CEZA MUHAKEMESİNDE ELEKTRONİK DELİLLERİN TESPİTİ VE TOPLANMASI

DETECTION AND COLLECTION OF DIGITAL EVIDENCES IN CRIMINAL PROCEDURE

Gürkan Özocak

ÖZET

Ceza Muhakemesinde, muhakeme makamları önlerine gelen delillerle maddi olayı çözmekte ve bu deliller ışığında, görülmekte olan davaya ilişkin bir karar vermektedir. Ancak 5271 sayılı Ceza Muhakemesi Kanunu'nda yer alan klasik deliller dışında, özellikle bilişim suçlarının ispatlanmasında önem arzeden elektronik deliller de bu ceza yargılamasının konusu olabilmektedir. Bir bilişim sisteminin içerisinde yer alan, toplanması uzmanlık gerektiren, klasik delillerin aksine soyut nitelik arzeden ve özellikle değerlendirilme aşamasına kadar adli bilişimin de konusu olan elektronik delillerin tespiti ve toplanması gerek iç hukukta, gerekse uluslararası hukuktaki uygulamada hem hukuk tekniği, hem de Avrupa İnsan Hakları Sözleşmesi ve İnsan Hakları Evrensel Beyannamesi gibi uluslararası hukuk metinlerince teminat altına alınmış özel hayatın gizliliği ve kişisel verilerin korunması gibi önemli evrensel ilkeler açısından kimi sorunlara yol açmaktadır.

ANAHTAR KELİMELER

Ceza Muhakemesi, Elektronik Delil, Bilişim Hukuku, Bilişim Suçları, Siber Suçlar, Adli Bilişim, Delillerin Tespiti ve Toplanması.

SUMMARY

At the criminal procedure, authorities of judging and investigation solve cases with evidences and give a judgement thanks to these evidences. However, except the usual evidences that involved by Turkish Code of Criminal Procedure (CMK) No. 5271, digital evidences, that are especially important to prove cybercrimes, can also be the subject of judging. Detection and collection of digital evidences, that are involved in an information system, needed specialization to collect and also the topic of computer forensic, create some matters in not only domestic law, also create some problems about right to respect for private life and protection of personal data that secured by international convention such as European Convention of Human Rights and Universal Declaration of Human Rights.

KEYWORDS

Criminal Procedure, Digital Evidence, Informatics Law, Cybercrimes, Computer Crimes, Computer Forensic, Detection and Collection of Evidence.

ÖZGEÇMİŞ

Edirne'de doğdu. Lise öğrenimini Edirne Anadolu Öğretmen Lisesi'nde, üniversite öğrenimini Bilkent Üniversitesi Hukuk Fakültesi'nde tamamladı. Halen Ankara Üniversitesi Sosyal Bilimler Enstitüsü Ceza ve Ceza Usul Hukuku Ana Bilim Dalı yüksek lisans öğrencisi ve Ankara Barosu avukatıdır. İyi düzeyde İngilizce ve orta düzeyde İtalyanca bilmektedir.

I. CEZA MUHAKEMESİNDE DELİL

A) Genel Olarak Delil

Ceza muhakemesinde, muhakeme makamları öncelikle önlerine gelen somut olayın maddi yönünü çözmekte, maddi gerçeğin ne olduğunu tespit ettikten sonra bunun hukuki yönünü değerlendirmektedir. Bu nedenle, öncelikli görevi maddi gerçeğe ulaşmak olan ceza mahkemeleri, işlendiği iddia olunan fiilin işlenip işlenmediğini, işlenmişse bu fiilin kanunlar nezdinde bir suç teşkil edip etmediğini ve suç teşkil ediyorsa bunun sanık tarafından işlenip işlenmediğini belirlemek durumundadır.[1] Bu değerlendirme sonucunda hüküm verecek olan hakim, eğer fiilin işlendiğine, suç olduğuna ve sanık tarafından işlendiğine kanaat getirirse, hükmü "*sabit görme*"; ancak bu kriterlerden birinin mevcut bulunmaması durumunda "*sabit görmeme*" biçiminde tezahür edecektir. O halde, birinci durumda maddi gerçek ispatlandığından suçu sabit görülen sanık cezalandırılacak, ikinci durumda ise suç sübut bulmadığından cezalandırılmayacaktır.[2] İşte, hakimin ceza yargılaması esnasında yapacağı maddi olayı çözmek ve bunun için olayın sabit görülüp görülmemesine karar verilmesi olduğundan, yapılacak olan muhakemenin temelinde bu yargıyı oluşturacak delillerin değerlendirilmesi yer almaktadır.

Ceza muhakemesinde, ispat edilecek somut olay geçmişe ilişkin olduğundan ve bu olayların ortaya çıktığı zamanın ve şartların önceden bilinmesi mümkün olmadığından, bu sebeple de hukuk muhakemesinde olduğu gibi delillerin önceden hazırlanamaması sebebiyle, *"delil serbestisi ilkesi"* benimsenmiştir.[3] Bu nedenle ceza yargılamasında hakim, tarafların ileri sürdüğü delillerle bağlı değildir. Bunun yanında yargılama esnasında süre sınırına bağlı olmaksızın her şey delil olabilir ve her husus her türlü delille ispatlanabilir.[4] Hakim, ortaya konulan bu delilleri değerlendirecek ve bir hususun sabit olduğu hakkındaki hükmünü tam bir inanışla ve kanaatle verecektir. (CMK md. 217) Ne var ki, hakimin delilleri serbestçe değerlendirmesi ve vicdani kanaatle karar vermesi, keyfi hareket edeceği anlamı taşımamaktadır. Hakimin yapacağı değerlendirme akla ve mantığa uygun bir değerlendirme olmak durumunda olduğundan, hakim toplanan hangi delillere neden inanıp inanmadığını ve hangi delilleri hükme neden esas alıp almadığını açıklamak zorundadır. Ancak, bu gerekçeleri açıklamak şartıyla, hakim hem delillerin toplanmasında hem de bu toplanan delillerin değerlendirilmesinde serbestiye sahip olup, bu sisteme *"vicdani delil sistemi"* adı verilmektedir.[5]

B) Ceza Muhakemesinde Delillerin Özellikleri

Ceza muhakemesinde delil serbestisi ilkesi ve deliller üzerinde hakimin takdir yetkisi bulunmakta ise de, bu serbesti sınırsız olmayıp, delil sayılabilecek hususların kimi özelliklere sahip

---

1 **TOROSLU, Nevzat / FEYZİOĞLU, Metin**; Ceza Muhakemesi Hukuku, Ankara, 2006, s. 165-166.

2 **FEYZİOĞLU, Metin**; Ceza Muhakemesinde Vicdani Kanaat, Ankara, 2002, s. 139; **KUNTER, Nurullah**; Ceza Muhakemesi Hukuku, İstanbul, 1989, s. 584; **TOSUN, Öztekin**; Türk Suç Muhakemesi Dersleri, C. I, İstanbul, 1981, s. 585.

3 **TOROSLU/FEYZİOĞLU**, s. 168.

4 Bu delil serbestisinin bazı istisnaları mevcuttur. Bu istisnaların en önemlisi Yargıtay'ın 24.03.1989 tarihli ve 1988/1 E., 1989/2 K. Sayılı İçtihadı Birleştirme Kararı olup, buna göre imzalı boş kağıdın anlaşma dışı doldurulduğu iddiasıyla açılan ceza davasında, bu fiil Hukuk Usulü Muhakemeleri Kanunu'nun cevaz verdiği istisnai haller dışında tanık beyanıyla ispat edilemeyecektir. Ne var ki, Yargıtay'ın söz konusu İçtihadı Birleştirme Kararı sert eleştirilere uğramış olup, gerçekten de ceza muhakemesinin en temel ilkelerinden birini ihlal eden ve fiilin ortaya çıkışı ve şartlarının yazılı delile bağlanamayacağı bir durum için yalnızca yazılı delille ispat zorunluluğu getiren bu İçtihadı Birleştirme Kararı'nın hiçbir hukuki yönü bulunmamaktadır.

5 **FEYZİOĞLU**, s. 49; **KUNTER**, s. 586.

olunması aranmaktadır.[6] Buna göre;

a) Deliller **gerçekçi** olmalıdır.

b) Deliller geçmişte vuku bulan somut olayı **temsil edici** nitelikte olmalıdır. Bir başka deyişle, ceza muhakemesinde deliller geçmişte gerçekleşen olaylarla ilgili olduğundan, ortaya konulan deliller bu olayın tamamını veya bir kısmını yansıtmalı, bu hususta sağlam ve güvenilir emareler taşımalıdır.

c) Deliller **akılcı** olmalıdır. Bu bağlamda delillerin, maddi gerçeği akla uygun, gerçekçi ve objektif niteliklere dayanan verilerle ispat eder özellikte olması gerekmektedir.

d) Delillerin **elde edilebilir** olması gerekli olup, somut olarak elde edilerek mahkemenin takdirine sunulması imkan dahilinde olmalıdır.

e) Deliller **kanuna uygun** olmalıdır. Bu kanuna uygunluk iki biçimde ortaya çıkmaktadır. Buna göre deliller hem kanuna uygun nitelikte delillerden, hem de kanuna uygun yollardan elde edilen delillerden olmalıdır.

Bazı deliller, kanuna uygun yollardan elde edilmelerine rağmen, mahkeme makamına sunulduklarında içerikleri sebebiyle delil olarak kullanılamazlar. Örneğin, hekimler, hekim sıfatları sebebiyle hastaları ve bunların yakınları hakkında öğrenmiş oldukları bilgileri, hukuki yollardan elde etmiş olsalar bile, bu kişilerin izinleri olmadan delil olarak mahkemeye sunamazlar. Bazı delillerin ise, elde edilme yöntemleri hukuka aykırı olduğundan dolayı delil olarak kullanılmaları yasaklanmıştır. Örneğin, 5271 sy. Ceza Muhakemesi Kanunu (CMK) md. 148'de yer aldığı üzere, kişinin özgür iradesine dayanmasını engelleyici nitelikte kötü davranma, işkence, ilaç verme, yorma, aldatma, cebir uygulama veya tehditte bulunma, bazı araçlar uygulama gibi kişinin iradesini bozan bedeni yahut ruhi müdahalelerle ya da kanuna aykırı bir menfaat vaadinde bulunarak elde edilen deliller, mahkemede delil olarak kullanılamaz.[7]

f) Deliller **müşterek** olmalıdır. Buna göre, delilin içeriğini yalnız mahkeme makamının bilmesi yetmemekte, bu delilleri muhakemenin taraflarının da bilmesinin sağlanması gerekmektedir. Ceza muhakemesinde buna *"delillerin müşterekliği ilkesi"* denilmekte olup, bu ilke uyarınca sunulan deliller bütün muhakeme taraflarınca tartışılmalı, hakim kişisel bilgisine dayanarak hüküm tesis etmemelidir. Nitekim, dava konusu olay hakkında davanın seyrine etki edecek nitelikte kişisel bilgisi olan hakim, hakim görevinden çekilerek, mahkemede tanıklık yapmalıdır.[8]

C) İspatın Konusu

Ceza muhakemesinde, tarafların ihtilaflı olduğu konular dışında uyuştukları konular da ispat konusu olmasına karşın, genel olarak dava konusu fiili ilgilendiren şüpheli olaylar ispat konusu olarak değerlendirilmelidir.[9]

Ceza muhakemesinde, *"delillerin doğrudan doğruyalığı ilkesi"* kabul edilmiştir.[10] Şekli ve

---

6 **TOROSLU/FEYZİOĞLU**, s. 170 vd.; **TOSUN**, C. I, s. 586-587.
7 **TOROSLU/FEYZİOĞLU**, s. 171.
8 **FEYZİOĞLU, Metin**; Ceza Muhakemesi Hukukunda Tanıklık, Ankara, 1996, s. 64.
9 **LEONE, Giovanni;** Diritto e Procedura Penale, Napoli, 1988, s. 439-440; **KUNTER**, s. 597; **TOROSLU/FEYZİOĞLU**, s. 172; **YURTCAN, Erdener**; Ceza Yargılaması Hukuku, İstanbul, 1994, s. 249 vd.
10 **ŞAHİN, Cumhur**; Ceza Muhakemesinde İspat, Ankara, 2001, s. 25 vd.

maddi anlamda iki boyutu olan delillerin doğrudan doğruyalığı ilkesi şekli olarak, hakim ile deliller ve muhakemeye katılanlar arasında daima bir "ilişkinin" varlığının gerekli olduğu anlamına gelmekte iken, maddi anlamda delillerin doğrudan doğruyalığı ilkesi uyarınca, hakim kanaatini oluştururken olabildiğince "olaya yakın" delilleri kullanacak, mümkün olduğunca doğrudan, olayı birinci elden ispat eden delillere dayanarak hükmünü tesis edecektir.[11]

Bu bağlamda, söz konusu ilkeler ışığında delilleri değerlendirecek olan hakim, sanığı mahkum edebilmek için gerekli şartların tamamının bulunduğu kanaatine varmak zorundadır. Zira, sanığın beraat etmesi için suçsuzluğunun sabit olması gerekmez, suçlu olduğunun sabit olmaması yeterlidir.[12] Bu itibarla, toplanan delillerin sanığın suçlu olduğunun kabulünü gerektirmesi halinde hakim sanığı cezalandıracak; aksi durumda, sanığın suçlu olduğuna dair yeterli delil bulunmaması durumunda sanık beraat edecektir.

II. ADLİ BİLİŞİM ve DELİLLERİN TOPLANMASI

Son yıllarda, bilişim hukukuna yardımcı bir disiplin olarak ortaya çıkan adli bilişim, yöntemlerine gerek hukuk gerekse ceza yargılamasında başvurulan ve özellikle delil elde etmeye yarayan önemli bir alandır. Biz, çalışmamızda adli bilişimin bugün için daha etkin rol oynadığı ceza muhakemesi boyutunu ve elektronik delil toplama hususunu ele alacağız. Ancak unutulmamalıdır ki adli bilişim, yakın vadede özel hukuk alanındaki uyuşmazlıkların çözümünde de etkin olacak ve hukuk yargılamasına delil katkısı yapacak, gelişmekte olan bir bilim dalı olarak önemini günden güne arttırmakta olan bir disiplindir.

Ülkemiz için henüz yeni sayılabilecek bir alan olan adli bilişim, özellikle bilgisayar ve bilişim endüstrisinin çok daha ileri olduğu Avrupa ülkelerinde ve ABD'de çok çeşitli alanlarda kullanılmaktadır. Disketlerden, sabit disklerden ve çıkartılabilir disklerden delil elde etme amacıyla veri kurtarma işlemi olan ve dijital delillerin muhteva ettiği bilgileri; delil inceleme prosedürlerini, hukuki ve etik sorumlulukları göz önünde bulundurarak; delilin bütünlüğünü koruyarak ve gerçeği açığa çıkarmak amacıyla; kopyalama, belirleme, çözümleme, yorumlama ve belgeleme süreci olarak tanımlanabilecek adli bilişimde, bu veriler bilgi saklamak amacıyla kullanılan medyaların aktif alanlarında, silinmiş alanlarında veya artık alanlarında bulunmaktadır.[13] Adli bilişimin geniş bir yelpazeye yayılan çalışma alanlarından başlıcaları olarak veri kurtarma, veri imha etme, veri saklama, veri dönüştürme, şifreleme, şifre kırma ve gizlenmiş dosyaların bulunması sayılabilir.[14]

Dünyamızda özellikle son 10-15 yılda bilişim sistemlerine bağlı olarak bilişim teknolojisi de önemli ölçüde gelişmiş ve insanlık teknolojik aygıtlarla birlikte yaşar hale gelmiştir. Elbette geliştirme yeteneği bulunan herkesin bilişim alanına yeni bir cihaz türü dahil edebilmesi mümkün olduğundan, bu alanla ilgili kategori sayısını sınırlandırmak mümkün gözükmemektedir.[15]

Hiç şüphe yok ki, gelişen teknoloji ile birlikte suç ve suçlular da bu gelişmelere paralel bir şekilde değişim göstermişler, bu bağlamda klasik suçların yapısı değişmiş, artık suçların bir çoğu bilişim alanlarında yahut bilişim sistemlerinin araç olarak kullanılması ile işlenir hale gelmiştir. Suç olgusu ve suçlularla mücadele ile suçluların yargılanmasında elde edilecek olan deliller, işin

---

11 **EREM, Faruk**; Diyalektik Açıdan Ceza Yargılaması Hukuku, Ankara, 1986, s. 290 vd.; **KANTAR, Baha**; Ceza Muhakemeleri Usulü, Birinci Kitap, Ankara, 1957, s. 220; **ŞAHİN**, s. 257-259; **YURTCAN**, s. 46.

12 **LEONE**, s. 440; **TOROSLU/FEYZİOĞLU**, s. 172.

13 **SAY, Kubilay**; Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi, Ankara, 2006, s. 16 (Yayımlanmamış yüksek lisans tezi).

14 **KESER BERBER, Leyla**; Adli Bilişim, Ankara, 2004, s. 19 vd.

15 **AKINCI, Hatice / ALIÇ, A. Emre / ER, Cüneyd**; *"Türk Ceza Kanunu ve Bilişim Suçları"*, İnternet ve Hukuk, İstanbul, 2004, s. 162.

içerisine teknoloji ve bilişim sistemleri girdiğinde daha önemli, ancak daha karmaşık bir hal almıştır. Bu itibarla, delil toplama ve değerlendirme sistemi kendine özgü bir nitelik arzeden bilişim suçlarında bu delillerin tespiti ve toplanması konusu adli bilişim alanını ilgilendirmekte olup, toplanması farklı bir rejime hayat veren elektronik deliller ışığında hakim gerekli değerlendirmeyi yapmak durumundadır.[16]

III. ELEKTRONİK DELİLLER

A) Elektronik Delillerin Tespiti

1) Genel Olarak Elektronik Delil

Elektronik deliller (e-delil), "*bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen soruşturma açısından değeri olan bilgi ve verilerdir*."[17] Elektronik delillerin *latent*, yani gizil yapıda olması, onların incelenmesinin uygun cihazlar ve ölçüm aletleri yardımıyla yapılmasını gerektirir. Çünkü içerdiği bilgiler yalnızca insanın duyu organları ile algılanamaz. Örneğin olay yerinde bulunan bir bıçağın, gerçekten bir bıçak olup olmadığını anlamak amacıyla nitel gözlem yapmak yeterlidir. Ancak yasa kapsamına girip girmediğini anlamak için bıçağın boyu ölçülmelidir. Yani nicel gözlem yapılmalıdır. Buna karşın elektronik delillerin içerisindeki dijital verileri anlayabilmek için ise mutlaka bir uzman tarafından, alet ve cihazlar ile nicel gözlemler yapılmalıdır. Çünkü genellikle makine dili ile kodlanmış olan bilgiler yine bir makine tarafından yorumlanmalıdır.[18]

Ceza muhakemesinde kullanılan klasik deliller gözle görülebilir nitelikte, üzerinde el koyma ve muhafaza altına alma kararları verilerek kolayca elde edilebilir deliller iken, bilişim suçlarında söz konusu olan elektronik deliller, klasik delillerden farklı olarak soyut bir yapıya sahiptirler. Şüphesiz ki, elektronik delillerin içerisinde yer aldığı somut bir donanım aygıtı bulunmakta ise de, ceza yargılaması bakımından esas delil teşkil edenler bu donanım aygıtının kendisi değil, içerisinde yer alan dijital nitelikteki delillerdir.

Bu anlamda, dijital aygıtlardan elde edilebilecek ve delil oluşturabilecek nitelikteki elektronik deliller şunlar olabilir:

- Video görüntüleri
- Fotoğraflar
- Yazı dosyaları (Word, Excell, Open Office vb. dosyaları)
- Çeşitli bilgisayar programları
- İletişim kayıtları (SMS, MSN Messenger, GTalk vb. kayıtları)
- Gizli ve şifreli dosyalar veya klasörler
- Dosyaların oluşturulma, değiştirilme ve erişim tarih kayıtları
- Son girilen ve sık kullanılan İnternet siteleri
- İnternet ortamından indirilen (download) dosyalar
- Ve bu türden olup, silinmiş dosya veya klasörler[19]

2) Elektronik Delillerin Bulunduğu Yerler

---

16 **KURT, Levent**; Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, 2005, s. 49 vd.
17 **KESER BERBER**, Adli Bilişim, s. 46.
18 **SAY**, s. 29.
19 http://www.edirnebarosu.org.tr/kutuphane/makaleler/89-adli-bilisim-computer-forensic.html. (15.08.2011)

Elektronik delillerin muhakkak bir elektronik donanım içerisinde bulunmasını gerektiren yapısı, bu delilleri ceza muhakemesinin klasik delillerinden ayıran en önemli özelliklerinin başında gelmektedir. Bu bağlamda, klasik deliller herhangi bir yerde bulunabilen ve herhangi bir şekilde ulaşılabilen delillerken; elektronik deliller yalnızca dijital donanım içerisinde yer alan ve ulaşması mutlaka uzmanlık gerektiren bir takım teknik inceleme ve analiz metotlarına başvurma zorunluluğu doğuran delillerdir. Bu itibarla elektronik deliller çabuk bozulabilir, değişebilir veya değiştirilebilir, kaybolabilir ve yok olabilir niteliktedir.

Gerek toplanması, gerekse muhafaza edilmesi uzmanlık gerektiren çok hassas nitelikteki deliller olan elektronik delillere, şu elektronik donanımlardan ulaşılması mümkündür:

a. Bilgisayar:

Verileri toplama, depo etme ve otomatik olarak işleme tabi tutma özelliğine sahip, donanım ve yazılım ünitelerinden oluşan elektronik düzenler olarak tanımlanabilecek bilişim cihazlarının[20] en önemlisi olan bilgisayar, adli bilişim açısından da hem içerisinden delil elde edilen hem de delil elde etme yöntemlerinde kullanılan bir araç olması nedeniyle elektronik delillerin ve delil elde etme araçlarının başında gelmektedir. Bilgisayarın araç olarak kullanılmasıyla işlenen suçlarda geride bırakılan emareler, bilgisayarların incelenmesinde ortaya konulabilmekte, bu sayede ceza yargılamasında kullanılabilecek yasal bir delil haline getirilmektedir. [21]

Genel olarak donanım ve yazılım kısımlarından oluşan bilgisayarda donanım bilgisayarın maddi yapısı, yani klavyesi, anakartı veya ekran kartı gibi elle dokunulabilir kısımları iken[22]; yazılım ise bilgisayarda elektronik biçimde toplanabilen, depolanabilen, işlenebilen ve bulunan her türlü veri yazılımıdır.[23] Bilgisayardan elde edilebilecek olan elektronik deliller, bilgisayarın her iki kısmından da elde edilebilmektedir.

Bilgisayar donanımında bulunan deliller, *hard disk* adı verilen bilgisayarın hafıza depolama bölümünde, çalışır durumda bulunan bilgisayarın önbelleğinde (*RAM*) bulunabilir. Özellikle bilgisayarların birbiriyle iletişimini sağlayan İnternet ağının günümüzde sahip olduğu yer, delillere ulaşma bağlamında bilgisayar donanımlarına ayrıca bir önem kazandırmaktadır. Bir başka deyişle, bilişim yoluyla suç işleyen bir kişinin oturduğu yerden dünyanın diğer ucunda bir suç işleyebiliyor oluşu, bilgisayarın ve İnternetin adli bilişim ve ceza muhakemesi açısından önemini arttırmaktadır.

Belirttiğimiz gibi, bilgisayarlarda yer alan deliller hafıza depo bölümü olan hard disk üzerinde bulunmaktadır. Çalışmamızda saydığımız elektronik delil olabilecek verilere ek olarak önbellek (*RAM*) kayıtları, sistem kayıt dosyaları, çeşitli zararlı bilgisayar yazılımları (virüs, solucan, *trojan*, *spy* vb.) da delil mahiyetinde bilgisayarda bulunabilir.[24]

Üzerinde delil incelemesi yapılacak olan bilgisayar bir İnternet sunucusu (*hosting PC*) ise[25], içerisinde barındırdığı web sitelerinin kayıtları ve bu sitelerde yayınlanan bütün dosyalar yahut bilgiler de bu hosting hizmeti veren bilgisayarlarda mevcut bulunur ve bunlar da ceza muhakemesi bakımından delil oluşturabilir.

b. İnternet:

---

20 **MALKOÇ, İsmail**; Açıklamalı İçtihatlı Türk Ceza Kanunu, Ankara, 2001, s. 1256; http://www.webopedia.com/TERM/I/IT.html. (15.08.2011)

21 **CİHAN, Erol / YENİSEY, Feridun**; Ceza Muhakemesi Hukuku, İstanbul, 1998, s. 210-211.

22 http://www.webopedia.com/TERM/h/harware/html. (15.08.2011)

23 **AKINCI/ALIÇ/ER**, s. 171; http://www.webopedia.com/TERM/s/software.html (15.08.2011)

24 **KURT**, s. 61 vd.; **LEVIN, Richard;** Bilgisayarda Virüs – Antivirüs, Çev. Ferhat Okan Sezer, Ankara, 1992, s. 27 vd.; **SIRIMCIYAN, Alis**; *"Pusuda Bekleyen Düşmanlar"*, CHIP, 1999, Sayı: 12, s. 156 vd.

25 **SINAR, Hasan**; İnternet ve Ceza Hukuku, İstanbul, 2001, s. 40 vd.

İnternet, kısaca, bilgisayarların birleşerek oluşturduğu bilgisayar ağı olup, dünyanın hemen her ülkesinin birbirine bağlı bulunduğu bu ağ üzerinden, bilgisayar ortamında bulunan her türlü veri aktarılabilmektedir.[26]

İnternet ortamındaki veriler de esasen bilgisayarlarda saklanmaktadır. "Sunucu" (*server*) adı verilen ve web hizmeti sunan bu bilgisayarlar, web sitelerine ilişkin kayıtları, kimi bilgileri ve çeşitli dosyaları barındırmaktadır. İnternet ortamında bulunabilecek deliller, bir e-posta, bir İnternet sitesinde yazılmış herhangi bir yorum, makale gibi değişik biçimlerde ortaya çıkabilir. Bunlar da yine ceza yargılamasına delil teşkil edebilecek nitelikte elektronik delillerdir.

c. El Bilgisayarları (PDA, PALM, Pocket PC vb.)

PDA, PALM gibi türleri olan el bilgisayarları da, kullanım özellikleri bakımından birçok işi yapmakta, ajanda işlevi görmekte, çeşitli kelime işlemci programları (Word, Excell vb.) kullanma hizmeti verebilmekte ve hatta kablosuz ağlar vasıtasıyla İnternete girebilmektedir. Bu cihazlarda -hafızasına bağlı olarak- genellikle bilgisayarda bulunabilecek türden veriler bulunmaktadır. Ayrıca kullanım amacına yönelik olarak adres ve telefon bilgileri, ajanda ve yapılacak işler listeleri, İnternete bağlanabiliyorsa girilen web sitelerinin erişim kayıtları ve silinmiş verileri de barındırabileceği gözden kaçırılmamalıdır. Bu tür cihazların bazılarında cep telefonu özelliği de bulunabileceğinden, cihaz inceleme araştırmasının buna göre yapılması, bunun için de delil elde etme işlemini gerçekleştirecek uzman tarafından bu tür cihazların iyi tanınıyor olması gereklidir. Bir el bilgisayarının cep telefonu özelliği barındırması durumunda ayrıca SMS kayıtları ve ajandada mevcut bilgilerin araştırılması da söz konusu olabilmektedir.

Bu cihazlar kendi hafızalarının yanında ayrıca bir kart ile ek hafızaya da sahip olabildiklerinden, bu hususların muhakkak bilinmesi ve elektronik delil analizi işlemlerinde dikkate alınması gereklidir.[27]

d. Cep Telefonları

İnsanın günlük kullanımında taşıdığı önem tartışılmaz bir hale gelen cep telefonları, teknolojinin ilerlemesiyle daha da gelişmiş, İnternete bağlanabilirlikten 3G teknolojisi sayesinde görüntülü konuşmaya kadar birçok özelliği barındırır hale gelmiştir. Cep telefonları, gerek mevcut ve gerek silinmiş kısa mesajlar (SMS), telefon rehberi kayıtları, son aramalar listeleri gibi emarelerin yanı sıra, kapasitesine bağlı olarak, müzik ve fotoğraf dosyaları, videolar, kelime işlemci program ve belgeleri, web site erişim kayıtları ve benzeri dokümanlar barındırabilir ve bunların hepsi suçluların tespiti veya cezalandırılmasında delil niteliği taşıyabilir.

Bununla beraber, günümüzde içerisinde word, excell dosyalarından binlerce sayfalık e-kitaplara kadar sayısız veri bulundurma özelliğine sahip olan, görüntülü konuşmanın ve İnternete bağlanabilmenin mümkün olduğu yeni teknoloji cep telefonlarının bir bilgisayardan farkı bulunmamaktadır. Buna karşın, uygulamada Ceza Muhakemesi Kanunu'nda düzenlenen koruma tedbirlerinin tatbiki sırasında, şüphelilerin bilgisayarlarına el konulması CMK md. 134'teki özel rejime tabi tutulurken, bilgisayar olarak kabul görmeyen cep telefonları niteliksiz suç eşyasıyla aynı muameleye tabi tutulmaktadır. Bu durumun yarattığı sorunlara çalışmamızın sonraki bölümlerinde değineceğiz.

---

26 **AKINCI/ALIÇ/ER**, s. 166.

27 http://www.edirnebarosu.org.tr/kutuphane/makaleler/89-adli-bilisim-computer-forensic.html. (18.08.2011)

e. Hafıza kartları, taşınır bellekler, CD ve DVD'ler:

Hafıza kartları (*flash disk, flash drive*) çeşitli türlere sahip olup, değişik donanımlarda, kullanımına bağlı olarak kapasiteleri de değişkenlik gösterebilen teknolojik aygıtlardır. Bir depolama veya yedekleme birimi olarak tasarlanan hafıza kartları, kapasitesine bağlı olarak her türlü dosya ve veriyi içerebilir. Çeşitli amaçlarla kullanılabilen hafıza kartları üzerinde web tasarımcılar, web site deneme çalışmaları yapmakta ve bunun için birtakım yazılımlar yüklemektedirler (*localhost*). Hafıza kartını bir web sunucu gibi kullanmaya yarayan bu yazılımların çalıştırılması durumunda delil niteliği taşıyabilecek önemli verilere ulaşılabilmektedir.[28]

Ayrıca hafıza kartlarının sürekli olarak değişiklik arzeden yapısı bize bir takım ipuçları da sunabilir. Örneğin inceleme konusu kartın yalnızca fotoğraf makinelerinde kullanılabilir türden oluşu, delil tespiti yaparken işe yarayabilecek önemli bir bilgidir.

Taşınır bellekler ile CD ve DVD'ler konusunda da, genel olarak hafıza kartları için söylenenlerin geçerli olduğunu ve bu araçların da içerdikleri veriler bakımından ceza muhakemesinde önemli delil elde etme vasıtaları olduğunu söylemek yanlış olmayacaktır.

f. Diğer Elektronik Donanımlar:

Yukarıda sayılanlar dışında, daha birçok elektronik donanımda elektronik delillere ulaşılması mümkün olup, gelişen ve yenilenen teknoloji düşünüldüğünde bu deliller bakımından sınırlayıcı bir tasnif yapmak imkansızdır. Günümüzde ceza muhakemesi bakımından önem arzeden elektronik delilleri kısaca sayacak olursak; MP3 çalarlar, yazıcı, faks ve fotokopi makineleri, kamera ve fotoğraf makineleri, modemler, GPS'ler (küresel konumlama cihazları), kredi kartı kopyalama aletleri gibi donanımlar da ceza yargılaması açısından önemli elektronik deliller içerebilmesi mümkün olan dijital araçlardır.

B) Elektronik Delillerin Toplanması

1) Adli Bilişim Aşamalarında Delil Toplamanın Yeri

Bilişim suçları alanında elektronik delillere ulaşılması ve bunların toplanarak muhafaza altına alınması kendine özgü nitelikler arzetmektedir. Örneğin, insan öldürme fiilinin gerçekleştiği bir olay yerinde bulunan ateşli silahın, işlenen suça ilişkin bir delil niteliği taşımasının yüksek ihtimal dahilinde olması nedeniyle bu delil kolayca muhafaza altına alınarak, gerekli balistik ve diğer incelemelerin yapılabilmesi için adli tıp kurumuna götürülür. Ancak toplanacak olan deliller elektronik deliller olduğunda, durum farklılaşmakta ve karmaşıklaşmaktadır.

Elektronik deliller, somut aygıtların içerisinde bulunan soyut verilerden meydana gelmektedir. O halde, içerisinde delil bulunduğu şüphesiyle muhafaza altına alınan bir elektronik aygıtın içerisinde suç delilinin bulunup bulunmadığı, hiçbir zaman kesin olarak belirli olmamaktadır. Dolayısıyla elektronik delillerin toplanmasında ortaya çıkan ilk önemli zorluk, delil olarak düşünülen aygıtların suça ulaşmada vasıta olup olamayacakları hususundaki belirsizliktir. Adli bilişimde, klasik delillerden farklı olarak, toplanan elektronik delillerin incelenmesi, değerlendirilmesi ve analizi de oldukça karmaşık, teknik uzmanlık gerektiren ve masraflı bir iştir.

---

28 http://www.edirnebarosu.org.tr/kutuphane/makaleler/89-adli-bilisim-computer-forensic.html. (18.08.2011)

Adli bilişimde, ulaşılan elektronik delillerin ceza yargılamasında kullanılacak hukuki delile dönüşme sürecine *adli bilişim safhaları* adı verilmektedir. Adli bilişim safhaları, bu hususta kimi görüş ayrılıkları olmasına karşın[29], genel itibariyle dört aşamada incelenmektedir:[30]

1. Toplama (*Collection*)

2. İnceleme (*Examination*)

3. Çözümleme (*Analysis*)

4. Raporlama (*Reporting*)

Biz, çalışmamızın sınırları gereği söz konusu safhalardan yalnızca delillerin toplanması aşamasını inceleyeceğiz.

2) Elektronik Delillerin Toplanma Aşaması

Ceza muhakemesi hukukunda, delillerin toplanmaya başlanabilmesi için öncelikle kanunun öngördüğü yasal durumun oluşması gerekmektedir. Söz konusu yasal durum Ceza Muhakemesi Kanunu'nun 116. maddesinde "*Yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe varsa; şüphelinin veya sanığın üstü, eşyası, konutu, işyeri veya ona ait diğer yerler aranabilir.*" şeklinde düzenlenmiştir. Eğer söz konusu yasal şart somut olayda mevcutsa bu durumda CMK md. 119'a göre arama kararı verilmesi gerekmektedir. Arama kararı verilebilmesinin şartları CMK md. 119'da şu şekilde düzenlenmiştir:

"*(1) Hâkim kararı üzerine veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının yazılı emri ile kolluk görevlileri arama yapabilirler.*

(2) Arama karar veya emrinde;

a) Aramanın nedenini oluşturan fiil,

b) Aranılacak kişi, aramanın yapılacağı konut veya diğer yerin adresi ya da eşya,

c) Karar veya emrin geçerli olacağı zaman süresi,

Açıkça gösterilir.

(3) Arama tutanağına işlemi yapanların açık kimlikleri yazılır. Arama sonucunda bazı eşyaya elkoyma söz konusu olduğunda 127 nci maddenin birinci fıkrası hükmü uygulanır.

(4) Cumhuriyet savcısı hazır olmaksızın konut, işyeri veya diğer kapalı yerlerde arama yapabilmek için o yer ihtiyar heyetinden veya komşulardan iki kişi bulundurulur.

(5) Askerî mahallerde yapılacak arama, hâkim veya Cumhuriyet savcısının istem ve katılımıyla askerî makamlar tarafından yerine getirilir."

---

29 Adli bilişim safhalarını beş aşamada inceleyen yazarlar da mevcuttur. KESER BERBER'e göre, adli bilişim safhaları ***Toplama***, ***İnceleme***, ***Analiz Etme***, ***Belge Hazırlama*** *ve* ***Raporlama*** olmak üzere beş aşamadan oluşmaktadır. (**KESER BERBER**, Adli Bilişim, s. 45)

Aynı şekilde, ŞEN de adli bilişim safhalarını ***Delil Tespit Etme***, ***Delil Toplama – Muhafaza Etme*** *(Evidence Collection and Preservation),* ***Delil Çıkartma*** *(Evidence Extraction),* ***Delil İnceleme*** *(Evidence Examination / Analysis) ve* ***Delil Organize Etme / Raporlama*** *(Evidence Organization)*olmak üzere beş aşamaya ayırmaktadır. (**ŞEN, Osman Nihat;** "*Adli Bilişim Bilimi ve Diğer Bilimlerle Olan İlişkisi"* http://www.bilgisayarpolisi.com/index.php?sayfa=makaleoku&kategori=11&id=121 (18.08.2011)

30 **KARAGÜLMEZ, Ali**; Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri, Ankara, 2009, s. 252.

Ancak, CMK'nun söz konusu maddesi klasik suçlara ilişkin genel bir arama rejimi ihtiva etmektedir. Oysa bilişim sistemlerinin kullanılması suretiyle işlenen suçlarda yahut klasik suçlara ilişkin delillerin bilgisayar sistemlerinde bulunma ihtimalinin söz konusu olduğu durumlarda, bilgisayarlarda yapılacak arama CMK md. 134'te özel olarak düzenlenmiş olup, bu hallerde arama kararının yalnızca hakim tarafından verilebileceği öngörülmüştür. Buna göre, "*Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, 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.*"

Şu unutulmamalıdır ki, delil araştırmasının bu aşamasında CMK tarafından öngörülen usule eksiksiz bir biçimde uyulması delillerin hukuki olması ve ceza yargılamasında verilecek hükme esas teşkil edebilmesi açısından son derece önemlidir.

Elektronik delillerin toplanmasında, klasik delillerde olduğu gibi olay yeri öne çıkmaktadır. Zira delillerin sağlıklı bir şekilde toplanabilmesi, olay yerine yapılan ilk müdahalenin sağlıklı olup olmamasıyla paralellik göstermektedir. Adli Önleme ve Aramaları Yönetmeliği'ne dayanarak olay yeri incelemesini; suçun aydınlatılması amacıyla olay yerlerinde her türlü iz, eser, emare ve delil niteliği taşıyabilecek bulguların uzmanlaşmış personelce, çeşitli bilimsel, teknik yöntem ve metot kullanarak araştırılması, elde edilen bulguların tespit edilmesi ve kayıt altına alınması (belgelenmesi), toplanması, muhafazası ve incelenmek üzere ilgili yerlere gönderilmesini sağlayan özel amaçlı bir araştırma işlemi olarak tanımlamak mümkündür.[31] Bu gibi durumlarda, klasik suçlarda söz konusu olduğu gibi, olay yerinin güvenliğinin sağlanması ve delillerin toplanması ile ilgisi bulunmayan kişilerin olay mahallinden uzaklaştırılması önem taşımaktadır. Bu şekilde, delil elde edilecek elektronik donanımların korunabilmeleri ve elde edilmesi amaçlanan delillerin zarar görmemesi sağlanabilmektedir. Bu aşamada yapılacak en doğru şey, delil toplaması için olay yerine bir adli bilişim uzmanının getirilmesi olacaktır. Bu gibi durumlarda adli bilişim uzmanı delil kaybı ihtimalini asgariye indirerek elektronik delilleri toplayabilecektir.[32]

Ancak olay yerinde elektronik delillerden farklı olarak klasik suç delillerinin yer alması da kuvvetle muhtemeldir. Özellikle söz konusu bir bilgisayar olunca, klavye ve fare (*mouse*) üzerinde bulunabilecek parmak izleri, mahalde bulunan şüpheliye ait giysiler, eşyalar vb. unsurlar da birer delildir. Bu nedenle, bu aşamada delil toplanırken kriminalistik inceleme de ihmal edilmemelidir. Ancak bu, toplanması ve incelenmesi azami hassasiyet gerektiren potansiyel dijital delillere zarar vermeden yapılmalıdır.[33] Örneğin, bir CD üzerinde yapılacak parmak izi araştırması, kullanılan kimyasallar CD'nin içerisindeki bilgilerin kaybını doğurabileceğinden, klasik suçlara ilişkin kriminal veri toplama ile adli bilişim verileri toplama arasında makul bir denge tutturulmalı, birine ilişkin inceleme yapılırken diğeri ile ilgili potansiyel delillere zarar verilmemeli ve mümkünse klasik delil toplanırken kullanılacak olan kimyasal maddelerin kullanımı, elektronik delilin kurtarılması işlemi tamamlanıncaya kadar ertelenmelidir.[34]

Eğer yapılan olay yeri incelemesi sonrasında potansiyel delillerin bulunduğu bilgisayar muhafaza altına alınacaksa, söz konusu aygıtların hassas yapıları gereği paketlenmesi, taşınması gibi hususlara özen gösterilmeli; söz konusu araçlar sarsıntı, elektrik akımı, elektromanyetik

---

31 **SAY**, s. 22.

32 Adli bilişim uzmanı ve nitelikleri hakkında ayrıntılı bilgi için Bkz. **KESER BERBER, Leyla;** "Adli Bilişim Uzmanı Kimdir?", http://turk.internet.com/haber/yaziyaz.php3?yaziid=16728. (17.08.2011)

33 **KARAKUŞ, Oğuz**; Kriminalistik, Ankara, 2009, s. 512-513.

34 **KARAKUŞ**, s. 513; **ÖZDİLEK, Ali Osman**; Bilişim Suçları ve Hukuku, İstanbul, 2006, s. 221.

ortamlar, aşırı sıcak, sıvı maddelerle temas gibi işlevlerini olumsuz yönde etkileyecek ve delil niteliğini ortadan kaldıracak zararlı etkilerden korunmalıdır.[35]

Elektronik deliller üzerinde yapılacak incelemeler, donanımlar üzerinde değil, bunlardan alınan kopyalar üzerinde yapılmalıdır. Bu metot, söz konusu elektronik donanımlar içerisinde oluşması muhtemel veri kayıplarını önlemeye yönelik delil toplama sürecine katkı sağlayacaktır.[36] Bilgisayarlardan inceleme yapılmak üzere kopya alınacağı durumlarda uyulacak olan rejim, CMK'nun 134. maddesinin 2., 3., 4. ve 5. fıkralarında düzenlenmiştir. Buna göre; bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir. Ancak şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, el konulan cihazlar gecikme olmaksızın iade edilir. Bu aşamada önem arzeden husus, 134. maddenin 3. fıkrasındaki bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesinin yapılacağı yönündeki zorunluluktur. Söz konusu kurala riayet edilmediği takdirde, elde edilen delil hukuka aykırı bir delil olacaktır.

Adli bilişimde, elektronik donanımların içerisinden yapılan birebir kopyalama işlemine imaj (*forensic image*) adı verilmektedir. Bu kopyalama işlemi, sistemdeki tüm verilerin özel yazılımlar kullanılmak suretiyle ve düşük seviye bit bazında başka bir ortamda bir örneğinin (*imajının yahut görüntüsünün*) oluşturulması ile yapılmaktadır. Burada düşük seviye bit bazında kopyalama yapılmasının nedeni, daha sonra yapılacak incelemelerde silinmiş, değiştirilmiş veya bozulmuş verilere de ulaşma olanağının bulunuyor olmasıdır. Söz konusu imaj alma işlemi yapılırken, manyetik yahut optik medyaların *bit-to-bit* (*sector-by-sector*) imajı alınmakta, orijinal medya üzerinde herhangi bir değişiklik yapılmamakta ve alınan imajların bütünlüğünün sağlanması *hash* değerleri hesaplanarak yapılmaktadır.[37]

Delil çıkartma aşamasında, silinen dosya, klasör ve bölümler (*partition*) kurtarılmakta, medya üzerindeki *swap* alanından, *slack* alanlardan, *unallocated* bölümlerden, geçici dosyalardan delil olabilecek veriler çıkartılmaktadır. Ayrıca, *hash* fonksiyonları kullanılarak bilinen dosyalar (*known files*) elimine edilerek, incelenecek dosya sayısı azaltılmaktadır. Delil çıkartma aşamasında, medyadan delil olabilecek dosyalar çıkartılmış olmaktadır.

Delil çıkartma işlemleri aşağıdaki başlıklarda sıralanabilir:

- Mevcut Dosya Araması
- Silinmiş Dosya Araması
- *Unallocated* Alandan Dosya Araması
- Kelime Araması
- İnternet işlemleri
- *Link* dosyaları
- *Print Spool* Dosyaları
- *Registry* İncelemesi
- Dosya İmza Analizi
- *Hash* Analizi
- Geri Dönüşüm Kutusu Kurtarma

---

35 El konulan bilgisayar donanımının el konma ve taşınma işlemleri esnasında dikkat edilmesi gereken hususlar hakkında bilgi için Bkz. **SAY**, s. 39-41.

36 **EKİZER, Ahmet Hakan**; "Adli Bilişim", http://www.ekizer.net/content/view/16/1/ (16.08.2011)

37 **ŞEN**, a.g.e. (18.08.2011)

- *Swap* Dosyası
- *Unused Disk Area*
- Windows Açılışında Otomatik Çalışan Programlar
- Saklanmış Bölümler (*Hidden partitions*)[38]

IV. CEZA MUHAKEMESİNDE ELEKTRONİK DELİLLERİN TOPLANMASINA İLİŞKİN YAŞANAN SORUNLAR

Ceza muhakemesinde, elektronik delil elde etmede en çok kullanılan koruma tedbiri CMK md. 134'te düzenlenen bilgisayarlarda ve bilgisayar kütüklerinde arama, kopyalama ve el koyma tedbiridir. Bu hükme göre, bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, 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. Ne var ki, uygulamada bu tedbirin uygulanmasıyla ilgili birçok sorun ortaya çıkmaktadır.

Bu sorunların başında, elektronik delil elde etme amacıyla, hakim kararıyla bilgisayarlara el koyan kolluk kuvvetlerinin CMK md. 134'te yer alan hususlara uygun işlem yapmaması gelmektedir. Zira bu hüküm uyarınca bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir. Ancak şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, el konulan cihazlar gecikme olmaksızın iade edilir. Bununla beraber bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. İstenmesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır. Bilgisayar veya bilgisayar kütüklerine el koymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır. (CMK md. 134/2, 3, 4, 5)

Bu koşullardan, özellikle, bilgisayarlara el konulması esnasında sistemdeki bütün verilerin yedeklemesinin yapılması ve talep edilmesi halinde bu yedekten bir kopyanın şüpheliye veya vekiline verilmesi çok önemlidir. Zira, söz konusu yedekleme işlemi yapılmaz ve kişinin bilgisayarına öylece el konulursa, sistemde değiştirilmesi son derece basit olan verilerin, bilgisayarına el konulan kişi aleyhine değiştirilmesi durumunda kişinin hiçbir güvencesi kalmayacak ve bu durum neticesinde kişi en temel hak ve özgürlüklerine halel gelecek biçimde mağdur olabilecektir. Nitekim, CMK'nda yer alan koruma tedbirleri kişilerin temel hak ve özgürlüklerini kısıtlayıcı tedbirler olduğundan, bu tedbirler uygulanırken muhakeme yönünden doğabilecek zararın ağırlığı ve bunun gerçekleşmesi ihtimalinin yoğunluğu ile orantılı olması gerekliliğinin yanı sıra[39], tedbir uygulanırken aleyhine uygulanan kişinin temel hak ve özgürlüklerinin hukuki sınırları aşar biçimde sınırlandırılmamasına ve kişisel verilerinin zarar görmemesine dikkat edilmesi gerekmektedir. Zira, özellikle CMK md. 134'teki koruma tedbirinin uygulanmasında, ceza muhakemesinin amacına uygun bir şekilde kişisel verilerin korunması, tedbiri uygulayan makamların birincil görevi olmalıdır.[40]

5271 sy. CMK'nun yanında, 5070 sy. Elektronik İmza Kanunu, Polis Vazife ve Salahiyet

38 **ŞEN**, a.g.e. (18.08.2011)
39 **TOROSLU/FEYZİOĞLU**, s. 211.
40 **KÜZECİ, Elif**; Kişisel Verilerin Korunması, Ankara, 2010, s. 291 vd.

Kanunu, Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik ve Telekomünikasyon Sektöründe Tüketici Hakları Yönetmeliği gibi birçok hukuki düzenlemede ve OECD, Avrupa Konseyi, Birleşmiş Milletler ve Avrupa Birliği'nin de birçok düzenlemesinde kişisel verilerin korunması titizlikle hüküm altına alınmıştır.[41] Buna karşın, uygulamada CMK hükmündeki hususlara, özellikle de yedekleme zorunluluğuna dikkat edilmemesi ve buna paralel olarak kişisel verilere zarar verilmesi, elektronik delillerin toplanması ile ilgili sorunların başında gelmektedir.

Bir başka ve önemli sorun ise, cep telefonlarına el konulması biçiminde tezahür eden koruma tedbirinin uygulanmasında ortaya çıkmaktadır. CMK md. 134, yalnızca bilgisayar ve bilgisayar kütüklerinde yapılacak arama, kopyalama ve el koyma işlemlerinden bahsetmektedir. Bu nedenle, bilgisayar dışındaki eşyalar üzerinde yapılacak arama ve el koyma işlemleri, CMK md. 116 – 129 hükümleri uyarınca yapılmaktadır. Buna göre, yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe varsa; şüphelinin veya sanığın üstü, eşyası, konutu, işyeri veya ona ait diğer yerler, hâkim kararı üzerine veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının, Cumhuriyet savcısına ulaşılamadığı hallerde ise kolluk amirinin yazılı emri ile aranabilir. Bununla beraber, hâkim kararı üzerine veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının, Cumhuriyet savcısına ulaşılamadığı hallerde ise kolluk amirinin yazılı emri ile kolluk görevlileri, el koyma işlemini gerçekleştirebilir. (CMK md. 127) Buna göre, CMK md. 134'ten farklı olmak üzere, bilgisayar dışındaki eşyalara el konulması hakim dışında Cumhuriyet savcısı ve ona ulaşılamaması durumunda kolluk amirinin vereceği yazılı emir ile mümkün olabilmektedir.

Ancak günümüzde, gelişen teknoloji ile birlikte, elektronik donanımı düşünüldüğünde birçok cep telefonu bilgisayardan farksız olup, bir bilgisayarla yapılabilecek her şey (İnternet bağlantısı, e-posta haberleşmesi, kelime işlemci programlarının kullanımı, veri saklanması vb.) yeni teknoloji cep telefonlarıyla da yapılabilmektedir. Ne var ki, bir suç şüphesinin var olduğu durumlarda, bilgisayarlardan farklı olmak üzere, cep telefonlarına kolluk amirinin yazılı emriyle el konulabilmekte ve bu el koyma işlemi esnasında hiçbir şekilde yedekleme vb. önlemlere başvurulmamaktadır. Hiç şüphe yok ki, uygulamadaki bu sorun, yukarıda bahsettiğimiz temel hak ve özgürlüklere doğrudan zarar verici nitelikte olup, kişilerin kişisel verilerinin ve özel hayatlarının gizliliğine de evrensel hukuka aykırı bir biçimde müdahale anlamına gelmektedir.[42]

Elektronik deliller, kişilerin kişisel verilerini barındıran ve tamamen özel hayatına ilişkin eşyalarında (bilgisayar, cep telefonu vb.) yer aldığından, bunlara yapılacak ulusal ve evrensel hukukun sınırlarını aşar bir müdahale, iç hukukta ve bilhassa uluslararası hukukta koruma altına alınan *"özel hayatın gizliliği hakkı"*nı da ihlal etmektedir. Elbette, özel hayatın gizliliği hakkı çeşitli hukuki temellere dayandırılabilmektedir. Ancak konumuzla ilgili olarak, özel hayatın gizliliği hakkı, teknolojik gelişmeler karşısında kişinin güvenliğinin güvence altına alınması anlamında tanımlanabilir.[43] Ne var ki, uygulamadaki bu sorunlar, kişilerin özel hayatlarının gizliliğini de ihlal edici nitelik taşımakta olup, yapılacak yasal düzenlemeler ve bunların yetkili makamlarca takibi ile bu sorunlar asgari düzeye indirilebilir. Bunun için, elektronik delil temin ederken CMK'ndaki hususlara dikkat etmeyen kolluk görevlileri bakımından caydırıcı yaptırımlar getirilmesi ve bahsettiğimiz ikinci hususla ilgili olarak, cep telefonlarının ve bilgisayar işlevi gören benzeri teknolojik aygıtların, arama ve el koyma tedbirleri bakımından CMK md. 134 kapsamına sokulması, bu sorunların çözümü için atılacak ilk adımlar olacaktır.

---

41 **KESER BERBER, Leyla / LOSTAR, Murat**; Bilişimde Biyometrik Yöntemler, Ankara, 2006, s. 82 vd.

42 **KÜZECİ**, s. 296 vd.; **UÇKAN, Özgür / BECENİ, Yasin**; *"Bilişim-İletişim Teknolojileri ve Ceza Hukuku"*, İnternet ve Hukuk, İstanbul, 2004, s. 372.

43 **ER, Cüneyd**; Biyometrik Yöntemler ve Özel Hayatın Gizliliği Hakkı, Ankara, 2007, s. 79.

V. ULUSLARARASI HUKUKTA ELEKTRONİK DELİLLERİN TOPLANMASINDA UYULACAK İLKELERE İLİŞKİN DÜZENLEMELER VE GÜNCEL SORUNLAR

Avrupa Birliği'nin 24 Ekim 1995 tarihli ve 95/46/EC sayılı yönergesi uyarınca, verilerin yalnız açıkça ve hukuka uygun olarak belirlenmiş bir amaç için toplanması ve işlenmesi mümkündür. Dolayısıyla bu amacın yazılı olarak belirlenmesi ve kesin bir biçimde ortaya konulması gerekmektedir. Ayrıca illiyet ilkesi uyarınca, toplanan verilerin ancak söz konusu amaç için gerekli olmaları halinde işleme konulmaları mümkündür. Yine elde edilen verilerin saklanma süresi de, bu amaç doğrultusunda belirlenmeli, belirlenen makul süre içerisinde güncel ve doğru kalmaları güvence altına alınmalıdır.[44]

Bununla beraber, elektronik delillerin toplanmasında dikkat edilecek en önemli hususlar olan kişisel verilerin korunması ilkesi ve özel hayatın gizliliği hakkı da, uluslararası hukuk metinlerinde düzenlenmiş ve güvence altına alınmıştır. Birleşmiş Milletler (BM) İnsan Hakları Evrensel Beyannamesi'nin 12. maddesi başta olmak üzere, BM Medeni ve Siyasi Haklara Dair Uluslar arası Misak'ın 17. maddesi, BM'nin çeşitli tarihlerde çıkarttığı Kişisel Verilerin Korunmasına Dair İlke Kararları'nda, OECD'nin çeşitli tarihlerde çıkartmış olduğu ilke kararlarında[45], Avrupa Birliği Yönergelerinde, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde, Avrupa Konseyince çıkartılan Kişisel Verilerin Korunmasına Dair Avrupa Konseyi Sözleşmesi'nde ve daha birçok Uluslar arası metinde özel hayatın gizliliği ve kişisel verilerin korunması güvence altına alınmış olup, elektronik deliller toplanırken uygulanacak olan tedbirler ve yapılacak olan işlemlerin bütün aşamalarında, ulusal ve uluslararası mevzuatta yapılan düzenlemelere ve konulan kurallara riayet edilmesi gerekmektedir.[46]

Avrupa ülkelerindeki teknolojik gelişmelerin ülkemize göre daha ileri düzeyde olduğu gerçeğine paralel olarak, siber suçlar ve bilişim sistemlerine yapılan saldırıların sayısı da gün geçtikçe artmaktadır. Örneğin, Alman Federal Hükümetinin açıkladığı resmi verilere göre, yalnızca Almanya'da bir günde yaklaşık 43 bin sanal saldırı meydana gelmektedir.[47] Bu bağlamda, 23.11.2001'de Budapeşte'de imzalanan Avrupa Konseyi Siber Suçlar Sözlşemesi'nin 25. maddesine göre, sözleşmenin imzacısı olan ülkeler, siber suçların faillerinin ortaya çıkarılabilmesi için elektronik delillerin toplanması konusunda birbirlerine her türlü yardımı göstermek durumundadırlar. Bunun yanında, Kasım 2009'da da Avrupa Komisyonu bir devletten diğer devlete delil toplanması ile ilgili bir "*Green Paper*"[48] yayınlamış, bu bağlamda devletler arası delil toplanması konusundaki yardımlaşmanın artması amacıyla bir ortak kabul (*mutual recognition*) mekanizması oluşturulmuştur.[49] Ne var ki bu konuyla ilgili Avrupa Konseyi'nde ve akademik alanda tartışmalar devam etmekte olup, konunun bir ortak kabulden ziyade ortak yardımlaşma (*mutual legal assistance*) ağı oluşturularak çözümlenmesi gerektiği, ülkelerin hukuk sistemlerini birbirleriyle ortaklaştırmalarındansa birbirlerinden yarım isteyerek her ülkenin kendi hukuk düzenine uygun bir biçimde diğer ülkenin istediği elektronik delilleri toplayarak diğerine vermesi gerektiği söylenmektedir.[50]

Bununla birlikte, özellikle Almanya siber suçlarla mücadele ve buna ilişkin elektronik

---

44 **ER**, s. 87.

45 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD, http://www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html. (22.08.2011)

46 **ER**, s. 79-103; **KESER BERBER/LOSTAR**, s. 94-98. Ayrıca söz konusu uluslararası düzenlemelere ilişkin detaylı bilgi için Bkz. **KÜZECİ**, s. 116 vd.

47 http://www.veteknoloji.com/almanya-siber-guvenlik-kararghi-kuruyor-39333—0.html. (24.08.2011)

48 Avrupa Birliği politkaları hakkında hazırlanan ve içerisinde işlemin konusuna ilişkin kimi teklifleri barındıran düzenleyici işlemler.

49 **SPENCER, John R.**; "The Green Paper on obtaining evidence from one Member State to another and securing its admissibility: the Reaction of one British Lawyer", http://www.zis-online.com/dat/artikel/2010_9_492.pdf, s. 602. (24.08.2011)

50 **SPENCER**, s. 604-606.

delillerin toplanması konusunda çalışmaların yapıldığı ve yoğun tartışmaların yaşandığı ülkelerin başında gelmektedir. Bu ülkede, açıklanan resmi rakamlara göre günde ortalama 43 bin sanal saldırı olmakta, siber suçlulukla mücadelede devletin yetersiz kaldığı eleştirileri yapılmaktadır. Yakın zamanda Alman İç İşleri Bakanlığı bu saldırılarla mücadele etmek amacıyla "Uzaktan Adli Yazılım" (*Remote Forensic Software*) adı verilen bir *Trojan* tasarlayarak, siber suç faili olduğundan şüphelenilen kişilerin bilgisayarlarına girme konusunda çalışmalar yapmaya başlamıştır.[51] Ancak Alman Federal Hükümetinin bu çalışmaları, oluşturulan yazılımla yalnızca "şüpheli hareketler" tespit edileceğinden, bu yolla yanlış delillere de gidilebileceği ve birçok kimsenin bu nedenle iletişim özgürlüğünün ve daha birçok temel hak ve özgürlüğünün kısıtlanacağı yönünde eleştirilere neden olmuş; buna rağmen, Alman hükümeti birkaç yıl önce çıkardığı yasayla siber suçlulukla mücadele adına elektronik delillere ulaşılabilmesi amacıyla üzerinde suç şüphesi olduğu düşünülen kişilerin bilgisayarlarına, telefonlarına, e-posta adreslerine girmesini kolaylaştırmış ve bu bağlamda, federal polisin gözaltı ve soruşturma yetkilerini arttırmıştır. Yasa çıktıktan sonra da Alman Meclisinde ve basında sıkça tartışılmış, muhalefet söz konusu yasaya kişilerin Anayasa tarafından garanti altına alınan en temel haklarının ihlal edildiği ve Doğu Almanya istihbarat birimi olan *Stasi*'ye benzer bir denetim mekanizmasının yaratıldığı gerekçesiyle karşı çıkmıştır.[52]

Ancak bütün bu düzenlemelere ve tartışmalara rağmen alınan tedbirler ve çıkarılan yasalar Almanya'da siber suçlulukla mücadele ve delillere ulaşma konusunda yeterli olmamış, bu nedenle henüz birkaç ay önce Federal hükümet tarafından bir "siber güvenlik stratejisi" hazırlanarak Köln'de bir "Siber Savunma Merkezi" kurulmuştur.

VI. SONUÇ

Ceza Muhakemesindeki klasik delillerden farklı olarak, özellikle bilişim suçlarının ispatlanmasında önem kazanan, bilgisayarlar başta olmak üzere birçok bilişim sisteminin içerisinden elde edilebilen ve tespiti ve toplanması özel uzmanlık gerektiren elektronik deliller, gerek iç hukuktaki kuralların ihlaline yol açabilecek, gerekse uluslararası hukuk metinlerinde öngörülen ve teminat altına alınan önemli insan hakları ilkeleriyle çatışma yaratabilecek sorunlar ortaya çıkarabilmektedir. Özellikle, 5271 sayılı CMK'nun bilgisayarlarda yapılacak aramalara ilişkin kurallarına uyulmaması, özel hayatın gizliliği ve kişisel verilerin korunması gibi evrensel insan hakları metinleriyle güvence altına alınmış ilkelerin ihlali sonucunu ortaya çıkarabilmektedir.

Şüphesiz ki, bu sorunların çözümünün ilk adımı olarak başta Ceza Muhakemesi Kanunu olmak üzere kanun hükümlerinde hem gelişen yeni teknolojinin ihtiyaçlarına cevap verebilecek, hem de bireylerin güvenliğini ve özel hayatlarının gizliliğinin korunmasını ön plana alacak yeni düzenlemeler yapılmalıdır. Ne var ki, kanunlardan doğan sorunların çözümünde söz konusu kanun metinlerinin değiştirilmesi yetmemekte, o kanunun uygulayıcılarının da görevlerini yerine getirirken titiz bir şekilde, kanundan doğan yetkileri kötüye kullanmadan ve insanlığın evrensel kazanımlarına zarar vermeden hareket etmeleri gerekmektedir. Zira, o ünlü vecizede söylendiği gibi, *"En iyi kanun kötü uygulayıcının elinde kötü sonuçlar doğururken, en kötü kanun bile iyi uygulayıcının elinde mucizeler yaratır."*

51 http://www.spiegel.de/international/germany/0,1518,502955,00.html. (24.08.2011)
52 http://www.spiegel.de/international/germany/0,1518,590198,00.html. (24.08.2011)

KAYNAKÇA

AKINCI, Hatice / ALIÇ, A. Emre / ER, Cüneyd; *"Türk Ceza Kanunu ve Bilişim Suçları"*, İnternet ve Hukuk, İstanbul, 2004.

CİHAN, Erol / YENİSEY, Feridun; Ceza Muhakemesi Hukuku, İstanbul, 1998.

EKİZER, Ahmet Hakan; *"Adli Bilişim"*, http://www.ekizer.net/content/view/16/1/ (16.08.2011)

ER, Cüneyd; Biyometrik Yöntemler ve Özel Hayatın Gizliliği Hakkı, Ankara, 2007.

EREM, Faruk; Diyalektik Açıdan Ceza Yargılaması Hukuku, Ankara, 1986.

FEYZİOĞLU, Metin; Ceza Muhakemesi Hukukunda Tanıklık, Ankara, 1996.

FEYZİOĞLU, Metin; Ceza Muhakemesinde Vicdani Kanaat, Ankara, 2002.

KANTAR, Baha; Ceza Muhakemeleri Usulü, Birinci Kitap, Ankara, 1957.

KARAGÜLMEZ, Ali; Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri, Ankara, 2009.

KARAKUŞ, Oğuz; Kriminalistik, Ankara, 2009.

KESER BERBER, Leyla; Adli Bilişim, Ankara, 2004.

KESER BERBER, Leyla; *"Adli Bilişim Uzmanı Kimdir?"*, http://turk.internet.com/haber/yaziyaz.php3?yaziid=16728. (17.08.2011)

KESER BERBER, Leyla / LOSTAR, Murat; Bilişimde Biyometrik Yöntemler, Ankara, 2006.

KETİZMEN, Muammer; Türk Ceza Hukukunda Bilişim Suçları, Ankara, 2008.

KUNTER, Nurullah; Ceza Muhakemesi Hukuku, İstanbul, 1989.

KURT, Levent; Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, 2005.

KÜZECİ, Elif; Kişisel Verilerin Korunması, Ankara, 2010.

LEONE, Giovanni; Diritto e Procedura Penale, Napoli, 1988.

LEVIN, Richard; Bilgisayarda Virüs – Antivirüs, Çev. Ferhat Okan Sezer, Ankara, 1992.

MALKOÇ, İsmail; Açıklamalı İçtihatlı Türk Ceza Kanunu, Ankara, 2001.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD, http://www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html. (22.08.2011)

ÖZDİLEK, Ali Osman; Bilişim Suçları ve Hukuku, İstanbul, 2006.

SAY, Kubilay; Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi, Ankara, 2006. (Yayımlanmamış Yüksek Lisans Tezi)

SIRIMCIYAN, Alis; *"Pusuda Bekleyen Düşmanlar"*, CHIP, 1999, Sayı: 12.

SINAR, Hasan; İnternet ve Ceza Hukuku, İstanbul, 2001.

SPENCER, John R.; "The Green Paper on obtaining evidence from one Member State to another and securing its admissibility: the Reaction of one British Lawyer", http://www.zis-online.com/dat/artikel/2010_9_492.pdf (24.08.2011)

ŞAHİN, Cumhur; Ceza Muhakemesinde İspat, Ankara, 2001.

ŞEN, Osman Nihat; "*Adli Bilişim Bilimi ve Diğer Bilimlerle Olan İlişkisi"* http://www.bilgisayarpolisi.com/index.php?sayfa=makaleoku&kategori=11&id=121 (18.08.2011)

TOROSLU, Nevzat / FEYZİOĞLU, Metin; Ceza Muhakemesi Hukuku, Ankara, 2006.

TOSUN, Öztekin; Türk Suç Muhakemesi Dersleri, C. I, İstanbul, 1981.

UÇKAN, Özgür / BECENİ, Yasin; "Bilişim-İletişim Teknolojileri ve Ceza Hukuku", İnternet ve Hukuk, İstanbul, 2004.

YURTCAN, Erdener; Ceza Yargılaması Hukuku, İstanbul, 1994.

http://www.edirnebarosu.org.tr/kutuphane/makaleler/89-adli-bilisim-computer-forensic.html. (15.08.2011)

http://www.spiegel.de/international/germany/0,1518,502955,00.html. (24.08.2011)

http://www.spiegel.de/international/germany/0,1518,590198,00.html. (24.08.2011)

http://www.veteknoloji.com/almanya-siber-guvenlik-kararghi-kuruyor-39333—0.html. (24.08.2011)

http://www.webopedia.com/TERM/I/IT.html. (15.08.2011)

http://www.webopedia.com/TERM/h/harware/html. (15.08.2011)

http://www.webopedia.com/TERM/s/software.html (15.08.2011)