Uzmanlık Tezleri Serisi No: 159

REKABET KURUMU

REKABET HUKUKU UYGULAMALARI KAPSAMINDA ADLİ BİLİŞİM

ZAHİDE ORMAN

REKABET HUKUKU UYGULAMALARI KAPSAMINDA ADLİ BİLİŞİM

ZAHİDE ORMAN

Ankara 2017

Baskı, Nisan 2017
Rekabet Kurumu-ANKARA

Bu kitapta öne sürülen fikirler eserin yazarına aittir;
Rekabet Kurumunun görüşlerini yansıtmaz.

Bu tez, Rekabet Kurumu Başkan Yardımcısı Hasan Hüseyin ÜNLÜ, Rekabet Kurumu Başkan Yardımcısı Kürşat ÜNLÜSOY, Bilgi Yönetimi Dairesi Başkanı Ferhat TOPKAYA, Baş Hukuk Müşaviri Salim AYDEMİR ve Prof. Dr. Fuat OĞUZ'dan oluşan Tez Değerlendirme Heyeti tarafından 24-25-26 Ekim 2016 tarihlerinde yürütülen Tez Savunma Toplantısı sonucunda yeterli ve başarılı kabul edilmiştir.

Tez yazarı Zahide ORMAN, 02.12.2016 tarihinde yapılan Yeterlik Sınavında başarılı olmuş ve Başkanlık Makamının 16.12.2016 tarih ve 13645 sayılı onayı ile Rekabet Uzmanı olarak atanmıştır.

YAYIN NO **337**

Eşime, çocuklarıma, adalete ve
güzel günlere inanan tüm çocuklara...

İÇİNDEKİLER

BÖLÜM 3

REKABET HUKUKU ALANINDA ADLİ BİLİŞİM UYGULAMALARI

BÖLÜM 4

TÜRK MEVZUATINDA ADLİ BİLİŞİM

ŞEKİL DİZİNİ

TABLO DİZİNİ

KISALTMALAR

AB	**:** Avrupa Birliği
ABAD	**:** Avrupa Birliği Adalet Divanı
ABD	**:** Amerika Birleşik Devletleri
ACPO	**:** Association of Chief Police Officers
Açıklayıcı Not	**:** 1/2003 Sayılı Tüzüğün 20. maddesinin 4. fıkrası Uyarınca Gerçekleştirilen İncelemelere İlişkin Açıklayıcı Not
Age	**:** Adı geçen eser
AİHM	**:** Avrupa İnsan Hakları Mahkemesi
AİHS	**:** Avrupa İnsan Hakları Sözleşmesi
AK	**:** Avrupa Konseyi
AYM	**:** Anayasa Mahkemesi
BDDK	**:** Bankacılık Düzenleme ve Denetleme Kurumu
bkz	**:** Bakınız
CCTV	**:** Closed-Circuit Television
CD	**:** Compact Disc
CMK	**:** Ceza Muhakemeleri Kanunu
DVD	**:** Digital Versatile Disc
FBI	**:** Federal Bureau of Investigation
FTC	**:** Federal Trade Commission
FTK	**:** Forensic Tool Kit
GM	**:** General Court (Avrupa Birliği Genel Mahkemesi)
GPS	**:** Global Positioning System
GSM	**:** Global System for Mobile Communications
ICN	**:** International Competition Network
IT	**:** Information Technology (Bilgi Sistemleri)
İDDK	**:** Danıştay İdari Dava Daireleri Kurulu
Komisyon	**:** Avrupa Komisyonu
Konsey	**:** Avrupa Konseyi
Kurul	**:** Rekabet Kurulu
Kurum	**:** Rekabet Kurumu
LAN	**:** Local Area Network

NIST	**:** National Institute of Standards and Technology
OECD	**:** Organisation for Economic Co-operation and Development
Örn	**:** Örneğin
para.	**:** paragraf
PC	**:** Personal Computer
PDA	**:** Personal Digital Assistant
RAM	**:** Random Access Memory
Rehber	**:** Avrupa Konseyi Dijital Delil Rehberi
RKHK	**:** 4054 sayılı Rekabetin Korunması Hakkında Kanun
SPK	**:** Sermaye Piyasası Kurulu
SSD	**:** Solid State Disk
SQL	**:** Structured Query Language
s.	**:** sayfa
Tasarı	**:** Rekabetin Korunması Hakkında Kanun'da Değişiklikler Öngören Kanun Tasarısı
TBMM	**:** Türkiye Büyük Millet Meclisi
USB	**:** Universal Serial Bus
US DOJ	**:** United States Department Of Justice
vb.	**:** ve benzeri
vd.	**:** ve diğerleri
VHS	**:** Video Home System

GİRİŞ

"Her temas bir iz bırakır."
Edmond Locard

Günümüzde teknoloji hızla gelişmekte; buna bağlı olarak tüm belgelerin bilgisayar, tablet ve telefon gibi dijital ortamlarda oluşturulması ve saklanması yaygınlaşmaktadır. Bu durum, bireylerin bilgiye erişimini kolaylaştırmakla birlikte, suçluların veya kanunları ihlal etme güdüsünde olanların ilgisini çekmekte, normal yollarla oldukça zor işlenebilecek çeşitli suçlar, bilişim teknolojileri yoluyla daha kolay işlenebilir hale gelmektedir. Bunun bir sonucu olarak gündeme gelen ve bilişim suçlarının takip/tespit edilebilmesi amacıyla ortaya çıkan *adli bilişim* kavramı, günümüzde birçok iş ve işlemin dijital ortamlarda yürütülmesinden dolayı sadece bilişim suçlarına özgü bir olgu olmaktan çıkmakta, diğer suçların tespitinde de kullanılmaya başlanmaktadır. Bu bağlamda suç şüphesi doğuran herhangi bir olayda ilgilinin kullandığı tüm dijital cihazlar konuyu aydınlatmak amacıyla incelenebilmektedir.

4054 sayılı Rekabetin Korunması Hakkında Kanun'da (RKHK) yasaklanan bazı eylemlerin de teknolojideki gelişmelerden etkilenerek, dijital ortamlarda gerçekleştirildiği görülmeye başlanmaktadır. E-postalar aracılığıyla haberleşebilen rakipler, anlık mesajlaşma yazılımları kullanarak toplantılar organize edebilmekte, bilgisayardan görüntülü konuşmalar yapmak suretiyle toplanabilmekte ve kararlar alabilmektedir. Bu sebeple RKHK'ya aykırı olan ilgili eylemlerin ortaya çıkarılması genellikle dijital ortamlarda inceleme yapmakla mümkün olabilmektedir. Ne var ki Rekabet Kurumu'nun (Kurum) ihlalleri ortaya çıkarmak amacıyla gerçekleştirdiği yerinde inceleme faaliyetinde, e-posta ve basit kavramsal aramaların dışına çıkılamadığı gözlemlenmekte; bunun ise delil bulmadaki etkinliği azalttığı ve teşebbüslerde caydırıcılığı sağlayamadığı düşünülmektedir. Bir bilgisayar incelemesi kapsamında dijital/elektronik delil bulma

etkinliğini artırmak amacıyla kullanılacak yöntemlerin en etkilisi şüphesiz ***adli bilişim uygulamaları***dır. Bu uygulamalar sayesinde dijital cihazlardan silinmiş, şifrelenmiş vb. verilerin çıkarılabildiği, anlamsal aramalar yapılabildiği, delil tasnifi esnasında hiçbir potansiyel delilin kaybedilmediği bilinmektedir.

Bu kapsamda RKHK'da yer alan yerinde inceleme hükümlerinin dijital delil bulma yollarından biri olan adli bilişim uygulamaları çerçevesinde irdelenmesi ve ihtiyaç halinde geliştirilmesi gerekmektedir. Yerinde incelemeler esnasında kullanılabilecek adli bilişim uygulamaları vasıtasıyla delil bulmada ne tür faydalar sağlanacağını ortaya koymayı amaçlayan bu çalışmada, Kurum'un klasik delil elde etme yöntemlerinden sıyrılarak adli bilişim uygulamaları yoluyla yeni bir usul belirlemesi üzerinden çeşitli tartışmalar yapılmakta ve önerilerde bulunulmaktadır.

Yukarıda yer verilen açıklamalar doğrultusunda dört bölümden oluşan bu çalışmanın ilk bölümünde adli bilişim hakkında genel bilgiler sunularak adli bilişim ile rekabet hukukunun ilişkisi irdelenmektedir. İkinci bölümde, adli bilişimin teknik boyutu hakkında bilgilere yer verilmektedir. Bu kapsamda dijital delillere ulaşılabilecek kaynakların neler olabileceği üzerinde durulmakta, bu kaynaklarda bulunan dijital delillerin nasıl elde edileceği hakkında açıklamalar yapılmaktadır. Çalışmanın üçüncü bölümünde, ilk olarak RKHK'nın mehazını da teşkil eden Avrupa Birliği (AB) mevzuatı ve uygulamalarında adli bilişimin nasıl ve ne şekilde uygulandığı hakkında yargı kararları dâhilinde detaylı açıklamalara yer verilmektedir. Bu bölümde ayrıca Türkiye'den farklı bir hukuki sisteme tabi ve rekabet hukuku uygulamasının ilk ortaya çıktığı ülke olan Amerika Birleşik Devletleri'nde (ABD) ve bazı ülkeler nezdinde adli bilişim uygulamaları hakkında genel bilgiler sunulmaktadır.

Çalışmanın son bölümünde ise ülkemiz mevzuatında yer alan adli bilişim uygulamalarına yer verilmektedir. Bu bölümde öncelikle adli bir süreç dâhilinde uygulanan Ceza Muhakemesi Kanunu (CMK) kapsamında adli bilişim uygulamalarına ilişkin yasal altyapı ortaya konulmakta, ardından Kurum gibi bağımsız idari otorite olan Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) ve Sermaye Piyasası Kurulu'nun (SPK) adli bilişime yönelik mevzuatları irdelenmektedir. Son olarak ise tüm bu bilgiler çerçevesinde RKHK kapsamında adli bilişim uygulamasının mümkün olup olmadığı tartışılmakta ve etkin bir uygulamanın nasıl olması gerektiği hususlarında önerilerde bulunulmaktadır.

BÖLÜM 1

ADLİ BİLİŞİM VE REKABET HUKUKU İLE İLİŞKİSİ

Bilişim teknolojilerindeki gelişmelere paralel olarak yeni iletişim ve haberleşme olanakları vasıtasıyla *sanal* ortamda sözleşmeler yapılmakta, mal/hizmet alım/satımı gerçekleştirilmektedir. Bilişim teknolojilerinin sunduğu olanaklar sayesinde fiziki olarak bir arada bulunmayan teşebbüsler veya teşebbüslerle müşteriler arasındaki işlemler dijital ortamda icra edilmekte ve bu işlemler sonucunda dijital belge/delil kavramları önem kazanmaktadır (Demircioğlu 2014, 28). Dijital verilerin bu kadar yoğun ve yaygın kullanılması, her türlü bilginin dijital ortamlarda (bilgisayar sabit diskleri, taşınabilir bellek vb.) saklanması, klasik evrak dolaplarının (ve klasik delillerin) yerini bilgisayarların alması sonucunu doğurmaktadır (Say 2006, 24). Bu kapsamda RKHK bağlamında ihlal olarak değerlendirilen her türlü veri de dijital ortamlarda paylaşılabilmektedir. Herhangi bir inceleme esnasında böylesi bir veri paylaşımını tespit etmek için kullanılan araçlardan biri de adli bilişim uygulama ve yöntemleridir. Bu itibarla öncelikle bu bölümde adli bilişim ve adli bilişim uzmanı kavramları ile ilgili açıklamalar yapılmakta, daha sonra adli bilişim türleri ile adli bilişimin rekabet hukuku ile bağlantısı hakkında bilgi verilmektedir.

1.1. ADLİ BİLİŞİM VE ADLİ BİLİŞİM UZMANI KAVRAMLARI

1.1.1. Adli Bilişim

Adli bilişim kavramı dilimize İngilizce "*computer forensic*[1]" (ya da Forensic IT) ifadesinden çevrilmiş olup, kapsamının genişliği ve kullanım kolaylığı nedeniyle "bilgisayar kriminalistiği[2]" ifadesi yerine tercih edilmektedir (Aydoğan 2009, 7).

Esasında adli bilişim, bir adli bilim dalıdır. Adli bilim ise meydana gelen adli olay içerisindeki delillere ulaşmak için teknolojik ve bilimsel teknikleri kullanmak olarak tanımlanmaktadır (Shinder 2002, 38). Adli bilim, tıp, fen bilimleri, mühendislik bilimleri gibi birçok mesleki bilginin adli görev ve hizmetlerde kullanılması amacıyla ortaya çıkmış olup (Henkoğlu 2014, 1), temelde "fen bölümleri", "tıp-sağlık bölümleri", "sosyal bölümler" ve "kriminalistik bölümler" şeklinde dörde ayrılmaktadır. Adli bilişim, adli bilimlerin kriminalistik bölümü altında incelenen bir alt dalıdır (Ünal 2011, 12).

Kruise ve Heiser (2002, 2) tarafından bilgisayar verisinin muhafazası, tanımlanması, elde edilmesi, dokümantasyonu ve yorumlanması olarak tanımlanan adli bilişimi, Ekizer (2014, 1) şu şekilde açıklamaktadır:

> Suçun aydınlatılabilmesi için bilimsel metotlar kullanılarak, çeşitli varyasyonlardaki dijital medyalar üzerinde bulunan, suçla ilgili **dijital delillerin bozulmadan ve zarar görmeden** anlaşılabilir bir şekilde adalet önüne sunulmaya hazır hale getirilmesini sağlayan ve başlı başına bilimsel teknik prensiplerin uygulandığı bir delil inceleme sürecinin bütünüdür.

Kendine özgü kuralları bulunan, bilişim teknolojilerinin gelişime ve sürekli yenilenmeye açık vizyonu ile çok disiplinli yeni bir bilim dalı olan (Ahi 2009, 34) adli bilişim; dijital cihazlarda bulunabilecek davacı veya davalının iddialarını kuvvetlendiren veya çürüten bilgilerin mahkemeye sunulması için yapılan bir inceleme faaliyeti olarak da tanımlanmaktadır (Keser Berber 2004, 39).

---

[1] Genelde "mahkeme ile alakalı" şeklinde Türkçe'ye çevrilen "*forensic"* kelimesi 16. yüzyılda Eski Roma'da halka açık olarak kurulan mahkeme alanlarını ifade eden "forum" kelimesinden türetilmiştir ve "yargılamaya uygun", "açığa çıkarma" gibi anlamlar ifade etmektedir. *Online Etymology Dictionary*, http://www.etymonline.com/index.php?allowed_in_frame=0&search=forensic&searchmode=none, Erişim Tarihi: 12.10.2015.

[2] Kriminalistik; suç ve suçlunun bilimsel yöntem ve araçlar kullanılarak tespit edilmesi, belirlenmesi, suçun aydınlatılması ve suç analizinin yapılmasıdır (Kaygısız 2008, 9).

Tüm bu tanımlardan hareketle, herhangi bir suça/ihlale ilişkin delil niteliği taşıyan bilgileri dijital ortamlardan zarar görmeden çıkarıp adaletin (adli veya idari karar vericilerin) kullanımına hazır hale getirmeyi adli bilişim olarak ifade etmek mümkündür.

1.1.2. Adli Bilişim Uzmanı

Adli bilişim, gerek teknik özellikleri, gerekse üzerinde inceleme yapılan konunun sonucuna göre temel hak ve özgürlükler üzerinde doğuracağı etkiler nazara alındığında ihtisas ve dikkat gerektiren bir bilim dalıdır. Bu nedenle bu alanda görev yapanların da görevin niteliğine uygun özelliklere sahip olması gerekmektedir.

Bir olay/dava ile ilgili suça veya suçsuzluğa konu olan bilişim sistemlerini teknik olarak inceleyen ve neticeyi adli mercilerin hizmetine anlaşılır ve güvenilir bir şekilde sunan kişilere *adli bilişim uzmanı* denilmektedir (Şengül vd. 2014, 95).

Avrupa Konseyi (Konsey) 2010 yılında, Avrupa'daki tüm polis teşkilatlarından katılımcılarla başlattığı "*CyberCrime@IPA*" projesinde adli bilişimin uluslararası standartlarda yapılabilmesi amacıyla çeşitli toplantılar düzenlemiştir. Toplantılar neticesinde 2013 yılında "*Avrupa Konseyi Dijital Delil Rehberi*[3] "ini (Rehber) yayımlamıştır. Rehber'e göre adli bilişim uzmanlarında bulunması gereken özellikler şu şekildedir:[4]

- Yeterli uzmanlık bilgisi ve alan uzmanlığı,
- Yeterli araştırma becerisi,
- Eldeki materyallerle ilgili yeterli bilgi sahibi olması,
- Yeterli hukuk bilgisi,
- Sözlü ve yazılı yeterli iletişim kabiliyeti,
- Başka dillerde sunulması gereken raporlar için yeterli yabancı dil bilgisi.

Adli bilişim uzmanlarının bilişim teknolojisi konusunda iyi bir bilgi birikimine sahip olması gereğinin yanı sıra, karar merciine sunulacak raporları amaçlanan tüm

[3] Avrupa Konseyi Dijital Delil Rehberi, Mart 2013, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp, Erişim Tarihi:15.10.2015.
[4] Age s.33-35.

bilgileri de içerecek bir biçimde eksiksiz oluşturabilmesi için ceza ve usul alanında (Ünal 2011, 15) yeterli hukuk altyapısına da sahip olmaları beklenmektedir (ICN 2014, 13).

1.2. ADLİ BİLİŞİM SÜREÇLERİ

Adli bilişim sürecinin aşamalarına ilişkin doktrinde farklı görüşler bulunmaktadır. Herhangi bir araştırma sürecinde olduğu gibi adli bilişim sürecini delilleri "toplama", "muhafaza etme", "filtreleme" ve "sunma" (Brown 2006, 7-8) olarak özetleyenler olmakla beraber, bu süreçleri detaylı delillendirme adımları ile tanımlayan görüşler de mevcuttur.[5] Doktrinde bu görüşlerden en yaygın kabul göreni adli bilişim sürecini dörde ayıran yaklaşımdır. Bu yaklaşıma göre adli bilişim sürecinin adımları "teşhis etme", "koruma", "analiz etme" ve "sunma"'dır (Uzunay ve Koçak, 2005, 4).

Yukarıdaki adımların daha sağlıklı ve yeknesak ilerleyebilmesi adına dünyada tüm kolluk ve adalet teşkilatları tarafından genel kabul görmüş çeşitli prensipler belirlenmiştir. Bu prensipler şu şekildedir (US DOJ 2004, 2-20):

- Delilin toplanması sırasında delilin bütünlüğüne ve güvenilirliğine dair önlemler alınmış olmalıdır.
- Dijital delil ile ilgilenecek kişi bu konuda eğitimli olmalıdır.
- Delillerle ilgili arama, el koyma, inceleme, yedekleme veya transfer etme işlemleri tutanağa geçirilmeli ve bu tutanaklar daha sonra incelenmek için saklanmalıdır.
- Mahkemede delil olarak kullanılabilecek veriyi içeren bilgisayar veya depolama aygıtında kanun uygulayıcılar tarafından veriyi değiştirebilecek herhangi bir işlem yapılmamalıdır (ACPO 2012, 6-7).

Takip eden bölümde adli bilişimin dört temel adımı irdelenmektedir.

[5] Casey'e (2004, 187-198) göre adli bilişimde delillendirme süreci: 1-suçlama ve vaka alarmı, 2-değer değerlendirmesi, 3-olay/suç yeri protokolleri, 4-tanımlama ve toplama, 5-koruma, 6-kurtarma, 7-ayrıştırma, 8-indirgeme, 9-organizasyon ve araştırma, 10-analiz, 11-raporlama, 12-ikna etme ve tanıklık olarak 12 adımdan oluşmaktadır.

1.2.1. Teşhis Etme

Olay yerindeki dijital delil kaynaklarının belirlenmesini ve usulüne uygun toplanmasını hedef alan teşhis etme aşaması, delillendirme sürecinin ilk adımı olması sebebiyle büyük önem taşımaktadır (Uzunay ve Koçak 2005, 4). Zira teşhis aşamasında yapılacak herhangi bir teknik hata, delillerin zarar görmesine, hatta yok olmasına sebep olabilmektedir. Bu nedenle ilk müdahale aşamasında hangi cihaza ne tür işlem yapılacağının doğru bir şekilde tespit edilmesi gerekmektedir. Bu kapsamda teşhis aşamasında yapılması gerekenler; olay yerinin güvenliğinin sağlanması, fotoğraflanması, tanımlanması ve krokisinin çizilmesi (Şimşek vd. 2012, 44), incelenecek cihazların tespiti, orijinal haliyle kopyalanması ve fotoğraflanması, sonraki aşamalarda işe yarayabilecek özel notlar yazılması ve tüm bu aşamaların detaylı bir şekilde raporlanması (Aydoğan 2009, 11) olarak sıralanabilir. Bu bağlamda örneğin, olay yerinde bulunmuş, halen açık durumdaki bir cep telefonunun veya bilgisayarın kapatılmasının önlenmesi, cihaz üzerindeki uçucu verilerin kaybolmasına engel olmak adına iyi bir adli bilişim pratiği olacaktır.

1.2.2. Koruma

Delillerin tespit edilip birebir kopyasının alınması işleminden sonra, delillerin doğru ortamlarda taşınması ve korunması aşamasına geçilmektedir. Bu aşama, delilin veya kopyanın orijinalliğinin bozulmaması için alınacak çeşitli önlemleri kapsamaktadır. Alınacak önlemler fiziksel ve dijital önlemler olarak ikiye ayrılabilir (Uzunay ve Koçak 2005, 5).

Olay yerinden alınan delillerin fiziksel olarak güvenli bir şekilde inceleme noktasına ulaştırılması için alınan önlemlere fiziksel önlemler denmektedir (Uzunay ve Koçak 2005, 5). Delilleri ısı, nem, manyetizma gibi dış etkenlerden korumak fiziksel önlemler arasındadır. Bu kapsamda örneğin olay yerinden elde edilmiş bir cep telefonunun hiçbir fiziksel zarar görmeden ve elde edildiği haliyle inceleme laboratuvarına taşınması için *Faraday Çantası'*na[6] konulması fiziksel bir önlemdir. İmajı alınmak[7] üzere el konulan

[6] Faraday çantası, cep telefonlarının açık kalması gereken durumlarda operatörle iletişimi engelleyen, ortamda bir sinyal kesici varmış gibi cihazın dış dünya ile bağlantısını kesmeye yarayan özel çantadır (Ekim 2013, 4).

[7] Bu işlem ikinci bölümde anlatılmaktadır.

dijital medyaların sarsıntı sırasında disk yüzeyinin hasar görmemesini ve laboratuvara sağlam ulaştırılmasını teminen, sarsıntıları emecek şekilde imal edilmiş özel kutulara konulması da fiziksel önlemlerin bir diğer örneğidir (Şimşek vd. 2012, 69). Benzer şekilde delillerin inceleneceği laboratuvardaki giriş-çıkışların yetki temelli yapılması, kimlik tanıma sistemleri kullanılması gibi önlemler de fiziksel önlemler arasındadır.

Alınan kopyaların ilk alındığı orijinalliği ile korunması, bütünlüğünün bozulmaması ise dijital önlemlerle sağlanmaktadır (Uzunay ve Koçak 2005, 5). Bu amaçla kullanılan en yaygın yöntem **kriptografik özet** (*hash*) fonksiyonlarıdır (Kruise ve Heiser 2002, 16). Bu fonksiyonlar esasında, kendisine girdi olarak verilen devasa büyüklükte verilere sabit büyüklükte bir çıktı anahtarı üreten bilgisayar yazılımlarıdır. Özet fonksiyonlarının en önemli özelliği ise birebir aynı girdilerin verilmesi halinde hep aynı çıktı anahtarını üretmesidir. Bu ise, birbirinin birebir aynısı olan iki ayrı konumdaki dosyanın esasen hiçbir değişikliğe uğramadığının ve orijinalliğini koruduğunun kanıtıdır (Göksu 2010, 49). Zira bir dosyada yapılacak tek harflik bir değişiklik bile hesaplanan özet değerinin değişmesi için yeterlidir. Özet fonksiyonları veriler üzerinde herhangi bir değişiklik yapılıp yapılmadığı konusunda bilgi sunabildiği için (Özbek 2013, 255) adli bilişim alanında veri bütünlüğünü doğrulamak amacıyla sıkça kullanılmaktadır (Kızılyar 2014, 86).

1.2.3. Analiz Etme

Sadece adli bilişim uzmanları tarafından yapılabilen analiz aşaması, en çok teknik bilgiye ihtiyaç duyulan ve en uzun süren adımdır (Uzunay ve Koçak 2005, 5). Bu aşamada tüm delil kaynakları uygun ortamlarda açılmakta ve -daha önce kopyaları alınmadı ise- birebir kopyalanmaktadır. Kolluk kuvvetleri tarafından genellikle mahkemeye, adli bilişim uzmanına, savcıya ve savunma tarafına verilmek üzere dört adet kopya alınmaktadır (Uzunay ve Koçak 2005, 5). Bu aşamada yapılan tüm analiz çalışmaları orijinal veriler üzerinde değil, kopyalar üzerinde gerçekleştirilmektedir. Analiz çalışması öncelikle kopya içerisindeki tüm dosyaların, inceleme ve yorumlama safhalarını daha kolay ve anlamlı hale getirmek amacıyla çeşitli kıstaslara göre sınıflandırılması ile başlamaktadır (Şimşek vd. 2012, 74).

Sınıflandırma aşamasından sonra inceleme aşamasına geçilmektedir. İnceleme esnasında olayla ilgisi olabilecek dosya içerikleri, resimler, video ve ses kayıtları, gezilen internet siteleri, dosyalara erişim tarihleri, silinmiş dosyalar gibi bilgilerden anlamlı ve bütüncül bir tablo elde edilmeye çalışılmaktadır. Bu esnada yapılan tüm işlemler tek tek kayıt altına alınmakta ve işlemi yapan uzmanların dijital imzaları, çıkarılan tüm belgelere eklenmektedir. Bu süreçte incelemeyi yapan kişinin yaptığı işten dolayı hukuki olarak sorumluluğu bulunmaktadır (Şimşek vd. 2012, 51).

1.2.4. Sunma

Adli bilişim süreçlerinin en son aşaması sunma olarak nitelendirilen raporlama safhasıdır. Bu adım, daha önceki adımlarda yapılan tüm teknik iş ve işlemlerin karar verici mercilerin anlayacağı şekilde yazılı hale getirilmesi ve bir sistematik içerisinde sunulmasını içermektedir. US DOJ'a (2004, 22) göre bir rapor dosyasında raporlamayı yapan birime ait bilgiler, soruşturma veya olay numarası, adli bilişim uzmanına ait bilgiler, başvurana ait bilgiler, kopyaların alınma tarihi, rapor tarihi, incelemeye tabi tutulan cihazların listesi, arama kararına ait bilgiler, incelemeyi başlatan talep ve ilgili yazılar, inceleme esnasında yapılan işlemlerin özeti ve sonuç kısımları bulunmalıdır. Bununla birlikte raporun daha anlaşılır olabilmesi için inceleme yapılan yerlere ilişkin bilgiler, sisteme ait ağ topolojisi, verilerin yedeğinin nasıl alındığına ilişkin bilgilere de ihtiyaç duyulabilmektedir (Şimşek vd. 2012, 78). Bu kapsamda Rehber'de (AK 2013, 174-175) sunulan, bir raporun taşıması gereken temel özellikler şu şekilde sıralanmıştır:

1. Kabul edilebilir deliller ortaya konulmalıdır.
2. Araştırılan olayla doğrudan ilgisi olan deliller ortaya konulmalıdır.
3. Sunulan deliller, hüküm verici heyete dar bir bakış değil toplu bir fotoğraf vermelidir.
4. Deliller hüküm vericiler tarafından değerlendirilirken inandırıcı ve anlaşılır olmalıdır.
5. Delillerin bütünlüğü ve doğrulanmasını sağlamak için kullanılmış olan bütün sistemler ayrıntılı bir şekilde açıklanmalıdır.

1.3. ADLİ BİLİŞİM VE REKABET HUKUKU

Bu bölümde öncelikle rekabet hukuku hakkında genel bilgilere, ardından da adli bilişimin rekabet hukuku ile olan bağlantısı hakkında değerlendirmelere yer verilmektedir.

1.3.1. Genel Olarak Rekabet Hukuku ve 4054 Sayılı Rekabetin Korunması Hakkında Kanun

Rekabet hukuku mal ve hizmet piyasalarında rekabetin korunması amacına yönelik oluşturulmuş kurallar bütünüdür.[8] Rekabet hukuku kurallarında öngörülen yasaklama ve kontrol ile temel olarak, mal ve hizmet piyasalarında kartelleşme ve tekelleşmenin önüne geçilmesi hedeflenmektedir (Sanlı 2013, 200). Ülkemizde rekabet hukuku 4054 sayılı Rekabetin Korunması Hakkında Kanun ile uygulanmaktadır. RKHK'da rekabete aykırılık teşkil eden fiil ve uygulamalar temel olarak RKHK'nın 4. ve 6. maddesinde yer almaktadır. Buna göre teşebbüslerin aralarında anlaşmak veya uyumlu eylemler sergilemek suretiyle bir piyasadaki rekabeti engellemesi ile hâkim durumlarını kötüye kullanmaları RKHK kapsamında ihlal olarak değerlendirilmektedir. Bununla beraber mal ve hizmet piyasalarındaki rekabeti engellemek suretiyle tüketici refahını olumsuz yönde etkileyen karteller "*en ciddi ihlaller*" olarak nitelendirilmekte (OECD 1998, 2) ve dünyadaki rekabet otoritelerinin birinci önceliğini oluşturmaktadır (Monti 2001, 14). Kartel terimi, Rekabet Terimleri Sözlüğü'nde (Sözlük 2014, 130)

> Fiyat tespiti, müşterilerin, sağlayıcıların, bölgelerin ya da ticaret kanallarının paylaşılması, arz miktarının kısıtlanması veya kotalar konması, ihalelerde danışıklı hareket konularında, rakipler arasında gerçekleşen, rekabeti sınırlayıcı anlaşma ve/veya uyumlu eylemler

şeklinde tanımlanmaktadır. Bu anlaşma veya uyumlu eylemler doğrudan müşteri/tüketicilerin zarar görmesine, müşterilerin daima gerekenden daha fazla ücret ödemesine, alternatiflerinin azalmasına ve genellikle de ürün/hizmet kalitesinin düşmesine sebep olmaktadır (Sanlı 2013, 204). Bu çerçevede rekabet hukuku ve Kurum, başta kartellerle mücadele olmak üzere rakipler arası anlaşmaların ve hâkim durumun kötüye kullanılmasının tespiti ve önlenmesi amacına hizmet etmektedir.

[8] http://www.rekabet.gov.tr/tr-TR/Sayfalar/Rekabet-Hukukunun-Esaslari, Erişim Tarihi:18.12.2016.

1.3.2. Adli Bilişimin Rekabet Hukuku İle İlişkisi

Serbest piyasa düzenini korumak amacıyla rekabet hukuku kurallarını uygulamaktan sorumlu rekabet otoritelerinin öncelikli görevi, rekabet ihlallerini delilleriyle birlikte ortaya çıkararak ihlalde bulunan teşebbüslere etkin ve caydırıcı yaptırımlar uygulamak veya uygulanmasını sağlamaktır. Böylece, bir yandan rekabet ihlalinden kaynaklı zararlar bir nebze telafi/tazmin edilmiş olurken, diğer yandan tespit edilme ve yaptırım tehdidi nedeniyle diğer teşebbüslerin kanunu ihlal etme güdülerinin azalması sağlanmış olacaktır.

Rekabet otoritelerinin rekabet ihlallerini tespit edebilmesi ve ihlalleri şüpheye yer bırakmayacak şekilde hukuka uygun delillerle ortaya koyması bazı araçlarla mümkündür. Nitekim Kurum açısından RKHK'nın 15. maddesinde düzenlenen yerinde inceleme imkân ve yetkileri bu araçlardan biridir.[9] Buna göre RKHK'nın 15. maddesinde şu ifadelere yer verilmiştir:

> Kurul, bu Kanun'un kendisine verdiği görevleri yerine getirirken gerekli gördüğü hallerde, teşebbüs ve teşebbüs birliklerinde incelemelerde bulunabilir. Bu amaçla teşebbüslerin veya teşebbüs birliklerinin:
>
> a) Defterlerini, **her türlü evrak ve belgelerini inceleyebilir ve gerekirse suretlerini alabilir**,
>
> b) Belirli konularda yazılı veya sözlü açıklama isteyebilir,
>
> c) Teşebbüslerin her türlü mal varlığına ilişkin mahallinde incelemeler yapabilir.

Görüldüğü gibi mevcut durumda yerinde inceleme esnasında görevli meslek personelleri, teşebbüslerin mal varlığında bulunan **her türlü** evrak, defter vb. üzerinde inceleme yapabilmektedir. Uygulamada ise meslek personeli, teşebbüs yöneticisi veya çalışanlarının bilgisayarlarında var olan dosyaları ve e-postaları basit arama terimleri yardımıyla taramakta ve rekabete aykırı olduğu düşünülen verilerin bir kopyası (sureti) basılı halde elden teslim alınmaktadır. Bu kapsamda yerinde incelemeler esnasında hali

[9] Kartellerin Ortaya Çıkarılması Amacıyla Aktif İşbirliği Yapılmasına Dair Yönetmelik kapsamında tarafların dosyaya sağladığı bilgi ve belgeler ile ihaleye fesat karıştırma gibi adli süreçlerde yasal olarak elde edilen delillerden RKHK kapsamında ihlal niteliğini haiz olanlar da bu araçlardandır. Ancak uygulamada Rekabet Kurulu (Kurul) kararlarına konu delillerin birçoğunun meslek personelinin yerinde incelemelerde elde ettiği delillerden oluştuğu görülmektedir.

hazırda uygulanmakta olan çeşitli pratikler üzerinden adli bilişimin rekabet hukukunda delil elde etme imkânları üzerindeki faydalarından bahsedilecektir.

Teşebbüsler; gerek tecrübeleri dolayısıyla (daha önce incelemeye tabi olmuşsa) gerekse başka şekilde bilgi sahibi olmak yoluyla Kurumun geleneksel yöntemlerle delil bulma imkânını ortadan kaldıracak önlemleri kolaylıkla alabilmektedir (Yalçınkaya, 2015, 21). Bu bakımdan 2006 yılında Türkiye Büyük Millet Meclisi'nde (TBMM) bir muhalefet partisi milletvekili tarafından, hükümete tevcih edilen 7/11885 sayılı soru önergesine ilişkin Kurum cevabında belirtildiği üzere:

> Özellikle çimento gibi defalarca rekabet soruşturmalarına maruz kalmış sektörlerde, belge ve bilgiye ulaşmak, teşebbüslerin bu tür inceleme ve araştırmalara hazırlıklı olmaları nedeniyle imkânsız hale gelmektedir.[10]

Teşebbüse intikal edilen zaman ile incelemeye başlanan zaman arasında geçen sürede veya inceleme esnasında delil değeri taşıyan dijital veriler teşebbüs yetkilileri tarafından yok edilebilmektedir. Nitekim *TTNET*[11] kararında, teşebbüste gerçekleştirilen yerinde inceleme esnasında, incelenen bilgisayardaki birtakım dosyaların silindiği gözlemlenmiş ve ilgili teşebbüse yerinde incelemeyi engelleme sebebiyle idari para cezası uygulanmıştır[12]. Anılan karara İdare Mahkemesi[13] nezdinde yapılan itirazda, yerinde incelemenin engellenmesi hususunun söz konusu olmadığı ve uygulanan idari para cezasının Anayasa'ya aykırılığı iddialarında bulunulmuştur. Buna karşılık İdare Mahkemesi "*15. maddenin getirilme amacının, mevcut evrak, doküman ve belgelere* ***o anda ve mevcut haliyle ulaşmak*** *ve bu belgeler ışığında bir sonuca varılmasını sağlamak*" olduğunu ifade ederek, itiraz başvurusunu reddetmiştir. Mezkûr karara konu olan olayda, yerinde incelemeyi gerçekleştiren meslek personelinin dikkati sayesinde ortaya çıkarılan dosya silme işleminin, tüm incelemelerde aynı şekilde tespit edilmesi mümkün gözükmemektedir. Ayrıca yerinde incelemelerdeki zaman darlığı dikkate alındığında bir günde bile yüzlerce yazışmanın (e-posta veya dijital belge gönderiminin)

[10] Rekabet Kurumu 8. Yıllık Rapor (2006 Yılı), s.182.
[11] Kurul'un 8.07.2013 tarihli,13-46/601-M sayılı kararı.
[12] Benzer durum için bkz: Kurul'un 05.08.2009 tarihli, 09-34/837-M sayılı *Koçak Petrol* kararı ve bu karara yönelik Danıştay 13. Dairesi'nin 26.03.2013 tarihli, E: 2009/5890, K: 2013/847 kararı.
[13] Ankara 13. İdare Mahkemesi E.2013/1598, K.2014/1495.

gerçekleştirildiği teşebbüslerde, tek tek bütün belgeleri ve/veya e-postaları inceleyip rekabet ihlali oluşturabilecek delilleri tespit etmenin güçlüğü açıktır.

Yerinde incelemeler esnasında gerçekleştirilen yüzeysel (klasik) arama araçları ile bilgisayarlar üzerinde yapılan kavramsal aramalar, adli bilişim araçları ile yapılan aramalara nazaran son derece sınırlıdır. Bu nedenle bu tür yüzeysel ve kavramsal aramalarla delil elde etme imkânı da adli bilişim uygulamalarına oranla kısıtlı kalmaktadır. Ancak *Nuix, EnCase* gibi birtakım adli bilişim programları silinmiş veya gizlenmiş verileri de kapsayacak şekilde arama yapabilmekte (Güllüce ve Benzer 2015, 208) ve kavramsal aramayla eş anlamlı kelimeler veya şifreli yazışmalar ortaya çıkarılabilmektedir (Beebe ve Clark 2007, 49). Ayrıca verilerin gizlenmesi veya bir cihazın şifresinin bilinememesi sebebiyle incelenememesi gibi durumlarda adli bilişim araçlarıyla inceleme yapabilmek mümkün hale gelebilmektedir (Yalçınkaya 2015, 22-23).

Yukarıda yer verilen açıklamalar dikkate alındığında, çimento sektöründeki gibi zaman içerisinde birçok soruşturmaya muhatap olan teşebbüslerde gerçekleştirilen yerinde incelemelerde, klasik delil araştırma yöntemleri ile delil elde etmenin gün geçtikçe zorlaştığı görülmektedir. Bununla birlikte bilgisayarlara, gerek inceleme başlayana kadar gerekse inceleme esnasında müdahale edilip edilmediğinin, aranan delillerin ortadan kaldırılıp kaldırılmadığının tespiti adli bilişim uygulamaları ile sağlanabilmektedir. Nitekim yukarıda bahsi geçen TBMM soru önergesine ilişkin Kurum cevabında şu açıklamalara yer verilmiştir:

> Kartelleri ortaya çıkarabilmek için ABD, İngiltere gibi ülkelerde **telefon görüşmelerinin dinlenmesi, e-maillerinin kontrolü, gizli kamera kullanılması** gibi ceza hukukunun araçları eskiden beri kullanılmakta ya da kullanılmaya başlanılmaktadır. Rekabet hukukunda en etkili delil elde etme yönteminin, söz konusu yetkilerin kullanılması olduğu kabul edilmelidir. Rekabet otoritelerinin kuruluş amaçlarından olan kartelleşme ile mücadele için modern rekabet kurumlarının kullandığı yetkilere sahip olması gerekmektedir[14].

Yukarıdaki ifadelerden de anlaşılacağı gibi, bazı rekabet otoritelerinin ihlalleri ortaya çıkarmak adına kullandığı araçlardan biri de adli bilişim teknik ve

[14] Rekabet Kurumu 8. Yıllık Rapor (2006 Yılı), s.182.

uygulamalarıdır. Adli bilişim uygulamaları sayesinde dijital ortamlarda var olan ve özellikle kartel tipi ihlallere delil teşkil edebilecek verilerin muhafazası ve şüpheye yer bırakmayacak şekilde ortaya çıkarılması daha da kolaylaşmaktadır. Rekabet ihlallerine yönelik delillerin daha etkin bir biçimde ortaya çıkarılıyor olması teşebbüsler nezdinde caydırıcılığı artıracağından teşebbüslerin ihlal konusundaki niyetlerini ortadan kaldırabilecektir. Bu bağlamda Kurum tarafından yayımlanan 2014-2018 dönemine ait Stratejik Plan'da yerinde inceleme yetkilerinin adli bilişim konularında genişletilmesi/belirginleşmesi gerektiği ifade edilmekte ve:

> Ekonomik ve sosyal hayatta gerçekleşen teknolojik gelişmeler Kurum'un asli misyonunu yerine getirmek üzere icra ettiği faaliyetlerden birisi olan denetim faaliyetinin etkinliğini azaltma potansiyelini barındırmaktadır. Çünkü teknolojik gelişmelerin teşebbüslere delillerin gizlenmesi yönünde sunduğu avantajlar, rekabet ihlallerine ilişkin inceleme, araştırma ve soruşturmalarda delil temini konusunda birtakım zorlukların yaşanmasına neden olmaktadır. Bu tehdidin bertaraf edilmesine yönelik olarak, bir yandan denetim faaliyetinin daha etkin sürdürülmesine olanak verecek bir örgütsel yapılanmaya gidilmesi, diğer yandan da **adli bilişim imkânlarından daha fazla yararlanmasını sağlayacak altyapının oluşturulması** gerekmektedir.

değerlendirmelerine yer verilmektedir. Bu kapsamda Kurum bünyesinde yapılan yerinde incelemelerde uzman bilişim personeline duyulan ihtiyaç (Kekevi 2008, 117) nedeniyle Meslek Personeli Yönetmeliği'nde değişiklik yapılarak bilişim konusunda uzman meslek personeli istihdamına başlanmıştır.

Sonuç olarak Kurum'un etkinliğinin artırılması ve rekabet hukuku ile amaçlanan hedeflere ulaşılabilmesinde adli bilişim araçlarının önemli katkıları olacağı düşünülmektedir. Bu doğrultuda kullanılan adli bilişim araçları hakkında teknik bilgilere ikinci bölümde yer verilmektedir.

BÖLÜM 2

ADLİ BİLİŞİMİN TEKNİK BOYUTU

Adli bilişim çoğunlukla yok edilen veya yok edildiği sanılan veriler üzerinden delil elde etmek ile ilgilenmektedir. Bu kapsamda dijital ortamda yok edildiği zannedilen birçok verinin esasen yok olmadığını, yalnızca uzman kişiler tarafından ortaya çıkarılabilecek şekilde gizlendiğini söylemek mümkündür. Aynı şekilde dijital ortamda saklanan verilerin, diğer veri türlerine göre çok daha kolay değiştirilebileceği de bilinen bir gerçektir (AK 2013, 11). Bu değişiklik, sistemi kullanan kişi tarafından bilerek ve isteyerek yapılabileceği gibi, zaman zaman işletim sistemi rutinleri içerisinde kullanıcının kontrolü dışında da gerçekleşebilmektedir. Böylesi bir durumda adli bilişimin yeteneklerinden faydalanarak olayın açığa çıkarılması mümkündür. Bu kapsamda bu bölümde adli bilişimin delil bulmadaki önemi vurgulanmaktadır.

2.1. DİJİTAL DELİL KAYNAKLARI

Dijital delillerin bulunduğu kaynaklar çok çeşitlilik göstermekle birlikte, "bilgisayar sistemleri" ve "ağ sistemleri" olarak ikiye ayrılmaktadır (AK 2013, 16). Bilgisayar sistemleri tanımıyla kastedilen, içerisinde farklı formatlarda veri taşıyan tüm dijital cihazlardır (AK 2013, 16). Ağ sistemleri terimi ise, çeşitli yönlerde veri taşıyan tüm iletişim hatlarını kapsamaktadır (AK 2013, 27). Konsey'in yayınladığı Rehber'de dijital delil elde edilebilecek cihazlar aşağıdaki şekilde sıralanmıştır (AK 2013, 16-27):

1. Bilgisayarlar: Masaüstü bilgisayarlar, dizüstü bilgisayarlar, PDA'lar, ana sistem bilgisayarları, sunucular,

2. Saklama üniteleri: Sabit diskler, taşınabilir diskler, disketler, CD'ler, DVD'ler, blu-ray diskler, hafıza kartları, tape diskleri, yazıcı, tarayıcı gibi yardımcı cihazlar,
3. Mobil telefonlar,
4. Multimedya cihazları: Dijital kameralar, dijital kayıt cihazları, VHS, CCTV kameralar, MP3 çalarlar, MP4 çalarlar,
5. Video oyun konsolları.

Ağ sistemleri olarak tanımlanan delil kaynaklarına ise, internet, yerel alan ağı denilen LAN (*Local Area Network*) ve kablosuz ağ sistemleri örnek verilebilir.

Bu bilgiler ışığında adli bilişim alanlarının, delil kaynağına göre çeşitlilik gösterdiğini söylemek mümkündür. Bu itibarla, örneğin bir cep telefonunun hafızasındaki bilgilere çeşitli teknikler yoluyla ulaşmak ile cep telefonunun iletişim kurduğu diğer cihazları tespit etmek iki farklı adli bilişim alanıdır (Daniel ve Daniel 2011, 17-23). Çalışmanın ilerleyen bölümlerinde her iki adli bilişim alanına ilişkin detaylı açıklamalara yer verilmektedir.

Yukarıda sayılan delil kaynaklarından, rekabet ihlali incelemeleri kapsamında dünyada en çok incelemeye maruz kalanlar şüphesiz ki, bilgisayarlar, saklama üniteleri ve mobil cihazlardır. Bu bağlamda aşağıda rekabet ihlali incelemeleri kapsamında en çok incelenen cihazların altyapıları, adli bilişim alanındaki önemleri ve çalışma usulleri hakkında bilgi verilmektedir.[15]

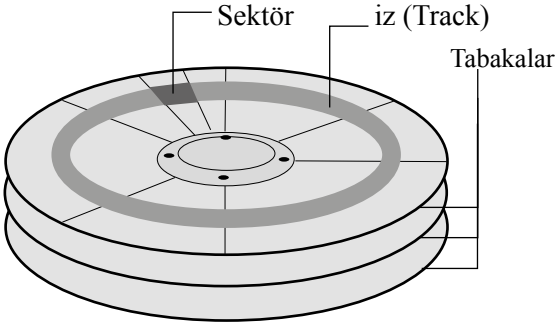
2.1.1. Sabit Disk Alanları Ve Sterilizasyon (*Wipe*) İşlemi

Adli bilişimde uzmanlaşabilmek için bilgisayar altyapısını ve özellikle saklama ünitelerinin yapılanmasını bilmek oldukça önemlidir (Şengül vd. 2014, 95). Bir cihazdaki verileri çeşitli formatlarda saklayan ve cihaz kapatıldığında bile kaybetmeyen donanımlara *sabit disk* denilmektedir. Günümüzde sabit diskler; cep telefonları, mp3 çalarlar ve dijital fotoğraf makineleri gibi aygıtlarda kullanılmaktadır (Zubaroğlu 2007,

[15] "*2.1. Dijital Delil Kaynakları*" başlıklı bölümde maddeler halinde verilen *bilgisayarlar, mobil telefonlar, multimedya cihazları ve video oyun konsolları*ndan elde edilen deliller esasında ilgili cihazların saklama birimlerinde tutulan verilerden çıkarılmaktadır. Bu sebeple ilgili bölümde daha çok saklama birimleri özelinde sabit disklere ilişkin adli bilişim tekniklerinden bahsedilmektedir.

1). Elektromekanik yapıda olan sabit diskler bilgiyi manyetik olarak saklamaktadır. Basit bir sabit disk yapısı aşağıda görüldüğü gibidir:

Şekil 1: Sabit Disk Bölümleri (Zubaroğlu 2007,1)



Şekil 1'de görüldüğü gibi bir sabit diskte birden çok tabaka bulunmaktadır. Her bir tabaka izlerden ve her bir iz (*track*) de sektörlerden oluşmaktadır. İşletim sistemleri, sektörleri, küme *(cluster)* denilen gruplu yapılar halinde topluca işlemektedir. Örneğin işletim sistemi bir diske yeni bir dosya yazmak istediğinde dosya boyutuna göre uygun miktarda kümeyi bu işe tahsis etmekte ve sıradaki bölüme ilgili dosyayı yazmaktadır. Her sektörünün boyutu 512 bayt olan bir işletim sistemi 4 sektörü bir küme olarak gruplamışsa, 2000 bayt uzunluğundaki bir dosyayı tek kümeye yazabilir. Her bir küme boyutu 512x4 = 2048 bayt olan bu işletim sisteminin, dosya için ayırdığı 2000 bayt dışındaki bölümü kullanılmamıştır. Örnekteki 2000 baytlık dosya, kullanıcı tarafından silinip; yerine 1500 baytlık başka bir dosya yazıldığında, arkada kalan 500 baytlık bölüme "*artık alan*" (Tok 2013, 27) denilmekte ve adli analizler esnasında ulaşılabilmektedir.[16]

Adli analiz açısından önemli olan bir diğer sabit disk bölümü ise tahsis edilmemiş alanları içine alan bölümdür (Balı 2015b, 1). Her işletim sisteminde dosyalara daha kolay erişebilmek için çeşitli dosya tanım tabloları tutulmaktadır. İşletim sistemi, yeni bir dosya oluşturulduğunda bu tabloya yeni bir kayıt atmakta ve ilgili dosyanın sabit diskteki yerini tabloya yazmaktadır. Böylece dosyaya yeniden ulaşılmak istendiğinde tüm diskte arama yapmak yerine, tablodan dosyanın kısa yoluna ulaşılabilmektedir (Tanenbaum 2009, 290-321). Ne var ki dosyanın silinmesi durumu söz konusu olduğunda esasen sabit diskten dosyanın kendisi değil, tanım tablosundaki erişim bilgileri silinmekte ve

[16] Slack Space, http://www.computerhope.com/jargon/s/slack-space.htm, Erişim Tarihi:10.02.2016.

sabit diskteki yeri "*tahsis edilmemiş alan*" olarak işaretlenmektedir. Bu durum kuşkusuz sabit disklerin daha hızlı çalışması için seçilmiş bir yöntem olmakla birlikte, adli bilişim açısından uzmanlara oldukça kolaylık sağlamaktadır. Çünkü dosyanın disk üzerinden fiziksel olarak silinmiyor olması, kullanıcı tarafından silindiği zannedilen birçok delile adli bilişim teknikleriyle erişmeye imkân tanımaktadır (Çakır ve Kılıç 2013, 31).

Sabit diskte saklanan bilgilerin en düşük düzeyde sıfır ve bir olmak üzere iki farklı değeri bulunmaktadır. Her bir küme, on binlerce sıfır ve birin birleşerek anlamlı kelime setleri oluşturmasından meydana gelmektedir. Diskten silindiği zannedilen verinin gerçekten diskten yok edilebilmesi için "*wipe*" adı verilen bir yöntem kullanılmaktadır. *Wipe* ifadesinin Türkçe karşılığı "*sterilize etmek*"tir.[17] Bir saklama ünitesinden veriyi sterilize etmek, verinin bilinen hiçbir teknikle geri getirilemeyecek şekilde silinmesi anlamına gelmektedir. Sterilize edilen bir dosyada, verilerin yerine yeni ve anlamsız sıfır ve birler yazılarak geçmiş dosyaya ait tüm bilgilerin geri döndürülemez şekilde yok edilmesi sağlanmış olur. Sterilize edilmiş bir diskten veri kurtarma olasılığı düştüğü için, bu verilere adli bilişim analizleri sırasında ulaşmanın oldukça zor olduğu belirtilmektedir (Balı 2015a, 1).

Dijital veriler sabit diskler dışında CD, DVD gibi optik disklerde ve SSD diskler gibi *dijital yongalar* üzerinde saklanabilmektedir (Özbek 2013, 257). Veri depolama ve okuma/yazma ömrü açısından bakıldığında sabit diskler diğer iki veri saklama ünitesine göre daha yaygın bir kullanıma sahiptir (Özbek 2013, 257). Bu sebeple bu çalışmada optik diskler ve dijital yongalı saklama üniteleri hakkında detaylı bilgi verilmemiştir. Her üç saklama türünde de saklanan veriler cihazda meydana gelen bir güç kesintisinde herhangi bir kayba uğramayacak şekilde tasarlanmıştır. Bununla birlikte dijital cihazlarda, meydana gelen bir güç kesintisinde kaybedilebilecek veriler de bulunmaktadır. Takip eden bölümde uçucu veri olarak isimlendirilen bu verilerin özellikleri anlatılmaktadır.

[17] 1/2003 Sayılı Tüzüğün 20. Maddesinin 4. Fıkrası Uyarınca Gerçekleştirilen İncelemelere İlişkin Açıklayıcı Not, s.3.

2.1.2. Uçucu Veriler

Olay yeri müdahalesine veya incelemeye gidildiğinde imajı alınacak olan cihazın, ilk müdahale esnasında açık veya kapalı durumda bulunması, bundan sonra yapılacak işlemlerin mahiyetini belirlemektedir (Şimşek vd. 2012, 54-55). Açık halde elde edilmiş bir cihazın kapatılması veya gücünün kesilmesi, içerisinde *uçucu veri* kavramıyla ifade edilen delillerin kaybolmasına sebep olabilmektedir. Cihaz açıkken korunan uçucu verilere cihaz kapatıldıktan sonra yeniden erişme imkânı olmadığı için, inceleme esnasında öncelikle uçucu verilerin saklandığı ünite olan *geçici belleğin imajının alınması* esastır (Süzen vd. 2016,1). Adli analiz açısından önem teşkil eden geçici bellek, cihazın kullandığı ağ bağlantıları, cihaza oturum açmış kullanıcı bilgileri, işletim sistemi üzerinde hâlihazırda çalışan işlemler, açık bırakılmış dosyalar, ağ yapılandırmaları, işletim sisteminin saat ve bölge bilgileri gibi çok önemli olabilecek bilgiler içermektedir (Kent vd. 2006, 5-8).

Uçucu verilerin imajını almak için kullanılan araçlardan bazıları *Belkasoft Live RAM Capturer, Encase Portable, Live Response,*[18] *MoonSols Window Memory Toolkit*'dir.

2.2. DİJİTAL DELİL ELDE ETME YÖNTEMLERİ

Bu bölümde, adli bilişim araçları hakkında bilgi verilmekte olup ilerleyen aşamada, incelemeler esnasında delilin hangi yöntemlerle toplandığı konusuna değinilmektedir.

Delil elde etme yöntemlerine geçmeden önce delilleri elde etmede kullanılan araçlara kısaca değinilmesinin isabetli olacağı düşünülmektedir. Adli bilişim araçları, ilgili kişilere ait cihazlarda saklanan ve dijital ortamlarda bulunan delillerin tespit edilmesine yardımcı olan yazılımsal ve/veya donanımsal araç veya araçlar bütünü olarak tanımlanmaktadır (Özdemir 2013, 1).

[18] Encase Portable ve Live Response USB cihazına entegre edilmiş taşınabilir bir adli bilişim yazılımıdır. Yani olay yeri inceleme esnasında USB disk ilgili kişinin bilgisayarına bağlanarak hızlı bir şekilde uçucu verilerin kopyalarını hedefteki bir dosyaya almayı sağlamaktadır. https://www2.guidancesoftware.com/products/Pages/encase-portable/overview.aspx, Erişim Tarihi:07.03.2016.

Özdemir (2013, 1)'in tanımından anlaşılacağı üzere adli bilişim araçları donanımsal ve yazılımsal araçlar olarak ikiye ayrılmaktadır. Bu araçlar dijital veriyi toplamak, işlemek ve analiz etmek gibi çeşitli amaçlara hizmet etmektedir. Yazılımsal adli bilişim araçları ICN (2014, 15) tarafından; başlatma yazılımları, bilgisayar adli bilişim yazılımları, yazılımsal yazma koruyucular [19] ve çoğaltıcılar, kriptografik özet yazılımları, analiz yazılımları, birebir kopyalama yazılımları,[20] akıllı analiz yazılımları, anti-virüs yazılımları, genel uygulama yazılımları, dava destek yazılımları ve yedekleme yazılımları şeklinde gruplandırılmıştır.

Donanımsal adli bilişim araçları ise; arama kutusu,[21] köprüler,[22] kamera,[23] mobil cihaz analiz araçları,[24] sürücü kopyalayıcıları,[25] sürücü temizleyiciler,[26] dizüstü bilgisayarlar, saklama ortamları (CD-ROM, disket, DVD, sabit disk, USB disk vb.), ağ ekipmanları (kablolar, kartlar vb.), veri depolama ağı,[27] PC kartları,[28] sunucu, takım çantası ve donanımsal yazma koruyucular şeklinde gruplandırılabilir (ICN 2014, 16).

2.2.1. İmaj Alma

Adli bilişimde delillerin yasal yollarla ve doğru bir formatta elde edilmiş olması, incelemeye konu olan dosyanın sonraki aşamaları açısından çok önemlidir (Henkoğlu

[19] Yazma koruyucular (*write blockers*) yanlışlıkla sürücü içeriğine zarar verme olasılığı yaratmadan bir sürücü hakkında bilgi edinilmesini veya sürücüye erişilmesini sağlayan araçlardır. (Lyle 2006, 1)

[20] Bu ifade İngilizce "*bit-stream imaging software*"'den çevrilmiştir. Bu yazılımlar sürücü üzerindeki tüm alanların orijinal hali ile kopyalanmasını sağlamaktadır. Bu yöntem ile, sürücüden daha önce silindiği zannedilen dosyalar, üzerine yeni bir bilgi yazılmamış ise kurtarılabilir ve incelenebilir. Bu bakımdan birebir kopyalama yöntemi adli bilişim incelemelerinde çok önemli bir yere sahiptir (Bellovin vd. 2015, 5).

[21] İncelemeye giderken götürülen donanımsal ekipmanı taşımak için kullanılan çantaya "arama kutusu" denilmektedir (ICN 2014,16).

[22] İncelenecek veya kopyası alınacak olan sürücüleri bir dizüstü veya masaüstü bilgisayara bağlamayı sağlayan bağlantı aparatlarının ve ara yüzlerinin tamamına "köprü" denilmektedir. http://searchsecurity.techtarget.com/definition/bridge, Erişim Tarihi:10.02.2016.

[23] Kameralar, inceleme yapılan yer ile ilgili detaylı fotoğraf ve video çekmek için kullanılmaktadır.

[24] Sim kart benzeri cihazların içerisindeki bilgileri doğrudan okuyup analiz etmeye yarayan araçlardır (ICN 2014, 16).

[25] Sürücü kopyalayıcılar, bir veya birden fazla diskten aynı anda kopya çıkarılmak istendiğinde kullanılan çoklu ortam kopyalayıcılardır (ICN 2014, 16).

[26] Sürücü temizleyiciler *drive wiper* olarak da bilinen, bir hedef sürücünün tüm bitlerini sıfıra ayarlamak suretiyle temizlenmesi işlemini gerçekleştiren cihazlardır (Balı 2015a, 1).

[27] Veri depolama ağı analiz yapılacak yerdeki kişilerin dijital bilgilere kolaylıkla ulaşabilmesi için oluşturulmuş bir paylaşım platformudur (ICN 2014, 16).

[28] PC kartları bir dizüstü bilgisayara farklı cihazların bağlanmasını sağlayan ara bağlantı üniteleridir (ICN 2014, 6).

2014, 49). Bu kapsamda, bilişim sistemleri yoluyla gerçekleştirilen suçların konu olduğu olaylarda, sistemlerden elde edilecek verilerin *doğruluğunun, bütünlüğünün ve inkâr edilemezliğinin* temin edilmesi gerekmektedir (Uzunay ve Koçak 2005, 3). Tüm bu özellikleri eksiksiz bir şekilde sağlayabilmek için geliştirilmiş veri kopyalama sistemine ***imaj alma veya birebir kopyalama işlemi*** denilmektedir (Berber 2015, 1). *Adlî imaj* olarak da adlandırılan bu işlem, silinmiş, deforme edilmiş, değiştirilmiş her türlü veriye ulaşma imkânı tanıması açısından önemlidir (Dülger ve Modoğlu 2013, 116). İmaj alma işlemi, bu amaca hizmet eden özel donanımlar ve yazılımlar yardımıyla orijinal medyada bulunan tüm bilgilerin aynen yeni bir ortama kopyalanması şeklinde icra edilmektedir (Aydoğan 2009, 35). Bir imaj alma aracında bulunması gereken minimum gereksinimler aşağıda listelenmiştir (Lyle 2003, 3):

- Orijinal disk ve bölümlerinin bit dizisi şeklinde birebir kopyasını alabilmeli,
- Orijinal diskte hiçbir şekilde değişiklik yapmamalı,
- Alınan yeni imajın bütünlüğünü doğrulayacak mekanizmalar içermeli,
- İmaj alma esnasında ortaya çıkan hataların kaydını tutmalı.

Bilgisayar, bilgisayar programları ve kayıtlarından elde edilecek delillerin kolaylıkla değiştirilebileceği gerçeği göz önünde bulundurularak, kopyalama işleminin bu konuda uzman personel ve ekipman[29] ile yapılması oldukça önemlidir. Zira kopyalama işlemi esnasında adli bilişim esaslarına uyulmaması, elde edilen delili hukuka aykırı delil haline dönüştürebilmektedir (Sarsıkoğlu 2015, 449).

İmaj alma işlemi, alınan imajın türüne göre mantıksal imaj alma ve fiziksel imaj alma olarak ikiye ayrılmaktadır. Mantıksal imaj, saklama ünitesinin tamamının değil, sadece dosya sistemi katmanı bazında bölümlerinin imajının alınması işlemine verilen addır (Öztürkci 2014, 1). Sonuca hızlı ulaşmanın gerektiği durumlarda kullanılan mantıksal imaj yönteminde, saklama ünitesinde kullanıcının gördüğü dosyalar haricindeki dosyalara ulaşmak mümkün değildir. Fiziksel imaj ise saklama ünitesinin tamamının bit seviyesinde kopyalanması anlamına gelmektedir.[30] Fiziksel imaj almada

[29] Uzman ekipmandan kasıt, dünyadaki adli bilişim otoriteleri tarafından kabul gören ve kullanılan tüm donanım ve yazılımlardır. Bunlara *EnCase, CelleBrite, Nuix* yazılımları örnek gösterilebilir.
[30] Fiziksel İmaj, http://www.kripteksforensic.com/tr/adli-bilisim/fiziksel-imaj, Erişim Tarihi:13.01.2016.

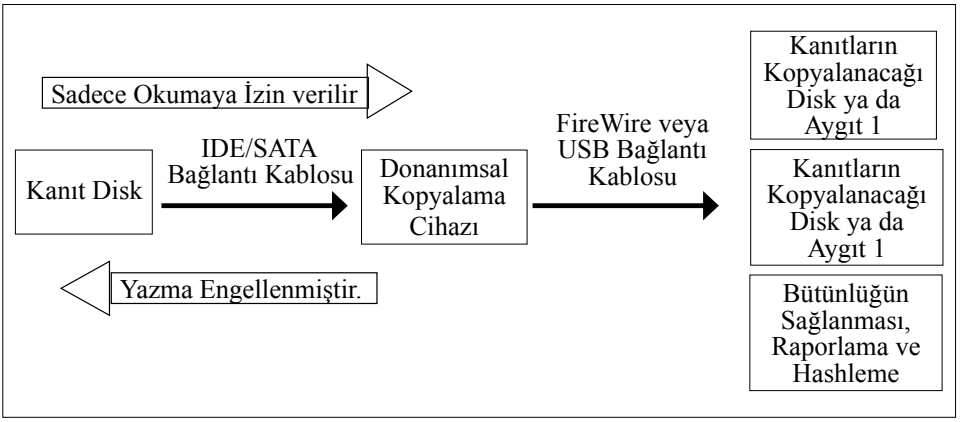
elde edilecek delil çeşitliliği daha fazla iken, adli bilişim uzmanlarının imaj üzerinde analiz yapması daha uzun sürmektedir.[31]

Kullanılan aracın cinsine göre ise imaj alma işlemi donanımsal ve yazılımsal imaj alma olarak ikiye ayrılmaktadır. Ancak alınan kopyanın geçerli bir imaj olabilmesi için sistem üzerindeki verilerin bit seviyesinde yansısının alınması, yani sabit disk düzeyinde kopyalanması gerekmektedir. Nitekim bit seviyesinde kopyalama yapabildiği, daha güvenli ve hızlı olduğu için donanımsal araçlar yazılımsal araçlara oranla daha çok tercih edilmektedir (Bostancı ve Benzer 2015, 1214).

Donanımsal imaj alma araçları, orijinal medyaya fiziksel veri bağlantı kablosu aracılığıyla bağlanarak, kendi içinde gömülü halde gelen işletim sistemine entegre edilmiş imaj alma yazılımı marifetiyle kaynaktaki medyanın birebir kopyasını almaktadır. Bu işlem gerçekleştirilirken kaynak medya üzerinde herhangi bir değişiklik yapılmamasını temin eden mekanizmaya "**yazma koruma** (*write block*)" denmektedir (NIST 2004, 1-2). Bu özellik sayesinde kaynak medyadaki veriler yalnızca okuma amaçlı açılmak suretiyle hedefteki medyaya aktarılır. Donanımsal imaj alma araçlarına örnek olarak *Tableau TD2* ve *TD3 Forensic Kit, Digital Intelligence, Data Copy King, Image MASSter* ve *MyKey* gösterilebilir. Bu araçların en önemli avantajları çoğu zaman hızlı ve pratik olmayı gerektiren olay yerinde, herhangi bir bilgisayara ihtiyaç duymadan hızlı bir şekilde kopyalama yapmaya imkân tanımaları, kolaylıkla taşınabilmeleri ve herhangi bir ek program yüklenmesini gerektirmemeleridir (Bostancı ve Benzer 2015, 1216). Bahsedilen bu hususlara ilişkin Şekil 2'de donanımsal imaj alma araçlarının örnek bağlantısı gösterilmiştir:

[31] Logical Imaging, https://www.cru-inc.com/data-protection-topics/logical-imaging, Erişim Tarihi: 03.02.2016.

Şekil 2: Örnek Bir Donanımsal Kopyalama Cihazı Bağlantısı (Kleiman vd. 2014, 8)



Şekil 3'te ise *Tableau* marka bir cihazla yapılan gerçek bir imaj alma işlemi örnek bağlantı şekilleriyle birlikte gösterilmektedir. Burada dikkat çeken husus kaynak verinin birden fazla cihaza kopyalanabiliyor olmasıdır. Bu özellik adli bilişim uzmanlarına, olay yerinde aynı cihaza ait iki kopya almayı, böylece kopyalardan birinin fiziksel olarak zarar görmesi durumunda diğerinden faydalanmayı sağlamaktadır.

Şekil 3: Tableau Marka Bir Cihazla Gerçekleştirilen İmaj Alma İşlemi[32]

[32] Kaynak: https://www2.guidancesoftware.com/products/Pages/tableau/products/forensic-duplicators/td2u.aspx, Erişim Tarihi:07.03.2016.

Yazılımsal imaj alma işlemleri ise bir bilgisayarın ilgili *port*una kaynak medyanın bağlanması suretiyle yapılmaktadır. Bu araçlar kaynak medyaya hiçbir veri yazmamaktadır ancak yazılımsal imaj alma araçları bazı korsan yazılımlar vasıtasıyla *bypass*[33] edilebilmektedir. Bu sebeple şayet imkân var ise imaj alma esnasında her zaman donanımsal araçların kullanılması önerilmektedir (Bostancı ve Benzer 2015, 1217). Yazılımsal imaj alma araçlarına *Forensic Explorer*, *FTK Imager, EnCase, Winimage, OSFClone* örnek olarak gösterilebilir.

2.2.2. Mobil Cihazlardan Veri Elde Etme

Son yıllarda, mobil cihazların kullanım kolaylığı ve sundukları çözümlerin farklı özellikleri nedeniyle, geleneksel masaüstü sistemlerden mobil cihazlara doğru geçiş hızlanmış ve mobil cihazların kullanımı yaygınlaşmıştır (Ekim 2013, 1). Ayrıca mobil cihazların artan veri saklama kapasiteleri ile bir bilgisayarda saklanabilecek neredeyse tüm verileri artık mobil cihazlarda saklamak mümkün hale gelmiştir. Bu sebeplerle günümüzde birçok birey işlemlerini masaüstü cihazlar yerine mobil cihazlar ile gerçekleştirmeye başlamıştır. Bu durum suç istatistiklerine de yansımıştır. Günümüzde işlenen suçların %70'den fazlasında mobil cihazlar, özellikle de cep telefonları aktif rol almaktadır (Ekim 2013, 1). Bu bağlamda, bir suç veya ihlalin tespitinde mobil cihazlarda adli analizler yapmak önemli bir adım haline gelmiştir.

Eski nesil cep telefonlarından kişinin rehberi, kısa mesajları, multimedya mesajları, gelen giden ve cevapsız aramaları, notları ve takvimi gibi sınırlı sayıda bilgi elde edilirken; yeni nesil cep telefonlarında yukarıdaki bilgilere ek olarak video, resim, ses, telefonun konum bilgisi, fotoğrafın hangi tarihte, hangi makine ile ve hangi konumda çekildiği bilgisi[34], e-postalar, internet geçmişi, internet yazışmaları ve uygulama bilgileri elde edilebilmektedir (Ayers vd. 2013, 51). Tüm bu bilgileri elde

[33] Bir programı *bypass* etmek, yazılımın normal akışını bozacak şekilde araya çeşitli kod parçaları eklemek suretiyle yazılımı başka amaçlara hizmet eder hale getirmektir. Bir adli bilişim yazılımının bypass edilmesi delillerin değiştirilebilmesine bile imkân verebilmektedir. IOS işletim sistemli bir cihazın bypass edilmesine ilişkin örnek için bkz: http://www.oxygen-forensic.com/download/articles/How%20to%20bypass%20iOS%20lockscreen%20protection.pdf, Erişim Tarihi:03.02.2016.

[34] Tüm bu bilgilerin saklandığı bilgi setine *metaveri* adı verilmektedir. Metaveri bir dosyaya ait, dosyanın hangi tarihte oluşturulduğu, boyutunun ne olduğu, dosyaya en son ne zaman erişildiği vb. bilgilerin saklandığı bölümdür. Metaveri bilgisi her dosya türüne göre farklılık göstermektedir. Örneğin bir fotoğraf dosyasında, fotoğrafın çözünürlüğü, hangi cihazla çekildiği gibi bilgilere de metaveri içinden erişmek mümkündür (TÜİK 2011, 33).

etmek ve hukukun kullanımına sunmak için yapılan işlemlere ***mobil cihaz adli bilişimi*** denilmektedir (Özen ve Özocak 2015, 48).

Mobil cihazlarda gerçekleştirilecek bir adli bilişim incelemesi, sabit disklerde yapılan incelemelerle kıyaslandığında görece daha meşakkatlidir. Bunun en önemli sebebi gelişen teknoloji ile birlikte her geçen gün piyasaya sürülen yüzlerce marka ve modeldeki cihazın adli bilişim araçları tarafından her zaman doğru şekilde okunamamasıdır (Sağıroğlu ve Karaman 2012, 63). Bu sebeple mobil cihaz incelemeleri konusunda adli bilişim alanında bir ihtisaslaşma söz konusu olmuş ve sadece mobil cihaz incelemeleri yapılabilmesi için özel araçlar geliştirilmiştir (Ekim 2013, 2).

Bir mobil cihaz incelemesinde deliller cihazın dâhili hafıza kartında, harici hafıza kartında ve sim kartında bulunabilmektedir. Sim kartlardan genellikle GSM ağ verileri (en son bulunulan konum, en son sinyal alınan GSM baz istasyonu vb.), kullanıcının cihaz hafızasını kullanma tercihine bağlı olarak kişi rehberi, silinmiş ve silinmemiş kısa mesajlar ve arama kayıtları çıkarılabilir. Sim karta erişim sağlamak ve analiz yapmak için *Device Seizure v2.0, Sim Manager Pro, Chiplt, SimScan, SIMPull* gibi uygulamalar kullanılmaktadır.

Dâhili ve harici hafıza kartlarından genellikle adres defteri bilgileri, kısa mesajlar ve görüşme kayıtları, GPS konum bilgileri, resimler, videolar, ses kayıtları, takvim bilgileri, yapılacaklar listesi, e-posta mesajları ve üçüncü parti uygulamalara (*Whataspp, Telegram, Chrome, Safari* vb.) ait bilgiler çıkarılmaktadır. Dâhili ve harici hafıza kartlarında yapılacak adli bilişim incelemesi fiziksel ve mantıksal imajlar üzerinden yapılmaktadır (Öztürkci 2014, 1). Mantıksal imaj alınırken izlenen adımlar, bir cep telefonundan veri yedeklerken yapılanlardan çok da farklı değildir. Günümüzde birçok mobil cihazın, bilgisayarlar üzerinde çalışan senkronizasyon araçları[35] mevcuttur. Bu araçlarla elde edilen imaj, bir adli bilişim yazılımı ile analiz edilerek delil çıkartma işlemi tamamlanmaktadır. Fiziksel imaj almak için ise, öncelikle cihazın yetkili erişim ehliyetinin imaj alacak kişinin elinde olması gerekmektedir. Yetkili erişim ehliyeti,

[35] *IOS* işletim sistemleri için tasarlanmış *ITunes* ve *ICloud* ile *Android* işletim sistemleri için tasarlanmış *Kies, Smart Switch* bunlara örnek olarak gösterilebilir.

cihazın açılış parolası veya şifreleme anahtarı gibi bilgileri kapsamaktadır.[36] Bu bilgiler cihaza tam yetki ile erişim olanağı vermektedir. Cihaza tam yetki ile erişim sağlandıktan sonra bir adli bilişim yazılımı ile fiziksel imaj alınmaktadır. Alınan imaj yine adli analiz yazılımları sayesinde incelenip raporlanmaktadır.

Mobil cihaz adli bilişiminde en çok kullanılan araçlar *CelleBrite, XRY, Paraben, Oxygen, Tarantula ve Mobil Edit*'tir.

2.2.2.1. Anlık Mesajlaşma Yazılımları

Bir bilgisayar programı sayesinde, üye olarak, listeye eklenen kişilerle gerçek zamanlı görüşme olanağı sağlayan yazılımlara *anlık mesajlaşma yazılımları* denilmektedir.[37] İnternetin hayatımıza girmesine paralel olarak gelişen anlık mesajlaşma yazılımları, internet kullanımının zamanla mobil dünyaya kaymasıyla birlikte, mobil cihazların ayrılmaz bir parçası haline gelmiştir. Bu sebeple adli analizlerde mobil cihazlardan elde edilen delillerin büyük bir çoğunluğunu anlık mesajlaşma yazılımlarından elde edilen yazışmalar oluşturmaktadır. Nitekim 2014 yılında adli bilişim uzmanları arasında yapılan bir ankette, katılımcıların %77'si anlık mesajlaşma uygulamalarından elde edilen verilerin en kritik veriler olduğunu ifade etmiştir (Cellebrite 2014, 4). Buna ek olarak, herhangi bir ihlale veya suça karışacak kişilerin, ihlalden önce, ihlal esnasında ve ihlalden sonra kolaylıkla iletişim kurabilmek için mobil uygulamalar kullandığı ifade edilmiştir (Mahajan vd. 2013, 38).

Mobil cihazlarda kullanılan anlık mesajlaşma yazılımlarına *WhatsApp, Telegram, WeChat, KakaoTalk, Facebook Messenger, Line* ve *Viber* örnek olarak gösterilebilir. Bu yazılımların en önemli ortak özellikleri ücretsiz olmaları, platform bağımsızlık

[36] Bazı durumlarda (kullanıcının parolayı söylemek istememesi, cihazın çalıntı olması vb.) cihazın yetkili erişim ehliyeti elde edilemeyebilir, böylesi durumlarda "*jailbreak*" veya "*superuser(rootlama)*" gibi giriş engellerini aşma yöntemleri kullanılarak cihazın şifreleri kırılır ve yetkili erişim sağlanır (Karaaslan vd. 2016, 4). Bir cihazı *jailbreak* veya *superuser* kullanarak kırmak, sistemdeki bilinen bir açığı kullanarak sistem üzerinde tam yetkili şekilde işlem yapabilmeyi sağlamak demektir. Bu işlem cihaz üzerinde bir takım değişiklikler yapar. Ancak yapılan değişiklikler sistem düzeyinde kaldığı için kullanıcı verileri herhangi bir zarar görmez. http://www.andronova.net/anlatim-root-nedir-root-erisimi-ve-yararlari, Erişim Tarihi:13.01.2016.

[37] Anlık Mesajlaşma, https://tr.wikipedia.org/wiki/Anl%C4%B1k_mesajla%C5%9Fma, Erişim Tarihi: 07.03.2016.

özellikleri sayesinde birçok farklı cihaza rahatlıkla kurulabilmeleri ve sorunsuz bir şekilde çalışabilmeleridir.

Anlık mesajlaşma yazılımlarının birçoğu verilerini şifrelenmiş bir şekilde, *SQLite* [38] ismi verilen bir veri tabanında saklamaktadır. Yazılım ilk açıldığında bu veri tabanındaki gerekli bilgiler hızlı işlem yapabilmek için, sabit diske oranla daha hızlı çalışan geçici belleğe (RAM) yüklenir ve yazılım tamamen kapatılana kadar burada kalmaya devam eder (Thakur 2013, 9). Bu sebeple anlık mesajlaşma yazılımlarından elde edilebilecek delillerde, alınan uçucu veri imajı oldukça önemli bir yere sahiptir.

Doğru bir şekilde elde edilmiş uçucu veri imajı ile silinmiş verilere de ulaşmak mümkündür. Alınan uçucu veri imajının ve diğer imajların adli bilişim yazılımına aktarılmasının ardından, çeşitli kıstaslara göre işlenme (*processing*) safhasına geçilir (Ukşal 2015, 67). Ancak burada dikkat edilmesi gereken husus, adli bilişim yazılımlarının yapamadığı sınıflandırmaların, adli bilişim uzmanı tarafından bizzat yapılmasıdır. Adli bilişim yazılımlarının her mobil uygulamanın dosyalarının saklandığı fiziksel yeri bilmesi mümkün değildir. Bu sebeple adli bilişim uzmanının hangi dosyanın hangi anlık mesajlaşma yazılımına ait olduğu konusunda bilgi sahibi olması gerekmektedir (Mahajan vd. 2013, 39). Örneğin aşağıda *Whatsapp* ve *Viber* isimli yazılımlara ait dosyaların, *Android* cihazlardaki isimleri görülmektedir:

[38] SQLite kendi kendine çalışabilen, yapılandırma ve sunucu gerektirmeyen bir SQL işlem kütüphanesidir. Herhangi bir kurulum gerektirmemesi ve kendisi dışında başka bir cihaza ihtiyaç duymaması nedeniyle, mobil platformlarda veri saklama amacıyla sıkça kullanılmaktadır. https://www.sqlite.org/about.html, Erişim Tarihi:14.01.2016.

Tablo 1: WhatsApp ve Viber Dosyaları (Mahajan vd. 2013, 39)

Uygulama	Dizin konumu	Dizin Adı	dosya Adı	SQlite Tablo Adı
whatsApp	/data/data/com.whatsapp/	/databases	1. Msgstore.db	1.1. messages 1.2. chat_list
			2. wa.db	2.1. wa_contacts
Viber	/data/data/com.viber.voip	/databases	1. Viber_call_log.db	1.1. Viber_call_log
			2. Viber_data (veri tabanı dosyası)	2.1. android_metadata
				2.2. phone book raw contact 2.3. phonebook contact 2.4. phonebook data 2.5. Viber numbers 2.6. Calls
			3. Viber_messages (veri tabanı dosyası)	3.1. android_metadata 3.2. messages 3.3. sqlite_sequence 3.4. threads 3.5. participants

Anlık mesajlaşma yazılımlarından delil olarak fotoğraflar, videolar ve yazışmalar elde edilebilmektedir. Özellikle yazışmaların veri tabanında şifrelenmiş bir şekilde saklanıyor olması adli analizi zorlaştırıyor gibi gözükse de, her geçen gün güncellenen "*yazılım açıklık veri tabanları*"[39] veya ilgili yazılımın açıklıklarından faydalanarak şifreleri çözmek mümkündür.

[39] Yazılım açıklık veri tabanı *exploit db* de denilen, internette uygulamaları inceleyerek açıklıklarını tespit eden kişilerin oluşturduğu ve güncellediği bir sistemdir. Bu sistem sayesinde popüler uygulamalara ait açıklıklar hakkında detaylı bilgilere ulaşmak mümkündür. Örneğin Whatsapp için hazırlanmış bir adli bilişim yazılımı olan *Whatsapp Xtract*'ın yaratıcısı, şifrelenmiş yazışmaları çözmek için AES şifresindeki açıklıktan yararlandığını ifade etmiştir (Thakur 2013, 4).

BÖLÜM 3

REKABET HUKUKU ALANINDA ADLİ BİLİŞİM UYGULAMALARI

Uluslararası rekabet otoritelerinin adli bilişim yaklaşımları ve mevzuatları kapsamında öncelikle ülkemizin takip ettiği mehaz mevzuat olan AB'nin uygulamaları Avrupa Komisyonu (Komisyon) pratikleri ışığında incelenmektedir. Daha sonraki bölümde rekabet ihlallerinin ortaya çıkarılmasında kolluk ile ortak çalışma yürüten ülkelerden biri olan ABD'nin adli bilişim usulü hakkında kısaca[40] bilgi verilmektedir. Son olarak ise, diğer ülke uygulamaları kısmında yer alan "ülkelere göre adli bilişim tablosu*"*nun özellikle AB ülkelerinin adli bilişime yaklaşımı hakkında genel bir kanı oluşturması hedeflenmektedir.

3.1. AVRUPA KOMİSYONU UYGULAMASI

Komisyon'un rekabet ihlallerine ilişkin inceleme yetkileri 2003 yılında yürürlüğe giren *1/2003 sayılı AB Konsey Tüzüğü* ile belirlenmiştir. Komisyon'a teşebbüs ve teşebbüs birliklerinin her türlü mülkünde ve taşıtında inceleme yapma yetkisi, söz konusu Tüzük'ün 20. maddesinin 2. fıkrasının (a) bendi ile verilmiştir. Aynı maddenin (b) bendinde ise Komisyon'a, nasıl ve ne şekilde saklandıklarına bakılmaksızın, işle ilgili tüm belgeleri ve kayıtları inceleme yetkisi tanınmıştır. Teşebbüs ve teşebbüs birliklerinden alınacak kopyaların mahiyeti ise aynı maddenin (c) bendinde yer bulmaktadır. Bu konuya ilişkin olarak *"Komisyon incelediği belgelerin ve kayıtların herhangi bir formatta kopyasını alma ve çıkartma hakkına sahiptir"* ifadelerine yer

[40] Çalışmada ABD'nin kısa anlatılmasının sebebi ABD'deki rekabet hukuku uygulamalarının adli rejime tabi olmasıdır.

verilmiştir. Bu itibarla, Komisyon incelemelerde izlenecek yol ve yöntemleri detaylı bir şekilde izah etmek amacıyla "*1/2003 Sayılı Tüzüğün 20. maddesinin 4. f*ıkrası *Uyarınca Gerçekleştirilen İncelemelere İlişkin Açıklayıcı Not (Açıklayıcı Not)*" [41] isimli bir çalışma yayımlamıştır.[42]

Açıklayıcı Not'ta, Komisyon'un rekabet ihlallerine karşı gerçekleştirdiği yerinde inceleme usulü tüm detayları ile irdelenmiş ve özellikle kartel dosyalarında edinilen dijital belgelere ilişkin atılacak adımlar sırasıyla ifade edilmiştir. 1/2003 sayılı Tüzük'te, yalnızca "*belgelerin ve kayıtların herhangi bir formatta kopyasının alınması*" şeklinde yer bulan durum, Açıklayıcı Not'un 9. maddesinde:

> Uzmanlar (*Inspectors*) işle ilgili tüm belgeleri ve kayıtları **-hangi ortamlarda saklandığına bakmaksızın-** incelemeye ve bu belge ve kayıtlardan **herhangi bir formda kopyalar almaya** yetkilidir. **Bu inceleme dijital bilgileri de içerir ve bu bilgilerin dijital ve kâğıt ortamda kopyalarını almayı da kapsar**.

şeklinde ifade edilmiştir.

Bilindiği gibi fiziksel belgeler, bir inceleme esnasında nerede bulundularsa oraya ait olarak değerlendirilmektedir (Karabulut vd. 2015, 400). Ancak dijital belgelerin incelemenin yapıldığı binada fiziksel olarak muhafaza edilmesi şartı söz konusu değildir. Yani dijital belgeler, herhangi bir yerden ulaşılabilen ancak başka bir binada, şehirde veya ülkede saklanabilen kayıtlardır. Dijital belgelerin bu özelliği sebebiyle Komisyon, yukarıdaki bölümde, kayıtların hangi ortamlarda saklandığına bakılmaksızın incelenebileceğini ifade etmiştir. Bu yetki genel olarak "**erişim yaklaşımı**"[43] olarak adlandırılmaktadır. ICN (2014, 28)'e göre erişim yaklaşımında genel kural;

---

[41] Explanatory Note On Commission Inspections Pursuant To Article 20(4) Of Council Regulation No 1/2003 http://ec.europa.eu/competition/antitrust/legislation/explanatory_note.pdf, Erişim Tarihi:12.12.2015.

[42] Açıklayıcı Not, Komisyon ve üye ülkelerin katkılarıyla sürekli güncellenmektedir. Bu çalışmanın hazırlandığı tarih itibariyle son güncellemesi 11 Eylül 2015'te yapılmıştır.

[43] Bir diğer yaklaşım ise **konum yaklaşımı**dır. Bu yaklaşımda otorite işine öncelikle dijital verinin hangi konumda saklandığına bakarak başlamaktadır. Eğer ilgili konum, otoritenin yasal olarak yetkilendirildiği binanın dışında ise, otorite yeni bir yetki belgesi düzenlemektedir. Bu belgede alternatif konumlardaki dijital verilerin kopyalanabileceğine ilişkin ibareler bulunmaktadır. Böylece otorite, incelenen teşebbüsün birçok mülkünde inceleme yapma yetkisi elde etmiş olmaktadır. Konum yaklaşımı, teşebbüsün bilgi sistemlerinin Komisyon'un/ülkenin yasal yetki sınırlarının içinde kaldığı durumlarda yetki genişliği sağlaması açısından oldukça avantajlıdır, ancak verilerin Komisyon'un/ülkenin yetkisi dışında kalan bir ülke sınırlarında saklanıyor olması konum yaklaşımını verimsiz hale getirmektedir. (ICN 2014, 28)

> …eğer teşebbüsün, kendi binası dışında bir veri ile ilgili erişim, kullanım ve kontrol etme yetkisi var ise bu; ilgili verinin teşebbüse ait olduğu gerçeğini ortaya koyar ve ilgili veri inceleme yapan otorite tarafından da erişilebilir, kullanılabilir, kontrol edilebilir

şeklindedir. Daha açık bir ifadeyle, incelenen bir teşebbüse ait dijital verilerin, fiziksel olarak başka bir teşebbüsün mülkünde saklanıyor olmasının erişim yaklaşımı açısından bir önemi yoktur. Zira incelenen teşebbüs kendi verilerine erişim hakkına sahip olduğu sürece, Komisyon'un ilgili verileri inceleme hakkı da saklıdır. Bu yaklaşım, otoritelere verinin saklandığı yerin bir sorun olmaktan çıkması ve incelemenin eksiksiz tamamlanması gibi avantajlar sağlamaktadır.

Açıklayıcı Not'un 10. maddesinde, yapılacak aramanın ve kopyalamanın detayları anlatılmış ve şu ifadelere yer verilmiştir:

> Uzmanlar teşebbüsün **bili**şimle ilgili tüm varlıklarını (Örn: S**unucular, masaüstü bilgisayarlar, dizüstü bilgisayarlar, tabletler ve diğer mobil cihazlar) ve tüm saklama ortamlarını (Örn: CD-ROM'lar, DVD'ler, USB-anahtarlar, harici diskler, yedekleme birimleri, bulut servisleri)** arayabilirler. Bu kural ayrıca **iş ortamında bulunan ve iş için kullanılan** (Kendi Cihazını Getir - Bring Your Own Device)[44] şahsi cihazları da kapsar. Bu amaçla, uzmanlar yalnızca sabit arama araçlarını değil, **kendi yanlarında getirdikleri bu iş için kullanılan yazılım ve/veya donanımları (Adli Bilişim Araçları-*Forensic IT Tools*) da kullanabilirler**. Bu adli bilişim araçları Komisyon'a, teşebbüsün sistemlerinin ve verilerinin bütünlüğüne zarar vermeksizin **kopyalama, arama ve veri kurtarma** imkânları sağlar.

Yukarıdaki ifadelerden Komisyon'un teşebbüslerin, yalnızca bilgisayarlarını değil, iş için kullanılan tüm unsurlarını inceleme yetkisi olduğu anlaşılmaktadır. Bu ise Açıklayıcı Not'un önceki sürümlerinde bulunmayan yeni bir durumdur. Yani Komisyon bundan sonraki uygulamalarında, teşebbüs çalışanlarının kullandıkları cihazların teşebbüse ait olup olmadığına bakmaksızın, hangi amaçla kullanıldığına odaklanacaktır.[45] Bu durumda, içerisinde teşebbüse ait e-posta hesabının tanımlı olduğu bir cep

[44] Kendi Cihazını Getir uygulaması bir şirket çalışanlarının dizüstü bilgisayar, akıllı telefon gibi mobil cihazlarını profesyonel amaçlar için kullanmayı öngören bir altyapı modelinin sloganıdır. http://www.bt.org.tr/makale/byod-bring-your-own-device-nedir/509 Erişim Tarihi:20.12.2015.

[45] Bu durum şüphesiz temel hak ve özgürlükler ile kişisel bilgilerin gizliliği alanlarında çeşitli ihlallere konu olması bakımından tartışmalara yol açmıştır. Söz konusu tartışmalar için bkz: (Kuschewsky ve Geradin 2013,18), (Brown 2015, 1) ve (Kinsella 2015, 1).

telefonunun da incelenmesi mümkün olabilecektir. Aynı zamanda artık Komisyon'un incelemelerde yalnızca teşebbüsteki imkânlarla araştırma yapmakla kalmayıp, uzmanlar tarafından hazır bulundurulan yazılım ve donanımları da inceleme için kullanabileceği ifade edilmektedir. Bu durum ise, yıllardır tartışılagelen, incelemelerde teşebbüs bilgi sistemlerinin bütünlüğünün bozulduğu tezlerini alevlendireceğe benzemektedir (Aktekin 2013, 1). Ancak bu tartışmaları sonlandırmak amacıyla Komisyon, 10. maddedeki ilerleyen ifadelerde, teşebbüsün bilgi sistemlerine ve verilerine herhangi bir zarar vermeyeceğini taahhüt etmektedir.

Açıklayıcı Not'un 11. maddesinde Komisyon, önceki sürümlerde yer verilen *teşebbüs işbirliği* kavramının, yeni sürümde hangi başlıkları kapsadığı hususunu detaylandırmıştır. Nitekim Komisyon'un, teşebbüslerden yalnızca bilişim altyapısı ve organizasyona dair bilgi almak yerine, ***gereken durumlarda bazı e-posta hesaplarının geçici olarak bloke edilmesini, bazı bilgisayarların geçici olarak ağdan çıkarılmasını, hard-disklerin bilgisayarlardan çıkarılması ve geri takılmasını ve uzmanlara "yönetici erişim yetkisi" verilmesini isteme yetkisi*** mevcuttur. Aynı zamanda teşebbüsün tüm bu işlemler yapılırken sisteme aksi bir müdahale etme hakkı yoktur ve olası iş kayıpları için ilgili çalışanları bilgilendirme görevi de teşebbüse verilmiştir (Açıklayıcı Not 11. madde). Bu halde teşebbüsün, Komisyon'un teknik işlemlerini kolaylaştırma yükümlülüğü vardır (Pınar 2011, 135).

Açıklayıcı Not'un, incelemelerdeki delil toplama usulüne ilişkin bir diğer önemli maddesi ise, incelemelerin öngörülen zamanda bitirilememesi durumunda alınacak aksiyonla ilgili ifadelerdir. Buna göre;

> Eğer teşebbüs binasındaki incelemeyle ilişkili olarak belgelerin seçilmesi işlemi öngörülen zamanda bitirilemezse, **arama yapılan verinin bir kopyası daha sonra incelenmek üzere alınabilir**. Bu kopya mühürlü bir zarfa konulmak suretiyle koruma altına alınır. Teşebbüs bu kopyanın bir kopyasını isteyebilir. Komisyon, mühürlü zarfın açılacağı gün Komisyon binasında hazır bulunması için teşebbüse davet gönderir. Buna alternatif olarak Komisyon, zarfı hiç açmadan teşebbüse geri gönderebilir. Komisyon ayrıca teşebbüsten zarfı daha sonra bildirilecek bir ziyarette incelenmek üzere saklamasını da isteyebilir (Not 14. madde).

Açıklayıcı Not'un 13. maddesinde, Komisyon'un almış olduğu delillerin veri bütünlüğünü korumak ve güvenliğini sağlamak için kullanacağı yöntemden bahsedilmektedir. Nitekim uzmanlar, inceleme sonunda, kendileri tarafından kullanılan ve teşebbüse ait bilgilerin analiz edildiği tüm adli bilişim araçlarını **sterilize** (*wipe*) işlemine tabi tutmak zorundadır.

Açıklayıcı Not'un 15 ve 21 arasındaki maddelerinde incelemenin nihayete erdirilmesi için yapılması gerekenler anlatılmıştır. İnceleme sonunda, uzmanlar tarafından Komisyon'un dosyasına eklenen tüm verilerin bir kopyası teşebbüse de bir veri taşıyıcı (Örn: DVD) aracılığı ile bırakılmaktadır. Teşebbüsün seçilen veri başlıklarının listesinin olduğu belgeyi imzalaması beklenmektedir. Bu verilerin bulunduğu iki kopya halinde oluşturulmuş veri taşıyıcı ise uzmanlar tarafından muhafaza edilmektedir.

Pratikte Komisyon'un inceleme usulü, inceleme yapılacak teşebbüse intikal edildikten sonra incelemenin konusu ve amacını da içeren[46] yetki belgelerinin ve Açıklayıcı Not'un teşebbüs yetkililerine sunulması ile başlamaktadır. Yetki belgelerinin yanında Açıklayıcı Not'un da sunulması, Komisyon uygulamalarının şeffaflığını temin etmek için yapılmaktadır (Erps 2013, 213). Teknik olarak ise inceleme, uzmanların teşebbüsün bilgi sistemleri altyapısı ile ilgili bilgi alması ile başlamaktadır. Açıklayıcı Not'ta belirtildiği üzere, uzmanlar teşebbüs yetkililerinden gerekli gördükleri takdirde bilgi sistemleri altyapısındaki bazı veri akışlarının kesilmesini isteyebilirler. Bu işlemler gerçekleştirilirken teşebbüs yetkililerinin yalnızca istenen aksiyonu almaları ve fazladan bir müdahale yapmamaları ayrıca önem taşımaktadır. Nitekim 2012 yılında yapılan bir yerinde inceleme esnasında *EPH*[47] unvanlı teşebbüse, Komisyon'un istediği e-posta hesaplarını bloke etmediği ve hatta bazı e-posta hesaplarına gelen postaları başka bir hesaba yönlendirdiği için, yerinde incelemeyi zorlaştırdığı gerekçesiyle 2,5 milyon Euro idari para cezası uygulanmıştır.

İncelemenin ilerleyen aşamasında uzmanlar tarafından inceleme konusu ile ilgili bilgi içerebileceği düşünülen tüm cihazlar (dizüstü ve masaüstü bilgisayarlar, mobil

[46] İncelemenin konusunun ve amacının belirtilmesi, sadece ilgili incelemenin haklılığını değil, aynı zamanda teşebbüsün sorumlu olduğu işbirliğinin sınırlarının doğru çizilmesi açısından da temeldir. (Gündüz 2009, 27) İlgili ABAD kararları için bkz: Case 46/87 and 227/88, *Hoechst AG v. Commission*, 21.09.1989, para.29 ile Case C-94/00, *Roquette Freres SA v. Commission*, 22.10.2002, para.47.

[47] Case Comp/39793, *EPH and Others*, 28.03.2012.

telefonlar, tabletler, USB cihazlar, CD-Romlar vb.) tespit edilmektedir. Bu cihazların inceleme bitimine kadar uzmanların kontrol ve gözetiminde kalması gerekebilmektedir. Daha sonra tespit edilen cihazlardan ilgili olabileceği düşünülen bölümlerin kopyaları çıkarılmaktadır. Belli tür rekabet ihlali dosyalarında bu kopyalar çoğunlukla adli kopya denilen *cihazın tüm unsurları ile klonlanması (imajının alınması)* şeklinde yapılmaktadır (Erps 2013, 214). Kopyalama işlemi tamamlandıktan sonra uzmanlar ilgili cihazı gecikmeden teşebbüse iade etmekle sorumludur. Kopyalanan verilerin transferi için uzmanlar, genellikle Komisyon'un kendi cihazlarını kullanmakta, ancak Açıklayıcı Not'un 11. maddesi uyarınca, gereken durumlarda teşebbüsten donanım talebinde bulunabilmektedir. Daha sonra kopyalanan tüm veriler uzmanlar tarafından incelemede hazır bulundurulan **yüksek işlem kapasitesine sahip bilgisayara**[48] yüklenmektedir. Bu bilgisayarlarda çeşitli kriterlere göre tasnif edilen dosyalar daha rahat incelenebilecek hale gelmekte ve "*gözden geçirme istasyonları*"[49] denilen cihazlarda kullanıma açılmaktadır (Erps 2013, 214).

Yukarıda ifade edilen tüm bu işlemlerin gerçekleştirilmesi için gereken süre eldeki kopyaların boyutuna da bağlı olarak değişmektedir. Bu kapsamda bazı durumlarda incelemenin aynı gün bitirilememesi söz konusu olduğu için uzmanlar, işlemler gerçekleştirilirken teşebbüsten kendilerine bir oda tahsis etmelerini isteyebilmektedir. İncelemenin aynı gün bitirilememesi durumunda uzmanlar ilgili odayı mühürleyerek, incelemeye ertesi gün devam etmek üzere teşebbüsten ayrılmaktadır (Erps 2013, 214). Komisyon yetkililerinin yeniden teşebbüse intikal etmesine kadar mührü ve odayı koruma görevi teşebbüse aittir. Bu kapsamda geçmiş yıllarda, Komisyon yetkilileri tarafından mühürlenen odanın mühürlerini kırmaktan *E.ON Energy AG*[50]'e 38 milyon Euro, *Suez Environment*[51]'e ise 8 milyon Euro idari para cezası uygulanmıştır.

[48] Burada yüksek işlem kapasiteli bilgisayar ifadesinden kasıt kullanılan adli bilişim platformudur. Komisyon, teşebbüslerdeki incelemeler esnasında veri ayrıştırma ve aramaları için *Nuix* platformunu kullanmaktadır. *Nuix* e-keşif, dijital soruşturma ve bilgi yönetim yazılımları da dâhil olmak üzere dünya çapında bir bilgi yönetimi teknolojileri sağlayıcısıdır. http://www.reuters.com/article/idUS98948+13-Nov-2012+BW20121113, Erişim Tarihi:09.03.2016.

[49] Gözden Geçirme İstasyonları (*Review Stations*): *Nuix* altyapısında bulunan bu sistem, verilerin tasnifi sağlandıktan sonra başka cihazlarda kullanıma açılmasıdır. Böylece aynı veri-seti üzerinde birden fazla kişinin eşzamanlı inceleme yapmasına olanak sağlanmış olur. http://www.nuix.com/products/nuix-reviewer, Erişim Tarihi: 09.03.2016.

[50] Case COMP/B-1/39.326, *E.ON Energie AG*, 30.01.2008.

[51] Case 39.796, *Suez Environment and LDE*, 24.05.2011.

İncelemenin daha sonraki aşamasında, sınıflandırılan dosyaların uzmanlar tarafından *işaretleme işlemi* yapılmaktadır. İşaretleme işlemi yapılırken, soruşturmanın kapsamına uygun hareket edebilmek amacıyla çoğunlukla Komisyon tarafından önceden belirlenen arama ifadeleri kullanılmaktadır (Polley 2013, 4). İşaretleme işleminin tamamlanmasının ardından ayrıştırılan tüm veriler tüm dosyaların isminin, dosya yolunun ve bağlantısının bulunduğu bir liste ile birlikte şifrelenmiş bir veri taşıyıcıya yüklenmektedir. Tüm dosyalardan üretilen tekil bir ayıraç olan *kriptografik özet* dosyası da veri taşıyıcıya yüklenmek suretiyle, verilerin değiştirilememesi garanti altına alınmaktadır. Hangi belgelerin alındığına ilişkin oluşturulan liste teşebbüs temsilcisi ve uzmanlar tarafından imzalanmaktadır. Komisyon tarafından alınan tüm belgelerin bir kopyası da teşebbüse, ek listesi ile birlikte bırakılmaktadır (Erps 2013, 214).

İncelemenin sonunda, uzmanlar inceleme boyunca veri taşıma, kopyalama ve inceleme için kullandıkları tüm ekipmanlarını sterilize etmektedir. Ancak teşebbüsten alınan ekipmanların sterilizasyonu uzmanlar tarafından yapılmamaktadır (Erps 2013, 214).

Uzmanlar -kopyalanacak cihazların tespitinin uzun sürmesi dolayısıyla incelemenin beklenen zamanda bitmemesi, teknik sorunlar oluşması veya işlemlerin teşebbüsün kendi işlemlerine engel oluşturacak denli uzun sürmesi gibi- istisnai bazı durumlarda yerinde inceleme süresi boyunca ilişkili belgeleri işaretleme işlemini bitiremeyebilmektedir. Bu durumda "mühürlü zarf usulü" uygulanmaktadır (Erps 2013, 214). İnceleme konusu ile ilişkili olduğu düşünülen, ancak henüz tam olarak ayrıştırılmamış veriler, şifrelenmiş bir veri taşıyıcıya yüklenmekte ve bu veri taşıyıcı bir zarfa konularak mühürlenmektedir. İlgili verilerin bir kopyası da teşebbüse bırakılmaktadır (Erps 2013, 214-215). Daha sonra mühürlü zarf Komisyon'un merkez binasına getirilmektedir. Zarfın açılışı esnasında teşebbüs temsilcilerinin Komisyon binasında hazır bulunması gerekmektedir. Temsilcilerin refakatinde açılan zarf ve içeriği, yine onların refakatinde incelenmekte ve işaretlenmektedir. İşaretlenen veriler, daha önce anlatılan işlemlere tabi tutulmaktadır (Erps 2013, 215).

Mühürlü zarf usulünün işlendiği bir olayda Komisyon, verilerin bir kısmını kendi ofisinde incelemek üzere teşebbüs binasından çıkardığı için Genel Mahkeme'ye (GM) şikâyet edilmiştir. Bu davada GM, mühürlü zarf usulünün şirketlerin yasal pozisyonunda belirgin bir değişim öngörmediğine hükmetmiş ve başvuruyu reddetmiştir[52].

Komisyon'un incelemelerde, teşebbüsün bilgi sistemlerini tümüyle veya kısmen kopyalama yetkisine sahip olması, teşebbüsler ve temsilcileri tarafından karşı çıkılan bir uygulamadır. Nitekim *Nexans*[53] davasında ilgili teşebbüs, güç kabloları dosyası kapsamında Komisyon tarafından yapılan yerinde incelemede birtakım dosyaların tümüyle kopyalanmasının hukuka aykırılığı iddiasıyla GM'ye başvurmuştur. Dava kapsamında GM, Komisyon'un inceleme hakkının henüz tam olarak bilinmeyen ve tanımlanmamış bilgileri de **arama yetkisini ima ettiğine**, çünkü böylesi bir yetki olmaksızın gereken bilgilere ulaşmanın imkânsız hale geleceğine hükmetmiştir. Ayrıca GM, başvuranın yerel inceleme esnasında çok özel (şahsi) dokümanlarının varlığı dolayısıyla koruma talep etmediği için Komisyon'da dava edilebilecek bir husus olmadığına işaret etmiştir. Ancak bununla birlikte GM, Komisyon'un teşebbüsteki aramalarının (*searches*),[54] teşebbüsün incelenme kararında belirtilen sektörlerdeki faaliyetleri ile sınırlandırılması gerektiğine, eğer Komisyon böylesi bir kısıtlamaya tabi olmazsa, bu durumda Komisyon'un teşebbüsün tüm aktivitelerine ait incelemeler yapabileceği sonucuna ulaşılacağına, bunun ise teşebbüsün **gizlilik hakkının ihlali** olacağına karar vermiştir.

Komisyon'un bilgisayarlardaki inceleme yetkisine ilişkin başka bir konu ile mahkeme gündemine gelen *Deutsche Bahn*[55] dosyasında ise GM, Komisyon tarafından ilgili incelemede kullanılan tüm arama terimlerini, incelemenin kapsamına riayet edilip edilmediğini tespit edebilmek için irdelemiştir. İtirazın arka planında teşebbüste yapılan ilk incelemede, inceleme konusu olmayan başka bir ihlale ilişkin delil bulunması, bunun üzerine ikinci bir soruşturma açılması bulunmaktadır. Başvuru sahibi teşebbüs, Komisyon'un incelemenin kapsamı dışında delil araması yaptığını iddia ederek GM'ye

[52] Case T-140/09, *Prysmian and Prysmian Cavi e Sistemi Energia v. Commission.*
[53] Case T-135/09, *Nexans France SAS and Nexans SA v. Commission.*
[54] Burada "*searches*" kelimesinden kasıt, Komisyon'un teşebbüs bilgisayarlarında yaptığı anahtar kelime aramalarıdır.
[55] Birleştirilen Dosyalar T-289/11, T-290/11, T-521/11 *Deutsche Bahn AG a.o. v.*

başvurmuştur. GM arama terimlerinin ve inceleme koşullarının detaylı analizini yaptıktan sonra başvuruyu reddetmiştir.

Pilkington Group[56] kararında ise GM; imaj alma veya anahtar kelimelerle dijital arama gibi yerinde inceleme sırasında alınan uygulama tedbirlerinin yargısal denetiminin zor olduğunu belirtmiştir. Bu kararlardan anlaşılacağı üzere GM Komisyon'a, dijital veriyi gözden geçirmesi ve arama terimlerini seçmesi için *makul bir özgürlük alanı* vermiştir. Örneğin, Komisyon'un dosya ile ilgili olduğunu düşündüğü herhangi bir belgeye bakmaya yetkili olduğunu ifade etmiş, **arama terimlerinin inceleme boyunca gelişebileceğine** hükmetmiştir.[57]

Tüm veri tabanının kopyalanması işlemi ve imaj almayı gerektirecek hususların varlığı konusu, *Robathin*[58] davasında Avrupa İnsan Hakları Mahkemesi'nin (AİHM) gündemine gelmiştir. Anılan davada AİHM; dijital incelemeyi haklı gösterecek genel nedenlerin varlığını ve tüm veri tabanının kopyalanmasını Avrupa İnsan Hakları Sözleşmesi'ne aykırı görmemiştir.

Bilgisayarların tam kopyasının alınmasını konu alan bir başka dava olan *Bernh Larsen Holding AS*[59] davasında ise, Norveç vergi otoritesinin, başvuran şirketlerin sunucu bilgisayarının kopyasını almasının ve incelenmek üzere kendi ofisine götürmesinin AİHS'nin 8. maddesine[60] uygunluğu değerlendirilmiştir. İlgili dosyada başvuru sahipleri, sunucunun birebir kopyasının alınmasının demokratik toplum gerekliliğine aykırı olduğunu ve otoritelerin yetkilerini kötüye kullanmamaları için herhangi bir etkili teminat bulunmadığını iddia etmişlerdir. Bu kapsamda AİHM, böylesi bir yetki kullanımının, 8. madde bakımından başvuranın "evine" ve "yazışmalarına" müdahale sayılacağını, sunucunun birebir kopyasının alınmasının, aynı zamanda vergi denetimi işlemleri ile ilgisi olmayan çok büyük miktarda veriye de el koymak olduğunu ifade

[56] T-462/12R.
[57] *Deutsche Bahn AG a.o. v.* para. 139,155.
[58] Başvuru No: 30457/06, *Robathin v Austria.*
[59] Başvuru No: 24117/08, *Bernh Larsen Holding AS v. Norway.*
[60] Özel hayatın gizliliğine yapılacak her türlü müdahale Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinin 2. fıkrasında aradığı üç şartla uyumlu olmalıdır. Bu çerçevede özel hayata müdahale 1- Hukuka uygun olmalı, 2- Demokratik toplum açısından gerekli olmalı, 3- Ulusal güvenlik, kamu güvenliği, ülkenin ekonomik durumu veya suçun veya düzensizliğin önlenmesi, sağlık veya ahlakın korunması veya diğerlerinin haklarının ve özgürlüklerinin korunması için gerekli olmalıdır.

etmiştir. Ancak, *sunucuda verilerin açıkça ayrıştırılmamış "karışık" arşivler şeklinde durması* gerçekliğinden hareketle AİHM, uzmanların mevcut yasaların onlara verdiği yetkiye dayanarak, **konuyu etraflıca değerlendirebilmek maksadıyla tam kopya aldıkları** ve etkili vergi denetimleri yapabilmek için sunucuların tam kopyasını almanın gerektiği sonucuna ulaşmıştır. Bu davada her ne kadar taraflardan hiçbiri rekabet otoritesi değilse de, rekabet otoritesinin de idarenin bir parçası olması bakımından vergi otoritesine benzer işlemler gerçekleştirdiği açıktır. Bu itibarla davanın Komisyon uygulamalarına emsal teşkil edebileceğini söylemek mümkündür (Polley 2013, 18).

Komisyon, incelemelerdeki teknik işlemler için kendi bünyesinde bilişim uzmanları istihdam etmektedir (Kerse ve Khan 2005, 171). Bunun yanında Komisyon'un bilgisayarların incelenmesi için kendi personeli dışında başka rekabet otoritelerinden veya dışarıdan kaynak temini yaptığı bilinmektedir (Devrim 2009, 27; Gündüz 2009, 26)

3.2. AMERİKA BİRLEŞİK DEVLETLERİ UYGULAMASI

ABD'de rekabet hukuku kuralları Adalet Bakanlığı'nın Antitröst Birimi (DOJ) ve Federal Ticaret Komisyonu'nun rekabet bürosu (FTC) tarafından uygulanmaktadır. Rekabet hukuku uygulamaları kapsamında dosyalar, ceza hukuku rejimine tabi olan davalar (*criminal cases*) ve diğer davalar (*civil cases*) olarak ikiye ayrılmaktadır. Ceza hukuku rejimine tabi olan davalarda hususi olarak DOJ görevli iken, diğer davalar ve birleşme/devralmalar gibi dosyalarda DOJ ve FTC sektör bazlı iş paylaşımı yapmaktadır (Yalçınkaya 2015, 29-30). Bu kapsamda kullanılan delil elde etme enstrümanları, dosyanın hususiyetine göre değişiklik göstermekle beraber yalnızca DOJ tarafından yürütülen ceza dosyalarında, adli arama yetkisi[61] söz konusu iken[62] (Coşgun 2009, 3), DOJ ve FTC'nin paylaşımlı yürüttüğü diğer dosyalarda bilgi ve belge isteme yetkisi ön plana çıkmaktadır (Everett vd. 2012, 21).

DOJ tarafından gerçekleştirilen adli aramalar, bir arama emri eşliğinde; Federal Soruşturma Bürosu (FBI) ajanları ile işbirliği içerisinde icra edilmektedir. Bu kapsamda

[61] Federal Rule of Criminal Procedure 18 U.S.C., Rule 41.

[62] DOJ'un ceza dosyaları kapsamında kullandığı bir diğer yetki ise iletişimin tespiti ve telefon dinleme yetkisidir. Bu başlık, çalışmanın ana omurgasını oluşturan adli bilişim konusunun dışında kaldığı için incelenmemiştir.

DOJ dijital cihazlar üzerinde arama, kopyalama ve el koyma yetkilerini haizdir (Everett vd. 2012, 23). Esasında DOJ tarafından gerçekleştirilen bu işlemler klasik bir adli bilişim sürecine işaret etmektedir. El konulan veya kopyası alınan cihazlar adli bilişim laboratuvarlarına götürülerek adli analize alınmakta ve delil elde etme süreçlerine tabi tutulmaktadır. Bu aşamada ABD yasaları, gerçekleştirilen adli analizin hangi araçlarla veya ne kadar gelişmiş tekniklerle yapıldığına herhangi bir kısıtlama getirmemiştir (Everett vd. 2012, 89). Aksine *Grimmett*[63] kararında Temyiz Mahkemesi "*bir bilgisayar araması, emirde açıklanan öğeleri bulmak için gerekli olan en makul genişlikte olabilir*" ifadelerini kullanmıştır. Bununla birlikte bir bilgisayarda, hakkında inceleme yapılan konu haricinde birçok farklı türde belgenin de bulunmasının mümkün olduğu gerçeğinden hareketle ABD Yüksek Mahkemesi *Andresen v. Maryland* kararında;

> bazı belgelerin, **en azından davayla ilgisi olup olmadığının tespit edilebilmesi amacıyla incelenmesinde herhangi bir sakınca olmadığı**, ancak yargı yetkilileri de dâhil olmak üzere sorumlu yetkililerin, [bu aramalardaki] gizliliğe yersiz müdahalelerini en aza indirecek şekilde yürütülmesini sağlamak için dikkat etmesi gerektiği [64]

ifadelerine yer vermiştir.

DOJ'un yürüttüğü ceza soruşturması dosyalarında, Soruşturma Kurulu tarafından teşebbüslerden, bireylerden ve gerekli görülen üçüncü makamlardan bilgi, belge ve tanıklık talep edilebilmektedir. Bu işlem Büyük Kurul Celbi (*grand jury subpoena*) olarak ifade edilmektedir (Everett vd.2012, 21). Aynı şekilde FTC de yürüttüğü dosyalar kapsamında teşebbüslerden bilgi, belge ve tanıklık talebinde bulunabilmektedir (Yalçınkaya 2015, 30).[65] Teşebbüsler açısından bu talebi karşılamak bazı durumlarda gönüllülüğe, bazı durumlarda zorunluluğa dayanmaktadır. Zorunlu bilgi paylaşımı (*compelled production*) olarak adlandırabilecek durumda, DOJ veya FTC bir celp aracılığıyla soruşturma ile ilgili olabilecek tüm belge ve kayıtların basılı veya dijital halde kopyasını isteyebilmektedir.[66] İstenen bilgi ve belgeleri temin etmek için teşebbüsler, kendi bilişim altyapılarında gereken aramaları yapmak ve ilgili otoritenin istediği formatta bilgi ve belgeleri sunmak zorundadır. Aynı zamanda bilgi ve belge talebinde

[63] *United States v. Grimmett*, 439 F.3d 1263, 1270 (10th Cir. 2006)
[64] *Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976)
[65] 15 U.S.C. § 49 (FTC)
[66] 15 U.S.C. § 57b-1 (FTC); 15 U.S.C. §§ 1311-1314 (DOJ)

bulunan otoritenin, temin süreci boyunca teşebbüsün bilgi sistemleri altyapısına ve teşebbüste hangi aksiyonların alındığına dair bilgi isteme yetkisi de mevcuttur (ICN 2014, 11).

Gönüllü bilgi paylaşımı (*voluntary production*) olarak adlandırılabilecek diğer durum ise, rutin bir pişmanlık başvurusu sürecinden farksız olduğu için bu bölümde detaylandırılmamıştır.

3.3. DİĞER ÜLKE UYGULAMALARI

Dünyadaki diğer ülkeler nezdinde rekabet ihlali dosyalarında adli bilişim araçlarını kullanma açısından genel duruma bakıldığında, birçok ülkenin imaj alma yetkisi olduğu göze çarpmaktadır. Özellikle ülkemizin takip ettiği AB mevzuatı açısından dikkat çeken nokta, Avrupa ülkelerinin birçoğunda yerinde incelemeler esnasında imaj alınabiliyor olmasıdır. Bununla birlikte bazı ülkelerde gerçekleştirilen yerinde incelemelerde bir takım işlemlerin gerçekleştirilebilmesi için rekabet otoritesi dışında bir otoritenin de (hâkim kararı, savcılık emri vb.) iznine ihtiyaç duyulmaktadır.

Tablo 2'de dünyadaki bazı ülkelerin adli bilişime ilişkin genel yaklaşımını görmek mümkündür. Buna göre, örneğin Almanya'da rekabet ihlali dosyalarında adli ve idari otorite birlikte hareket edebilmekte, teşebbüs mülkünde ve konutlarda yapılacak bir incelemede mahkemeden alınan bir yetki belgesi çerçevesinde her iki otorite de hazır bulunabilmekte ve incelemeler esnasında adli imaj alınabilmektedir.[67] Benzer şekilde örneğin İtalya'da rekabet ihlali dosyaları yalnızca ülkenin rekabet otoritesi tarafından yürütülürken, yerinde incelemelerde yalnızca teşebbüsün mülküne girilme yetkisi mevcuttur. Öte yandan İtalyan rekabet uzmanlarının yerinde incelemelerde imaj alma yetkileri de bulunmaktadır.[68]

[67] http://www.iclg.co.uk/practice-areas/cartels-and-leniency/cartels-and-leniency-2016/germany, Erişim Tarihi:10.02.2016.

[68] http://www.iclg.co.uk/practice-areas/cartels-and-leniency/cartels-and-leniency-2016/italy, Erişim Tarihi:10.02.2016.

Tablo 2: Ülkelerin İnceleme Yetkileri Özeti[69]

ÜLKE	Özel belgeler ya da bilgiler isteme yetkisi		Teşebbüs mülkünde habersiz inceleme yapma etkisi		Konutlarda habersiz inceleme yapma yetkisi		Adli Bişim araçları kullnılarak imaj alma yetkisi	
	(İO) İdari Otorite Yürütüyor	(İO) Adli Otorite Yürütüyor	İO	AO	İO	AO	İO	AO
Almanya	Evet	Hayır	Evet*	Evet*	Evet*	Evet*	Evet*	Evet*
ABD	Evet	Evet	Hayır	Evet*	Hayır	Evet*	Hayır	Evet*
Arnavutluk	Evet	Hayır	Evet	Hayır	Evet*	Hayır	Evet	Hayır
Avusturalya	Evet	Evet	Evet*	Evet*	Evet*	Evet*	Evet*	Evet*
Avusturya	Evet	Kısmen	Evet*	Kısmen	Evet*	Kısmen	Evet*	Kısmen
Belçika	Evet	Hayır	Evet*	Hayır	Evet*	Hayır	Evet	Hayır
Çin	Evet	Hayır	Evet	Hayır	Evet	Hayır	Evet	Hayır
Danimarka	Evet	Hayır	Evet	Hayır	Evet*	Hayır	Evet	Hayır
Finlandiya	Evet	Hayır	Evet	Hayır	Evet*	Hayır	Evet	Hayır
Fransa	Evet	Evet*	Evet*	Evet*	Evet*	Evet*	Evet*	Evet*
Hindistan	Evet	Hayır	Evet*	Hayır	Evet*	Hayır	Evet*	Hayır
İngiltere	Evet	Evet	Evet*	Evet*	Evet*	Evet*	Evet	Evet
İspanya	Evet	Hayır	Evet*	Hayır	Evet*	Hayır	Evet	Hayır
İtalya	Evet	Hayır	Evet	Hayır	Hayır	Hayır	Evet	Hayır
Japonya	Evet	Evet*	Evet	Evet*	Hayır	Evet*	Evet	Evet*
Kanada	Evet*	Evet*	Evet*	Evet*	Evet*	Evet*	Evet*	Evet*
Norveç	Evet	Evet*	Evet*	Evet*	Evet*	Evet*	Evet*	Evet*
Rusya	Evet	Evet	Evet	Evet	Hayır	Evet*	Evet	Evet

(Yanında yıldız işareti bulunan cevaplar, ilgili işlem için söz konusu otorite dışında ikincil bir otoritenin iznine tabi olunduğunu göstermektedir.)

Tablo 2'den de anlaşılacağı üzere ABD ve AB ülkelerinde geniş yetkilerin bulunduğu ve bunun sonucu olarak adli bilişim araçlarının etkin bir şekilde kullanıldığı görülmektedir. Takip eden bölümde ülkemizdeki adli bilişim mevzuatına ve idari rejimlerin adli bilişim yetkilerine değinilmektedir.

[69] Bilgiler Uluslararası Karşılaştırmalı Hukuk Rehberi'nden derlenmiştir. http://www.iclg.co.uk/practice-areas/cartels-and-leniency/cartels-and-leniency-2016, Erişim Tarihi:27.01.2016.

BÖLÜM 4

TÜRK MEVZUATINDA ADLİ BİLİŞİM

Türk yargı sistemi genel olarak; adli ve idari yargı şeklinde ikiye ayrılmaktadır. Bu bölümde Türk mevzuatında yer alan ve uygulayıcılar açısından adli ve idari birimlerin görev alanına giren adli bilişime ilişkin hükümlere ve uygulamalara yer verilmektedir.

4.1. ADLİ BİRİMLERCE YÜRÜTÜLEN İŞLEMLERDE UYGULANAN ADLİ BİLİŞİM MEVZUATI

Adli birimler tarafından gerçekleştirilen delil elde etme uygulamalarının temel kaynağını CMK oluşturmaktadır. CMK'nın 116. maddesine göre *"Yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe varsa; şüphelinin veya sanığın üstü, eşyası, konutu, işyeri ve ona ait diğer yerler aranabilir"*. Aynı CMK'nın 119. maddesine göre ise *"Hâkim kararı üzerine veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının yazılı emri ile kolluk görevlileri arama yapabilirler"*. Söz konusu madde, klasik suçlara ilişkin genel bir arama rejimi ihtiva etmektedir (Özocak 2011, 121). CMK'nın 134. maddesindeki düzenleme ile ise, aramanın teknik kısmı dikkate alınarak dijital delillerin toplanmasında şekilsel kurallar belirlenmiştir (Bostancı ve Benzer 2015, 6-7).[70] CMK'nın "*Bilgisayarlarda, Bilgisayar Programlarında ve Küt*üklerinde Arama, Kopyalama ve El *Koyma*" başlıklı 134. maddesi[71] şu şekildedir:

[70] "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." (Yücetürk 2011, 102)

[71] İlgili madde ile birlikte Adli ve Önleme Aramaları Yönetmeliği'nin 17. maddesi ile Suç Eşyası Yönetmeliği'nin 9. maddesi de bilişim sistemlerinde arama, kopyalama ve el koymaya ilişkin hükümler içermektedir.

(1) Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

(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 el konulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, el konulan cihazlar gecikme olmaksızın iade edilir.

(3) Bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.

(4) İstemesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

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

CMK kapsamındaki genel aramadan (CMK m. 116 ve 119) farklı olarak 134. madde bağlamında bilişim sistemlerinde arama, kopyalama ve el koyma yapılabilmesi için, başka surette delil elde etme imkânının bulunmaması ve hâkim kararı[72] şartları söz konusudur. Bununla birlikte kanun kapsamında veri alınacak olan bilgisayar, şüpheliye ait olabileceği gibi üçüncü kişilerin veya resmi bir kuruluşun da olabilmektedir. Yasada bu konuda herhangi bir sınırlama yer almamaktadır (Centel ve Zafer 2014, 412). 134. maddenin üç ve dördüncü fıkralarında, bilgisayarında inceleme yapılan kişinin haklarının hukuki güvence altına alınması adına yapılması gereken işlemler sıralanmıştır (Sevimli 2007, 997)[73]. 134. maddenin lafzından ayrıca, ilgili maddede öngörülen tedbirlerin yalnızca CMK kapsamına giren suçlar dolayısıyla işletilebileceği, disiplin soruşturması,

[72] Oysa CMK'nın 116. ve 119. maddeleri bağlamında arama yapılabilmesi için makul şüphe ve gecikmesinde sakınca bulunan hallerde Cumhuriyet Savcısı'nın yazılı emri yeterlidir.

[73] Bu kapsamda Yargıtay 11.Ceza Dairesi 16.04.2007 tarih ve E: 2005/6376, K: 2007/2551 sayılı kararında söz konusu prosedür ve ilkelere uyulmadığı gerekçesiyle ilk derece mahkemesinin kararını bozmuştur.

idari soruşturma benzeri diğer soruşturma usullerinde bu maddeden yararlanılamayacağı anlaşılmaktadır (Özen ve Baştürk 2011, 144).

4.2. İDARİ BİRİMLERCE YÜRÜTÜLEN İŞLEMLERDE UYGULANAN ADLİ BİLİŞİM MEVZUATI

Ülkemizde Kurum dışında kalan çeşitli idari otoritelere de, yürütülen denetim faaliyetleri kapsamında bilişim sistemleri üzerinde belirli ölçüde inceleme yapma yetkisi tanındığı bilinmektedir. Bu çerçevede takip eden bölümde Kurum gibi bağımsız idari otoritelerden olan SPK ve BDDK mevzuatı hakkında genel bilgilere yer verilmektedir.

4.2.1. SPK Mevzuatı

SPK'nın görev ve yetkilerini düzenleyen 6362 sayılı Sermaye Piyasası Kanunu'nun "Denetim faaliyetinin icrası" başlıklı 89. maddesinin birinci fıkrasında:

> Denetimle görevlendirilen personel[74], ilgili gerçek ve tüzel kişilerden bu Kanun ve ilgili diğer mevzuatın sermaye piyasasına ilişkin hükümleriyle ilgili görecekleri bilgi ve belgeleri istemeye, bunların vergi ile ilgili kayıtları dâhil olmak üzere tüm defter ve belgeleri ile **dijital ortamda tutulanlar dâhil tüm kayıtlar** ve sair bilgi ihtiva eden vasıtaları, **bilgi sistemlerini incelemeye, bunlara erişimin sağlanmasını istemeye ve bunların örneklerini almaya**, işlem ve hesaplarını denetlemeye, ilgililerden yazılı ve sözlü bilgi almaya, gerekli tutanakları düzenlemeye yetkilidir. (…) Aramada bulunan ve incelenmesine lüzum görülen defterler ve belgeler ayrıntılı bir tutanakla tespit olunur ve **yerinde incelemenin mümkün olmadığı hâllerde, muhafaza altına alınarak inceleme yapanın çalıştığı yere sevk edilir.**

ifadeleri yer almaktadır.

Yukarıda yer verilen hükümlerden anlaşılacağı üzere SPK'daki denetim faaliyetleri tıpkı Kurum'unda olduğu gibi meslek personeli eliyle yürütülmektedir. Denetimle görevlendirilen meslek personeli de denetim faaliyeti esnasında sermaye piyasası hükümleri dahilinde ilgili görecekleri bilgi ve belgeleri istemeye, dijital ortamda tutulanlar dahil tüm kayıtlar ve sair bilgi ihtiva eden vasıtaları, bilgi sistemlerinini incelemeye, bunlara erişiminin sağlanmasını istemeye ve bunların örneklerini almaya

[74] Sermaye Piyasası Kanunu'nun 88. maddesinde bu personelin, Kurul Başkanı tarafından görevlendirilen meslek personeli olduğu belirtilmektedir.

yetkilidir. Bu kapsamda bir denetim faaliyetinde incelemenin, mezkur mahalde bitirilememesi veya yapılamıyor olması halinde, ilgili evrakların muhafaza edilerek meslek personelinin çalıştığı yere götürülmek suretiyle tamamlanması öngörülmüştür.

Sonuç olarak ilgili maddenin imaj almayı ve alınan imajı analiz etmek için başka bir yere götürmeyi de içeren adli bilişim uygulamalarına cevaz verdiği görülmektedir.

4.2.2. BDDK Mevzuatı

BDDK'nın görev ve yetkilerini düzenleyen 5411 sayılı Bankacılık Kanunu'nun "Yerinde Denetim ve Gözetim" başlıklı 95. maddesinde, yerinde denetiminin BDDK Başkanı tarafından görevlendirilen kurumun meslek personellerince gerçekleştirileceği ifade edilmektedir. Söz konusu maddenin 8. fıkrasına göre ise;

> Kurum, bankalardan, bunların bağlı ortaklıklarından, nitelikli paya sahip oldukları ortaklıklardan, birlikte kontrol ettikleri ortaklıklardan, şubeleri ile temsilciliklerinden, destek hizmeti kuruluşlarından ve diğer gerçek ve tüzel kişilerden bu Kanun hükümleri ile ilgili görecekleri bütün bilgileri gizli dahi olsa istemeye, bunların vergiyle ilgili kayıtları dâhil olmak üzere tüm defter, kayıt ve belgelerini incelemeye yetkili olup, bilgi istenenler de istenilen bilgileri vermekle, defter, kayıt ve belgeleri incelemeye hazır bulundurmakla, **tüm bilgi işlem sistemini denetim amaçlarına uygun olarak Kurumun yerinde denetim yapan meslek personeline açmakla, verilerin güvenliğini sağlamakla** ve muhafaza etmek zorunda oldukları her türlü defter, belge ve karneler ile vermek zorunda bulundukları bilgilere ilişkin mikrofiş, mikrofilm, manyetik teyp, disket ve benzeri ortamlardaki **kayıtlarını ve bu kayıtlara erişim veya kayıtları okunabilir hale getirmek için gerekli tüm sistem ve şifrelerini inceleme için ibraz etmek ve işletmekle yükümlüdür**.

14.02.2005 tarihinde Bakanlar Kurulu tarafından kararlaştırılan ve 30.03.2005 tarihinde TBMM'ye sevk edilen Bankacılık Kanunu Tasarı'sının yukarıda yer verilen maddesine ilişkin gerekçesinde;

> Genellikle teknolojide yaşanan gelişmelerin getirdiği imkânlar kullanılarak bankacılığa ilişkin faaliyet alanlarında da gelişmeler görülmektedir. (…) Söz konusu teknolojik gelişmeler sonucunda denetim tekniklerinde ve denetim konularında da gelişmeler olmaktadır. Özellikle risk ölçümü, bilgi teknolojileri denetimi bu konudaki başlıca örneklerdir.

ifadelerine yer verilmiştir. Bu çerçevede BDDK meslek personelinin yerinde denetimler esnasında ilgili teşebbüsün bilişim sistemlerinde gerekli bilgilere erişme yetkisi olduğunu söylemek mümkündür. Ancak ilgili kanun maddesinin lafzından adli bilişim açısından önem arz eden "*imaj alma*" işlemine benzer bir anlam çıkarmak oldukça güç görünmektedir. Nitekim ilgili maddede zımnen de olsa "*suretini alma*", "*kopyalama*" benzeri ifadelere yer verilmediği dikkat çekmektedir. Bu kapsamda BDDK tarafından gerçekleştirilen yerinde denetimlerde, teşebbüslerin bilişim sistemlerini tümüyle meslek personelinin hizmetine açma sorumluluğu göze çarpsa da, ilgili maddeden gerekli görülen verilerin kopyalanabileceği sonucu çıkmamaktadır.

4.3. TÜRK REKABET MEVZUATI BAĞLAMINDA ADLİ BİLİŞİM HÜKÜM VE UYGULAMALARI

Bu bölümde, teşebbüste yapılan incelemelerde teşebbüs yönetici ve çalışanlarının bilgisayar ve diğer dijital araçlarının incelenip incelenemeyeceğine, bu incelemenin özel hayatın gizliliği kuralını ihlal edip etmeyeceğine, RKHK'nın adli bilişim uygulamalarına cevaz verip vermediğine, benzer uygulamalara idari yargının yaklaşımına ve bu konuda çeşitli çözüm önerilerine yer verilmektedir.

4.3.1. Rekabet Hukuku Bağlamında Adli Bilişimin Normlar Hiyerarşisindeki Yeri

Normlar hiyerarşisi, hukuk normlarının derece ve kuvvetini belirlemekte ve bir hukuk düzeninde var olan normların çokluğu anlamına gelmektedir (Kuluçlu 2008, 3). Gözler (2000, 33)'e göre ise bu normlar farklı kademelerde yer almakta, normlar arasında astlık üstlük ilişkisi bulunmakta ve her norm geçerliliğini bir üst normdan almaktadır. Bu çerçevede hukuk düzeni bir piramide benzetilecek olursa bu piramit (yukarıdan aşağıya); anayasa, kanun, yönetmelik ve adsız düzenleyici işlemlerden oluşan birçok normu barındırmaktadır (Kuluçlu 2008, 3-4).

Adli bilişim uygulamalarının hukuki geçerliliği (uygunluğu) açısından normlar hiyerarşisindeki yeri son derece mühimdir. Bu sorunun cevabı CMK'nın bilgisayarlarda ve bilgisayar kütüklerinde arama, kopyalama ve geçici el koymayı düzenleyen 134. maddesinin gerekçesinde şu şekilde verilmiştir:

> Madde, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve geçici elkoyma konularını düzenlemektedir. Bireye ait kişisel bilgiler üzerindeki hak, temel insan haklarından olduğundan hakkın kısıtlanabilmesi için yasal düzenleme gerekeceği açıktır.

Adli bilişim uygulamaları Anayasa'nın "*Temel Hak ve Ödevler*" başlıklı ikinci kısmında yer alan "Özel Hayatın Gizliliği", " *Haberleşme H*ürriyeti" gibi haklarla ilgili olup bu hakları ihlal etme riskini de taşımaktadır. Anayasa'nın 13. maddesine göre temel hak ve hürriyetler ancak kanunla sınırlanabilir. Gerek Anayasa'nın 13. maddesi gerekse CMK'nın 134. maddesinin gerekçesinden de anlaşılacağı üzere adli bilişim uygulamaları, şahısların doğrudan veya dolaylı olarak özel hayatlarını da ilgilendirdiğinden hukuki güvenlik açısından ancak **yasal düzenlemelerde yani kanunda** yer alması halinde mümkündür. Bu kapsamda RKHK'da adli bilişim uygulamalarına ilişkin bir hüküm olup olmadığının irdelenmesi gerekmektedir. RKHK'nın doğrudan adli bilişim uygulamalarına ilişkin olmasa da, yorum yoluyla genişletilebilecek hükümler içeren "Yerinde İnceleme" başlıklı 15. maddesindeki ifadeler şu şekildedir:

> Kurul, bu Kanunun kendisine verdiği görevleri yerine getirirken gerekli gördüğü hallerde, teşebbüs ve teşebbüs birliklerinde incelemelerde bulunabilir. Bu amaçla teşebbüslerin veya teşebbüs birliklerinin:
>
> a) Defterlerini, **her türlü evrak** ve belgelerini inceleyebilir ve **gerekirse suretlerini alabilir**,
>
> b) Belirli konularda yazılı veya sözlü açıklama isteyebilir,
>
> c) Teşebbüslerin her türlü mal varlığına ilişkin mahallinde incelemeler yapabilir.

İlgili maddenin, Anayasa'nın 13. maddesinde ve CMK'nın gerekçesinde öngörülen yasal düzenlemeyi şeklen karşıladığını söylemek mümkündür. Bununla birlikte anılan kanun maddesindeki "*her türlü evrak*" ve "*suretini alma*" ifadelerini, adli bilişim uygulamaları şeklinde yorumlamak da mümkündür. Bu bağlamda yukarıdaki maddenin Kurum'a adli bilişim uygulamalarının gerçekleştirilmesine ilişkin yetki verip vermediğiyle ilgili tartışma ileriki bölümlerde yapılmaktadır. Ancak, öncesinde RKHK'nın adli bilişimin konusunu teşkil eden bilgisayar ve dijital araçlarda inceleme yapmaya yetki verip vermediği irdelenmektedir.

4.3.2. Teşebbüs Çalışanlarının Bilgisayar ve Dijital Araçlarının İnceleme Kapsamındaki Hukuki Durumu

Kurum tarafından gerçekleştirilen yerinde incelemelerde teşebbüs çalışanlarının bilgisayarları ve e-postaları Kurum meslek personelince incelenmekte ve bu sayede elde edilen deliller birçok Kurul kararına dayanak oluşturmaktadır. Bu kapsamda yerinde inceleme esnasında incelenen teşebbüs çalışanına ait bilgisayarın hangi amaçla kullanıldığının net bir şekilde ortaya konulması, temel hak ve hürriyetlere müdahalenin sınırlarını belirleme açısından önem arz etmektedir.

Şahsi bir bilgisayar incelendiğinde o bilgisayarı kullanan kişinin özel verilerine ulaşılması kuvvetle muhtemeldir. Dolayısıyla şahsi bilgisayar, özel hayatın önemli bir unsuru niteliğindedir (Yavuzcan 2009, 1). Adli bilişim uygulaması idari veya adli usullerle gerçekleştirilmesine bakılmaksızın kişilerin özel hayatına müdahale riskini/tehlikesini doğurmaktadır. T.C. Anayasası'nın "özel hayatın gizliliği" başlıklı 20. maddesinde şu ifadeler bulunmaktadır:

> Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.
>
> Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırk sekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.

Yukarıda yer verilen hüküm ve hükümde yer alan sebeplerle özel hayatın gizliliğine ve bu çerçevede şahsi bilgisayarlara, CMK'nın 134. maddesinde belirtildiği üzere **ancak hâkim kararıyla** müdahale edileceği açıktır. Ancak bu hususun şahsa ait bilgisayarlar için geçerli olduğu, işyerinde iş için kullanılan yani şahsi olmayan bilgisayarlar için aynı korumanın geçerli olmadığı düşünülmektedir. Nitekim Yargıtay 9. Hukuk Dairesi[75] "*görevi gereği işverenin işlerini yürütmesi için işveren tarafından işçiye verilen bilgisayar*

[75] Yargıtay 9. Hukuk Dairesi, Karar Tarihi: 13.12.2010, Esas No: 2009/447, Karar No: 2010/37516.

ve e-mail adreslerini işverenin her zaman denetleme yetkisi bulunmaktadır" şeklinde bir karar vermiştir (Yurdseven 2012, 1). İşveren ve işçi arasında var olan özel hukuk ilişkisi içerisinde bile işçinin bilgisayarının (şirket malı olduğu için) işverence incelenebileceğinin yargı tarafından kabul edildiği görülmektedir. Öte yandan idari kuralların ihlal edilmesinin önlenmesi ve ihlalin tespit edilip yaptırım uygulanması amacıyla denetim faaliyetleri yürüten idari otoritelerin, kamu yararı ve hizmeti bakımından bu yetkiye sahip olmaları gerekmektedir. Zira kamu yararı söz konusu olduğunda, devletin ve kamunun menfaatinin bireysel menfaate tercih edildiği kabul edilmektedir.[76]

Öte yandan bir önceki kısımda yer verilen SPK ve BDDK mevzuatlarında da denetim/inceleme yetkilerini içeren ilgili kanun maddelerinin icrası için herhangi bir hâkim kararı ön görülmemiş ve bu husus anayasaya aykırı görülmemiştir.

Bununla birlikte ülkemizin de anayasa hükmü gereği bağlı ve kararlarını uygulamakla yükümlü olduğu AİHM[77] de Fransız Rekabet Otoritesi'nin teşebbüste gerçekleştirdiği yerinde inceleme esnasında teşebbüs çalışanlarının bilgisayarlarında inceleme yapılmasını ve e-posta dökümlerinin alınmasını AİHS'nin 8. maddesindeki "özel hayatın ve aile hayatının korunması" ilkesine aykırı görmemiştir. ABAD[78] ise, özel hayatın ve aile hayatının korunmasına yönelik AİHS'nin 8. maddesindeki korumanın şahıslar için geçerli olduğunu, bu korumanın işyerini kapsayacak şekilde genişletilemeyeceğini belirtmiştir (Yalçınkaya 2015, 36). Ancak ABAD, daha sonra işyerindeki cihazların incelenmesini salt özel hayatın gizliliğini ihlal olarak değerlendirmemekle birlikte; kamu yararı ile temel hak özgürlükler arasında denge kurulması gerektiği yaklaşımını benimsemiştir (Yalçınkaya 2015, 36).

4.3.3. RKHK'da Adli Bilişim Uygulamalarına Yönelik Yetki Tartışması

RKHK 15. maddede; Kurul'un emrinde çalışan meslek personeli aracılığıyla teşebbüs ve teşebbüs birliklerinde incelemelerde bulunabileceği, bu amaçla teşebbüs veya teşebbüs birliklerinin; defterlerini, her türlü evrak ve belgelerini inceleyebileceği

[76] "*Kamu yararı birey ve topluluk menfaatleri yarışmasında tercih edilen üst yardır. Kamu yararının topluluk, toplum ve devlet lehine bireysel veya topluluk yararından vazgeçme, topluluk, toplum ve devlet yararlarının yarışması durumunda da büyük olan menfaati koruma amaçlı olarak mahkeme kararlarında yargısal tercihte bulunma durumudur*." (Gül 2014, 537)

[77] Başvuru No: 63629/10 ve 60567/10,*Vinci Construction and GMT genie civil and services v. France*

[78] Cases 46/87 and 227/88, *Hoechst AG v. Commission*, [1989] ECR 2859, 21.9.1989 para. 18

ve gerekirse suretlerini alabileceği, belirli konularda yazılı ve sözlü açıklama isteyebileceği, teşebbüsün her türlü mal varlığına ilişkin mahallinde incelemeler yapabileceği belirtilmektedir.

Her ne kadar daha önceki kısımlarda yer verilen CMK'nın 134. maddesi, Sermaye Piyasası Kanunu'nun 89. maddesi kadar detaylı ve açıkça yazılmasa da RKHK'nın 15. maddesinde yer alan "*gerekirse suretini alabileceği*" hükmünün Kurum tarafından gerçekleştirilen yerinde incelemelerde adli bilişim uygulamasına cevaz verip vermediği tartışılması gereken bir husustur.

Gözler (2012, 49), bir anayasal organa verilen bir yetkinin belirli bir şeyi içerip içermediği konusunda tereddüdün ortaya çıkması durumunda, o yetkinin o şeyi içermediğini kabul etmek gerektiğini, anayasa hukukunda anayasal organların yetkisiz olmasının asıl, yetkili olmalarının istisna olduğunu ve istisnaların yorum yoluyla genişletilemeyeceğini ifade etmektedir.

Öte yandan Demircioğlu (2014, 53)'na göre, BDDK ve SPK mevzuatında meslek memurlarına ancak amaçla orantılı olarak özel hayata, haberleşme hürriyetine ve mahremiyet hakkına saygı çerçevesinde birtakım yetkiler verilmiş olmasına rağmen RKHK'da meslek personelinin, teşebbüsün bilgi işlem sistemine giriş yapmasına, kişilere ait dijital yazışmaları okumasına/el koymasına ve dijital belgeleri kopyalamasına izin veren herhangi bir düzenleme bulunmamaktadır.

Öztunç (2014, 11)'a göre ise CMK'daki arama ve el koyma işlemlerinde Anayasa hükümleri dikkate alınmasına rağmen aynı anayasal hükümlerin RKHK'nın 15. maddesi için dikkate alınmamış olması madde hükmünü Anayasaya aykırı kılmaktadır.

Yukarıda yer verilen görüşler çerçevesinde, kanunda açıkça yer almayan hiçbir işlemin idare tarafından gerçekleştirmesi mümkün görünmemektedir. Bu görüşün kabulü halinde Kurum'un yerinde incelemelerde uyguladığı, teşebbüs çalışanlarının bilgisayarını ve e-postalarını incelemesi usulü de hukuka aykırıdır. Bu halde yerinde inceleme esnasındaki e-posta incelemeleri Anayasanın "Haberleşme Hürriyeti" başlıklı 22. maddesinde yer alan

> Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır. Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya

> başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; haberleşme engellenemez ve gizliliğine dokunulamaz. Yetkili merciin kararı yirmi dört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar; aksi halde, karar kendiliğinden kalkar. İstisnaların uygulanacağı kamu kurum ve kuruluşları kanunda belirtilir.

hükmüne aykırı sayılmış olacaktır. Çünkü RKHK'nın 15. maddesinde ***"e-postaların incelenebileceği"*** *açıkça* yer almamaktadır. Oysa birçok Kurul kararına konu olan ve idari para cezası ile sonuçlanan soruşturmada deliller; teşebbüs yönetici veya çalışanlarının e-posta belgelerinden oluşmaktadır. Üstelik e-posta belgelerine dayanarak verilen birçok karar Danıştay'ın denetiminden geçmiş, Danıştay e-posta incelemelerinin Anayasa'ya, kanuna aykırı olduğu yönünde bir karar vermemiş, e-posta belgelerine dayanak yapılarak verilen idari para cezalarını da onamıştır.

Örneğin Kurul'un *ABC Türkiye*[79] Kararı'nda teşebbüs birliği ile bağımsız olmayan hukuk müşaviri arasında gerçekleşen e-posta mesajı delil olarak alınmış ve kullanılmıştır[80]. Danıştay 13. Dairesi[81] ise söz konusu delili hukuka aykırı görmemiştir. Yine Kurul'un *EBT*[82] Kararı'nda delillerden biri olan bilgisayarı incelenen teşebbüs yetkililerinin e-posta mesajlarının delil olarak kullanılmasını Danıştay 13. Dairesi[83] hukuka aykırı bulmamıştır. Üstelik delillere konu olan bilgisayar incelemesi ve e-postalar Danıştay İdari Dava Daireleri Kurulu'nca[84] (İDDK) incelenmiş ve hukuka uygun bulunmuştur. Kurul'un *Tıbbi Sarf Malzemeleri*[85] kararına konu olan delillerden biri olan teşebbüs yetkililerinin e-posta yazışmaları, ilgili teşebbüslerden biri tarafından idari yargıya taşınmıştır. Söz konusu davada, davacı teşebbüs e-postaların hukuka aykırı

[79] Kurul'un 24.4.2007 tarihli, 07-34/347-127 sayılı kararı
[80] E-postaların delil olarak kullanıldığı benzer nitelikte Kurul kararları için bkz: 20.5.2008 tarihli, 08-34/456-161 sayılı *Akücüler*, 9.12.2009 tarihli, 09-58/1405-367 sayılı *Reysaş*, 13.10.2009 tarihli, 09-46/1154-290 sayılı *CNR Fuarcılık*, 25.11.2009 tarihli, 09-57/1393-362 sayılı *Beyaz Et* kararları.
[81] Danıştay'ın 24.6.2008 tarihli, E.2006/2143, K.2008/5037 sayılı kararı
[82] Kurul'un 4.7.2007 tarihli, 07-56/672-209 sayılı kararı
[83] Danıştay'ın 9.5.2012 tarihli, E.2008/9443, K. 2012/969 sayılı kararı
[84] İDDK'nın 27.11.2014 tarihli, E. 2012/2184, K. 2014/4526 sayılı kararı
[85] Kurul'un 16.3.2007 tarihli, 07-24/236-76 sayılı kararı

olarak elde edildiğini iddia etmiştir. Buna karşılık Danıştay 13. Dairesi[86] e-postaları Kurul'un kararına konu olan delillerden biri olarak açıkça zikrederken, bunların hukuka aykırı olduğu iddialarına itibar etmemiştir. Anayasa'nın 152. maddesine göre;

> …bir davaya bakmakta olan mahkeme, uygulanacak bir kanun veya kanun hükmünde kararnamenin hükümlerini anayasaya aykırı görürse veya taraflardan birinin ileri sürdüğü aykırılık iddiasının ciddî olduğu kanısına varırsa, AYM'nin bu konuda vereceği karara kadar davayı geri bırakır.

Dolayısıyla Danıştay, yukarıda bahsi geçen kararlarda teşebbüs çalışanlarının bilgisayarlarında elde edilen e-postaları Anayasa'nın "Haberleşme Hürriyeti" veya "Özel Hayatın Gizliliği" kapsamında değerlendirmemiş, bunlara ilişkin yapılan yerinde incelemeleri Anayasa'ya veya kanuna aykırı bulmamıştır. Nitekim hukuka uygunluk denetiminden geçmiş birçok kararı ve uygulaması ışığında, mevcut durumda Kurum'un, bilişim sistemlerinde inceleme yapmasının, hukuka uygunluk konusunda herhangi bir çelişki olmadığı görülmektedir.

Öte yandan RKHK'nın 15. maddesinde belirtilen "***her türlü evrak***"ın "***suretini alma***" işlemi özünde kopyasını alma işlemi olup, adli bilişimin en önemli konusu olan imaj alma da bilgisayar veya bilgisayar benzeri dijital cihazlardaki belgelerin kopyalarının alınmasıdır. Nitekim bir sonraki bölümde detaylıca irdelenecek olan "*Rekabetin Korunması Hakkında Kanun'da Değişiklikler Öngören Kanun Tasarısı*"nda (Tasarı) değişiklik öngörülen 15. maddede "***her türlü ortamda tutulan veri***" ve "***her türlü kopya ve çıktılarını***" ifadeleri tercih edilmiştir. Anılan Tasarı maddesinin gerekçesinde yerinde incelemelerde, defterlerin veya her türlü ortamda tutulan verilerin, bilgi ve belgelerin incelenebilmesi, bunların bulunduğu **elektronik ortamların imajlarının alınması dâhil her türlü kopya ve çıktılarının alınabilmesi** yetkisinin tanımlandığı belirtilmiştir.

Sonuç olarak mevcut durumda; RKHK'nın, yerinde incelemede görevli meslek personeline bilgisayar sistemlerinde detaylı aramalar yapma, teşebbüsteki bilgisayarların imajını alma ve alınan imajı teşebbüste analiz etme konusunda yetki verdiği, ancak

[86] Danıştay'ın 16.2.2010 tarihli, E. 2007/11670, K. 2010/1346 sayılı kararı

alınan imajı analiz edebilmek amacıyla teşebbüs dışındaki bir yere (Kurum vb.) taşıma noktasında yetki vermediği düşünülmektedir.

Yukarıda yer verilen tartışmalara son vermek amacıyla tam ve işlevsel bir adli bilişim uygulaması gerçekleştirmeye yönelik çeşitli adımlar atılması gerektiği düşünülmektedir. İlgili adımlara ilişkin önerilere takip eden bölümde yer verilmektedir.

4.3.4. Adli Bilişim Uygulamalarına İlişkin Çözüm Önerileri

Kurum'un mevcut uygulamaları dikkate alındığında adli bilişim açısından üç farklı durumun olduğunu söylemek mümkündür. Bunlardan birincisi hali hazırda yapılan e-posta ve bilgisayar aramalarıdır. Kurum'un yerinde incelemeler esnasında teşebbüs bilgisayar ve e-postalarındaki aramaları kolaylaştırmak amacıyla özel yazılımlar kullanmadığı bilinmektedir. Ancak bu durum bilgisayarlarda yapılan aramaların, yalnızca ilgili bilgisayarda kurulu olan işletim sisteminin yetenekleriyle sınırlı kalmasına sebep olmakta, aramaların etkinliğini azaltmakta ve istenilen delillere ulaşmayı engellemektedir. Bu kapsamda yerinde incelemelerde teşebbüs bilgisayarlarına, aramaları kolaylaştıracak özel yazılımlar kurulabilmesinin, bu amaçla gerekli yazılımların Kurum'ca tedarik edilmesinin, yerinde incelemede görevlendirilecek personele bu yazılımların eğitiminin verilmesinin ve aramaların anılan yazılımlar vasıtasıyla yapılmasının delil arama etkinliğini artıracağı düşünülmektedir.

İkinci durumda ise, yerinde incelemelerde RKHK'nın zımnen yetki verdiği imaj alma işleminin gerçekleştirilmesi hususu söz konusudur. Böylesi bir durumda izlenecek yol ve yöntemlere ilişkin üçüncü bölümde açıklanan AB pratiklerinin örnek alınmasının ve bu kapsamda imaj alma ve diğer teknik işlemler için yazılım ve donanımların Kurum'ca tedarik edilmesinin, imaj alma işleminin uzmanlık bilgisi gerektirmesi sebebiyle uzman personel istihdamı ile bu personelin eğitimlerinin artırılmasının uygun olduğu düşünülmektedir. Ancak teşebbüs mülkünden alınan imajın Kurum binasına getirilmesi ve Kurum'da incelenmesi hususları RKHK'da açıkça veya zımnen yer almamaktadır. Bu bağlamda ortaya çıkabilecek problemler için hukuki metinlerin düzenlenmesi ihtiyacı doğmaktadır.

Üçüncü durum şeklinde nitelendirilebilecek olan bu durumda ise öncelikle, hukuki güvence amacıyla kanun metinlerindeki yetkilerin, farklı yorumlara ve tartışmalara yer

vermeyecek şekilde net ve açık olarak ortaya konmasının son derece önemli olduğu düşünülmektedir. Bu kapsamda daha önce de ifade edildiği üzere, adli bilişimin rekabet hukuku açısından önemi dikkate alındığında; Kurum tarafından hazırlanmış olan *Tasarı*'da yerinde inceleme esnasında adli bilişim uygulamalarına açıkça cevaz veren ve bu uygulamaların hukukiliğini zedelememesi açısından temel prosedürleri içeren hükümlerin eklenmesi en uygun yoldur. Nitekim Tasarı'da değişiklik öngörülen 15. maddede şu ifadeler kullanılmıştır:

> Kurul, bu Kanunun kendisine verdiği görevleri yerine getirirken gerekli gördüğü hallerde, teşebbüs ve teşebbüs birliklerinde incelemelerde bulunabilir. Bu amaçla teşebbüslerin veya teşebbüs birliklerinin ve bunların yöneticilerinin ve çalışanlarının:
>
> a) Defterlerini veya **her türlü ortamda tutulan veri** ve belgelerini inceleyebilir, bunların **her türlü kopya ve çıktılarını** alabilir.

Bununla birlikte Tasarı'nın gerekçesinde yer alan şu ifadeler oldukça dikkat çekicidir:

> Yapılan değişiklikle, özellikle kartellerin ortaya çıkarılmasında hayati önemi haiz olan yerinde inceleme yetkisinin kapsamı belirginleştirilmiştir. Bu bağlamda, yerinde incelemelerde; defterlerin veya her türlü ortamda tutulan verilerin, bilgi ve belgelerin incelenebilmesi, bunların bulunduğu **elektronik ortamların imajlarının alınması dâhil her türlü kopya ve çıktılarının alınabilmesi** yetkisi (…) tanımlanmıştır.

Tasarı'nın bu haliyle yukarıda ifade edilen adli bilişim uygulamalarından birinci (detaylı arama) ve ikinci duruma (imaj alma) cevaz verdiği, üçüncü duruma (alınan imajın Kurum'da analiz edilebilmesi) yetki vermediği görülmektedir. Farklı yorum ve eleştirilere sebebiyet vermemek adına Tasarı metninde, SPK mevzuatında olduğu gibi; "**dijital ortamda tutulanlar dâhil tüm kayıtlar**", "**bilgi sistemlerini incelemeye, bunlara erişimin sağlanmasını istemeye ve bunların örneklerini almaya**" ve "**yerinde incelemenin mümkün olmadığı hâllerde, muhafaza altına alınarak inceleme yapanın çalıştığı yere sevk edilir**" ifadelerinin tercih edilmesinin daha doğru olduğu düşünülmektedir.

Çalışmanın üçüncü bölümündeki AB mevzuat ve uygulamalarında görüldüğü üzere AB, rekabet ihlali incelemelerindeki adli bilişim uygulamalarına yasada yer vermemiştir. Ancak şurası açıktır ki hukuki güvenliğin en önemli ilkesi hukuki belirlilik, yani ilgililerin karşılaşabilecekleri durumları önceden açıkça ve net olarak bilebilmesidir.

AB'de rekabet ihlallerine ilişkin inceleme yetkileri 2003 yılında yürürlüğe giren 1/2003 sayılı AB Konsey Tüzüğü ile belirlenmiştir. Ayrıca Komisyon incelemelerde izlenecek yol ve yöntemleri detaylı bir şekilde izah etmek amacıyla "*1/2003 Sayılı Tüzüğün 20. Maddesinin 4. Fıkrası Uyarınca Gerçekleştirilen İncelemelere İlişkin Açıklayıcı Not"* isimli bir çalışma yayımlamıştır. Buradan hareketle söz konusu Tasarı'nın yasalaşamaması halinde Kurul'un, daha önce çıkardığı yönetmelikler gibi, RKHK'nın 27. maddesinin kendisine verdiği ikincil mevzuat yapabilme yetkisini kullanarak RKHK'nın 15. maddesi çerçevesinde adli bilişim uygulaması ve prosedürlerini içeren bir yönetmelik hazırlamasının uygun olduğu düşünülmektedir.[87] Söz konusu Yönetmelik'te, yerinde incelemede teknik işlemlerle görevli personelin özellikleri, yerinde inceleme esnasında ihtiyaç halinde adli bilişim süreçlerinin nasıl hukuka uygun bir şekilde ve kimler tarafından gerçekleştirilebileceği, teşebbüs temsilcilerinin bilgilenme hakkına ilişkin hususlar, teşebbüs çalışanlarının inceleme konusunu oluşturmayan dosyalarına ilişkin ayıklama talepleri ile ilgili hususlar, kopyalanan verilerin hukuka uygun bir şekilde muhafazası, analiz süreçleri ve öngörülen vakitte bitirilemeyen yerinde incelemelerde yapılacak işlemlere ilişkin hususlar yer almalıdır. Bu ilkeler çerçevesinde hazırlanmış olan Yönetmelik Tasarısı Önerisi Ek-1'de bulunmaktadır.

[87] Yönetmeliğin henüz uygulanmadan, iptali istemiyle ilgili taraflarca idari yargıya götürülmesi halinde RKHK'nın 15. maddesinin adli bilişim uygulamalarına cevaz verip vermediği yönündeki hukuki belirsizlik yargı tarafından ortadan kaldırılmış olabilecektir.

SONUÇ

Rekabet ihlallerinin serbest piyasa sistemi üzerinde önemli ölçüde etkileri olduğu bilinen bir gerçekliktir. Serbest piyasa düzeninin sağlıklı işlemesi konusunda önemli bir görevi olan Kurum'un da serbest piyasa düzenini bozan fiil ve eylemleri ortaya çıkarması ve bunun neticesinde ihlalde bulunanlara idari yaptırım uygulaması birincil görevidir.

Teknolojinin gelişimine paralel olarak günümüzde klasik delillerin yerini dijital deliller almakta ve rekabet ihlalini ortaya koyan deliller de bu çerçevede bilgisayar donanım ve ağlarının içerisinde ve mobil cihazların hafızalarında bulunmaktadır. Dijital ortamlarda yer alan ve rekabete aykırı fiilleri işaret eden bilgi ve belgeler silinmiş, gizlenmiş, şifrelenmiş dahi olsa adli bilişim uygulamaları ile ortaya çıkarılabilmektedir. Bu kapsamda dijital delilin hukuka uygun bir şekilde elde edilmesi, muhafaza edilmesi, kuşkuya mahal vermeyecek şekilde analiz edilmesi ve karar verici mercilere sunulması son derece önemli ve titizlikle yürütülmesi gereken bir süreçtir.

Adli bilişimin rekabet otoriteleri açısından uygulanabilirliğine en önemli örneklerden birisi AB Komisyonu'dur. Komisyon bu kapsamda, yerinde inceleme için gittiği teşebbüslerde özel yazılım ve donanımlar kullanmak suretiyle ilgililerin bilgisayarlarındaki tüm verileri hangi amaçla kullandığını dikkate alarak kopyalamaktadır. Daha sonraki aşamada kopyalanan veriler yüksek işlem kapasiteli cihazlara yüklenerek ayrıştırılmakta ve yerinde incelemede görevli uzmanların kullanımına açılmaktadır. İncelemenin öngörülen zamanda bitirilememesi durumunda ise, Komisyon'un inceleme yaptığı odayı mühürleme yetkisi mevcuttur. Rekabet ihlallerinin kısmen adli süreçler dâhilinde incelendiği ABD'de ise DOJ, FBI ajanları ile birlikte teşebbüs mülküne girerek ilgili cihazlarda adli bilişim işlemleri yapabilmektedir.

Ülkemizde ise adli bilişim uygulamalarına CMK kapsamında yer verildiği görülmektedir. CMK'da herhangi bir suç tipi ayırımına gidilmeksizin delil elde edilebilmesini teminen adli bilişim uygulamaları öngörülmekte, bazı eksiklikler dışında bu sürecin sıkı kurallara bağlandığı ve delil elde edilme sürecinde şüphelinin haklarının muhafaza edilmeye çalışıldığı görülmektedir. Öte yandan Türk idari teşkilatı dâhilinde de SPK ve BDDK mevzuatlarında adli bilişim uygulamalarına yer verilmektedir. RKHK kapsamında ise adli bilişim uygulamalarına yönelik, anılan idari otoritelerin mevzuatlarında olduğu gibi açık bir ifade olmadığı dikkat çekmektedir.

Adli bilişimin rekabet ihlallerinin ortaya çıkartılması hususundaki önemi dikkate alındığında, adli bilişime ilişkin yetkilerin, gündemde olan Rekabetin Korunması Hakkında Kanunda Değişiklik Öngören Kanun Tasarısı'na açık ve anlaşılır şekilde yazılarak yasalaşmasının uygun olduğu düşünülmektedir. Ancak bunun mümkün olmaması durumunda, RKHK'nın Kurul'a verdiği yetkiler çerçevesinde ikincil düzenleme yapılması ve bu düzenleme yoluyla hukuki belirsizliğin giderilebileceği değerlendirilmektedir. Bu durumun da mümkün olmaması halinde, Kurum'un mevcut yerinde inceleme yetkileri dâhilinde bilgisayar terimlerini arama seçeneklerinin genişletilmesinin uygun olduğu düşünülmektedir. Bu kapsamda Kurum tarafından satın alınacak özel yazılımlar sayesinde, uzmanların yerinde incelemelerde daha etkin aramalar yapacağı ve delil bulma konusundaki başarımın artacağı hususu açıktır.

Sonuç olarak adli bilişim uygulamaları sayesinde mevcut klasik yöntemlerle elde edilmesi mümkün olmayan bilgi ve belgelerin ortaya çıkarılmasının sağlanması, ihlal yapma güdüsündeki teşebbüslerin motivasyonlarını düşürecek; böylece serbest piyasa sistemi en üst düzeyde korunmuş olacaktır.

ABSTRACT

There is no doubt that, the most important tool of gathering evidence in *competition law investigation*s is *dawn raids* conducted in premises of *undertakings*. The efficiency and success of these dawn raids heavily relies on finding **material evidences** regarding the alleged infringements. However, in parallel to the developments in technology, it becomes more and more difficult for competition authorities to detect infringements and find material evidences by using conventional methods of inspection. At this point, using **IT Forensic Tools** emerges as an indispensable element of effective competition law enforcement. Correspondingly, this paper primarily focuses on technical and legal aspects of using IT Forensic techniques in competition law enforcement. In this regard, throughout this paper, first, technical aspects and legal framework of using IT Forensic Tools in EU, US and Turkey competition laws are examined in the light of selected cases from these jurisdictions, and then *suggestions* are made to improve the effectiveness of the dawn raids of *Turkish Competition Authority*.

KAYNAKÇA

ACPO (2012), "Good Practice Guide for Computer-Based Electronic Evidence Version 5", England Wales & N. Ireland Association of Chief Police Officers, http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf, Erişim Tarihi:19.10.2015.

AHİ, G. (2009), "Adli Bilişim ve Hukuk", *Güncel Hukuk Dergisi*, Mart 2009 Sayısı, İstanbul.

AK (2013), *Avrupa Konseyi Dijital Delil Rehberi*, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp, Erişim Tarihi: 15.10.2015.

AKTEKİN, E. (2013), "Avrupa Komisyonu Yerinde İncelemelere İlişkin Bilgilendirme Notunu Güncelledi", Rekabet Yazısı, http://www.rekabet.gov.tr/tr-TR/Rekabet-Yazisi/Avrupa-Komisyonu-Yerinde-Incelemelere-Iliskin-Bilgilendirme-Notunu-Guncelledi, Erişim Tarihi: 25.11.2015.

AYDOĞAN, H. (2009), "Adli Bilişimde Yeni Elektronik Delil Elde Etme Yöntemleri", Polis Akademisi Güvenlik Bilimleri Enstitüsü Yüksek Lisans Tezleri Serisi, Ankara.

AYERS, R., S. BROTHERS ve W. JANSEN (2013), *Guidelines on Mobile Device Forensics (Draft) Recommendations of the National Institute of Standards and Technology*, Special Publication 800-101, Revision 1 (Draft).

BALI, Y. (2015a), "Wipe (Kalıcı silme=Data üzerine data yazma) işleminden sonra veri kurtarılabilir mi?", http://www.dijitaldeliller.com/wipe_kurtarma.html, Erişim Tarihi:24.11.2015.

BALI, Y. (2015b), "Hard Diskteki Alanlar", http://www.dijitaldeliller.com/harddiskteki-alanlar, Erişim Tarihi:12.01.2016.

BEEBE N. L., CLARK J. G. (2007), "Digital Forensic Text String Searching: Improving Information Retrieval Effectiveness By Thematically Clustering Search Results", Elsevier Digital Investigation Journal, 49–54 http://www.dfrws.org/2007/proceedings/p49-beebe.pdf, Erişim Tarihi: 13.03.2016.

BELLOVIN S.M., M. BLAZE ve S. LANDAU (2015), "Searching Securely: Technical Issues with Warrants for Remote Search", Workshop on Surveillance and Technology, Philedelphia.

BERBER, F. (2015), "Adli Bilişimde Kullanılan İmaj Alma Yazılımları", http://fatihberber.com/2-adli-bilisimde-kullanilan-imaj-alma-yazilimlari/, Erişim Tarihi: 07.03.2016.

BOSTANCI, Ü ve R. BENZER (2015), "Türk Hukuk Sisteminde Bilgisayarlarda Arama, Kopyalama ve El Koyma", *International Journal of Human Sciences*, 12(2), s.1192-1229.

BROWN, C. L.T. (2006), *Computer Evidence Collection and Preservation*, Charles River Media, Massachusetts.

BROWN, M. (2015), "EU Dawn Raids: the Updated Inspection Explanatory Note Sends a Clear Message", https://www.mayerbrown.com/EU-Dawn-Raids-the-Updated-Inspection-Explanatory-Note-Sends-a-Clear-Message-10-01-2015/, Erişim Tarihi: 09.03.2016.

CASEY, E. (2004), *Digital Evidence and Computer Crime: Forensic Science, Computers,and the Internet*, 2nd Ed., Academic Press.

CELLEBRITE (2014), "Cellebrite's Outlook For The Mobile Forensics Industry 2014", http://www.cellebrite.com/collateral/OUTLOOK_FOR_THE_MOBILE_FORENSICS_INDUSTRY_2014_WP.pdf, Erişim Tarihi:13.01.2016.

CENTEL, N. ve H. ZAFER (2014), *Ceza Muhakemesi Hukuku*, Beta Yayınevi, Eylül 2014, İstanbul.

COŞGUN, H. (2009), ABD, AB ve Türk Rekabet Otoritelerinin Bilgi Edinme Yetkileri ve Bilgi Kaynağı Olarak Fonksiyonları, Rekabet Kurumu Uzmanlık Tezleri Serisi No:107, Ankara.

ÇAKIR, H. ve M. S. KILIÇ (2013), "Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bir Bakış", *Polis Bilimleri Dergisi,* 15(3)2013, s.23-44.

DANIEL, L. E. Ve L. E. DANIEL (2011), "Digital Forensic: The Subdisciplines", *Digital Forensic for Legal Professions*, s. 17-23.

DEMİRCİOĞLU, M.Y. (2014), "Rekabet Kurumu Tarafından Yürütülen Soruşturmalarda Teşebbüsler Arası Elektronik Yazışmaların Delil Değeri", *Bankacılar Dergisi*, Sayı 88.

DEVRİM, F. (2009), İdare Hukukunda ve Ceza Hukukunda Kartellerle Mücadelede Soruşturma Yöntemleri, Rekabet Kurumu Uzmanlık Tezleri Serisi, No:102, Ankara.

DÜLGER, M.V. ve G. MODOĞLU (2013), *Bilişim Suçları, Soruşturma Ve Kovuşturma Yöntemleri İle İnternet Ve İletişim Hukuku Uygulama Rehberi*, Türk Ceza Adalet Sisteminin Etkinliğinin Geliştirilmesi, Avrupa Birliği - Avrupa Konseyi Ortak Projesi, Ankara.

EKİM, A. (2013), "Mobil Cihazlarda Adli Bilişim ve Malware Analizi", 1st International Symposium on Digital Forensics and Security (ISDFS'13), Elazığ.

EKİZER, A. H. (2014), "Adli Bilişim (Computer Forensics)", http://www.ekizer.net/adli-bilisim-computer-forensics, Erişim Tarihi:12.10.2015.

ERPS, D.V. (2013), "Digital evidence gathering : An up-date : The EC Practice", *Concurrences*, No:2-2013, s.213-215, http://www.aedc.es/wp-content/uploads/2013/09/20130708155558824.pdf, Erişim Tarihi: 02.01.2016.

EVERETT, J. C., S. P. DUFFY, D. A. SCHIFFER ve D. BRENNEMAN (2012), "Handbook On Multijurisdictional Competition Law Investigations", http://www.americanbar.org/content/dam/aba/publications/antitrust_law/at311000_treatise_unitedstates.authcheckdam.pdf, Erişim Tarihi:26.01.2016.

GÖKSU, M. (2010), "Hukuk Yargılamasında Elektronik Delil", Ankara Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk (Medeni Usul Ve İcra-İflas Hukuku) Anabilim Dalı, Doktora Tezi.

GÖZLER, K. (2000), "İnsan Hakları Normlarının Anayaüstülüğü Sorunu", *Türkiye'de İnsan Hakları,* Ankara, TODAİE Yayını, 2000, s.25-46.

GÖZLER, K (2012), "*Yorum İlkeleri*", Kamu Hukukçuları Platformu, Anayasa Hukukunda Yorum ve Norm Somutlaştırması, Ankara, Türkiye Barolar Birliği, Yayın No: 236.

GÜL, İ. (2014), "Danıştay Kararlarında Kamu Yararı Kavramı", *Ankara Barosu Dergisi*, 2014/2, s.533-552

GÜLLÜCE, Y. Z. ve R. BENZER (2015), "Adli bilişimde hard disk arızaları ve arızalı disklerden veri kurtarma yöntemleri", *International Journal of Human Sciences*, Volume:12, Issue:1, Year:2015, s.206-225.

GÜNDÜZ, H. (2009), "Avrupa İnsan Hakları Sözleşmesi'nin Rekabet Hukuku Uygulamasına Etkisi", Rekabet Kurumu Uzmanlık Tezleri Serisi No. 99, Ankara.

HENKOĞLU, T. (2014), *Adli Bilişim: Dijital Delillerin Elde Edilmesi ve Analizi*, Pusula Yayınları Güncellenmiş 2. Baskı, Ankara.

ICN (2014), *Anti Cartel Enforcement Manual-Chapter 3:Digital Evidence Gathering*, Cartel Enforcement Subgroup-2 ICN Cartels Working Group.

KARAASLAN, E., M. DEMİR ve V. FETAH (2016), "Akıllı Telefonlarda Gizlilik ve Mahremiyet: Durum Saptaması ve Öneriler", 18. Akademik Bilişim Konferansı, Adnan Menderes Üniversitesi, *Bildiriler Kitabı*, No:42, Aydın.

KARABULUT, F., E. KARAPAZARLIOĞLU ve H. TOSUN (2015), "Ceza Muhakemesinde Delil Kavramı Ve Kovuşturma Sürecinde Hâkimlerin Delil Algısı", *TBB Dergisi,* 2015 (120), s.385-422.

KAYGISIZ, M. (2008), *Adli Bilimler Suç Analizi*, Adalet Yayınevi, Ankara.

KEKEVİ, G. (2008), "ABD, AB ve Türk Rekabet Hukukunda Kartellerle Mücadele", Rekabet Kurumu Lisansüstü Tez Serisi, No: 15, Ankara.

KENT, K., S. CHEVALİER, T. GRANCE ve H. DANG (2006), *Guide to Integrating Forensic Techniquesinto Incident Response Recommendations, Recommendations of the National Institute of Standards and Technology*, http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf, (11.01.2016).

KERSE, C. ve N. KHAN (2005), *EC Antitrust Procedure*, Sweet & Maxwell, London.

KESER BERBER, L. (2004), *Adli Bilişim*, Yetkin Yayınları, Ankara.

KINSELLA, S. (2015), "Call My Bluff", Kluwe Competition Law Blog, http://kluwercompetitionlawblog.com/2015/10/20/call-my-bluff/, Erişim Tarihi:09.03.2016.

KIZILYAR, M. (2014), " Ceza Yargılamasında Dijital Verilerin Delil Değeri", *Adalet Dergisi*, Sayı:50, s.72-89.

KLEIMAN, D., K. CARDWELL, T. CLINTON, M. CROSS, M. GREGG, J. VARSALONE, ve C. WRIGHT (2007). *The Official CHFI Exam 312-49 Study Guide For Computer Hacking Forensics Investigators*, Syngress Publishing, USA.

KRUISE, W. G. ve J. G. HEISER (2002), *Computer Forensics Incident Response Essentials*, Addison-Wesley, Indianapolis.

KULUÇLU, E. (2008), "Türk Hukuk Sisteminde Normlar Hiyerarşisi ve Sayıştay Denetimine Etkileri", *Sayıştay Dergisi*, Ekim-Aralık 2008, Sayı: 71.

KUSCHEWSKY, M. ve D. GERADIN (2013), "Data Protection in the Context of Competition Law Investigations: An Overview of the Challenges", *Tilburg Law School Legal Studies Research Paper Series,* No. 020/2013, Tilburg University.

LYLE, J. R. (2003), "National Institute of Standards and Technology 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, Erişim Tarihi: 04.01.2016.

LYLE, J. R., (2006), "A strategy for testing hardware write block devices", *Digital*

Investigation 3S (2006) S3–S9, National Institute of Standards and Technology (NIST), USA.

MAHAJAN, A., M. S. Dahiya ve H. P. Sanghvi (2013), "Forensic Analysis of Instant Messenger Applications on Android Devices", *International Journal of Computer Applications* (0975 – 8887), Volume 68– No.8, April 2013.

MONTI, M. (2001), "Why Should We Concerned with Cartels and Collusive Behaviour?", Fighting Cartels-Why and How?: Swedish Competition Authority (Konkurrensverket), Stockholm, s. 14-22.

NIST (2004), *Hardware Write Blocker Device (HWB) Specification*, National Instiute of Standarts and Technology, Version 2.0 May 19, 2004.

OECD (1998), "Recommendation of the Council Concerning Effective Action against Hard Core Cartels", https://www.oecd.org/daf/competition/2350130.pdf, Erişim Tarihi: 29.03.2016.

ÖZBEK, M. (2013), "Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları", *1. International Symposium On Digital Forensics And Security Proceding Book*, 255-262.

ÖZDEMİR, A. (2013), "Adli Bilişim Araçları", *1. International Symposium On Digital Forensics And Security Proceding Book*, s.1-4.

ÖZEN, B., İ. BAŞTÜRK (2011), *Temel Hak ve Özgürlükler Bağlamında Bilişim İnternet ve Ceza Hukuku*, Adalet Yayınevi, 1. Baskı, ANKARA.

ÖZEN, M. ve G. ÖZOCAK (2015), "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)", *Ankara Barosu Dergisi*, 2015/ 1, s.41-79.

ÖZOCAK, G.(2011), "Ceza Muhakemesinde Elektronik Delillerin Tespiti ve Toplanması", İzmir 2. Uluslararası Bilişim Hukuku Kurultayı 17-19 Kasım 2011 Bildiriler Kitabı, 110-125.

ÖZTUNÇ, T.(2014), "Rekabetin Korunması Hakkında Kanun'un 15. Maddesinin Anayasaya Ve Aihs'ne Aykırılığı", Rekabet Forumu, Sayı 84, Mayıs, 2014.

ÖZTÜRKCİ, H. (2014), "Adli Bilişim İncelemelerinde Sabit Disk İmajları–Giriş", http://halilozturkci.com/adli-bilisim-incelemelerinde-sabit-disk-imajlari, Erişim Tarihi: 13.01.2016.

PINAR, H. (2011), "Avrupa Birliği Rekabet Hukukunda AB Komisyonunun İnceleme Yetkisi", *Rekabet Dergisi 2011*, 12(4): 127-154.

POLLEY, R. (2013), "Digital Evidence Gathering in Dawn Raids- a Risk fort he

Company's Rights of Defence and Fundamental Rights", 20th St. Gallen International Competition Law Forum ICF, 4-5 Nisan 2013.

SAĞIROĞLU, Ş. ve M. KARAMAN, "Adli Bilişim", *Telepati Dergisi*, Sayı: 203, Ağustos 2012.

SANLI, K. C. (2013), "Avrupa Birliği Rekabet Hukuku ve Politikası", *Avrupa Birliği Hakkında Merak Ettikleriniz*, s.200-211.

SARSIKOĞLU, Ş. (2015), "Ceza Muhakemesinde Delil Ve İspat Hukuku Açısından Elektronik Delil (E-Delil) Kavramı", *TAAD*, Yıl:6, Sayı:22 (Temmuz 2015).

SAY, K. (2006), "Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi", Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, (Yayımlanmamış Yüksek Lisans Tezi), Ankara.

SEVİMLİ, G. (2007), "Bilgisayar ve Bilgisayar Kütüklerine El Konulması Ve Uygulamadaki Sorunlar", İstanbul Barosu Dergisi, Cilt: 81 Sayı: 3 993-1000.

SHINDER, D.L. (2002), *Scene Of The CyberCrime*, Syngress Publishing, Rockland USA.

SÖZLÜK (2014), *Rekabet Terimleri Sözlüğü,* Rekabet Kurumu, Ankara.

SÜZEN, A.A., K. TAŞDELEN ve E.U. KÜÇÜKSİLLE (2016), "Adli Bilişimde Uçucu Veri Analizi ve Yöntemleri", XVIII. Akademik Bilişim Konferansı, *Bildiriler Kitabı*, Aydın.

ŞENGÜL, G., F.K. ATSAN ve A. BOSTAN (2014), "Adli Bilişim Alanındaki Mevcut Problemler, Çözüm Önerileri ve Gelecek Öngörüleri", *1. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, s.95-101, İstanbul.

ŞİMŞEK, Y., M. DURMAZ, ve N. KARATAŞ (2012), *Dijital Delil Yönetimi*, Polis Akademisi Yayınları, Ankara.

TANENBAUM, A.S. (2009), *Modern Operating Systems*, Third Edition, Pearson Education International.

THAKUR, N.S. (2013), "Forensic Analysis of WhatsApp on Android Smartphones", University of New Orleans Theses and Dissertations, USA.

TOK, A. (2013), "Adli Bilişim İncelemelerinde Bir Farkındalık Artık alan (Slack Space) İncelemesi", 1st International Symposium on Digital Forensics and Security (ISDFS'13), *Bildiriler Kitabı*, s. 25-28.

TÜİK, (2011), *Bilgi ve Verilere Erişim*, Sorularla Resmi İstatistikler Dizisi-9.

UKŞAL, M. (2015), "Mobile Forensics-Mobil Cihazlarda Adli Bilişim", İstanbul Bilgi

Üniversitesi Sosyal Bilimler Enstitüsü Bilişim Ve Teknoloji Hukuku Yüksek Lisans Tezi.

US DOJ (2004) , *Forensic Examination of Digital Evidence:A Guide For Law Enforcement*, Office of Justice Programs – National Institute of Justice, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf, Erişim Tarihi:19.10.2015.

UZUNAY, Y. ve M. KOÇAK, (2005), "Bilişim Suçları Kapsamında Dijital Deliller", Ankara Emniyet Müdürlüğü, Ankara.

ÜNAL, O.G. (2011), "Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama ve El Koyma", Gazi Üniversitesi Sosyal Bilimler Enstitüsü Yüksek Lisans Tezleri Serisi, Ankara.

YALÇINKAYA, M. (2015), "Rekabet Hukuku Uygulamaları Kapsamında Elektronik Delil", Rekabet Kurumu Uzmanlık Tezleri Serisi No:142, Ankara.

YAVUZCAN, E. (2009), "Bilgisayarlarda, Bilgisayar Programlarında Ve Kütüklerinde Arama, Kopyalama Ve Elkoyma (Cmk 134)", http://www.hukuki.net/showthread.php?62314-Bilgisayarlarda-Bilgisayar-Programlarinda-ve-Kutuklerinde-Arama-Kopyalama-ve-Elkoyma-CMK-134, Erişim Tarihi: 10.02.2016.

YURDSEVEN, S. (2012), "İşyerinde Bilgisayar İle Yapılan İşlemler- İşçinin Bilgisayar Ve E-Mail Yazışmalarının İşverence Denetlenmesi", http://www.telekomculardernegi.org.tr/haber-4174-isyerinde-bilgisayar-ile-yapilan-islemler.html, Erişim Tarihi: 10.02.2016.

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

ZUBAROĞLU, A. (2007), "Sabit Disk ve Yapısı", *E-Bergi ODTÜ Bilgisayar Topluluğu Elektronik Dergisi*, http://e-bergi.com/y/Sabitdisk-ve-Yapisi, Erişim Tarihi: 12.01.2016.

AİHM Kararları

Başvuru No: 24117/08, *Bernh Larsen Holding AS v. Norway*, 14.03.2013

Başvuru No: 30457/06, *Robathin v Austria*, 03.07.2012

Başvuru No: 63629/10 ve 60567/10,*Vinci Construction and GMT genie civil and services v. France*, 02.04.2015

ABAD Kararları

Cases 46/87 and 227/88, *Hoechst AG v. Commission*

Case C-94/00, *Roquette Freres SA v. Commission*

GM Kararları

Case T-140/09, *Prysmian and Prysmian Cavi e Sistemi Energia v. Commission*

Case T-289/11, T-290/11, T-521/*11, Deutsche Bahn AG a.o. v. Commission*

Case T-462/12R, *Pilkington Group v Commission*

Case T-135/09, *Nexans France SAS and Nexans SA v. Commission*

ABD Üst Derece Mahkemeleri ve Yüksek Mahkeme Kararları

United States v. Grimmett, 439 F.3d 1263, 1270 (2006)

Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976)

Yargıtay Kararları

Yargıtay 11.Ceza Dairesi, Karar Tarihi: 16.04.2007, Esas No: 2005/6376, Karar No: 2007/2551

Yargıtay 9. Hukuk Dairesi, Karar Tarihi: 13.12.2010, Esas No: 2009/447, Karar No: 2010/37516

Komisyon Kararları

Case Comp/39793, *EPH and Others*, 28.03.2012

Case Comp/B-1/39.326, *E.ON Energie AG*, 30.01.2008

Case 39.796, *Suez Environment and LDE*, 24.05.2011

Danıştay Kararları

Danıştay 13. Dairesi'nin 24.6.2008 tarih ve 2006/2143 E. 2008/5037 K. sayılı Kararı *(ABC Türkiye)*

Danıştay 13. Dairesi'nin 9.5.2012 tarih ve E.2008/9443 ve K. 2012/969 sayılı Kararı *(EBT)*

Danıştay 13. Dairesi'nin 16.2.2010 tarihli, E.2007/11670, K. 2010/1346 sayılı Kararı *(Tıbbi Sarf Malzemeleri)*

Danıştay 13. Dairesi'nin 26.03.2013 tarih, E: 2009/5890, K: 2013/847 sayılı Kararı (Koçak Petrol)

İDDK'nın 27.11.2014 tarih ve E. 2012/2184, K. 2014/4526 sayılı Kararı *(EBT)*

İdare Mahkemesi Kararları

Ankara 13. İdare Mahkemesi Esas No:2013/1598, Karar No:2014/1495 *(TTNET)*

Kurul Kararları

08.07.2013 tarih ve 13-46/601-M sayılı Kurul Kararı *(TTNET)*

24.4.2007 tarih ve 07-34/347-127 sayılı Kurul Kararı (*ABC Türkiye*)

4.7.2007 tarih ve 07-56/672-209 sayılı Kurul Kararı (*EBT*)

16.3.2007 tarih ve 07-24/236-76 sayılı Kurul Kararı (*Tıbbi Sarf Malzemeleri*)

05.08.2009 tarih ve 09-34/837-M sayılı Kurul Kararı (Koçak Petrol)

20.5.2008 tarih ve 08-34/456-161 sayılı Kurul Kararı (*Akücüler)*

9.12.2009 tarih ve 09-58/1405-367 sayılı Kurul Kararı (*Reysaş)*

13.10.2009 tarih ve 09-46/1154-290 sayılı Kurul Kararı (*CNR Fuarcılık)*

25.11.2009 tarih ve 09-57/1393-362 sayılı Kurul Kararı (*Beyaz Et*)

EKLER

EK-1 Taslak Yönetmelik Önerisi

4054 SAYILI REKABETİN KORUNMASI HAKKINDA KANUN KAPSAMINDA TEŞEBBÜS VE TEŞEBBÜS BİRLİKLERİNDE GERÇEKLEŞTİRİLEN YERİNDE İNCELEMELERDE YAPILACAK ADLİ BİLİŞİM UYGULAMALARINA İLİŞKİN YÖNETMELİK

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak ve Tanımlar

Amaç ve Kapsam

MADDE 1 – (1) Bu yönetmeliğin amacı, 4054 sayılı Rekabetin Korunması Hakkında Kanunun 15 inci maddesince teşebbüs ve teşebbüs birliklerinde gerçekleştirilen yerinde incelemelerde yapılacak adli bilişim uygulamalarına ilişkin usul ve esasları düzenlemektir.

Dayanak

MADDE 2 – (1) Bu Yönetmelik, 7/12/1994 tarihli ve 4054 sayılı Rekabetin Korunması Hakkında Kanunun 15 inci ve 27 nci maddelerine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 3 – (1) Bu Yönetmelikte geçen;

a) Adli bilişim: Bilgisayarlarda, veri tabanlarında, her türlü dijital ortamlarda ve işletim sistemlerinde yer alan verilerin tespiti, muhafazası, tanımlanması, elde edilmesi, dokümantasyonu, analizi ile yorumlanması süreç ve işlemlerini,

b) Adli bilişim uygulamaları: Adli bilişimde kullanılan işlemler ile adli bilişim yazılım ve donanımlarını,

c) Anahtar kelime: Bilgisayarlarda, veri tabanlarında, her türlü dijital ortamlarda ve işletim sistemlerindeki aramalarda inceleme konusu ile ilgili olduğu düşünülen verileri aramak amacıyla kullanılan kelimeyi,

ç) Başkanlık: 4054 sayılı Rekabetin Korunması Hakkında Kanunun 29 uncu maddesi çerçevesinde Kurulu Başkanını,

d) Dijital veri: Bilgisayarlarda, veri tabanlarında, her türlü dijital ortamlarda ve işletim sistemlerinde bulunan ve delil olabileceği düşünülen her türlü bilgi ve belgeyi,

e) Hash: Kopyalanan verilerin değiştirilmediğini garanti etmek için kullanılan yazılımları,

f) Kanun: 4054 sayılı Rekabetin Korunması Hakkında Kanunu,

g) Kurul: Rekabet Kurulunu,

h) Kurum: Rekabet Kurumunu,

ı) Meslek personeli: Teşebbüs veya teşebbüs birliğinde yerinde inceleme yapmakla görevlendirilen başta raportör olmak üzere rekabet başuzmanı, uzmanı veya uzman yardımcısını,

i) Raportör: 4054 sayılı Rekabetin Korunması Hakkında Kanun çerçevesince Kurulca ya da Daire Başkanlığınca inceleme yapmak ve rapor hazırlamakla görevlendirilen meslek personelini,

j) Sterilize etmek: Verinin bilinen hiçbir teknikle geri getirilemeyecek şekilde silinmesini,

k) Taraf: Yerinde inceleme esnasında bilgisayarlarında, veri tabanlarında, her türlü dijital ortamlarında ve işletim sistemlerinde adli bilişim uygulamaları ve araçları kullanılan teşebbüs veya teşebbüs birliği yöneticisi veya çalışanını,

l) Yerinde İnceleme: 4054 sayılı Rekabetin Korunması Hakkında Kanunun 15 inci maddesi çerçevesinde teşebbüs ve teşebbüs birliklerinde gerçekleştirilen incelemeyi

m) Plan: Yerinde incelemeye gitmeden önce raportör tarafından hazırlanan ve yerinde incelemede dikkat edilmesi gereken hususları içeren bilgi notunu

ifade eder.

İKİNCİ BÖLÜM
Adli Bilişim Uygulamalarına Karar Verilmesi ve Adli Bilişim Uygulama Planı

Adli Bilişim Uygulamalarına Karar Verilmesi

MADDE 4 – (1) Yerinde incelemenin adli bilişim uygulamaları ile gerçekleştirilmesinin gerektiği durumlarda; raportör görevlendirildiği süre içerisinde, dosyanın Kanunla kısıtlanmış yasal sürelerini de dikkate alarak adli bilişim uygulamalarını kullanma konusunda Kuruldan yazılı talepte bulunabilir.

(2) Bu maddenin birinci fıkrasında belirtilen talep, gerekçesi de bildirilmek suretiyle ilgili raportör tarafından Başkanlığa yazılı olarak yapılır. Başkanlık, talebi en kısa sürede karara bağlanmak üzere Kurula sevk eder.

(3) Gecikmesinde sakınca bulunan hallerde veya yerinde inceleme esnasında adli bilişim uygulamalarının kullanılmasının gerekmesi halinde adli bilişimden yararlanma talebi, raportör tarafından mümkünse e-posta veya faks yoluyla, mümkün değilse sözlü olarak ilgili Daire Başkanına yapılabilir.

a) Bu halde ilgili Daire Başkanı, adli bilişim uygulamalarının kullanılması konusundaki kararını verir, bu kararını mümkünse faks veya e-posta yoluyla, bunun mümkün olmaması durumunda sözlü olarak ilgili raportöre iletir. İlgili raportör bu kararın kendisine ulaşması ile bu yönde faaliyete başlar.

b) İlgili Daire Başkanı adli bilişim uygulamalarının kullanılması konusunda vermiş olduğu kararı vakit kaybetmeksizin bir yazı ile Kurul Başkanına sunar. İlgili yazıda yerinde incelemede görevli raportörün sözlü talebi, bu talebin gerekçesi ve Daire Başkanının bu yöndeki gerekçeli kararı ile bu kararı faks veya e-posta yoluyla raportöre iletememişse bunun gerekçesi yer alır.

c) Kurul Başkanı, talebin görüşülüp kararlaştırılmasını teminen mümkünse hemen, mümkün değilse 72 saati geçmemek üzere Kurul'u toplantıya çağırır. Kurul'un adli bilişim uygulamalarının kullanılması yönünde karar vermesi halinde bu karar vakit geçirilmeksizin e-posta veya faks yoluyla raportör ile teşebbüs veya teşebbüs birliğine ve her halükarda posta yoluyla teşebbüs veya

teşebbüs birliğine bildirilir. Kurulun adli bilişim uygulamalarının kullanılması yönünde yetki vermemesi halinde ilgili raportör bu süre zarfında ve bu yöntemle elde ettiği delilleri inceleyemez ve raporunda kullanamaz.

(4) Kurul gerek önaraştırma yapılması veya soruşturma açılması kararını verirken re'sen, gerekse bu maddenin 1. Fıkrasında belirtilen hususlarla raportörün talebi üzerine, makul bir süre içinde adli bilişim uygulamalarının kullanılıp kullanılmayacağı konusunda karar verir ve bu kararını gerekçesiyle birlikte ilgili raportöre yazıyla bildirir.

Adli Bilişim Uygulama Planının Hazırlanması

MADDE 5 – (1) Kurulun adli bilişim uygulamaları konusunda raportöre yetki vermesine müteakip raportör adli bilişim uygulamalarının nasıl gerçekleştirileceğine yönelik uygulama planı hazırlar. Söz konusu planda;

a) Hangi teşebbüs veya teşebbüs birliklerinde adli bilişim uygulamaları gerçekleştirileceği,

b) Bu amaçla hangi yazılım ve donanımların kullanılacağı,

c) Anahtar kelime listesi,

d) Yerinde incelemede görevlendirilen meslek personeli haricinde adli bilişim alanında uzmanlaşmış meslek personeli talebi olup olmadığı,

belirtilir.

(2) Raportörce hazırlanan plan yazısı ilgili Daire Başkanının görüşüne sunulur. İlgili Daire Başkanı, sunulan planı uygun görüyorsa Kurula bilgi vermek amacıyla Başkanlığa gönderir. Bu aşamada;

a) İlgili Daire Başkanı, sunulan planın tamamının veya bir kısmının yeniden değerlendirilmesini raportörden isteyebilir.

b) Bu halde, Daire Başkanının önerilerini değerlendiren raportör hazırladığı nihai planı Daire Başkanına sunar.

c) Daire Başkanı, raportörce nihai hali verilen planı, varsa karşı görüşlerini de ekleyerek Başkanlığa gönderir. Başkan, planı ya uygun bulur ya da nihai kararın verilmesi amacıyla Kurula sevk eder. Bu halde Kurul en geç 72 saat içinde

toplanır. Kurulca kabul görmeyen planda yer alan adli bilişim uygulama ve araçları ile elde edilen verileri raportör inceleyemez, raporunda kullanamaz.

(3) Yerinde inceleme esnasında gerektiğinde raportör, incelemenin konusu ve amacını aşmamak kaydıyla plan dışında başka adli bilişim uygulamaları, yazılım ve donanım kullanılması ile anahtar kelimelerde değişiklik yapılmasına karar verebilir. Bu durum; ilgili raportörce gerekçesi de belirtilmek üzere tutanak ile kayıt altına alınır. Söz konusu tutanak en kısa zamanda Kurul Başkanının bilgisine sunulmak üzere ilgili Daire Başkanına teslim edilir.

(4) Raportörün yerinde incelemede adli bilişim alanında uzmanlaşmış meslek personeli görevlendirilmesi hususunda talep yapması halinde, raportörün kendi Daire Başkanı, adli bilişim alanında uzmanlaşmış meslek personelinin Daire Başkanı ile irtibata geçer. Bu durumda her iki Daire Başkanı da adli bilişim uygulamalarının tüm aşamalarında gerekli işbirliği ve yardımı sağlamakla mükelleftir.

ÜÇÜNCÜ BÖLÜM
Yerinde İncelemede Adli Bilişim Uygulaması ve Prosedürü

Tarafa Bilgi Verilmesi

MADDE 6 – (1) Yerinde incelemede görevli meslek personeli inceleme öncesi Tarafa şifahen veya yazılı bilgi vermek ve bu amaçla hazırlanan yetki belgesinin bir örneğini sunmakla mükelleftir. Yetki belgesi olmayan meslek personeli;

a) Tarafa açıklamalarda bulunamaz,

b) Tarafın bilgisayarlarında, veri tabanlarında, her türlü dijital ortamlarında ve işletim sistemlerinde adli bilişim uygulaması yapamaz,

c) Adli bilişim uygulamaları ile elde edilen dijital verileri inceleyemez, bu veriler hakkında yorum yapamaz.

(2) Taraf yerinde incelemede görevli raportörden adli bilişim planının bir örneğini talep edebilir. Tarafın, planı incelemesinde veya bir örneğini almasında sakınca olmaması halinde planın bir örneği Tarafa verilir. Raportörce, Tarafın planı incelemesinin veya bir örneğini almasının sakınca oluşturacağının değerlendirilmesi halinde, bu durum

gerekçesi ile birlikte tutanakta belirtilir. Bu tutanak, adli bilişim uygulamalarına başlanmasının aciliyet oluşturması durumunda daha sonra da tutulabilir.

(3) Taraf, adli bilişim uygulamaları veya planda belirtilen hususlara ilişkin meslek personeline sözlü veya yazılı itirazda bulunabilir. Bu itiraz, meslek personelince hemen değerlendirilip karara bağlanır. Bu karar, gerekçesiyle birlikte tutanakta belirtilir. Tarafın sözlü itirazı, tutanakta tam ve eksiksiz yazılmak durumundadır.

(4) Taraf, meslek personelinin yetki belgesini, verilmişse planı inceledikten ve açıklamaları dinledikten sonra vakit kaybetmeksizin varsa itiraz ve taleplerini dile getirmek, aksi halde işleme derhal izin vermek ve bu konuda meslek personeline yardımcı olmak zorundadır. Tarafın itirazlarını ve taleplerini değerlendiren meslek personeli bu itiraz ve talebi yerinde görmüyorsa daha sonra Tutanağa geçirilmek kaydıyla sözlü olarak reddedebilir. Bu halde meslek personeli vakit kaybetmeksizin adli bilişim uygulamalarına başlar.

(5) Taraf, adli bilişim uygulamaları konusunda dışardan hukuki bir danışmanlık alabilir. Ancak, böylesi bir hukuk danışmanının varlığı, uygulamanın geçerliliği için hukuki bir şart değildir. Meslek personeli tarafın hukuki danışmanını beklemeksizin adli bilişim uygulamalarını başlatabilir. Ancak Tarafın hukuki danışmanı adli bilişim uygulamalarının yapıldığı mahalle geldiği andan ve Taraf ile arasındaki hukuki danışmanlık akdini belgeledikten sonra Taraf ile aynı haklara sahip olur. Taraf gibi adli bilişim uygulamalarına refakat edebilir, inceleme öncesi ve sonrası adli bilişim uygulamalarına ve buradan elde edilen belgelere ve alınan imaja yönelik itirazlarda ve taleplerde bulunabilir.

Adli Bilişim Uygulamalarının Kullanılması

MADDE 7 – (1) Meslek personeli plan çerçevesinde veya yerinde inceleme esnasında raportörce verilen karar doğrultusunda tarafın bilgisayarında, veri tabanlarında, her türlü dijital ortamlarında ve işletim sistemlerinde adli bilişim uygulamalarını başlatır. Bu amaçla yazılımlar veya donanımlar kullanabilir.

(2) Adli bilişim uygulamaları sürecince, bu işlemlerden etkilenecek diğer çalışanlara bilgi verme görevi Tarafa aittir.

(3) Meslek personeli, yerinde inceleme boyunca teşebbüs veya teşebbüs birliğince sağlanan veya teşebbüs veya teşebbüs birliğinde var olan donanımları ve yazılımları kullanabilir. Ancak Taraf, meslek personelini teşebbüste veya teşebbüs birliğinde var olan donanım ve yazılımları kullanmaya zorlayamaz.

(4) Meslek personeli adli bilişim uygulamaları esnasında yerinde incelemenin ve planın amacı doğrultusunda hareket etmek zorundadır. Bu amaçlar dışında herhangi bir gaye güdemez ve uygulama yapamaz.

(5) Meslek personeli adli bilişim uygulamaları esnasında teşebbüs veya teşebbüs birliğinin kendi iç işleyişine (mümkün olduğunca az müdahale eder veya) müdahale edemez, işleyişine, çalışmalarına engel olamaz.

(6) Meslek personeli adli bilişim uygulamalarını mümkün olan en kısa sürede tamamlamak ve aksi gerekmedikçe adli bilişim uygulamalarından elde edilen verileri teşebbüs veya teşebbüs birliğinde analiz edip suretini almak ve bir suretini de teşebbüs veya teşebbüs birliğine bırakmak zorundadır. Alınan suretlerin dijital ortamda olması durumunda ilgili verilerin Hash değerleri hesaplanır ve Tutanağa geçirilir.

(7) Zorunlu hallerde veya yerinde incelemedeki süre kısıtı halinde meslek personeli adli bilişim uygulamalarından elde edilen dijital verileri veya alınan imajı analiz etmek üzere Kuruma ya da teşebbüs veya teşebbüs birliği dışına götürebilir. Bu durumda alınan verilerin bir örneği Hash değerleri ile birlikte Tutanağa da geçirilmek suretiyle tarafa verilmek zorundadır.

(8) Adli bilişim uygulamaları esnasında Taraf veya Tarafın hukuki danışmanı, meslek personeline refakat edebilir, incelenen dijital veriler hakkında bilgi verebilir, meslek personelinden verilere ilişkin genel izahat isteyebilir.

(9) Yerinde inceleme esnasında Taraf, bilgisayarında, veri tabanlarında, her türlü dijital ortamlarında ve işletim sistemlerinde yapılan aramalarda veya alınan verilerde şahsi bilgi ve belgelerinin olduğunu veya arama ile alınan dijital verilerin yerinde inceleme konusu ile ilgisinin bulunmadığını sözlü veya yazılı olarak meslek personeline bildirebilir. Bu bildirim meslek personelince hemen değerlendirilip karara bağlanır. Bu karar, gerekçesiyle birlikte tutanakta belirtilir. Tarafın sözlü bildirimi, tutanakta tam ve eksiksiz yazılmak durumundadır.

(10) Adli bilişim uygulamaları ile elde edilen dijital veriler; inceleme süresinin sonuna değin incelenmek amacıyla meslek personelinin kontrolünde tutulabilir. Meslek personeli bu dijital verileri kopyasını/imajını aldıktan sonra iade edebilir. Bu kopya orijinal ortamında saklanan dijital verinin bütün parçaları içeren özgün bir kopyası olmak durumundadır. Özgün kopyayı incelemek orijinal ortamında var olan dijital veriyi incelemek ile eş değerdedir.

Adli Bilişim Uygulamalarının Tamamlanması

MADDE 8 – (1) İncelemenin sonunda meslek personeli, yanında getirdiği ve Tarafın bilgilerini analiz etmek amacıyla kullanılan tüm adli bilişim araçlarını sterilize eder. Taraf tarafından sağlanan donanımlar sterilize edilmez, ancak Tarafa iade edilir.

(2) Eğer Tarafın adli bilişim uygulamalarına konu dijital verilerinin seçilmesi işlemi öngörülen zamanda bitirilemezse, uygulama yapılan dijital verilerin bir kopyası daha sonra incelenmek üzere meslek personelince alınabilir. Alınan dijital veri kopyaları mühürlü bir zarfa konulmak suretiyle koruma altına alınır. Taraf bu kopyanın bir kopyasını isteyebilir. Kurum, mühürlü zarfın açılacağı gün Kurum binasında hazır bulunması için teşebbüse davet gönderir. Buna alternatif olarak Kurum zarfı hiç açmadan teşebbüse geri gönderebilir. Kurum ayrıca Taraftan zarfı daha sonra bildirilecek bir inceleme veya uygulamada incelenmek üzere saklamasını isteyebilir.

(3) Meslek personeli tarafından seçilen dijital veriler inceleme sonucunda elde edilen diğer belgelere eklendikten sonra, Tarafa bu verilerin aynılarının ve hash değerlerinin olduğu bir kopya DVD gibi bir veri taşıyıcı aracılığı ile bırakılır. Seçilen veri başlıklarının listesinin olduğu belge Tarafça imzalanır. Bu verilerin bulunduğu iki kopya halinde oluşturulmuş veri taşıyıcı ise meslek personelince alınır.

(4) Adli bilişim uygulamaları boyunca seçilen tüm delillerin kendi teknik bütünlüğünü koruduğuna dikkat edilmelidir. Dijital verilerin, analiz edilmek amacıyla teşebbüs veya teşebbüs birliği dışında başka bir yere veya Kuruma götürülmesi halinde son işlem esnasında, her dijital veri kaleminin bileşenlerine tek tek ayrılması ve bunların tek tek listelenmesi ve her birinin bireysel referans numarası almak suretiyle sıralanması gerekmektedir.

DÖRDÜNCÜ BÖLÜM
Adli Bilişim Uygulamalarından Elde Edilen Verilerin Analizi

Dijital Verilerin Analiz Yeri

MADDE 9 – (1) Adli bilişim uygulamalarından elde edilen dijital verilerin analizinin teşebbüs veya teşebbüs birliğinde ve sakınca bulunmayan hallerde Tarafın huzurunda yapılması esastır. Ancak süre kısıtı veya teknik nedenlerle analiz işlemi Kurumda yapılabileceği gibi Kurum ile teşebbüs veya teşebbüs birliği dışında bir yerde de yapılabilir.

(2) İncelemeyle ilgili olmayan ve alınmış olan dijital veriler en fazla inceleme sonuna kadar tutulabilir/depolanabilir.

(3) İncelemeyle ilgili olmayan veya başka bir incelemede kullanılmayacak alınmış dijital veriler, inceleme sonunda Tarafa iade edilir veya Kurum tarafından tamamen yok edilir.

Dijital Verilerin Analizi Esnasında Tarafın Hakları

MADDE 10 – (1) Analiz işlemi teşebbüs veya teşebbüs birliğinde Tarafın huzurunda yapılmıyorsa analizin yapılacağı yer ve saate ilişkin Tarafa yazılı bilgi verilir. Taraf belirtilen yer ve saatte hazır bulunup analiz aşamasına refakat edebilir, bu aşamada itiraz ve talepte bulunabilir. İtirazı ve talebi raportörce karara bağlanır ve bu karar daha sonra Tutanağa geçirilmek kaydıyla sözlü olarak Tarafa bildirilebilir.

(2) Taraf, analiz işleminin başlayacağı süre içerisinde yazılı olarak meslek personelince alınan dijital verilerde şahsi bilgi ve belgelerinin olduğunu veya yerinde inceleme konusu ile ilgisinin bulunmadığını yazıyla Kuruma bildirebilir. Bu durumda bahse konu dijital verilerin Tarafın huzurunda analiz edilmesi için Taraf davet edilir. Tarafın bu davete uymaması halinde veya talebinden vazgeçmesi halinde analiz işlemine başlanır.

(3) Taraf, adli bilişim uygulaması öncesi, uygulama esnasında veya dijital verilerin analizi esnasında raportöre ilettiği ancak raportörce kabul görmeyen itirazları için ilgili tutanakla birlikte 3 gün içinde Kurula itirazda bulunabilir. Bu halde en geç 3 gün içinde Kurul konuya ilişkin kararını vererek Tarafa ve raportöre yazıyla ivedi

olarak bildirir. Kurulca kabul gören Tarafın itirazlarına ilişkin dijital veriler raportörce raporunda kullanılamaz, analiz edilemez ve bir başkasıyla paylaşılamaz.

BEŞİNCİ BÖLÜM
Son Hükümler

Dijital Verilerin Başka İncelemelerde Kullanılması ve Başkalarıyla Paylaşılması

MADDE 11 – (1) Adli bilişim uygulamaları esnasında alınan dijital veriler, Kanun ile ilgili bir başka incelemede kullanılabilir.

(2) Adli bilişim uygulamaları sürecinde alınan dijital veriler, gerektiği durumlarda adli ve diğer idari birimlerle paylaşılabilir.

(3) Alınan dijital verilerin üçüncü kişilerle paylaşılması durumunda buna ilişkin yazılı bir belge düzenlenir ve söz konusu belgede paylaşılan dijital verilerin nereden geldiği belirtilir.

Yönetmelik Hükümlerinin İhlali

MADDE 12 – (1) Bu Yönetmelik hükümlerinin tarafça ihlali halinde Kanunun 15 inci, 16 ıncı ve 17 nci maddeleri uygulanır.

Devam Eden İncelemeler

GEÇİCİ MADDE 1 – (1) Adli bilişim uygulamaları raporu teslim edilmemiş devam eden incelemelerde de kullanılabilir.

Yürürlük

MADDE 13 – (1) Bu Yönetmelik, Resmi Gazete'de yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 14 – (1) Bu Yönetmelik hükümlerini Rekabet Kurumu Başkanı yürütür.

REKABET KURUMU

Üniversiteler Mahallesi
1597. Cadde No: 9
06800 Bilkent/ANKARA
http:// www.rekabet.gov.tr