International Journal of Human Sciences
ISSN:1303-5134

Volume: 12 Issue: 2 Year: 2015

Search, copy and seizure on the computers in the Turkish legal system

Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma

Ümit Bostancı[1]
Recep Benzer[2]

Abstract

In the context of computer forensics, computer is merely the one of the devices that can be used to commit IT crime. Nowadays, there is an increase related to IT crimes committed consciously or unconsciously. In addition, cyber crimes can be committed through a variety of electronic devices. In related to this matter, there are some legal regulations in both Turkish Penal Code and Law of Criminal Procedure.

In the globalizing world, together with expansion of use of Internet quickly, uncontrolled and unconsciously, dimension of IT crimes have become beyond the country's border and cooperation with each of the countries to struggle with this issue has become compulsory. Indeed, as investigation are getting deeper, a computer crime that seems to have been commited in a country through misleading IP addresses can be observed that this crime actually had been committed in an another country.

In an investigation or prosecution phase of a committed cyber crime, searching on the computer, copying data of the computer and even seizing the computer as an evidence of a crime may be required.

In societies using Information systems so intense; making more specific regulations regarding how incident response of cyber crimes and other crimes committed by means of

Özet

Adli bilişim bağlamında bilgisayar, bilişim suçu işlemede kullanılabilecek aygıtlardan sadece birisidir. Günümüzde bilişim suçlarının bilinçli ya da bilinçsiz olarak işlenmeleri ile ilgili göze çarpan bir artış söz konusudur. Ayrıca bilişim suçları çeşitli elektronik aletler vasıtasıyla işlenebilmektedir. Bu konuyla ilgili olarak gerek TCK'da gerek Ceza Muhakemeleri Kanununda bazı yasal düzenlemeler yer almaktadır.

Globalleşen dünyada İnternet kullanımının hızla, kontrolsüz ve bilinçsiz bir şekilde yayılmasıyla birlikte bilişim suçlarının boyutları ülke sınırlarını aşar hale gelmiş ve bilişim suçları ile mücadele edebilmek için ülkelerin birbirleriyle işbirliği yapmaları zorunlu hale gelmiştir. Zira, yanıltıcı IP adresleri vasıtasıyla bir ülkede işlenmiş gibi gözüken bir bilişim suçunun araştırmalar derinleştikçe aslında o ülkede değil başka ülkede ya da ülkelerde yer alan sunucular vasıtasıyla işlenebildiği gözlemlenmektedir.

İşlenen bir bilişim suçunun soruşturması ya da kovuşturma aşamasında bilgisayarlar üzerinde arama yapılması, bilgisayar üzerindeki verilerin birebir kopyalanması ve hatta suç delili olarak bu bilgisayarlara el konulması gerekebilir.

Bilgi sistemlerini bu kadar yoğun kullanan toplumlarda, bilişim suçlarına ve bilişim sistemleri vasıtasıyla işlenen diğer suçlara müdahale, soruşturma ve kovuşturma'nın nasıl yapılması gerektiğine ilişkin daha özel yasal

[1] Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim ABD, umit.bostanci@hotmail.com
[2] Dr., Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim ABD, rbenzer@gazi.edu.tr

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

information systems, investigation and prosecution should be done will ensure more effective results in the fight against these crimes. The main purpose of this study, to expose the legal arrangements about search, copy and seizure on the computers in the Turkish legal system, to express encountered problems in practice and to reccomend some solutions related to these.

Keywords: Cyber Crime, Search, Copy, Seizure.

(Extended English abstract is at the end of this document)

düzenlemelerin yapılması bu suçlarla mücadelede daha etkili sonuçların alınmasını sağlayacaktır.
Çalışmanın temel amacı, Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koymaya ait yasal düzenlemelerin ortaya konulması, uygulamada karşılaşılan aksaklıkların dile getirilerek bunlara ilişkin çözümlerin önerilmesidir.

Anahtar Kelimeler: Siber Suç, Arama, El Koyma, Kopyalama, Adli Bilişim

Giriş

Küreselleşen dünyada teknolojinin her geçen gün akıl almaz bir hızda gelişmesiyle birlikte ortaya çıkan cep telefonu ve bilgisayar gibi ürünler insan hayatını eskiye göre daha rahat ve daha kolay bir hale getirmektedir. Yirminci yüzyılın ortalarında icat edilen bilgisayar her geçen gün hayatımızı daha kolay hale getiren ürünlerin başında gelmektedir. Yerel Alan ağlarının kullanılmaya başlanması bilgisayarların birbirleriyle iletişim kurmalarını sağlamış. İnternetin keşfedilmesi ve hızla yaygınlaşmasıyla birlikte bilgisayarların birbirleri arasındaki iletişim ülke sınırlarına sığmaz bir duruma gelmiştir.

İnsan hayatını bu denli kolaylaştıran, bir çok işin onsuz yapılamaz hale geldiği ve insan hayatında çok önemli bir yere sahip olan bilgisayarlar ve bilgisayar teknolojisine sahip birçok aygıt ile bilinçli ya da bilinçsiz olarak suç işlemek mümkün hale gelmiştir. İnsanoğlu kendisine bu kadar kolaylık sağlayan cihazı bir şekilde bilişimle ilgili ya da ilgisiz olarak işlenen suçlara karıştırmayı başarmıştır. Günümüzde bilgisayar, insan hayatını kolaylaştıran bir devrim olma vasfını yitirerek suç kavramı ile birlikte hatırlanan bir cihaz haline de gelmiştir (Dokurer, 2001).Bilişim cihazları kullanılarak işlenen suçlar vasıtasıyla bilişim suçu kavramı ortaya çıkmıştır. Bilgisayar teknolojisini kullanan ülkeler için bilişim suçları ortak bir sorun haline gelmiştir. İnternet sayesinde bilgi paylaşımı ve bilgiye erişimin küresel boyutlara ulaşmasıyla birlikte bilişim suçlarının işlenişi klasik anlamdaki ülke sınırlarını aşmıştır. Ulusal hukuk düzenlemelerinin bu suçlarla mücadelede yetersiz kaldığı gözlemlenmektedir. Bu nedenle, bilişim suçlarıyla mücadelede uluslararası hukuk ve ülkeler arası işbirliği büyük önem kazanmıştır.

Uluslararası sahnede bilişim suçlarının suç yasalarına aktarılmasındaki problemleri araştırmak için 1983 yılında kapsamlı bir çalışma başlatan ilk kuruluş olan Ekonomik Kalkınma ve İşbirliği Örgütü (OECD) tarafından Bilişim suçu; "bilgileri otomatik işleme tâbi tutan veya verilerin nakline

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış" şeklinde tanımlanmıştır (Ulrich, 1998:19). 1983 yılında, bir grup OECD uzmanının Avrupa bilgisayar suçları yasalarının uyumlaştırılması için üstlendiği girişim neticesinde sorun 1983-1985 yılları arasında çalışılmış ve 1986 yılında "Computer Related Crime: Analysis of Legal Policy" başlığını taşıyan bir rapor hazırlanmıştır (Goodman, 24.03.2015:326).

Bilişim suçları çok çeşitli adlar altında isimlendirilmektedir: "Bilgisayar Suçu", "Bilgisayar Suçluluğu", "Bilgisayarla İlgili Suç", "Bilişim Suçları" , "Siber Suçlar", "İnternet Suçları" (Ergün 2008: 13, Dülger 2004: 65). Amerika Birleşik Devletleri Adalet Bakanlığı da yayımladığı Bilgisayar Suçları Kovuşturması Dokümanında ilgi alanlarında bilgisayar ağını hedef alan ya da kullanan ve "Bilgisayar Yoluyla İşlenen Suç", "Siber Suçlar" ve "Bilgisayar Ağındaki Suçlar" gibi birbirlerinin yerine kullanılan suç tiplerinin olduğunu açıklamıştır. Bilgisayar yoluyla işlenen suçlara bilgisayara sızmak, hizmet dışı bırakma saldırıları, virüsler, bilgisayar kurtçukları örnek olarak verilmiştir (USDOJ, 2015:V).

Bilgisayarlarda Arama, Kopyalama ve El Koyma konusu suçun tespit edilmesi ile başlayıp, çeşitli suçların soruşturma ya da kovuşturması evresinde gündeme gelebilen özel hayatın gizliliği ve mahremiyet kavramlarının da dikkate alınarak zorunlu olmadıktan sonra başvurulmaması gereken hukuki bir tedbirdir.

Türk Hukuk Sisteminde Bilişim Suçları

5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları

Bilişim suçları, 2005 yılında yürürlüğe giren 5237 sayılı Türk Ceza Kanununun "Topluma Karşı Suçlar" başlığını taşıyan üçüncü kısmının "Bilişim Alanında Suçlar" başlığını taşıyan onuncu bölümünde düzenlenmiştir. Bu kapsamda TCK'nun 243, 244 ve 245"inci maddeleri incelenmiştir.

TCK'da bilişim alanındaki suçlar, "hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu" madde 243, "bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu" madde 244/1-2, "bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu" madde 244/4, "banka veya kredi kartlarının kötüye kullanılması suçu" madde 245 şeklinde özetlenebilir.

Bilişim sistemine girme (TCK-Madde 243)

(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veorada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemlerhakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yılakadar hapis cezasına hükmolunur.

5237 sayılı TCK'da düzenlenen bilişim sistemine hukuka aykırı erişimin engellenmesi ile birden farklı hukuki değerler korunmaktadır (Karagülmez, 2009:166). Bunlar arasında örnek olarak, verilerin korunması, özel hayatın gizliliği, kurumsal ve bireysel güvenliğin sağlanması sayılabilir.(Gözüşirin, 2011:44)

Bu maddede yer alan suç tipiyle, Avrupa Siber Suç Sözleşmesinin 2. Maddesinde belirtilen "hukuka aykırı erişim" düzenlemesine uyum sağlandığı (Değirmenci, 2005:207; Yazıcıoğlu, 2004:177) ve özellikle veriler ele geçirilmeksizin verilere yetkisiz erişimin suç tipi haline getirildiği (Dülger, 2004:213) görülmektedir.

Sistemi engelleme, bozma, verileri yok etme veya değiştirme (TCK, Madde 244)

(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.

Banka veya kredi kartlarının kötüye kullanılması (TCK, Madde 245)

(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis cezası ve adlî para cezası ile cezalandırılır.

(2) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan yedi yıla kadar hapis cezası ile cezalandırılır.

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

Tüzel kişiler hakkında güvenlik tedbiri uygulanması (TCK, Madde 246)

(1) Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

Yukarıdakilerin yanı sıra TCK'da bilişim sistemleri aracılığıyla işlenebilecek, ancak bilişim suçu vasfını taşımayan suçlar da yer almaktadır. Bunlara örnek olarak aşağıdaki suçlar verilebilir.

TCK'da Bulunan Bilişim Cihazlarını Kullanmak Suretiyle İşlenebilecek Diğer Suçlar

1. Haberleşmenin Engellenmesi (TCK, Madde 124)
2. Hakaret (TCK, Madde 125. fkr.2.)
3. Haberleşmenin gizliliğini ihlâl (TCK, Madde 132)
4. Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması (TCK, Madde 133)
5. Özel hayatın gizliliğini ihlâl (TCK, Madde 134)
6. Kişisel verilerin kaydedilmesi (TCK, Madde 135)
7. Verileri hukuka aykırı olarak verme veya ele geçirme (TCK, Madde 136)
8. Verileri yok etmeme (TCK, Madde 138)
9. Nitelikli hırsızlık (TCK, Madde 142.fkr.2 b. "e")
10. Nitelikli dolandırıcılık (TCK, Madde 158. fkr.1 b. "f")
11. Müstehcenlik (TCK, Madde 226)
12. Devletin birliğini ve ülke bütünlüğünü bozmak (TCK, Madde 302)
13. Devlete karşı savaşa tahrik (TCK, Madde 304)
14. Hükûmete karşı suç (TCK, Madde 312)
15. Türkiye Cumhuriyeti Hükûmetine karşı silâhlı isyan (TCK, Madde 313)
16. Silâhlı örgüt (TCK, Madde 314)
17. Devletin güvenliğine ilişkin belgeler (TCK, Madde 326)
18. Devletin güvenliğine ilişkin bilgileri temin etme (TCK, Madde 327)
19. Siyasal veya askerî casusluk (TCK, Madde 328)
20. Devletin güvenliğine ve siyasal yararlarına ilişkin bilgileri açıklama (TCK, Madde 329)
21. Gizli kalması gereken bilgileri açıklama (TCK, Madde 330)
22. Uluslararası casusluk (TCK, Madde 331)
23. Devlet sırlarından yararlanma, Devlet hizmetlerinde sadakatsizlik (TCK, Madde 333)
24. Yasaklanan bilgileri temin (TCK, Madde 334)
25. Yasaklanan bilgilerin casusluk maksadıyla temini (TCK, Madde 335)

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

26. Yasaklanan bilgileri açıklama (TCK, Madde 336)
27. Yasaklanan bilgileri siyasal veya askerî casusluk maksadıyla açıklama (TCK, Madde 337)
28. Taksir sonucu casusluk fiillerinin işlenmesi (TCK, Madde 338)
29. Devlet güvenliği ile ilgili belgeleri elinde bulundurma (TCK, Madde 339)

Diğer Kanunlarda Bilişim Suçları

TCK dışındaki diğer kanunlarda geçen bilişim suçları ile ilgili hususlar aşağıda belirtilmiştir:

5846 Sayılı Fikir ve Sanat Eserleri Kanunu (5846, 2008)

1. Manevi, mali veya bağlantılı haklara tecavüz (Madde 71)
2. Koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri (Madde 72)

5070 sayılı Elektronik İmza Kanunu (5070, 2004)

1. İmza oluşturma verilerinin izinsiz kullanımı (Madde 16)
2. Elektronik sertifikalarda sahtekârlık (Madde 17)

5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (5651, 2015)

1. Erişimin engellenmesi kararı ve yerine getirilmesi (Madde 8)
2. Gecikmesinde sakınca bulunan hallerde içeriğin çıkarılması ve/veya erişimin engellenmesi (Madde 8/A)

Türk Hukuk Sisteminde Bilgisayarlarda Arama, Kopyalama ve El Koyma

Bir suçun işlenip işlenmediği ile ilgili olarak; işlenmisse, bunun kim tarafından işlendiği ve yaptırımının ne olması gerektiği sorusuna cevap vermek maksadıyla, kural olarak CMK'ya göre yürütülen iddia, savunma ve yargılama niteliğindeki bir dizi faaliyete ceza muhakemesi, bununla ilgilenen hukuk dalına da Ceza Muhakemesi Hukuku denilmektedir (Öztürk ve Erdem, 2006:57).

Yargıçlar ve Savcılar Birliği Başkan Yardımcısı Bülent Yücetürk verdiği bir röportajda yasaya göre öncelikle bilgisayarlarda ve bilgisayar kütüklerinde arama yapılması gerektiğini, sonrasında elde edilen veriler değerlendirilerek gerekirse el koyma tedbirine başvurulabileceğini belirtmiştir (Bilişim, 2011:101).

Yücetürk'e göre yasada yer verilmemiş olsa dahi genel arama kurallarına göre bilgisayarlar üzerinde arama yapılıp el konulma tedbiri uygulanabilirdi. Fakat, yapılan düzenleme ile işin teknik

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

kısmı dikkate alınarak sayısal delillerin toplanmasında şekilsel kurallar belirlenmiştir. Bu düzenlemeden önce bilgisayarlarda arama ve el koyma konusunda Türk hukuk sisteminde açık bir düzenlemeye yer verilmemesinden ötürü, bu konuyla ilgili tüm işlemler genel hükümlere göre yapılmıştır. Bilgisayarlarda arama ve el koymaya ilişkin hükümler ilk kez 5271 Sayılı CMK ile hukuk sistemimizde yerini almıştır. (Bilişim, 2011:102).

Türk Hukuk Sisteminde Bilgisayarlarda Arama, Kopyalama ve El Koyma tedbiri genel itibariyle 17.12.2004 tarihinde resmi gazetede yayımlanan 5271 Sayılı Ceza Muhakemesi Kanununun 134'üncü maddesinde belirlenmiştir. Bunun dışında, Adli ve Önleme Aramaları Yönetmeliği'nin 17'nci maddesinde de Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma işleminin nasıl yapılacağına dair hükümler bulunmaktadır. 17.12.2004 tarihinden önce yürürlükte olan 1412 Sayılı Ceza Muhakemeleri Usulü Kanununda Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma işleminin nasıl yapılacağına dair bir düzenleme bulunmadığından o dönemde Bilgisayarlar üzerinde yapılan işlemler genel esaslar dikkate alınarak yerine getirilmiştir.

5271 Sayılı Ceza Muhakemesi Kanununun 134'üncü maddesinde belirtilen esaslar çerçevesinde Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma işlemi yapılabilmektedir. Bu esaslar aşağıdaki açıklanmıştır:

(1) Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve (6526, 2014) 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 (CMK, 2004).

(2) 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 elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir (CMK, 2004).

(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır (CMK, 2004).

(4) Üçüncü fıkraya göre alınan(6526, 2014), bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır (CMK, 2004).

(5) Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır (CMK, 2004).

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

Bilgisayarlarda, bilgisayar programları ve kütüklerinde arama tedbirininusul ve esasları maddenin 1 inci fıkrasında, kopyalama işlemine ilişkin düzenlemelere, maddenin 1 ve 5 inci fıkralarında, el koyma tedbiri ile ilgili esaslara maddenin 2, 3 ve 4 üncü fıkralarında yer verilmiştir.

6 Mart 2014 tarihinde resmi gazetede yayımlanarak yürürlüğe giren 6526 sayılı Terörle Mücadele Kanunu ve Ceza Muhakemesi Kanunu İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun ile 2004 tarihinde çıkartılan CMK'da bilgisayarlarda ve bilgisayar kütüklerinde arama ve kopyalamaya dair hükümler daha sıkı şartlara bağlanmış ve kopyalanan bilgilerin bir nüshasının şüpheliye ya da vekiline verilmesi şartı getirilmiştir.

Adli ve Önleme Aramaları Yönetmeliğinin 17'nci maddesi bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma işleminin nasıl yapılacağına dair aşağıdaki düzenlemeleri içermektedir:

- Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması hâlinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir (AÖAY, 2005).
- Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması hâlinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması hâlinde, elkonulan cihazlar gecikme olmaksızın iade edilir (AÖAY, 2005).
- Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır (AÖAY, 2005).
- İstemesi hâlinde, bu yedekten elektronik ortamda bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır (AÖAY, 2005).
- Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan verilerin mahiyeti hakkında tutanak tanzim edilir ve ilgililer tarafından imza altına alınır. Bu tutanağın bir sureti de ilgiliye verilir (AÖAY, 2005).

Suç Eşyası Yönetmeliği'nin 1'inci maddesinde "suç eşyası ve suçla ilgili ekonomik kazancın, muhafaza altına alınması, el konulması, elden çıkarılması, iadesi, müsaderesi ve imhasına ilişkin işlemlerin yapılmasında uygulanacak usul ve esaslar" belirtilmiştir (AÖAY, 2005).

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

Yine aynı yönetmeliğin kıymetli eşya ve evrak ile bozulacak, değerini kaybedecek veya muhafazası zor olan suç eşyası hakkında yapılacak işlemler başlığı altındaki dokuzuncu maddesinde, "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" hükmü bulunmaktadır.

Bu madde ile CMK'nın 134'üncü maddesinde belirtilmeyen bilgisayar, bilgisayar kütükleri ve bu sisteme ilişkin verilerin bulunduğu depolama aygıtlarının nasıl muhafaza edileceği sorusuna açıklık getirilmiştir. Buna göre; el konulan bilgisayar, bilgisayar kütükleri ve bu sisteme ilişkin verilerin bulunduğu depolama aygıtlarının nem, ısı, manyetik alan ve darbelerden korunmalarını sağlayacak ortamlarda muhafaza edilmesi gerekmektedir.

CMK'nın 134'üncü maddesi esas itibariyle Avrupa Konseyi Siber Suç Sözleşmesi'nin 19'uncu maddesinde yer alan "Saklanan Bilgisayar Verilerinin Aranması ve Bunlara El Konulması" başlığı altındaki düzenlemenin iç hukuka uyarlanmış şeklini ifade etmektedir (Bilişim,2011:102). Avrupa Konseyi Siber suç Sözleşmesi 10 Kasım 2010 tarihinde ülkemiz tarafından imzalanmış ve 02 Mayıs 2014 tarihinde TBMM'de kabul ederek aynı gün resmi gazetede yayınlanarak yürürlüğe girmiştir. Bu konuda ortak ilkeler belirleyen ve uluslararası işbirliği yapılmasına imkan veren Siber Suç Sözleşmesi, bu tip suçlarla mücadelede etkin ve hızlı adımlar atılmasını sağlamaktadır (Aktaş, 2014:519).

Hukuki Bir Tedbir Olarak Arama

Arama hukuki niteliği itibarıyla bir koruma tedbiridir. Ceza Muhakemesi yürütülürken bir takım tedbirlere başvurulması gerekmektedir. Koruma tedbirleri denilen bu işlemler, delillere ulaşmayı, muhakemenin sağlıklı bir biçimde yapılıp maddi gerçeğe ulaşmayı ve verilen hükmün kağıt üzerinde kalmasını önlemeyi hedeflemektedir (Aydın, 2009:20).

Adli ve Önleme Aramaları Yönetmeliği'nin 5. Maddesinde Adlî arama,bir suç işlemek veya buna iştirak veyahut yataklık etmek makul şüphesi altında bulunan kimsenin, saklananın, şüphelinin, sanığın veya hükümlünün yakalanması ve suçun iz, eser, emare veya delillerinin elde edilmesi için birkimsenin özel hayatının ve aile hayatının gizliliğinin sınırlandırılarak konutunda, işyerinde, kendisine ait diğer yerlerde, üzerinde, özel kâğıtlarında,eşyasında, aracında 5271 sayılı Ceza Muhakemesi Kanunu ile diğer kanunlaragöre yapılan araştırma işlemidir şeklinde tanımlanmaktadır.

Oldukça kolay değiştirilebilmesi ve kolaylıkla yok edilebilmesi bilişim suçlarının aydınlatılmasını zora sokmaktadır. Hukukumuzdaki aramaya ilişkin mevcut genel hükümlerin bilgisayar ortamına uygulanmasının mümkün olmaması sebebiyle; bilgisayarlarda, bilgisayar programlarında ve

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

kütüklerinde arama, kopyalama ve el koyma'ya ait hükümler ayrıca düzenlenmiştir (Bilişim, 2011:103).

Arama Yapmanın Şartları

Günümüzde insan hayatında vazgeçilmez bir yeri olan bilgisayar sistemlerinin içerisinde bireylerin özel hayatlarına ve ticari hayatlarına ilişkin pek çok bilgi bulunmaktadır. Bu nedenle bu sistemlere müdahale, üzerlerinde arama yapma ve bunlara el koyma basit el koyma işlemine göre daha sıkı koşullara bağlanmıştır (Aydın, 2009:173).

Makul Şüphe Sebebinin Bulunması

5271 sayılı CMK'nın 116/1'inci maddesinde aramanın yapılabilmesi için, arama yapılacak yerde şüphelinin yakalanabileceği veya delil elde edilebileceği yolunda "makul şüphe" bulunması şartı, 6526 sayılı kanun ile "somut delillere dayalı kuvvetli şüphe"(6526, 2014) şeklinde değiştirilmiştir. Ancak mevcut düzenleme uygulamadaki zorluklar gerekçe gösterilerek 6572 sayılı kanunla "makul şüphe"(6572, 2014) şeklinde değiştirilerek, tekrar eski haline getirilmiştir. Aramanın maksadı yakalama ve delil elde etme olduğuna göre böyle bir amaca ulaşılabileceği ile ilgili olarak makul şüphe sebebi bulunmuyor ise arama işleminin yapılmaması gerekmektedir (Aydın, 2009:25). Arama kararlarının gerekçesi olarak gösterilen makul şüphe sebebinin herhangi bir kuşkuya mahal vermemek için arama kararında açık bir şekilde ifade edilmesi gerektiği değerlendirilmektedir.

CMK 116/1'de genel aramalarda makul şüphenin yeterli olacağından bahsedilmesine rağmen, kanunda makul şüpheye ilişkin herhangi bir tanım verilmemiştir. AÖAY'nin 6'ıncı maddesinde, "Makul şüphe, hayatın akışına göre somut olaylar karşısında genellikle duyulan şüphedir. Makul şüphe, aramanın yapılacağı zaman, yer ve ilgili kişinin veya onunla birlikte olanların davranış tutum ve biçimleri, kolluk memurunun taşındığından şüphe ettiği eşyanın niteliği gibi sebepler göz önünde tutularak belirlenir. Makul şüphede, ihbar veya şikâyeti destekleyen emarelerin var olması gerekir. Belirtilen konularda şüphenin somut olgulara dayanması şarttır. Arama sonunda belirli bir şeyin bulunacağını veya belirli bir kişinin yakalanacağını öngörmeyi gerektiren somut olgular mevcut bulunmalıdır." (AÖAY, 2005) şeklinde tanımlanmıştır.

Makul şüphe akla uygun şüphedir. Kanun, arama için kuvvetli veya yeterli şüpheyi değil bunlardan daha az yoğunluğa sahip olan makul şüpheyi arama kararı verilmesi için yeterli saymıştır (Öztürk ve Erdem, 2006:537).

Makul şüphe, ihbar veya şikayeti destekleyen emareler ve şüphenin somut olgulara dayanması ile açıklanabilir. Arama sonunda belirli bir şeyin bulunacağı veya belirli bir kişinin yakalanacağı ile ilgili somut olgular mevcut olmalıdır (Koparan, 2006:7).

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

Genel arama ile ilgili hükümlerde "makul şüphe" sebebi yeterli görülmekte iken, bilgisayarlarda ve bilgisayar kütüklerinde arama yapabilmek için "**somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı**" ibaresi yapılan değişikliklerle CMK'nın 134 üncü maddesinde şart olarak yerini almıştır. Bu nedenle arama kararlarının gerekçesi olarak gösterilen "somut delillere dayalı kuvvetli şüpheyi" oluşturan nedenlerin herhangi bir kuşkuya mahal vermemek için arama kararında açık bir şekilde ifade edilmesi gerektiği değerlendirilmektedir. Bireylerin özel ve iş yaşamlarına dair birçok sırrı barındırabilen bilgisayarlarda arama tedbirinin "somut delillere dayalı kuvvetli şüphe sebeplerinin varlığı" şeklinde daha sıkı şartlara bağlanmış olması insan hakları ve özgürlükler açısından değerlendirildiğinde önemli ve olumlu bir değişiklik olarak görülmektedir.

Hakim Kararının Bulunması

Bireye ait bilgisayar kayıtlarındaki kişisel veriler, temel insan hakları arasında bulunmaktadır (Kızılkaya, 2010:515). Arama işlemi ile kişinin mahremiyeti ihlal edileceğinden bu işlemin hukuk güvenliği açısından hakim kararına bağlanması yerindedir. Bu konuda karar alınmadan önce; arama için somut delillere dayalı kuvvetli şüphe sebeplerinin var olup olmadığı, arama işleminin aramanın yakalama ve el koyma amacına yönelik olup olmadığının değerlendirilmesi gerekmektedir. Şartlar oluşmuş ise arama kararı verilebilir. Anayasaya göre, hakim kararları yazılı olmalı ve bir gerekçeye dayandırılmalıdır (Aydın, 2009:25).

Bilgisayar sistemlerinde yapılacak arama ve el koyma işlemi sadece hakim kararı ile yapılabilmektedir. Cumhuriyet savcısının veya kolluk amirinin bu yönde bir emir verme yetkisi yoktur (Aydın, 2009:175). Gecikmesinde sakınca olan hallerde dahi savcının karar verme yetkisi bulunmamaktadır (Bilişim, 2011:104).

CMK'nın 119'uncu maddesinde arama kararında yazılması gereken hususlar ile ilgili olarak; aramanın nedenini oluşturan fiil, aranılacak kişi, aramanın yapılacağı konut veya diğer yerin adresi ya da eşya, karar veya emrin geçerli olacağı zaman süresi'nin açıkça gösterilmesi gerektiği belirtilmiştir (CMK, 2004).

Her ne kadar CMK madde 134'te düzenlenen koruma tedbirine kovuşturma safhasında başvurulabileceğine ilişkin maddede açık bir hüküm bulunmasa da, koşulların oluşması durumunda, kovuşturma aşamasında mahkemenin talebi üzerine yahut re'sen bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama ve kopyalama kararı verebileceği değerlendirilmiştir. Nitekim, Yargıtay 1. Ceza Dairesi,14.11.2005 tarih ve 3891/3230 sayılı kararında; "olay tarihinde sanıkla maktulün internet üzerinde sohbet ettikleri söylenen kafede sanığın Kaan kodadıyla 21 nolu masada ve maktulün kullandığı belirtilen bilgisayarların ve kullandıkları programın saptanarak bilgisayarlarda ve bilgisayar programının merkezi sisteminde sohbet kaydının mevcut olup olmadığı ve içeriğinde

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

hakaret ve tahrik içeren sözler olup olmadığı tespit edilmeden ..” hüküm kurulmasını bozma sebebi saymıştır (Yaşar / Dursun, 2013).

Başka Suretle Delil Elde Etme İmkanı Bulunmaması

CMK’nın 134/1 maddesinde başka suretle delil elde etme imkanı bulunmaması durumu açık bir şekilde ifade edilmiştir.

Bunun yanı sıra, bilgisayar, bilgisayar programları ve kütükleri üzerinde yapılacak arama ve el koyma işlemleri, genel arama ve el koyma hükümlerinden ayrı olarak düzenlenmiş, bireyin mahremiyetine ve kişisel verilerine yönelik olumsuz etkiler dikkate alınarak, “son çare” olarak başvurulabilecek “özel koşullara bağlı” bir koruma tedbiri olması öngörülmüştür(Özbek / Tepe / Doğan v.d., 2013:362).

Bu tedbir en son çare olarak görülmelidir. Şayet bu koruma tedbirine başvurmaksızın delil elde etme imkanı var ise, maddenin uygulanma şansı yoktur. Temel hak ve özgürlüklere müdahale açısından bu durum önemlidir. Ölçülülük ilkesi gereği de öncelikle kişi bakımından daha az müdahaleyi öngören tedbirlerin uygulanması gerekmektedir. Ancak, suç delillerinin elde edilmesi adına öncelikle bu tedbirin uygulanması gerekiyorsa, buna da bir mani yoktur (Aktaş, 2014:526).

Aramanın Yapılacağı Zaman

Bilgisayar ve bilişim ile ilgili cihazların ev ve işyerlerinde yoğun olarak kullanıldığını düşündüğümüzde, aramalarla ilgili olarak CMK’da yer verilen aramanın yapılması gereken zaman diliminden de söz etmekte yarar görülmektedir.

CMK madde 118’de "konutta, işyerinde veya diğer kapalı yerlerde gece vaktinde arama yapılamaz. Suçüstü veya gecikmesinde sakınca bulunan hâller ile yakalanmış veya gözaltına alınmış olup da firar eden kişi veya tutuklu veya hükümlünün tekrar yakalanması amacıyla yapılan aramalarda, birinci fıkra hükmü uygulanmaz" hükmü bulunmaktadır (CMK, 2004). Gece vakti, TCK’nın 6’ncı maddesinde; güneşin batmasından bir saat sonra başlayan ve doğmasından bir saat evvele kadar devam eden zaman süresi olarak belirlenmiştir. Gece vaktinin tespit edilebilmesi için güneşin doğuş ve batış saatlerinin bilinmesi gerekmektedir. Güneşin doğuş ve batış saatleri www.adalet.gov.tr internet adresinden veya bulunulan yerin enlem ve boylam bilgilerinin girilmesiyle güneşin doğuş ve batış saatlerini veren internet sitelerinden tespit edilebilir.

Yukarıda bahsedilenler ışığında konut, işyeri ve diğer kapalı yerlerde aramaların gündüz vakti yapılması gerekmektedir. Bunun nedeni, bireylerin gece vakti konut ve işyerinde veya diğer kapalı mekanlarda rahatsız edilmek istenmemesidir. Bireyler özellikle gece vakti ve özellikle de evlerinde huzur ve güven ortamında bulunmak isterler. Kişiler özel hayatlarının en mahrem ve özel anlarını

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

çoğu kez geceleri yaşamaktadırlar ve bir insan için hayati bir ihtiyaç olan dinlenme ve uyku ihtiyaçlarını genellikle gece gidermektedirler. İşte bu nedenledir ki kanun koyucu aramanın gece vakti yapılması söz konusu olduğunda kural olarak kişi hak ve özgürlüklerini suçun soruşturulması amacına tercih etmiş ve kural olarak gece vakti aramaya izin vermemiştir. Ancak, çok özel ve istisnai durumlar söz konusu olduğunda gece vakti arama yapılabileceği kabul edilmştir (Aydın, 2009:49).

Aramada Hazır Bulunacak Kişiler

Bilgisayar, bilgisayar programları ve kütükleri üzerinde yapılacak arama ve el koyma işlemlerinde hazır bulunacak kişilerle ilgili olarak CMK'da herhangi bir hüküm bulunmamaktadır. Ancak, söz konusu bilişim cihazlarının genellikle kişinin konut ya da evinde bulunması dolayısıyla yapılacak olan aramalarda CMK madde 120'de belirtilen genel hükümlere uyulması gerektiği açıkça görülmektedir.

CMK'nın 120'nci maddesinde aramada hazır bulunabileceklerle ilgili olarak; aranacak yerlerin sahibi veya eşyanın zilyedi aramada hazır bulunabilir; kendisi bulunmazsa temsilcisi veya ayırt etme gücüne sahip hısımlarından biri veya kendisiyle birlikte oturmakta olan bir kişi veya komşusu hazır bulundurulur.117'nci Maddenin birinci fıkrasında gösterilen hâllerde zilyet ve bulunmazsa yerine çağrılacak kişiye, aramaya başlamadan önce aramanın amacı hakkında bilgi verilir. Kişinin avukatının aramada hazır bulunmasına engel olunamaz hükmü bulunmaktadır. Ayrıca CMK'nın 119'uncu maddesinde Cumhuriyet Savcısı hazır olmaksızın konut, işyeri veya diğer kapalı yerlerde arama yapabilmek için o yer ihtiyar heyetinden veya komşulardan iki kişi bulundurulması gerektiği ve bu kişilere de arama tanığı denildiği yer almaktadır. Askerî mahallerde yapılacak aramaya ilişkin olarak da Cumhuriyet Savcısının istem ve katılımının bulunması gerektiği ve aramanın askerî makamlar tarafından yerine getirilmesi gerektiği belirtilmiştir.

Arama işlemi yapılırken kanun koruyucu "arama tanığı" bulundurulmasını zaruri kılmıştır. Bunun sebebi sonradan ortaya atılabilecek iddiaların, yani aramanın yapıldığı mahalde olmayan delillerin aramayı yapan kişilerce konulduğu gibi suçlamaların önünü kesmek ve aramanın her türlü şüpheden yoksun bir şekilde yerine getirilmesini sağlamaktır. Kanunda arama tanığının bulundurulması zaruri olarak istense de Yargıtay bazı durumlarda arama tanığı bulundurulmadan aramanın gerçekleştirilmesini şekli hukuka aykırılık olarak kabul etmiş ve yapılan aramanın kanuna aykırı olmasına rağmen (CMK 206/1) "hukuka uygun" (CMK 217/2) kabul etmiştir (Yenisey, 2015).

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

Arama İşleminin Uygulanması

Bilgisayar ve Bilgisayar Programları ile kütüklerinde aramanın nasıl yapılacağına dair CMK'da bir hüküm bulunmamaktadır. Maalesef bu konuda uygulamanın nasıl yapılması gerektiğine ilişkin AÖAY'nde herhangi bir hüküm bulunmamaktadır. Bu durumda arama ile ilgili hususlarla ilgili kolluk personelinin becerisi ve olayı ele alış tarzı önemli rol oynamaktadır.

Asıl olan bilgisayarlara el konulmadan sistemde arama yapıp sadece gereken verilere el konulmasıdır (Sırma, 2008:651). Uygulamada kolluk kuvvetleri, genellikle suça konu olabilecek yerde arama yaparken suç ile ilişkili olabilecek her türlü cihaza el koyarak bu işlemi yerine getirmektedir. Bunun sebebi olarak adli bilişim incelemelerinin uzun ve zaman alıcı bir süreç olması gösterilmektedir. Ortalama bir sabit diskin bire bir bit seviyesinde kopyalanması bile yaklaşık 4-5 saatlik zaman dilimine denk gelmektedir ki arama işlemi bundan daha uzun bir sürede gerçekleştirilebilir. Bu durumda uzun süre kolluk kuvvetlerinin bilgisayarın genellikle bulunduğu ortam olan ev ya da iş yerinde misafir edilmesi gerekmektedir.

Ayrıca el konulan delillerin nasıl taşınması, nakledilmesi ve incelenmesi gerektiği ile ilgili olarak da CMK'da ve ilgili yönetmeliklerde herhangi bir husus yer almamaktadır. Ayrıca, konunun uygulanmasına yönelik olarak kolluk kuvvetlerinin hazırladığı herhangi bir kılavuza da rastlanmamıştır.

Aramanın nasıl gerçekleştirilmesi gerektiği hususunda CMK'da açık bir hüküm bulunmamaktadır. Uygulamada kolluk kuvveti arama esnasında el koydukları bilgisayar, bilgisayar programları ve kütüklerini karton kutuların içine koymak suretiyle el konan eşyaları kendi görev yerlerine götürüp üzerinde inceleme yapmakta bu şekilde tartışmalı bir delil elde etmektedirler. Şüpheliye tanınan güvenceler ışığında, adli makamlar ceza yargılaması işlem ve tedbirlerine başvururken o tedbir ve işlemler ile öngörülen hukuk kurallarına uymak ve belirtilen kurallar çerçevesinde delil toplama işlemini yerine getirmekle yükümlüdürler. Bu kurallara aykırı davranmak suretiyle elde edilen her delil hukuka aykırı delil olarak nitelendirilebilir (Bilişim,2011: 104).

Tüm bu işlemler yapılırken, içeriğinde birçok ilgisiz kişisel verinin de yer alabileceği verilere el konulması ile T.C. Anayasası ile güvence altına alınmış olunan kişinin temel hak ve özgürlüklerinin ihlal edilebileceği unutulmamalıdır.

Ülkemizde adli bilişim işlemlerinin bütünüyle adli kolluk tarafından yerine getirilmesi, olay mahalline giden kolluk görevlilerinin adli bilişim konusunda uzman olmalarını gerekli kılmaktadır. Olay mahalli bütünüyle fotoğraflanmalı, tüm materyallerin yeri belirlenip çizilecek kroki üzerinde gösterilmelidir. Sayısal deliller birebir kopyası alınmak suretiyle yedeklenmeli, bir örneği talep üzerine şüpheliye veya vekiline verilmelidir. Bilgisayarın ya da delil barındıran dijital cihazların yedekleme işlemi asla kolluk biriminin görev yaptığı yere getirilerek yapılmamalıdır. Bilgisayar ve

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

donanımlarına kanunun belirttiği hüküm uyarınca dosyaların şifreli olması, açılamaması gibi durumlar hariç el konulmamalıdır. Zaruri nedenlerle el konulan aygıtlar ise derhal iade edilmelidir. Kanun koyucunun kesin olarak belirlemediği, bizatihi suç teşkil eden materyaller ise şüpheliye teslim edilmeyerek bunlara el konulması gerekmektedir (Bilişim,2011: 104).

Arama Tutanağının Düzenlenmesi

Arama sonunda tutanağın düzenlenmesine ilişkin olarak hem CMK'nın 119/3, 121/1,121/2,121/3'üncü maddelerinde hem de Adli ve Önleme Aramaları Yönetmeliğinin 11'inci maddesinde düzenlemeler yasal bulunmaktadır.

Aydın tarafından bu durum, "Yapılan adli arama sonucunda bir tutanak düzenlenir ve tutanak aramaya katılanlar tarafından imzalanır. İmza atmak istemeyenler olur ise bu durum tutanağa yazılır. Arama tutanağı aramanın baştan sona anlatılması ile düzenlenir. Böylece arama işlemi sırasında orada olmayan soruşturma ve kovuşturma makamları aramanın nasıl yapıldığı konusunda bilgi sahibi olurlar. Aramaya karşı yapılacak itirazlar bu tutanaktaki bilgilere göre çözümlenir." şeklinde ifade edilmiştir (Aydın, 2009:88).

Adli ve Önleme Aramaları Yönetmeliğinin 11'inci maddesinde arama sonunda düzenlenecek tutanağın neleri içermesi gerektiği düzenlenmiştir. Buna göre tutanakta; arama kararının tarih ve sayısı, hâkim kararı yoksa verilmiş olan yazılı emrin tarih ve sayısı ile emri veren merci, aramanın yapıldığı yer, tarih ve saat, aramanın konusu, aranan kişinin kimlik bilgileri, adını söylemediği takdirde eşkâl bilgileri, araçta, konutta, işyeri ve eklentilerinde arama yapılmışsa, aracın plaka numarası, markası, konutun, işyerinin ve eklentilerinin açık adresi, su üstü aracının aranmasında su üstü aracının cinsi, ismi, sahibi ve kullananı, deniz aracının aranması hâlinde ise deniz aracının cinsi, ismi, donatanı, bağlama limanı, tonajı, acentesi, kaptanı ve arama mevkiî, aramanın sonuçları, el konulan suç eşyasına ilişkin belirleyici bilgiler, aramada yakalanan kişiler varsa kimlik bilgileri, kimliği belirlenemiyorsa eşkâl bilgileri, arama sonucunda yaralanma veya maddî bir zarar meydana gelip gelmediği, arama işlemini yapanların adı, soyadı, sicili ve unvanı, hususları yer alır. Tutanak arama işlemine katılmış olanlar ve hazır bulunanlarca imzalanır. Tutanağın bir sureti ilgiliye verilmesi gerektiği hüküm altına alınmıştır.

Tutanak aramaya maruz kalan kişinin yokluğunda düzenlendi ise onun yerine aramada hazır olan kişiye, o da arama esnasında bulunmadı ise arama tanıklarından birisine verilip bu durumun da tutanağa yansıtılması gerekmektedir (Aydın, 2009:88).

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

Arama Sonunda Talep Halinde Verilecek Belge

Adli ve Önleme Aramaları Yönetmeliğinin 12'nci maddesinde arama sonunda talep halinde verilecek belgenin neleri içermesi gerektiği düzenlenmiştir. Buna göre arama sonunda istendiğinde; aramanın, şüpheli veya sanık olması ve yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe bulunması sebebiyle mi, şüphelinin veya sanığın yakalanabilmesi veya suç delillerinin elde edilebilmesi amacıyla mı, gerçekleştirildiğini, yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe bulunan şüphelinin veya sanığın üstünün, eşyasının, konutunun, işyerinin veya ona ait diğer yerlerin aranması durumunda, soruşturma veya kovuşturma konusu fiilin vasfını, aramada el konulan veya koruma altına alınan eşyanın listesini, aramada şüpheyi haklı kılan bir şey elde edilmemiş ise bu durumu, hakkında arama işlemi uygulanan kimsenin, el konulan eşyanın mülkiyetine ilişkin görüş ve iddialarını, içeren belge veya belgeler verilir. Koruma altına alınan veya el konulan eşyanın tam bir listesi yapılarak resmî mühürle mühürlenir. Bu eşyanın resmî mühürle mühürlendiğine dair tutanak düzenlenerek, bir sureti ilgilisine verilir hükmü bulunmaktadır (AÖAY, 2005).

Hukuka Aykırı Arama

Hukuka aykırı olarak yerine getirilen bir aramanın ceza ve tazminat sorumluluğu bulunmaktadır. Bunların yanı sıra; hukuka aykırı bir şekilde icra edilen arama sonucu elde edilen bulguların delil değerini yitirmesi, hukuka aykırı olarak yapılan arama işleminin en önemli sonucudur(Aydın, 2009:138).

5271 sayılı CMK'nın 206'ıncı maddesinde delil kanuna aykırı olarak elde edilmiş ise "bu delil reddolunur ve hükme esas alınmaz" denilmektedir. Bunun yanı sıra, CMK'nın 217'nci maddesinde yüklenen suçun, hukuka uygun bir şekilde elde edilmiş her türlü delille ispat edilebileceği belirtilmiştir. Bu nedenle, bilgisayarlarda ve bilgisayar kütüklerinde arama faaliyetini yürüten kolluk kuvvetlerinin ve bilirkişilerin arama esnasında kanuna aykırı en ufak bir davranışta dahi bulunmamaları gerekmektedir. Adı geçen görevlilerin hukuka aykırı davranışları, aslında delil olabilecek bir bulgunun hukuka aykırı elde edilmesinden dolayı mahkeme tarafından delil niteliğinde sayılmamasına sebep olabilmektedir.

Hukuki Bir Tedbir Olarak El Koyma

Öztürk ve Erdem'e göre el koymanın; ispata yarayan bir araç oluğu dikkate alındığında ceza muhakemesinde maddi gerçeğe ulaşma açısından faydalı görülen veya müsadereye tabi bulunan eşyanın, eşyayı elinde bulunduran kimse istekli olmasa dahi, adliyenin koruması altına alınmasıdır (Öztürk / Erdem, 2006:551).

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

AÖAY'nin 4'üncü maddesinde el koyma, suçun veya tehlikelerin önlenmesi amacıyla veya suçun delili olabileceği veya müsadereye tâbi olduğu için, bir eşya üzerinde, rızası olmamasına rağmen, zilyedin tasarruf yetkisinin kaldırılması işlemi olarak tanımlanmıştır.

El koyma işlemi ile müsadere işlemi arasında bazı farklılıklar bulunmaktadır. Zira, el koyma işlemi yukarıda da açıklandığı gibi koruma tedbiri niteliğindedir. Ancak, müsadere TCK'nın 54 ve 55'inci maddelerinde belirtilen yaptırım niteliğinde bir tedbirdir. El koyma kararı tedbir niteliğinde olduğu için geçicidir, müsadere kararı ise hüküm niteliği taşımaktadır. El koyma işlemi ile, eşyanın maliki mülkiyet hakkını kaybetmez iken müsadere kararı ile eşyanın mülkiyeti devlete geçmektedir (Aydın, 2009:145).

El Koymanın Şartları

Bilgisayarda arama ve el koyma işleminin yapılabilmesi için başka surette delil elde etme imkânının bulunmaması gerekmektedir. Esas olan bilgisayarlara el konulmadan sistemde arama yapıp sadece gerekli verilere el koymaktır. CMK'nın 134/2 maddesine göre bilgisayarlara el koyma ancak, bilgisayar programlarına ve kütüklere şifre nedeniyle girilememesi ya da gizlenmiş bilgilere ulaşılamaması halinde mümkün olabilir. Gerekli verilere ulaşıldıktan sonra ve gerekli kopyalar alındıktan sonra bilgisayarın gecikmeden iade edilmesi gerekmektedir. (Sırma, 2008:651).

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

Bilgisayarlara ve bilgisayar programlarına el konulabilmesi için, öncelikle bu araçlar üzerinde hukuka uygun olarak verilmiş bir arama ve kopyalama kararı bulunmalıdır. CMK 134 üncü madde kapsamında el konulacak araç ve gereçler üzerinde, daha önceden verilen bir arama ve kopyalama kararı mevcut bulunmalıdır. Zira, bilgisayarlar, bilgisayar programları ve bilgisayar kütüklerine el konulabilmesi için CMKm.134/2'de öngörülen "bu araçlara şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamamış olması" koşulunun oluşabilmesi, her şeyden önce bu araçlar üzerinde arama ve kopyalama yapılmasını tesis edecek bir hakim kararını gerektirmektedir.(Yaşar / Dursun, 2013:14)

Bilgisayarlar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması

CMK 134/2'de, Bilgisayarlara ve bilgisayar programlarına ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir denilmektedir.

Soruşturma ya da kovuşturma aşamasında somut delillere dayalı kuvvetli şüphenin ortaya çıkması ile birlikte verilen arama ve kopyalama kararı neticesinde, bilgisayarlar, bilgisayar programları ve kütükleri üzerinde gerçekleştirilen aramada, tedbiri bizzat gerçekleştiren adli kolluğun uzman birimleri ya da bu hususta görevlendirilen uzman bilirkişi, soruşturma konusu suçla bağlantılı olarak, aramaya konu olan veriyi bulamamışsa, verilerin kopyalanmasının uygun olmadığı değerlendirilmektedir. Bu durumda, arama neticesinde suçla ilgili bir veri bulunamadığından, hâkim tarafından verilen kopyalama kararı da konusuz kalmaktadır (Yaşar/ Dursun, 2013:14).

El koymaya konu olacak bilgisayar sisteminin kime ait olduğunun önemi yoktur. Söz konusu sistem şüpheliye ait olabileceği gibi olayla ilgili olmayan üçüncü kişilere de ait olabilir. Önemli olan el koyma işleminin delil elde etme amacına hizmet etmesidir (Aydın, 2009:145).

Şifre çözüldükten ve gerekli kopyalar alındıktan sonra el konulan cihazların gecikme olmaksızın iade edilmesi gerekmektedir. CMK'da, bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır şeklinde hüküm bulunmaktadır. CMK m. 134'ün gerekçesinde bu tedbire iki yıl veya daha fazla hürriyeti bağlayıcı cezayı gerektiren durumlarda başvurabileceği belirtilmiştir. (Kızılkaya, 2010:528)

Hakim Kararının Bulunması

Bilişim teknolojisinin hızlı bir şekilde gelişmesiyle oluşan koşullarda bilgisayarlar ve bilgisayar programları hayatın önemli ve ayrılmaz bir parçası haline gelmiştir. Pek çok birey gibi suç işleyen kişilerde bilgisayar sistemlerini kullanmakta ve işledikleri suçlarla ilgili olarak bazı emareler bırakmaktadırlar. CMK, delilden sanığa gitmeyi hedeflemekte ve teknik delillere önem vermektedir. Bu nedenle, CMK'da bilgisayar sistemlerinde bulunması muhtemel delillerin elde edilmesine ilişkin bazı hükümler yer almaktadır (Aydın, 2009:173).

CMK'nın 134'üncü maddesi 2'nci fıkrasında şifrenin çözülememesinden veya gizlenmiş bilgilere ulaşılamaması halinde gerekli kopyaların alınabilmesi için, bilgisayarlara elkonulabileceği, gerekli kopyaların alınmasından sonra elkonulan cihazların gecikme olmaksızın iade edilmesi gerektiği hususu hükme bağlanmıştır. Bu bağlamda, el koymanın amacının bilgisayarda bulunan dijital verilerin kopyasının alınması olduğu düşünüldüğünde, CMK'nın 134'üncü maddesinde belirtilen arama kararında olduğu gibi el koyma tedbirinin de hakim kararı güvencesinde olduğu değerlendirilebilir. Bütün bunların ışığında, hakim dışında hiçbir yetkili mercii ya da makamın

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

bilgisayarlara ya da bilgisayar programlarına veya kütüklerine el konulmasına karar veremeyeceği düşünülmektedir.

El Koyma İşleminin Uygulanması

El koyma işleminin yapılabilmesi için yukarıda bahsedilen şartların oluşması gerekmektedir. İmkan var ise el koyma işlemi yapmaksızın şüpheli ya da vekili huzurunda bilgisayarın bulunduğu yerde adli bilişim ilkelerine uygun bir şekilde bilgisayarın ya da bilgisayar medyalarının silinmiş veriler dahil bire bir kopyalarının alınması kafalardaki şüphelerin giderilmesi bakımından şüpheli açısından daha ikna edici olduğu değerlendirilmektedir. Zira el koymanın birinci öncelikli amacı adli bilişim ilkelerine uygun bir şekilde bilgisayar medyasındaki verilerin birebir kopyasını almaktır. Adli bilişim ilkelerine göre kopya alındıktan sonra bu işleme ilişkin tutanak hazırlanmalı ve ilgili medya vakit geçirmeksizin şüpheliye iade edilmelidir. Bu husus CMK'da "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" şeklinde hükme bağlanmıştır. Ancak, bilgisayar sistemleri üzerinde kopyalama işlemi farklı şekillerde (copy komutu, yüzeysel imaj alma programları, bit seviyesinde imaj alma programları vb.) yapılabilmektedir. Yasada bu kopyalama metodlarından hangisinin kullanılması gerektiği konusunda bir açıklık bulunmamaktadır. Dolayısı ile adli bilişim metodlarına aykırı bir şekilde kopyası alınmış bilgisayar medyaları üzerinde yapılacak inceleme delil elde etme açısından istenilen verileri tam olarak içermeyebilir.

Özbek tarafından, şifrenin çözülememesi veya gizlenmiş verilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi yetkisinin bağımsız bilirkişilere verilmesi önerilmektedir. Türkiye'de uzman bilirkişilerin bulunmaması nedeniyle deşifre işlemlerinin kolluk kuvveti tarafından yerine getirildiği belirtilmiştir. Ancak, kolluğun soruşturmada taraf olması nedeniyle bu işin kolluk görevi olmaktan çıkarılması gerektiği, kopyalama ve kopyalanan verilerin çıktısının alınması safhasında kolluğun görev yapmasının elde edilen verileri hukuka aykırı hale getirebileceği, bu işlemler için mutlak surette bağımsız adli bilişim uzmanlarının görevlendirilmesi gerektiği önerilmiştir (Bilişim,2011:110).

Yine Özbek tarafından, asıl olanın kopya çıkarılmak olmasına rağmen, zaman zaman bilgisayar, bilgisayar programları ve kütüklerine el konulması karşılaşılan en büyük problem olarak belirtilmiştir. El koyma tedbirine, şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere erişim sağlanamaması durumunda çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi maksadıyla başvurulması gerektiği açıklanmıştır. Zira el koyma tedbirinin uygulanması sonucunda,

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

bilgisayara dayalı faaliyeti olan kişi ya da kurumlar faaliyetlerini sürdürememektedirler (Bilişim, 2011: 111).

Diğer tüm muhakeme işlemlerinde olduğu gibi (CMK 169/2) bu işlemlerin sonucunda da yapılan işlemler, bu işlemlerin kim tarafından nasıl gerçekleştiği, ne zaman ve nerede yapıldığı bir tutanağa bağlanır ve işleme katılanlar tarafından imzalanır. İmza etmek istemeyen bulunur ise bu husus tutanağa yazılarak görevliler tarafından imza altına alınır (Aydın,2009:191).

CMK'nın 134'üncü maddesinde "Bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. İstemesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır" hükmü bulunmaktadır. Bu hüküm karşısında yedek çıkarılması için şüphelinin veya vekilinin istemde bulunmasına gereksinim yoktur. Yedekleme işlemi bilgisayar medyasındaki verilerin (silinmiş veriler dahil) bire bir kopyasının başka bir aygıt üzerine alınması şeklinde gerçekleştirilmektedir. Bu kopyalama işleminden sonra alınan kopyanın ve kopyası alınan orjinal bilgisayar medyasına ait hash değerlerinin de şüpheliye ve vekiline verilmesi kopyaların bire bir alındığını gösteren en önemli kanıt unsurudur. Hash değerleri karşılaştırılarak kopyanın üzerinde herhangi bir değişiklik yapılıp yapılmadığı anlaşılabilmektedir. Herhangi bir şüpheye mahal vermemek için kopyalama işleminin ardından hash değerleri çıkartılarak ilgililere verilmeli ve istenildiğinde gösterilecek şekilde muhafaza edilmelidir.

Verilerin yedeği her durumda alınmalıdır. Tutanağa, alınan yedekten bir kopya çıkarılmasının istenmediğine dair herhangi bir ibare yazılmadığı durumlarda, şüpheli veya vekili kendilerine yedekten kopya verilmesini istedikleri halde verilmediğini ve el konulan verilerin değiştirildiğini iddia edebilirler. Bu durumda, elde edilen verilerin yasaya aykırı olarak elde edilmiş delil haline gelmesi söz konusu olabilmektedir. Bu sebepten ötürü, bu nitelikteki deliller hükme esas alınmaz (Aydın, 2009:191).

Bu konuyla ilgili olarak T.C. Anayasası 38/6'ncı maddesinde "kanuna aykırı olarak elde edilmiş bulgular delil olarak kabul edilemez" hükmüne yer verilmiştir. Ayrıca, CMK'nın 206'ncı maddesinde konuya ilişkin olarak "delil kanuna aykırı olarak elde edilmiş ise reddolunur ve hükme esas alınmaz" denilmektedir. Bunun yanı sıra, CMK'nın 217'nci maddesinde "Yüklenen suç, hukuka uygun bir şekilde elde edilmiş her türlü delille ispat edilebilir" hükmüne yer verilmiştir. Tüm bu hükümler ışığında, icra edilen el koyma işlemi esnasında kanuna ve hukuka aykırı hareket edilmesi ile elde edilen deliller geçersiz hale gelerek delil niteliğini kaybederler.

Bu noktada şunu da ifade etmekte yarar görülmüştür. Hukuka aykırı olarak yapılan el koyma işlemi aynı zamanda bir haksız fiil olduğu için bu şekilde bir işleme maruz kalan kişinin bu nedenle

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

tazminat talep etme hakkı bulunmaktadır (Aydın, 2009:200). Bu konuda T.C. Anayasası 125'inci madde ve CMK'nın 141'inci maddesinde hükümler bulunmaktadır.

Teknik Olarak Bire Bir Adli Kopyanın Oluşturulması (İmaj Alma)

Bire bir adli kopyalama aşamasına geçilmeden önce şuça konu olan bilgisayarın bulunduğu yere gidildikten sonra adli bilişim esaslarına uygun olarak olay yeri müdahalesi safhasındaki adımların takip edilmesi delil bütünlüğüne zarar gelmemesi açısından hayati derecede önem arz etmektedir.Olaya müdahale esnasında bilinçli ya da bilinçsizce yapılabilecek bir hamle delil bütünlüğüne zarar verebilir ve hatta tüm delillerin yok edilmesine neden olabilmektedir.

Delil tespit etme, delil toplama-muhafaza etme, delil çıkartma, delil inceleme ve delil organize etme/raporlama işlemleri adli bilişimin safhaları olarak belirlenmiştir (TBD Kamu, 2007:99).

Fiziksel ve dijital bozulabilir deliller koruma altına alınmalıdır; ilk müdahale grubu olay yerinde bozulabilir verilerin varlığını her zaman düşünmeli bunların derhal çevre güvenliğini sağlamalı, dokümante etmeli ve fotoğraflamalıdır (TBD Kamu, 2007: 100).

Ekizer'e göre, adli bilişimde normal kriminalistik biliminde olduğu gibi ilk olay yeri müdahalesi oldukça önemlidir. Muhtemel suç delillerinin güvenilir bir şekilde eksiksiz olarak tespit edilmesi ve zarar görmeden elde edilmesi olaya ilk müdahalenin uygun şekilde yapılması ile mümkün olabilmektedir. Bunun için öncelikle olay yeri güvenliğinin alınmasının ardından, adli bilişim uzmanları dışında herhangi bir kişinin delil olması muhtemel bilişim sistemleri ve çevre birimlerinin yer aldığı ortama girmesi engellenmelidir. İlk olay yerinde yetkisiz üçüncü şahısların bulunması bilişim sistemlerinin ve çevre birimlerinin içermesi muhtemel suç delillerinin kasıtlı veya kasıt dışı olarak bozulmasına ve delil niteliğini kaybetmesine neden olabilir. Bunun yanı sıra olay yerindeki sahnenin ilk durumu bile bazı durumlarda suç araştırmacısına muhtemel suça ilişkin bilgiler sağlayabilmektedir. Bilişim sistemlerinin fiziki konumu, cihazların birbirleri ile bağlantıları, ağ cihazlarının bağlantı pozisyonları, bilişim sistemlerinin etrafında bulunabilecek dokümanlar ve notlar suç araştırmacısına azda olsa suç ile ilgili bilgi verebilecektir. Şu ana kadar ilk olay yeri sahnesi karşılaşma anı ile ilgili olarak geleneksel kriminalistik biliminin olay müdahalesinin ilk aşaması ile aynı süreçler izlenmektedir. Bu her ne kadar bilgisayar kriminalistiğinde ki teknik bilgi ve beceriyi ortaya koymasa da çoğu durumda olası suç delillerinin zarar görmeden elde edilmesi ve suça ilişkin bazı fikirler vermesi açısından önem arz etmektedir (Ekizer, 2014).

Olay yeri araştırılırken adli bilişime katkı sağlayabilecek yardımcı delillerin de dikkate alınması olayın aydınlatılması açısından faydalı olacaktır. Bu yardımcı deliller genellikle bilgisayar masalarında bulunmaktadır. Elektronik delillerin incelenmesi esnasında katkı sağlayabilecek bu bilgiler genellikle kağıtlara not alınmış bilgisayar kullanıcı adı ve şifreleri, e-posta adresleri ve şifreleri, sonradan şifre

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

kırmada kullanılabilecek notlar ve donanım/yazılım kılavuzları olarak belirlenmiştir (Kiçeci, 2014:166).

Herhangi bir delil elde etmek amacıyla suça konu bilgisayar kullanılmamalıdır. Herhangi bir delilin yeri değiştirilmeden önce olay yeri, bilgisayarın önünne ve arkasına kablolarla bağlanmış cihazlar mutlaka fotoğraflanmalıdır. Bilgisayar kapalı ise açılmamalı, açıksa kaparılmamalıdır. Bilgisayar ekranı boş ise mouse hareket ettirilmeli ekranda birşey gözükür ise fotoğraflanmalıdır. Bilgisayar normal kapatma adımları izlenmeden güç kablosu çıkartılarak kapatılmalıdır. Taşınabilir bilgisayarların pilleri sökülmelidir. Bağlı cihazların kabloları etiketlenmeli ve bağlantı şekli çizilmelidir. Tüm bağlı cihazlar ve kablolar sökülmelidir. Bileşenler hassas birşey gibi taşınmalı ve depolanmalıdır. Tüm aygıtlar manyetik alandan, radyo sinyallerinden uzak tutulmalıdır. Bilgisayar ve bileşenlerine ait el koyma işlemi dökümante edilmelidir, (USSS, 2014). Ancak, bilgisayar açık ise kapatılmadan önce hafızadaki uçucu verilerin imajının alınması şüpheli bilgisayarda en son hangi programların çalıştırıldığı ve hangi işlemlerin yapılmaya çalışıldığı hususunda bazı bilgilerin atlanmamasını sağlayacaktır. Bilgisayarın işletim sistemleri açılırken çok sayıda konfigürasyon dosyasına erişim sağlamaktadır. Bu durum suç delili olabilecek verilerin zarar görmesine neden olabilmektedir. Dosya erişim tarihlerinin önemli bir delil olabileceği dikkate alındığında bu durum oldukça sakıncalıdır. Bunun yanı sıra, işletim sistemlerinin açılış esnasında oluşturulan geçici dosyalar ve geçici hafıza disk alanları daha önceden silinmiş olan veri alanlarının üzerine yazılabileceği için silinmiş verilerin delil niteliğinde kurtarılabilme olasılığını ortadan kaldırarak, delilin bütünlüğüne zarar verebilir. Bu nedenlerle incelemesi yapılacak bilgisayar sistemleri ile bazı ağ cihazları kapalı durumda iseler kesinlikle açılmamalıdır (Ekizer, 2014).

Delil niteliğinde olabilecek aygıtlara el konulması gerekiyor ise el koyma işlemi esnasında delil bütünlüğünün bozulmaması için uyulması gereken kurallar Ekizer tarafından şöyle ifade edilmiştir: Delillerin toplanması, paketlenmesi ve nakil edilmesi esnasında elbette zarar görme olasılığı bulunmaktadır. Özelikle bilgisayar sistemleri ve veri depolama birimleri sarsıntı, statik elektrik, yüksek seviyedeki radyo frekansı, ısı, nem ve bir çok dış etkenden etkilenerek zarar görebilmekte, ya inceleme safhasından önce bozulabilmekte ya da inceleme safhasında oluşabilecek teknik sorunlar nedeniyle delil elde edilme olasılığı ortadan kalkabilmektedir. Bu aşamada olay yerindeki diğer işlemler (güvenliğin alınması, fotoğraflama, normal delil elde etme prosedürleri ve çalışan sistemlerin durdurulması gibi) bittikten sonra delil içermesi olası aygıtlar zarar görmemesine dikkat edilerek toplanmalıdır. Mümkünse, manyetik alanlardan ve statik elektrikten etkilenmeyecek şekilde anti statik paketlere konulmalı, sarsıntıdan korunması sağlanarak inceleme için laboratuara götürülmelidir. Bunun yanı sıra, olay yerinden inceleme maksadıyla götürülen tüm eşyanın listesi çıkartılarak, el koyma işleminin hukuksal boyut kazanmasına dikkat edilmelidir (Ekizer, 2014).

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

Sayısal delillerin uygun şekilde korunması delillerin kullanabilirliği açısından çok önemlidir. Sayısal deliller yapısı gereği, özel toplama, paketleme ve taşıma sistemi gerekmektedir. Statik elektrik, manyetik, radyo vericileri ve bu gibi diğer cihazların oluşturduğu manyetik alandan zarar görme veya delil niteliğini kaybetme olasılığına karşı incelemek için alınan aygıtlar önemle korunmalıdır. Toplanan bütün delillerin paketlenmeden önce dokümante edildiğinden, etiketlendiğinden ve kaydı yapıldığından emin olunmalıdır. Hassas veya örtülü/gizli delillere özel dikkat gösterilmeli ve korunması için gerekli önlemler alınmalıdır. Manyetik cihazlar anti statik paketlerle veya statik plastik çantalarla paketlemeli, standart plastik çantalar gibi statik elektrik üreten malzemelerden uzak durulmalıdır. Disket, CD-ROM ve manyetik bantlar gibi bilgisayar aygıtlarınının üzerleri kazınmamalı, bu cihazlar bükülmemeli ve katlanmaya çalışılmamalıdır (TBD Kamu, 2007:104).

Bilgisayar ya da bilgisayar programları ve kütüklerinden elde edilecek delillerin kolayca değiştirilebileceği gerçeği daima göz önünde bulundurularak bilgisayar medyalarının kopyalanması sürecinde bilinçli ya da bilinçsiz olarak delillerin karartılmaması için adli bilişim ilkelerine uygun olarak kopyanın alınması sağlanmalıdır. Bu yüzden, bu işlemlerin yapılması esnasında ehil personel görevlendirilmeli, herhangi şekilde bir bilgisayar eğitimi almış kişilerden ziyade konuyla ilgili üst düzey bilgi ve beceriye sahip olan uzmanlaşmış personelin görev yapması sağlanmalıdır. Zira kopyalama işlemi esnasında adli bilişim ilkelerine uyulmaması, adli bilişimde kullanılan ekipman ya da programlardan farklı alelade bazı program ya da ekipmanlar vasıtasıyla kopyalama işleminin gerçekleştirilmesi ile bire bir kopyalama unsuruna aykırı hareket edilmiş olunacağından ötürü elde edilen kopya hukuka aykırı alınan bir kopya haline dönüşebilmektedir. Adli bilişimde esas olan bilgisayar medyasına ait bire bir kopyalamanın yapılmasıdır. Bilgisayar medyasının bire bir kopyası alındıktan sonra veri bütünlüğünün korunduğunun ispat edilebilmesi için medyanın tamamına ait hash değeri hesaplanmalıdır. Hash değeri bilgisayar medyası üzerinde yapılan en küçük bir değişiklikle değişmektedir.

Delil içermesi muhtemel bilgisayar sistemleri üzerindeki incelemeler, sistemin veri depolama birimlerinin yazma korumalı bir ortamda ve dijital imzalı doğrulaması yapılmış olarak birebir alınmış kopyaları üzerinde gerçekleştirilmelidir. İncelemede kullanılan birebir kopyaya adli bilişimde Adli İmaj (Forensic Image) denilmektedir. Bu birebir kopyalama yani İmaj alma işlemi, incelemeye tabi hedef sistem üzerindeki verilerin bit bazında düşük seviyede kopyalanması ile gerçekleştirilmelidir (Ekizer, 2014). Alınan kopyanın geçerli bir imaj olabilmesi için sistem üzerindeki verilerin bit seviyesinde yansısının alınması yani düşük seviyede kopyalanması gerekmektedir.Kopyalama işlemi esnasında daha istikrarlı olmaları sebebiyle donanımsal yazma koruma araçlarının kullanılması tavsiye edilmektedir. Kopyası alınacak sistemin delil bütünlüğünün bozulmaması için gerekli önlemler alındıktan sonra imaj alma işlemi gerçekleşmelidir.

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

Verileri topladıktan sonra, kanıtlara ait MD5 hash değeri oluşturması gerekmektedir. Hash, orjinal veri ile adli kopyasının karşılaştırılması için kullanılabilir. Hash değerleri eşleştiğinde verinin tam kopyasını ifade eden kanıt olarak kabul edilmektedir (Kleiman, D. / Cardwell, K. / v.d.,2014:10).

Hash değeri, bilgisayar medyasında bulunan tüm 0 ve1'lerin birbirleri ile belirli bir algoritma kullanılarak çarpılması sonucu elde edilen değerdir. Hash, MD5 için 0-9 ve a-f karakterlerinden oluşan 32 karakter uzunluğunda bir değer iken, SHA-1 için aynı karakterleri içeren 40 karakter uzunluğunda bir değerdir (Kılıç, 2014:149). Birden fazla hash algoritması mevcuttur. Ancak, genellikle en çok kullanılan ikisi MD5 ve SHA1'dir (Kent, 2006:4-8). Bu algoritmalar rastgele uzunlukta bir veriyi girdi olarak alırken seçilen hash algoritmasının tipine göre değişik uzunlukta veri üretmektedir

Elektronik deliller açısından imaj alma sırasında oluşturulan hash değeri ile güvenilirlik sağlanması amaçlanmaktadır. Dava sürecinde bir itiraz vuku bulduğunda, hash değeri üzerinden delile müdahale olup olmadığı hususu açıklığa kavuşturulabilecektir (Demirkaya, 2009:74). Burada amaç; benzer şekilde elde edilen ve mahkemeye delil olarak sunulan tüm bulgulara, farklı kişiler tarafından, farklı yer ve zamanlarda da aynı yöntem ve metodlar kullanılarak ulaşılmasıdır (Henkoğlu, 2011:7). Böylece delillerin geçerliliği konusundaki şüphe yok edilebilir.

İmaj alma işlemi orijinal medyada bulunan tüm bilgilerin aynen yeni bir ortama kopyalanması olarak açıklanmaktadır. İmaj alma işlemi neticesinde elde edilen kopya Forensic Duplicate (adli kopya) olarak adlandırılmaktadır (Aydoğan, 2009:35).

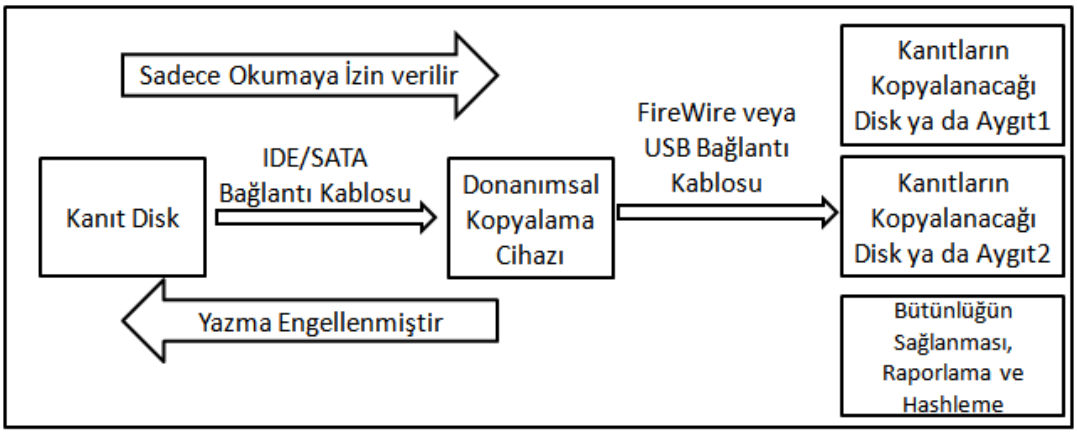
Verilerin toplanması esnasında, araştırmacı ilgili dosya veya dosya sistemini genellikle ana kopya ve çalışılacak kopya gibi birden fazla kopyasını alması tavsiye edilmektedir. Araştırmacı, çalışma kopyasındaki veya ana kopyadaki orijinal dosyaları etkilemeksizin üzerinde işlem yapabilir (Kent, 2006:4-5).

İmaj alma işlemi bu iş için geliştirilmiş özel donanımların yanı sıra imaj alma yazılımları yardımıyla da yapılabilmektedir. Disk imajı alma araçlarındaki minimum gereksinimler aşağıda listelenmiştir.

- Orjinal disk ve bölümünün bit dizisi olarak birebir kopyasını alabilmeli,
- Orjinal diskte değişiklik yapmamalı,
- Alınan imajın bütünlüğünü doğrulayabilmeli,
- I/O(Girdi/Çıktı) hatalarını kaydedebilmelidir (Lyle, 2003:3)

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

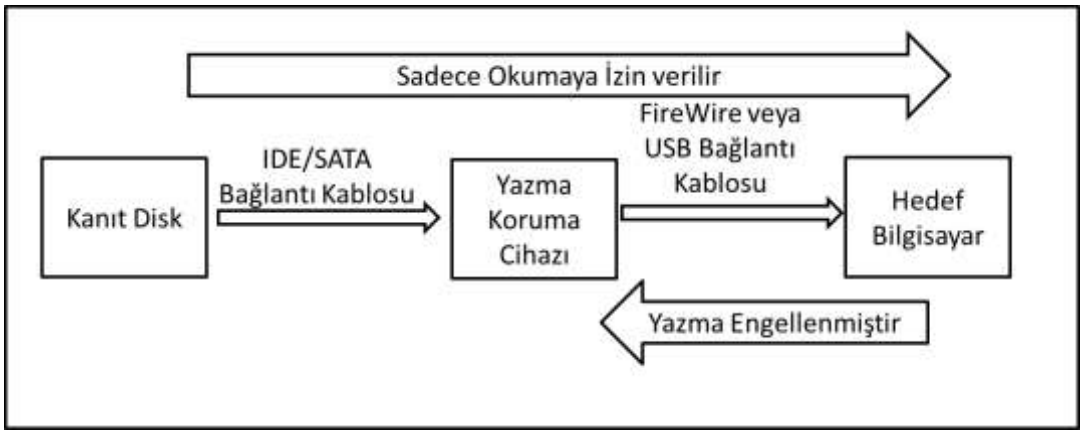
Donanımsal imaj alma araçları orijinal delile fiziksel veri bağlantı kablosu aracılığıyla bağlantı kurularak kendi üzerinde gömülü olarak gelen işletim sistemindeki imaj alma programları vasıtasıyla hedefteki diskin imajını almaktadırlar. İmaj alma işlemi sırasında veri bütünlüğünü korudukları "Yazma koruma" (Write Block) özellikleri sayesinde sadece kaynak olarak tanımlanan bilgisayar medyasından bit seviyesinde kopyalama yaparak hedefteki depolama biriminde ya da kendi üzerinde mevcut olan depolama biriminde imaj dosyası oluşturur. Kaynak olarak tanıtılan bilgisayar medyasına yazma işlemi "yazma koruma" özelliği sayesinde fiziksel olarak engellenmiştir. Herhangi bir bilgisayara ihtiyaç duymamaları, olay yerinde hızlı bir şekilde imaj almaya elverişli olmaları, kaynak olarak tanıtılan bilgisayar medyasına hiçbir şekilde bir şey yazmaması, kolayca taşınabilmeleri ve herhangi bir programın yüklenmesine ihtiyaç duyulmaması bu donanımların avantajları olarak görülebilir. Tableau TD2 Forensic Kit, Digital Intelligence, Data Copy King, Image MASSter, MyKey donanımsal imaj alma araçlarına örnek olarak verilebilir. Donanım olarak imaj alma araçlarının örnek bağlantısı Şekil 1.'de sunulmuştur.



Şekil 1. Örnek Bir Donanımsal Kopyalama Cihazı Bağlantısı (Kleiman, D. , Cardwell, K. v.d., 2014:38).

Bazı donanımsal aygıtlar ve yazılım tabanlı araçlar, imaj alma özelilikleri olmasa bile "yazma koruma" özellikleri sayesinde kopyası alınacak diske hiçbir şey yazmadan sadece bu diskten okuma işlemi yaparak bu bilgileri hedefteki bilgisayara aktarmaktadırlar. Bu aygıtlara ya da yazılımlara da "yazma koruyucusu" (write blocker) denilmektedir (Kent, 2006:4-7). Bu aygıtlar kullanılacağı zaman kopyası alınacak disk IDE, SATA portundan write blocker cihazına, write blocker cihazı da USB portundan kopyanın alınacağı bilgisayara bağlanabilir. Tableau T35u, Tableau T6es, WiebeTech, Forensic UltraDock, yazma koruma cihazlarına örnek olarak verilebilir. Donanım olarak imaj alma araçlarının örnek bağlantısı Şekil 2'de sunulmuştur.

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385



Şekil 2. Örnek Bir Yazma Koruma Cihazı Bağlantısı (Kleiman, D., Cardwell, K., v.d., 2014:36).

Üzerindeki verilerin kopyalanması istenen bilgisayara fiziksel veri bağlantısı kurulduktan sonra, bazı imaj alma yazılımları vasıtasıyla kaynak bilgisayar medyasının imajı alınabilmektedir. Bu ürünler kaynak bilgisayara hiçbir şey yazmadıklarını garanti ederler. Ancak, bu ürünlerle dahi imaj alınsa araya bir yazma koruma cihazı konularak kaynak diske hiçbir şey yazılmadığının donanımsal olarak garanti altına alınması daha garanti bir yöntem olacaktır. Kopyalama esnasında delilin değişmediği imaj alma işlemi sonucunda bazı doğruluma algoritmaları (MD5 ve SHA1 gibi) kullanılarak üretilen değerlerin doğru olduğu tespit edilebilmektedir. Forensic Explorer, FTK Imager, Encase, Win image, OSFClone, Tableau Imager bu türimaj alma yazılımlarına örnek olarak verilebilir.

İmaj alma işlemi bilgisayarın açık ya da kapalı olmasına göre farklılık göstermektedir. Olay yerine gelindiğinde bilgisayar açık ise her şeyden önce uçucu verilerin de imajı alınmalıdır. Açık olan bir bilgisayarın kapatılması ya da güç kablosunun çekilmesi hafızada bulunan verilerin silinmesine sebep olur. Daha sonra sabit diskin bire bir kopyasını almak için gerekli işlem adımları işletilmelidir. Bilgisayarın hafızasındaki bilgilerin kolaylıkla hafızadan silinebileceği ve bu verilerin işlenmiş olabilecek bir bilişim suçunun aydınlatılmasında çok önemli rol oynayabileceği asla unutulmamalıdır.

Mevcut ağ bağlantıları, açık oturum bilgileri, geçici bellek (RAM), İşletim sistemi üzerinde hali hazırda çalışan işlemler, açık olan dosyalar, ağ konfigürasyonu, işletim sisteminin saat ve saat bölgesi bilgileri sırasıyla kopyalanması gereken uçucu verilerdir (Kent, 2006:5-8).

Bellekteki verinin alınması, geçici hafızadaki verinin tamamının kalıcı hafızaya kopyalanmasını içermektedir. Bu belki de geçici bellek adli inceleme sürecindeki en riskli ve en önemli adımlardan biridir. Maalesef, birçok araştırmacı bu kopyalama araçlarının nasıl çalıştıklarını, ilerde ne gibi problemle karşılaşabileceklerini düşünmeden körü körüne bu araçlara güvenmektedir (Ligh / Case / v.d., 2014:69).

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

Bu araçlardan bazıları Belkasoft Live RAM Capturer, Encase Portable (USB Cihazı ve yazılımdan oluşan bir ekipman), Live Response (USB ve yazılımdan oluşan bir ekipman), MoonSols Windows Memory Toolkit gibi donanım ve yazılımdan oluşan ekipmanlar olarak sayılabilir.

Veriler toplanırken karşılaşılan temel sorun aygıtın boş ya da yazmaya izin verilen alanında daha önceki kullanımlarda silinmiş ve artık kalan bilgilerdir. Kullanıcılar çeşitli teknikler kullanarak bu tip verilerin toplanmasını engelleyebilirler. Aygıtın bir kısmının ya da özel bir dosyanın üzerine bit seviyesinde tamamen 0 yazabilecek birçok yardımcı program mevcuttur. Bu tip yardımcı programların güvenilirlikleri değişmekle birlikte birkaç kez silme işlemi yapıldığında çoğu yardımcı program etkili olmaktadır. Kullanıcılar verilerin kopyalanmasını engellemek için cihazın üzerindeki manyetik alana zarar vererek veriye erişimi fiziksel olarak yok edebilmektedirler (Kent, 2006:5-8).

Diğer bir sorun ise daha önce delil toplamada kullanılan aygıtların içeriğinin tam olarak silinmeden yeni delil toplama işlemine başlanmasıdır. Bu durum cihazdaki delil bütünlüğünü bozmaktadır. Bu yüzden herhangi bir veri depolama aygıtı üzerine delil sayılabilecek veriler kopyalanmadan önce cihazın tamamen temizlenmesi gerekmektedir. Bu da üzerindeki verilerin bit seviyesinde silinmesi veya var olan bitlerin üzerine "0" yazılması ile mümkün olabilmektedir (Kleiman / Cardwell v.d., 2007:45).

Verilerin toplanmasından sonraki aşama delil çıkartmadır. Delil çıkartma, imaj alma yazılımları ile bire bir kopyalanan imaj dosyalarından delil olabilecek nitelikteki verilerin bulunması işlemidir. Delil çıkartma esnasında, mevcut dosyalar çeşitli programlar vasıtasıyla aranıp, listelendiği gibi, silinmiş ve gizlenmiş dosyalar da bulunabilmektedir. Delil çıkartma işlemleri aşağıdaki başlıklarda sıralanabilir (TBD Kamu, 2007:105);

- Mevcut dosya araması,
- Silinmiş dosya araması,
- Ayrılmamış alanda dosya araması,
- Kelime araması,
- İnternet işlemleri,
- Link dosyaları,
- Print spool dosyaları,
- Registry incelemesi,
- Dosya imza analizi,
- Hash analizi,
- Geri dönüşüm kutusu kurtarma,
- Takas dosyası,
- Kullanılmamış disk alanı,
- Windows açılısında otomatik çalısan programlar,
- Saklanmıs bölümler (hidden partitions),

Sonraki aşama olan sayısal delil inceleme safhası farklı bir uzmanlaşmayı gerektirmektedir. Adli bilişim uzmanları bilgisayardaki bütün dosyaları teker teker inceleyemeye zaman bulamayabilirler.

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

Sürekli genişleyen disk kapasiteleri dikkate alındığında diskler içerisinde çeşitli tiplerde (ses, resim, görüntü, yazı vb.) binlerce hatta yüz binlerce dosya bulunabileceği görülmektedir. Adli bilişim uzmanları dosya inceleme işlemlerini hızlandıracak ve inceleme işlemini yerine getirenlere kolaylık sağlayacak yazılımları kullanmaya ihtiyaç duymaktadırlar. Üç ayrı kategoriye ayrılan delil inceleme uygulamaları bu ihtiyacı karşılamak üzere hazırlanmış programlardır. Bunlar:

1. Dosya listeleme programları,
2. Kelime arama programları,
3. Dosya tanımlama/görüntüleme programlarıdır.

Sayısal delillerin incelenmesinde hataya neden olmamak için birden fazla delil inceleme yöntemi kullanılmak suretiyle ortaya çıkartılan deliller doğrulanmalıdır. (TBD Kamu, 2007:106)

Son yıllarda, yapay zeka ve veri madenciliği tekniklerinin kullanımı ile yoğun veri kümesi barındıran adli bilişim incelemelerinin daha hızlı ve güvenilir bir şekilde yerine getirilmesi mümkün olabilmektedir.

Kopyası alınan imaj üzerinde incelemelerin yapılması , orjinal deliller üzerinde yazma korumalı ortamda bire bir kopyasının alınması dışında herhangi bir işlem yapılmaması adli bilişimin olmazsa olmaz kurallarından birisidir. Yazma koruması, imaj alma işlemini gerçekleştirenler tarafından ihmal edilmemesi gereken çok önemli bir tedbirdir. Yazma koruması olmadan alınan imajlarda hash değerleri değişebilmektedir.

Son aşama olan sayısal delillerin organize edilip raporlanması adli bilişimin en önemli safhalarından birini oluşturmaktadır. Suç araştırmalarında bulunan delillerin iyi raporlanması her zaman önem arz etmektedir. Zira bu deliller çoğu zaman konu ile ilgili olarak teknik bilgisi olmayan yetkililer tarafından değerlendirilip karara bağlanmaktadır. Bu sebeple delillerin iyi organize edilerek onların anlayacağı şekilde ifade edilmesi gerekmektedir. Delillerin organize edilmesi, hem sayısal olmayan, hem de sayısal deliller için geçerlidir. Sayısal deliller organize edilirken elde edilen sayısal olmayan delillerle ilişkilendirilebilir. Delillerin doğru sırada sunulması anlaşılabilmesi açısından oldukça önemlidir. Özellikle miktar açısından yoğunluğu bulunan ve iyi düzenlenmemiş sayısal deliller günümüzde araştırmacıların delil inceleme safhasında boğulmalarına, gerçeğe ulaşamamalarına ve gecikmelere neden olmaktadır. İyi organize edilmiş ve yetkilileri ikna eden raporlar hazırlanmadan adli bilişim safhalarının etkin bir şekilde yerine getirildiğinden bahsedilemez. İnceleme sonunda hazırlanacak raporda aşağıdaki bilgilere yer verilmesi önem arz etmektedir:

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

1. Araştırmayı yapan kurum ya da kişi ile ilgili bilgiler,
2. Olayla ilgili bilgiler,
3. Araştırmaya başlanma tarihi ve bitiş tarihi,
4. El konan ve inceleme yapılan dijital delillerle ilgili bilgiler,
5. Araştırmada kullanılan donanım ve yazılımla ilgili bilgiler,
6. Araştırmada izlenen yol ve kullanılan yöntem ve teknikler,
7. Gözetim zinciri (hangi delil hangi tarihte kimden kime aktarıldı),
8. Araştırma sonucu bulunanlar, nereden ve nasıl bulundukları rapor edilmelidir. (TBD Kamu, 2007: 106)

Sonuç ve Öneriler

Teknolojinin baş döndürücü bir şekilde her geçen gün gelişmesiyle birlikte evlerimizden iş yerlerimize kadar her ortamda bilgisayar ve akıllı telefon, akıllı televizyon gibi bilgisayar işlevine sahip cihazların kullanımı da hızlı bir şekilde artmaktadır. Her ne kadar doğru ve yeterli bir tanımını yapmak zor olsa da; hukuku, toplum hayatını düzenleyen kuralların kamu gücüyle uygulandığı kurallar bütünü olarak düşündüğümüzde, toplum yaşamının her alanını düzenleyen bu kuralların bilişim sistemlerine yönelik faaliyetlerin yerine getirilmesine ilişkin olarak da çağın gereklerine göre düzenlenmesine ihtiyaç duyulmaktadır. Böylece bilişim alanında faaliyet gösteren bireylerin ya da kuruluşların yerine getirdikleri ya da getirmedikleri işlemlerden ötürü hukuksal boşluktan doğabilecek zafiyetlerin önüne geçilmesi mümkün olabilecektir. Ayrıca, bilgi sistemlerini bu kadar yoğun kullanan toplumlarda, bilişim suçlarına ve bilişim sistemleri vasıtasıyla işlenen diğer suçlara müdahale, soruşturma ve kovuşturma'nın nasıl yapılması gerektiğine ilişkin daha özel yasal düzenlemelerin yapılması bu suçlarla mücadelede daha etkili sonuçların alınmasını sağlayacaktır. Ancak, bu yasal düzenlemelerin teknolojinin hayatımıza girdiği ölçüde onun hızına yetişerek yapılması yasal boşluğun giderilmesi açısından önem arz etmektedir. Ne yazık ki, mevcut düzenlemeler çoğu zaman teknolojiye ayak uyduramamaktadır. Üstelik bu konuda yapılacak çalışmaların sadece hukuk ve bilgisayar biliminde görev alan kişilerce değil diğer alanlarda görev yapan bireylerin katılımlarıyla çok boyutluluk kazanması, çalışmaların etkinliğini arttırması bakımından fayda sağlayacaktır.

Bilişim teknolojilerinde her geçen gün ortaya çıkan yeni zafiyetler bu alandaki teknolojik aygıtların ve yazılımların açıklıklarını kullanmaya istekli bilgisayar korsanlarının iştahlarını kabartmaktadır. Elbette günümüzde bilgisayarlar aracılığı ile suç işleyebilecek tek insan profili bilgisayar korsanları değildir. Söz konusu sistemlerin kullanımının yaygınlaşması ve bu sistemlere olan erişimin geçmişe nazaran nispeten daha kolay hale gelmesi geleneksel anlamda işlenen suçlara

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

yeni bir boyut kazandırmıştır. Bilişim suçlarının hızla artmasının yanı sıra bilişim sistemleri vasıtasıyla işlenen suçların çeşitleri ve miktarları konusunda da hızlı bir artış söz konusudur. İşte bu noktada suçların soruşturulması, kovuşturulması ve sanıkların cezalandırılmasına ilişkin yasal düzenlemelerin yerine getirilmesiyle, uygulamada söz konusu eylemlere karşı yapılan işlemler hukuka uygunluk ya da hukuka aykırılık kazanmaktadır. Anayasa, kanunlar, tüzükler, yönetmelikler hukuk kurallarını oluşturan yazılı birer kaynaktırlar. Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma işlemine ilişkin Ceza Muhakemesi Kanunu'nda, Adli ve Önleme Aramaları Yönetmeliğinde ve Suç Eşyası Yönetmeliğinde bu işlemlerin nasıl yapılması gerektiğine ilişkin bazı düzenlemeler yer almaktadır.

1982 T.C. Anayasasına göre, normlar hiyerarşisi bakımından kanunların arkasında yer alan yönetmelikler başbakanlık, bakanlıklar ve kamu tüzel kişileri tarafından kendi görev alanları ile ilgili kanunların ve tüzüklerin uygulanmasını temin etmek maksadıyla ve bunlara aykırı olmamak koşuluyla çıkartılabilmektedir. CMK'da bilgisayarlarda arama, kopyalama ve el koyma işlemlerine ilişkin kanun düzeyinde düzenlemelerin yer alması, bu koruma tedbirinin uygulanmasının hakim kararına bağlanması elbetteki memnuniyet verici bir durumdur. Ancak, işin uygulanmasında kolluk güçleri ya da işin uzmanları tarafından dikkate alınması beklenen ve esas itibariyle bu konuda detayları içermesi beklenen Adli ve Önleme Aramaları Yönetmeliğinde yeterli detaya yer verilmediği değerlendirilmektedir. Bunun bir sebebi'nin kanunla sınırları çizilen arama ve el koyma işlemine ait daha fazla sınırlama getirmenin kolluk kuvvetinin elini bağlayacağı olduğu düşünülmektedir. Burada işlemlerin nasıl yapılacağına dair daha fazla detay verilmemesinden ötürü, bu konuda genel kabul görmüş bilimsel normlara aykırı olarak yapılan bir takım işlemlerle elde edilen delillerin hukuka aykırı hale gelmesi söz konusu olabilmektedir. Nitekim, son yıllarda gündeme oturan birkaç davada elde edilen delillerin hukuka uygunluğu kamu oyunda büyük tartışmalar yaratmış iç hukukta son başvuru mercii olan Anayasa mahkemesi tarafından bu davalarda yeniden yargılama yapılması gerektiği karara bağlanmıştır.

Teknolojinin hızla gelişmesi bilişim alanında işlenen suçların çeşitliliğini arttırdığı gibi, bilişim cihazlarının işlenen diğer suçlarda kullanılmasıyla buradaki verilerin dijital delil olarak olayın aydınlatılmasında ve yargılama aşamasında kullanılmasını kaçınılmaz hale getirmiştir. Bu gün en basit bir suçun soruşturmasında dahi suçun işlendiği ortamda bulunan veya şüphelilerin kullanmış olabileceği bilgisayarın veya üzerinde veri depolaması yapılabilen ve iletişim amacıyla kullanılan aygıtlar (akıllı telefon, mp3 çalar, USB flash bellek, hafıza kartları vb.)'ın üzerinde olayı aydınlatmaya yarayabilecek ve olayla ilgili çok sayıda delil elde edilebilmektedir. Bu noktada önemli olan bu cihazlara müdahalede bulunurken delil bütünlüğüne zarar verilmemesi ve deliller hakkında herhangi bir şüphe yer vermeden delillerin adli bilişim ilkelerine uygun bir şekilde toplanarak mahkeme

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

heyetinin anlayabileceği şekilde raporlanmasıdır. Bu da ancak ve ancak bu konuda iyi eğitilmiş profosyonel kişiler tarafından olaya müdahale edilmesiyle mümkün olabilmektedir. Ülkemizde maalesef bu konuda yetişmiş insan gücünün az olması sebebiyle suça konu olan veya suç işlemede kullanılan bilişim aygıtı üzerinde yapılan incelemelerde yargılama açısından bazı sıkıntılar ortaya çıkmaktadır. Kimi zaman burada elde edilen delillere uygun müdahale edilmediği için toplanan deliller hukuka aykırı bulunup yargılama açısında dikkate alınmamaktadır. Bu konuyla ilgili olarak; olaya ilk müdahale eden kolluk kuvvetlerine dijital delil bulundurabilecek aygıtlara nasıl müdahale edilmesi gerektiği ile ilgili eğitim verilmesi sorunu bir nebze çözebilir. Ancak, kanunla genel çerçevesi çizilmiş olan bilgisayarlar üzerindeki arama, kopyalama ve el koyma ile ilgili detayları içerecek bir yönetmelik çıkarılmasının olaya müdahale eden kolluk kuvvetlerinin ve adli makamların elini güçlendireceği, soruşturmada ortaya koyulan hareket tarzlarının hukuka uygunluğu açısından oluşabilecek şüpheleri gidereceği değerlendirilmektedir. Kopyalama işlemi ile ilgili olarak CMK'nın 135'inci maddesinde bir hüküm bulunmaktadır. Ancak Adli ve Önleme Aramaları Yönetmeliğinde de aynı ifadelere yer verilmiştir. Delil barındırdığından şüphelenilen bilgisayar medyası üzerinde kopyalamanın nasıl yapılması gerektiğinin hukuki açıdan düzenlenmesine ihtiyaç duyulmaktadır. Nitekim, bilgisayar medyası üzerinde kopyalama işlemleri çeşitli metodlarla yapılabilmektedir. Çıkarılacak yönetmelikte bu metodlardan hangisinin kullanılması gerektiği, konuyla ilgili uygulanacak işlem adımlarına yer verilmesi gerektiği değerlendirilmektedir.

Günümüzde dijital veri cep telefonundan bilgisayara kadar birçok cihazda bulunabilmektedir. CMK'da bu hususta sadece Bilgisayar ve Bilgisayar Kütüklerinde Arama, Kopyalama ve El Koyma ile ilgili düzenlemeler bulunmaktadır. Düzenlemenin dijital veri bulunduran tüm cihazları kapsayacak şekilde genişletilmesi bu cihazlar vasıtasıyla işlenen suçların soruşturulması ve kovuşturulması noktasında akıllarda oluşabilecek şüpheye yer bırakmayacaktır.

Ayrıca sadece bilişim suçları ile ilgili suçların yargılamasını yapacak ihtisas mahkemelerinin kurulması ve bu konuda işlenen suçların soruşturmasını yapacak savcıların yetiştirilmesi ile teknik bir konu olan bilişim suçlarının yargılamasının daha etkin bir şekilde yerine getirileceği düşünülmektedir. Nitekim, günümüzde hırsızlık, tecavüz gibi suçların yargılamasına bakan bir ceza reisi az sonraki bir davada teknik bilgi ve becerinin ağırlığını fazlasıyla hissettirebileceği bilişim suçuyla ilgili bir davanın yargılamasıyla karşılaşabilmektedir. Zaten çok yoğun bir iş yüküne sahip olan hakimlerin ve savcıların bu denli teknik bir konuda davaya yoğunlaşabilmesi bir hayli zor olmaktadır. Hakimler ve savcılar bu konularda suçun soruşturulması ve kovuşturulması ile ilgili olarak bilirkişilerden yardım almaktadırlar. Ancak, bu noktada bilirkişilerin tarafsızlığı hususu ayrı bir tartışmayı doğurmaktadır. Günümüzde bilirkişilerin büyük bir kısmı soruşturma safhasında suça müdahalede bulunan kolluk kuvvetlerindeki personelden teşkil edilmektedir. Kanımca kolluk

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

kuvvetleri soruşturma esnasında görevlendirildikleri için taraf olarak kabul edilmelidirler. Bu konuda mahkeme tarafından ihtiyaç duyulan teknik incelemenin yapılması maksadıyla tamamen adli bilişim uzmanlarının görev aldığı bağımsız bir kurumun teşkil edilmesi incelemenin tarafsız bir şekilde yerine getirilmesi için önem arz etmektedir. Ayrıca, el konulan ya da kopyalanan dijital medyalar üzerinde nelerin, kimler tarafından, hangi maksatla, ne zaman arandığı aramayı talep eden makam ve aramayı gerçekleştiren uzmanlar tarafından kesinlikle yazılı bir şekilde belgelendirilmeli ve bu belgenin bir kopyası üzerinde arama yapılan dijital medya ile ilgisi olduğu düşünülen şüpheliye verilmelidir. Böylece, başka soruşturmalar sebep gösterilerek el konulan dijital medya üzerinde konuyla ilgisi bulunmayan hususlar hakkında arama yapılmadığının ya da sadece konu ile ilgili arama yapıldığının güvencesi sağlanmış olacaktır. Soruşturmayla ilgili olmayan başka hususlar hakkında da arama yapılması talep ediliyor ise bu konuda yeni bir hakim kararı alınması ve bu arama işleminin belgelendirilmesi ile bu durum mümkün olabilecektir. Nitekim, Temel hak ve özgürlükler bakımından bilgisayarlar üzerinde arama yapılması değerlendirildiğinde, yasada bu konuda arama işleminin ancak hakim kararı ile yapılabileceği hususunda hüküm bulunmaktadır. Bu durum, temel hak ve özgürlüklerin sınırlandırıldığı bilgisayarlar üzerinde arama ve el koyma işleminin gelişi güzel ya da şartlar oluşmadan yerine getirilmemesi açısından sevindiricidir. Zira, günümüzde bilgisayarlar üzerinde kişilerin bir çok özel verisi, şirketlerin de bir çok ticari sırrı olabilmektedir. Ancak, burada uygulamada şöyle bir problemden söz etmek mümkündür. Suç eşyası vasfı taşımayan bilgisayarların incelemeden hemen sonra vakit geçirmeksizin sahibine geri iade edilmesi gerektiği yasal düzenlemelerle hükme bağlanmış durumdadır. Bununla beraber, arama ya da el koyma işleminden sonra delillere savcılık tarafından el konulup kopyalanan nüshaların bilirkişilere inceleme için gönderilmesi bilirkişilerin adli kopya üzerinde inceleme yaptıktan sonra herhangi bir suç unsuruna rastlanmadı ise adli kopyaların güvenli bir şekilde silinmesi gerektiğine ve bu işlemin de gerekli incelemeyi yaptıran makam ile bilirkişi tarafından tutanağa bağlanması gerektiğine dair yasalarda ve yönetmeliklerde herhangi bir hüküm bulunmamaktadır. Herhangi bir şekilde bu verilerin üçüncü kişiler tarafından elde edilmesi ile bilirkişiler ve adli makamlar zan altında kalabilecektir. Ayrıca, el konulan ya da kopyalanan özel ya da tüzel kişiliğe ait dijital medyalarda bulunan verilerin hiçbir şekilde amacının dışında kullanılmadığını bilmek bu işlemin mağduru olan kişilerin hak ettiği yasal bir güvence olduğu değerlendirilmektedir.

Kişinin temel hak ve özgürlüklerini sınırlandırması bakımından bilgisayarlarda arama ve el koyma işleminin makul şüphe yerine "somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı" durumunda yapılması, aramanın zorunlu olarak yapıldığı hususunda şüpheye yer vermemesi açısından önemli bir değişiklik olarak değerlendirilmektedir.

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

Olay müdahalesi esnasında veya el konan bir dijital medya üzerinde arama yapılırken uzmanlar tarafından uygulanması gereken standartlar ve yöntemler belirli bir otorite tarafından tanımlanmadığı için olayı ele alış şekli, inceleme yöntemi ve rapor hazırlama hususunda bu işlemi gerçekleştiren uzman kişinin bilgi, beceri ve tecrübesi önemli rol oynamaktadır. Bu konuda dünyanın bazı ülkelerinde hazırlandığı gibi bu işlemleri yapan kurum ya da kuruluşların bilgisayardaki adli bir vakaya nasıl müdahale edilmesi gerektiği, müdahale esnasında nasıl kayıt tutulacağı ve müdahale sonrasında ne şekilde rapor hazırlanacağı hususunda kullanılabilecek bir kılavuzun hazırlanmasına ya da bu konuda standartların oluşturulmasına ihtiyaç olduğu değerlendirilmektedir. Ayrıca, dijital delillerin toplanmasından raporlanmasına kadar geçen süreçte, delillerin taşınmasından incelenmesine kadar yapılan her işleme dair delillere müdahalede bulunan tüm kişilerin krolonojik olarak kayıt altına alınması için standart formlar oluşturulmalı, uygulamada doğabilecek soru işaretleri giderilmelidir. Aynı şekilde, bu kişilerin deliller üzerinde yaptığı bütün işlemler de ayrı bir formda kayıt altına alınmalıdır. Bununla birlikte; adli bilişim vakalarında bu kılavuzda belirtilen standartlar ve yöntemlerle olaya müdahale edilmesi gerektiği, bu durumun da hukuki düzenlemeler vasıtasıyla güvence altına alınması gerektiği değerlendirilmektedir. Böylece, hukuki boşluktan kaynaklanan keyfi davranışların ve hukuka aykırı müdahalelerin bir nebze olsun önüne geçilebileceği değerlendirilmektedir.

Adli bilişimde, elde edilen dijital delillerin hiç kimsenin aklında şüpheye mahal vermeyerek, aynı metotların kullanılmasıyla tekrar aynı sonuçları verecek şekilde toplandığı, delillerin toplanmasından sonra bu deliller üzerinde herhangi bir ekleme ve çıkarma yapılmadığı ve delillerin tam bir tarafsızlık içerisinde, bilimsel metotlara bağlı kalınarak incelendiği hususunda adli makamların ikna edilmesi önemlidir. Ayrıca, elde edilen dijital deliller yargılama esnasında iddia edilen suçun işlendiği hususunda tek başlarına yeterli görülmemeli, suçun vasfı, niteliği ve işleniş şekline göre bu delillerin oluşumu ile şüpheli ya da sanığın kati bir şekilde ilişkilendirilmesi gerekmektedir.

Bilişim suçlarının soruşturulması ve kovuşturulması için uluslararası işbirliği imkanlarının genişletilmesi gerekmektedir. Nitekim, teknolojinin ve internet kullanımının hızlı bir şekilde toplumun her kesimi tarafından tüm dünya çapında yaygınlaşmasıyla birlikte; bilişim suçlarının işleniş şekillleri daha karmaşık hale gelmiş ve ülke sınırları içine sığmaz bir durum almıştır. Zararlı yazılımlar ve bilgisayarlarda kullanılan yazılımların açıklıkları kullanılmak suretiyle masum insanların kullandığı bilgisayarlar bir anda profosyonelce tasarlanmış bir bilişim suçunu işleyen köle bilgisayar ağlarının bir parçası olabilmektedirler. Saldırganlar x ülkesinden, z ülkesinin kritik altyapı sistemlerini kontrol eden bilgisayar ağlarına karşı bir saldırı başlatıp; y ülkesindeki bazı bilgisayarları bu saldırıyı gerçekleştirmek maksadıyla uzaktan kontrol ederek kullanabilmektedirler. Gerçek failler x ülkesinde bulunmasına rağmen, z ülkesi tarafından saldırının y ülkesindeki bilgisayarlar tarafından yapıldığı

bilgisine ulaşılabilmektedir. Bu tip suçların soruşturma ve kovuşturma aşamalarında uluslararası işbirliği önem arz etmektedir.

Sonuç olarak; yasal mevzuat hükümlerinin uluslararası sözleşmeler ve ulusal düzenlemeler de dikkate alınarak çağın gereklerine uygun hale getirilmesi yasayı uygulayan personelin bu konuda eğitilmesi mutlaka sağlanmalıdır. TCK'da "topluma karşı işlenen suçlar" bölümünde yer alan "bilişim alanında suçlar" bölümünün günümüzde çok yaygın olan bilgi ve iletişim teknolojileri kulanılarak kişilere zarar vermeyi amaçlayan siber zorbalık gibi hususları da içine alacak şekilde genişletilmesi ve çağın gereklerine uygun hale getirilmesi gerektiği değerlendirilmektedir. Aynı şekilde bu suçların soruşturulması ve kovuşturulması esnasında başvurulacak yasal tedbirleri içeren CMK ve diğer yasal mevzuat hükümleri daha açık hale getirilerek uygulamada ortaya çıkabilecek aksaklıkların giderilebileceği düşünülmektedir. Yasal mevzuatın oluşturulması ile ilgili olarak Louis D. Brandeis tarafından "Eğer yasalara saygı gösterilmesini istiyorsak, önce saygı duyulacak yasalar yapılması lazımdır." sözü ile yasalar oluşturulurken toplum tarafından kabul görmesi ve ihtiyaca cevap vermesi gerektiğinin önemi vurgulanmıştır.

Kaynaklar

5070, Elektronik İmza Kanunu, (2004). http://www.resmigazete.gov.tr/eskiler/2004/01/20040123.htm#1, (15.10.2015).

5651, 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, (2015). http://www.tib.gov.tr/tr/tr-menu-42-kanunlar.html, (15.10.2015).

5846, Fikir ve Sanat Eserleri Kanunu, (2008). http://www.resmigazete.gov.tr/eskiler/2008/02/20080208-1.htm, (15.10.2015).

6526, Terörle Mücadele Kanunu ve Ceza Muhakemesi Kanunu İle Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun, (2014). http://www.resmigazete.gov.tr/eskiler/2014/03/20140306M1-1.htm, (03.11.2015).

6572, Hâkimler ve Savcılar Kanunu ile Bazı Kanun ve Kanun Hükmünde Kararnamelerde Değişiklik Yapılmasına Dair Kanun, (2014). http://www.resmigazete.gov.tr/eskiler/2014/12/20141212M1-1.htm, (03.11.2015).

Aktaş, K., (2014). Karşılaştırmalı Hukukta Elektronik Deliller. Editör: Çakır, H. Kılıç M.S. Adli Bilişim ve Elektronik Deliller, 519, Ankara.

AÖAY, Adlî ve Önleme Aramaları Yönetmeliği, (2005). http://www.resmigazete.gov.tr/eskiler/2005/06/20050601-15.htm, (15.10.2015).

Aydın, M., (2009). Arama ve El Koyma, Seçkin Yayıncılık, Ankara.

Aydoğan, H., (2009). Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri, Yayımlanmamış Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara.

Bilişim, (2011). "CMK'da Aramanın Nasıl Gerçekleştirileceği Konusunda Bir Açıklık Yok", Türkiye Bilişim Derneği Aylık Bilişim Dergisi, Nisan 2011, Y:39, S:131,

http://www.bilisimdergisi.org/s131/, http://www.yarsav.org.tr/index.php?p=170#.VQql-U39nIU.

CMK, Ceza Muhakemesi Kanunu, (2004). https://www.tbmm.gov.tr/kanunlar/k5271.html, (15.10.2015).

Çakır, H., Sert, E., (2011). Bilişim Suçları ve Delillendirme Süreci. Örgütlü Suçlar ve Yeni Trendler. Uluslararası Terörizm ve Sınır aşan suçlar Sempozyumu (UTSAS 2010) Seçilmiş bildirileri, Polis Akademisi Yayınları, Ankara, sf.143-173.

Değirmenci, O., (2005). 2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi, TBB Dergisi, Sayı:58, sf. 195-208.

Demirkaya, V., (2009). Delil Güvenliği, Yayımlanmamış Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü, Ankara.

Dülger, M.V., (2004). Bilişim Suçları, Seçkin Yayınları, Ankara.

Ergün, İ., (2008). Siber Suçların Cezalandırılması ve Türkiye'de Durum, Adalet Yayınevi, Ankara.

Goodman, M., International Dimensions of Cybercrime, http://ebooks.narotama.ac.id/files/Cybercrimes%20A%20Multidisciplinary%20Analysis/Chapter%2017%20International%20Dimensions%20of%20Cybercrime.pdf, (24.03.2015).

Gözüşirin, M., (2011). 5237 Sayılı Türk Ceza Kanununda Bilişim Suçları Ve Bilişim Suçları İle Mücadeleye İlişkin Model Önerisi, Kara Harp Okulu Savunma Bilimleri Enstitüsü, Ankara.

Henkoğlu, T., (2011). Adli Bilişim (Dijital Delillerin Elde Edilmesi ve Analizi), Pusula Yayıncılık, Ankara.

Karagülmez, A., (2009). Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Seçkin Yayınları, Ankara.

Kent, K., Chevalier, S., Grance, T., Dang, H., (2006). Guide to Integrating Forensic Techniques into Incident Response Recommendations, Recommendations of the National Institute of Standards and Technology, http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf, (24.03.2015).

Kılıç, M.S., (2014). Elektronik Deliller ve Yapısal Özellikleri. Editör: Çakır, H. Kılıç M.S. Adli Bilişim ve Elektronik Deliller, 149, Ankara.

Kızılkaya, E., (2010). Türk Hukuku ve Karşılaştırmalı Hukukta Arama, Elkoyma ve Gözaltı, http://tbbdergisi.barobirlik.org.tr/m2010-89-635, (15.03.2015).

Kiçeci, H., (2014). Bilgisayar Medyalarına İlk Müdahale. Editör: Çakır, H. Kılıç M.S. Adli Bilişim ve Elektronik Deliller, 166, Ankara.

Kleiman, D./ Cardwell, K. / Clinton, T. / Cross, M. / Gregg, M. / Varsalone, J. / Wright, C., (2007). The Official CHFI Exam 312-49 Study Guide For Computer Hacking Forensics Investigators, Syngress Publishing, United States Of America.

Koparan, R., (2006). Bir Koruma Tedbiri Olarak Arama, http://www.ceza-bb.adalet.gov.tr/makale/193.doc, (16.03.2015).

Ligh, M.H., Case, A., Levy, J., Walters, A., (2014). The Art of Memory Forensics, John Wiley & Sons, United States of America.

Lyle, J.R., (2003). NIST CFTT: Testing Disk Imaging Tools, International Journal of Digital Evidence, Winter 2003, V:1, I:4, https://www.utica.edu/academic/institutes/ecii/publications/articles/A04BC142-F4C3-EB2B-462CCC0C887B3CBE.pdf, (23.03.2015).

Öztürk, B., Erdem, M.R., (2006). Uygulamalı Ceza Muhakemesi Hukuku, Seçkin Yayınları, Ankara.

Özbek, V.Ö., Tepe, İ., Doğan K., Kanbur, M.N., Bacaksız, P. (2013). Ceza Muhakemesi Hukuku, Seçkin Yayınları, Ankara.

Sırma, Ö., (2008). 5271 Sayılı Ceza Muhakemesi Kanunu'nda Elkoyma, Uğur Alacakaptan'a Armağan, C. 1, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.

TBD Kamu, (2007). Bilişim Teknolojilerinin Kullanılmasının Hukuksal Boyutu, Türkiye Bilişim Derneği 2 nci Çalışma Grubu, http://www.tbd.org.tr/usr_img/cd/kamubib12/raporlarPDF/RP2-2007.pdf, (05.04.2015)

TCK, Türk Ceza Kanunu, (2004). https://www.tbmm.gov.tr/kanunlar/k5237.html, (15.10.2015).

USDOJ, U.S. Department of Justice, Prosecuting Computer Crimes, http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf, (14.03.2015).

USSS, Best Practices For Seizing Electronic Evidevce v3 A Pocket Guide For First Responder, U.S. Secret Service, http://www.crime-scene-investigator.net/SeizingElectronicEvidence.pdf , (23.03.2015).

Ulrich, S., (1998). Legal Aspect Of Computer-Related Crime in the Information Soceity-COMCRIME-Study-prepared for the European Commission, http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf, (24.03.2015).

Yazıcıoğlu, Y., (2004). "Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi", Hukuk ve Adalet: Eleştirel Hukuk Dergisi, İstanbul, Y:1, S:1, Ocak-Mart.

Yaşar, Y., Dursun, İ.,(2013). Marmara Üniversitesi Hukuk Fakültesi Hukuk Raştırmaları Dergisi, Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve ElkoymaKoruma Tedbiri, Cilt:19, Sayı:3, Yıl:2013, (http://e-dergi.marmara.edu.tr/maruhad/issue/download/5000001574/5000000684), (15.03.2015)

Yenisey, F., Feridun Hoca İle Ceza Muhakemesi Hukuku, Adli Arama, (http://www.caginpolisi.com.tr/eski_sitemiz/144/7-8-9-10-11-12-13-14-15-16.htm), (16.03.215)

Extended English Abstract

In our globalized world; with the development of technology at an inconceivable speed in each passing day, generated products have made human life easier and more comfortable than ever before. Computer, invented in the mid-twentieth century, is one of the leading of the products that make our lives easier in each passing day. The introduction of local area network of computers that allows them to communicate with each other. With the discovery and widespread use of internet, communication between computers haven't bounded in the frontiers of the countries.

With computers and many devices computer technology which facilitating our lives so much, becoming lots of work we can not do without it, having very important place in our life, has become possible to commit a crime conscious or unconscious. Mankind has managed to associate this device which facilitate his life so much, with in a crime related to information system or irrelevant. Today the computer has become a tool not only ceased to be a revolutionary concept that just facilitates our lives, but also cited with the concept of crime (Dokurer,2001). The concept of cyber crimes has emerged by means of cyber crimes committed by using IT devices. For countries using the computer technology, cyber crimes has become a common problem. Thanks to

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

the Internet, with the help of reaching global size in information sharing and access to information, committing IT crimes have been exceeded beyond the countries' borders. National regulations are observed that they are inadequate in combating this crime. Therefore, international law and transnational cooperation has gained tremendous importance in the fight against IT crimes.

Search, copy and seizure in computers is a legal measure, starting with the detection of crime and may come up in the investigation or prosecution phase of various crimes also taking into consideration the confidentiality and privacy of the concept of private life, should not be applied unless mandatory.

Whether or not commited a crime; if it is committed, it is by whom in order to bring a solution to what would be the question of what sanctions processed claims held by CMK as a rule, defense and a series of activities to criminal proceedings in the trial nature is Criminal Procedure. The branch of law dealing with this is called the Law of Criminal Procedure (Öztürk/Erdem, 2006:57).

In an interview given by Vice President of Judges and Prosecutors Association, Bulent Yücetürk, has stated that according to the law that need to be searched for computers and computer files primarily, and then according to the data obtained from them if it is necessary, seizure measure can be applied. (IT, 2011: 101).

According to Yücetürk even if it had not been involved in the law, it could have done a search on computers and confiscated by the general search rules. However, the formal rules have been adopted in the collection of digital evidence by considering the technical part of the job with the arrangements made. As previously not to be available in a clear arrangement about search and seizure of computer in our legislation, all of the search and seizure were conducted in accordance with general provisions. The provisions relating to Law of Criminal Procedure No. 5271 search and seizure on computers for the first time were introduced (Bilişim, 2011:102).

Search in computers, Copy and Seizure measures in the Turkish Legal System generally are set out in the Code of Criminal Procedure Aricle 134 published in the Official Journal on 17.12.2004. Apart from this, there are some provisions in the Judicial and Prevention Searches Regulation Article 17 about how to make process of search, copy and seizure in the computer, the computer programs and files. Before the date 17.12.2004, because there wasn't any regulation that would be made how to fulfill search, copy and seizure on computer programs and computer files, the transactions made on the computer were performed taking into account the general principles at that time.

In the context of the principles stated in Law of Criminal Procedure No.5271 article 134, search on computers, computer programs and files, copying and seizure operation can be performed.

With each passing day emergence of new vulnerabilities in information technology are blistered the appetite of hackers who are eager to use the vulnerabilities in the field of technological devices and software. Of course, nowadays hackers are not the only people profile that can commit a crime by computer. The widespread use of these systems and becoming relatively easy access to these systems compared to the past have brought a new dimension to the crimes committed in the traditional sense. The Constitution, laws, statutes, regulations are written sources that make up the rule of law. In the Turkish legal system relating to the process of search on computer, copying and seizure there are some regulations how these process need to be done in the Law of Criminal Procedure, Regulations of Judicial and Prevention Searches, and in the Regulation of Crime Goods.

Bostancı, Ü., & Benzer, R. (2015). Türk hukuk sisteminde bilgisayarlarda arama, kopyalama ve el koyma. *International Journal of Human Sciences*, *12*(2), 1192-1229. doi: 10.14687/ijhs.v12i2.3385

In Criminal Procedure Law relating to process of search, copy and seizure on computer, being regulations at the level of law, binding decision of the judge to the implementation of these protection measures are a satisfactory condition, of course. Nevertheless, in the enforcement of law taking into account expected by police forces or experts and essentially expected to include the details of this matter in Regulations of Judicial and Prevention Searches is considered not given sufficient details. One of the reasons of this, boundaries drawn by law, bringing more restrictions process of search and seizure is thought to restrict security forces. Due to the non given more details about how to do procedures here, the evidences obtained through a number of transactions carried out in violation of generally accepted scientific norms on this issue can be said to become unlawful. Indeed, the evidence of which was obtained in a few cases on the agenda last year in compliance with public law has created major debate, and decided needs to be done retrial by the Constitutional Court is the last resort in domestic law.

In computer Forensics, by avoidance of doubt in the mind of anyone in the obtained digital evidence, collecting digital evidence using the same methods so as to give the same results again, after the collection of the evidence on which any addition and subtraction not to be done, and in complete neutrality of evidence, examined adherence to the scientific methods are important to convince the judicial authorities. In addition, digital evidence obtained during the trial should not be considered sufficient alone in respect of the alleged crime was committed, characteristic of of the crime, according to the nature of the course must be strictly linked with the formation of such evidence a suspect or defendant.

In the light of mentioned above; adapting the provisions to the requirements of the era taking into consideration the regulations of international treaties and national legislation, training security forces on this issue, the establishment of specialized courts, recruiting expert staff in these courts must be provided.