinde en az 4,5-5 saat ve en çok 12-13 saat misafir etmesi gerekmektedir. Harddiskin özellikleri, aranacak bilginin, elde edilmesi istenen neler olduğuna bağlı olarak bu yelpazede bir süreye ihtiyaç olmaktadır."*(Leyla Keser Berber, "Adli Bilişim, CMK md. 134. ve Düşündürdükleri", (Erişim) http://www.leylakeser.org, 10 Aralık 2008, s. 2).

B- ARAMA SONUCUNDA KAYITLARDAN KOPYA ÇIKARILMASI VE KAYITLARIN METİN HALE GETİRİLMESİ

1- Arama Sonucunda Kayıtlardan Kopya Çıkarılması

Madde hükmü gereği ilk adım verilerin aranmasıdır. Arama tedbirlerinin uygulanmasında cihazların bulundukları yerden ayrı bir yere götürülmesine lüzum bulunmamaktadır[361]. Arama, özellikle delilin hemen bulunabileceği klasik suçlarda şüphelinin bilgisayarları üzerinde uygulanabilir. Örneğin; bir bilgisayarda hakaret suçuna ilişkin delilleri veya lisansız programa yönelik delilleri tespit edebilmek için bilgisayar üzerinde hızlı bir şekilde arama yapılabilir.

Bilgisayar programlarından elektronik delil araması son kullanılan dosyaları tarama şeklinde olabilir. Suç konusu ile ilgili kelime taratma biçimde de arama yapılabilir. Bunlar gibi başka şekillerde de bilgisayar programlarından elektronik delil elde edilebilir. Delil araması yapılmadan önce işletim sistemi, programlama dilleri ve uygulama yazılımları hakkında bir önbilgi edinilmelidir.

Adli bilişim sürecinde ise imaj alma işlemi, yani bilgisayar sistemindeki verilerin kopyalanması için tasarlanmış özel programlar ve teçhizatlar kullanılmalıdır. Belirtilen sürece uygun bir metod takip edilmelidir. Delil güvenliğini ve bütünlüğünü sağlamak adli bilişimin önemli amaçları arasında olduğundan bilgisayar çevresinde titizlikle davranılmalıdır. Bir bilgisayarda arama yapılmasına başlanmadan önce kolluk birimleri bilgisayar çevresini koruma altına almalıdır. Böylece adli bilişim uzmanlarının incelemesi için gerekli önlemler sağlanmış olur[362]. Şüpheliden bilgisayardaki programları çalıştırmada kesinlikle yardım istenmemelidir[363]. Şüpheli yardım etme görünümü altında delilleri silerek veya bozarak karartabilir.

Adli bilişim çerçevesinde arama işlemi çıkarılan kopya üzerinde yapılmaktadır. Çoğaltılan kopyanın orijinaline uygun olduğu kontrol

---

[361] Baştürk, **a.g.m.**, s. 29.
[362] Kaygısız, **a.g.e.**, s. 292.
[363] Berber, **Adli Bilişim**, s. 46, 47, vd.

edilmelidir. Bunun için özetleme (hash) işlemi yapılarak verilerin değiştirilmediği ve suç içerecek delillerin eklenmediği ispatlanmalıdır. Özetleme işlemiyle bir veri sayısı belirlenir. Belirlenen değer imza altına alınır[364]. Bu işlem yapılmazsa en küçük veri değişimi sonucunda veri sayısı aynı olmayacağından verilerin değiştirildiği ileri sürülerek delillerin tutarlılığı tartışmalı hale gelecektir. Elde edilen delillerin hukuka aykırı olmaları söz konusu olmasa bile ispat kuvvetleri azalacaktır. Yapılan incelemeler sonucu veri sayısının değişmediği tespit edilirse elde edilen verilerin delil olmadığı iddiası çürütülmüş olacaktır.

Arama işlemi yapılırken yine özetleme (hash) işlemiyle bilinen dosyalar ile silinmiş dosyalar birbirinden ayrılır. Böylelikle incelemeye alınacak dosya sayısı azaltılarak daha kolay araştırma yapılabilecektir[365]. Arama işlemleri sadece bu yöntemlerle sınırlı değildir. Adli bilişim uzmanları dosya yığınları arasında saklanan elektronik delillere ulaşabilmek için bilinen dosya türleri incelemesi, kelime incelemesi, görüntü incelemeleri vb. gibi bir takım yöntemler kullanılabilirler[366].

Arama işlemi sonucu soruşturma konusu suçla ilgili delil bulunduğu takdirde bir kopyası çıkarılacaktır. Kopyalama elkoymanın soyut alanda yapılmasını ifade etmektedir. Diğer bir ifadeyle kopyalama elkoymanın veriler üzerinde gerçekleşmesidir. Keza AK-SSS'de de kopyalamanın, elkoymanın bir türü olduğundan bahsedilmektedir[367].

Ulaşılan delilin kopyası olay mahalline getirilen bir bilgisayara veya veri saklama birimlerine kaydedilir. Mümkünse elde edilen delillerin çıktıları alınabilir. Böylelikle veri çıktısına elkonulmuş olacaktır. Arama tutanağı

---

[364] *"Bu işlem, bir manada "elektronik mühür" diyebileceğimiz bir işlemdir."* (Şen, **a.g.m.**, s. 378).

[365] Kaygısız, **a.g.e.**, s. 298.

[366] Kaygısız, **a.g.e.**, s. 299.

[367] Memorandumun 199. maddesi aynen,
"Dolayısıyla verilere el koyma ya da onları benzer şekilde güven altına almanın iki işlevi vardır: 1) Örneğin verileri kopyalamak yoluyla delil toplamak, ya da 2) örneğin verileri kopyalamak ve daha sonra orijinal versiyonlarını erişilmez kılmak ya da taşımak yoluyla verileri müsadere etmek. El koymak, el konan verilerin nihai olarak silinmesi anlamına gelmemektedir." şeklindedir. Avrupa Konseyi Siber Suç Sözleşmesi, Çev: İnternet ve Hukuk Platformu: İVHP, (Erişim) http://www.binbilen.org/belgeler/Siber_Suclar_Sozlesmesi.pdf, 25 Haziran 2009. s. 56).

düzenlenirken arama işleminin özetini belirten hususlar CMK'nın 134. maddesine uygun bir biçimde ortaya konulacaktır. Arama tutanağındaki unsurlar buradaki tedbirlerin özelliklerine göre biçimlenecektir. Arama tutanağında hangi bilgisayarın, programların, bilgisayar kütüklerinin delil aramasına konu olduğunu, hangi veri saklama birimlerine bakıldığı ve bunların seri numaraları, özellikleri, bilgisayarın modeli, markası, IP numaralarıyla birlikte hangi bölümlerde hangi delillere ulaşıldığı veya ulaşılamadığı vb. gibi diğer hususlar tutanağa kaydedilmelidir. Aranılan bilgisayarların, veri saklama birimlerinin ve bölümlerin birbirlerinden ayırt edilebilmeleri için tutanakta açıkça belirtilmesi gerekmektedir. Tutanakta araştırmayı yapan adli bilişim uzmanlarının açık kimlikleri yazılmalı ve imzalanmalıdır. Arama şüphelinin kullandığı üçüncü kişiye ait bilgisayarlar üzerinde yapılıyorsa arama ve elkoymadaki genel hükümler uyarınca bu kişiler aramada hazır bulunabilirler. Ayrıca savcının katılmadığı aramalarda iki kişinin hazır bulundurulması kuralı burada da uygulanmalıdır. Elektronik deliller, çok hassas olduğundan ani bir hareket verilerin zarar görmesine sebebiyet verdiğinden bu kişiler bilgisayar çevresinden uzak tutulmalıdır. Savcının gözlemi ve bilgi alması soruşturmanın güvenliği açısından ne kadar yararlıysa bilgisayardan elektronik delil elde edilmesinde o kadar yararlı olacaktır[368].

Bilgisayarlarda aramanın uzaktan erişim sağlanarak gizli bir şekilde de yapılabileceğini ifade eden bir görüş ileri sürülmüştür[369]. Kanaatimizce uzaktan erişim sağlanarak bilgisayarda arama yapma, CMK'nın 134. maddesinde öngörülen bir arama çeşidi değildir. Ayrıca böyle bir yöntem temel hak ve özgürlüklere ağır müdahale anlamına gelmektedir. Dolayısıyla özel bir düzenleme gerekmektedir. Ancak böyle bir düzenleme getirilirken

[368] Kaygısız, **a.g.e.**, s. 292.
[369] "*Elektronik veri takibi (veya kanundaki ifadesiyle bilgisayarlarda arama) bilgisayar donanımı (kasa vs.) kolluğun hakimiyetine alınarak açık olarak yapılabileceği gibi, bilgisayara uzaktan erişim sağlanarak yazılım üzerinden gizli olarak da yapılabilir.*" (Bıçak, **a.g.e.**, s. 583).

Alman Federal AYM'nin bu konuda verdiği kararın gerekçesinde bahsedilen yeni bir hakkın içeriğinin incelenmesi faydalı olacaktır[370].

2- Kayıtların Çözülerek Metin Haline Getirilmesi

Kayıtların metin hale getirilmesi en basit haliyle yazıcı çıktısıyla mümkün olacaktır. Kanunun "*kayıtların çözülerek metin hale getirilmesi"* ifadesi elektronik delillerin nitelikleri gereği hasara uğramasının öngörülebilir olması nedeniyle ispat bakımından önemlidir. Burada kanun koyucunun elektronik delili, belge deliline dönüştürmesindeki asıl amacı elektornik delillerin kaybolma riskini en aza indirmektir. Aynı durum maddenin 5. fıkrasında da öngörülmüştür. Fıkraya göre kopyası elde edilen veriler kâğıda yazdırılacak, bu durum tutanağa geçirilecek ve ilgililer tarafından imzalanacaktır. Adli bilişim sürecinde bir kısmının kopyasının alınması, kopyaların incelenmesinin uzun sürmesi ve doğru analizlerin yapılamaması gibi sorunlar doğabileceğinden uygulamada bu fıkranın etkinliğinin düşük olduğu iddia edilmiştir[371]. Bir bilgisayarda bulunan bütün verilerin milyonlarca sayfaya tekabül edebilmesi mümkün olduğundan kopyası alınan veriler suçla ilgili olmalıdır[372]. Kanımızca bir kısmının kopyasının alınması şüphelinin en çok kullandığı veya delil saklaması muhtemel olarak öngörülen birimler üzerinde olmalıdır. Adli bilişim uzmanları şüphelinin en çok kullandığı birimleri bir inceleme ile tespit edeceklerdir.

Arama sonucunda bulunan delil içerdiği düşünülen dosyaların bir dökümü alınmalı, diğer bir deyişle metin haline getirilmeli ve metinler içerisinde delil olabilecek dosyalar ile ilgili teknik ayrıntılar bulunmalıdır[373]. Delillerin teknik ayrıntılarının yazılması aksine iddiaların çürütülmesine hizmet edecektir.

---

[370] Bkz. Sözleşmeye Taraf Olan Ülkelerde Bilgisayarlara Yönelik Arama, Kopyalama ve Elkoyma Tedbirleri, Almanya, s. 56; (BverfG, NJW 2008, 822).
[371] Tan, "Adli Bilişim", s. 12.
[372] Özbek, **a.g.e.**, s. 504.
[373] Aktepe, **a.g.m.**, s. 69.

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. Öte yandan bilgisayar çevresinde yazıcının önceden bulunup bulunmadığının bilinemeyeceği gibi kolluğun yanında her zaman yazıcı getirmesi de beklenemez. Kopyası alınan verilerin belge haline getirilmesi daha sonradan da yapılabilir. Bu durumda şüphelinin bu belgelere erişme imkânı da sağlanmalıdır.

C- BİLGİSAYARA ELKONULMASI VE YEDEKLEME YAPILMASI

1- Genel Olarak

Kanun koyucu yalnızca iki halde bilgisayarlarda elkoymaya cevaz vermiştir: şifrenin çözülememesi ve gizlenmiş bilgilere ulaşılamaması. Bu iki şart kanunda tahdidi olarak öngörülmüştür. Bahsedilen şartların yorum yoluyla genişletilmesi, koruma tedbirlerindeki kıyas yasağına aykırılık oluşturur.

Tedbirlerin asıl amacı bilgisayarları olduğu yerde bırakarak delil elde etmektir. Bu nedenle bilgisayara elkoymanın şartları söz konusu olursa elkoyma derhal uygulanmamalıdır. Öncelikle CMK'nın md. 134/5'teki hüküm değerlendirilmelidir. Buna göre bilgisayar veya bilgisayar kütüklerine elkoyma uygulanmadan sistemdeki verilerin tamamı veya bir kısmının kopyasının alınması gerekmektedir. Fıkra hükmünün uygulanaması halinde bilgisayara elkoymaya başvurulacaktır.

Maddenin son fıkrası, koruma tedbirlerindeki ölçülülük ilkesinin vücut bulmuş şeklidir. Her durumda şifrenin çözülememesi veya gizlenmiş bilgilere ulaşılamaması şartlarına istinaden elkoyma yapılamaz. Örneğin; şifrenin çözülmemesi veya gizlenmiş bilgilere ulaşılamaması bir kopyasının alınmasına engel oluşturmayabilir. Alınan kopya üzerinden şifre çözümlenebilir ya da gizlenmiş bilgilere erişilebilir. Bahsedilen koşullar mümkünse öncelikle bu fıkra hükmü uygulanmalıdır.

2- Bilgisayara Elkonulmasını Gerektiren Haller

a- Şifrenin Çözülememesi

Şifreleme verinin içeriğinin gizlenmesi için matematiksel algoritmalar kullanılarak karıştırılan veri sürecidir[374]. Bir anahtarın kapıyı açması gibi şifreyi çözmeye muktedir numaraların veya harflerin bilinmesiyle veri kolaylıkla ve çabuk bir şekilde okunabilir duruma geçecektir[375].

Şifreleme özellikle e-ticaret alanında büyük ölçüde yaygındır. Özel hayatın veya ticari alanda gizliliğin ve güvenliğin zedelenmemesi için bu tekniğe kişiler, özel ve kamu kuruluşları önem vermişlerdir[376]. Şifreleme kullanılarak, saklanan bilgilere istenmeyen kullanıcıların erişmemeleri sağlanır. Şifrelemenin bu avantajlarının yanında dezavantajları da vardır. Şifre soruşturma ve kovuşturmanın en dikkat çekici yerinde konuşlandırılabilir. Karmaşık bir yapıda tasarlanmış olabilir. Şifre aynı zamanda adli kolluğun delil elde etmedeki bütün çabalarını boşa da çıkarabilir[377].

Bilgisayarın, bilgisayar programlarının veya kütüklerinin açılması şifrelenmiş olabilir. Delil bulunan bir veriye veya bir dosyaya şifreleme yöntemi ile erişim engellenebilir. Elkoyma tedbirinde ölçülülük ilkesini esas aldığımızda öncelikle şifreyi olay yerinde çözmek gerekmektedir. Bu şifrelerin çözümü bilgisayar çevresinde yapılamadığı takdirde bilgisayara veya veri saklama birimlerine elkoyma imkânı doğacaktır.

Olay yerinde elektonik delillerden ayrı olarak bilgisayarın çevresinde bulunan yazılı parolalar, elyazısı notları, yazılım ve donanıma ait kitaplar, takvimler literatür, metin veya grafik şeklindeki bilgisayar çıktıları ve fotoğraflar birer elektronik olmayan delil niteliğinde olup adli bilişimin analiz basamağında kullanılabildiğinden muhafaza altına alınmalıdır[378]. Bu

---

[374] Phlip R. Reitinger, **"**Encryption, anonymity and markets", **Cybercrime: Law Enforcement, Security And Surveillance In The Information Age**, Ed: Douglas Thomas, Brian D. Loader, London and Newyork, Routledge, 2003, s. 133.
[375] Reitinger, **a.g.m.**, s. 134.
[376] Sınar, **a.g.e.**, s. 58.
[377] Reitinger, **a.g.m.**, s. 134
[378] Berber, **a.g.e,**, s. 68.

elektronik olmayan deliller şifrenin kırılmasında da büyük önem taşıyabilmektedir. Şifre, bu bulguların içinde olabilir.

Şifre, olay yerinde çözülemiyorsa bilgisayara elkonulur ve adli bilişim laboratuvarlarında bu şifre çözülmeye çalışılır. Şifrenin çözülmesinde adli bilişim uzmanları bilgi sahibi olmalı ve bunun için gerekli programları kullanmalıdır. Çözümün yapılmasıyla birlikte gerekli kopyalar alınacak ve elkonulan birimler gecikme olmaksızın iade edilecektir.

b- Gizlenmiş Bilgilere Ulaşılamaması

Gizlenmiş bilgilere ulaşılamaması halinde" ibaresi TBMM Adalet Komisyonu'nda tartışılmış olup gizlenmiş veya silinmiş verilerin geri getirilmesini sağlamak için maddeye konulmuştur[379]. Böylelikle gizlenmiş verilerden sadece verilerin gizlenmiş olması değil; silinmiş verilerin ortaya çıkarılması da anlaşılacaktır.

Elektronik deliller şüpheli tarafından gizlenmiş olabilir. Bu itibarla maddenin 2. fıkrası maddi gerçeğin ortaya çıkarılması bakımından önemlidir. Şüpheli veya sanık suç bakımından delil olabilecek verileri gizleyebilir. Bilgisayar programlarının gelişmişliği düşünüldüğünde bunun yapılması mümkündür. Verileri gizlemek üzere özel programlar tasarlanmış olabilir[380]. Gizlenmiş bilgilere olay yerinde ulaşılması mümkün değilse elkoyma tedbirine başvurulabilecektir.

Verilerin silinmiş olması her zaman onun yok olduğu anlamına gelmez[381]. Silinen veriler kurtarıcı programlarla geri getirilebilir. Lâkin veriler özel programlar kullanılarak geri getirilmesi mümkün olmayacak şekilde yok edilebilir. Silinmiş verilerin geri getirilmesi adli bilişim incelemesi içerisinde yer alan veri kurtarma servislerinde yapılmaktadır.

---

[379] Ayrıntılı bilgi için bkz. **Tutanaklarla Ceza Muhakemesi Kanunu**, s. 576, 577 ve 578.

[380] "*Amerika'daki serbest piyasa ortamında devletin yaptığı kanuni çalışmalara karşı özel sektörde özel kişi veya kurumlara yönelik özde delillendirmeyi önleyecek makinenin hard diskindeki verilerin, bulunamayacak şekilde, istenilen zamanda ve/veya her makine açılıp kapandığında ortadan kaldıran programları piyasaya sürmüştürler*." (Güven Şeker, "Bilişim Suçlarının Delillendirilmesinde Amerikan Uygulaması Ve Ülkemizdeki Durum**",** (Erişim), **http://www.egm.gov.tr/egitim/dergi/eskisayi/29/yeni/bilal_sen.doc,** 22 Mayıs 2009. s. 6).

[381] Dokurer, **a.g.m.**, s. 246.

3-Bilgisayara Elkoymanın Uygulanması ve Yedekleme Yapılması

a- Bilgisayara Elkoymanın Uygulanması

Bilgisayarlara, bilgisayar kütüklerine veya veri saklama birimlerine yapılacak elkoyma diğer eşyalar gibi değildir. Bilgisayarlara uygulanan elkoyma tedbiri genel elkoymadan daha sıkı şartlara tabi olduğu gibi daha özgün bir içeriğe sahiptir. Elektronik cihazlar hassas oldukları için ısı, nem, statik elektrik, manyetik alanlar ve fiziksel ortamlardan çabuk etkilenirler. Cihazların zararlı ve bozucu etkilere maruz kalmaması için gerekli teçhizatlar edinilmelidir.

Elkoymada öncelikle olay yerinde envanter defteri tutulmalı ve belgelemeye başvurulmalıdır. Elkoyma yapılırken elektronik delilin niteliği göz önüne alınacaktır. Elkoyma, adli bilişim sürecinin toplama basamağına uygun bir şekilde yapılmalıdır. Anti-manyetik ve fiziksel darbelere dayanıklı özel kutulara ihtiyaç vardır[382]. Bilgisayarlar ve veri saklama birimleri bu kutulara konulmalı ve kutular üzerinde etiketleme yapılmalıdır. Yapılan bu etiketlemeler arama tutanağına ek bir biçimde belirtilmelidir. Birbirine karıştığı takdirde delil bütünlüğü bozulmuş olacaktır.

Bilgisayarlara uygun bir şekilde elkoyma yapıldıktan sonra nakliyesi önemlidir. Nakliye sırasında da elkonulan cihazlara dikkat edilmelidir. Nakliye sırasında bilgisayarın donanımını oluşturan parçalara zarar gelmemesi için fiziksel darbelere karşı dikkatli olunmalıdır. Aksi takdirde bilgisayar veya veri saklama birimi zarara uğrayacaktır.

Elkonulan eşyanın değerinin korunması ve zarar görmesini engellemek amacıyla gerekli tedbirler alınacaktır (CMK md. 132/4). Bilgisayarların muhafaza edilmesi Suç Eşyası Yönetmeliği'nin 9. maddesinin 2. fıkrasına göre yapılacaktır[383]. Hüküm gereği bilgisayarların ısı, nem, manyetik ve fiziksel etkilerden korunması için gerekli ortam hazırlanacaktır.

---

[382] Dokurer, **a.g.m.**, s. 243.

[383] SEY'in 9. maddesinin 2. fıkrası aynen,
"*Bilgisayar, bilgisayar kütükleri ve bu sisteme ilişkin verilerin asıl ya da kopyaları, ses ve görüntü kayıtlarının bulunduğu depolama aygıtları gibi eşya, bozulmalarını engelleyecek, nem, ısı, manyetik alan ve darbelerden korunmalarını sağlayacak uygun ortamda muhafaza edilir.*" şeklindedir.

Gerekli ortamdan maksat örneğin bu yerlerin sıcaklığının belli bir derecede tutulmasıdır. Adli bilişim sürecinin inceleme basamağında da bu ortam oluşturulmalıdır. Bilgisayarlardaki sabit disklerin incelenmesi özellikle "tozsuz laboratuar" denilen tozun hiç girmediği yerlerde yapılır[384].

Bazı elektronik delillerin; tarih, zaman ve sistem yapılanışları bakımından bir süre sonunda kaybolabilmesi mümkündür. Bu husus dikkate alınırsa bu delilleri saklayan bilgisayarların ve birimlerin uzun süre koruma altında tutulmaması önem arzetmektedir[385].

Bilgisayarlara elkoyma işlemi gerçekleştirilmeden önce bilgisayarın özelliklerine bakılmalıdır. Örneğin kesintisiz olarak hizmet veren servis sağlayıcı türündeki bilgisayarların elkonularak incelenmeye alınması çoğu kez faydalı sonuçlar vermez[386]. Mümkünse gerekli ekipmanlar götürülerek bu tür bilgisayarların bulunduğu yerde inceleme yapılması daha doğru olacaktır.

Elkoymanın genel hükümleri bilgisayarlarda elkoymaya uygun düştüğü ölçüde burada da uygulanacaktır. Elkonulan bilgisayarlar hakkındaki tedbire maruz kalan kişinin görüş ve iddiaları arama sonucunda verilecek belgede yer almalıdır (CMK md. 121/2, md. 123). Elkonulan bilgisayar ve girdi-çıktı işlemlerinin yürütülmesini sağlayan donanıma ait parçalar veya veri saklama birimleri hakkında bir defter yapılmalıdır (CMK md 121/1). Bu defter envanter defteri veya bununla uyumlu farklı bir defter olabilir.

SEY'in 8. maddesinin 1. fıkrası inceleme için eşyanın teslimini düzenlemiştir[387]. Düzenlemeye göre emanet memurluğunda saklanan eşya mahkeme ve diğer resmi dairelere incelenmek üzere suç eşyasını bir yazı ile imza karşılığında teslim edecektir. Teslimin Cumhuriyet savcısının iznine tabi

---

[384] *"Böyle bir laboratuvarın hem kurulması, bakımı ve işletilmesi oldukça masraflı olduğundan hem de bunların hepsi finanse edilebilecek olsa da teknolojisi kolayca transfer edilebilir olmadığından tüm dünyada Amerika, İsrail, Finlandiya gibi gelişmiş birkaç ülkede bulunmaktadır."* (Dokurer, **a.g.m**., s. 248.)

[385] Berber, **Adli Bilişim.**, s. 73.

[386] Dokurer, **a.g.m.**, s. 246.

[387] SEY'in 8. maddesinin 1. fıkrası aynen,
"Emanet memuru, mahkeme ve diğer resmî daireler tarafından incelenmek üzere yazılı olarak istenilen suç eşyasını, üzerindeki etiketlerde yazılı bilgiyi kapsayan bir yazı ile isteyen makama, esas defterindeki özel yere görevlinin imzasını almak suretiyle teslim eder." şeklindedir.

olmaması eleştirilmiştir[388]. Ayrıca "*diğer resmi daireler*" ibaresinden kolluğun da buna dahil olacağı düşünülerek savcının iznine tabi olmadan bilgisayarları incelemeye yetkili olduğu ileri sürülmüştür[389]. Halbuki böyle bir düzenleme olsa da savcı elkonulan bilgisayarları veya veri saklama birimlerini kolluk birimlerine inceleme için tevdi eder. İnceleme adli bilişim süreci içerisinde olacağından kolluk birimlerinin adli bilişim alanında bilgi sahibi olmaları uygulanan tedbirlerin başarıya ulaşmasında son derece önemlidir.

Şifre çözüldükten sonra veya gizlenmiş bilgilerden gerekli kopyaların alınması halinde elkonulan cihazlar gecikme olmaksızın iade edilecektir. Gecikme olmadan iadesinin gerçekleşmesi incelemenin makul sürede bitirilmesi nedeniyledir.

CMK'nın 63. maddesi bilirkişinin atanmasını düzenlemiştir[390]. Maddenin 3. fıkrası savcının bilirkişi atamasında hâkimin yetkilerini kullanabileceğini belirtmiştir. Cumhuriyet savcısı bu fıkraya dayanarak soruşturma aşamasında bilirkişiye tedbire konu olan bilgisayarı incelettirebilir. Adli bilişimle ilgili bilirkişiler uygulamada genellikle emniyet müdürlüklerinden seçilmektedir[391]. Buna karşılık 2004 yılında Adli Tıp içerisinde Fizik İhtisas Dairesi Başkanlığı adli bilişim alanında resmi bilirkişilik görevini edinmiştir[392]. Kanımızca bu bilirkişiler yukarıda bahsedildiği üzere adli bilişim sertifakalarına sahip olmalıdır.

---

[388] Sevimli, **a.g.m.**, s. 998.
[389] Sevimli, **a.g.m.**, s. 999.
[390] CMK'nın 63. maddesi aynen,
"*1- Çözümü uzmanlığı, özel veya teknik bilgiyi gerektiren hâllerde bilirkişinin oy ve görüşünün alınmasına re'sen, Cumhuriyet savcısının, katılanın, vekilinin, şüphelinin veya sanığın, müdafiinin veya kanunî temsilcinin istemi üzerine karar verilebilir. Ancak hâkimlik mesleğinin gerektirdiği genel ve hukukî bilgi ile çözülmesi olanaklı konularda bilirkişi dinlenemez.*
2- Bilirkişi atanması ve gerekçe gösterilerek sayısının birden çok olarak saptanması, hâkim veya mahkemeye aittir. Birden çok bilirkişi atanmasına ilişkin istemler reddedildiğinde de aynı biçimde karar verilir.
3- Soruşturma evresinde Cumhuriyet savcısı da bu Maddede gösterilen yetkileri kullanabilir."
şeklindedir.
[391] Berber, "Adli Bilişim, CMK md. 134. ve Düşündürdükleri", s. 2.
[392] Berber, "Adli Bilişim, CMK md. 134. ve Düşündürdükleri", s. 3.

b- Yedekleme Yapılması

İmaj alma, bilgisayarlardaki verilerin birebir kopyasının alınmasını ifade etmektedir. Yedekleme, sistemin çökmesi veya doğal afet risklerine karşı sistemi kurtarmak için verilerin kopyasının çıkarılmasıdır[393]. 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[394].Yedekleme fıkranın hükmünden yola çıkılarak tüm verilerin kopyasının elde edilmesi olduğuna göre imaj alma işlemiyle aynı anlamda kullanılmaktadır. Örneğin sabit diskin imajının alınması onun birebir kopyasının çıkarılmasını veya onun yedeklendiğini göstermektedir.

Yedekleme, maddenin 3. fıkrasında düzenlendiği üzere bilgisayar veya bilgisayar kütüklerinde elkoyma işlemi sırasında yapılacaktır. "*sistemdeki tüm verilerin yedeklemesi*" ibaresi bilgisayarın bir bilişim sistemi olduğu anlayışına uygundur.

İlgili fıkrada "bilgisayar programları" ibaresi yer almamıştır. Bilgisayar programları genellikle bilgisayarın sabit diskinde bulunduklarından dolayı bilgisayardaki tüm verilerin yedeklenmesi bilgisayar programlarını da kapsamaktadır. Bu nedenle söz konusu ibarenin yer almaması bir eksiklik teşkil etmez.

Bilgisayarlara ve bilgisayar kütüklerine elkoymada bütün veriler için yedekleme yapılması zorunludur[395]. Verilerin kaybolması veya bir zarar tehlikesi olmasa da yedekleme uygulanmalıdır. Yedekleme yapılmasının en önemli nedeni bilgisayara veya veri saklama birimine sonradan delil konulduğu iddiasının önüne geçmektir[396]. Yedekleme sayesinde verilerin zarar görme ihtimali azalmaktadır. Yedek zarar görse bile orijinalinden imaj alma işlemiyle bir yedek daha çıkarılabilir.

---

[393] Berber, **Adli Bilişim**, s. 104.
[394] Berber, **a.g.e.**, s. 104.
[395] Çolak, Taşkın, **a.g.e.**, s. 609.
[396] Çolak, Taşkın, **a.g.e.**, s. 609.

Büyük kapasitedeki bilgisayarların ve bilgisayar kütüklerinin veya birden çok şüphelinin bilgisayarlarında elkoyma uygulanırken kolluk birimlerinin yedekleme yapması için gerekli programları ve cihazları olay yerine getirmeleri her zaman mümkün olmamaktadır[397]. Bu nedenle ve adli bilişim sürecinin etkisiyle olay yerinde yedekleme yapılmasının mümkün olmadığı ve sonuçta bu hükmün uygulama alanının bulunmadığı iddiası söz konusudur[398]. Böyle bir durumda yedekleme, bilgisayarlara elkonulduktan sonra adli bilişim laboratuvarında yapılacaktır. Yedekleme bir defaya mahsus olarak yapılmaz. Birden fazla yapılmalıdır. Uygulamada yedekleme yapılarak (imaj alma işlemiyle) başta adli bilişim analiz işlemlerine olmak üzere biri mahkemeye, biri savcıya, biri savunma tarafına toplam 4 adet kopya sunulmaktadır[399].

Yedeklemenin sadece sabit diske yapılmaması gerektiği AÖAY'nin 17. maddesinin 3. fıkrasındaki hükümlerden çıkarılmaktadır. Nitekim ilgili fıkradaki hükümler bu yargıyı doğrular niteliktedir. Yedekleme bilgisayar ağları, diğer uzak bilgisayar kütükleri ve bilgisayarın takılıp çıkarılabilen donanımlarında da uygulanabilecektir. Konu içerisinde bahsedildiği üzere fıkradaki "*çıkarılabilir donanımları"* ibaresinden CD, USB ve diğer veri saklama birimleri anlaşılacaktır. Bu birimler bağlandıklarında bir donanım olarak bilgisayarda görünmektedirler.

4- Şüpheliye veya Vekiline Yedekten Bir Kopya Verilmesi

Maddenin dördüncü fıkrası yedekten bir kopya çıkarılmasını, bu kopyanın şüpheliye veya vekiline verilmesini konu edinmiştir. Fıkradaki hükme göre kopyanın çıkarılıp şüpheliye veya vekiline verilmesi talep şartına bağlanmıştır. Talep olmadan yedeklenen verilerin bir kopyası verilmeyecektir. Kopyanın verilmesi konusu tutanakta belirtilerek imza altına alınacaktır.

CMK'nın 134. maddesinden olay yerindeki Cumhuriyet savcısının veya kolluğun, şüpheliye veya sanığa, kopyalardan bir örnek alma hakkının

---

[397] Berber, "Adli Bilişim, CMK md. 134. ve Düşündürdükleri", s. 2.
[398] Berber, "Adli Bilişim, CMK md. 134. ve Düşündürdükleri", s. 2.
[399] Uzunay, Koçak, **a.g.m.**, s. 5.

olduğunu hatırlatmasının zorunlu olup olmadığı anlaşılamamaktadır. Şüphelinin böyle bir talep hakkının varlığından haberdar olması her zaman beklenemez. Kanımızca arama tutanağı düzenlenirken arama sonucunda verilecek belgede kişinin görüş ve iddialarına başvurulduğunda böyle bir bilgilendirme yapılması faydalı olacaktır. Zira şüphelinin veya sanığın eşyası, üstü, konutu, işyeri veya ona ait diğer yerlerin aranması durumunda şüpheli veya sanığa da aramanın amacı ile ilgili bilgilendirme yapılabilir[400]. Şüphelinin veya vekilinin talebi doğrultusunda yedekten bir kopya çıkarılması eleştirilmiş olup talep aranmadan bir kopya verilmesi gerektiği ifade edilmektedir[401]. Kanun hükmü talep şartını aradığı için talep aranmadan kopya verilmesi düşünülemez. Talep şartına bağlı olmaksızın şüpheliye veya vekiline kopya verilebilmesi için söz konusu fıkranın yeniden formüle edilmesi gerekmektedir. Fikrimizce delilin, hukuka aykırılık iddiasıyla karşılaşmaması için talep olmasa dahi şüpheli veya sanığa verilmek üzere bir kopya çıkarılması fayda sağlayacaktır. Konu içerisinde bahsedildiği üzere uygulamada da bu yapılmaktadır. Şayet talep yapılmamışsa çıkarılmış olan kopya elde tutulacaktır. Talebin elkoymadan sonra yapılamayacağına ilişkin yasaklayıcı bir durum maddede bulunmamaktadır. Şüpheli bu talep hakkı konusunda bilgilendirilmemişse talep sonra da yapılabilir. Bilgilendirilmenin yapılmamış olması uygulanan tedbirin hukuka aykırılığını etkilemez. Talebin sonradan yapılması ihtimaline karşılık yedekten bir kopya daha çıkarılmalıdır.

Bilgisayardaki bulunan bilgiler kişinin örneğin iş yaşamı bakımından hayati derecede önemli olabilirler. Talep edilmesi halinde yedeğin bir kopyasının çıkarılması kişinin tedbirin ağırlığından daha az etkilenmesi açısından olumlu bir düzenlemedir. Buna karşılık bir bilişim suçu iddiasıyla hakkında soruşturma başlatılmış bir bilgisayar korsanına bu yedeğin verilmesi, üzerinde düşünülmesi gereken bir konudur[402]. Bir görüşe göre iadenin şüphelinin bilgisayarındaki verilere ihtiyaç duyabilmesi veya şirketin ticari işlerini sürdürmesinin sağlanması amacıyla gerçekleştirilmesi

[400] Centel, Zafer, **a.g.e.**, s. 380.
[401] Taşkın, **a.g.e.**, s. 204.
[402] Ünver, Hakeri, **a.g.e.**, s. 424.

mümkünse de şüphelide suç eşyası niteliğindeki verilerin bulunması durumunda verilerin kişiye iade edilmemesi gerekir[403]. Bu durumda suç eşyası durumunda olan eşyaların geri verilmesi söz konusu olmadığı gibi örneğin şüphelide bulunan başka kişilerin kredi kartı bilgileri ve çocuk pornografisi görüntüleri de iade edilmeyecektir[404]. Fikrimizce bu gibi hallerde geri verme kopya üzerinden olmalı ve orijinal birim elde tutulmalıdır. Bununla ilgili olarak bir kopyası verilecekse suçla ilgili veriler silinerek verilebilir. Silinen veriler ayrı bir tutanakta belirtilmelidir. Söz konusu verilerin silinerek iadenin gerçekleşmesi şüphelinin en az mağdur olacak şekilde tedbirin uygulanmasına hizmet edecektir.

Söz konusu fıkradaki yedekten bir kopya çıkarılıp şüpheliye veya vekiline verme talebinin tutanağa geçirilmesi ve imza altına alınmasının amacı elde edilen delilin, hukuka aykırılık iddiasını çürütmektir. Olay yerinde yedekten bir kopya çıkarılması mümkün olmayabilir. Bu nedenle şüphelinin veya vekilin talebi tutanağa geçirilmelidir. Talep, kolluğa veya adli bilişim uzmanlarına derhal yedekten bir kopya çıkarması ve vermesi yükümlülüğünü yükleyecektir. Buna ek olarak adli bilişim analizlerine başlanmadan önce talep yerine getirilmelidir ki hukuka aykırılık iddiasının önüne geçilebilsin. Talebin yerine getirilmemesi halinde bilgisayardan elde edilen deliller hukuka aykırı olmasalar bile bunlar üzerinde hukuka aykırılık şüphesi doğacaktır.

Fıkrada belirtilen vekil kavramının ilk bakışta şüpheli bakımından uygun olmadığı akla gelmektedir. Buna göre maddede şüpheli kavramına yer veriliyorsa CMK'nın "Tanımlar" başlığı altında düzenlenen 2. maddesinin 1/c'deki müdafii[405] kavramının burada yer alması gerekirdi. Ayrıca fıkrada geçen vekil kavramı ise aynı fıkranın d bendinde tanımlanmıştır[406]. Buradan vekilin; katılan, suçtan zarar gören veya malen sorumlu kişiyi ceza

---

[403] Şen, **a.g.m.**, s. 378.
[404] Şen, **a.g.m.**, s. 379.
[405] CMK'nın 2. maddesinin 1. fıkrasının c bendi aynen,
"Müdafi: Şüpheli veya sanığın ceza muhakemesinde savunmasını yapan avukatı, ... ifade eder." şeklindedir.
[406] CMK'nın 2. maddesinin 1. fıkrasının d bendi aynen,
"*Vekil: Katılan, suçtan zarar gören veya malen sorumlu kişiyi ceza muhakemesinde temsil eden avukatı, ... ifade eder.*" şeklindedir.

muhakemesinde temsil eden avukatı olduğu ifade edilerek şüpheli veya sanığı kapsamadığı ileri sürülebilir[407]. Buna karşılık vekil kavramının kullanılmasında herhangi bir yanlışlık da bulunmamaktadır. Vekil burada olay yerinde şüpheliyi temsil eden kişi olarak anlaşılmalıdır. Bu husus müdafii veya vekilin olay yerinde şüpheliyi temsil etmesine engel değildir. Olay yerinde şüphelinin kullandığı bilgisayar bir başkasına ait olabilir ve şüpheli olay yerinde bulunmayabilir. Bu nedenle vekil kavramının yalnızca müdafi olarak anlaşılması olay yerindeki üçüncü kişinin herhangi bir talepte bulunmasına engel teşkil edebilir. Dar bir yorum yedekten bir kopya çıkarılmasını isteyememe sonucunu doğuracaktır. Bu nedenle vekil kavramının hem müdafii hem de onu temsil edecek herhangi bir kişi olarak algılanması gerekir. Bir çocuğun bile bir bilişim suçunu işleyebilecek durumda olduğu söylenebiliyorsa yedekten bir kopya çıkarılması talebini anne veya babası yapacaktır. Anne veya babası bulunmasa bile hali hazırda o evde bulunan bir kimsenin bu talebi yapmasında herhangi bir sakınca yoktur.

D- TESADÜFEN ELDE EDİLEN DELİLLERİN AKIBETİ

Bir bilgisayardaki bütün verilerin incelemeye açık olması kişinin bütün sırlarının ortaya çıkması anlamına gelmektedir. Arama kararına dayanarak uygulanacak tedbirler iddia edilen suç şüphesiyle bağlantılı olmalıdır. Arama kararında aramanın nedenini oluşturan fiil belirtilmek zorundadır (CMK md. 119). İddia edilen fill belirtilmezse yapılan arama hukuka aykırılıkla karşılaşır. Karşılaştırmalı hukukta (özellikle Amerikan hukukunda) bununla ilgili mahkeme kararları mevcuttur. Şüpheli veya sanıkla ilgili olan herşeyin bilgisayarlarda bulunması nedeniyle tedbirler işletilirken soruşturma konusu suç ile sınırlı tutulmasına dikkat edilmelidir. Böylece temel hak ve özgürlüklere nispeten daha az müdahale edilecektir. Aramanın nedenini oluşturan fiil dışında başka bir fiilden ötürü arama yapılması halinde arama

[407] "*CMK 134/4'de yer verilen "vekil" kavramını "müdafi" olarak anlamak gerekir*." (Baştürk, **a.g.m.**, s. 31).

tedbiri genişletilmiş olacaktır. Böyle bir genişletme hukuka aykırıdır. Bundan dolayı elde edilen deliller de hukuka aykırı olacaktır.

Tesadüfen elde edilen deliller başlığı altında düzenlenen CMK'nın 138. maddesinin 1. fıkrası arama ve elkoyma yapılırken ilgili soruşturma ve kovuşturma dışında diğer bir suçun işlendiği şüphesini uyandırabilecek delillerin elde edilmesini konu edinmiştir. Bu hüküm genel arama ve elkoyma hükümlerinin uygulanması sonucunda elde edilen delillerle ilgilidir.

Tesadüfen elde edilen deliller genel arama ve elkoyma hükümlerinin icrası evresinde elde edilmişse bu delillerin kullanımı hakkında herhangi bir sınırlama mevcut değilken; (yani her suç bakımından kullanılabilirken) iletişimin denetlenmesi tedbirleri sırasında elde edilen delillerin kullanımının sadece katalog suçlarla sınırlı olduğu açık bir şekilde düzenlenmiştir[408](CMK md. 138/2). Avrupa İnsan Hakları Mahkemesi kararlarında söz konusu olduğu üzere telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbirine "*ancak demokratik kurumları korumak bakımından mutlak zorunluluk*" bulunması şartıyla başvurulması gerektiğinden, bu tedbire konu olacak suçların tahdidi bir şekilde sayılması zorunluluk arzetmektedir[409]. Suçların tahdidi bir şekilde sayılması bu katalog suç kapsamına girmeyen suçlarda bu tedbirlerin işletilemeyeceğini göstermektedir (CMK md. 135/6). Bununla birlikte iletişimin denetlenmesi tedbirleri uygulanırken katalog suçlar kapsamında bir suç delili elde edildiğinde bu delil derhal muhafaza altına alınır ve durum Cumhuriyet savcılığına bildirilecektir (CMK md. 138/2). Katalog suçlar kapsamında girmeyen bir suç tesadüfen elde edilirse bu delilin değerlendirilip değerlendirilmeyeceğine ilişkin kanunda bir hüküm yoktur[410]. Ancak katalog suçlar dışında bir suçun delilleri iletişimin denetlenmesi tedbirleri sırasında tesadüfen elde edilmişse bu deliller kullanılmayacaktır. Aksi halde CMK md. 138/2 hükmü işlevini kaybedecektir. Dolayısıyla

[408] Ünver, Hakeri, **a.g.e.**, s. 455.
[409] Öztürk, Erdem, **a.g.e.**, s. 644, 645.
[410] Centel, Zafer, **a.g.e.**, s. 412.

hakkında tedbir uygulanması mümkün olmayan suçların ortaya çıkarılması amacıyla tedbirin kötüye kullanılması ihtimali doğacaktır[411].

CMK'nın 138. maddesi hükümleri ele alındığında bilgisayarlara yönelik tedbirlerin işletilmesi sırasında başka bir suçun işlendiğine ilişkin bir delilin tesadüfen bulunması sırasında bu delillin akıbetinin ne olacağı sorusu akla gelmektedir. CMK'nın 134. maddesinde katalog suçlara ilişkin özel bir düzenleme bulunmamaktadır. Tedbirler her suç tipi bakımından uygulanabilir. Temel hak ve özgürlüklere müdahalenin sınırlı olmasından bahisle katalog suçlar gibi özel bir düzenlemenin getirilmesi gerektiği savunulabilir. Bu sayede temel hak ve özgürlüklere müdahale belirli suçlarla bağlantılı olarak yapılacaktır.

CMK'nın 134. maddesinde katalog suçların öngörülmemesi ve bu düzenlemenin genel arama ve elkoymanın özel bir halini oluşturması nedeniyle CMK md.138/1 hükmü uygulama alanı bulacaktır. CMK md. 138/2 hükmünün uygulanabilmesi için tedbiri düzenleyen maddede katalog suçların öngörülmesi gerekmektedir. Tesadüfen elde edilen deliller konusuna dikkatli bir şekilde yaklaşılmalıdır. Öncelikle arama sırasında soruşturulan suç dışına çıkılmamalıdır. Şüphelinin bilgisayarı üzerinde soruşturmaya konu olan suçla ilgili bir arama sırasında başka bir suçun işlendiğini gösteren deliller tespit edilmiş olup bu delillerin tamamı kopyalanıyorsa, arama kararında bahsedilen fiilin dışına çıkılmış olacaktır. Bu halde soruşturma konusu suç bahane edilerek başka suçlarla ilgili delil aramasına olanak sağlanır ki bu durum, maddede öngörülen bir suç soruşturmasının varlığı şartına aykırılık teşkil edecektir. Yalnızca elde edilen suç delillerin arasında başka bir suçun işlendiğine ilişkin bir bilgi varsa bu delil değerlendirilmelidir. 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. Sınırlı ve

[411] Öztürk, Erdem, **a.g.e.**, s. 648.

ölçülü bir şekilde uygulama yapılamadığı takdirde tedbir suç soruşturması dışında kayacaktır ki bu durum hukuka aykırılıkla karşılaşacaktır.

E- BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA, KOPYALAMA VE ELKOYMAYA SON VERİLMESİ VE VERİLERİN YOK EDİLMESİ

Bilgisayarda delil bulunamadığı takdirde arama son bulmamalıdır[412]. Diğer veri saklama birimleri üzerinde arama devam etmelidir. Arama sonucunda soruşturulan suçla ilgili herhangi bir delil bulunamadığı takdirde bu durum arama tutanağında belirtilecektir. Bilgisayarlardan şüpheyi haklı kılacak bir delil elde edilmemişse CMK'nın 121. maddesindeki hükümler gereğince bu durumu belirten belge, tedbirlere maruz kalan kişiye talep üzerine verilecektir. Delil bulunduğu takdirde bir kopyası çıkarılır, çözülerek metin haline getirilir ve savcıya veya mahkemeye sunulur. İddia edilen suçla ilgili yeterli delile ulaşılmışsa arama bitirilmelidir.

Elde edilen delillerin hukuka aykırı olmaması için uygulanan tüm metod ve işlemler mutlaka kayda geçirilmelidir[413]. Kayıtlar arama tutanağına ek olarak yer almalıdır. Bu metod ve işlemlerin kaydedilmemesi söz konusu olursa uygulanan metodların yanlışlığı ve buna bağlı olarak elde edilen delillerin hukuka aykırılığı ileri sürülebilir. Bundan ayrı olarak elde edilen delillerin bütünlüğü bozulursa veya veriler ceza muhakemesindeki delilin özelliklerini taşımazlarsa mahkeme bunları delil olarak kabul etmeyecek ve bu veriler belirti niteliğinde kalacaktır. Tedbirlerin sonunda hazırlanacak olan rapor, bu tür iddiaları çüretecek nitelikte olmalı; delillerin doğruluğunu yüzde yüze yakın bir şekilde ispatlamalıdır.

Bilgisayarlara ve veri saklama birimlerine elkoyma tedbirinin uygulanmasından sonra şifre çözümünün yapılması ve gerekli kayıtların alınması gerçekleştirilmişse elkonulan birimlerin iadesi gecikmeksizin

---

[412] Karagülmez, **a.g.e.**, s. 302.
[413] Aktepe, **a.g.m.**, s. 68.

yapılmalıdır (CMK md. 134/2). İlgili hüküm koruma tedbirlerinin geçici olma özelliğine uygun bir şekilde düzenlenmiştir. Ancak veri kapasitesinin büyük olduğu hallerde inceleme uzun sürebilmektedir.

Savcının kovuşturmaya yer olmadığına ilişkin kararında verilerin akıbetinin ne olacağı sorusu akla gelmektedir. CMK'ın 134. maddesinde elde edilen kişisel verilerin yok edilmesiyle ilgili bir hüküm yoktur. AK-SSS'nin "Kararların Yerine Getirilmesi İletişim İçeriklerinin Yok Edilmesi" başlığı altında düzenlenen CMK'nın 137. maddesinin 3. fıkrası sadece telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbirleriyle ilgili bir düzenlemedir. Ancak burada temel hak ve hürriyetlerin önemi gözetilerek şüphelinin lehine olacak şekilde kıyasın işletilebilmesi mümkündür. Ayrıca yeni yürürlülüğe giren anayasa değişikliğince kişisel verilerin korunması temel hak ve özgürlükler alanında önemli bir yer tutmaktadır (Anayasa md. 20/3). Kişi, bu değişikliğe göre kendisiyle ilgili verilerin silinmesi konusunda başvuruda bulunabilecektir. Bu nedenle CMK'nın 137. maddesinin 3. fıkrasındaki elde edilen verilerin yok edilmesiyle ilgili olan hüküm kıyasen işletilmelidir. Bu bakımdan kovuşturmaya yer olmadığı dair karar verilmesi halinde bilgisayardan elde edilen veriler Cumhuriyet savcısının denetimi altında on gün içinde yok edilecek ve bu durum bir tutanakla tespit edilecektir. Bunun yanında kişisel verilerle ilgili anayasada bulunan hüküm uyarınca elde edilen verilerin yok edildiğini belirten tutanağın bir örneği kişiye bildirme amaçlı olarak verilmelidir. Elde edilen veriler veya kopyalar yok edilmezse TCK'nın 138. maddesindeki verileri yok etmeme suçu oluşacaktır.

AK-SSS'nin 19. maddesinin 7. paragrafı verilerin erişilmez kılınmasını ve silinmesini düzenlemektedir. Bu konuyla ilgili olarak memorandumun 198. maddesi "*verileri erişilmez kılmak*" ibaresini verilerin şifrelenmesini ya da başka bir biçimde teknolojik olarak kimsenin verilere erişememesini sağlama olarak açıklamaktadır. Söz konusu 198. maddede virüs veya bomba imalatıyla ilgili bilgiler gibi toplumsal zarar ve tehlikenin söz konusu olduğu ya da çocuk pronografisi gibi verilerin ya da içeriklerin kanun dışı olduğu durumlarda verileri erişilmez kılmanın veya silmenin yararlı olacağı

vurgulanmıştır. CMK'nın 134. maddesi yargılama sonucunda bu tür durumlarda nasıl bir uygulama yapılacağı konusunda bir hüküm içermemektedir. Bu verilerin erişilmez kılınması veya silinmesiyle ilgili bir hüküm SEY'de de bulunmamaktadır. Sadece verilerin saklanmasıyla ilgili SEY'in md. 9/2 hükümü mevcuttur. Bu nedenle bahsedilen verilerle ilgili olarak kanuna veya yönetmeliğe özel bir düzenleme getirilebilir.

F- BİLGİSAYARLARDA, BİLGİSAYAR PROGRAMLARINDA VE KÜTÜKLERİNDE ARAMA, KOPYALAMA VE ELKOYMANIN UYGULANMASINA KARŞI BAŞVURU YOLLARI

Arama, kopyalama ve elkoyma kararları bir hâkim kararı olduğuna göre bu karara karşı CMK'nın 267. maddesi gereğince itiraz yapılabilecektir. İtiraz süresi kanunun 35. maddesinin 2. fıkrasındaki esaslar dâhilinde işlemeye başlayacaktır. Bu itibarla şüpheliye herhangi bir tebliğ yapılmasına gerek yoktur.

Bilgisayarlara elkoyma uygulandığı takdirde bu konuda başka bir hukuki yol CMK'nın 127. maddesinin 4. fıkrasında belirtilmiştir. Bu fıkraya göre eşyasına elkonulan kişi, hâkimden bu konuda, yani elkoymanın gerekli olup olmadığı konusunda karar verilmesini her zaman talep edebilmektedir. Bu konudaki kararı; soruşturma aşamasında elkoymanın uygulandığı yerdeki sulh ceza hâkimi, kovuşturma aşamasında kamu davasına bakan mahkeme verecektir[414]. Hâkim veya mahkeme, bilgisayar üzerindeki incelemenin sona erip ermediğini kolluğa ya da bilirkişiye sorabilir.

CMK'nın 131. maddesinin 1. fıkrası elkonulan eşyanın iadesini düzenlemektedir. Fıkraya göre şüpheliye, sanığa veya üçüncü şahıslara ait olup elkonulmuş eşya iade edilebilir. Bunun için eşyanın soruşturma ve kovuşturmada muhafazasına gerek kalmaması veya müsadereye tabi olmadığının anlaşılması gerekir. Başka bir ifadeyle, elkoymanın amaçlarına ulaşılamayacaksa, ispat açısından herhangi bir yarar yoksa, müsadere

[414] Şahin, **a.g.e.**, s. 252.

yapılamayacaksa, elkonulan eşya iade edilecektir[415]. İade re'sen veya talep üzerine yapılır. İade, soruşturmada Cumhuriyet savcısı veya sulh ceza hakimi; kovuşturmada ise mahkeme tarafından verilecek bir karar üzerinde gerçekleşecektir. İade kararı kesin olduğundan buna yönelik bir itiraz edilemez[416]. Lâkin iade talebinin reddi kararlarına itiraz edilebilir (CMK md. 267 vd.). Bilgisayara elkoyma halinde şifrenin çözülmesi ve gerekli kopyaların alınması halinde elkonulan bilgisayarın gecikmeksizin geri verilmesi, zaten elkoymaya ihtiyaç kalmadığını göstermektedir. Fakat bu husus elkonulan eşyanın talep edilmesine engel değildir. Şayet iade talebi yapılmışsa ancak bilgisayarın şifresi çözülememişse ve gerekli kopyalar alınamamışsa bu talep reddedilebilecektir. CMK'nın 131. maddesinin 1. fıkrası elkonulan bilgisayarlar hakkında da uygulanabilir.

Elkonulan bilgisayarlar ve veri saklama birimleri bakımından ilk bakışta CMK'nın 132. maddesindeki elkonulan eşyanın muhafazası veya elden çıkarılması hükümleri uygulanabileceği öngörülebilir. Ancak bilgisayarlara elkoyma şifre çözümünün yapılması ve gerekli kopyaların alınmasıyla sona erecek ve elkonulan bilgisayar derhal geri verilecektir. Bu nedenle elden çıkarmaya gerek bulunmamaktadır. Sonuç olarak CMK'nın 132. maddesindeki hükümler 4. fıkra hariç olmak üzere; bilgisayarlar bakımından uygulanamayacaktır. Eğer SEY md. 9/2'de yer alan şartlara göre koruma altına alınan birimler birden fazlaysa ve bunların daha fazla tutulmaları zarar görebilme olasılıklarını arttırıyorsa iade için bütün birimlerin incelenmesi beklenmemelidir. İncelemesi tamamlanan birimler gecikme olmaksızın iade edilmelidir. Bu yorum koruma tedbirlerindeki ölçülülük ilkesine uygun düşmektedir.

Koruma tedbirlerinde hukuka uygun olmayan uygulamalar ve meydana gelen zararlar için tazminat hükümleri karşımıza çıkmaktadır. Ayrıca bilgisayarlar veya veri saklama birimleri arama, kopyalama ve elkoyma sırasında hem donanım hem de yazılım açısından zarar görmüşlerse (örneğin donanımda fiziki bir arıza varsa) veya programlar

[415] Özbek, **a.g.e.**, s. 489.
[416] Şahin, **a.g.e.**, s. 254.

çalışmıyorsa tazminat hükümlerine gidilebilmelidir. Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde yapılan arama, kopyalama ve elkoyma özel bir arama ve elkoyma türü olduğundan CMK'nın 141. maddesinde açık bir şekilde belirtilmese de maddedeki hükümlere uygun ölçüde meydana gelen zararı tazmin etme yoluna gidilebilir[417]. Elkonulan bilgisayarlar, sökülüp takılabilen donanımlar, veri saklama birimleri veya diğer elektronik cihazlar eksiksiz bir biçimde iade edilmelidir. Geri verilmeyen veya eksik iade edilen parçalar için CMK'nın 141. maddesinin 1. fıkrasının "j" bendindeki tazminat koşulları gündeme gelecektir[418].

CMK'nın 141. maddesinin 1. fıkrasının "i" bendinde arama kararının ölçüsüz olarak icra edilmesi bir tazminat nedeni olarak öngörüldüğü için ölçülülük ilkesinin önemi büyüktür. Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoymanın ölçülü yapılması gerektiği AİHM kararlarında da vurgulanmaktadır[419].

---

[417] Özbek, **a.g.e.**, s. 505.

[418] CMK'nın 141. maddesinin 1. fıkrasının j bendi aynen,
"…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." şeklindedir.

[419] "Smirnov vs. RUSYA";
"…Müşteki Smirnov bu davada Rus adli makamlarının ciddi suç tiplerinden ötürü suçladığı bir grup sanığı temsil eden bir avukattır. Arama kararı, dava soruşturmacısının bu nesnelerin ve belgelerin avukatın evinde olduğu konusunda şüphelenmesi üzerine, şikayetçinin evine suçla ilgili olarak nesneleri ve belgeleri aramak için verilmiştir. Avukat aramada hazır olduğu esnada birkaç belgeye ve bilgisayarına elkonulmuştur. Şikayetçi bilgisayara erişememesi nedeniyle, elkoymaya karşı çıkmıştır. Belgelere ve bilgisayara elkonulmasıyla elde edilenler, ceza davasında avukatın müvekkillerine karşı kullanılan fiziksel delillerin bir parçası haline gelmiştir. Daha sonra sözleşmenin bu maddesine (13. maddesi) uygun olarak müşteki evinde yapılan arama ve elkoymanın hukuka uygun olmadığı iddiasıyla yargısal bir karar için başvuru yapılmıştır. Müşteki belgelerinin ve bilgisayarlarının aranması ve elkonulmasının müvekkillerinin savunma hakkını ihlale uğrattığını da öne sürmüştür. Şikayetçinin başvurusundan sonra Rus yargısı bazı belgeleri ona geri vermiş ama bilgisayarı elinde tutmuştur. İlk derece mahkemesi şikayetçinin sözleşmenin 8. maddesi kapsamında arama ve elkoymanın hukuka aykırılığı iddiasını reddetmiştir. Mahkeme müştekinin evinde yapılan arama ve elkoymanın iç hukuka uygun olarak yapıldığına ve bilgisayar parçalarının yargısal denetime konu olmadığına hükmetmiştir. Temyizde ise ilk derece mahkemesinin kararı onanmıştır.
Bunu müteakiben Müşteki, Rus adli makamlarının, müvekkillerinin belgelerine ve kendi bilgisayarının arama ve elkoymasının özel hayatını ve mülkiyetten yararlanma hakkını Sözleşmenin 8. maddesine göre ihlal ettiğini ileri sürmüştür. Ayrıca yerel mahkemeler müştekinin sözleşmenin 13. maddesi kapsamında durumun düzeltilmesine yönelik başvurusunu da reddetmiştir.

CMK'nın 141. maddesinde öngörülen tazminat talebi maddi olabileceği gibi manevi de olabilir. Bu özel tedbirler 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.

AİHM sözleşmenin 13. maddesi madde kapsamında yurt içinde başvurulacak yolların reddedildiğini Rus adli makamları arafından yapılan arama ve elkoyma işleminin sözleşmenin 8. maddesini ihlal ettiğini hükmetmiştir.
Mahkeme kararını 3 önemli noktada açıklamaktadır.
1- Müştekiye ait olanlar üzerinde elkoymanın bireysel bina ve eklentilerde aramanın demokratik toplum düzeninde uygun olduğu; esas üzerinde arama izninin düzenlendiğine, iznin içeriğine ve kapsamına ve arama yapılacağına ilişkin usul, işiyle ilgili olması, bireyin etkilenen itibarı durum analizini gerektirir. Müştekinin davasında müşteki davanın konusu değildir ama onun müvekkillerinin eylemleri davaya konudurlar. Arama emri geniş ve belirsizdir ki bu da polise geniş bir yetki vermiştir. Emir, yargının yönetimine uygunluk için kritik bir öneme sahip olan avukatın evinde bulunan bir takım belgelerine, ilişkin mesleki muafiyetine yönelik herhangi bir tedbir içermemektedir. Bu nedenle şikayetçinin evinde yapılan arama; belgelerine ve bilgisayarlarına elkonulma demokratik toplumun gereklerine uygunluk bakımından uygun değildir. Bu nedenlerle Rusya sözleşmenin 8. maddesini ihlal etmiştir.
(Mahkeme Funke vs. Fransa (ECHR 10828/84); ve Niemietz vs. Almanya[1992] ECHR 13710/88. davasına atıfta bulunmuştur.).
2- Fiziki delillerin elde tutulmasıyla ilgili olarak AİHM toplumun yerel ilgisini ve yargı yönetiminin ilgisi bakımından bunun uygun olduğuna karar vermiştir. Yine de **kullanıma sokulmaması ve aramanın hedefi arasında makul ölçü ilişkisi** bulunmalıdır. Toplumun genel çıkarları ile bireysel insan hakları arasında bir denge olmalıdır. Bu davada müştekinin bilgisayarı, herhangi bir cezayı gerektiren bir suçun delili olarak addedilemez. Müştekinin bilgisayarının 6 günden daha uzun bir süre içerisinde alıkonulmasının bir nedeni yoktur. Bilgisayar müştekinin mesleğini ifa etmesi için bir araçtır ve elkoyma-müsadere onun mesleki faaliyetlerini bozmuştur. Bu sayede Rus adli makamları toplumun genel çıkarları ve avukatın hakları arasındaki adil dengeye müdahalede başarısız olmuştur ve yapılan işlem hukuka aykırıdır…" Bkz. "Home Searches and Computer Seizures Under the European Convention On Human Rights", 16.03.2009, Marta L. Arias, (Erişim) http://www.ibls.com/internet_law_news_portal_view.aspx?=slastestnews&id=2213, INTERNET LAW, 05 Nisan 2009; Ayrıca kararın orijinali için bkz. (erişim)http://cmiskp.echr.coe.int/tkp197/portal.asp?sessionId=39341604&skin=hudoc-en&action=request, 05 Nisan 2009.

IV- CMK'NIN 134. MADDESİNİN BİLİŞİM SUÇLARI ve 5651 SAYILI KANUN BAKIMLARINDAN UYGULANABİLİRLİĞİ

A- BİLİŞİM SUÇLARI BAKIMINDAN

Bilişim suçlarından ne anlaşılması gerektiği konusunda herhangi bir tanımlama yapılmamıştır. Doktrinde birden fazla tanım yapılmış olmasına rağmen üzerinde uzlaşmaya varılmış ortak bir tanımlama yoktur[420]. Teknolojinin sürekli gelişmesi bu tanımlamayı zorlaştırmaktadır. Ayrıca tanımlama arasındaki farklılıklar uluslararası sözleşmelerde de (AK-SSS'de de örneğin "cybercrime"-"siber suç" gibi) göze çarpmaktadır. Buna karşılık kısa bir tanımlama yapılacak olursa; bilişim suçu bilişim sistemine yönelik veya bilişim sisteminin araç olarak kullanıldığı bir suç tipidir[421].

TCK'nın Bilişim Alanında Suçlar başlığı altında düzenlenen bilişim sistemine girme (TCK md. 243), sistemi engelleme, bozma, verileri yok etme veya değiştirme (TCK md. 244), ve banka veya kredi kartlarının kötüye kullanılması suçları (TCK md 245) yapıları gereği diğer suç tiplerinden ayrıdır. Bilişim suçu dışındaki suç tiplerinde genellikle suçun sonucunun gerçekleştiği alana veya suçun mağduruna yönelik bir fiziki yakınlık mevcuttur[422]. Bilişim suçları ise "*uzaktan kumanda ile işlenebilen suçlar*" olarak tanımlanabilir ve birden fazla yerden işlenebilirler[423]. Verilerin kaybolmasının engellenmesi, korunması ve gözle görülebilmesi teknik bir bilgiyi gerektirmektedir. Öte yandan elektronik delil elde etmenin teknik cihaz ve aletlere bağlı olması ve bu nedenle delil elde edilmesinde bütünlüğün bozulmamasının önemli oluşu bilişim suçlarını diğer suç tiplerinden ayrı bir yere koymaktadır.

Diğer suçları delillendirmede teknik bir bilgiye ihtiyaç duyulduğu ileri sürülebilir. Fakat bilişim suçlarında soyut olarak bir bilişim alanı ve bilişim

---

[420] Ergün, **a.g.e.**, s. 12.
[421] Karagülmez, **a.g.e.**, s. 38.
[422] Ali Karagülmez, "Bilişim Suçlarında Delil Elde Etmeyi Etkileyen Başlıca Konular", (Erişim) http://www.caginpolisi.com.tr/46/7-8-9-10.htm - _ftn1, 09 Ocak 2009, s.3.
[423] Karagülmez, **a.g.m.**, s. 3.

sistemi vardır. Oysaki diğer suç tiplerinde somut bir durum söz konusu olup soyut bir alan yoktur.

Suçüstü hallerinde CMK'nın 90. maddesi gereğince "yakalama" koruma tedbirine başvurulabilir. Bilişim suçlarında yakalamanın uygulanmasına hukuken bir engel olmasa bile kendisine özgü yapısı gereği bunun imkânın bulunmadığı iddia edilmektedir[424]. Buna karşılık yakalama bilişim suçlarında da gerçekleşebilir. Şöyle ki; bankanın bilişim sistemine girmeye çalışan bir bilgisayar korsanın fiili tespit edildiği takdirde suçüstü halinden bahsedilecektir. Böylece failin bu fiilinden haberdar olan herhangi kişi, yakalama yetkilerini kullanabilecektir.

CMK'nın 134. maddesinin 1. fıkrasında yer alan "*bir suç dolayısıyla*" ibaresi kapsamına bilişim suçları da dâhildir. Bilgisayarlara yönelik tedbirler ile bilişim suçlarının özellikleri birlikte düşünüldüğünde sorunların ortaya çıktığı ileri sürülmektedir. Elektronik verilerin kaybolma tehlikesiyle karşılaşılmaması için bu tedbirlere derhal başvurulmalıdır. Başka surette delil elde etmemiş olmak şartı nedeniyle delillerin kaybolmasının gündeme gelebileceği ve arama işleminin istenen amaca ulaşamaycağı iddia edilmiştir[425]. Bilişim suçlarında ilk olarak şüphelinin kullandığı bilgisayarına bakılması gerekebilir[426]. Buna karşılık bilişim suçlarında bilgisayarda arama, kopyalama ve elkoymanın hemen yapılamaması delillere erişmeyi imkansız kılabilir. Buradaki görüşler çerçevesinde son çare ilkesinin yansıttığı durumlar bilişim suçlarının delillendirilmesinde yavaşlığa neden olacak; bilişim suçlarının soruşturulmasında ve maddi gerçeğe ulaşmada ciddi sorunlar getirecektir. Bu nedenle CMK'nın 134. maddesine bilişim suçlarıyla ilgili özel bir hüküm konulması gerektiği ifade edilmiştir[427].

Yukarıda ifade edildiği gibi başka surette delile elde etme imkanının bulunmaması şartı bir koruma tedbirinde yer almışsa bu husus tedbirin ikincil nitelikte olduğunu göstermektedir. Bu şartı içeren koruma tedbirlerinin temel hak ve özgürlüklere etkisi ağır olduğundan diğer koruma tedbirleri

---

[424] Karagülmez, **a.g.m.**, s. 3.
[425] Taşkın, **a.g.e.**, s. 171.
[426] Karagülmez, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, s. 287.
[427] Taşkın, **a.g.e.**, s. 171.; Aynı yönde bkz. Karagülmez, **a.g.e.**, s. 287.

uygulanmadan bu tedbirlere başvurulmamalıdır. Bununla birlikte temel hak ve özgürlüklere diğer tedbirlere oranla daha az müdahale eden genel arama ve elkoyma tedbirlerinin işletilmesi durumunda, amacın gerçekleşmeyeceği henüz tedbirlere başvuru yapılmadan öngörülmüşse ikincil olan tedbir öncelikli hale gelebilmektedir. Başka bir ifadeyle arama ve elkoyma uygulansa da delile ulaşılamayacağı önceden anlaşılmışsa, başka surette delil elde etme imkânının bulunmaması şartı gerçekleşmiş olacaktır. Bu itibarla bilişim suçlarında genel arama ve elkoyma hükümleri ile delil elde edilemeyeceği ilk bakışta anlaşıldığından CMK 134. maddesi hükümleri öncelikle uygulanacaktır. Neticede bilişim suçlarıyla ilgili olarak CMK'nın 134. maddesine özel bir düzenleme getirilmesine gerek bulunmamaktadır. İleri sürülen görüşler, başka surette delil elde etme imkanının bulunmaması şartını dar bir anlamla algılamaktadırlar.

Bilişim suçlarında arama, kopyalama ve elkoyma hükümleri derhal uygulanmalıdır. Her ne kadar suçtan zarar gören tüzel kişinin bilgisayarlarından delil elde edilmesiyle ilgili olsa da bir Yargıtay kararında bilişim suçlarında arama ve kopyalama tedbirlerinin değil; tedbire benzeyen işlemlerin derhal yapılması gerektiği belirtilmiş ve aynı zamanda üzerinde adli bilişim sürecindeki basamaklara atıfta bulunulmuştur[428].

Bilişim suçlarıyla mücadelede, yeni bilişim suçu tiplerini; bunların soruşturulmasını ve kovuşturulmasını düzenleyen ayrı bir kanuna ihtiyacın bulunup bulunmadığına yönelik bir tartışma vardır. Ortaya atılan görüşlerin çoğunluğunda bilişim suçlarının özel bir ceza kanunu olarak düzenlenmesi

---

[428] *"...öncelikle e-posta yolu ile virüs göndererek sistemine zarar verilmiş bir bilgisayarda incelemenin, olayın hemen akabinde yapılması ya da inceleme yapılacak bilgisayarın veya bilgisayara ait veri içeren ünitelerin, olaydan sonra inceleme yapılana kadar hiç kullanılmaması gerektiği, incelenecek bilgisayarın diskine bazı bilgilerin yazılması, değişmesi veya silinebilmesini önlemek ve söz konusu diskin bütünlüğünü sağlamak için bilgisayarda virüslü dosya üzerinde inceleme yaparken ilk işlem olarak, söz konusu dosyanın birebir (sector-by-sector) yedeğinin alınması (yani incelemenin orijinal dosya üzerinde yapılmaması), daha sonra ikinci olarak alınan birebir yedeğinin değiştirilip değiştirilmediğini tespite yarayacak zaman ve bütünlük kontrolü imkanı sağlayan değerin (hash) belirlenmesi, bir e-postanın kimden gedliğini tespiti içinde, ilk olarak e-postayı gönderen IP adresinin bulunması..."*. Yarg. 11. CD. 16.04.2007, 2005/6376E, 2007/2551K. (Malkoç, Yüksektepe, **a.g.e.**, s. 643, 644 vd..)

gerektiği savunulmuştur[429]. TCK'nın 5. maddesi genel ve özel kanun ilişkisini düzenlemiştir. Buna göre TCK'nın genel hükümleri özel nitelikteki diğer ceza kanunları ve ceza içeren kanunlardaki suçlar bakımından uygulanacaktır. Maddenin gerekçesi: "*Özel ceza kanunlarında ve ceza içeren kanunlarda suç tanımlarına yer verilmesinin yanı sıra, çoğu zaman örneğin teşebbüs, iştirak ve içtima gibi konularda da bu Kanunda benimsenen ilkelerle çelişen hükümlere yer verilmektedir. Böylece, ceza kanununda benimsenen genel kurallara aykırı uygulamaların yolu açılmakta ve temel ilkeler dolanılmaktadır. Tüm bu sakıncaların önüne geçebilmek bakımından, ayrıca hukuk uygulamasında birliği sağlamak ve hukuk güvenliğini sağlamak için; diğer kanunlarda sadece özel suç tanımlarına yer verilmesi ve bu suçlarla ilgili yaptırımların belirlenmesi ile yetinilmelidir. …*" şeklindedir. Böylelikle özel bir ceza kanunun getirilmesi TCK'daki genel hülümleri kısmında bulunan temel ilkelerin dolanılması potansiyelini taşımaktadır. Bununla birlikte "Bilişim Alanında Suçlar" TCK'nın özel hükümler kısmındadır. Şayet mevcut ve yeni suç tipleriyle ilgili düzenleme yapılacaksa bu "Bilişim Suçlarıyla Mücadele Kanunu" gibi özel bir kanun ile değil; TCK'daki Bilişim Alanında Suçlar" başlığı altında ek maddeler getirilerek yapılmaldır. Bu suçların soruşturulması ve kovuşturulmasına ilişkin usul hükümleri de özel bir kanunla düzenlenmemelidir. CMK'nın 134. maddesine ek fıkralar konulabilir veya ayrı bir madde şeklinde çeşitli düzenlemeler yapılabilir.

B- 5651 SAYILI KANUN BAKIMINDAN

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun; içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı ve toplu kullanım sağlayıcılarının sorumluluklarını belirlemek ve internet ortamında işlenen belirli suçlarla ilgili mücadelede ele alınan esas ve usulleri hüküm altına almak amacıyla düzenlenmiştir (md.1).

---

[429] Taşkın **a.g.e.**, s. 207.; Aynı yönde bkz. Karagülmez, **a.g.e.**, s. 391.

Bu kanunda yalnızca yukarıda bahsedilen internet süjelerle ilgili düzenlemeler yer almamaktadır. Ayrıca yayınlarla ilgili olarak bir takım özel koruma ve idari tedbirler bu kanunda öngörülmüştür.

Erişimin engellenmesi hem koruma tedbiridir hem de idari bir tedbirdir (md. 8). İnternet ortamında yapılan ve içeriği kanunda belirtilen suçları oluşturduğu hususunda yeterli bir şüphe varsa yayınlarla ilgili erişimin engellenmesi kararı verilecektir. Katalog suç olarak da adlandırılan bu belirli suçlar kanunun 8. maddesinin 1. fıkrasında düzenlenmiştir[430]. Söz konusu 8. maddeden ve kanunun genel gerekçesinden anlaşıldığı üzere erişimin engellenmesi kararının katalog suçlar dışında uygulanamayağı sonucuna varılmaktadır[431]. Lakin uygulamada katalog suçlar haricinde de erişimin engellenmesi kararlarına hükmedilebilmektedir[432]. Bu hal katalog suçların getirilme amacını Erişimin engellenmesi kararını soruşturma aşamasında hakim, kovuşturma aşamasında ise mahkeme verecektir. Soruşturma aşamasında gecikmesinde sakınca bulunan hal kapsamında erişimin engellenmesi kararını Cumhuriyet savcısı verecektir. Cumhuriyet savcısı kararını yirmidört saat içerisinde hakimin onayına sunacaktır. Bu durumda hakim, en geç yirmidört saat içerisinde kararını verecektir. Erişimin engellenmesi kararları derhal ve engeç kararın bildirilmesi anından itibaren yirmidört saat içerisinde yürürlülüğe konulacaktır. Erişimin engellenmesi kararlarının icrasında Telekomünikasyon İletişim Başkanlığı merkezi bir birim olarak görev yapmaktadır[433]. Erişimin engellenmesi kararlarına karşı CMK hükümlerince itiraz yolu işletilebilir.

---

[430] Bu suç tipleri şunlardır: 5237 sayılı TCK'da yer alan, İntihara yönlendirme (TCK md. 84), çocukların cinsel istismarı (TCK md. 103/1), uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (TCK md. 190), sağlık için tehlikeli madde temini (TCK md. 194), müstehcenlik (TCK md. 226), fuhuş (TCK md. 227), kumar oynanması için yer ve imkân sağlama (TCK md. 228) ve 25.07.1951 tarihli 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.

[431] Necati Meran, "İnternet Yoluyla İşlenen Suçlarda Erişimin Engellenmesi ve İçeriğin Yayından Çıkarılması", **Terazi Aylık Hukuk Dergisi**, Yıl: 5, Sayı: 47, Ankara, Temmuz 2010, s. 121.

[432] Doğan Kılınç, "Türk Hukukunda ve Mukayeseli Hukukta İnternet Sitelerine Erişimin Engellenmesi ve İfade Hürriyeti", **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: XIV, Yıl: 2010, Sayı: 2, Ankara, Aralık 2010, s. 411.

[433] Kılınç, **a.g.m.**, s. 412.

5651 sayılı kanunun 5. maddesinin 1. ve 2. fıkrası yer sağlayıcıların sorumluluklarını düzenlemiştir. İlk fıkraya göre yer sağlayıcılar içeriği kontrol etme veya hukuka aykırı bir faaliyetin gerçekleşip gerçekleşmediğini araştırmakla yükümlü değildirler. İkinci fıkraya göre yer sağlayıcının, hukuka aykırı içerik nedeniyle erişimin engellenmesi (md. 8) ve içeriğin yayından çıkarılması ve cevap hakkı (md.9) hükümlerine göre haberdar edilmesi durumunda ve teknik açıdan imkanları ölçüsünde yayından kaldırması bir yükümlülük olarak öngörülmüştür. Öte yandan yer sağlayıcı, Telekomünikasyon İletişim Başkanlığı tarafından kendilerine iletilen kararları teknik olarak uygulamaya koymaktadır[434].

Söz konusu fıkraya göre ceza hukuku sorumluluğu saklıdır. Böylelikle konusu suç oluşturan içeriği barındıran sistemi, suç failiyle birlikte suçun işlenmesi için kasten kullanıma sunan ve işleten yer sağlayıcı, suça iştirak hükümleri bakımından sorumlu tutulacaktır[435].

Konusu suç teşkil eden hukuka aykırı bir içerik yer sağlayıcıların bilgisayarlarında, veri tabanlarında veya kütüklerinde bulunabilir. 5651 sayılı kanun erişimin engellenmesi koruma tedbirini düzenlemektedir. Erişimin engellenmesi kararı ile sadece içeriğin yayınlandığı siteye erişim kısıtlanmaktadır. Ancak içerik, yer sağlayıcının kütüklerinde bulunmaya devam etmektedir. Öte yandan suç teşkil eden içerik şüpheli tarafından yer sağlayıcısını aracı kullanılarak da yayınlanabilir. Bu durumda içerik hem şüphelinin bilgisayarında hem de yer sağlayıcının donanımında bulunabilmektedir. Şüphelinin daha sonra kendi bilgisayarından bu içeriği yok ettiği veya sildiği düşünülürse yer sağlayıcısındaki verilerin delil olarak elde edilip edilemeyeceği sorunu ortaya çıkmaktadır. Şayet bu verilerden delil edilecekse hangi koruma tedbirlerinin uygulanacağı konusunda açık bir düzenleme bulunmamaktadır. İlk bakışta CMK'nın 134. maddesindeki tedbirlerin uygulanabileceği gündeme gelmektedir. Fakat CMK'nın 134. maddesindeki düzenlemeler şüphelinin kullandığı bilgisayar, bilgisayar programı ve kütükleriyle sınırlıdır. Burada şüphelinin içeriği yayınlamasıyla

[434] Kılınç, **a.g.m.**, s. 412.
[435] Meran, **a.g.m.**, s. 120.

yer sağlayıcının kütüklerini uzaktan da olsa kullandığı iddia edilebilir. Şüphelinin kütükleri uzaktan kullanması CMK'nın 134. maddedeki aranan fiili kullanımın kapsamına girmekte olup olmadığının belirlenmesi gerekmektedir.

AK-SSS'nin 19. maddesinin 3. paragrafında bilgisayarlarda yapılan arama kapsamının, kendi ulusal sınırları içerisinde başka bir bilgisayar sisteminde veya bu sistemin bir kısımına yönelecek şekilde genişletilebileceğini öngören bir hüküm mevcuttur. Arama kapsamının genişletilmesi için sözleşmeye taraf ülkelerin gerekli yasama işlemlerini yapması gerekecektir. AK-SSS'nin 22. maddesi ise içerikle ilgili bilgilere müdahale edilmesini ele alan hükümlere yer vermiştir. Buna göre taraf ülkeler kanunla belirtilen ciddi suç tipleriyle ilgili olarak içerikte bulunan bilgilerin gerçek zamanlı olarak toplanma ve kaydedilme yetkilerini öngören yasama işlemlerini gerçekleştireceklerdir. Bahsi geçen maddenin 2. paragrafı herhangi bir hizmet sağlayıcının, mevcut teknik imkanlar çerçevesinde içerikle ilgili (ciddi suç tipleriyle ilgili) bilgileri gerçek zamanlı olarak, ilgili tarafın ulusal sınırları içinde bulunan teknik imkanların kullanılması suretiyle toplaması ya da kaydetmesi hakkında bir düzenlemenin yer alması gerektiğini belirtmektedir. Maddenin 3. paragrafı ise içerikle ilgili bilgilerin gerçek zamanlı olarak toplanması ya da kaydedilmesi konusunda yetkili mercilerle işbirliği yapılmasını ve onlara bu konuda yardımcı olunmasını öngören düzenlemelerin ortaya konulmasını belirtmektedir.

Hukukumuzda ise yer sağlayıcıların suç soruşturması kapsamında içerikle ilgili yetkili mercilerle bilgi paylaşımını öngören bir düzenleme bulunmamaktadır. Özel bir düzenleme olmadığından Cumhuriyet savcısının CMK'nın 160. ve 161. maddelerindeki yetkilerini kullanarak yer sağlayıcıdan bilgi isteyebileceği akla gelmektedir. Ancak yer sağlayıcıların sakladıkları bilgilerin kişilerin sırlarını içeren bilgilerle yüklü olması tabiidir. Ayrıca bu kütüklerde sadece şüphelinin kullandığı içerik değil; diğer kişilerinde içerikleri bulunmaktadır.

CMK'nın 134. maddesinde aramanın nasıl genişletileceğine dair bir hüküm mevcut değildir. Sadece AÖAY'nin 17. maddesinin 3. fıkrasında

yedekleme işleminin bilgisayar ağları ve diğer uzak bilgisayarlar kütükleri bakımından uygulanabileceğini gösteren bir hüküm vardır. Şüphelinin kullandığı bilgisayar, bir bilgisayar ağı sisteminin bir parçası olabilmektedir. Keza bu bilgisayar diğer uzak bilgisayar kütükleri ile bağlantı kurabilmektedir. Özetle AÖAY'nin 17. maddesindeki bu hükümden sadece yedekleme işlemi anlaşılıyorsa bu cihazlar üzerinde arama genişletilmeyecek sadece sistem güvenliğinin korunması bakımından bir yedek alınacaktır. Söz konusu yedekleme işlemi de sadece incelenen bilgisayar çevresindeki ağ bilgisayarları ve kütükleriyle sınırlıdır. Buna karşılık yönetmelik hükmünden yalnızca yedekleme işlemi anlaşılmayıp arama işlemi de anlaşılabilir. Böylelikle aramanın kapsamı genişletilmektedir.

Kanımızca CMK'nın 134. maddesindeki "şüphelinin kullandığı bilgisayar" ifadesinden dar anlamda bir bilgisayar kullanımı anlaşılmaktadır. Şüpheli burada kullandığı bilgisayarla sınırlı olarak işlem yapmaktadır. Yani diğer bilgisayar kütüklerine uzaktan erişimle bir işlem gerçekleştirilmemektedir. Buna ek olarak AK-SSS'deki arama kapsamının genişletilmesine ilişkin özel bir hüküm CMK'da bulunmamaktadır. Özel bir düzenlemenin yer almaması nedeniyle AÖAY'nin md. 17/3'teki ifadeyi sadece yedekleme işlemiyle sınırlı tutmak gerekmektedir[436]. 5651 sayılı kanun kapsamındaki şüpheli tarafından hazılanan içeriğin yer sağlayıcıları vasıtasıyla yayınlanması geniş anlamda kullanımayı ifade etmektedir. CMK'nın 134. maddesi uygulanarak yer sağlayıcıların kütüklerinde arama yapılması diğer kişilerin temel hak ve özgürlüklerine ölçüsüz müdahaleye neden olacakır. Bu nedenle CMK'nın 134. maddesi, şüphelinin geniş anlamda kullanımından hareketle yer sağlayıcının donanımları ve veri saklayan kütükleri üzerinde teşmil edilemez. Buna karşılık yer sağlayıcının kütükleri dar anlamda bir suçta kullanılmışsa diğer bir ifadeyle şüpheli bu kütükleri herhangi bir vasıtaya gerek duymadan kullanıyorsa ve bu durum tespit ediliyorsa CMK'nın 134. maddesindeki hükümler işletilebilir.

---

[436] Şayet yönetmelikteki bu hükümden arama kapsamı belirlenecekse kanımızca yanlızca incelenen bilgisayar çevresindeki ağ bilgisayarları veya kütükleri ile bir sınırlamaya gidilmelidir. Geniş kapsamda düşünebilmek için kanuna özel bir düzenleme getirilmesi şarttır.

V- DEĞERLENDİRME

A- ADLİ BİLİŞİM SÜRECİ BAKIMINDAN

Adli bilişim süreciyle bilgisayarlardan veya veri saklama birimlerinden elde edilen elektronik veriler, çözülerek anlaşılır bir biçimde birer delil haline getirilirler. Verinin kaynağı, ne zaman bilgisayara indirildiği, üzerinde değişiklik yapılıp yapılmadığı, yapıldıysa ne zaman yapıldığı vb. gibi soruşturmaya etki edebilecek hususlar adli bilişim süreciyle belirlenmektedir.

CMK'nın 134. maddesinin ilk fıkrasından, doğrudan doğruya şüphelinin kullandığı bilgisayardan delil elde edilmesi gerektiği anlaşılmaktadır. Adli bilişim sürecinde ise, şüphelinin kullandığı bilgisayara mümkün olduğu kadar az müdahale edilmesi, yedeğinin çıkarılması ve elde edilen yedek üzerinden delil aramasının yapılması esastır. Bu bahisle maddenin ilk fıkrasındaki hükmün adli bilişim süreciyle uyumlu olmadığı iddia edilmektedir. Kanaatimizce her olayda adli bilişim sürecinin uygulanması şart değildir. Elde edilen delilin güvenilirliği, basit bir teknik inceleme sonucunda da kanıtlanabilir.

Kanun, niteliği gereği genel ve soyut olmalıdır. Teknik bilgi gerektiren hususların kanunda yer alması, onun niteliğini donuklaştırmaktadır. Bu açıdan teknik bilgi gerektiren işlemlerin AÖAY'nde veya sadece adli bilişim süreçlerini düzenleyen bir yönetmelikte yer alması gündeme gelebilir. Ancak adli bilişim süreçleri ve bu süreç içerisinde incelenen modeller sürekli olarak güncellenmektedir. Buna uygun yönetmelikler çıkarılsa da yönetmeliklerin sık sık değiştirilmesi sorunu gündeme gelebilmektedir. Bu gibi sorunlarla karşılaşılmaması için bilgisayardan delil elde etmeye yönelik pratik ihtiyaçlar için bir takım kurallar oluşturulabilir. Örneğin; İngiltere'deki polisin adli bilişimde kullandığı "Bilgisayar Temelli Elektronik Deliller İçin İyi Pratik Rehberi"'ndeki gibi kurallar örnek alınarak kendi hukukumuza uygun rehber kurallar hazırlanabilir.

Elektronik verilerin korunması; adli bilişim alanındaki gelişmelere, delil bütünlüğüne ve maddi gerçeğin ortaya çıkarılmasına hizmet edecektir. Nitekim SEY'nin 9. maddesinin 2. fıkrasında böyle bir düzenlenmenin yer alması adli bilişim süreci açısından olumlu olarak addedilebilir. Gerekli ortamların hazırlanmasıyla özellikle kişilere ait cihazların ve içindeki verilerin muhafaza edilmesinin başta mülkiyet hakkı olmak üzere, kişisel veriler ve diğer temel hak ve özgürlüklerin korunması açısından önemi büyüktür.

Bilirkişilik alanında adli bilişim uzmanları ile diğer bilgisayar uzmanları arasında yaklaşım farklılığı ortaya çıkmaktadır. Adli bilişim uzmanları kendi alanlarıyla ilgili hukuki bilgiye sahip olup dünyaca kabul gören bir takım adli bilişim standartlarına vâkıftırlar. Bu standartlara vâkıf olma; konu içerisinde ayrıntılı bir şekilde ele alındığı üzere bir takım sertifikalarla kanıtlanmaktadır. Bilirkişi seçilirken bu sertifikaların dikkate alınması adli bilişim sürecinin başarılı işletilmesinde ön ayak olacaktır. "Bilişim Ağı Hizmetlerinin Düzenlenmesi Ve Bilişim Suçları Hakkında Kanun Tasarısı"'nın 35. maddesinde "adli bilişim uzmanı" düzenlenmişti. Tasarıdaki bu madde kanunlaşmasa da Adli Tıp içerisinde Fizik İhtisas Dairesi Başkanlığı adli bilişim alanında resmi bilirkişilik görevini yürütmektedir. Cumhuriyet savcıları veya hakimler bilgisayarlara yönelik koruma tedbirlerinin uygulanmasında bu resmi bilirkişilere başvurabilirler.

B- AK-SSS ve KARŞILAŞTIRMALI HUKUK BAKIMINDAN

Sözleşmenin 19. maddesi taraf ülkelere saklanan bilgisayar verilerinin aranması ve bunlara elkonulması konusunda yasama işlemleri yapma yükümlülüğünü yüklemiştir. Ülkemiz sözleşmeye imza koymuştur. Saklanan bilgisayar verilerinin aranması ve bunlara elkonulması tedbirleri, sözleşmeye imza koymadan önce CMK'nın 134. maddesinde öngörülmüştür. Bu durum dünyadaki bilişim hukuku alanındaki gelişmelerin takip edilmesinde önemli bir adımdır.

Sözleşmenin 19. maddesi bir bilgisayar sisteminden gerekli koşullar varsa başka bir bilgisayar sisteminin aranabileceğini düzenlemişken aynı konu CMK'da yoktur. AÖAY'nin 17. maddesinin 3. fıkrasında bilgisayar ağları sadece yedeklemenin yapılacağı bir unsur olarak anlaşılmaktadır. AÖAY md. 17/3'teki hükmün sadece yedekleme ile sınırlı olmayıp aramayı da kapsadığı düşünülürse bilgisayar ağları ve diğer uzak bilgisayar kütükleri üzerinde de arama yapılabilmesi mümkün olabilecektir. Fakat böyle bir aramanın özel olarak kanunda öngörülmesi gerekirdi. Yönetmelik hükmüne dayanılarak arama kapsamının genişletilmesi temel hak ve özgürlüklere ölçülü bir müdahale ile bağdaşmamaktadır.

Ağ sistemi temelli olan internetteki veriler daha önce belirttiğimiz üzere akışkandır. Bu akışkan verilerin ceza muhakemesinde delil olması konusunda herhangi bir düzenleme yoktur. İnternet ortamından delil elde edilmesini ele alan hukuki bir düzenlemenin olmaması da kanımızca bir eksiklik teşkil eder. Bu eksikliğe bağlı olarak internet ortamından veri elde edilmesi sorunu doğacaktır. İnternet kütüklerinin ve iletişim durumu gözetilmeden internette arama tedbirinin kanunda düzenlenmeyişinin hatalı olduğu ifade edilmektedir[437]. Söz konusu internet ortamında bulunan veriler ile bilgisayarlar ve veri saklama birimlerinde olan veriler birbirinden farklılık arzetmektedir.

AK-SSS'nin 19. maddesindeki arama ve elkoyma tedbirleri "kopyalama"yı da içerecek şekildedir. Tüm verilerin kopyalanması veya bir kısmının kopyalanması verilere elkonulması anlamına gelmektedir. Elkoyma burada hem bilgisayarın maddi varlığına hem de verilerin kopyalanmasını ifade ettiği gibi ayrı bir tedbir olarak da nitelendirilmiştir. Karşılaştırmalı olarak düşünülürse, bu düzenlemeler CMK'daki hükümlerden farklı değildir. Verilerin kopyalanması soyut alandaki verilerin elkonulmasıyla aynı anlamdadır.

CMK'nın 134. maddesinin 3. fıkrasında yedekleme işlemlerinde "sistemdeki tüm verilerin yedeklenmesi" ibaresiyle anlaşılan bilişim sistemi kavramı ile AK-SSS'deki bilgisayar sistemi kavramı arasında bir karşılaştırma

[437] Ünver, Hakeri, **a.g.e.**, s. 426.

yapıldığında her iki kavramın da aynı şeyi kastettiği anlaşılmaktadır. Söz konusu bu iki kavramda verilerin otomatik olarak işlenmesi esas alınmıştır. Bu durumdan bilişim hukuku alanında dünyada yaşanan gelişmelerin kavramsal olarak yakından takip edildiğini anlamak mümkündür.

Verilerin korunmasına AK-SSS ayrı bir önem vermiştir. Sözleşmenin 16. maddesinde "Saklanan Bilgisayar Verilerinin Korunmasının Kolaylaştırılması" başlığı altında taraf ülkelere verilerin korunmasına yönelik bir takım yasama işlemleri yapma yükümlülüğü öngörülmüştür. Bilgisayarların ve veri saklayan birimlerin uygun ortamlarda muhafaza edilmesini düzenleyen SEY'in 9. maddesinin 2. fıkrası, AK-SSS'nin 16. maddesindeki düzenlenen yükümlülüğü karşılamaktadır.

Sözleşmenin 19. maddesinin 7. maddesindeki bilgisayar verilerin erişilmez kılınması ve kullanılamaz hale getirilmesi ile ilgili bir hüküm CMK'nın 134. maddesinde ve AÖAY'de bulunmamaktadır. Bulundurulması suç teşkil eden verilerin yok edilmesi veya bunların kullanılamayacak duruma getirilmesi ile ilgili hükümlere ihtiyaç duyulabilir.

Bilişim suçlarının delilleri ulusal sınırları aşan mahiyette olabilir. Örneğin bir ülkedeki bir bilgisayar sistemi vasıtasıyla sonuçları başka ülkenin sınırları içerisinde bilişim suçu işlenebilir. Sözleşme bu durumu öngörerek bilişim suçlarında mücadelede işbirliğini öne çıkarmıştır. Bu işbirliğini sağlayabilmek amacıyla sözleşmeye taraf devletler yargılama yetkilerini ve adli yardım hükümlerini daha özgün bir şekilde düzenleme yükümlüğü altındadır. Ülkemiz sözleşmeye taraf olsa da henüz iç hukuk uyarınca yürürlülük işlemlerinin yapılmamış olması nedeniyle genel hükümlerdeki adli yardım kurumuna başvurulacağı akla gelmektedir. Buna karşılık adli yardım işletilse dahi AK-SSS'ne taraf olan ülkelerle bilişim suçları içerisinde bir işbirliği sözleşme yürürlülük kazanmadığından yapılamamaktadır.

Trafik verilerinin gerçek zamanlı olarak toplanmasıyla ilgili bir tedbir CMK'da yoktur. Sadece 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 2. maddesinde trafik bilgisi ile ilgili bir tanım

yapılmıştır[438]. Bu tanım AK-SSS'ndeki trafik verisi kavramını karşılamaktadır. Lâkin trafik verisine ilişkin bir koruma tedbiri öngörülmemiştir. Böyle bir tedbir düzenlenmese bile erişim sağlayıcıların trafik bilgilerini tutma yükümlülüğü vardır. İnternet ortamında birbirleriyle bağlantılı bilgisayarların aralarında yaptıkları web sitesi yayını, siteye girme, veri trafiğini düzenleme, e-posta gibi işlemleri zaman, süre, yararlanılan hizmetin türü, aktarılan veri miktarı ve bağlantı noktaları ve diğer kayıtların tutulmasıyla elektronik delilin elde edilmesi amaçlanmıştır[439]. Aynı zamanda sözleşmenin 21. maddesi içerikle ilgili bilgilerin ulusal sınırlar dahilinde gerçek zamanlı olarak toplanmasını; yer sağlayıcıya bu hususta kaydetme ve bilgi toplama görevlerin yüklenmesini; kaydedilen ve toplanan bu bilgi ile yetkili mercilerle işbirliği yapılmasını esas almıştır. Sözleşmeye taraf ülkeler, ciddi suç tipleri söz konusu olduğunda bu imkana başvurmayı mümkün kılabilecek düzenlemeler getirmekle yükümlüdürler. Hukukumuzda içerikle ilgili bilgileri saklayabilen internet süjelerin yükümlülükleri 5651 sayılı kanunla öngörülmüştür. Lakin bu verilerin bir suç soruşturmasında nasıl elde edileceğine ilişkin bir düzenleme mevcut değildir.

Karşılaştırmalı hukukta bazı ülkeler bakımından bilişim hukukunda bir mevzuat çeşitliliği göze çarpmaktadır. ABD'deki mevzuat çeşitliliğine ek olarak mahkeme kararları bilişim hukukunun güncel olarak gelişmesine katkıda bulunmuştur. ABD'de bu tedbirler daha çok bilişim suçları, müstehcenlik, çocuk pornografisi, elektronik olarak haberleşme alanında ve diğer bilgisayarla ilişkili suçlarda söz konusuyken CMK'nın 134. maddesinin ise bilişim suçları dışındaki diğer suçlar tiplerinden delil elde edilmesi amacıyla düzenlendiği anlaşılmaktadır.

Şifrelenmiş verilerin elde edilmesi CMK'nın 134. maddesinde sadece bir elkoyma sebebidir. İngiltere'de ise her ne kadar iletişimin tespiti ve teknik takip alanlarında düzenlemeler varsa da (RIPA-2000) ister bilgisayar olsun

---

[438] 5651 sayılı Kanun'un 2. maddesinin j fıkrası aynen,
"*Trafik bilgisi: İnternet ortamında gerçekleştirilen her türlü erişime ilişkin olarak taraflar, zaman, süre, yararlanılan hizmetin türü, aktarılan veri miktarı ve bağlantı noktaları gibi değerleri.. ifade eder..*" şeklindedir.

[439] Ahi, "Adli Bilişim Nedir" s. 2.

ister başka bir cihaz olsun şifrelenmiş bilgilere erişim hakkında özel düzenlemelerin varlığı dikkat çekicidir. CMK'daki bütün koruma tedbirlerinde şifreli verilerle ilgili özel bir düzenleme bulunmamaktadır. Yanlızca delil olabilecek verilerin çözülerek metin haline getirilmesi konusunda ise bir benzerlik kurulabilir.

Alman Ceza Muhakemesi Kanunu'nda (StPO) bilgisayarlara ilişkin böyle özel bir tedbir düzenlenmemiştir. Arama ve elkoymadaki genel hükümler bilgisayarlar ve veri saklama birimleri üzerinde uygulanacaktır. Böylece şüpheli veya sanığın haricindeki kişilerin bilgisayarları da bu tedbirlere konu olsa da böyle bir durum CMK'da yoktur.

Bununla birlikte Almanya'da kişisel verilerle ilgili olarak bilgisayar destekli arama veya trol ağı metodu gibi aramalarda ise şüphelinin kullandığı bilgisayarda delil araması değil; çeşitli kurum ve kuruluşlardaki şüpheli ait ilgili verilerin toplanmasını esas almaktadır. Almanya'da uygulanan RFS (Remote Forensic Software) gibi programlarla uzaktan şüphelinin bilgisayarına virüs gönderilerek delil aranması CMK'da yoktur. Kaldı ki bu tür tedbiri düzenleyen kanunu Alman AYM'si iptal ederek "Bilgi teknolojisi sistemlerinde mahremiyet ve doğruluk hakkı" gibi anayasada olmayan bir hak ihdas etmiştir. Bilişim hukuku alanında yeni kanuni düzenlemeler yapılacaksa bu hakkın içeriğinin esas alınmasının yararlı olacağı düşüncesindeyiz.

Fransa'da bu özel koruma tedbiriyle ilgili hükümler ile CMK'daki düzenlemeler karşılaştırıldığında genel elkoyma kararı ile bir farklılık göze çarpmaktadır. Bilgisayarlarda arama ve elkoyma yapabilmek için genel olarak elde edilmiş bir arama veya elkoyma kararı yeterlidir. Karar yeterli olsa da bilgisayara elkoymayla bağlantılı bir takım özel durumlar dikkate alınacaktır. Bilgisayardaki verilerin aranma, kopyalanması ve elkonulması CMK'daki 134. maddesiyle karşılaştırıldığında benzer olduğu görülebilmektedir. Farklılık olarak bir bilgisayar üzerinden Fransa sınırları dışındaki başka bilgisayarların üzerinde delil aramasının ikili sözleşmeler çerçevesinde yapılması ve bunun Fransız Ceza Muhakemesi Kanunu'nda (md. 57-1) özel bir düzenleme olarak yer alması gösterilebilir. Böyle bir düzenlemenin var olması Fransa'nın AK-

SSS'ne taraf olmasının bir gereğidir. Ceza mevzuatımızda ise böyle bir düzenleme bulunmamaktadır.

Şifrelenmiş verilerin aranması (Fransız Ceza Muhakemesi Kanunu'na 2001 yılında eklenmiştir.) aynı İngiltere'de olduğu gibi ayrıntılı olarak düzenlenmiştir. Tedbirde dikkat çekici yönler ise incelemenin belirli bir süreyle sınırlandırılması, şifrelenmiş verilere erişimin yapılması, çözülmesi ve belge biçimine getirilmesi için uzman bir kişi atanabilmesidir. CMK'da ise genel hükümlerdeki bilirkişilik uygulaması söz konusu olacaktır.

Ulusal sınırlar içerisinde bir bilgisayar üzerinden başka bir bilgisayarın ağ sistemleri temelinde aranması, Fransız Ceza Muhakemesi Kanunu'nda öngörülmüştür. Kanunla özel bir düzenleme yapılmadan CMK'nın 134. maddesi ağ sistemleri üzerinde genişletilemez.

Ülkemiz kıta avrupası sistemini benimsemiştir. Bu nedenle elektronik delillerin mahkemede diğer delillerden bir farkının olmadığı hususu hukukumuz açısından da geçerlidir.

Bilgisayarlara yönelik tedbirlerin uygulanması temek hak ve özgürlüklere bir müdahale teşkil ettiğinden hakim kararı esastır. İncelediğimiz bütün hukuk düzenlerinde hakim kararı genel kuraldır. Fakat istisnaları da sınırlı bir şekilde öngörülmüştür. ABD'de bilgisayarlara yönelik arama-elkoymanın uygulanmasında rıza, çıplak gözle görme doktirini, acil durum ve özel hayatın gizliliğine ilişkin beklentisine girmeyen hususlarda hakim kararı aranmamaktadır. Hâkim kararının istisnai halleri kendi hukukumuz açısından öngörülmemiştir. Hatta hâkim kararı savcının talebiyle güçleştirilmiştir. Bu tedbirlerle ilgili Amerikan Federal Yüksek Mahkemesi'nin veya yerel mahkemelerin temel hak ve özgürlüklere ilişkin kararları önemlidir. Hukukumuzda bu konuya temas eden henüz bir yargı kararı bulunmamaktadır.

ABD'de elde edilen delillerin kabul edilip edilmediği bir takım bilimsel testlerin sonucuna göre belirlenmektedir. CMK'daki delilin bütünlüğünü ve güvenilir olup olmadığını belirlemek amacıyla uygulanacak bilimsel testler ancak bilirkişi incelemesi kapsamında söz konusu olur. Neticede bir bilirkişi

incelemesi olduğundan vicdani delil sistemi gereği hakim bununla bağlı değildir.

Avustralya'daki düzenlemelerle hukukumuzdaki düzenlemeler arasında arama, kopyalama, elkoyma, elektronik verilerin belge haline getirilmesi bakımından bir benzerlik kurulabilirse de arama ve inceleme süresi, sürenin aşılacağı anlaşılırsa ek süre istemi, olay yerine delil elde etmede kullanılan cihazların getirilmesi, bir bilgisayarla diğer ağ bilgisayarlarında arama yapılabilmesi gibi düzenlemeler CMK'nın 134. maddesinde mevcut değildir. Avsutralya'da adli birimlere bilgisayarda arama ve kopyalamada mahkemenin görevlendirmesine uygun olarak olay yerindeki kişilere yardımcı olma yükümlülüğü öngörülmüştür. Bilgisayarlara yönelik arama, kopyalama ve elkoymada adli bilişim uzmanlarına veya kolluk birimlerine yardımcı olma yükümlülüğü CMK'da yoktur.

ABD ve Avustralya'da bilgisayarlara yönelik bu tedbirler tek değil; birden fazla kanunda yer almakta ve konularına göre bir ayrım yapılmaktadır. Avustralya'daki Gümrükler Kanunu'nda (The Customs Act) gümrük işleri içerisinde çalışan bilgisayarlara yönelik tedbirlerin düzenlenmiş olması bu duruma bir örnektir. CMK'nın 134. maddesindeki bu düzenleme başka hiçbir yerde yoktur. Bu özel tedbirler her suç tipi açısından uygulancaktır.

İsrail'in ceza muhakemesi düzenlemelerine göre şüpheli veya sanık dışındaki diğer kişilerin bilgisayarlarına veya veri saklama birimlerine bu tedbirlerin uygulanması mümkündür. İsrail'de verilerin metin haline getirilmesine benzer bir şekilde bilgisayar çıktıları delil olarak kabul edilmektedir. Lâkin bu bilgisayar çıktılarının delil olabilmesi de şarta bağlanmıştır. Ayrıca delilin konu bakımından sınırlanması da dikkat çekicidir. Söz konusu tedbirlerde hâkim kararı ve bilirkişiden yardım istenmesi gibi koşullar burada da geçerlidir. Diğer ülkelerden farklı olarak varlığı suç teşil edecek sitelere, bu siteyi yapan organizasyonların mal varlıklarına kadar bir elkoyma yapılacaktır. Siberterörle ilgili hukukumuzda böyle özel bir düzenleme mevcut değildir.

VI- SONUÇ

Bilgisayarlara, bilgisayar programlarına ve kütüklerine yönelik arama, kopyalama ve elkoymayı düzenleyen CMK'nın 134. maddesi özellikle bilgisayarlara özgü tedbirlerin düzenlenmesinde olumlu bir adımdır. Böylelikle arama ve elkoymadaki genel hükümlerin uygulanmaya başlanmasıyla ortaya çıkabilecek muhtemel sorunlara çözüm getirilmeye çalışılmıştır. Bilgisayarın, bilgisayar programlarının ve kütüklerinin veya veri saklama birimlerinin aranması, kopyalanması ve elkonulmasında özel bir düzenlemenin yer almasıyla temel hak ve özgürlüklere yapılacak müdahalenin ölçülü olması gerektiği ve elektronik delilin önemi belirtilmiştir.

Bilgisayarlarda delil olabilecek verilerin aranmasının adli bilişim süreciyle mümkün olabileceğini ileri süren görüşler kanunun adli bilişim sürecine uygun bir şekilde değiştirilmesi gerektiğini açıklamaktadırlar. Buna karşılık maddede adli bilişim sürecinin uygulanmasına yönelik engelleyici bir hüküm de bulunmamaktadır. Nitekim Yargıtay, yukarıda bahsettiğimiz bir kararında adli bilişim basamaklarına atıfta bulunmuştur. Kanunda nasıl bir arama ve elkoymanın nasıl yapılacağı ile ilgili olarak yalnızca genel bir çerçeve çizilmektedir. Adli bilişim sürecine dayalı ayrıntılı hükümlerle CMK'nın 134. maddesine ek düzenlemeler getirmek maddenin bir koruma tedbiri olduğu gerçeğini değiştirebilecektir. Ayrıca adli bilişim sürecindeki esasların kanunun 134. maddesine getirilmesi, her zaman yeni kanun ve yeni yönetmelik düzenleme ihtiyacını ortaya çıkaracaktır. Çünkü adli bilişim teknolojinin ilerlemesine bağlı olarak sürekli gelişmesi nedeniyle kanuna konulan metodlar zamanla eskiyecektir. Bu nedenlerle adli bilişim sürecine uygun olarak kanunun veya yönetmeliğin değiştirilmesi kanaatimizce yerinde değildir. Ancak adli bilişim servisleri rehber kurallar veya SOP dökümanları gibi bir takım prosedürler hazırlayabilirler.

CMK'nın 134. maddesinin bir koruma tedbiri olması nedeniyle koruma tedbirlerinin özellikleri burada dikkate alınmalıdır. Bununla birlikte madde hükmü yorumlanırken arama ve elkoymanın özel bir düzenlemesi olduğu ve

benzer koruma tedbirlerdeki hususların burada da uygulanabileceği gözden kaçırılmamaldır. CMK'nın 134. maddesinin asıl amacı, şüphelinin kullandığı bilgisayarın, şüphelide kalacak şekilde arama yapılması ve delil elde edilmesidir. Maddedeki şartlar dahilinde elkoymaya gidilmelidir. Zira bu yorum ölçülülük ilkesine son derecede uygundur.

Maddedeki savcının talebi, hakim kararı ve son çare ilkesine yer verilmesi tedbirin müdahale ettiği temel hak ve özgürlükler ve yol açtığı ağır sonuçlara hemen neden olunmaması bakımından olumlu bir düzenlemedir. Karşılaştırmalı hukukta, başka surette delil elde edilmemesi imkanının bulunmaması şartının öngörülmemesi, temel hak ve özgürlüklerin korunmasında hukukumuzdaki düzenlemelerin daha başarılı olduğu ileri sürülebilir. Karşılaştırmalı hukukta yanlızca (özellikle Amerikan ve Alman hukuklarında) bireyin temel hak ve özgürlüğünün korunması bakımından ölçülü bir şekilde hareket edilmesi gerektiği vurgulanmıştır.

Bilişim suçlarının ülkemizde yoğunluğu ise diğer suçlara oranla düşüktür. Lâkin gün geçtikçe bilişim suçlarının gözle görülebilir bir artışı mevcuttur. Bilişim suçlarında ise delillerin derhal elde edilmesinin gerekmesi nedeniyle maddede öngörülen son çare ilkesi, ilk çareye dönüşmektedir. Başka surette delil elde etme imkanının bulunmaması şartının genellikle arama ve elkoyma tedbirlerinden sonra uygulanacağı şeklinde anlaşılması nedeniyle maddi gerçeğin bulunmasında bir etkisinin bulunmayacağı iddia edilmiştir. Söz konusu şart tedbirin ikincillik niteliğini vurgulamaktadır. İkincil nitelikteki tedbir, birincil tedbirin uygulansa da sonuç getirmeyeceğinin anlaşılması üzerine derhal uygulanabilir. Başka bir ifadeyle söz konusu şart sadece ilk anlamı kastetmemektedir. Bu nedenle bilişim suçları bakımından CMK'nın 134. maddesiyle ilgili herhangi bir sorun görünmemektedir. Ancak bir bilişim suçunun işlendiği hemen tespit edilebiliyorsa delillerin kaybolmaması için sadece gecikmesinde sakınca bulunan hal kapsamı altında Cumhuriyet savcısının derhal müdahale edebileceğine ilişkin bir düzenleme getirilebilir.

Başka surette delil elde etme imkanının bulunmaması şartının varlığı, kuvvetli şüphenin göz önüne alınmasını gerektirmektedir. Maddede kuvvetli şüphenin yer almaması doğrudan makul şüphenin uygulanması anlamına gelmez. Özellikle temel hak ve özgürlüklerin etkin bir şekilde korunmasında kuvvetli şüphenin varlığı önemlidir. Ancak kuvvetli şüphenin madddede yer almasıyla; hakim, savcı ve kolluğun uygulamada karşı karşıya kaldıkları tereddütler giderilebilecektir.

Telekomünikasyon yoluyla iletişimin denetlenmesi tedbirlerinde katalog suç tipleriyle sınırlanması tedbirin müdahale ettiği temel hak ve özgürlükler bakımından olumludur. Her suç tipi açısından (istisnalar haricinde) bu tedbire son çare olsa da başvurulmayacaktır. Buna karşılık CMK'nın 134. maddesinde katalog suç tiplerine yer verilmemesi, cezasının az olduğu suç teşkil eden haksızlıkta bile uygulanmasını gerektirebilir. Nihayetinde bu durum temel ve hak özgürlüklerin ağır bir şekilde etkilenmesine açık kapı bırakacaktır. Bu nedenle tedbirin niteliği açısından katolog suç tipleri bu madde içerisinde de dahil edilebilir.

Karşılaştırmalı hukukta (ABD'nde ve Avustralya'da) bilgisayarlara arama, kopyalama ve elkoymada inceleme, yedeğinin verilmesi veya bizzat kendisinin verilmesi bir üst süreye bağlanmıştır. Süre aşılacaksa buna ilişkin ek süre de verilebilir. Telekomünikasyon yoluyla iletişimin denetlenmesi tedbirlerinde de bir üst süre söz konusudur. Temel hak ve hürriyetlere müdahalenin makuliyet içerisinde kalması gerektiğinden tedbir için bir üst süreden bahsedilmesi ölçülülük ilkesine son derece uygundur. Bilgisayarlara yönelik tedbirlerde böyle bir süre düzenlemesinin öngörülmesi tartışmaya açık bir konudur. Zira delil bulununcaya kadar aramaya devam edilmelidir. Yeterli delil elde edildikten sonra aramanın bitirilmemesi zaten ölçülülük ilkesine aykırlık oluşturur. Elkoyma tedbirinde şifrenin çözümünün yapılması ve gerekli kopyaların alınmasıyla elkonulan cihazlar derhal geri verilecektir. Burada bir süreden bahsedilmemesinin kanımızca asıl nedeni elkonulan birimlerin birden fazla olabilmesi ihtimalidir. Ayrıca incelenecek cihazlar ve veri saklama birimlerinin modelleri çok çeşitli olabilir. Elkonulan cihazlardan

veya veri saklama birimlerinden yedek çıkarılması çok vakit alabilir. Neticede talep üzerine yedeğinin çıkarılmasında üst süre koşulunun getirilmesi bazı birimlerin yedeklenmemesi sonucunu doğurabilir ve yedeklenmeden geri verilmesine yol açabilir. İster elkoyma halinde cihazların geri verilmesi olsun isterse yedekten bir kopya çıkarılması olsun, makul süre aşılmamalı ve şüpheli tedbirden aşırı şekilde etkilenmemelidir.

Konu içerisinde değinildiği üzere internetteki akışkan nitelikteki verilerin, trafik verileri, yer sağlayıcının içerikle ilgili bilgilerin toplanması ve kaydelilmesiyle ilgili özel koruma tedbirleri getirilmelidir. Zira CMK'nın 134. maddesi ise durağan haldeki verilerin elde edilmesini dikkate aldığından bu iki hususu tam karşılamamaktadır. Örneğin 5651 sayılı kanunda erişim sağlayıcılarının sakladığı trafik bilgilerinden bahsedilmiştir. İnternet ortamına erişim sağlayan taraflar, zaman, süre, yararlanılan hizmetin türü, aktarılan veri miktarı ve bağlantı noktaları birer trafik bilgisidir ve suça ilişkin bilgiler bunların arasında bulunabilir. Katalog olarak öngörülen suç tipleri kapsamında hakim kararıyla ve başka surette delil elde etme imkanının bulunmaması nedeniyle bu bilgiler internet süjelerinden temin edilebilmelidir. İçeriğin, yer sağlayıcının veya içerik sağlayıcının donanımında veya kütüklerinde bulunması nedeniyle AK-SSS'in 21. maddesinin 2. ve 3. paragraftaki yetkiler bir koruma tedbiri olarak düzenlenebilir. Yani bir suç soruşturmasında veya kovuşturmasında yargılama süjeleriyle bir bilgi paylaşımı yapılabilir. Bu alanlarda vukubulan eksikliklerin tamamlanmasında, AK-SSS'ndeki hükümlere başvurulabilir.

CMK'nın 134. maddesine bulundurulması suç teşkil eden bir verinin geri verilmeyeceğine ilişkin bir düzenleme ek bir fıkra şeklinde getirilebilir. Böyle bir düzenlemenin bulunmaması halinde şüphelinin talep üzerine bu veriyi tekrar elde edilebilme imkanına sahip olacaktır. Ayrıca hükümden sonrası bu verilerin müsaderesine ilişkin bir hükümde CMK'da yoktur. Müsadere edilen bir mal olmadığı sadece bir veri olduğu için bunların yok edilmesi, silinmesi veya kullanılamaz hale getirilmesi gerekmektedir. AK-

SSS'nin 19. maddesinin 7. fıkrası bu imkanları sağlayan hukuki düzenlemeler yapılmasını bir yükümlülük olarak dikkate almıştır.

Maddenin 4. fıkrasındaki vekil kavramı CMK'nın tanımlar kısmındaki müdafi ve vekil kavramlarına uygun bir biçimde hazırlanmalıdır. Buna karşılık salt müdafi ve vekil kavramlarının olması şüpheliyi olay yerinde temsil edebilmeyi sınırlayacaktır. Olması gereken açısından yaklaşıldığında müdafi ve vekil kavramlarına ek olarak onu temsil edebilecek "aile üyeleri" veya CMK'da şüpheliyi olay yerinde temsil edebilmeyi sağlayan ifadeler getirilebilir. Böylece kanunun belirliliği ve açıklığı sağlanmış olacak; pratikteki sorunlar aşılacaktır.

Kopyalanan verilerin yazdırılmasında belge deliline öncelik verilmiştir. Kanaatimizce elektronik delillerin bozulma, yok edilme ve silinme risklerinden dolayı böyle bir yol tutulmuştur. Aynı zamanda belge haline dönüştürme karşılaştırmalı hukukta da öngörülmüştür. Riskleri en aza indirmek için delil olabilecek veriler kağıda yazdırılmakta ve bu yolla güvence altına alınmaktadır. Belge deliline öncelik verilmesi elektronik verilerin başlı başına delil olamayacağı anlamına gelmeyecektir. Elektronik deliller elektornik ortamlar kullanılarak (örneğin ağ sistemleri veya UYAP gibi) da sunulabilir. Ancak ispat bakımından belgeye dönüştürülmesinde yarar vardır.

Savcılığın bilgisayarlara uygulanan tedbirler neticesinde iddia edilen suçla ilgili bir delil elde edilmemesi ve akabinde kovuşturmaya yer olmadığına ilişkin kararı vermesi halinde şüphelinin bilgisayarından kopya çıkartılan verilerin akıbetinin ne olacağı konusunda yukarıda değinildiği üzere CMK'nın 137. maddesinin 3. fıkrasındaki hükmün kıyasen işletilmesi gerekmektedir. Buna karşılık kıyasen bir çözüm yolu bulunmaya çalışılsa da özellikle 5982 sayılı kanunla anayasanın özel hayatın gizliliği başlığı altındaki 20. maddesine getirilen kişisel verilerin korunması ile ilgili ek fıkraya uygun olarak CMK'nın 134. maddesine elde edilen verilerin silinmesini ele alan bir fıkra getirilebilir. Düzenlenecek bu yeni fıkra ile kıyas yolu yerine doğrudan fıkra hükmü icra edilecektir. Zira söz konusu kişisel verilerle ilgili anayasa değişikliğinin son cümlesinde kişisel verilerle ilgili maddi ve usule ilişkin

hususların kanunla düzenleneceğine hükmedilmiştir. Kanunla düzenleme yapılmasa da CMK md. 137/3'ün kıyasen uygulanmasıyla bu sorun aşılabilmektedir.

AK-SSS'ndeki düzenlemelerin takip edilmesi çok önemlidir. Söz konusu 19. maddedeki düzenlemelerin karşılığını CMK'nın 134. maddesi oluşturmaktadır. Söz konusu gelişmeleri takip edebilmede CMK'nın 134. maddesini olumlu bir gelişme olarak nitelendirmekteyiz. Ayrıca bilişim suçlarıyla mücadele ve sözleşmede özel olarak düzenlenen adli yardımdan faydalanabilmek amacıyla sözleşmeye imza koyulması kanımızca doğru bir adımdır. Sözleşmenin iç hukukta yürürlülük kazanmasıyla, delil elde etmede sözleşmeye taraf olan ülkelerle yapılan yazışmalar sonuç getirecek ve bilişim suçlarıyla mücadelede etkinlik sağlanacaktır. Sözleşmeye taraf olunması halinde mevzuat hazırlamada ülkemiz bir yükümlülük altına girecektir. Lâkin bu yükümlülüğün ülkemizdeki bilişim mevzuatının gelişmesinde katkısının olacağı kuşkusuzdur. Mevzuatın hazırlanmasında ABD'deki düzenlemeler örnek alınabilir. Bunun yanında CTOSE projesiyle getirilen yenilikler incelenmeli ve AB'nin elektronik delil politikası anlaşılmaya çalışmalıdır.

Uluslararası alanda kabul edilen adli bilişim ilkelerine ülkemizde de önem verilmektedir. Ancak bu ilkelerin benimsenmesinden önce buna uygun teknolojik alt yapı kurulmasına ağırlık verilmelidir. Teknolojik alt yapı kurulsa dahi teknoloji üretilmedikçe delil elde etmede kullanılan programlar, cihazlar ve teçhizatlar zamanla eskiyecek ve yenilerini edinebilmek için hep ithal edilmek zorunda kalınacaktır. Adli bilişim pahalı bir süreçtir. Ne kadar pahalı bile olsa laboratuvarların kurulması ve bilirkişilik bakımından personel eğitimi için gerekli sermayenin sağlanması şarttır.

Adli bilişimde güncelenen gelişmeleri takip edebilmek için özellikle üniversite de bilişim ve bilgisayar derslerinin yanında hukukçuların da bir araya gelerek ortak çalışma yapmaları gerekmektedir. Adli bilişimle ilgili konferans, panel ve seminerler düzenlenerek hukukçuların ve bilişim uzmanlarının katılımı sağlanmalıdır. Bilgilendirmenin yapılmasıyla CMK'nın

134. maddesinin önemi daha iyi bir şekilde kavranacak ve bilişim şuuru geliştirilerek bilişim suçlarının mücadelesinde etkinlik artacaktır.

KAYNAKÇA

ABEL, Wieke; "Agent, Trojans and Tags: The Next Generation of Investigators", **International Review of Law, Computers & Technology**, March 2009, Volume 23, Issue 1&2, s. 101. (Erişim) http://www.informaworld.com/smpp/section?content=a910308496&fulltext=713240 9, 15 Eylül 2009. s. 99-108.

ABEL, Wieke SCHAFER, Burkhard; "The German Constitutional Court on the Right Confidentially and Integrity of Information Technology Systems – A Case Report on BverfG, NJW 2008, 822." **SCRIPTed - A Journal of Law, Technology & Society**, April 2009, Volume I, Issue I, (Erişim), http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/abel.asp, 14 Eylül 2009., s. 106-123.

AHİ, Gökhan; "Adli Bilişim Nedir ?", **Güncel Hukuk Dergisi**, Mart 2009, (Erişim), http://www.ahi-gurler-taygun.av.tr/?adli-bilisim-nedir-av.-m.gokhan-ahi,52,11 Temmuz 2009.

AKTEPE, Basri; "Emniyet Personelinin Bilgisayar ve Bilgisayarla İlintili Suçlarla Mücadelede Dikkat Edilmesi Gereken Hususlar", **1. Polis Sempozyumu**, Ankara, EGM Bilgi-İşlem Daire Başkanlığı, 2003, s. 66-69.

Ankara Barosu Uluslararası Hukuk Kurultayı, Cilt 2, Ankara, 2008.

ATICI, Bünyamin, GÜMÜŞ Çetin; "Sanal Ortamda Gerçek Tehditler: Siber Terör", **Polis Dergisi**, Sayı 37, y.y., (Erişim) http://www.egm.gov.tr/egitim/dergi/eskisayi/index.htm, 01 Ekim 2009.

AYDIN, Emin Doğan; **Bilgisayar, Bilgi İşlem ve Telekomünikasyon Terimleri Sözlüğü**, 6. Bası, Cilt 1, İstanbul, Yalın Yayıncılık, 2007.

BALAY, Mustafa, ERSES, Neşe; **Bilgisayar Kullanımı ve İnternet**, Ed: Aysan Şentürk, Bursa, Ekin Kitabevi, 2. baskı, Kasım 2005.

BALI, Yunus; "Adli Bilişim Rapor Metinlerinin Yargılama Sürecinde Kullanımı Ve Anlamlandırabilirliği", **Ses Görüntü ve Data İncelemeleri**, Ed: Levent Bayram, Ankara, Adalet Yayınevi, 2008. s. 231-238.

BAŞTÜRK, İhsan; "Bilgisayar Sistemleri ile Verilerinde Arama, Kopyalama ve Elkoyma", **Fasikül Aylık Hukuk Dergisi**, CEHAMER, Sayı: 9, Ağustos 2010 s. 28-

BERBER, Leyla Keser; **Adli Bilişim**, Ankara, Yetkin Yayınları, 2004.

BERBER, Leyla Keser; "Adli Bilişim Uzmanı Kimdir? -1" (Erişim) http://turk.internet.com/haber/yazigoster.php3?yaziid=16731, 12 Temmuz 2009.

BERBER, Leyla Keser; "Adli Bilişim, CMK md. 134. ve Düşündürdükleri", (Erişim) http://www.leylakeser.org, 10 Aralık 2008.

BERBER, Leyla Keser; "Adli Bilişimle İlgili Olarak AB ve ABD'deki Yasal Düzenlemeler ve Kişisel Verilerin Korunması", **Bilişim Hukuku Konferansı-YARGITAY**, Ankara, 09-10 Ekim 2008, s. 19-53.

BİÇKİN, İnci; "Siber Suç Sözleşmesi, 5237 sayılı Türk Ceza Kanunu, Bilişim Suçları", **Bilişim ve Hukuk**, Sayı: 1, Yıl: 1, Ankara, Ankara Barosu, 2006. s. 65-75.

BIÇAK, Vahit; **Suç Muhakemesi Hukuku,** Ankara, Seçkin Yayınevi, 2010.

BRONIT, Simon, GANI, Miriam; "Shifting Boundaries of Cybercrime: From Computer Hacking to CyberTerrorism", **Crime Law Journal**, Number 27, (Erişim) http://law.anu.edu.au/UnitUploads/LAWS8164-2581-Bronitt%20and%20Gani.pdf, 24 Ekim 2009, s. 303-323.

CASEY, Eoghan; **Digital Evidence and Computer Crime**, Newyork-London Academic Press, 2000.

CENTEL, Nur, ZAFER, Hamide; **Ceza Muhakemesi Hukuku**, 7. Bası, İstanbul, Beta Yayınevi, 2010.

ÇOLAK, Haluk, TAŞKIN Mustafa; **Ceza Muhakemesi Kanunu Şerhi**, 2. Baskı, Ankara, Seçkin Yayınevi, 2007.

DOKURER, Semih; "Adli Bilişim"**, Ses Görüntü ve Data İncelemeleri**, Ed: Levent Bayram, Ankara, Adalet Yayınevi, 2008., s.239-249.

EKİZER, Ahmet Hakan; **Adli Bilişim (Computer Forensics-Bilgisayar Kriminalistiği)**,(Erişim) http://www.bilgisayarpolisi.com/index.php?sayfa=makaleoku&kategori=11&135, 10 Temmuz 2009.

EKİZER, Ahmet Hakan; "Adli Bilişim Uzmanlığı Sertifikasyonları", (Erişim) http://www.bilgisayarpolisi.com/index.php?sayfa=makaleoku&kategori=11&id=136, 16 Ekim 2008, s.1-3.

ERGÜN, İsmail; **Siber Suçların Cezalandırılması ve Türkiye'de Durum**, Ankara, Adalet Yayınevi, 2008.

FERRERA, Gerald R,. LİCHTENSTEİN Stephen D., REDER, Margo E. K. vd... **CyberLaw: Text and Cases**, , Ohio, Thomson\South-Western\West, Second Edition 2004.

GALVES, Fred, GALVES, Christine; "Ensuring Admissibility of Electronic Forensic and Enhancing Its Probative Value At Trial", **Criminal Justice Magazine,** Vol: 19, Number 1, Spring 2004, (Erişim) http://www.abanet.org/crimjust/cjmag/19-1/electronic.html, 13 Ekim 2009.

GOLUMBIC, Martin C.; "The Legal Framework in Israel", **Fighting Terror Online**, Newyork, 2008, Springer, (Erişim) http://www.springerlink.com/content/u61n05j928p62476/fulltext.pdf, 24 Kasım 2008, s. 107-136.

GROSS, Emmanuel; "The Struggle of a Democracy Against Terrorism-Protection of Human Rights: The Right to Versus The National Interest – The Proper Balance, **Cornell International Law Journal**, Volume 37, 2004, (Erişim) http://papers.ssrn.com/sol3/papers.cfm?abstract_id=683942, 27 Ekim 2009, s. 102-165.

GÜLCÜ, Aslan, ALAN, M. Ali; **Bilgisayarın Temelleri Ve İnternet Rehberi**, Ankara, Detay Yayıncılık, Ekim 2003.

GÜRER, H. Vedat; "Hukukçu Gözüyle Sayısal İmza, Sayısal Kimlik, Sayısal Evrak
ve Sayısal Sözleşme", (Erişim) http://www.bilisimrehber.com.tr/arastirma/tr_arastirma_vedat_gurer_1.phtml, 18 Eylül 2009.

HAMES, Joanne Banker, EKERN, Yvonne; **Constitutional Law: Principles and Practice**, The West Legal Studies Series, Clifton Park-New York, Thomson Delmar Learning.

HELVACIOĞLU, Aslı Deniz; "Avrupa Konseyi Siber Suç Sözleşmesi-Temel Hükümlerinin İncelenmesi", **İnternet ve Hukuk**, Der: Yeşim M. Atamer, İstanbul, İstanbul Bilgi Üniversitesi Yayınları 51, Hukuk 2, Ocak 2004, s. 281-299

HODGE, Matthew J.; **"**The Fourth Amendment and Privacy Issues On The "New" Internet: Facebook.com, and MySpace.com", **Sourthern Illinois University Law Journal**, 31, 95, 2006-2007 (Erişim) www.law.siu.edu/research/31fallpdf/**fourthamendment**.pdf, 20 Ekim 2009, s. 95-123.

KARAGÜLMEZ, Ali; **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, 2. Bası, Ankara, Seçkin Yayıncılık, 2009.

KARAGÜLMEZ, Ali; "Bilişim Suçlarında Delil Elde Etmeyi Etkileyen Başlıca Konular", (Erişim) http://www.caginpolisi.com.tr/46/7-8-9-10.htm - _ftn1, 09 Ocak 2009.

KARAKEHYA Hakan; "Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu", **TBBD**, Sayı 81, Mart-Nisan, 2009, s. 187-211.

KAYGISIZ, Mustafa; **Adli Bilimler Suç Analizi**, Ankara, Adalet Yayınevi, 2008.

KAYGISIZ, Mustafa; **Suç Yeri Ve Delil Güvenliği**, Hukuk Yayınları Dizisi-295, y.y., Adalet Yayınevi, Ekim 2007.

KENNEALLY, Erin; "Computer Forensics" **Login**, Berkeley, The Magazines of Usenix&Sage, August 2002, (Erişim), http://www.usenix.org/publications/login/2002-08/pdfs/kenneally.pdf, 11Temmuz 2009, s. 1-11.

KERR, Orin S.; "Searches and Seizures In a Digital World", **Harward Law Review**, Vol 116, 531, December 2005 - 2006, (Erişim) http://web.si.umich.edu/tprc/papers/2005/495/orinkerrhlr.pdf, 03 Ekim 2009, s. 1-58.

KILINÇ, Doğan "Türk Hukukunda ve Mukayeseli Hukukta İnternet Sitelerine Erişimin Engellenmesi ve İfade Hürriyeti", **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, Cilt: XIV, Yıl: 2010, Sayı: 2, Ankara, Aralık 2010, s. 407-454.

KOCA, Mahmut; "Avrupa Konseyi Siber Suç Sözleşmesin'nin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku", **Bilgi Toplumunda Hukuk**, **Ünal Tekinalp' Armağan**, Cilt III, İstanbul, Beta Yayınevi, 2003, s. 788-810.

KOCA, Mahmut "Ceza Muhakemesi Hukukunda Delilller", **CHD,** Yıl: 1, Sayı: 2, Seçkin Yayınevi, 2006, s. 207-226.

KÖKSAL, Aydın; "Türkçe Bilim Sözleri; Bir Deneyim", **Bilim ve Ütopya Dergisi,** Şubat, 2001. (Erişim) http://www.bilimbilmek.com/sayfa/Aydin_Koksal-Turkce_Bilim_Sozleri.html, 25 Haziran 09, s. 14-21.

KUNTER, Nurullah, YENİSEY, Feridun, NUHOĞLU, Ayşe; **Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku**, 16. bası, İstanbul, Beta Yayınevi, Ocak 2008.

KURT, Levent; **Açıklamalı ve Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunu'ndaki Uygulaması,** Ankara, Seçkin Yayınevi, Eylül 2005.

LEROUX, Oliver; “Legal Admissibility of Electronic Evidence”, **International Review of Law, Computers and Technology**, 01 July 2004, Volume 19, Number 2, (Erişim)http://dx.doi.org/10.1080/1360086042000223508, 17 Eylül 2009, s.193-220.

LEVUSH, Ruth; “Law Library of Congress Israel: Computer Security and Protection of Computer Information”, (Erişim) http://www.mafhoum.com/press4/236.pdf, 28 Kasım 2009, s.1-22.

MAHMUTOĞLU, Fatih Selami; “Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu” **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt LIX, Sayı 1-2, İstanbul, Beta Basım Dağıtım, 2001, s. 39-49.

MALKOÇ, İsmail, YÜKSEKTEPE, Mert; **Açıklamalar ve Yorumlarıyla 5271 Sayılı Yeni Ceza Muhakemesi Kanunu**, 1. Cilt, Ankara, Malkoç Kitabevi, 2008.

MERAN, Necati; “İnternet Yoluyla İşlenen Suçlarda Erişimin Engellenmesi ve İçeriğin Yayından Çıkarılması”, **Terazi Aylık Hukuk Dergisi**, Yıl: 5, Sayı: 47, Ankara, Temmuz 2010, s. 115-129.

MOORE, Robert; “Plain View and Digital Evidence”, **American Journal of Criminal Justice**, Volume 29, Number 1, 2004, (Erişim) http://www.springerlink.com/content/rj8x868346127281/, 05 Ekim 2009, s. 57-74.

ÖLMEZ, Aslan; “Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Kopyalama ve Bunlara Elkoyma”, **Terazi Aylık Hukuk Dergisi**, Sayı: 30, Şubat, 2009, s. 49-58.

ÖZBEK, Veli Özer; “Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi”, **İÜHFM**, Cilt LIX, Sayı 1-2, İstanbul, Beta Basım Dağıtım, 2001, s. 181-202.

ÖZBEK, Veli Özer; **CMK İzmir Şerhi**: **Yeni Ceza Muhakemesi Kanunun Anlamı**, Ankara, Seçkin Yayınevi, 2005.

ÖZDEMİR, Kenan; “Türk Hukukunda ve Avrupa İnsan Hakları Sözleşmesi ile AİHM Kararlarında Özel Hayatın Gizliliği”, (Erişim) http://www.hukuki.net/hukuk/index.php?article=515, 05.06.2009.

ÖZGENÇ, İzzet; **Türk Ceza Kanunu Gazi Şerhi**: **Genel Hükümler**, 3. Bası., Ankara, Adalet Bakanlığı Eğitim Dairesi Başkanlığı, 2006.

ÖZTÜRK, Bahri, ERDEM, Musatfa Ruhan; **Uygulamalı Ceza Muhakemesi Hukuku**, 12. Bası, Ankara, Seçkin Yayınevi, 2008.

PICOTTI, Lorenzo, SALVODORI Ivan; "National Legsitation Implementing The Convention On Cybercrime-Comparative Analysis and Good Practises", **(Discussion Paper)**, 12.03.2008, Strasbourg, (Erişim), http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/DOC%20567%20study2-d-version8%20provisional%20(12%20march%2008).PDF, 26 Eylül 2009.

REITINGER, Phlip R.; **"**Encryption, anonymity and markets", **Cybercrime: Law enforcement, security and surceillance in the information age**, Ed: Douglas Thomas, Brian D. Loader, London and Newyork, Routledge, 2003.

ROSENOER, Jonathan; **Cyberlaw: The Law of Internet**, New York, Springer, 1997,

SAY, Kubilay; "Bilişim Suçlarında Olay Yeri İncelemesinin Hukuki Boyutu", **Ses Görüntü ve Data İncelemeleri**, Ed: Levent Bayram, Ankara, Adalet Yayınevi, 2008., s. 251-260.

SEVİM Güçlü; "Bilgisayar ve Bilgisayar Kütüklerine El Konulması ve Uygulamadaki Sorunlar", **İBD**, Cilt 81, Sayı 3, 2007, s. 993-1000.

SINAR, Hasan; **İnternet ve Ceza Hukuku**, İstanbul, Beta Yaynevi, 2001.

SOYASLAN, Doğan; **Ceza Muhakemesi Hukuku**, 3. Baskı, Ankara, Yetkin Yayınları, 2007.

SREMACK, Joseph C.; "Formalizing Computer Forensic Analysis: A Proof-Based Technology", **Department of Computer Science**, Raleigh, 2004, (Erişim), http://www.lib.ncsu.edu/theses/available/etd-03312004-230130/unrestricted/etd.pdf, s. 1-115.

ŞAHİN, Cumhur; **Ceza Muhakemesinde İspat (Delillerin Doğrudan Doğruyalığı İlkesi)**, Ankara, Yetkin Yayınları, 2001.

ŞAHİN, Cumhur; **Ceza Muhakemesi Kanunu**: **Gazi Şerhi**, Ankara, Seçkin Yayınevi, Aralık 2005.

ŞAHİN, Cumhur; **Ceza Muhakemesi Hukuku**, Cilt 1, Ankara, Seçkin Yayınevi, 2007.

ŞAHİN, Cumhur; "Telekomünikasyon Yoluyla İletişimin Denetlenmesi-Yargıtay Kararları Çerçevesinde Bir Değerlendirme" **Bilişim Hukuku Konferansı-YARGITAY**, Ankara, 09-10 Ekim 2008, s.124.

ŞEKER, Harun; "Adli Analiz İşlemlerine Başlamak", (Erişim) http://www.cehturkiye.com/adli_analiz_islemleri.pdf, 27 Temmuz 2009.

ŞEN, Evren; "Kriptografi ve Kullanım Alanları I", (Erişim), http://www.scribd.com/doc/2581535/Kriptografi-ve-Kull-Alan-I, 17 Eylül 2009.

ŞEN, Osman Nihat "Adli Bilişim Bilimi Ve Diğer Bilimlerle Olan İlişkisi", 01 Mayıs 2007, (Erişim) http://www.bilgisayarpolisi.com/index.php?sayfa=makaleoku&kategori=11&id=121, 29 Temmuz 2009.

ŞEN, Osman Nihat; "Ceza Hukukunda Bilgisayar Araştırmaları", **CHD**, Sayı:1, Ekim 2006, s. 374-388.

TAN, Aydoğan; "Adli Bilişim", 26 Haziran 2009, (Erişim) http://www.hukuksokagi.com/makale/adli-bilisim-computer-forensic.html, 09 Temmuz 2009.

TAŞKIN, Şaban Cankat; **Bilişim Suçları**, Bursa, Beta Yayınevi, Kasım 2008.

TDK, Türkçe Sözlük, 10. baskı, Ankara, 2005, s. 271.

TEISSERIE, David; "Cybercrime Legistation – The Kangaroo Perspective", (Erişim) http://www.scribd.com/doc/7545925/Cyber-Crime-Legislation-The-Kangaroo-Perspective, 23 Ekim 2009.

TOSUN, Nilgün, KARAMANLIOĞLU Aytaç, YERLİKAYA, TARIK, vd.; **Bilgisayara Giriş**, Ed: Nilgün Tosun, y.y. Kriter Yayınları, Ekim 2007.

Tutanaklarla Ceza Muhakemesi Kanunu, Ankara, Adalet Bakanlığı Yayın İşleri Dairesi Başkanlığı, 2005.

URBAS, Gergor, CHOO, Kim-Kwang Raymond; "Resource Materials Technology - Enabled Crime", **Australian Institute of Criminology,** Technical and Backround Paper, No: 28, (Erişim) http://aic.gov.au/documents/E/7/8/%7BE78191C1-5833-4658-BD07-DEA35DAC184A%7Dtbp028.pdf, 21 Ekim 2009, s. 1-96.

UZUNAY, Yusuf; "Dijital Delil Araştırma Süreci", **2. Polis Bilişim Sempozyumu**, Ankara, EGM Bilgi-İşlem Daire Başkanlığı, Nisan 2005.

UZUNAY, Yusuf, KOÇAK Mustafa; "Bilişim Suçları Kapsamında Dijital Deliller", **Akademik Bilişim Konferansı**, Gaziantep, Şubat 2005, (Erişim), http://www.ii.metu.edu.tr/~yuzunay/Download/ab05.pdf, 12 Haziran 2009.

ÜNVER, Yener, HAKERİ Hakan; **Ceza Muhakemesi Hukuku**, 4. Baskı, Ankara, Adalet Yayınevi, 2011.

WEGMAN Jerry; “Computer Forensics: Admissibility of Evidence In Criminal Cases”, **Journal of Legal, Ethical and Regulatory Issues,** Volume 8, Number 1, 2005, (Erişim) http://www.cbe.uidaho.edu/wegman/Computer%20Forensics%20AA%202004.htm, 05 Ekim 2009.

WEISE, Joel, POWEL, Brad; “Using Computer Forensics When Investigating System Attacks”, April 2005, (Erişim), www.sun.com/blueprints/0405/819-2262.pdf, 09 Temmuz 2009.

YAZICIOĞLU, Recep Yılmaz; **Bilgisayar Suçları**, İstanbul, Alfa Yayınevi, 1997.

YETİM, Servet; “Dijital Kanıt Araştırma Yöntemleri”, **İstanbul Barosu Dergisi**, Cilt:82, Sayı:3, 2008, (Erişim) http://www.istanbulbarosu.org.tr/yayinlar/BaroDergileri/ibd/20083/ibd2008312.pdf, 24 Haziran 2009, s. 1201-1221.

YURTCAN, Erdener; **Ceza Yargılaması Hukuku**, 12 Bası, İstanbul, Beta Yayınevi, 2007.

ZİFF, David J. S.; “Fourth Amenment Limitations On The Execution Of Computer Searches Conducted Pursuant To A Warrant”, **Columbia Law Review**, Vol 105, Issue 3, April 2005, (Erişim), http://web.ebscohost.com/ehost/pdf?vid=3&hid=5&sid=916b04fe-ccb4-4635-bb13-60b508d6615b%40sessionmgr7, 03 Ekim 2009, s. 841-872.;

İNTERNET KAYNAKLARI

Update to the Handbook of Legal Procedures of Computer and Network Misuse In Eu Countires For Assiting CSIRT, D: 15 Final Report”, Ed: Lorenzo Valeri, **RAND EUROPE & LAWFORT**, December 2005, (Erişim) ftp://ftp.cordis.europa.eu/pub/ist/docs/directorate_d/trust-security/ec-csirt-d15.pdf, 26 Eylül 2009, s. 115.

Informatics (Erişim) http://en.wikipedia.org/wiki/Informatics, 25.06.2009, s. 1.

Inserted by Law n° 2003-239 of 18 March 2003 Article 17 °1 Official Journal of 19 March 2003, (Erişim). http://www.legislationline.org/download/action/download/id/1674/file/848f4569851e2ea7eabfb2ffcd70.htm/preview, 24 Eylül 2009.

Amerikan Anayasasındaki Dördüncü Değişiklik (U.S.-The Fourth Amendment) (Erişim) http://caselaw.lp.findlaw.com/data/constitution/amendment04/, 03 Ekim 2009.

The Federal Rules of Evidence (Erişim) http://www.law.cornell.edu/rules/fre/rules.htm#Rule1001 20 Ekim 2009.

Cybercrime Legistation – Counntry Profile – Germany, (Erişim) http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/567-LEG-country%20profile%20Germany%20_1%20June%2007_En.pdf, 08 Eylül 2009, Güncelleme 01 Aralık 2010.

The Police and Justice Act, (Erişim), http://www.opsi.gov.uk/si/si2008/uksi_20082503_en_1, 10 Eylül 2009

Computer Misuse Act. (Erişim) http://www.davros.org/legal/cma.html#s14, 10 Eylül 2009

Computer Crime & Intellectual Propety, Cybercrime (Erişim) http://www.cybercrime.gov/ssmanual/02ssma.html#A, 15 Kasım 2009.

The USA Patriot Act Sunset, Expiring Sections, (Erişim) http://epic.org/privacy/terrorism/usapatriot/sunset.html#intro, 20 Ekim 2009

U.S. Code, Title 18, Chapter: 119, Wire And Electronic Communications Interception and Interception Of Oral Communications, (Erişim) http://www.law.cornell.edu/uscode/html/uscode18/usc_sup_01_18_10_I_20_119.html.

Police and Criminal Evidence Act, (Erişim), http://www.statutelaw.gov.uk, 8 Eylül 2009.

Avrupa Konseyi Siber Suç Sözleşmesi http://www.binbilen.org/belgeler/Siber_Suclar_Sozlesmesi.pdf (Erişim), 25 Haziran 2009. s. 3.

Proposed Standarts For The Exchange Of Digital Evidence", **Digital Evidence: Standarts and Principles**, Forensic Science Communications, April 2000 Volume 2 Number 2, (Erişim) http://www.fbi.gov.tr/hq/lab/fsc/backissu/april2000/swgde.htm, 17 Mart 2009, s. 1.

Inquiry into Provisions of The Cybercrime Bill 2001 – August 2001, (Erişim) http://www.aph.gov.au/senate/Committee/legcon_ctte/completed_inquiries/1999-02/cybercrimebill01/report/report.pdf, 24 Ekim 2009. s. 34.

The Crimes Act 1914, (Erişim) http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/, 19 Ekim 2009

Commonwealth Consolidated Acts (Erişim) http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/s3c.html, 19 Ekim 2009.

European Convention On Cybercrime, (Erişim) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG, 08 Eylül 2009.

http://www.scribd.com

Home Searches and Computer Seizures Under the European Convention On Human Rights", 16.03.2009, Marta L. Arias, (Erişim) http://www.ibls.com/internet_law_news_portal_view.aspx?=slastestnews&id=2213, INTERNET LAW, 05 Nisan 2009

European Court of Human Rights http://cmiskp.echr.coe.int/tkp197/portal.asp?sessionId=39341604&skin=hudoc-en&action=request, 05 Nisan 2009.

ÖZET

ÜNAL, OSMAN GAZİ, Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma. (CMK md. 134), YÜKSEK LİSANS, ANKARA, 2011.

Bilgisayarlar çağımızı etkileyen en önemli cihazların başında gelmektedir. Bilgisayarlar veya veri saklama birimleri içerisinde bulunan veriler özellikle ceza muhakemesinde maddi gerçeğin bulunmasına hizmet edebilirler. Bu nedenle CMK'nın 134. maddesinde "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma" tedbirlerini incelemek gerekir. Bilgisayarlara yönelik bu özel koruma tedbirlerini ele alırken öncelikle verileri ve elektronik delilleri konu edinen adli bilişim alanına bakılacaktır. Ayrıca tedbirin konusu olan bilgisayarın ne olup olmadığına ilişkin bir belirlemeyi yapmamız şarttır. Avrupa Konseyi Siber Suç Sözleşmesindeki bu tedbirle ilgili hükümler ve sözleşmeye taraf olan veya olmayan ülkelerdeki düzenlemeler karşılaştırmalı olarak ele alınmıştır. Özellikle ABD'deki düzenlemelere ayrıca dikkat edilmiştir. CMK'nın 134. maddesinde düzenlenen hükümler bir koruma tedbiri olduğu için genel arama ve elkoyma hükümlerine tabidir. Maddenin düzenlemesi temel hak ve özgürlükler bakımından sıkı şartlara sahiptir. Bilgisayarlara yönelik bu özel tedbir sadece şüphelinin kullandığı bilgisayar açısından uygulanabilir. Bu tedbire sadece soruşturma aşamasında değil; kovuşturma aşamasında da başvurulabilir. Bilgisayarlara yönelik arama, kopyalama ve elkoyma veri saklama birimlerine de uygulanır. Elektronik delillerin bilgisayardan ve veri saklama birimlerinden adli bilişim süreciyle toplanması delil bütünlüğünü ve güvenirliliğini etkinleştirecektir.

ANAHTAR KELİMELER:

1- Bilgisayar

2- Arama

3- Elkoyma

4- Elektronik Delil

5- Adli Bilişim

ABSTRACT

ÜNAL, Osman Gazi, The Search and Seizure of Computer, Computer Programmes and Logs. MASTER PROGRAM, ANKARA 2011 (Criminal Procedure Code, section 134)

Computers are the most impressive machines in our age. Electronic datas which included in computers and devices could serve to find the truth in the criminal procedure law. Therefore observing the search and seizure of computer, computer programs and logs measures are important. Firstly it will be focused on Computer Forensic which interests in datas and electronic evidence observing these measures about computer. These rules about the search and seizure of computer were examined with European Convention on Cybercrime's clauses and comparative law. Especially it was viewed at the United States Law importantly. Section 134's conditions are held in a subject the general provisions of search and seizure in the Criminal Procedure Law. Section 134. has strict conditions in that fundamental rights and freedoms. These special measures will execute on only suspected person who using computer. Not only search and seizure of computer is in investigation that will be in prosecution. Computer search measures are able to be used on devices. Evidence integrity and safety will activate that collecting electronic evidence in computer forensic rules.

KEY WORDS:

1- Computer,

2- Search

3- Seizure

4- Electronic Evidence

5- Computer Forensic