

BİLİŞİM SİSTEMLERİ ÜZERİNDE ARAMA, KOPYALAMA VE EL KOYMA TEDBİRİ

Yrd. Doç. Dr. Murat Volkan Dülger¹

Günümüzde ister bilişim suçu olsun, ister klasik suçlar olsun bilişim sistemlerinin kullanılmadığı ya da suçun izlerinin bilişim sistemleri üzerinden takip edilmediği bir eylem neredeyse kalmamıştır. Ancak suçun ve suçlunun araştırılması bilimsel bir yaklaşım ve hukuki bir alt yağı gerektirmektedir. Ülkemizde bu alt yapı 5271 sayılı CMK'nın 134. maddesiyle yapılmıştır. Makalemizde bu önemli yasa maddesiyle yapılan düzenleme hakkında bilgi verilmektedir².

1. Yasal Dayanak

Bilişim sistemlerine karşı veya bilişim sistemleri kullanılmak suretiyle bir suç işlendiğinde yapılması gereken en önemli işlemlerden biri söz konusu sistem üzerinde inceleme yapılmasıdır. Bu sistem suçun failine ait olabileceği gibi mağdura ya da üçüncü bir kişiye de ait olabilir. Ancak bu arama işleminin, aynen evde ya da iş yerinde yapılan aramalar gibi, bir yasa normuna dayanılarak yapılması gerekir; zira bu temel hak ve özgürlükleri kısıtlayan bir işlemdir. Aksi takdirde keyfi ve hukuksuz uygulamaların gerçekleşmesi kaçınılmazdır. Bu ise hem maddi gerçeğin ortaya çıkarılmasına zarar verecek hem de elde edilen deliller gerçeği yansıtsa da hukuka aykırı elde edildiği için yasak delil olacak ve soruşturmada ve kovuşturmada kullanılamayacaktır. İşte bu nedenlerle 5271 sayılı CMK'nın 134. maddesinde “bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma” başlığı altında bilişim sistemlerinde yapılacak delil araştırması yöntemi düzenlenmiştir. Ayrıca *Adli ve Önleme Aramaları Yönetmeliği*'nin 17. maddesinde de yasa maddesindeki aynı başlıkla düzenleme yapılmıştır. Ancak birkaç ifade dışında yönetmelikte CMK'nın 134. maddesi aynen tekrar edilmiştir.

2. Somut Delillere Dayanan Kuvvetli Şüphe Sebeplerinin Varlığı

CMK'nın 134. maddesinin 1. fıkrasında “Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkanının 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 haline getirilmesine hakim tarafından karar verilir.” denilmektedir.

¹ İstanbul Medipol Üniversitesi, Hukuk Fakültesi Ceza ve Ceza Muhakemesi Hukuku Öğretim Üyesi; İstanbul Medipol Üniversitesi Bilişim Hukuku Uygulama ve Araştırma Merkezi Müdürü; İstanbul Barosu Bilişim Hukuku Komisyonu Başkanı.

² Konu hakkında ayrıntılı açıklama için bkz: **Murat Volkan Dülger**, Bilişim Suçları ve İnternet İletişim Hukuku, 5. Baskı, Ankara, Seçkin Yayıncılık, 2014.

Maddede özellikle “*şüphelinin kullandığı*” ifadesine yer verilmiştir; zira üzerinde arama ve kopyalama işlemi yapılacak bilişim sisteminin şüpheliye ait olması gerekmez. Şüphelinin maliki olduğu, kiraladığı, ödünç aldığı ya da ortak kullanıma açık bir bilgisayarı eylemini gerçekleştirirken kullanması bu tedbirin uygulanması için yeterlidir. Ancak delile ulaşmak için sadece failin kullandığı bilişim sisteminde arama yapılması yeterli değildir. Bazı durumlarda failin kullandığı sistemle birlikte söz konusu kişilerin hatta yalnızca üçüncü kişilerin bilişim sistemlerinde bu tedbirin uygulanması gerekebilecektir. Yasanın bu durumu düzenlememiş olması bize göre önemli bir eksiklik ve yapılacak bir düzenleme ile bu eksiklik giderilmelidir.

Bilişim sistemlerinde delil elde etmek için araştırma yapılabilmesi için öncelikle “*somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı*” ve “*başka surette delil elde etme imkânının bulunmaması*” gerekir. Somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı şartı bu maddenin ilk halinde bulunmaktaydı. 21.2.2014 tarih ve 6526 sayılı “*Terörle Mücadele Kanunu ve Ceza Muhakemesi Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun*”un 11. maddesiyle CMK’nın 134. maddesinde yapılan değişiklik ile bu ifade maddeye eklenmiştir³. Buna göre bilişim sistemlerinde arama (veya elkoyma) koruma tedbirinin uygulanabilmesi için öncelikle iki şartın birlikte bulunması gerekir. Bunlardan ilki yasa değişikliği ile fıkraya eklenen “*somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı*”dır.

CMK ya da öğretimizde “*somut delil – soyut delil*” ayrımı yapılmamıştır, mantıksal olarak böyle bir ayrımın yapılması da anlamsızdır. Deliller, yargılama konusu olayı temsil eden ve ister beyana, ister belgeye ister ise belirtilere dayansınlar somut olan olgulardır; dolayısıyla burada somut delil kavramı, soyut delil kavramı karşılığı olarak kullanılmadığı kanısındayız. Öte yandan Anglosakson hukuk sisteminde “*somut (gerçek) delil – ikrar delili*” ayrımı yapılmaktaysa da⁴, ülkemizin de dâhil olduğu Kıta Avrupa’sı hukuk sisteminde böyle bir ayrım bulunmamaktadır. Nitekim ülkemiz ceza muhakemesi hukuk sisteminde yukarıda belirttiğimiz üzere ikrarı da kapsayan beyan delilleri, somut delil niteliğindedirler. O halde geriye kalan tek seçenek, bu kavramın, ulaşılabilir, gerçekçi (rasyonel – akılcı) delillerin karşılığı olarak kullanılmasıdır⁵. Ancak bunların ayrıca belirtilmesine gerek yoktur, zira bunlar zaten ceza muhakemesinde kullanılabilecek delillerin biz özelliği olup, delil kavramının içinde yer alırlar.

Kuvvetli şüphe ise, genellikle koruma tedbirleri için ön şart olarak aranan şüphe türüdür. Örneğin CMK’nın 100. maddesinde tutuklama kararı verilebilmesi için “*kuvvetli suç şüphesinin varlığını gösteren olguların ...bulunması halinde, şüpheli veya sanık hakkında tutuklama kararı verilebilir*” denilerek bu tür bir şüphenin varlığı aranmıştır. Kuvvetli şüphe,

³ 21.2.2014 tarihli ve 6526 sayılı Kanunun 11 inci maddesiyle, bu maddenin birinci fıkrasında yer alan “soruşturmada,” ibaresinden sonra gelmek üzere “somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve” ibaresi eklenmiş ve dördüncü fıkrasında yer alan “İstemesi halinde, bu” ibaresi “Üçüncü fıkraya göre alınan” şeklinde değiştirilmiştir.

⁴ Bu konuda bkz: **Kerri Mellifont**, Fruit of the Poisonous Tree – Evidence Derived from Illegally or Improperly Obtained Evidence, Sydney, The Federation Press, 2010, s.7, 8.

⁵ Delillerin ayrımı konusunda bkz: **Murat Volkan Dülger**, Ceza Muhakemesi Hukukunda Dışlama Kuralı ve Hukuka Aykırı Delillerin Uzak Etkisi (Zehirli Ağacın Meyvesi Öğretisi), Ankara, Seçkin Yayıncılık, 2014.

şüphelinin/sanığın suçu işlediği konusunda, somut olaylarla desteklenmiş, dayanağı olan delille mahkûmiyet kararı verilebilmesinin kuvvetle muhtemel olduğu şüphedir. Yasaya göre failin yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe var ise, şüphelinin veya sanığın üstü, eşyası, konutu, işyeri veya ona ait diğer yerler aranabilir (CMK m.116). Eldeki delillerle yapılacak muhakeme sonucunda, sanığın mahkûm olması olasılığı, beraat etmesi olasılığından daha fazla ise “*yeteli şüphe (delil)*” söz konusudur. Kamu davasının açılabilmesi için “*yeterli şüphe*” aranmıştır (CMK m.170/2)⁶.

İşte kuvvetli şüphe, bunların da üstünde, mahkûmiyetin çok yüksek bir ihtimalle gerçekleşeceği durumlarda söz konusu olur. Dolayısıyla madde metnine yapılan ekleme ile inceleme konusu koruma tedbirinin uygulanması zorlaştırılmak istenmiştir. Bundan sonra söz konusu tedbir talep edilirken ve karar verilirken çok dikkatli ve titiz olunması gerekir. Aksi takdirde deliller hukuk aykırı olarak elde edilmiş olacak ve kullanılmaları mümkün olmayacaktır.

3. Başka Surette Delil Elde Etme İmkânının Bulunmaması

Yukarıda da belirttiğimiz üzere, “*somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı*” inceleme konusu arama (ve el koyma) tedbirine karar verilmesi için yeterli değildir. Bunun yanı sıra “*başka surette delil elde etme imkânının bulunmaması*” da gerekir. İki ifadenin arasında “ve” bağlacı bulunduğu için somut olayda tedbire karar verilmesi için her iki ön şartın birlikte bulunması gerekir.

Yürürlükte bulunan hukuk açısından bu şartlar gerçekleşmeden karar verilmesi hukuka aykırıdır ve bu şekilde verilen karar neticesinde elde edilen deliller de “*hukuka aykırı delil*”dir ve CMK m.217/2 gereğince hükme esas alınmamalıdır.

Somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ile başka surette delil elde etme imkânının neden bulunmadığı ve hangi nedenlerle bu yola başvurulduğu hem savcılığın talep yazısında hem de hâkimin kararında açık ve gerekçeli bir şekilde belirtilmelidir. Ancak bugüne kadarki uygulamada, bazı istisnalar dışında, bu kurala hemen hemen hiç uyulmadığı, yalnızca “yasa maddesi tekrar edilerek” talepte bulunulduğu ve karar verildiği görülmektedir. *Dolayısıyla verilen kararların büyük çoğunluğu hukuka aykırıdır.* Beklentimiz CMK’nın 134. maddesinde yapılan değişiklikten sonra, artık bu konuda hassasiyet gösterilmesi ve hem taleplerin hem de kararların yasanın şartlarını karşılar şekilde gerekçelendirilmesidir.

Ayrıca ön koşul niteliğindeki “*başka surette delil elde etme imkânının bulunmaması*” halinin soruşturma evresinin hangi aşamasında belirleneceği de belli değildir. CMK’nın 134. maddesinin normatif yapısı gereği, soruşturmaya konu yapılan suçla ilgili olarak belirli bir delil araştırmasının yapılmış olması, bu araştırmanın sonucunda bir delil elde edilememiş olması ve bunun da açıkça tutanağa bağlanması gerekir.

Olması gereken hukuk açısından, bu şartın aranmasının özellikle bilişim suçları ve bilişim sistemleri aracılığıyla işlenmiş suçlar için yapılacak soruşturmalar açısından son derece hatalı olduğu kanaatindeyiz. Zira bilişim sistemlerine karşı ya da bilişim sistemleri

⁶ Nur Centel/Hamide Zafer, Ceza Muhakemesi Hukuku, 10. Bası, İstanbul, Beta Yayıncılık, 2013, s.78, 79.

aracılığıyla işlenen suçlarda yapılması gereken ilk iş, sistemin yapısı ve veri bütünlüğü bozulmadan içindeki verilerin ve bağlantıların tespit edilmesidir. Bu suçlar hakkında yapılan soruşturmalarda genellikle başka şekilde delil elde etme imkânı da bulunmamaktadır. Başka şekilde delil elde etmeye çalışıldıktan sonra en son çare olarak bilişim sistemlerinde araştırma yapılmaya girişildiğinde ise çok geç kalınmış olacak, faillere ve delillere ulaşmak son derece güçleşecektir. *Nitekim uygulamada soruşturmaların tümünde bu maddenin sanki böyle bir ön şart yokmuş gibi uygulanmasının altında yatan gerekçe de budur.*

Bu görüşümüze karşın, her suç soruşturması için ilk olarak bilişim sistemlerinde arama ve el koyma koruma tedbirinin uygulanması halinde kişisel verilerin güvenliğinin ve özel hayatın gizliliğinin kalmayacağı şeklinde içinde haklılık payı olan bir karşı görüş de ileri sürülebilir. Ancak bu eleştirinin de CMK'nın 134. maddesiyle eklenen *“somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı”* şartının gerçek anlamda uygulanması suretiyle karşılanması mümkündür.

Bu görüşler doğrultusunda, bilişim suçu soruşturmalarının gerektirdiği hız dikkate alınarak, 134. maddenin 1. fıkrasına getirilecek bir istisna hükmüyle, *“TCK'nın bilişim alanında suçlar bölümünde ve 135, 136, 138, 142/2-e 158/1-f maddelerinde yer alan suçlar için başka surette delil elde etme imkânının bulunmaması şartı aranmaz”* denilmek suretiyle kısmen hatalı norm ve yanlış uygulama düzeltilebilir. Ancak bugünkü haliyle hem madde düzenlemesi hatalıdır, hem de uygulama ve bu yöntemle elde edilen deliller hukuka aykırıdır.

Ayrıca maddede *“bilgisayar, bilgisayar programları ve bilgisayar kütükleri”* terimleri yerine kısaca *“bilişim sistemi”* denmesi yeterli olurdu. Maalesef TCK'da günümüze uygun bir terminoloji kullanılması rağmen CMK'da aynı yöntem izlenmemiştir. Bilgisayar kütüğü terimiyle ifade edilmeye çalışılan, sabit ya da taşınabilir her türlü veri taşıyan ve depolamaya yarayan araçlardır.

4. Arama ve Kopyalama Tedbiri

134. maddenin 1. fıkrasının metninde açıkça anlaşıldığı üzere bu tedbir kural olarak; şüphelinin kullandığı bilişim sistemlerinde arama yapılması, sistemdeki verilerin kopyasının çıkarılması ve kayıtların çözümünün yapılarak metin haline getirilmesini içermektedir. Yani *kural olan arama tedbiridir*; şüphelinin kullandığı bilişim sistemi olduğu yerde bırakılacak ve kopyalama işlemi sistemin bulunduğu yerde yapılacaktır. Ayrıca kolluk güçleri sistemin ya da veri taşıma aracının aslını almayacaktır. Kural olan budur ve öncelikle bu tedbirlerin uygulanması gerekir.

CMK'nın ilk halinde, şüphelinin veya müdafinin talebi halinde alınan yedeklemelerin bir kopyasının talepte bulunana verileceği düzenlenmiştir. Biz de o dönemde soruşturmalarda müdafilik görevini üstelenen tüm meslektaşlarımıza, bu kopyayı mutlaka almalarını, ileride delillerin bütünlüğünün ve dolayısıyla güvenilirliğinin denetlenebilmesi için bu kopyanın çok önemli olduğunu özellikle ifade ediyor idik.

Yasa koyucu, düzenlemeye ilişkin öğretici ve uygulamadan gelen eleştirileri dikkate alarak, 21.2.2014 tarih ve 6526 sayılı Yasanın 11. maddesiyle CMK'nın 134. maddesinde

değişiklik yapmış⁷, 4. fıkra da yer alan “*istenmesi halinde*” ifadesini maddeden çıkartarak yerine “*üçüncü fıkraya göre alınan*” ifadesini getirmiştir. Böylelikle arama tedbiri sonucu çıkartılan yedeğin bir kopyasının şüpheli veya müdafine verilmesi isteğe bağlı olmaktan çıkartılmış ve zorunlu hale getirilmiştir. Bu değişikliği olumlu karşıladığımızı belirtmeliyiz.

5. El Koyma Tedbiri

134. maddenin 2. fıkrasında ise 1. fıkranın istisnası olarak el koyma tedbiri düzenlenmiştir. Buna göre “*Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülmemesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.*”

Bu fıkra çok açık biçimde bir istisnayı düzenlemesine rağmen, ülkemiz mevzuatında yer alan pek çok istisna hükmünün uygulamada kural haline getirilmesinde olduğu gibi, bilişim sistemlerinde yapılan aramalarda da bu istisna, kural haline getirilmiştir. Kolluk güçleri CMK’nın 134. maddesine göre yaptıkları aramaların tamamında 2. fıkradaki istisna hükmünü işletmekte, bunun için arama yapacakları bilişim sisteminde şifre olduğuna ilişkin işleme katılan diğer kolluk güçleriyle birlikte bir tutanak tutmakta ve böylelikle yasayı dolanmak suretiyle görünüşte de olsa yasaya uygun davrandıkları düşüncesiyle görevlerini yerine getirmektedirler. Bunun gerekçesi olarak ise “*yeterli personellerinin olmadığını, eğer sistemin olduğu yerde arama ve kopyalama yapmaya kalkarlarsa hiçbir işi yetiştirmeyeceklerini*” beyan etmektedirler. Aslında içinde büyük oranda gerçeklik payı olan bu bahane yasa maddesini değiştirme hakkını vermediği gibi bu şekilde elde edilen delili de hukuka uygun hale getirmemektedir. Zira tutulan tutanaklarda ne tür bir şifrenin ya da gizli verinin bulunduğu, bunun işin uzmanı olan bilişim polisi tarafından neden etkisiz kılınmadığına ilişkin herhangi bir kayıt bu tutanaklarda yer almamaktadır. Dolayısıyla bu tutanağın gerçekle bir ilgisi ve denetlenebilir bir tarafı olmadığı gibi, hukuken hiçbir değeri de bulunmamaktadır. Bu işlem açıkça yasanın arkasına dolanmaktadır ve hukuka aykırıdır. Söz konusu işlemin yapılış şekli hukuka aykırı bir delil elde etme yöntemi olduğu gibi bu yolla elde edilen deliller de yasak delil niteliğindedir ve yargılamanın hiçbir aşamasında kullanılmamaları gerekir.

134. maddenin 3. fıkrasında “*Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.*” denilmek suretiyle 2. fıkradaki istisna hükmünün uygulanması halinde yapılması gerekenlere yer verilmiştir. Bununla bağlantılı olarak 4. fıkrasında 6526 sayılı Yasa ile değişiklik yapılarak “*Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.*” denilmek suretiyle el koyma tedbirinin uygulanması halinde çıkarılan yedeğin bir kopyasının şüpheliye veya müdafine verilmesi bir zorunluluk halinde getirilmiştir.

⁷ RG., 6.3.2014, 28933.

Düzenlemeler bu şekilde olmakla birlikte uygulama böyle olmamaktadır. Kolluk güçleri bilişim sistemleri üzerinde arama, kopyalama ve el koyma tedbiri için bilişim sisteminin bulunduğu yere gittiklerinde yukarıda da belirttiğimiz üzere yasayı dolanarak el koyma tedbirini uygulamakta ve yedek alma işlemini de kendi çalıştıkları merkezlerde yapmaktadırlar. Yedekleme için gerekli olan veri depolama araçlarını da şüpheliden istemektedirler. Bu uygulama tamamen hukuka aykırıdır. Çünkü el koyma koruma tedbiri uygulandığında yedekleme işlemi, soruşturmanın güvenilirliği, tarafsızlığı ve adil yargılanma hakkına uygunluğu açısından son derece önem taşımaktadır. Şöyle ki:

Üzerinde tedbir uygulanan bilişim sisteminin sabit diski ya da veri taşıma aracı örneğin 320 GB veri taşıma kapasitesine sahiptir. Ancak bunun tamamı hiçbir zaman kullanılmamaktadır. Örneğin; bu diskte 100 GB veri olduğunu kabul ettiğimizde geri kalan 220 GB boştur. Yalnızca veri bulunan kısımlar yedeklendiğinde boş kalan 220 GB’lık kısımlara daha sonra başka verilerin yazılması mümkündür. Dolayısıyla dolu ve boş kısımlarıyla tüm diskin olduğu gibi yedeklenmesi teknik tabiriyle “*imajının alınması*” ve bunun sonucunda “*hash değeri*”nin alınması yani işlem yapıldıktan sonra diskin bir nevi mühürlenmesi gerekir. İşlemlerin şüpheli ve müdafî önünde yapılmaması halinde, imaj alınmadan önce veri yerleştirildiği ve daha sonra imaj alındığı şüphesi ve iddiaları daima söz konusu olacaktır. Bu durum doğru ve adilane yürütülen soruşturmaların da güvenilirliğini etkileyecektir. Oysa adil yargılanma hakkının ihlal edilmemesi için hem görünüşte hem de içerikte tüm soruşturma ve yargılama işlemlerinin tarafsız ve hukuka uygun şekilde, dürüst işlem ilkesi uyarınca yerine getirilmesi gerekir. Ayrıca bilişim sistemleri üzerinde yapılan adli bilişim incelemeleri daima bu yedekler üzerinde yapılmaktadır; delilin aslının saklanması ve ileride söz konusu olabilecek itirazlarda incelenmek üzere bozulmamış halde muhafazası için aslı üzerinde hiçbir işlem yapılmaması gerekir.

Oysa uygulamada bilişim sistemleri kolluk güçleri tarafından yasa maddesi dolanılmak suretiyle olduğu yerden alınarak kolluk merkezlerine götürülmekte, yedekleme ve hash değerlerinin alınması şüpheli ve/veya müdafinin olmadığı ortamda yapılmaktadır. *Bu uygulama kesinlikle hukuka aykırıdır!* Bu yöntemle delil elde edilmesi hukuka aykırı olduğu gibi, elde edilen deliller de yasak delildir; kullanılması ve hükme esas alınması mümkün değildir. Ne yazık ki; bugün ülkemizde yürütülen “kamuoymunda en çok yer alanlar da dâhil olmak üzere” davaların hemen hepsinde bu tür deliller kullanılmakta ve adil yargılanma hakkı ihlal edilmektedir.

134. maddenin son fıkrasında ise “*Bilgisayar ve bilgisayar kütüklerine el koymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kağıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır.*” denilmek suretiyle yukarıdaki düzenlemelerle çelişki yaratan bir fıkra yer verilmiştir. Çünkü yukarıda belirttiğimiz üzere bilişim sistemlerinden delil elde edilmesinde kural, bilişim sisteminin olduğu yerde arama yapılması ve sistem verilerinin kopyalanmasıdır; el koyma ise istisnadır. Oysa bu fıkradaki düzenlemede sanki el koyma kural, bu tedbir uygulanmadan sistemin olduğu yerde kopyasının alınması istisna imiş gibi bir anlam

çıkılmaktadır. Dolayısıyla bu fıkra gereksiz yere maddede yer alan ve anlam karışıklığına yol açan bir düzenlemedir.

6. CMK m.134 Özel Bir Düzenlemedir

CMK'nın 116. ve 123. maddelerindeki genel nitelikteki arama hükümlerine rağmen 134. maddeye yer verilmesi bunun özel nitelikte bir düzenleme olduğunu göstermektedir. Dolayısıyla 116. maddeye dayanılarak şüphelinin işyeri ya da konutunda yapılan bir arama sırasında ayrıca 134. maddeye göre arama yapılmasına ilişkin bir karar alınmamışsa, şüphelinin kullandığı bilgisayarlar üzerinde arama yapılması mümkün değildir. 116. maddeye dayanılarak yapılan aramada şüphelinin üzerinden çıkan bilgisayar özelliklerine sahip cep telefonunda arama yapılması için dahi 134. maddeye göre karar alınması gerekir. Buna uyulmaksızın yapılan aramalar hukuka aykırı yöntemle delil elde etme olacak ve elde edilen delil de yasak delil niteliğinde olacaktır.

7. Uygulamadaki Eleştiriler ve Uygulanan Yöntem

Dikkat edilirse ne CMK'nın 134. maddesinde ne de yönetmelikte *“imaj alma”* dan ya da *“hash değeri”*nden bahsedilmemektedir. Bunun yerine *“yedek alma”* ve *“kopyalama”* terimleri kullanılmaktadır. Oysa yukarıda açıkladığımız üzere, bir veri taşıma aracının yedeğinin ya da kopyasının alınması ile imajının alınması ve bunun sonucunda hash değerinin elde edilmesi çok farklı işlemlerdir. Yedekleme ve kopyalamada, boş sektörler kopyalanmadığı gibi, veri bütünlüğü ve güvenliği de sağlanamaz. Bu ise dijital verilerin *“güvenilir delil”* olma özelliğini ortadan kaldırır. Bu yöntemlerin ne CMK'da ne de yönetmelikte düzenlenmemesi büyük bir eksikliklerdir.

Uygulamada ise soruşturma görevlileri *“tamamen kendi iyi niyetleri ve görevi düzgün yapma istekleriyle”*, bu alandaki uluslararası standartları takip ederek her soruşturmada imaj ve hash değerini almaktadırlar. Ancak bu işlemi yapmasalar, kendilerine neden bu standardı kullanmadıklarını sorgulayacak bir yasal dayanak mevzuatımızda bulunmamaktadır. Bu büyük eksikliğin bir an önce hem CMK'da hem de yönetmelikte yapılacak değişiklik ile giderilmesi gerekir.

Yukarıda da belirttiğimiz üzere soruşturma görevlilerine yapılan önemli bir eleştiri, arama (imaj alma) işleminin veri taşıma aracının bulunduğu yerde değil, el koyma tedbiri uygulanmak suretiyle soruşturma görevlilerinin bulunduğu merkezde yapılması, istisna olan el koyma tedbirinin kural haline getirilmesidir. Söz konusu görevliler bunun gerekçesi olarak haklılık payı olan bazı gerekçeler ileri sürmekte ve çözüm yolları da üretip uygulamaktadırlar. Söz konusu gerekçelerden bazıları şunlardır:

- Yeterli sayıda ve nitelikte adli bilişim uzmanı ve olay yeri inceleme ekibi bulunmaması,
- Çoğunlukla şifrelerin çözülmesinin ya da gizlenmiş verilerin bulunmasının uzun zaman ve özel ekipman gerektirmesi,

- Uzun zaman alan arama faaliyeti sırasında, üzerinde arama yapılan bilişim sisteminin bulunduğu, ev ya da iş yerinde bulunan kişilere rahatsızlık verilmesi ya da bu yerlerin çalışmaya uygun ve/veya hijyenik olmaması,
- Bilişim sisteminin imajının alınacağı yerde, veri bütünlüğünün sağlanması için kesintisiz güç kaynağının bulunmaması, özellikle veri kurtarma yapılması gereken durumlarda toz olmayan ve özel ekipmanların bulunduğu ortamlarda bu işlemlerin yapılması gerekliliği.

Bu listeyi daha uzatmak mümkündür ve bunlarda haklılık payının olduğu da bir gerçektir. Soruşturma görevlileri, hem yukarıda anılan olumsuzluklardan kurtulmak hem de delillerin hukuka aykırı olarak elde edildiği –haklı– itirazını engellemek için şu şekilde bir yöntem uygulamaktadırlar:

CMK'nın 134. maddesine göre arama ve el koyma tedbirinin uygulanmasına ilişkin kararı aldıktan sonra, tedbirin uygulanacağı yere gitmekte ve şüphelinin kullandığı tüm veri taşıyabilen araçları usulünce fişten çektikten sonra bunları özel yapılmış torbalara koymakta ve ağzını mühürlemektedirler. Bu esnada yapılan tüm işlemleri tutanağa bağlamaktadırlar. Merkeze götürülen bu araçlar üzerinde inceleme yapılacağı zaman duruma göre şüpheli ve/veya müdafii incelemenin yapılacağı merkeze çağrılmakta ve bu işlem için hazırlanmış özel yere alınmaktadırlar. Adli bilişim uzmanı tozdan arındırılmış özel yerlerinde araçlar üzerinde inceleme yaparlarken, buraya yerleştirilmiş kameralar sayesinde, şüpheli ve/veya müdafii kendilerine ayrılan yerde kameralardan aktarılan bu görüntüleri canlı olarak monitörlerden izlemektedirler. Böylelikle bir yandan araçların olduğu yerde inceleme zorunluluğundan kurtulup kendi laboratuvarlarında inceleme yaparlarken, bir yandan da verilere müdahale edildiği ve hukuka aykırı delil elde edildiği itirazından kurtulmaya çalışmaktadırlar.

Bu sadece soruşturma görevlilerinin oluşturduğu ve uyguladığı bir yöntemdir. Bunun, bir benzerinin ya da daha gelişmişinin bir an önce yasal bir zemine oturtulması ve bir an önce uygulamaya geçirilmesi gerekir. Aksi takdirde ülkemizde hem “hukuka aykırı delil” elde edilmeye devam edilecek, hem de bilişim suçları ve bilişim sistemleri aracılığıyla işlenen suçlar hakkında “olması gerektiği şekilde” soruşturma yapılamayacaktır.