CEZA YARGILAMASINDA ELEKTRONİK DELİLLERİN ELDE EDİLMESİNE VE KORUNMASINA İLİŞKİN USUL HÜKÜMLERİ

PROCEDURAL PROVISIONS FOR OBTAINING AND PROTECTING ELECTRONIC EVIDENCES IN CRIMINAL JUSTICE

Yusuf BAŞLAR[1*2**]

ÖZET

Elektronik ortamda bulunan delillerin kısa süre içerisinde karartılabilir olma özellikleri, söz konusu delillerin karartılabilme olasılığını en aza indirgeyecek ceza muhakemesi hukuku koruma tedbirlerini gerekli kılmaktadır. Bununla birlikte bu koruma tedbirlerinin uygulanması sırasında temel hak ve özgürlüklerin ihlal edilmemesinin de sağlanması gerekir. Bu makalede Türk Hukuk sisteminde elektronik delillerin elde edilmesi ve korunması amacına ilişkin mevzuatta yer alan düzenlemeler, etkinliği, özel hayatın gizliliğinin korunması ve Avrupa Siber Suç Sözleşmesine uygunluğu bakımından incelenmiştir.

Anahtar Kelimeler: Elektronik Delil, Bilgisayarlarda Arama ve Elkoyma, Özel Hayatın Gizliliği, Avrupa Siber Suç Sözleşmesi

ABSTRACT

Because of its feature of being easily tampered with, the evidence of electronic environment requires criminal procedural precaution measures in order to minimize the possibility to be tampered with. However it is necessary to ensure the non violation of the fundamental rights and freedoms during the implementation of these measures of precaution. In this article, the current legal regulation regarding the gathering and protection of the electronic evidence was examined from the perspective of its effectiveness, its alignment with the European Convention on Cyber Crime and respect for protection of the right of privacy.

Keywords: Electronic Evidence, Search and Seizure in Computer, Privacy of Private Life, Europe Convention on Cybercrime

***

1 *Viranşehir Cumhuriyet Başsavcısı.

2 **Sakarya Üniversitesi Sosyal Bilimler Enstitüsü Doktora Öğrencisi.

GİRİŞ

Bilişim teknolojilerinin hızlı bir şekilde gelişmesi nedeniyle ceza muhakemesi hukuku, işlenen suçların etkin şekilde soruşturulması bakımından uyumluluk gösterme zorunluluğu içerisinde bulunmaktadır. Özellikle elektronik ortamda bulunan delillerin saniyeler içerisinde karartılabilir olma nitelikleri, söz konusu delillerin karartılabilme olasılığını en aza indirgeyecek ceza muhakemesi hukuku koruma tedbirlerini oluşturmayı gerekli kılmaktadır. Aksi takdirde, elektronik ortamda işlenen suçların faillerinin ve bu suçların ispatı için aranan delillerin elde edilememesi durumu ile karşı karşıya kalınabilmektedir[3].

Bununla birlikte elektronik delillerin elde edilmesi sırasında şüphelilerin bilişim sistemleri üzerinde uygulanacak koruma tedbirlerinin kişilerin temel hak ve özgürlüklerine müdahale anlamını taşıdığı da bir gerçektir. Zira, bu koruma tedbirleriyle şüphelilerin özel hayatlarına doğrudan müdahale edildiği gibi kişisel verilerinin de deşifre olmasına neden olunmaktadır.

Bu bakımdan bir taraftan elektronik ortamda bulunan delillerin elde edilmesi ve bu delillerin karartılmasının engellenmesi amacıyla gerekli koruma tedbirlerinin uygulanması diğer taraftan da bu koruma tedbirlerinin uygulanması sırasında temel hak ve özgürlüklerin ihlal edilmemesi amacıyla uluslararası hukuk ve iç hukukumuzda düzenlemeler yapılmak suretiyle söz konusu koruma tedbirlerinin belirli bir düzen ve disiplin içerisinde uygulanması amaçlanmıştır.

Biz de bu çalışmamızda Türk Hukukunda elektronik delillerin elde edilmesi ve korunması sürecinde uyulması gereken usul hükümlerini düzenleyen 5271 Sayılı Ceza Muhakemesi Kanunu ile Adli ve Önleme Aramaları Yönetmeliği ve Suç Eşyası Yönetmeliği'nin ilgili maddelerini incelemeye çalışacağız.

3 KESKİN, Serap, Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Yıl: 2001, Cilt: 59, Sayı: 1-2, s. 155.

I.CEZA MUHAKEMESİ KANUNU'NUN 134. MADDESİ UYARINCA UYGULANAN ARAMA, KOPYALAMA VE EL KOYMA TEDBİRİ

A. Genel Olarak

Günümüzde bilgisayar teknolojisinin hızla ilerlemesi ve bir çok işlemin bilgisayar aracılığı ile gerçekleştirilmesi, yapılan işlerde büyük kolaylık ve verim artışı sağlamasına karşın bilgisayarların işlenen suçlarda yaygın şekilde kullanılması da dikkat çekici boyutlara ulaşmıştır[4].

Diğer taraftan bilgisayar teknolojisinin kullanılması suretiyle işlenen suçlarda, klasik delil elde etme yöntemlerinin yetersiz kaldığı görülmektedir. Zira, soruşturmanın konusunu oluşturan elektronik veriler elle tutulan ve gözle görülen nesneler değildir. Bu veriler, her gün gelişen ve yenilenen teknoloji kullanılarak saklanmakta ve bir yerden başka bir yere kolaylıkla gönderilebilmektedir. Hatta bu veriler bazen şifrelenmekte bazen de hiçbir özellik göstermeyen resim veya ses içeren veriler içerisine gizlenerek kullanılabilmektedir[5].

Elle tutulamayan, gözle görülemeyen ve elektrik devrelerinden oluşan bilgisayar verilerinin ceza yargılamasında delil olarak değerlendirilmesi yeni bir olgudur. Bununla birlikte devletin "koruma tedbirleri" çerçevesinde bilgisayar programlarında bulunan verileri elde edip saklayarak yargılamada delil olarak kullanması artık yaygın şekilde görülmektedir. Bununla birlikte CMK m. 116 vd. ve m. 123'de arama ve elkoyma tedbirlerine ilişkin genel hükümler bulunmasına rağmen bu tür verilerin elde edilmesi özel bir arama ve elkoyma kararını gerekli kılmaktadır. Zira, bir bilgisayarın içerisinde veya birbirlerine ağ şeklinde bağlanmış olan bilgisayarların bağlı bulunduğu sistem içerisinde delil aranması ve bunlara elkonulması ayrı bir işlem niteliğindedir[6].

Bu bakımdan CMK m. 134'de genel nitelikteki arama ve el koyma tedbirinin özel bir şeklini ifade eden bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma tedbiri düzenlenmiştir. Genellikle arama tedbiri, bina ve eklentileri,

4 ÖLMEZ, Aslan, Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Kopyalama ve Bunlara El Koyma, Terazi Hukuk Dergisi, Yıl: 2009, Sayı: 30, s. 45.

5 KUNTER, Nurullah/YENİSEY, Feridun/NUHOĞLU, Ayşe, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 18. Bası, Beta Yayınevi, İstanbul, 2010, s. 1093.

6 KUNTER/YENİSEY/NUHOĞLU, s. 1092.

araç ve kişiler üzerinde gerçekleşmesine karşın söz konusu tedbirde aramanın konusunu bilgisayarlar, bilgisayar programları ile bilgisayar kütükleri oluşturmaktadır[7].

B. Tedbirin Amacı

Tedbirin amacı elektronik delil elde etmektir. Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma özellikle bilişim suçlarına ilişkin elektronik delillerin elde edilmesinde büyük önem arz etmektedir. Bununla birlikte söz konusu tedbir klasik suçların soruşturulmasında da kullanılmaktadır. Ceza Muhakemesi Kanunundaki klasik arama tedbirine ilişkin hükümlerin bilgisayar ortamına uygulanması mümkün olmadığı için hukukumuzda bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbiri ayrıca düzenlemiştir.

C. Tedbirinin Kapsamı

CMK m. 134/1'de tedbirin kapsamı şüphelinin kullandığı bilgisayar, bilgisayar programları ve kütükleri olarak belirtilmiştir. Buna göre;

Bilgisayar, çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin olarak tanımlanmaktadır[8].

Bilgisayar programı, 5846 sayılı FSEK m. 1/B'de "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 çalışmaları" şeklinde tanımlanmıştır. Dünya Fikrî Mülkiyet Teşkilatı Fikrî Haklar Anlaşması'na göre ise bilgisayar programı, "makinenin okuyabileceği bir taşıyıcıya yüklendikten sonra, bilgi işleme yeteneğine ehil böyle bir makinenin belirli bir işlev veya görevi yerine getirmesini ya da belirli bir sonuca ulaşmasını sağlayabilen komutlar dizini" şeklinde tanımlanmaktadır[9].

Bilgisayar kütükleri'nin ise hard disk olarak anlaşılması gerektiği belirtilmektedir. İngilizce "log" kelimesinin karşılığı olan kütükler

7 ÖZBEK, Veli Özer, Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, Ankara, 2006, s. 359.

8 www.tdk.gov.tr, İ.E.T: 27.02.2014

9 EROĞLU, Sevilay, Rekabet Hukukunda Bilgisayar Programlarının Korunması, Beta Yayınevi, İstabul, 2002, s. 2

daha çok internet servis sağlayıcılarının internet erişimi sağladıkları kullanıcılara ait IP numaralarını ve diğer erişim bilgilerini depoladıkları veri tabanlarını ifade etmektedir[10].

CMK m. 134/1'de tedbirin kapsamı şüphelinin kullandığı bilgisayar, bilgisayar programları ve kütükleri olarak belirtilmiş olmasına karşın kullanım amaçları çok çeşitli olmakla birlikte içeriğinde bilişim teknolojisi barındıran cep telefonu, cep bilgisayarı, dijital fotoğraf makinesi, dijital kamera vb. gibi taşınabilir cihazlara yönelik herhangi hüküm bulunmadığı görülmektedir. Adli bilişimin esas konusunun elektronik deliller olması nedeniyle elektronik delillerin kaynağını sadece bilgisayar ile sınırlandırmak meseleye çok dar bir pencereden bakmak anlamını taşımaktadır. Teknolojinin gelişimi ile günümüzde hemen herkesin kullanmış olduğu bu cihazlarda adli bilişim uzmanlarınca elde edilebilecek çok önemli delillerin bulunduğu da aşikardır[11].

Bu bakımdan kullanım amaçları çok çeşitli olsa da içeriğinde bilişim teknolojisi barındıran cihazlar bu kapsamda değerlendirilmelidir. Cep telefonu, çağrı cihazı, dijital kamera ve fotoğraf makinesi, özel amaçlı kameralar (ısıya hassas, kızıl ötesi, vb.), fotokopi makinesi, ATM cihazı, elektronik ajanda, faks makinesi, elektronik veri bankası, akıllı kart ve POS makinesinin bu kapsamda değerlendirilmesi gerekmektedir. Son zamanlarda günlük kullanıma sunulan elektronik veya mekanik ürünlerin pek çoğunda bilişim çözümleri ile bütünleşme sağlanmıştır. Bu nedenle bu kapsama alınabilecek pek çok ürün daha bu listede sayılabilir.

Uygulamada bu tür cihazlarda bulunması muhtemel delillere ulaşmak için CMK'nın 116 ve 123. maddelerinde düzenlenen arama ve elkoymaya ilişkin genel hükümler kullanılmaktadır. Ancak, bilgisayar ve bilgisayar programları ile bilgisayar kütüklerine yönelik işlemlerin genel arama ve elkoyma hükümlerinden ayrı tutulup özel bir hüküm konumundaki CMK m. 134 uyarınca işleme tabi tutulmaları karşısında, teknik açıdan aynı kapsamda değerlendirilmesi gereken ve yukarıda verilen bilgisayar tanımı içerisinde değerlendirilebilecek cep telefonu, cep bilgisayarı ve

10 ÖZBEK, s. 363

11 AYDOĞAN, Hakan, Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri, Polis Akademisi, Güvenlik Bilimleri Enstitüsü, Yüksek Lisans Tezi, Ankara, 2009, 19; ÖZTÜRK, Mustafa İlker, Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri, Ankara Üniversitesi, Sağlık Bilimleri Enstitüsü, Yüksek Lisans Tezi, Ankara, 2007, s. 62

elektronik veri barındıran bir çok cihaza yönelik arama ve elkoyma işlemleri de ek bir hükme gerek olmaksızın CMK'nın 116 ve 123. maddelerinde belirtilen genel arama ve elkoyma hükümleri yerine CMK'nın 134. maddesi uyarınca gerçekleştirilmesi gerektiği kanaatindeyiz.

D. Tedbirin Uygulanma Koşulları

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma tedbirinin uygulanacağı suç tipleri bakımından kanunda herhangi bir sınırlayıcı düzenleme bulunmamaktadır. Tedbirin niteliği gereği daha çok bilişim suçları için uygulanabileceği yönünde bir izlenim bulunmakta ise de diğer suçlar bakımından da uygulanabileceği açıktır[12]. Bununla birlikte tedbirin uygulanması kanunda belirli koşullara bağlanmıştır.

1. Suç Dolayısıyla Başlatılmış Bir Soruşturmanın Bulunması

Tedbirin uygulanabilmesi için öncelikle suç dolayısıyla başlatılmış bir soruşturmanın bulunuyor olması gerekmektedir. CMK m. 134/1'de suçun ağırlık derecesi bakımından her hangi bir sınırlama getirilmemesinin yanı sıra madde metninin ilk halinde şüphenin niteliğinden de bahsedilmemekteydi. Bu bakımdan CMK m. 134/1'de 6520 sayılı Kanunla yapılan değişiklikten önce herhangi bir suçun işlendiğine dair basit şüphenin varlığı tedbirin uygulanabilmesi için yeterliydi.

Bu durum öğretide; temel hak ve özgürlüklerin korunması bakımından bu tedbirin uygulanmasının ancak "kuvvetli suç şüphesi"nin varlığında[13] ve belli ağırlıktaki suçlar bakımından uygulanması gerektiği, tasarıda yer alan *"iki yıl veya daha fazla hürriyeti bağlayıcı cezayı gerektiren cürümler hakkında yapılan soruşturmalarda"* bu tedbirin uygulanabilmesine ilişkin şartın mevcut yasada yer almamasının ise orantılılık ilkesi bakımından ciddi bir eksiklik olduğu[14] yönünde eleştirilere neden olmaktaydı.

Bununla birlikte CMK'nın 134/1 maddesine 6520 sayılı Kanunun 11. maddesiyle yapılan değişiklik ile yukarıda belirtilen eleştiriler

12 ÖZBEK, s. 364.

13 CENTEL, Nur/Hamide Zafer, Ceza Muhakemesi Hukuku, 5. Bası, Beta Yayınevi, İstabul, 2008, s. 385.

14 DAĞ, Güray, Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, Doktora Tezi, İstanbul, 2011, s. 237.

kısmen karşılık bulmuştur. Buna göre tedbirin uygulanması "somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı" şartına bağlanmıştır. Bu değişiklik tedbirin uygulanmasını güçleştirmesine karşın temel hak ve özgürlükler bakımından olumlu bir gelişmedir.

Bununla birlikte kanunda bu tedbire başka türlü delil elde etme imkanının bulunmaması halinde başvurulabileceği hususunun belirtilmiş olması karşısında somut delillere dayanan "kuvvetli şüphe sebeplerinin varlığı" şartının da eklenmesiyle uygulama alanı önemli derecede sınırlanmış bu tedbire başvurulması için "belli ağırlıktaki suçlar bakımından uygulanma" şartının da aranması durumunun tedbiri uygulanamaz hale getirmesi muhtemeldir. Bu nedenle kanunda son değişiklikle oluşan mevcut düzenlemeye tedbirin "belli ağırlıktaki suçlar bakımından uygulanma" şartının da eklenmesinin gerekli olmadığı düşüncesindeyiz.

Tedbirin uygulaması bakımından suç tipiyle ilgili de herhangi bir kısıtlama getirilmemektedir. Tedbir, genellikle bilişim suçları ile birlikte anılmakta ise de "bir suç dolayısıyla yapılan soruşturma" ibaresinden de anlaşılacağı üzere bu tedbir bilişim suçlarına özgü olmayıp bilişim suçları da dahil olmak üzere tüm suçlardan dolayı yapılan soruşturmalarda, bilişim sistemlerinden elektronik delil elde edilmesine yöneliktir[15].

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma tedbiri soruşturma aşaması sona ermeden önce uygulanması gerekmektedir. Nitekim, kanunda sanıktan bahsedilmeyip sadece şüpheliden bahsedilmesinin yanı sıra tedbire ancak soruşturma aşamasında başvurulabileceği açıkça belirtilmiştir. Bu bakımdan bu tedbire kovuşturma aşamasında başvurulabilmesi mümkün değildir[16].

Bu tedbire başvurmanın amacı, başka türlü elde edilemeyen elektronik delili elde etmektir. Kamu davasının açılarak kovuşturmanın başlaması ise kamu davası için yeterli şüphenin oluşmasını sağlayacak delilin elde edildiğini gösterir. Bu durumda ise söz konusu tedbire başvurmaya gerek bulunmamaktadır[17]. Nitekim, aleni bir duruşmada mahkemenin bu tedbire karar

15 PARLAR, Ali/HATİPOĞLU, Muzaffer, 5271 Sayılı Ceza Muhakemesi Kanunu Yorumu ve İlgili Mevzuat, 1. Cilt, Ankara, 2008, s. 531

16 KUNTER/YENİSEY/NUHOĞLU, s. 1098

17 ÇOLAK, Haluk/TAŞKIN, Mustafa, Açıklamalı-Karşılaştırmalı-Uygulamalı Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, Ankara, 2005, s. 434

vermesi durumunda, tedbirden haberdar olan ilgililerin delilleri yok etmesi söz konusu olacak ve bu tedbire başvurmadaki yarar ortadan kalkacaktır[18].

Bununla birlikte, öğretide yargılama aşamasında delil toplanmasını engelleyen bir hüküm bulunmaması ve mahkemenin re'sen araştırma yetkisine sahip bulunması karşısında kovuşturma aşamasında da bu tedbire başvurulabilmesini mümkün kılan yasal bir düzenleme yapılması gerektiği de dile getirilmektedir[19].

2. Son Çare Prensibi

Tedbirin uygulanabilmesi için başka surette delil elde etme imkanının bulunmaması gerekmektedir. Tedbire karar verecek hakimin öncelikle tedbiri gerekli kılan şüpheyi değerlendiren ve başka surette delil elde etme imkanının bulunmadığını saptayan bir gerekçe yazması gerekmektedir[20] .

Bu tedbir de her koruma tedbirinde olduğu gibi hükümden önce bazı temel hak ve özgürlüklere müdahale etmektedir. Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma özel hayatla doğrudan bağlantılıdır. Zira kişilerin kendilerine ilişkin önemli verileri sakladıkları bilgisayarları bu tedbir sonucunda deşifre olmaktadır[21]. Bu bakımdan, başka surette delil elde edilememesi ön koşulu temel hak ve özgürlükler açısından önemli ve yerindedir.

Bununla birlikte, öğretide bir görüşe göre[22]; bilişim suçlarında, işin doğası gereği, öncelikle şüphelinin kullanmış olduğu bilgisayarda arama ve diğer tedbirlerin uygulanması gerektiğinden, söz konusu ön koşulun bilişim suçları ile ilgili yürütülen soruşturmalarda uygulanmasının elektronik delillere ulaşmada soruna neden olacağı savunulmuştur. Bu görüşe göre; CMK m. 134 uyarınca önce başka delillerin var olup olmadığının araştırılması, sonra başka delil elde etme imkanının olmadığının ortaya konulması ve akabinde şüphelinin bilgisayarında arama, kopyalama ve el koyma

18 CENTEL/ZAFER, s. 355.

19 ŞAHİN, Cumhur, Ceza Muhakemesi Hukuku I, Seçkin Yayıncılık, Ankara, 2007, s. 262; PARLAR/HATİPOĞLU, s. 532.

20 KUNTER/YENİSEY/NUHOĞLU, s. 1098.

21 ÖZBEK, s. 362.

22 KARAGÜLMEZ, Ali, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, 2. Baskı, Seçkin Yayıncılık, Ankara, 2011, s. 391.

işlemlerine izin verilmesi, bilişim suçlarının soruşturulmasında sıkıntıya neden olmaktadır. Bu nedenle, CMK m. 134'de en azından bilişim suçlarının bünyesine uygun ayrık hükümlere yer verilerek bu suçların soruşturma evresindeki bilişim sistemlerinde arama, analiz ve muhafaza altına alma işlemlerinde "somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı" koşulu yeterli sayılmalıdır.

3. Cumhuriyet Savcısı Talebi ve Hakim Kararı

Tedbir Cumhuriyet savcının talebi üzerine hakim kararı ile uygulanabilmektedir. Tedbir kararı verecek hakim ise soruşturmanın yürütüldüğü yer sulh ceza hakimidir. Ancak soruşturma Cumhuriyet savcısı tarafından yürütülmekte ve bu tedbir sadece soruşturma aşamasında uygulanabilir nitelikte olması nedenleriyle hakimin, savcılık talebi olmaksızın, re'sen bu tedbirin uygulanmasına karar vermesi mümkün değildir.

Kanun, bu tedbirin Cumhuriyet savcısının doğrudan vereceği karar ile uygulanmasına cevaz vermemekte ise de; bilişim teknolojilerindeki hız ve değişkenlik, delillerin derhal ele geçirilmesini gerektirdiğinden delillerin geç elde edilmesinde sakınca bulunduğu hallerde sonradan hakim onayına sunulmak kaydıyla Cumhuriyet savcısının kararı ile de bu tedbirin uygulanabilmesi yönünde bir kanun değişikliği yerinde olacaktır.

4. Tedbirin Şüphelinin Kullandığı Bilgisayar, Bilgisayar Programları ve Kütüklerinde Uygulanabilmesi

Bu tedbir şüphelinin kulladığı bilgisayar, bilgisayar programları ve kütükleri üzerinde uygulanabilecektir. Bu bakımdan sanık statüsüne geçmiş kişiler veya üçüncü kişilerin bilgisayar, bilgisayar programları ve kütükleri üzerinde bu tedbir uygulanamaz. Diğer taraftan şüphelinin "sahip olduğu" ibaresi değil şüphelinin "kullandığı" ibaresine yer verilmiştir. Şüphelilerin işlemiş oldukları suçta kendi adlarına kayıtlı olan veya faturalardan kendileri adına alındığı tespit edilebilecek bilgisayar, bilgisayar programları ve kütüklerini kullanmayabilecekleri hususu dikkate alındığında madde metninin yerinde olduğu görülmektedir. Eğer sadece "sahip oldukları" denilmiş olsaydı tedbirin uygulama alanı oldukça daraltılmış olacaktı[23].

23 ÇOLAK/TAŞKIN, s. 435.

E. Tedbirin Uygulanması

CMK m. 134/1 hükmü uyarınca yukarıda belirtilen koşulların varlığı halinde öncelikle şüphelinin bilgisayar, bilgisayar programları ve kütüklerinde arama yapılarak suçla ilgili elektronik delillerin varlığı araştırılacak, bu delillere ulaşıldığı takdirde de bunlar kopyalanabilecek ve ayrıca elde edilen ve kopyalanan deliller çözülerek metin haline getirilebilecektir.

Bununla birlikte, CMK m. 134/2'ye 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 elkonulabilecektir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde ise, elkonulan cihazların gecikme olmaksızın iadesi yapılacaktır.

Bazı bilişim sistemlerine ait şifrelerin çözülmesi zaman alabildiği için kanun koyucu şifre içeren bilişim sistemlerinin yer aldığı araçlara el koyma yetkisi vermiştir. Bununla birlikte yasa koyucu, oranlılık ilkesinin bir gereği olarak bilgisayar, bilgisayar programları ve kütüklerine elkoyma tedbirinin uygulanabilmesi için şifrenin çözülememesinden dolayı sisteme girilememesi veya gizlenmiş bilgilere ulaşılamaması koşulunun varlığını aramıştır[24] .

Bununla birlikte madde metninde belirtilen bilişim sistemlerine el koyma şartının bilişim sistemlerindeki şifrenin çözülememesine bağlanması doğru bir yaklaşım tarzı değildir. Bu bağlamda, bir bilgisayardaki verilere erişim için bu bilgisayarı çalışır hale getirmek ve bilgisayardaki işletim sistemini açmak gerekmemektedir. Bu bilgisayardaki hard diskin fiziken sökülerek içerisinde bulunan verilerin başka bir medyaya kopyalanması da mümkündür[25].

Diğer taraftan, elkoyma işleminin sadece bilişim sistemlerine ait şifrelerin çözülememesi şartına bağlanmış olmasının da doğru olmadığı kanaatindeyiz. Zira, bilgisayar veya çıkarılabilir depolama aygıtları ve bunların içerisindeki verilerin çok fazla olması durumlarında kopyalama işleminin çok uzun zaman alabildiği ve bu nedenle de uygulamada kolluğun şifrenin çözülebilir olup olmadığına bakmaksızın şifrenin çözülemediğine ilişkin tutanak tutmak suretiyle elkoyma işlemini gerçekleştirerek kopyalama

24 ÖZBEK, s. 365

25 AYDOĞAN, s. 112

işlemini olay mahalli yerine kolluk birimlerine ait laboratuvarlarda gerçekleştirdikleri görülmektedir. Bu bakımdan, uygulamada karşılaşılan bu sorunun çözümü yönünde yasal düzenleme yapılması gerekmektedir.

Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılmalıdır (CMK m. 134/3). Elkoyma işlemi nedeniyle bazı bilgilerin kaybolması ve bu sebeple şüphelinin mağdur olmasının önlenmesi amacıyla yedekleme yapılması zorunludur. Nitekim kanunda elkoyma sırasında yedekleme yapılması, şüpheli talebine veya görevlilerin gerek duymasına bırakılmamış, zorunlu olarak yedekleme yapılması hükme bağlanmıştır. Bu bakımdan, bilgilerin kaybolması veya bir zarar meydana gelmesi söz konusu olmasa bile yedekleme yapılmak zorundadır. Bu önlemin bir amacı da delil uydurmanın önüne geçmektir[26].

Diğer taraftan kanun metninde kullanılan "elkoyma işlemi sırasında" ifadesini, incelemeye başlamadan önce şeklinde yorumlamak yerinde olacaktır. Zira, elektronik veriler üzerinde inceleme yaparken verilerin zarar görmesi, değişmesi veya yok olması muhtemeldir[27].

CMK m. 134/3 uyarınca elkoyma işlemi esnasında sistemdeki bütün verilerin yedeklenmesi işlemi sonucunda bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilmeli ve bu husus tutanağa geçirilerek imza altına alınmalıdır (CMK m. 134/4). Madde metninin ilk halinde bu durum şüpheli ya da vekilinin istemi durumunda gerçekleşmekteydi. Ancak CMK'nın 134/4 maddesinde 6520 sayılı Kanunun 11. maddesiyle yapılan değişiklik ile herhangi bir talebe gerek duyulmaksızın yedekleme işlemi sonucunda elde edilen yedekten bir kopya şüpheli ve vekiline verilmek zorundadır.

Bununla birlikte, suç unsuru bulunan medyanın bir kopyasının da şüpheliye verilip verilmeyeceği, şüpheliye hangi formatta ve nasıl bir medya üzerinde verileceği, bu medyayı kimin sağlayacağı, diğer taraftan bu yedeklerin kimin tarafından, nasıl ve ne kadar süreyle muhafaza edilecekleri, veri depolama aygıtlarının kapasitelerinin giderek arttığı dikkate alındığında ilgili birimlerde bu kadar medyayı saklayacak depolama ünitelerinin bulunup bulunmadığı gibi hususlar kanunda belirtilmemiş olması nedenleriyle

26 ÇOLAK/TAŞKIN, s. 436

27 ÖZBEK, s. 365

uygulamada soruna neden olmakta, bu benzeri hususların açıklığa kavuşturulması gerekmektedir[28].

Gerçekten de, özellikle suçta kullanılan bir silahın şüpheliye iadesi anlamına gelecek içerisinde (çocuk pornografisi, kişilerin kredi kartı bilgileri vb.) suç unsurunun bulunduğu bir elektronik medyanın şüpheliye geri verilebileceği anlamına sahip olan mevcut düzenlemenin bir an önce değiştirilmesi gerektiği düşüncesindeyiz.

Bilgisayar veya bilgisayar kütüklerine elkonulmaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyasının alınması mümkündür. Bu durumda kopyası alınan verilerin kağıda yazdırılarak, bu hususun tutanağa bağlanması ve ilgililer tarafından imza altına alınması gerekmektedir (CMK m. 134/5).

Bu hüküm sayesinde şüpheli bilgisayar sistemini, programlarını ve verilerini kullanmaya devam edebilmektedir. Tutanak altına alınarak yedeklenen verilerin değiştirilmesi, bu aşamadan sonra bir anlam taşımamaktadır. Uygulamada, kolluk görevlilerinin bu hükmü üç kopya çıkartarak, birini şüpheliye vermek, birini incelemek, diğerini ise daha sonra ortaya çıkabilecek uyuşmazlıkların giderilmesi için ayrı bir birimde koruma altına almak şeklinde yerine getirdiği görülmektedir[29].

Bununla birlikte, kanun, arama sırasında kopyalanacak olan verilerin yazdırılması hususunu bir mecburiyet haline getirmekte ise de, büyük hacimli dosyaların yazdırılması pratikte bazı zorlukları beraberinde getirmektedir[30]. Gerçekten de, günümüzde çok büyük hacimlere sahip hard disklerde bulunan ve milyonlarca A4 sayfası tutabilecek verilerin yazdırılması mecburiyetinin uygulanabilirliği bulunmamaktadır. Kaldı ki bu miktardaki yazdırılmış verinin adli makamlarca da incelenebilmesi imkan dahilinde değildir[31].

F. Genel Hükümlerin Geçerliliği

Arama ve elkoyma tedbirinin özel bir şekli niteliğindeki bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirinin uygulanması sırasında Ceza

28 HEKİM, Hakan/BAŞIBÜYÜK, Oğuzhan, Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları, Uluslararası Güvenlik ve Terörizm Dergisi, Yıl: 2013, Cilt: 4, Sayı: 2, s. 152

29 KUNTER/YENİSEY/NUHOĞLU, s. 1102

30 KUNTER/YENİSEY/NUHOĞLU, s. 1100; AYDOĞAN, s. 22

31 BALI, Yunus, CMK 134. madde düzeltilmelidir, http://www.dijitaldeliller.com/cmk134.htm (İET: 04.03.2014)

Muhakemesi Kanunu'ndaki arama ve elkoymaya ilişkin genel hükümler geçerliliğini korumaktadırlar. Bu bağlamda, arama kararında bulunması gereken bilgiler, arama ve elkoymanın tutanağa bağlanması, aramayı yapan kolluk görevlilerinin isimlerinin tutanağa yazılması, arama sırasında bulunulması gereken kişiler, arama sonucunda verilecek belge, elkonulmayacak belgelerle ilgili hükümler bu tedbire aykırı olmadığı sürece geçerli olacaktır[32].

Diğer taraftan CMK m. 134 uyarınca yapılacak arama, kopyalama ve elkoyma tedbirinin kişi bakımından uygulanmasına ilişkin istisnai bir düzenleme bulunmamaktadır. Bu nedenle CMK m. 134 hükmünün CMK m. 130 hükmü ile birlikte değerlendirilmesi sonucunda bahse konu tedbirin avukatların bürolarında da uygulanabilmesi mümkündür[33].

Ayrıca, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirinin uygulanmasına karşı hangi kanun yollarına başvurulabileceği hususunda açık bir hüküm bulunmamaktadır. Bu durumda söz konusu husus da genel hükümler çerçevesinde çözülmelidir. Buna göre, CMK m. 267 uyarınca hakimin ilgili tedbir kararı üzerine şüpheli veya müdafii itiraz yoluna gidebileceklerdir. Bununla birlikte CMK m. 35/2 uyarınca bu koruma tedbiri hazır bulunmayan ilgililere tebliğ olunmayacağı için şüpheli ve müdafii bu tedbir kararına öğrendikleri tarihten itibaren itiraz edebileceklerdir.

Şüphelinin bilgisayar, bilgisayar programlarında ve kütüklerinde yapılacak aramanın ölçüsüz biçimde yerine getirilmesi durumlarında tazminat hükümlerinin uygulanması da genel hükümlere göre belirlenecektir. Böyle bir durumda şüpheli veya müdafii CMK m. 141/1-i uyarınca tazminat talebinde bulunabilecektir.

G. Tesadüfen Elde Edilen Deliller

CMK m. 138/1 uyarınca bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama yapılması sırasında, yapılmakta olan soruşturma ve kovuşturmayla ilgisi olmayan, ancak diğer bir suçun işlendiği şüphesini uyandırabilecek bir delilin elde edilmesi durumunda, bu delilin muhafaza altına alınması ve durumun Cumhuriyet Başsavcılığına bildirilmesi gerekmektedir.

32 ÇOLAK/TAŞKIN, s. 436

33 ÖZBEK, s. 364

H. Tedbirin Özel Hayatın Gizliliğinin Korunması Bakımından Değerlendirilmesi

Özel hayat, hukuk tarafından korunması gereken bir temel hak olmasının yanı sıra bireylerin özel bilgileri, sosyal ilişkileri, haberleşme hürriyeti gibi bir çok kavramı da içinde barındırmaktadır. Özel hayatın gizliliği ve koruması ise; bireyin, kişiliğini geliştirmek, maddi ve manevi değerlerine güvence sağlamak için başkaları tarafından bilinmesini istemediği hususların oluşturduğu ve korunması hukuken gerekli görülen hayat alanı üzerindeki hakkı ifade etmektedir[34].

Yukarıda da değinildiği üzere bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbiri, her koruma tedbirinde olduğu gibi hükümden önce bazı temel hak ve özgürlüklere müdahale etmektedir. Bu bağlamda söz konusu tedbir de özel hayatın gizliliği ile doğrudan bağlantılıdır.

Bununla birlikte bu tedbir, özel hayatın gizliliği kavramının içinde yer alan ve hatta ayrılmaz bir parçasını teşkil eden kişisel verilerin korunması bakımından da özellik göstermektedir. Zira, bilgisayarların nitelikleri gereği kişilerin gerek özel yaşamlarına gerekse iş yaşamlarına ilişkin bir çok kişisel veriyi depolamaları nedeniyle bu tedbirinin uygulanması sonucunda birçok kişisel veriye ulaşılmakta ve kişilerin kendileriyle ilgili gizledikleri önemli kişisel verileri deşifre olmaktadır[35].

Özel hayatın gizliliğinin korunması insan haklarına ilişkin en temel metinlerden biri olan Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi ile güvence altına alınmıştır. Sözleşmeye göre, özel hayatın gizliliği hakkı sözleşmede belirtilen hallerde, ölçülülük ilkesine uymak kaydıyla ancak kanunla sınırlandırılabilir.

Anayasa'nın 20. maddesinde de herkesin, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı, ayrıca kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahip olduğu hükme bağlanmıştır.

Bu bakımdan, kişilerin özel bilgilerinin yer aldığı bilişim

34 ŞEN, Ersan/YURTTAŞ, Yasemin, Bilgisayar Programları Karşısında Özel Hayatın Korunması, Terazi Hukuk Dergisi, Yıl: 2010, Sayı: 42, s. 29.

35 DAĞ, s. 235, 238.

sistemlerine ulaşabilmek ve bu surette delil elde edebilmek, mevcut yasal düzenlemelere ve Anayasa m. 20/2 hükmüne aykırı davranmamakla mümkündür[36]. Ayrıca, kişilerin kendilerine ait olan özel hayatları ve kişisel verileri üzerinde karar verme ve belirleme yetkisi bulunduğundan bu Anayasa ve mevcut yasalara göre düzenlenen tedbirin de uygulanmasının sıkı koşullara tabi tutulması da önem arz etmektedir.

CMK m. 134'de ifadesini bulan tedbirle ilgili düzenlemeye bakıldığında söz konusu tedbirin gerek Avrupa İnsan Hakları Sözleşmesinin 8. maddesinde gerekse Anayasanın 20/2 maddesinde belirtilen istisna hallerde ve ölçülülük ilkesine uygun şekilde uygulanabilir olduğu görülmektedir.

Bununla birlikte her ne kadar yasal düzenleme Avrupa İnsan Hakları Sözleşmesi ve Anayasaya uygunluk göstermekte ise de uygulama sırasında hakkında söz konusu tedbir uygulanan kişinin temel hak ve özgürlüklerinin hukuki sınırlarını aşar biçimde sınırlandırılmamasına dikkat edilmelidir. Özellikle bu tedbirin uygulanmasında, ceza yargılamasının amacına uygun bir şekilde özel hayatın gizliliğinin ve kişisel verilerin korunması, tedbiri uygulayan mercilerin birinci görevi olmalıdır.

I. Tedbirin Siber Suç Sözleşmesi Bakımından Değerlendirilmesi

Avrupa Konseyi Bakanlar Komitesinin 4 Şubat 1997 tarihli toplantısında alınan karar ile oluşturulan "Siber Uzay Suçları Uzmanlar Komitesi (PC-CY)", Nisan 1997'de toplanarak uluslararası alanda ortak bir ceza politikasının oluşturulup toplumun siber suçlara karşı korunması, ortak suç tanımlarının getirilmesi, soruşturma yöntemlerinin tanımlanması (veriyi saklama, trafik verisini arama, toplama ve elkonulması ile iletişim yetkisi) ve uluslararası işbirliğinin geliştirilmesi amacıyla siber suçlara ilişkin uluslararası bir konvansiyon taslağını görüşmeye başlamıştır. Görüşmelerden sonra, gözden geçirilmiş ve son halini almış konvansiyon taslağı ve gerekçesi Haziran 2001'de genel kurulda onaylanmak üzere Avrupa Suç Sorunları Komitesine ve ardından kabul edilip imzaya açılmak üzere Bakanlar Komitesine sunulmuştur[37].

36 ŞEN/YURTTAŞ, s. 30.

37 İÇEL, Kayıhan, Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında "Avrupa Siber Suç Politikasının Ana İlkeleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Yıl: 2001, Cilt: 59, Sayı: 1-2, s. 5-6; ÖZTÜRK, s. 47.

2004 yılında yürürlüğe giren ve Avrupa Konseyi Siber Suç Sözleşmesi olarak bilinen bu sözleşmenin temel amacının "gerekli mevzuatın kabul edilmesi ve uluslararası işbirliğinin geliştirilmesi yoluyla siber suçlara karşı toplumun korunmasını amaçlayan ortak bir ceza politikasının izlenmesi" olduğu söylenebilir. Ayrıca sözleşme de, "siber suçların ortak tanımlarının yapılması; cezai soruşturma ve kovuşturma yöntemlerinin belirlenmesi; siber suçlara karşı uluslararası işbirliği yollarının oluşturulmasını" hedeflenmektedir. Sözleşme, taraf olan ülkelere, tanımlanan suçların işlenmesi ve söz konusu suçların işlenmesine yardım veya yataklık yapılmasını ulusal mevzuatta cezai bir suç olarak tanımlanma ve gerekli yasama işlemlerini ve diğer işlemleri yapma yükümlülüğü getirmektedir. Sözleşme, söz konusu suçlara yönelik soruşturma ve kovuşturmaların yanı sıra işlenen suçlara delil teşkil edebilecek verilerin toplanması, saklanması, araştırılması ve el konulması gibi ulusal düzeyde alınması gereken önlemleri de içermektedir[38].

Elektronik ortamda özgürlüklerin, insan haklarının ve güvenliğin korunması ile risklerin azaltılmasına ilişkin kabul edilmiş tek uluslararası rehber ve hükumetlerin vatandaşlarını korumasına yönelik önemli bir araç niteliğinde olan bu sözleşme, özellikle telif hakları ihlalleri, bilgisayarlarla bağlantılı sahtecilik eylemleri, çocuk pornografisi, ağ güvenliğine ilişkin suçlar tanımlanmakta ve bu suçlarla mücadele etmede işbirliği öngörülmektedir. Bununla birlikte sözleşmede Ceza Muhakemesi Hukukuna ilişkin hükümlerin ceza yargılaması sürecinde elektronik delillerin elde edilmesi ve korunmasına ilişkin koruma tedbirleriyle ilgili olduğu da görülmektedir.

Avrupa Konseyi bünyesinde hazırlanan ve internet ve bilgisayar ağları aracılığıyla işlenen suçlara ilişkin uluslararası nitelikteki ilk belge olma özelliği taşıyan sözleşmenin 14 ila 21. maddeler arasında düzenlenen koruma tedbirleri, elektronik ortamda işlenen suçu ve bu suçun fail veya faillerini ortaya çıkartabilmek için delil elde edebilmek amacıyla ceza muhakemesi hukukunun klasik koruma tedbirlerinden olan arama ve elkoyma tedbirlerinin elektronik ortamdaki özel bir türünü teşkil etmektedir. Sözleşmede ayrıca, arama tedbirinde elektronik delile özgün niteliği ile elde etme bakımından geç kalınma tehlikesinin varlığı halinde

38 BİLİŞİM AJANDASI, Nihayet Türkiye de "Sanal Suçlar Sözleşmesi"ni imzaladı, Bilişim Kültür Dergisi, Yıl: 2010, s. 12, http://www.bilisimdergisi.org/s127, (İ.E.T: 04.03.2014).

elektronik verileri arama işlemi öncesinde aramayı olanaklı kılacak, veriler üzerinde ön koruyucu niteliğe sahip tedbirlere de yer verilmiştir[39]. Bu kapsamda Sözleşmesi'nin 19. maddesinde ise "Saklanan bilgisayar verilerinin aranması ve bunlara el konulması" düzenlenmiştir.

2001 yılında imzaya açılan ve 2004 yılında yürürlüğe giren Avrupa Konseyi Siber Suç Sözleşmesi 10 Kasım 2010 tarihinde Türkiye tarafından da imzalanmıştır. Henüz TBMM tarafından onaylanmamış olan sözleşme TBMM onayından sonra yürürlüğe girecektir. Bu bağlamda sözleşmenin Türkiye açısından bağlayıcılık durumu bulunmamaktadır. Bununla birlikte CMK m. 134'ün bazı eksikliklerin varlığının kabulüyle birlikte esas itibariyle Sözleşmesi'nin 19. maddesinde düzenlenen "Saklanan bilgisayar verilerinin aranması ve bunlara el konulması" koruma tedbirinin iç hukuka uyarlanmış şeklini ifade ettiği söylenebilir. Buna göre;

CMK m. 134/1 ve m. 134/2'de bilgisayar ve bilgisayar kütüklerinde hangi hallerde arama yapılacağı ve bunlara ne şekilde elkonulabileceği hükme bağlanmıştır. Yukarıda da değinildiği üzere maddenin birinci fıkrasına getirilen arama işleminin "somut delillere dayanan kuvvetli suç şüphesinin varlığı" şartının da eklenmesi, tedbirin uygulanmasıyla ilgili temel hak ve özgürlükler bakımından olumlu bir gelişme sağlamıştır. Tüm bunlar göz önüne alındığında mevcut düzenlemelerin sözleşmeye uygun olduğu belirtilmelidir.

CMK m. 134/3'de düzenlenen bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında sistemdeki bütün verilerin yedeklemesinin yapılmasına ilişkin hüküm verilerin bütünlüğünün korunması ve soruşturma sonuçlanıncaya kadar soruşturma ile ilgili delil niteliği taşıyabilecek verilerin değiştirilmesi, bozulması, erişilmez hale getirilmesi ve silinmesinin engellenmesi bakımından sözleşmeyle paralellik arz etmektedir. Ancak CMK'da elkoyma gerekçelerinin detaylı bir şekilde açıklanmamış olması eksiklik olarak görülmektedir[40].

CMK m. 134/4'de sistemdeki bütün verilerin yedeklemesinin yapılması durumunda bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilmesi ve bu hususun tutanağa geçirilerek imza altına alınmasına ilişkin düzenleme ile CMK m. 134/5'te düzenlenen

39 KESKİN, s. 156.

40 KUNTER/YENİSEY/NUHOĞLU, s. 1102.

bilgisayar veya bilgisayar kütüklerine elkoymaksızın da sistemdeki verilerin tamamının veya bir kısmının kopyasının alınabileceğine ilişkin hükmü de sözleşme ile uyumluluk göstermektedir.

Bununla birlikte, verilerin suç oluşturan içerik veya virüs programı ya da çocuk pornografisi gibi başlı başına suç unsuru veya suç aracı olması durumunda erişilmez kılınması ve hatta kopyaları alındıktan sonra taşınması veya silinmesi gerekmektedir. Sözleşmede bu hususta bir düzenleme getirilmesine rağmen CMK'da bu duruma ilişkin herhangi bir düzenlemenin bulunmaması önemli bir eksikliktir[41].

Sözleşme, arama ve elkoyma yetkisinin internet vb. telekomünikasyon ağları ile yasal olarak erişilebilen diğer sistemler ya da bilgisayar sistemine doğrudan bağlı bulunan veya yakınında bulunan veri depolama aygıtları için de genişletilebileceğini öngörmekte ve uygulamayı taraf devletlerin iç hukukuna bırakmakta ise de CMK m. 134'te bu yönde herhangi bir hükmün bulunmuyor olması bir diğer eksiklik olarak görülmektedir[42]. Bu eksiklik aşağıda inceleyeceğimiz üzere Adli ve Önleme Yönetmeliği m. 17/3 hükmü ile kısmen de olsa giderilmeye çalışılmıştır.

II. Adli ve Önleme Aramaları Yönetmeliği'nin 17. Maddesi'nin İncelenmesi

Adli ve Önleme Aramaları Yönetmeliği'nin 17. maddesinin 1, 2 ve 4. fıkraları CMK'nın 134. maddesinin 1, 2 ve 4. fıkraları ile birebir aynı niteliktedir. Yönetmeliğinin 17. maddesinin 3 ve 5. fıkralarına ise CMK'nın 134. maddesinin 3 ve 5. fıkralarındaki eksiklikleri gidermeye yönelik ek hükümler getirilmiştir.

Yönetmeliğinin 17/3 maddesi CMK'nın 134/3 maddesi ile paralel olarak "Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır" hükmü ile başlamış ancak CMK 134/3'de olmayan "Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır" hükmüne de yer verilmiştir.

Yönetmeliğe eklenen "Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır" ifadesi ile olay mahallindeki bilgisayarların yanı sıra

41 KUNTER/YENİSEY/NUHOĞLU, s. 1102.

42 KUNTER/YENİSEY/NUHOĞLU, s. 1102.

CD, DVD, disket, çıkarılabilir hafıza birimleri (usb memory, SD Card vb.) gibi veri depolama ünitelerinin yedeklenebileceği belirtilmektedir. Ayrıca, bu hüküm ile network'e (LAN, WAN gibi) bağlı bilgisayarlardan uzaktan yedekleme yapılabileceği öngörülmektedir. Yönetmelikte yapılan bu düzenleme, CMK m. 134/3'deki eksiklikleri giderme noktasında önemli bir adımdır[43].

Bununla birlikte, bilişim sistemlerinin yapısı ve bilgisayar sistemlerinin birbirlerine bağlanabilir olma özellikleri dikkate alındığında, bilgisayar verilerinin ağa bağlı başka bir sistemde saklanabilmesi de her zaman mümkündür. Bu bakımdan tek cümle ile ifade edilen bu düzenleme yetersiz olup arama ve elkoyma işleminin genişletilmesi hususunda sınırların mümkün oldukça net çizilmesine imkan sağlayıcı düzenlemelerin yapılması gerekmektedir[44].

Yönetmeliğinin 17/5 maddesi CMK'nın 134/5 maddesi ile paralel olarak "Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir" hükmü ile başlamış ancak CMK m. 134/5'de yer alan ve uygulamada çokça tartışılan "Kopyası alınan veriler kağıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır" hükmü yerine "Kopyası alınan verilerin mahiyeti hakkında tutanak tanzim edilir ve ilgililer tarafından imza altına alınır. Bu tutanağın bir sureti de ilgiliye verilir" hükmüne yer verilmiştir.

Yönetmelikte yapılan bu düzenlemeyle kopyalanan verilerin ne olduğu içerik olarak değil, liste bazında adlarının neler olduğu ele alınacaktır. Bu şekilde kopyalanan verilerin liste bazında adlarının neler olduğunun raporlanması yedekleme işleminde kullanılan bilgisayar programları ile raporlanabilmektedir. Bu sayede CMK m. 134/5 hükmünde belirtilen yığınlarca doküman çıktısı alma işlemine gerek kalmamaktadır[45].

III. Suç Eşyası Yönetmeliğinin 9. Maddesi'nin İncelenmesi

Elektronik deliller, hassas yapılarından dolayı, yanlış muhafaza koşulları altında kolaylıkla değişikliğe uğrayabilir, bozulabilir ya da yok olabilirler. Bu nedenle, elektronik delilleri muhafaza

43 AYDOĞAN, s. 23.

44 KUNTER/YENİSEY/NUHOĞLU, s. 1102-1103.

45 AYDOĞAN, s. 24.

etmek için özel önlemler alınması gerekir. Aksi halde, elektronik deliller kullanılamaz veya sonuca götüremez duruma gelebilirler. Bu bakımdan elektronik delillerin bu hassas yapıları Suç Eşyası Yönetmeliğinin 9. maddesinde ortaya konulmuştur.

Bu bağlamda, Suç Eşyası Yönetmeliğin "Kıymetli eşya ve evrak ile bozulacak, değerini kaybedecek veya muhafazası zor olan suç eşyası hakkında yapılacak işlemler" başlıklı 9. maddesinin 2. fıkrasında "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" hükmüne yer verilmiştir.

Siber Suç Sözleşmesi'nin " Saklanan Bilgisayar Verilerinin Hızlı Bir Biçimde Korunması" başlıklı 16. maddesinde elde edilen bilgisayar verilerinin silinmeden, değiştirilmeden, bozulmadan özgün niteliği ile korunması hedeflenmekte ve taraf ülkelere verilerin korunmasına yönelik bir takım yasama işlemlerini yerine getirme mükellefiyeti yüklemektedir. CMK m. 134'te bu konu ile ilgili herhangi bir düzenleme bulunmamaktadır.

Yönetmelikte yapılan bu düzenlemeyle CMK m. 134 hükmünde belirtilmeyen elektronik delillerin nasıl muhafaza edileceği sorununa çözüm getirilmiştir. Buna göre el konulan elektronik delillerin nem, ısı, manyetik alan ve darbelerden korunmalarını sağlayacak uygun ortamda muhafaza edilmeleri gerekmektedir. Bu düzenlemeyle CMK m. 134'de öngörülmeyen ve adli bilişim süreci bakımından da bir eksiklik niteliğinde olan "elektronik delil muhafaza etme" hususunun da düzenlemeye dahil edilmesi sağlanmıştır[46].

SONUÇ

Elektronik delillerin elde edilmesine ilişkin koruma tedbirleri, özel bilgi kullanımını gerektiren ve hızlı işleyen bir usul işlemidir. Diğer taraftan bu tedbirlerin kullanılması sonucunda elde edilen verilerin ceza yargılamasında delil olarak kullanılmalarını sağlayacak ve temel hak ve özgürlükleri korumaya yönelik garantilerle donatılmış özel yasal yetkileri de içermesi gerekmektedir. Bu bakımdan bu tedbirlerin uygulanmasına yönelik yasal düzenlemelerde hem elektronik delillerin kullanıldığı suçlarla mücadele imkanını

46 AYDOĞAN, s. 25

sağlayacak hem de bunu yaparken kişilerin temel hak ve özgürlüklerini müdahale niteliği taşıyan bu tedbirlerin uygulamasını ölçülülük ilkesine bağlı kalarak gerçekleşmesini sağlayacak yasal düzenlemelere ihtiyaç duyulmaktadır.

Türk hukukunda elektronik delillerin elde edilmesine yönelik usul işlemleri Ceza Muhakemesi Kanununda yapılan tek maddelik bir yasa hükmüyle düzenlenmeye çalışılmıştır. CMK'nın 134. maddesinde ifadesini bulan bilgisayar, bilgisayar programları ve bilgisayar kütüklerinde arama, kopyalama ve elkoyma koruma tedbirine ilişkin hükmü, en önemli temel hak ve özgürlüklerden olan özel hayatın gizliliğinin ve kişisel verilerin korunması bakımından gerek Avrupa İnsan Hakları Sözleşmesinin 8. maddesine gerekse Anayasa'nın 20. maddesine aykırılık teşkil etmemektedir. Bununla birlikte tedbirin uygulanması sırasında yasa hükümlerinin doğru yorumlanmaması veya kolluğun yanlış tutumundan kaynaklı ihlallerin gündeme geldiği de bir gerçektir.

Özellikle bilgisayarın tüm niteliklerine haiz olması nedeniyle bilgisayar tanımı içerisinde kabul edilmesi gereken ve fakat uygulamada bilgisayar olarak tanımlanmayan cep telefonu, cep bilgisayarı ve elektronik veri barındıran bir çok cihazın CMK m. 134 hükmü yerine CMK m. 116 ve 123 hükümlerine göre arama ve elkoyma işlemlerine tabi tutulması temel hak ve özgürlükler bakımından ihlallere neden olabilmektedir. Bu bakımdan madde metninde belirtilen ve söz konusu koruma tedbirin konusunu teşkil eden bilgisayar, bilgisayar programları ve bilgisayar kütükleri terimlerinin uygulamadaki tereddütü ortadan kaldıracak şekilde yeniden düzenlenmesi yerinde olacaktır.

Diğer taraftan Avrupa Siber Suç Sözleşmesinin 14 ila 21. maddelerinde elektronik delillerin elde edilmesi ve korumasına ilişkin koruma tedbirleri düzenlenmiştir. Sözleşmenin 19. maddesinde ise "Saklanan bilgisayar verilerinin aranması ve bunlara el konulması" ele alınmıştır. CMK m. 134'deki söz konusu düzenlemenin de büyük ölçüde Sözleşmenin 19. maddesinde düzenlemeye uygunluk gösterdiği söylenebilir.

Bununla birlikte Sözleşmede yer alan suç unsuru veya suç aracı olan verilerin erişilmez kılınması ve hatta kopyaları alındıktan sonra taşınması veya silinmesine ilişkin hükmünün CMK m. 134'de yer verilmeyerek maddede sanki bu tür verilerin de şüpheliye iade

edilebileceği anlamına gelen ifadelere yer verilmesi, söz konusu yasal düzenleme için getirebilecek en önemli eleştirilerden birini teşkil etmektedir. Bu nedenle mevcut eksikliğin bir an önce giderilmesi gerekmektedir.

Ayrıca yukarıda açıklamaya çalıştığımız ve CMK m. 134'de eksik düzenlenen veya hiç düzenlenmeyen bazı hususlar Adli ve Önleme Arama Yönetmeliğinin 17. ve Suç Eşyası Yönetmeliğinin 9. maddelerinde giderilmeye çalışılmış ise de bu eksikliklerin tam manasıyla giderilebildiğini söylemek çok da mümkün olmamıştır. Kaldı ki; özellikle bilişim suçlarının etkin şekilde soruşturulmasında birinci derece önemli olan ve temel hak ve özgürlükleri doğrudan ilgilendiren bir yasa hükmündeki eksikliklerin yönetmelikle giderilmeye çalışılması da doğru değildir. Bu bakımdan mevcut eksikliklerin de kapsamlı bir yasal değişiklikle giderilmesi yerinde olacaktır.

***

KAYNAKÇA

AYDOĞAN, Hakan, Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri, Polis Akademisi, Güvenlik Bilimleri Enstitüsü, Yüksek Lisans Tezi, Ankara, 2009

BALI, Yunus, CMK 134. madde düzeltilmelidir, **http://www.dijitaldeliller**.com/cmk134.htm (İET: 04.03.2014)

BİLİŞİM AJANDASI, Nihayet Türkiye de "Sanal Suçlar Sözleşmesi"ni imzaladı, Bilişim Kültür Dergisi, Yıl: 2010, s. 10-12, **http://www.bilisimdergisi.org/s127**, (İ.E.T: 04.03.2014)

CENTEL, Nur/Hamide Zafer, Ceza Muhakemesi Hukuku, 5. Bası, Beta Yayınevi, İstabul, 2008

ÇOLAK, Haluk/TAŞKIN, Mustafa, Açıklamalı-Karşılaştırmalı-Uygulamalı Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, Ankara, 2005

DAĞ, Güray, Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, Doktora Tezi, İstanbul, 2011

EROĞLU, Sevilay, Rekabet Hukukunda Bilgisayar Programlarının Korunması, Beta Yayınevi, İstabul, 2002

HEKİM, Hakan/BAŞIBÜYÜK, Oğuzhan, Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları, Uluslararası Güvenlik ve Terörizm Dergisi, Yıl: 2013, Cilt: 4, Sayı: 2, s. 135-158

İÇEL, Kayıhan, Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında "Avrupa Siber Suç Politikasının Ana İlkeleri", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Yıl: 2001, Cilt: 59, Sayı: 1-2, s. 3-10

KARAGÜLMEZ, Ali, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, 2. Baskı, Seçkin Yayıncılık, Ankara, 2011

KESKİN, Serap, Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Yıl: 2001, Cilt: 59, Sayı: 1-2, s. 155-180

KUNTER, Nurullah/YENİSEY, Feridun/NUHOĞLU, Ayşe,

Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, 18. Bası, Beta Yayınevi, İstanbul, 2010

ÖLMEZ, Aslan, Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Kopyalama ve Bunlara El Koyma, Terazi Hukuk Dergisi, Yıl: 2009, Sayı: 30, s. 45-52

ÖZBEK, Veli Özer, Ceza Muhakemesi Hukuku, Seçkin Yayıncılık, Ankara, 2006

ÖZTÜRK, Mustafa İlker, Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri, Ankara Üniversitesi, Sağlık Bilimleri Enstitüsü, Yüksek Lisans Tezi, Ankara, 2007

PARLAR, Ali/HATİPOĞLA, Muzaffer, 5271 Sayılı Ceza Muhakemesi Kanunu Yorumu ve İlgili Mevzuat, 1. Cilt, Ankara, 2008

ŞAHİN, Cumhur, Ceza Muhakemesi Hukuku I, Seçkin Yayıncılık, Ankara, 2007

ŞEN, Ersan/YURTTAŞ, Yasemin, Bilgisayar Programları Karşısında Özel Hayatın Korunması, Terazi Hukuk Dergisi, Yıl: 2010, Sayı: 42, s. 28-44

www.tdk.gov.tr, İ.E.T: 27.02.2014