Uzmanlık Tezleri Serisi No: 142

REKABET KURUMU

REKABET HUKUKU UYGULAMALARI KAPSAMINDA ELEKTRONİK DELİL

MAZLUM YALÇINKAYA

REKABET HUKUKU UYGULAMALARI KAPSAMINDA ELEKTRONİK DELİL

MAZLUM YALÇINKAYA

ANKARA 2015

Baskı, Haziran 2015
Rekabet Kurumu-ANKARA

Bu tez, Rekabet Kurumu Başkan Yardımcısı Ali İhsan ÇAĞLAYAN, III. Denetim ve Uygulama Dairesi Başkanı Vekili Hakan Suat ÖLMEZ, Mesleki Koordinatör Salim AYDEMİR, Mesleki Koordinatör Abdülgani GÜNGÖRDÜ ve Yrd. Doç. Dr. Gamze ÖZ AŞÇIOĞLU'ndan oluşan Tez Değerlendirme Heyeti tarafından 27 - 28 Mayıs 2014 tarihlerinde yürütülen Tez Savunma Toplantısı sonucunda yeterli bulunmuş, Başkanlık Makamının 9.6.2014 tarih ve 6221 sayılı onayı ile tezin yazarı Mazlum YALÇINKAYA Rekabet Uzmanı olarak atanmıştır.

YAYIN NO **317**

İÇİNDEKİLER

Bölüm 2

ÖRNEK ÜLKE UYGULAMALARI VE GENEL OLARAK ELEKTRONİK DELİLLERİN ELDE EDİLMESİ SÜRECİNDE TEMEL HAK VE ÖZGÜRLÜKLER BAĞLAMINDA ORTAYA ÇIKAN PROBLEMLER

Bölüm 3
4054 SAYILI KANUN ÇERÇEVESİNDE ELEKTRONİK DELİL

SUNUŞ

Yaklaşık 18 yıldır bağımsız bir idari otorite olarak faaliyetlerini sürdürmekte olan Rekabet Kurumu, 4054 sayılı Rekabetin Korunması Hakkında Kanun'un uygulanmasını gözeterek, piyasalarda kartelleşmeyi ve tekelleşmeyi engellemek yönünde önemli adımlar atmaktadır. Piyasa ekonomilerinde hayati bir role sahip olan rekabetin korunması ile tüketicilerin, yaşamın her alanında daha kaliteli ürünü, daha ucuza ve daha çok miktarda satın alabilmeleri sağlanmaktadır. Bu yöndeki çalışmaları ile de Rekabet Kurumu, yalnızca Türkiye'deki kurumlar arasında değil, dünyadaki rekabet otoriteleri arasında da hak ettiği yeri almaya başlamıştır. Nitekim Avrupa Birliği Komisyonu ilerleme raporları ile OECD gözden geçirme raporunda bu durum ifade edilmekte ve Kurumun ulaşmış olduğu idari kapasite ve mesleki düzey takdirle karşılanmaktadır.

Rekabet Kurumunun ulaşmış olduğu bu idari kapasite ve mesleki düzeyin en önemli yansımalarından biri de uzmanlık tezleridir. Rekabet uzman yardımcıları, üç yılı aşan meslekî çalışmalarından elde ettikleri tecrübeleri, yoğun bilimsel araştırmalarla birleştirerek tez hazırlamaktadır. Rekabet hukuku, politikası ve sanayi iktisadı alanlarında hazırlanan ve gerek Rekabet Kurumuna gerekse diğer ilgililere yönelik önemli bir kaynak niteliğini haiz olan bu tezlerden bazılarında, rekabet hukuku ve politikasının temel konu başlıklarını içeren teorik hususlar derin analizlerle irdelenmekte, diğerlerinde ise rekabet hukuku uygulamaları bakımından önem arz eden sektörlere ilişkin çalışmalara yer verilmektedir. Bu sayede daha önce ele alınmamış pek çok konuda değerli eserler ortaya çıkmaktadır.

Bu eserlerin yayımlanması, doktrine katkı sağlanmasını ve toplumun rekabet konusunda bilgilendirilmesini hedeflemekte; bu yönüyle rekabet otoritelerinin en önemli görevleri arasında yer alan rekabet savunuculuğunun bir parçasını teşkil etmektedir. Rekabet Kurumu, uzmanlık tezlerinin yayımlanmasını, rekabet savunuculuğu çerçevesinde tek başına veya üniversitelerle, barolarla ve benzeri örgütlerle işbirliği halinde yürütmekte olduğu konferanslar, sempozyumlar, eğitim ve staj programları düzenlemek gibi faaliyetlerine ilave bir etkinlik olarak değerlendirmektedir.

Ele alınan konular bakımından kaynak olarak kullanılabilecek yerli eserlerin sayıca az olması nedeniyle, rekabet uzman yardımcılarımızca hazırlanan uzmanlık tezlerinin değerleri bir kat daha artmaktadır. Bu çerçevede tez süreçlerini başarıyla tamamlayarak Rekabet Uzmanı unvanını alan bütün arkadaşlarımı gönülden kutluyor, başarılarının devamını diliyorum. Meslek personelimizin uzmanlık tezlerini, önemli bir başvuru kaynağı olacağı inancıyla ilgili kamuoyunun bilgisine sunuyorum.

Prof. Dr. Nurettin KALDIRIMCI
Rekabet Kurumu Başkanı

KISALTMALAR

AB	: Avrupa Birliği
ABAD	: Avrupa Birliği Adalet Divanı (European Court of Justice)
ABD/Birleşik Devletler	: Amerika Birleşik Devletleri
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Haklan Sözleşmesi
AST	: Adli Soruşturma Talebi
BKartA	: Alman rekabet otoritesi-Bundeskartellamt
bkz.	: Bakınız
CMK	: Ceza Muhakemesi Kanunu
DOJ	: Department of Justice-ABD Adalet Bakanlığı Birimi
FBI	: Federal Soruşturma Bürosu (Federal Bureau of Investigation)
FTC	: Federal Trade Commission- Federal Ticaret Komisyonu
HMK	: Hukuk Muhakemeleri Kanunu
HUMK	: Hukuk Usulü Muhakemeleri Kanunu
ICN	: International Competition Network
İDDK	: Danıştay İdari Dava Daireleri Kurulu
İDM	: İlk Derece Mahkemesi (Court of First Instance)
Kanun/4054 Sayılı Kanun	: 4054 Sayılı Rekabetin Korunması Hakkında Kanun
Komisyon	: Avrupa Birliği Komisyonu Rekabet Genel Müdürlüğü
Kurum	: Rekabet Kurumu
Kurul	: Rekabet Kurulu
OJ	: Official Journal (AB Resmi Gazetesi)
Para.	: Paragraf
s.	: Sayfa
V.	: Versus
vd.	: ve diğerleri
Vol.	: Volume

GİRİŞ

Rekabet Kurumu kurulduğu günden bu yana karteller başta olmak üzere rekabet ihlalleri ile ciddi bir mücadele yürütmektedir. Bu mücadele kapsamında; rekabet ihlallerinin ortaya çıkarılmasında neredeyse her zaman Kurum'un denetim yetkilerini oluşturan yerinde inceleme[1] ve bilgi isteme yetkileri çerçevesinde elde edilen bilgi ve belgelere istinat edilmektedir. Bu açıdan, Kurum'un söz konusu denetim yetkilerinin, özellikle de yerinde inceleme yetkisinin etkin kullanılması, rekabet ihlalleri ile başarılı bir mücadele gerçekleştirmek için zaruret teşkil etmektedir. Nitekim bu durumun bilincinde olan Kurum, yerinde incelemeler için önemli ölçüde kaynak ayırmakta Kurum uzmanları da yerinde incelemelerin en etkin şekilde gerçekleştirilebilmesi için yerinde incelemenin öncesinde ve sonrasında büyük çaba sarf etmektedir. Fakat yerinde incelemelere verilen bu öneme rağmen, 17 yıllık kurumsal tecrübe, rekabet ihlalleri ile mücadelenin alışılagelmiş yollarla devam edilmesinin sürdürülemez olduğunu göstermiştir. Bu açıdan Kurum'un mevcut delil toplama yöntemlerinin, çağın gerekliliklerine hızla uyum sağlayan ve işleyişlerini de buna göre düzenleyen teşebbüslerin geçirdiği dönüşüme paralel olarak geliştirilmesi, yeni yöntem ve metotlarla uyumlaştırılması gerekmektedir.

Öte yandan, sosyal ve hukuki olaylar ya da toplumsal ihtiyaçlardan ziyade doğrudan bilişim teknolojilerinin gelişimine bağlı olarak yol alan bu dönüşüm sürecinde hukukun rolünün bulunmadığı görülmektedir. Keza, teknolojik gelişmeler yeni ürün ve hizmetler aracılığıyla önce toplumsal hayata aksetmekte, ancak ardından ortaya çıkan gereksinimlere göre mevzuat oluşturma faaliyetlerine başlanılmaktadır. Her geçen gün geleneksel iş ve işleyişler, alışılagelmiş formlarından sıyrılarak, dijital gerçeklikte yerini aldığından, bunlara ilişkin hukuki anlaşmazlıkların, haksız fiillerin ve suçların sübuta erdirilmesinde daha çok başvurulmaya başlanılan elektronik delillere ilişkin uyarlamaların yapılması ihtiyacı ortaya çıkmaktadır. Zira elektronik delillere uygulanan hukuk, bugün

[1] "Surprise Inspections", "Dawn raid" gibi karşılıkları olan baskın şeklindeki yerinde incelemeler kast olunmaktadır.

kullanılan teknolojilerin insanlığın ufkunda dahi yerini almadığı dönemlerde gelişmiştir (Çakmak 2005, 300).

Bu bağlamda, elektronik delillerin kendilerine özgü nitelikleri dikkate alınarak hazırlanmış düzenlemelerin eksik olduğu, geleneksel delil türlerine ilişkin kural ve kaidelerin yorum yoluyla elektronik delillere de uygulandığı görülmektedir (Cybex 2006, 32). Bu nedenle, elektronik delillerin elde edilmesinden, Kurul'a sunulmasına kadar geçen süreçte başvurulan bir takım yerleşik uygulamaların, elektronik delillerin elde edilmesi sürecinde işlevsel kılınan genel kabul görmüş standartlar çerçevesinde değerlendirilmesi gerekmektedir. Nitekim delillerin gerçeğine uygunluğunun, delillerin ve delil zincirinin bütünlüğü koşulları sağlanarak elektronik delillerin kabul edilebilirliğine ilişkin şartların yerine getirilmesi, delil hukuku açısından önem arz etmektedir.

Yukarıda yer verilen açıklamalar ve değerlendirmeler doğrultusunda bu çalışma kapsamında, öncelikle elektronik delil kavramına açıklık getirilmeye çalışılacak, ardından rekabet ihlallerinin ortaya çıkarılmasında elektronik delillerin elde edilmesi sürecinin daha etkin hale getirilmesinin gerekliliği ve bu amaçla başvurulabilecek yollar irdelenecektir. Çalışmanın izleyen bölümünde ise elektronik delil elde edilmesine yönelik başvurulan uygulamalar temel hak ve özgürlükler bağlamında değerlendirilecek ve önde gelen ülke uygulamaları incelenecektir. Çalışmanın son bölümünde ise Kurum'un elektronik delil elde edilmesine ilişkin uygulamaları, 4054 Sayılı Rekabetin Korunması Hakkında Kanun (4054 sayılı Kanun) çerçevesinde Kurum'un elektronik delil elde etme yetkileri değerlendirilerek, nihayetinde ülkemiz uygulamasına yönelik politika ve düzenleme önerilerinde bulunulacaktır.

BÖLÜM 1

GENEL OLARAK ELEKTRONİK DELİL VE TÜRK HUKUK SİSTEMİ İÇİNDE ELEKTRONİK DELİL

1.1. GENEL OLARAK ELEKTRONİK DELİL

1.1.1. Dijital (Elektronik) Ortam

İnsanoğlu medeniyetin farklı dönemlerinde taş, bakır, parşömen ve nihayet kâğıt gibi farklı metalar üzerinde yaptığı anlamlı çizimlerle bilgiyi muhafaza etme yolunu seçmiştir. Bir diğer ifadeyle, fiziksel zemin üzerinde izler bırakmak kaydıyla insan gözünün algılayabileceği şekilde bilgiler oluşturulmuş ve bilgi kalıcı kılınmıştır. Günümüzde; bilginin oluşturulduğu ve saklandığı ortam fiziksel gerçeklikten, dijital gerçekliğe doğru hızla evrilmektedir.

Bu değişimin bir sonucu olarak; ilerleyen bölümlerde elektronik delillerin elde edilmesinden karar mercilerine sunulmasına kadarki süreçler irdelenirken "dijital ortam" kavramına sıklıkla başvurulacak, elektronik delilin mahiyeti ile ilgili, geleneksel delillerden ayrıldığı ve özel olarak ele alınması gereken hususiyetleri tartışılırken "dijital ortam" vurgusu ön plana çıkacaktır. Bu bakımdan, en genel çerçevesiyle dahi olsa dijital ortam kavramının ve kendine has dinamiklerinin anlaşılması önem taşımaktadır.

Fiziksel büyüklüklerin sayısal değerler ile ifade etmenin analog ve dijital olmak üzere iki temel yolu bulunmaktadır. Analog yöntemde fiziksel büyüklükler belirli iki uç değer arasında ve sürekli ölçekte ifade edilebilir (Maini 2007, 2). Dijital ifade etme yönteminde ise miktarların sayısal değerleri kesintili ölçekte aralıklı olarak belirlenir. Örneğin, analog bir saatin akrep ve yelkovanı saatin kadranı üzerinde yer değiştirdikçe bir gün içindeki tüm zamanı gösterebilir, oysa dijital bir saat sadece sınırlı sayıda önceden belirlenen aralık dâhilinde (her bir saniyeyi, onda birini, yüzde birini vs.) zamanı gösterecektir.

İnsanların dünyayı algılayış şeklinin de analog olduğunu ifade etmek mümkündür. Mesela, insan gözü dış dünyadaki renkleri ve şekilleri yekpare bir

bütün olarak algılar, renkler arasındaki geçiş mükemmele yakındır. Öte yandan, bilgisayar ekranındaki ya da gazete sayfasındaki bir resim bir birinden farklı renkte ve tondaki noktaların uygun diziliminden oluşur[2]. Benzer şekilde, ses dijital ortama aktarılırken; her bir saniye için sesin genliği defalarca kez ölçülür, daha sonra bu nümerik değerler temel alınarak ses dijital olarak kaydedilir[3]. Bu nedenle, analog sistemlerin dijital formattaki halleri esasında yakınsamadan ibarettir.

Analog formattaki bilgiler dijital ortama genellikle *"bayt"*lar halinde aktarılır, her bayt 8 *"bit"*ten oluşmaktadır, her bit ise 0 ya da 1 değerine sahiptir. Bilgilerin bu şekilde dijital ortamda 0 ve 1'in farklı dizilimleri şeklinde ifade edilmelerinde ikili sayı sistemi *(binary)* kullanılmaktadır. Ses, resim, video, yazı gibi her türlü bilgi dijital ortamda bit dizileri şeklinde depolanır ve kullanılır. Buradan hareketle, dijital ya da elektronik ortam gerçek hayata dair her türlü bilginin rahatlıkla saklanması ve işlenmesine olanak sağlayacak şekilde sayısallaştırılarak bir araya getirildiği ortam olarak tanımlanabilir.

1.1.2. Elektronik Delil

Delil ya da kanıt ispat edilmesi gerekli olan vakıaların vuku buldukları ya da bulmadıkları hususunda karar merciinde kanaat oluşturmak için başvurulan ispat aracıdır (Çetinkaya 2013, 176). Maddi gerçeğin aydınlatılmasında kullanılacak ispat araçları delil ile sınırlı olmayıp, delilin yanı sıra emare gibi ispat faaliyetinde kullanılan başka ispat araçları da bulunmaktadır. Emareler de delil niteliğinde olmakla birlikte, vakıanın tamamını değil de bir kısmını gösteren ispat araçlarıdır. Bu nedenle, tek başına ispat kuvvetini haiz olmamakla beraber, birbirlerini tamamladıkları takdirde delil olarak kabul edilebilirler (Konuralp 2007, 18).

İspat hukukunda delillerin esas alınan ölçüte göre değişik şekilde tasnif edilebildikleri görülmektedir. Örneğin, hâkimin sunulan delil karşısındaki durumuna göre medeni usul hukukunda kesin delil ve takdiri delil ayrımına gidilmiştir, her şeyin delil olabildiği ve hâkimin delilleri serbestçe takdir edebildiği ceza muhakemesi hukukunda ise maddi deliller, beyan delilleri ya da doğrudan deliller ve dolaylı deliller şeklinde tasniflerde bulunulabildiği görülmektedir. Elektronik delillerin ise başlı başına bir delil türü olduğunu söylemek mümkün değildir. Kaldı ki, Türk hukukunda, serbest delil sisteminin geçerli olmasının bir sonucu olarak elektronik delillerin bir delil türü altında yer almasına gerek olmadığı da literatürde öne sürülmektedir (Çetin 2011, 34). Bu bakımdan, elektronik delil kavramı,

[2] http://mason.gmu.edu/~montecin/digits.htm Erişim tarihi: 05.12.2013

[3] http://webopedia.internet.com/TERM/d/digitize.html Erişim tarihi: 28.12.2013

elektronik ortamda var olan delillere farklı bir kimlik kazandırmamaktadır. Sadece, başvurulacak delilin oluşturulduğu ve muhafaza edildiği ortama vurgu yapmakta, bir iddianın lehinde veya aleyhinde kanaat oluşturabilecek, delil niteliği taşıyan belge/bilginin elektronik ortamdaki halini ifade etmektedir.

Bu çerçevede elektronik delil[4] özelinde çalışma yürüten, Standart Working Group on Digital Evidence (SWGDE) tarafından elektronik delil, dijital formatta saklanan ya da iletilen her türlü bilgi olarak tanımlanmaktadır. Uluslarası Rekabet Ağının (ICN) kartel çalışma grubu tarafından hazırlanan *"elektronik delillerin elde edilmesi"* başlıklı metinde ise elektronik delil bir davada delil olarak kullanılabilecek her türlü dijital formattaki bilgi olarak tanımlanmaktadır (2010, 2). Mason ise (2008, 180) "elektronik delil" kavramının "analog" ve "dijital" delil formatlarını kapsayıcı bir üst kategoriyi ifade ettiğini belirtmektedir. Bu doğrultuda, dijital ortamda oluşturulan, delil niteliği taşıyan bir elektronik verinin de, dijital ortama aktarılmış analog bir çıktının da elektronik delil olarak adlandırılabileceğini ifade etmektedir. Buradan hareketle, dijital ortamda oluşmuş veya oluşturulmuş ya da dijital ortama aktarılmış, muhakeme konusu olay bakımından delil değeri taşıyan her türlü bilgiyi elektronik delil olarak tanımlayabiliriz.

1.1.2.1. Elektronik Delillerin Yer Aldığı Ortamlar

Elektronik delile ilişkin yapılan tanımlardan da anlaşılacağı üzere elektronik deliller açısından, geleneksel delillerden farklı olarak mutlaka elektronik bir ortamda bulunma zorunluluğu söz konusudur. Bu bakımdan, bilgisayarlar, bilgisayar sistemleri ve elektronik delil içerebilecek her türlü cihaz, genel bir ifadeyle bilişim altyapısı[5] ihlale ilişkin delillerin taşıyıcısı konumundadır. Elektronik delillerin bu ortamlarda belirmesi, genel olarak bir bilginin kullanıcı tarafından dijital ortama aktarılmasıyla, kullanıcının komutları doğrultusunda, bilginin bilgisayar tarafından üretilmesiyle ya da bilgisayarın kendi işleyişi içinde bir bilgiyi kaydetmesi, işlemesi ile oluşabilmektedir (Chung ve Byer 1998, 184).

Kullanıcının direktifiyle bilgisayar tarafından oluşturulan ya da kullanıcı tarafından elektronik ortama aktarılan ve delil niteliği arz edebilecek elektronik

[4] Her ne kadar telefon ve ortam dinlemeleri de elektronik delil başlığı altında incelenebilecek olsa da ülkemizde rekabet ihlallerine ilişkin mevcut hukuk rejimi göz önünde bulundurularak, bu tür deliller çalışmamız kapsamına dâhil edilmemiştir.

[5] TCK 243. maddesinin gerekçesinde yer alan "Bilişim sistemi" ve Siber Suçlar Sözleşmesi'nin 1. maddesinde yer alan "Bilgisayar sistemi" kavramlarından hareketle; bu çalışmada üzerinde elektronik delil araması yapılan teşebbüse ait bilgisayarlar, tablet bilgisayarlar, mobil telefonlar, sunucular başta olmak üzere her türlü elektronik aygıttan müteşekkil sistem "Bilişim Altyapısı" olarak adlandırılacaktır.

verilerin bazılarını yazı dosyaları (*word, excell* vb.), e-postalar, sohbet mesajları (*chat*), yer imleri, veri tabanı dosyaları, resimler, diyagramlar, çizimler, video ve ses dosyaları olarak sıralayabiliriz. Bilgisayarın kendi işleyişi içinde ürettiği elektronik verilerden bazıları ise, e-posta başlıkları, üst veriler, işlem geçmişine ilişkin kayıtlar (*loglar*), internet geçmişi, önbellek, çerezler, dosya yetkileri ve tarihleri, sistem kayıt bilgileri, erişim ve yönlendirme bilgileri, yedekleme dosyaları, yazıcı kuyruğu (*spool*) dosyaları, getir götür dosyaları (*swap files*) ve diğer geçici verilerdir. Sistem üzerinden elde edilebilecek elektronik delillere örnek olarak ise internet iletişim kuralı IP adresi, FTP ve Web sunucusu erişim kayıtları, E-posta sunucusu kullanıcı kayıtları, Abone hesap bilgileri, LAN sunucu kayıtları olarak sıralanabilir (NCJRL 2007, 7).

Gerek bu çalışmanın kapsamı, gerekse de elektronik ortamlara ilişkin verilecek yüzeysel bilgilerin herhangi bir yarar sağlamayacak olması nedenleriyle, incelemeye konu olabilecek elektronik aygıtlar daha ayrıntılı ele alınmamıştır. Sadece, ilerleyen bölümlerde; incelemeye konu olup olamayacağı açısından belli tartışmaların söz konusu olduğu mobil iletişim araçlarına değinilmiştir.

1.2. GENEL OLARAK TÜRK HUKUK SİSTEMİ İÇERİSİNDE ELEKTRONİK DELİL

1.2.1. Ceza Muhakemeleri Kanunu Kapsamında Elektronik Delil

Elektronik delilin delil niteliğine ilişkin esaslı tartışmaların yapıldığı alanlardan birisi de ceza hukukudur. Bunun bir sebebi şüphesiz ceza hukukunda mahkûmiyet hükmü verilebilmesi için suçun şüpheye yer vermeyecek şekilde ortaya konulması gerekliliğidir. Bu sebeple ceza yargılamasında fail, fiil ya da fiil ile bağlantılı bir hususa delalet eden her şey delil olabilmektedir (Özbek 2001, 182). Bu bağlamda bilgisayarlar ve bilgisayar sistemleri üzerindeki kayıtlara da delil olarak başvurulabilmektedir (Malkoç ve Yüksektepe 2008, 639).

Ceza hukukunda ispat standardının yüksek oluşu, kanun koyucuyu elektronik delilin elde edilmesinden yargılama makamınca değerlendirilmesine kadarki sürece ilişkin özel düzenleme yapmaya sevk etmiştir. Bu kapsamda, bilişim sistemleri üzerinden elde edilebilecek elektronik delillerin adaletin hizmetine sunulması amacıyla, 5271 Sayılı Ceza Muhakemesi Kanunu'nda (CMK) elektronik delillerin elde edilmesine ve bilgisayar sistemleri üzerinde arama yapılmasına ilişkin bir arama rejimi oluşturulmuştur.

Türk Ceza Kanunu ve diğer kanunlarda suç olarak tanımlanan fiillerin aydınlatılmasına ilişkin şüphelinin kullandığı bilgisayarlar, bilgisayar programları

ve kütüklerinde arama, kopyalama ve geçici el koyma tedbirlerinin uygulanması CMK'nın 134. maddesi çerçevesinde düzenlenmiştir. Ayrıca, Adli ve Önleme Aramaları Yönetmeliğinin 17. maddesi ve Suç Eşyası Yönetmeliği'nin 9. maddesi[6] ile CMK 134. maddede düzenlenen koruma tedbirlerinin[7] uygulanmasında dikkat edilmesi gereken bazı hususlar düzenlenmiştir.

CMK'nın 134. maddesinin birinci fıkrasında bilgisayar, bilgisayar programları ve veri kütüklerinde yapılacak aramanın şartları düzenlenmiştir. Buna göre, öncelikle *"bir suç dolayısıyla yürütülen bir soruşturma"* kapsamında, *"başka surette delil elde etme imkânının bulunmaması halinde"*, ancak cumhuriyet savcısının talebi üzerine hâkim tarafından verilecek izin çerçevesinde aramanın gerçekleştirilebileceği belirtilmektedir. Buradan hareketle öncelikle; CMK'nın 134. maddesinde öngörülen koruma tedbirlerine sadece CMK kapsamında yürütülen suç soruşturmalarında başvurulabileceği, diğer hukuk alanlarındaki usul ve esaslara göre yürütülen soruşturmalarda (disiplin soruşturması, idari soruşturma vs.) başvurulamayacağı anlaşılmaktadır (Özen ve Baştürk 2011, 144).

Bir diğer önemli husus ise bilgisayarlar üzerinde arama, kopyalama ve el koyma tedbirlerinin uygulanmasında son çare prensibinin (*ultima ratio*) geçerli kılınarak, eğer başka surette delil elde etme yolu[8] varsa bu koruma tedbirlerine başvurulamayacağının hükme bağlanmış olmasıdır. Malkoç ve Yüksektepe'ye (2008, 640) göre başka surette elde edilen delillerin hüküm vermeye yeter derecede kuvvetli olmadığı hallerde de bu koruma tedbirlerine başvurulabilecektir. Zira aynı yazarlar, Kanun koyucunun amacının, diğer yollarla suçun aydınlatılması için yeterli delil elde edilebildiği hallerde, kişinin özel hayat alanında bulunan bilgisayarlara müdahale edilmesinin önüne geçilmesi olduğunu belirtmişlerdir.

CMK'nun 134/1. maddesinde, söz konusu koruma tedbirlerinin *"şüphelinin kullandığı"* bilgisayarlar üzerinde uygulanabileceği düzenlemesine yer verildiği

[6] Suç Eşyası Yönetmeliği m. 9 "… *Bilgisayar, bilgisayar kütükleri ve bu sisteme ilişkin verilerin asıl ya da kopyaları, ses ve görüntü kayıtlarının bulunduğu depolama aygıtları gibi eşya, bozulmalarını engelleyecek, nem, ısı, manyetik alan ve darbelerden korunmalarını sağlayacak uygun ortamda muhafaza edilir…"*

[7] '…Ceza muhakemesinde maddi gerçeğe ulaşılabilmesini sağlayacak delillerin elde edilmesi, delillerin karartılmasının ve şüphelilerin kaçmasının önlenmesi maksadıyla gecikmesinde sakınca bulunan hallerde, geçici olarak bazı kanuni çarelere başvurulmaktadır. Koruma tedbiri olarak adlandırılan ve kesin hükme ulaşılabilmesi için gerekli olan bu tedbirlerin icrası bazı temel hak ve özgürlüklere müdahale edilmesini gerekmektedir.' (Öztürk ve Erdem 2006, 483).

[8] Başka suretle delil elde edememe durumu, diğer delil elde etme yollarının denendiği ve başarılı olunamadığı durumlar ile suçun niteliği itibariyle ancak şüphelinin bilgisayarlarında CMK 134. maddede öngörülen tedbirlere başvurulmak suretiyle delil elde edilebilecek durumlara karşılık gelmektedir.

görülmektedir. Zira şüphelinin kullandığı yerine şüpheliye ait olan ifadesi tercih edilseydi, suçluların kendilerine ait olmayan veya onlara ait olduğu ispatlanamayacak bilgisayarları kullanarak söz konusu tedbirlerin uygulanmasından kaçmalarına olanak sağlayan bir hukuki boşluk doğmuş olacaktı. Dolayısıyla, CMK 134. maddede yer verilen koruma tedbirlerinin uygulama alanı son derece daraltılmış olacaktı (Çolak ve Taşkın 2007, 608).

CMK'nun 134/1. maddesinin ele alınışı bakımından üzerinde durulması gereken bir başka husus ise söz konusu koruma tedbirlerine kovuşturma aşamasında başvurulup başvurulamayacağıdır. Keza maddenin lafzı esas alındığında söz konusu koruma tedbirlerine bir suç dolayısıyla yürütülen soruşturmada başvurulabileceği düzenlenerek *"şüpheli"* gibi soruşturma safhasına has nitelemelere yer verildiği ancak kovuşturma ile ilgili her hangi bir referans içermediği görülmektedir.

Özen ve Baştürk (2011, 144) yargılama esnasında kişinin bilgisayarlarında inceleme yapılmasına engel teşkil edecek bir hüküm olmasa da, Kanun metninde sanık yerine şüpheliden bahsedildiği için kovuşturma aşamasında CMK 134. maddeye başvurulamayacağı ayrıca böyle bir kararın açık duruşmada alınmasının delillerin tahrif edilmesi riskini doğuracağını ifade etmiştir. Malkoç ve Yüksektepe de (2008, 640) böyle bir riskin varlığını kabul etmiş fakat yok edilmemiş olan elektronik delillerden kovuşturma aşamasında yararlanmanın mümkün olduğunu belirtmiştir.

Çolak ve Taşkın ise (2007, 607) bu görüşün tersi yönünde CMK 134. maddede düzenlenen koruma tedbirlerine kovuşturma aşamasında başvurulamayacağını, zira söz konusu tedbirlere ancak başka türlü delil elde edilemeyen durumlarda başvurulabileceğini ifade etmektedir. Buna gerekçe olarak ise kamu davası açılmış olmasının, soruşturma evresinde makul şüphe oluşturacak delile ulaşıldığı anlamını taşıdığını ve ondan sonra CMK 134. maddeye başvurulamayacağını öne sürmektedir.

CMK 134. maddenin devam eden fıkralarında ise koruma tedbirlerinin uygulanması sırasındaki usul ve esasların düzenlendiği görülmektedir. CMK 134. maddenin 2. fıkrasında kişi temel hak ve özgürlüklerine daha kapsamlı bir müdahale anlamı taşıyan el koyma tedbirinin uygulanması isabetli olarak belli şartlara bağlanmış ve etkinen tarafa bir takım hukuki güvenceler tanınmıştır. Bunlar, el koyma tedbirlerine ancak şifre engeli ile karşılaşılması veya gizlenmiş bilgilere ulaşılamaması halinde başvurulabileceği, inceleme tamamlandıktan sonra ise el

koyulan cihazların gecikme olmaksızın iade edileceği yönündeki hükümlerdir.

CMK 134. maddesinin 3. fıkrasında el koyma işlemi sırasında bütün verilerin yedekleneceği, 4. fıkrasında ise istenmesi halinden yedekten bir kopya da şüpheliye veya vekiline verileceği belirtilmektedir. Bu suretle, elektronik ortamdaki verilerin geride iz bırakılmadan değiştirilmesi, ekleme ve çıkarma yapılması mümkün olduğundan, elektronik deliller üzerinde kolluk kuvvetlerinin tasarrufu sınırlandırılarak şüpheli bakımından hukuki güvence sağlanmaktadır (Sevimli 2007, 997; Özen ve Baştürk 2011, 158). Aynı maddenin 5. fıkrasında ise el koymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyasının alınabileceği, kopyası alınan verilerin kâğıda yazdırılarak tutanağa bağlanacağı ve ilgililer tarafından imzalanacağı düzenlenmektedir.

Adli ve Önleme Aramaları Yönetmeliğinin 17. maddesi de temelde CMK 134. maddeye paralellik arz etmekle birlikte CMK 134. maddeden farklı olarak, el koyma işleminin bilgisayarların yanı sıra, bilgisayar ağları, uzak bilgisayarlar ve çıkarılabilir donanımlar için de geçerli kılındığı görülmektedir.

Her ne kadar CMK 134. madde ile ihdas edilen bu hukuki çerçeve bir yandan delil elde edilmesine ve bu arada şüpheli haklarının korunmasına yönelik bir hüküm olsa da, bir takım altyapı yetersizliklerinin de katkısıyla kanun hükmüyle uygulamanın uyumundan söz etmek güçleşmektedir. Gelecekte Kurum uygulamasını geliştirmeye dönük düzenlemeler açısından yol gösterici olabileceği düşüncesinden hareketle CMK 134. maddede öngörülen arama rejiminin aksayan yönlerine bilahare Ek:1'de yer verilmektedir.

1.2.2. Hukuk Yargılamasında Elektronik Delil

1.2.2.1. 6100 Sayılı Hukuk Muhakemeleri Kanunu Kapsamında Elektronik Delil

6100 sayılı Hukuk Muhakemeleri Kanunu'nda (HMK) yürürlükten kalkan 1086 sayılı Hukuk Usulü Muhakemeleri Kanun'dan (HUMK) farklı olarak "senet[9]" yerine "belge ve senet" ibaresine yer verilerek, "belge" kavramı da delil olarak düzenlenmiştir. Böylece, Türk hukukunda ilk kez belge kavramı senet kavramından ayrıştırılarak; senet kavramını da içine alan bir üst kavram olarak kabul edilmiştir. Belge, HMK'nın 199. maddesinin 1. fıkrası ile "uyuşmazlık konusu vakıaları ispata elverişli yazılı veya basılı metin, senet, çizim, plan, kroki, fotoğraf, film,

[9] Senet, kesin olarak kullanılan ve kanunun özel bir anlam yüklediği belge türüdür. Oysa her belge senet olmadığı gibi, kanunun senet dışında da delil olarak kabul ettiği belgeler mevcuttur. Örneğin; yazılı delil başlangıcı, niteliği itibarıyla bir belgedir, ancak kanunda kabul edilen şekliyle senet değildir.

görüntü veya ses kaydı gibi veriler ile elektronik ortamdaki veriler ve bunlara benzer bilgi taşıyıcıları" olarak tanımlanmaktadır[10]. Bu tanım ile elektronik verilere delil olarak başvurulup başvurulamayacağı konusunda oluşabilecek belirsizlik ortadan kaldırılmış, ayrıca HMK 219 vd. maddelerinde yer alan "belgelerin ibrazı zorunluluğu"'nun elektronik veriler açısından uygulanabilmesinin önü açılmıştır (Göksu 2011, 148).

Göksu'ya göre (2011, 149) HMK'da senet tanımı yapılmadığı ve elektronik belgelerin senet yerine geçebilecekleri bir istisnadan bahsedilmediği için elektronik belgelere senet olarak dayanılamayacak, sadece senetle ispat mecburiyetinin bulunmadığı uyuşmazlıklar bakımından delil olarak başvurulabilecektir. Bu bakımdan delil sözleşmeleri ile kesin delil yaratılamayacağından, taraflar arasında elektronik kayıtların delil olarak kabul edileceğine ilişkin akdedilecek delil sözleşmesi ile elektronik kayıtlara delil olarak dayanılabilecektir. Aksi takdirde ancak, delil başlangıcı veya özel hüküm sebebi olarak kullanılabilmeleri mümkün olacaktır (Avşar ve Öngören 2010, 195) .

HMK 202. maddesinin ikinci fıkrasında: *"Delil başlangıcı; iddia konusu hukuki işlemin tamamen ispatına yeterli olmamakla birlikte, söz konusu hukuki işlemi muhtemel gösteren ve kendisine karşı ileri sürülen kimse veya temsilci tarafından verilmiş veya gönderilmiş belgedir"* denilmektedir. Bu kapsamda, HMK'nın 199. maddesinin 1. fıkrası çerçevesinde "belge"[11] tarifine uyan, tek başına ispat gücünü haiz olmayan fakat söz konusu hukuki işlemi muhtemel gösteren ve karşı taraftan sadır olmuş araçların "delil başlangıcı" olabileceği hususunun düzenlendiği görülmektedir.

Düzenlemeye ilişkin bir başka dikkate değer nokta ise HUMK m.292[12]'den farklı olarak, HMK'nın 202. maddesinde "gönderilmiş" ibaresine yer verilmesidir. Kanun koyucunun bu tercihinin belirlenmesine ilişkin olarak HMK 202. maddenin

[10] Kanun gerekçesinden belge kavramına ilişkin tereddütlerin ortadan kaldırılması ve senet kavramı ile karıştırılmaması için sınırlayıcı olmayan fakat belgenin ne olduğuna yönelik çerçeveyi belirleyen bir tanım getirildiği anlaşılmaktadır. Bu sayede gelecekte, senet ve güvenli elektronik imza ile imzalanmış elektronik belge gibi kesin delil olarak kabul edilebilecek ispat gücüne ve güvenilirliğe sahip bir bilgi taşıyıcısı ortaya çıkarsa kanunun sistematiği değişmeden kesin delil olarak kabul edilebilecektir. Ayrıca; her belgenin bir "bilgi taşıyıcısı" olduğu ancak sadece uyuşmazlık konusu vakıaları ispata elverişli olanların, yargılama hukuku anlamında belge niteliği taşıyacağı belirtilmiştir.

[11] HUMK m.292'deki *"yazılı delil başlangıcı (tahrirî mukaddimei beyine)" ifadesi, HMK m.202'de, "**delil başlangıcı**" ifadesiyle değiştirilmiştir. Bu doğrultuda "delil başlangıcı" için "yazılı olma" şartının yerine "belge" olma şartı getirilmiştir.*

[12] HUMK m. 292: *'...Mukaddimei beyyine müddeabihin tamamen sübutuna kafi olmamakla beraber bunun vukuuna delalet eden ve aleyhine ibraz edilmiş olan taraf canibinden **verilen** evrak ve vesaiktir.'*

gerekçesinde; *"haberleşmenin önemli bir türünü oluşturan faks mesajlarının delil değerini, delil başlangıcı olarak benimseyen içtihatlarla uyum sağlanması amacıyla, ... **faks mesajı** ve bu konudaki benzer yollarla göndermenin, bir belgenin verilip verilmemesi sayılmasına ilişkin tereddüt ve tartışmaların önüne geçilebilecek, teknik araçlarla gönderilen belgeler de delil başlangıcı sayılabilecektir"* açıklamasına yer verilmiştir (Yılmaz 2011, 243).

HMK'nın 219. maddesinde tarafların, kendilerinin veya karşı tarafın delil olarak dayandıkları ve ellerinde bulunan tüm belgeleri mahkemeye ibraz etmek zorunda oldukları, elektronik belgelerin ise belgenin çıktısı alınarak ve talep edildiğinde incelemeye elverişli şekilde elektronik ortama kaydedilerek mahkemeye ibraz edilebileceği düzenlenmektedir. HUMK'ta sadece özel belgelerin halefler aleyhine kullanılması düzenlenmiş iken, bunun elektronik veriler de dâhil tüm belgeleri kapsayacak şekilde değiştirildiği görülmektedir.

1.2.2.2. 4054 Sayılı Kanun'da HUMK'a Yapılan Atıf Çerçevesinde Elektronik Delil

4054 sayılı Kanun *"Sözlü Savunma Toplantısına İlişkin Esaslar"* 47. maddesinde *"Sözlü savunmada ilgili taraflar Hukuk Usulü Muhakemeleri Kanununun İkinci Babının Sekizinci Faslında düzenlenen her türlü delil ve ispat vasıtasından yararlanabilirler."* ifadesiyle HMK'ya[13] atıfta bulunulmuştur. Bu atıf çerçevesinde sözlü savunmalarda rekabet hukukunda geçerli olan diğer ispat vasıtalarıyla birlikte HMK'da yer alan delil ve ispat vasıtalarına başvurulabileceği anlaşılmaktadır.

HUMK'nın yürürlükte olduğu dönemde, elektronik kayıtların delil olmalarına ilişkin herhangi bir düzenleme yer almamakta ve elektronik kayıtlar özel hüküm sebepleri kapsamında değerlendirilmekteydi. Fakat buna rağmen, sözlü savunma aşamasında kullanılabilecek ispat araçları HUMK'a yapılan atıfla sınırlandırılmadığı için elektronik kayıtlara delil olarak başvurulması mümkün olmaktaydı.

HMK ile birlikte belge kavramının düzenlenmesi, Kanun'da HUMK'a yapılan atıf bakımından, rekabet hukuku incelemelerinde ağırlıklı olarak kullanılan elektronik kayıtların delil niteliğini netleştirmiştir. Bu sebeple HMK ile getirilen

[13] 4054 sayılı Kanun'un 47. maddesinde HUMK'a atıf yapılmış, fakat 6100 sayılı HMK'nın 01.10.2011 tarihinde yürürlüğe girmesi ile HUMK mülga olmuştur. Dolayısıyla, HMK'nın 447/2. maddesi uyarınca diğer kanunlarda 1086 sayılı Kanun'a yapılan yollamalar bakımından HMK'nın ilgili hükümleri geçerli olacaktır.

yenilikler, elektronik delillerin özel hukuk alanında kullanımı açısından önemli bir değişikliği ifade ediyor olsa da 4054 sayılı Kanun'da yapılan göndermenin işlevselliği açısından yenilik doğurmadığını söylemek yanlış olmayacaktır.

1.3. GENEL OLARAK REKABET HUKUKU UYGULAMALARI KAPSAMINDA ELEKTRONİK DELİL

1.3.1. Yerinde İncelemeler Açısından Elektronik Delil Elde Etmenin Önemi

Rekabeti kısıtlayıcı eylemlere kalkışanların, rekabet ihlallerinin doğası gereği bu eylemlerinin gizli kalması için çaba gösterdikleri dikkate alındığında yerinde incelemeler bu ihlallerin ortaya çıkarılması için gerekli delilleri elde edebilmenin tek alternatifi olarak karşımıza çıkmaktadır (OECD 2013, 4). Elektronik ortamda, verilerin daha hızlı ve kolay bir şekilde işlenebilir, erişilebilir ve paylaşılabilir olması, etkin bir yönetim isteyen teşebbüslerin ticari faaliyetlerini ve iletişimlerini elektronik ortama kaydırmasına neden olmaktadır[14]. Bu açıdan, iddia konusu bir rekabet ihlali bakımından delil değeri taşıyan çoğu bilgi ve belge[15], elektronik ortam haricinde var olmamaktadır. Teşebbüsün rakipleri ve müşterileri ile yazışmaları, teşebbüsün stratejilerine ilişkin iç yazışmalar bu kapsamda örnek olarak gösterilebilir. Kâğıda dayalı sistemde elde edilmesi mümkün olmayan birçok belge, taslak metin, belgenin ne zaman, kim tarafından oluşturulduğu gibi bilgiler, elektronik ortamda saklanmakta ve tespit edilebilmektedir.

Nitekim farklı ülke uygulamalarına bakıldığında rekabet ihlalleri ile mücadelede elektronik delil aramasının yoğun olarak kullanıldığı görülmektedir. ICN'in "Elektronik Delillerin Elde Edilmesi" konulu çalışmasına göre (2010, 5) çalışmaya iştirak eden rekabet otoritelerinin %92'sinin elektronik delil elde etme yetkisi bulunmakta ve %83'ü ise aktif olarak elektronik delil araması gerçekleştirmektedir.

Bu bakımdan günümüzde yerinde incelemeler nerdeyse tamamen teşebbüsün bilişim alt yapısı üzerinde elektronik delil araması şeklinde cereyan etmektedir. Bu açıdan, rekabet ihlalleri ile mücadelede yerinde incelemelerin etkin kılınması;

[14] Cybersecurity Information Exchange Techniques Initiative'nin (CYBEX) "Elektronik Delillerin Mahkemede Kabul Edilebilirliği" konulu raporda her yıl kurum ve kuruluşlarda oluşturulan belgelerin %90'ından fazlasının elektronik ortamda oluşturulduğu ve bunların %30'undan daha azının basılı kopyasının alındığı istatistiğine yer verilmiştir (2006, 25).

[15] Bu çalışma boyunca; elektronik belge, elektronik kayıt, bilgisayar kayıtları terimleri, elektronik ortamda oluşturulan bir bilgiyi ifade edecek şekilde, aynı anlamda kullanılmıştır.

sıradan elektronik delil toplama yöntemlerinin ötesine geçen uzmanlaşma, kabiliyet ve tecrübeyi gerektirmektedir.

1.3.2. Elektronik Delil Aramasının Geleneksel Delil Araması İle Karşılaştırılması

1.3.2.1. Elektronik Delillerin Geleneksel Delillere Göre Sunmuş Olduğu Avantajlar

Elektronik delillerin, geleneksel delillerden ayrılan ilk yönü kolayca ortadan kaldırılamamalarıdır. Sanılanın aksine bilgisayarda gerçekleştirilen basit silme işlemi elektronik veriyi tamamen ortadan kaldırmamakta, silinen elektronik verinin hard disk üzerinde kapladığı yer boşluk olarak işaretlenerek sonradan veri yazmaya müsait hale getirilmektedir. Bilgisayar tarafından silinmiş olarak işaretlenen bölüm üzerine yeni veri yazılmadığı sürece silinen verilerin geri getirilmesi mümkün olmaktadır. Ayrıca, bir dosya silindiğinde genellikle, yedekleme ünitesinde ya da arşiv dosyaları arasında belli bir süre için sistem tarafından muhafaza edilmektedir. Bu nedenle, kullanıcı tarafından silindiği sanılan elektronik veriler, adli bilişim uzmanları tarafından çeşitli veri kurtarma yöntemleri ile çoğu zaman kurtarılabilmekte[16] ve suçun aydınlatılmasında adaletin hizmetine sunulabilmektedir (Chung ve Byer 1998, 186).

Aynı zamanda, delilleri yok etme saiki ile hareket eden teşebbüsün, elektronik delilleri tam olarak ortadan kaldırdığına emin olabilmesi daha zordur. Şöyle ki bir bilgisayar sisteminde gerçekleşen her bir işlem için o işleme ilişkin sistemin birden çok yerinde kayıt tutulmaktadır. Bu bakımdan, elektronik delillere yapılacak herhangi bir müdahale sistem üzerinde adli bilişim uzmanlarının gözünden kaçmayacak izler bırakmaktadır (Yıldız ve Zirve 2013, 366).

Elektronik deliller ile geleneksel deliller arasındaki bir diğer fark ise delillerin içeriği noktasında ortaya çıkmaktadır. Basılı halde bulunan dokümanlardan elde edilebilecek bilgiler, dokümanın içeriği ile sınırlıdır. Dijital ortamdaki bilgilerden ise üst veri *(metadata)* olarak adlandırılan, bilginin içeriğinin yanı sıra, bilginin ne zaman, kim tarafından oluşturulduğu, değiştirildiği, erişildiği, silindiği gibi, hatta bazı durumlar da hangi değişikliklerin yapıldığı gibi ikincil veriler de elde etmek mümkündür (ICN 2010, 4).

[16] Veri kurtarma veriye ulaşmayı engelleyen donanımsal arızalar veya veriye ulaşmayı engelleyen yazılım unsurlarının aşılarak veriye tekrardan ulaşılmasının sağlanmasıdır (Dokurer 2013, 362).

1.3.2.2. Elektronik Delillerin Geleneksel Delillere Göre Dezavantajları

Elektronik ortamda gerçekleştirilen delil araması, sağladığı avantajların yanı sıra birtakım dezavantajları da beraberinde getirmektedir. Bu dezavantajlardan en önemlisi elektronik delillerin değişikliğe uğramaya müsait yapıları olarak gösterilebilir. Zira basılı dokümanların iradi olarak yok edilmeleri dışında ancak yangın, sel gibi istisnai durumlarda yok olmaları söz konusuyken, elektronik deliller bilişim sistemlerinin günlük işleyişi içinde, inceleme esnasında, manyetik ortam, yüksek sıcaklık gibi fiziki şartlar nedeniyle değişikliğe uğrayabilir ya da yok olabilir. Örneğin ağ üzerinde çalıştırılan bir uygulama kullanıcının bilgisi haricinde ağ üzerindeki kayıtları değiştirebilir, yok edebilir. Yine benzer şekilde bir bilgisayarın çalıştırılması ya da bir dosyanın açılması sabit disk üzerinde değişikliğe yol açabilir (Zheng 2009, 4).

Üzerinde durulması gerekli olan bir diğer husus ise delil niteliği taşıyabilecek elektronik verilerin saptanması sorunudur. Elektronik veriler basılı dokümanlara kıyasen çok daha hızlı ve kolay bir şekilde başka bir yere nakledilebilmekte ve çok büyük miktarlarda olsalar bile zahmetsizce muhafaza edilebilmektedir. Elektronik veriler bu özellikleri itibariyle incelemenin gerçekleştirildiği yerden farklı bir yerde, hatta farklı bir ülkede, teşebbüsün kendisine veya başkasına ait sunucular üzerinde bulunabilmektedir. Bu nedenle, elektronik verilerin gerek sanal ortamda herhangi bir yerde tutulabilmeleri ve bu verilere zaman ve mekân kısıtı olmadan ulaşılabilmesi, gerekse de büyük miktarda verinin küçük bir elektronik aygıtın içine sığdırılabilmesi nedeniyle elektronik verilere ulaşılmasının fiziki dokümanlara göre daha zor olduğu ifade edilebilir (Withers 2000).

1.3.3. Rekabet Otoritelerinin Elektronik Delil elde Etme Yöntemleri

Rekabet otoriteleri tarafından yerinde inceleme yetkisi ve bilgi isteme yetkisi olmak üzere iki temel yetki çerçevesinde elektronik delil elde edilebilmektedir (ICN 2010, 6). Bunlar, teşebbüsün bilgi isteme talebinin gereği olarak elektronik delilleri sağladığı bilgi isteme yetkisi ve teşebbüsün bilişim sistemleri üzerinde delil aramasının gerçekleştirildiği yerinde inceleme yetkisidir.

Neredeyse bütün rekabet otoritelerinin elektronik delil elde etme yetkisi bulunmaktadır. Fakat yerinde inceleme yetkisi bakımından belirleyici olan yetkinin sınırlarıdır. Elektronik delil elde etme yetkisinin kimi rekabet otoriteleri tarafından sabit disklerin adli kopyaları alınarak kendi ofislerinde incelenmesi şeklinde kullanılabildiği, kimi rekabet otoritelerinin ise sadece basit kopya almaya yetkili oldukları ve elektronik verileri teşebbüste ayrıştırmakla yükümlü oldukları

görülmektedir (ECN 2012, 14). Dolayısıyla, elektronik delil elde edilmesi süreci yetkinin kapsamı çerçevesinde şekillenmektedir.

Aynı şekilde, bilgi isteme yetkisi kapsamında da benzer bir ayrımdan bahsedilebilir. Elektronik delillerin elde edilmesi açısından bilgi isteme yetkisinin, teşebbüslerin rekabet otoritesi tarafından talep edilen, mevcutta olan veya talep üzerine üretilen elektronik belgeleri sağlaması aracı olarak kullanılması, sınırlı bir anlam ifade etmektedir. Elektronik delil elde etme açısından anlamlı olan; bilgi isteme yetkisinin ICN metninde *"compelled discovery"* terimi altında açıklanan, teşebbüsün inceleme konusu açısından delil değeri taşıyabilecek her türlü bilgi ve belgeyi muhafaza etmekle yükümlü olduğu, bilgi talebi çerçevesinde delil aramasını rekabet otoritesi adına teşebbüsün gerçekleştirdiği uygulama şeklidir (2010, 6). Bilgi isteme yetkisinin bu şekliyle kullanımı Birleşik Devletler uygulamasının ele alındığı kısımda irdelenmiştir.

1.4. REKABET HUKUKU UYGULAMALARI KAPSAMINDA ADLİ BİLİŞİM

1.4.1. Genel Olarak Adli Bilişim

Elektronik delillerin, delil niteliğini kaybetmeden, karar mercileri tarafından kabul edilebilirlik niteliğini haiz olarak dış dünyaya aktarılmaları açısından bir takım bilimsel inceleme ve analiz metotlarına başvurulması gerekmektedir. Bir adli bilim dalı olan adli bilişim ise bu noktada, elektronik ortamda yer alan her türlü verinin ispat hukuku açısından delil niteliği taşıyacak şekilde elde edilmesinden, mahkemeye sunulmasına kadar geçen süreçlerde bilgisayar bilimlerinin kullanılması olarak karşımıza çıkmaktadır.

Gerek bu çalışmanın kapsamı, gerekse de genel kabul görmüş standartlara göre yürütülen adli bilişim uygulamalarına ilişkin esaslı tartışmaların bulunmaması nedeniyle; oldukça geniş bir alanı kapsayan adli bilişimle ile ilgili olarak daha detaylı değerlendirmelerde bulunulmasına gerek görülmemiştir. Çalışmamızda Kurum'un elektronik delil elde etme süreci bakımından önem arz eden bazı temel adli bilişim ilkeleri ile Kurum'un mevcut uygulaması dâhilinde adli bilişim araçlarının işlevsel kılınmasının gerekliliğine değinilecektir.

1.4.2. Adli Bilişim Süreçleri

Suç mahallinde bulunan ve kolayca suçla ilişkilendirilebilen klasik delillerden farklı olarak elektronik ortamdaki bulguların delil niteliği kazanmaları ve karar mercileri tarafından geçerliliklerinin kabul edilmesi için belli süreçlerin takip edilmesi ve birtakım prosedürlerin yerine getirilmesi gerekir. Elektronik delillerin

elde edilmesine ilişkin adli bilişim süreci; delillerin elde edilmesi (*acquisition*), tanımlanması (*identification*), değerlendirilmesi (*evaluation*) ve sunulması (*presentation*) olmak üzere dört aşamaya indirgenerek ele alınabilir (Maras 2012, 32; Akarslan 2012, 123).

Adli bilişim sürecinin belli aşamalara indirgenerek ele alınması elektronik delillerin kendilerine has niteliklerinin oluşturduğu bir gerekliliktir. Elektronik delillerin değişmeye müsait yapıları ve elektronik delil ile delilin atfedildiği kişi arasındaki ilişkinin farazi olması nedeniyle; gerek elektronik delillerin her aşamada aslına uygun olarak korunması gerekse de elektronik delilin kaynağı ile bağının güvenli bir şekilde kurulabilmesi bu türden bir sistematiğin takip edilmesini zorunlu kılmaktadır. Örneğin, elektronik delillerin karar mercileri tarafından anlaşılmasında ve kabul edilmesindeki zorluklar, elektronik delillerin raporlanması ve sunulması gerekliliğini doğurmaktadır.

Adli bilişim süreçlerinin ilki olan, elektronik delillerin elde edilmesi aşaması genellikle adli bilişim incelemesinin gerçekleştirildiği mahaldeki uygulamaları kapsamaktadır. Laboratuvar ortamında elektronik delillerin açığa çıkartılması ve değerlendirilmesi bu aşamada elde edilen adli kopyalar ya da el koyulan elektronik cihazlar[17] üzerinde gerçekleştirilmektedir. Delillerin elde edilmesi süreci, takip eden adli bilişim süreçlerinin geçerliliğini etkileyecek öneme sahiptir, bu nedenle olay yerinden başlayarak bir dizi önlemler alınması ve olay yerinde gerçekleştirilen adli bilişim uygulamalarına ilişkin genel kurallar[18] çerçevesinde hareket edilmesi gerekmektedir (Henkoğlu 2011, 24).

Elektronik delillerin tanımlanması aşaması; delilin nerede, ne şekilde, hangi formatta kaydedilmiş olduğunu ve bu doğrultuda hangi araç ve yöntemlerin (*keyword searching*, *file carving* vb.) kullanılacağının belirlendiği aşamadır. Elektronik delillerin analizi aşaması ise elektronik delillerin bulundukları ortamdan açığa çıkartıldığı ve yorumlandığı aşamadır. Elde edilen elektronik delillerin geçerliliği ve güvenilirliği de bu aşamada sınanır. Zira sadece hukuka uygun olarak elde edilmiş; açığa çıkartılması, analiz edilmesi, taşınması, muhafaza edilmesi

[17] Adli bilişim incelemesi her zaman alınacak bire bir kopyalar üzerinden gerçekleştirilir, orijinal kopyalar üzerinde işlem yapılmaz.

[18] Amerika Birleşik Devletleri Adalet Bakanlığı tarafından yayımlanan Bilgisayar ve bilgisayar sistemleri üzerinde gerçekleştirilecek adli bilişim uygulamalarına ilişkin olarak olay yeri davranışlarını düzenleyen örnek kılavuz için Bkz. A Guide for First Responders https://www.ncjrs.gov/pdffiles1/nij/187736.pdf erişim tarihi: 26.01.2013

süreçleri standartlara uygun olarak gerçekleştirilmiş elektronik deliller geçerlilik kazanacak ve değerlendirmeye alınacaktır (Maras 2012, 35).

Nihai aşama olan elektronik delillerin sunumu aşaması ise elektronik delilin elde edilme sürecinde kullanılan araç ve yöntemlerin niteliği, güvenilirliği ve elektronik delilin anlaşılması için gerekli olan uzman görüşünün karar mercilerine raporlanması, ya da bu hususların adli bilişim uzmanı tarafından yargılama sürecinde bizzat sunulmasını kapsamaktadır (Ghosh 2004, 24).

1.4.3. Adli Bilişim süreçlerinde Uyulması Gerekli İlkeler

Bir materyalin yüzeyinde fiziksel kalıntılar bırakılarak oluşturulan yazılı kayıtlar bakımından, bu kayıtların kim tarafından oluşturulduğu, değişip değişmediği, ne ölçüde değiştiği gibi unsurlar, çıplak gözle ya da laboratuvar ortamında test edilmek suretiyle saptanabilmektedir. Fakat elektronik deliller açısından, elektronik ortamda bulunan veri fiziksel bir materyale ilişkilendirilmeden, manyetik ortam üzerinde sayı dizileri şeklinde muhafaza edilmektedir. Elektronik deliller bu yapıları itibariyle gerek çevresel etmenlerin etkisiyle, gerekse de yazılım veya donanım hataları sebebiyle değişikliğe uğramaya müsaittirler.

Eğer önceden elektronik delillerin daha sonra aslına uygun korunup korunmadığını test etmeye imkân tanıyacak tedbirler alınmazsa, elektronik delillerin gerçekliğinin saptanması mümkün olmayacaktır. Bu nedenle, delil hukuku açısından bu durum, elektronik delillerin güvenilirliğinin ve geçerliliğinin önünde engel teşkil etmekte ve elektronik delillerin gerçekliğinin ortaya konabilmesi için adli bilişim süreçlerinde belli kurallara riayet edilmesini zorunlu kılmaktadır (Paul 2008, 15).

1.4.3.1. Elektronik Delillerin Gerçekliği (Authentication)

Elektronik delillerin elde edildiği haliyle, değişmeden korunup korunmadığının belirlenmesinde *üç* temel yöntem kullanılmaktadır. Bunlardan ilki, elektronik delilin orijinalinin[19] bir diğer ifadeyle elde edildiği andaki halinin kriptografik özet değerinin, son durumdaki özet değeri ile kıyaslanmasıdır. İkincisi, *"Checksum"* olarak adlandırılan elektronik verinin her *"bayt"ına* 16 ya da 32 *"bit"*lik bir polinomun uygulanması ve çıkan 16 ya da 32 *"bit"*lik değerin muhafaza

[19] Teknik açıdan elde edilen verinin her zaman orijinal hali ile kıyaslanması mümkün değildir. Örneğin; çalışır durumdaki bir bilgisayarın geçici belleğinin (RAM) içeriği sürekli olarak değişmektedir, benzer şekilde bir ağ üzerindeki trafik te kısa aralıklarla değişkenlik gösteren bir yapıdadır. Bu yüzden bu tür değişken sistemler üzerindeki verilerin kopyaları, belli bir an için alınabilmekte, sonrasına orijinali ile kıyaslama imkânı olmamaktadır (Casey 2011, 59).

edilerek, daha sonra aynı işlem tekrarlandığında bulunan değerle kıyaslanmasıdır. Üçüncüsü ise, imza sahibinin kimliğini elektronik veriyle ilişkilendirerek elektronik verinin değiştirilmediğini ispatlayan güvenli elektronik imzadır (Hosmer 2002). Bu uygulamalardan ağırlıklı olarak kullanılan, kriptografik özet alma işlemine aşağıda genel hatlarıyla değinilmiştir.

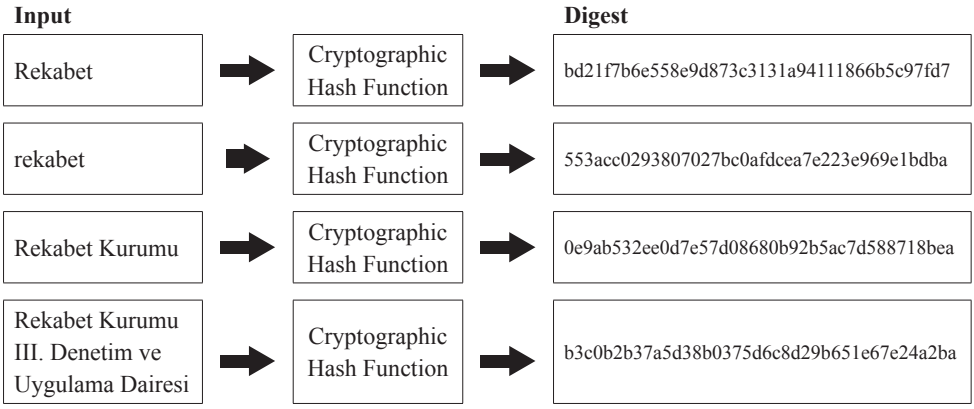
Bununla birlikte; Adli bilişim uygulamaları ağırlıklı olarak adli bilişim yazılımları ve donanımları ile yürütüldüğünden elektronik delilin sağlamlığı, kullanılan adli bilişim araçlarının standartlara[20] uygun ve hatasız olarak fonksiyonlarını yerine getirebilmesine bağlıdır (Giova 2011, 2). Kullanılan adli bilişim araçlarından kaynaklı en küçük hata bile elektronik delilin tahrif olmasına yol açarak ulaşılmak istenen gerçeğin yönünü saptırabilir (Özdemir 2013, 2). Bu nedenle adli bilişim araçlarının standartlara uygunluğu adli bilişim alanında fazlaca üzerinde durulan bir husustur.

1.4.3.1.1. Kriptografik Özet (Hash Value)

Elektronik veri setinin elde edildikten sonra herhangi bir değişikliğe uğramadığının, veri bütünlüğünün korunduğunun gösterilmesi için elektronik verinin elde edildiği andaki kriptografik özeti ile mevcut durumdaki kriptografik özetinin karşılaştırılması yöntemi kullanılmaktadır. Uygulamada, adli kopyası alınmış olan orijinal elektronik delil üzerinden tekrar adli kopya alınarak kriptografik özet değerleri karşılaştırılmakta, karşılaştırma sonucu özet değerleri birbirini teyit etmez ise elektronik aygıt üzerinde değişiklik yapıldığı gerekçesiyle delil olarak kabul edilmemektedir (Özbek 2013, 255).

Kriptografik özet bir verinin veya veri depolama biriminin ilk sektörden başlanıp son sektöre kadar tamamının, belirli bir algoritmik fonksiyondan geçirilmesiyle elde edilmektedir (Özbek 2013, 256). Kriptografik özet değerini hesaplamada kullanılan çeşitli algoritmik fonksiyonlar bulunmakla birlikte, en yoğun olarak kullanılan MD5 ve SHA-1 algoritmalarıdır. Örneğin, Birleşik Devletler adli bilişim uygulamalarında SHA algoritmik fonksiyonunu kullanmaktadır (Casey 2011, 22). Şekil 1'de SHA algoritmik fonksiyonundan geçirilmiş verilere karşılık gelen kriptografik özetler görülmektedir.

[20] Adli bilişim uygulamalarında kullanılan yazılımların testlerine ilişkin sonuçlar için bkz. Computer Forensics Tool Testing Handbook (2012) http://www.cftt.nist.gov/CFTT-Booklet-Revised-02012012.pdf



Şekil 1: SHA1 *Kriptografik Özet Algoritması İle Farklı Verilerin Kriptografik Özet Değerleri*

Yerinde incelemelerde elektronik formatta alınan verilerin mutlaka, kriptografik özetlerinin alınarak tutanağa geçirilmesi gerekmektedir. Bu gereklilik, incelemede elde edilen elektronik verilerin daha sonra delil olarak kullanılacak elektronik verilerle aynı olduğunun kesin olarak ortaya konulabilmesi ve bu suretle teşebbüse elektronik delillerin değişikliğe uğramadığına ilişkin hukuki güvence sağlanması açısından önem taşımaktadır.

1.4.3.2. Delil Zinciri

Delil zincirinin sağlanması, adli bilişim süreçleri izlenirken elektronik deliller üzerinde yapılan her türlü işlemin, işlemi gerçekleştirenin, işlemin nerede, ne zaman ve hangi aşamada gerçekleştirildiğinin kayıt altına alınmasını ifade etmektedir (Casey 2011, 20). Delil zincirinin kurulması elektronik delillerin elde edilmesinden sonra kolluk veya adli makamlar elinde değiştirilmiş olduğuna ilişkin öne sürülebilecek iddiaların gerçek olup olmadığını değerlendirilebilmesi açısından önem taşımaktadır. Öte yandan, adli bilişim süreçlerinde temel amaç elektronik delillerin herhangi bir değişikliğe uğramamasını sağlamak olsa da bazı durumlarda elektronik delillerin değişmesi kaçınılmazdır. Bu nedenle delil zincirinin sağlanması, değişmenin kaçınılmaz olduğu bu gibi durumlarda değişikliğin gerekçesinin ve niteliğinin açıklanarak ele alınmasını da kapsamaktadır (Ghosh 2004, 4).

Aynı zamanda, delil zincirinin sağlanması kapsamında elektronik delillere hangi aşamada kim tarafından temas edildiğinin kaydedilmesi, o kişinin tanıklığına başvurulabilmesi açısından önemlidir. Delil zincirinde eksikliklerin olması, delilin ele alındığı her aşamada dokümantasyonun gereği gibi yapılmaması durumunda

karar mercii tarafından delilin hukuka uygun olarak elde edilmediği, üzerinde oynandığı, suç unsuru delille değiştirildiği öne sürülebilir (Casey 2011, 60).

Nitekim delil zincirinin kurulmuş olması, delilin aslına uygunluğunu ortaya koymak suretiyle hukuka uygunluğunu göstereceği için Yargıtay 9. Dava Dairesinin bir kararında[21] öncelikle sanığa ait USB belleklerden elde edilen elektronik delillerin elde edilmelerinden itibaren güvenli biçimde korunarak adli makamlara teslim edilip edilmedikleri saptanmış ardından içerik yönüyle değerlendirilmiştir.

Kurum'un mevcut uygulamasında elektronik deliller bilgisayar çıktıları halinde teslim alındığından dolayı delil zinciri ilkeleri uygulama alanı bulamamaktadır. İleriki dönemde yerinde incelemelerde elde edilen elektronik delillerin elektronik formatta muhafaza edilmesi benimsendiği takdirde, konuya ilişkin yerleşmiş ilkelerin[22] elektronik delil elde etme sürecinin bir parçası olarak işlevsel kılınması gerekecektir.

1.4.4. Adli Bilişim Araçları

Elektronik delillerin elde edilmesi süreci, herhangi bir yerde bulunabilen ve herhangi bir şekilde ulaşılabilen klasik delillerden farklı olarak, uygun yazılım ve donanımların kullanılması gerekliliğini ortaya çıkarmaktadır (Özocak 2011, 114). Bu nedenle, adli bilişim uygulamalarında amaca özgülenmiş çeşitli adli bilişim araçlarına başvurulmaktadır.

Adli bilişim alanında kullanılan gerek açık kaynak kodlu ve gerekse de ticari olmak üzere çok sayıda yazılım bulunmaktadır. Adli bilişim uzmanlarınca bu yazılımların içinden fonksiyonellik, kullanım kolaylığı, maliyet ve incelenen suçun niteliği gibi kriterler göz önünden bulundurularak seçim yapılabilmektedir (Arthur ve Venter 2004, 3). Bu durumu bir örnek ile açıklamak gerekirse; mobil iletişim cihazları üzerinde elektronik delil araması yapılması gerekliliği doğacak bir soruşturmada cep bilgisayarları ve cep telefonlarının incelenmesine olanak sağlayan *Paraben®,* muadili sayılabilecek *FTK®* yazılımından bir adım öne çıkacaktır (Henkoğlu 2011, 44). Maliyet unsuru ise yazılımın ticari yazılım mı yoksa ücretsiz kullanılabilen açık kaynak kodlu yazılım olduğuna göre şekillenmektedir.

Rekabet otoriteleri elektronik delillerin elde edilmesinde çoğunlukla piyasada mevcut adli bilişim araçlarını kullanmaktadır. Otoritenin ihtiyacına göre

[21] Yargıtay 9. Dava Dairesi, Esas No: 2012/11543, Karar No: 2013/3370, Karar Tarihi: 06.03.2013

[22] Delil zincirinin korunmasına ilişkin ayrıntılı bilgi için bkz. (ICN 2010, 15), (Casey 2011, 21), (Cosic ve Cosic 2012)

özel olarak geliştirilmiş yazılım oldukça az bulunmaktadır (ICN 2010, 11). Örneğin; Avrupa Birliği Komisyonu Rekabet Genel Müdürlüğü (Komisyon), dünyada başka elektronik delil araması yapan kurumların da kullandığı, ticari bir yazılım olan *Nuix*® yazılımını kullanmaktadır. Fransız rekabet otoritesi ise benzer nitelikteki *Encase*® yazılımını kullanmaktadır (Doury 2013, 216).

1.4.4.1. Kurum Uygulaması Açısından Adli Bilişim Araçları Kullanılması Gerekliliği

Kurum'un mevcut elektronik delil araması bilişim sistemleri üzerinde bulunan dâhili arama araçları ile gerçekleştirilmekte, adli bilişim uygulamalarına başvurulmamaktadır. Görece sığ olarak nitelendirilebilecek bu arama faaliyetine karşı; teşebbüsler eğer daha önce yerinde incelemeye muhatap olmuşsa bizzat tecrübe ederek, muhatap olmamışsa da Kurum'un yerinde inceleme usul ve yöntemleri hakkında bilgi sahibi olan avukatlarca[23] gerçekleştirilen kurgusal yerinde incelemeler sayesinde aşinalık kazanabilmektedir. Dolayısıyla; teşebbüslerce Kurum'un geleneksel yöntemlerle delil bulma imkânını ortadan kaldıracak önlemler kolaylıkla alınabilmektedir.

Veri kurtarma işlemi mevcut uygulama açısından bir eksiklik, adli bilişim araçlarının kullanılması açısından ise önemli bir gereklilik olarak ortaya çıkmaktadır. Elektronik verilerin korunmasına yönelik önlemler alınmadığı takdirde teşebbüse intikal edilen zaman ile incelemeye başlanan zaman arasında geçen sürede veya inceleme esnasında[24] dahi elektronik veriler kolayca silinebilir. Ayrıca, delilleri ortadan kaldırma güdüsüyle hareket edilmemiş olsa dahi normal iş akışı içinde iradi ya da gayri iradi olarak delil değeri taşıyan elektronik verilerin silinmiş olması mümkündür.

Bu açıdan daha etkin bir arama gerçekleştirmek için adli bilişim araçlarının kullanılması gerekliliği ortaya çıkmaktadır. Zira dâhili arama araçları sadece aktif alanlarda ve sınırlı olarak arama gerçekleştirme kapasitesine sahiptir. Örneğin; en yaygın kullanılan adli bilişim yazılımlarından *EnCase*®'i ele alırsak, dâhili arama araçlarına göre çok daha yüksek arama kapasitesi sunan *EnCase*® sabit disk üzerinde *"bit"* düzeyinde, aktif, tahsis edilmemiş ve artık alanlarda silinmiş ya da gizlenmiş verileri de kapsayacak şekilde arama gerçekleştirebilmektedir (Stanley

[23] Örnek olarak bkz. Cartonboard, [1994] OJ L243/1.

[24] 18.07.2013 tarih, 13-46/601-M sayılı Kurul kararında, *(TTNET)* yerinde inceleme sırasında, incelenmekte olan bir bilgisayara uzaktan erişim sağlanarak bazı dosyaların silinmesi üzerine 4054 sayılı Kanun'un 16. maddesinin ilk fıkrasının (d) bendi uyarınca idari para cezası uygulanmasına karar verilmiştir.

2008, 192). Bu nedenle, adli bilişim araçlarının kullanılması silinmiş veriler üzerinde de elektronik delil araması yapabilme imkânı sunacaktır.

Adli bilişim araçlarının sunacak olduğu bir diğer gelişmiş özellik ise kavramsal arama yapılabilmesidir. Mevcut uygulamada dâhili arama araçları kullanılarak gerçekleştirilen basit aramada *(keyword searching)* sisteme girilen arama ibaresi tüm belgelerde aranarak, arama ibaresini içeren belgeler arama sonucunda gösterilir. Arama sonucu, sadece ve sadece arama ibarelerinin yer aldığı belgeler ile sınırlıdır. Bu yüzden, belirlenen arama ibarelerini içermeyen benzer nitelikteki, aynı konunun farklı bir anlatımla ele alındığı belgeler arama sonucunda gösterilmez. Dolayısıyla, basit arama ile etkin bir arama yapılabilmesi için tüm potansiyel arama ibarelerinin belirlenebilmesi gerekir. Teknik olarak ise bunun gerçekleştirilmesi pek mümkün değildir (Beebe ve Clark 2007, 49).

Fakat, kavramsal arama tüm potansiyel arama ibarelerinin belirlenmesini gerektirmez zira kavramsal arama, arama sonucu bulunan belgeleri konsept benzerliğine göre kategorize edecek şekilde dizayn edilmiştir. Buna göre kavramsal aramayla eş anlamlı ifadeler, şifreli yazışmalar hatta yazışmaya yansıyan duygular (korkulu, heyecanlı vs.) dahi saptanabilmektedir (Beebe ve Clark 2007, 51). Dolayısıyla, kavramsal arama gibi oldukça gelişmiş arama kabiliyetlerini barındıran adli bilişim yazılımlarının kullanılması bu açıdan da mevcut uygulamanın etkinliğini arttıracak niteliktedir.

Öte yandan, bilişim sistemleri üzerinde delil niteliği taşıyabilecek elektronik veriler, basit bilgisayar taramasıyla erişilemeyecek şekilde kolaylıkla[25] gizlenilebilir. Verilerin kriptolanması, stenografi[26] uygulanması, dosya uzantısının değiştirilmesi, watermarking[27] bu amaçla kullanılabilecek yöntemlerden bazılarıdır. Sabit disk üzerindeki gizlenmiş halde bulunan bu tür verilerin saptanabilmesi ve şifre engelinin aşılarak erişilebilmesi adli bilişim yazılımlarının kullanılmasını

[25] Kavramı somutlaştırmak adına; gizlenmek istenilen dosyaların yer aldığı ":D" diskini *"hidden partition"* yöntemiyle gizlenmesi uygulaması ele alınabilir: *"Run"pencesini* aç®*"cmd" komutunu gir®açılan pencereye "cd \"komutunu gir enter tuşla® "diskpart" komutu ve enter®"list volume" ve enter®:D diskine karşılık gelen volume'yi seç "select volume X" komutunu gir ve enter® "remove letter D" ve enter.* Bu şekilde birkaç dakika içinde kolaylıkla elektronik veriler ancak adli bilişim araçları ile tespit edilebilecek şekilde gizlenebilir (Maras 2012, 186).

[26] Stenografi, bir dosyanın aynı ya da farklı formatta başka bir dosyanın içine gizlenmesidir. Örneğin, bir "MS Word" dosyasının video ya da resim formatındaki bir dosyanın içine gizlenmesi uygulaması stenografiye örnek verilebilir.

[27] Watermarking, orijinal mesajın, dosya üzerinde fark edilmesi güç bir şekilde yerleştirilmesidir (Henkoğlu 2011, 86).

gerektirmektedir (Henkoğlu 2011, 84). Gizlenmiş veriler Kurum'un elektronik delillerin elde edilmesi sürecinin bir parçası olarak adli bilişim araçlarını işlevsel kılmasının bir başka gerekçesini oluşturmaktadır.

Adli bilişim araçları kullanımının sağlayacak olduğu teknik faydaların yanı sıra bir takım pratik faydalardan da söz edilebilir. Kurum'un uygulaması açısından, yerinde incelemelerde teşebbüse ait fakat kişilerin kullanımına tahsis edilmiş, sistem yöneticisinin de erişimi olmayan bilgisayarlarla karşılaşılmakta, ancak kullanıcılara ulaşılarak şifrelerin temin edilmesiyle inceleme gerçekleştirilmesi mümkün olmaktadır. Kişilere ulaşılamadığı ya da geç ulaşılabildiği de olabilmektedir. Adli bilişim araçları ile çoğunlukla[28] işletim sistemine, dolayısıyla şifreye gerek duyulmadan incelemenin gerçekleştirilebilmesi bu tür gecikmelerin önüne geçilmesi açısından fayda sağlayabilecektir.

[28] Microsoft İşletim sistemine sahip bilgisayarlar açısından imaj almak için şifre engeli bulunmamaktadır. Fakat açık kaynak kodlu Linux işletim sistemi için imaj alma işleminden önce şifre alınması gerekmektedir. (Özbek 2008, 8)

BÖLÜM 2

ÖRNEK ÜLKE UYGULAMALARI VE GENEL OLARAK ELEKTRONİK DELİLLERİN ELDE EDİLMESİ SÜRECİNDE TEMEL HAK VE ÖZGÜRLÜKLER BAĞLAMINDA ORTAYA ÇIKAN PROBLEMLER

2.1. ÖRNEK ÜLKE UYGULAMALARI

Ülke uygulamaları kapsamında, Komisyon, Birleşik Devletler ve Almanya uygulamaları incelenmiştir. Söz konusu üç rekabet hukuku rejimi belirlenirken Komisyon'un rekabet ihlallerinin idari rejimde ele alındığı rekabet hukuku uygulamaları bakımından, Birleşik Devletler'in ise rekabet ihlallerinin kriminal rejimde ele alındığı ülke uygulamaları bakımından öncü olması, Almanya'nın ise rekabet ihlalleri ile mücadelede adli bilişim uygulamalarının etkin kullanımına örnek teşkil etmesi göz önüne alınmıştır. Adli bilişim araçlarının kullanıldığı ülke uygulamaları bakımından hangi prosedürlerin takip edildiği, hangi adli bilişim araçlarının kullandığının irdelenmesi ilave bir fayda sağlamayacaktır. Zira adli bilişim uygulamaları genel kabul görmüş standartlar çerçevesinde şekillenmekte ve birbirinden önemli ölçüde farklılaşmamaktadır. Bu yüzden, örnek ülke uygulamalarının ele alındığı bu kısım, üç ülke uygulaması ile sınırlandırılmıştır.

2.1.1. Avrupa Birliği Komisyonu Uygulaması

Komisyon'un teşebbüslerin bilgi işlem alt yapısı üzerinde inceleme yapma yetkisi[29] ve incelemelerde elde ettiği elektronik delilerin elektronik ya da basılı

[29] Komisyon tarafından gerçekleştirilen yerinde incelemeler 1/2003 sayılı tüzüğün 20/3. maddesinde düzenlenen "inceleme talebi" ya da 20/4. maddesinde düzenlenen "inceleme kararı" kapsamında gerçekleştirilmektedir. İnceleme talebi için Komisyon'un başındaki yetkilinin imzası yeterli olurken, İnceleme kararı Avrupa Birliği Komisyon'u tarafından alınmaktadır. Uygulamada bu yetki rekabetten sorumlu komisere devredilmekte ve doğrudan bu Komiserin imzası ile alınmaktadır. İnceleme talebine karşı teşebbüsün karşı koyma hakkı vardır ve sonucunda herhangi bir yaptırım uygulanmaz. Teşebbüs inceleme talebini bir kez kabul ettikten sonra incelemeye tam olarak katlanma ve işbirliği yükümlülüğü altına girmektedir ve vazgeçme hakkı bulunmamaktadır. Ancak inceleme talebi ile teşebbüste bulunan Komisyon yetkilileri, bizzat arama yapamaz, sadece teşebbüsten bilgi ve belge talebinde bulunabilir. Bu

haldeki kopyasını alma yetkisi 1/2003 Sayılı Tüzük'ün 20. Maddesinin 2. fıkrası ile belirlenmiştir. 1/2003 Sayılı Tüzüğün 20/2. maddesinin (b) bendinde teşebbüsün defterlerini ve hangi ortamda kayıtlı olduğundan bağımsız olarak iş ile ilgili her türlü kayıtlarını inceleyebileceği, (c) bendinde ise incelediği dokümanların, belgelerin her hangi bir formatta kopyasını alabileceği belirtilmektedir.

"1/2003 Sayılı Tüzüğün 20. Maddesinin 4. Fıkrası Kapsamında Gerçekleştirilen Yerinde İncelemelere İlişkin Bilgi Notu[30]*"*nda (Bilgi Notu) ise Komisyon'un elektronik delil elde etme süreçleri hakkında olabildiğince detaylı açıklamalara yer verilmektedir. Bilgi Notu Komisyon'un yerinde inceleme yetkisinin hukuki dayanağı hakkında tarafsız, açıklayıcı bilgiler ve Komisyon'un incelemeyi nasıl gerçekleştirileceği ile ilgili açıklamalar içermektedir. Komisyon tarafından yerinde inceleme sürecinin başlangıcında Bilgi Notu, Komisyon'un inceleme yapılmasına ilişkin karar metni ile birlikte teşebbüs temsilcisine sunulmaktadır.

Bilgi Notu 18 Mart 20013 tarihinde güncellenerek diğer bazı konularla birlikte, yerinde incelemelerdeki adli bilişim prosedürüne ilişkin ilave bilgiler eklenmiştir. *Nuix*® yazılımının kullanılmaya başlanılmasıyla aynı döneme rastlayan bu revizyon ile Komisyon'un *Nuix*® üzerine kurulu yeni uygulaması hakkında, şeffaflık ilkesi doğrultusunda rekabet çevrelerinin bilgilendirilmesinin amaçlandığını ifade etmek mümkündür.

Komisyon bünyesinde, elektronik delil toplanması süreçleri 2006 yılından bu yana kartel birimine bağlı olarak faaliyet gösteren, adli bilişim grubu tarafından yönetilmektedir. 250'den fazla incelemede görev alan adli bilişim grubu tam zamanlı çalışan beş adli bilişim uzmanı ve yerinde incelemeler sırasında adli bilişim araçlarını kullanma konusunda eğitim almış 50 civarında Komisyon yetkilisinden oluşmaktadır. Komisyon'un büyük hacimli elektronik veri setlerini etkin şekilde incelemesine imkân tanıyan adli bilişim araçları 2006 yılından bu yana 50 civarında yerinde incelemede kullanılmıştır (Erps 2013, 213).

Komisyon yetkilileri, standart elektronik delil arama prosedürüne yerinde incelemenin konusuyla ilgili elektronik delil ihtiva edebilecek dizüstü ve masaüstü bilgisayarlar, cep telefonları, tablet bilgisayarlar, taşınabilir bellekler gibi cihazların tespit edilmesiyle başlamaktadır. Üzerinde arama yapılacak elektronik cihazlara yetkililer tarafından yerinde inceleme bitimine kadar el konulabilmektedir.

açıdan elektronik delil aramaları Komisyon'un inceleme kararı kapsamında yapılabildiği için konumuz itibariyle Komisyon'un İnceleme kararı kapsamındaki yerinde inceleme yetkileri ele alınmaktadır. Ayrıntılı bilgi için bkz. (Pınar 2011, 143).

[30] http://ec.europa.eu/competition/antitrust/legislation/explanatory_note.pdf.

Komisyon üzerinde delil incelemesi yaptığı cihazlardan ilgili verilerin dijital kopyasını ya da geçici suretle adli kopyasını[31] almaktadır[32].

Bilgi Notu'nun 10. Paragrafında Komisyon yetkililerin teşebbüsün bilgi işlem alt yapısı üzerinde ve dijital veri saklama ortamlarında (masaüstü, dizüstü ve tablet bilgisayarlar, cep telefonları, CD, DVD, USB Bellek vb.) arama yapabileceği, arama yaparken dahili arama araçlarını ya da kendilerinin belirleyeceği adli bilişim yazılım ve/veya donanımlarını kullanabilecekleri belirtilmektedir (Piazza 2013, 421). Komisyon'un Genel çerçevesine Bilgi Notu'nun 10. paragrafında yer verilen, adli bilişim aracı merkezli elektronik delil aramasına ilişkin uygulaması Şekil-2'de resmedilmektedir.

Uygulama, incelenecek bilişim sistemlerinin adli kopyalarının alınması ile başlamaktadır. Ardından bu kopyalar, özünde üzerinde değişik işlevleri yerine getiren adli bilişim yazılımları yüklü bulunan yüksek işlem kapasiteli bir dizüstü bilgisayar olan taşınabilir sunucuya aktarılmaktadır[33]. Sunucuya aktarılan elektronik veriler adli bilişim yazılımları aracılığıyla işlenmekte, bunun ardından sunucuya

[31] Adli Kopya (forensic image) : Elektronik verilerin yer aldığı disklerin, artık alan (slack space) ve tahsis edilmemiş (unallocated space) alanları da kapsayacak şekilde birebir kopyasının alınmasıdır.

[32] Bilgi Notu para. 12

[33] Komisyon Dünya'da kendisi dışında 34 organizasyonun daha kullandığı *Nuix*®yazılım platformunu kullanmaktadır. *Nuix*® diğer adli bilişim yazılımlarından çok büyük miktarda veri setini çok kısa sürede proses edebilmesi ile ayrışmaktadır. Kaynak: http://www.forensicfocus.com/c/aid=53/interviews/2012/eddie-sheehy-ceo-nuix/ Erişim: Ocak 2014

bağlanılarak işlenmiş veri seti üzerinden inceleme gerçekleştirilmektedir. Bu suretle büyük miktardaki verinin daha hızlı ve daha ayrıntılı bir şekilde incelenmesi sağlanmaktadır.

İncelenen veri seti içinde delil niteliği taşıyan veriler, bu verilerin dosya adı, yolu, link köprüsü (hyperlink) ve özet değerini içeren bir liste ile şifreli bir veri taşıyıcısına kaydedilmektedir. Daha sonra taraflarca imzalanan tutanağın bir sureti ve alınan elektronik veri setinin bir kopyası teşebbüse bırakılmaktadır. Elektronik formattaki verileri, elektronik ortamda muhafaza etme yoluna giden Komisyon'un bu uygulamasını, yazılı dokümanları da kapsayacak şekilde genişlettiği görülmektedir (Erps 2013, 214).

Teşebbüslerin yerinde incelemelerde elektronik delillerin elde edilmesi süreci bakımından göstermeleri gereken işbirliğinin[34], çerçevesi Bilgi Notu'nun 11. paragrafında belirlenmektedir. Teşebbüsün, Komisyon yetkililerine bilişim alt yapısı hakkında bilgi vermesiyle başlayan teşebbüsün aktif ve tam destek verme yükümlülüğünün, elektronik delilin güvenliğinin sağlanması amacına yönelik olarak e-posta hesaplarının geçici olarak bloke edilmesi, bilgisayarların ağ bağlantısının kesilmesi gibi görevlerin Komisyon yetkililerinin talebi üzerine yerine getirilmesini de kapsadığı görülmektedir. Ayrıca, teşebbüsün bu süreçler devam ederken inceleme sürecinin salahiyetini tehlikeye atacak herhangi bir müdahalede bulunmaması ve çalışanlarını da bu doğrultuda uyarmasının teşebbüsün sorumluluğunda olduğu açıkça belirtilen hususlardandır.

İlk yayımlandığında bir sayfa uzunluğunda dahi olmayan Bilgi Notu'nun bugün üç sayfayı bulmasında, Komisyon'un uygulamada karşılaşılan sorunlar ışığında Bilgi Notu'na yeni eklemeler yapması etkili olmuştur (Piazza 2013, 422). Bu kapsamda, teşebbüslerin bilişim alt yapısı üzerinde gerçekleştirilen elektronik delil aramalarındaki iş birliği yükümlülüklerine ilişkin düzenlemeleri Komisyon'un EPH[35] kararı ile ilişkilendirmek mümkündür. EPH gruba e-posta hesaplarının yetkililer tarafından bloke edilmesi talep edildiği halde bloke etmediği[36] ve inceleme sırasında gelen mailleri başka hesaplara yönlendirdiği için idari para cezası uygulanmıştır.

[34] ABAD'ın teşebbüslerin yerinde inceleme sırasında aktif işbirliği yapmakla yükümlü olduklarına ilişkin kararı: Bkz. Case 374/87, *Orkem v. Commission*, [1989] ECR 3283, 18.5.1989, para. 22, 27.

[35] CASE COMP/39793-*EPH and others*, 28.03.2012.

[36] Ibid para. 22.

Benzer şekilde, Bilgi Notu'nda yerinde incelemenin sağlıklı bir şekilde yürütülebilmesi için, süreç hakkında çalışanların bilgilendirilmesi sorumluluğunun teşebbüsün kendisine ait olduğuna açıkça yer verilmesini de yakın geçmişte *E.ON Energy AG* ve *Suez Environment* unvanlı teşebbüsler hakkında alınan kararlarla[37] ilişkilendirebiliriz. Komisyon yetkililerinin yerinde incelemenin bir sonraki güne sarkması üzerine incelenen dokümanları bir odaya koymak ve mühürlemek suretiyle muhafaza altına aldıkları her iki olayda da mühürler teşebbüs çalışanları tarafından kırılmıştır. Komisyon'un *E.ON Energy AG* hakkındaki kararı[38] Avrupa Birliği Adalet Divanı (ABAD) tarafından da onanmıştır[39]. *Suez Environment* kararı ise temyiz edilmemiştir.

Bilgi Notu'nun 13. paragrafında yerinde incelemenin sonunda Komisyon'un inceleme sırasında kullandığı, içinde teşebbüse ait dijital verilerin kopyalanmasında kullandıkları ekipmanları teşebbüsü terk etmeden önce, bu ekipmanlara kaydedilmiş verilerin herhangi bir bilinen teknikle geri getirilemeyecek şekilde temizleneceğinin izahı yapılmaktadır. Komisyon'un bu uygulama ile teşebbüse ait verilerin bilgisi dışında alınmasının önüne geçilmesini hedeflediğini ifade etmek mümkündür.

Teşebbüslerin faaliyetleri çok büyük oranda bilişim alt yapısı üzerinden yürütüldüğü için, rekabet otoriteleri, özellikle de el koyma ya da adli kopya alma yetkisi bulunmayan rekabet otoriteleri, yerinde incelemelerde çok büyük hacimli veri setlerini incelemek, inceleme konusu kapsamındaki elektronik verileri ayrıştırmak zorunda kalmaktadır. Verilerin ayrıştırılması dolayısıyla teşebbüste normalden daha uzun süre kalınması, gerek incelemeyi yürüten yetkililerin etkinliği, gerekse yetkililerin teşebbüste kaldıkları sürenin artmasının teşebbüsün işleyişi üzerinde neden olabileceği aksaklıklar nedeniyle çok arzu edilen bir durum değildir.

Bilgi Notu'nun 14. paragrafında bu hususa ilişkin olarak; incelenen elektronik veri setinin ayrıştırılması işleminin bitirilemediği durumlarda[40] incelenmesine devam edilecek elektronik verilerin, bir kopyası teşebbüse bırakılmak suretiyle, bir zarfa konularak mühürleneceği ve daha sonraki bir tarihte incelenmek üzere Komisyon'un merkezine götürüleceği belirtilmektedir. Ayrıca, istenildiği takdirde

[37] Case COMP/39.796-*Suez Environnement*, 24.05.2011.

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

[39] Case 89/11 P, *E.ON Energie v. Commission*, [2012] 22.11.2012

[40] Bu durumlara örnek olarak yetkililerin inceleme yapmak istedikleri bir cihazı incelemenin sonuna doğru geç saatte belirlemeleri, teknik problemler yaşanması ya da incelemenin teşebbüsün faaliyetlerini sekteye uğratması gösterilebilir.

teşebbüs vekilinin de bu inceleme sürecine iştirak edebileceği ifade edilmektedir.

Özellikle üzerinde durulması gereken hususlarda biri de, Komisyon'un teşebbüs çalışanlarına ait Yahoo, Gmail gibi kişisel e-posta hesapları ile mobil iletişim araçlarına ilişkin nasıl bir yaklaşım geliştirdiğidir. Komisyon'un kişisel e-posta hesaplarına ilişkin uygulaması erişim yaklaşımı[41] doğrultusunda daha önce teşebbüsten erişildiği tespit edilebilen her türlü kullanıcı hesabına, internet üzerinden erişilebilen her türlü bulut bilişim uygulamaları da dahil olmak üzere, erişilmesi şeklindedir.

Komisyon kullanmış olduğu adli bilişim araçları yardımıyla ağ tabanlı e-posta yazışmalarını tespit edebilmekte, yazışmaların bir kısmına da ulaşabilmektedir. Bu doğrultuda, erişim sağlandığı tespit edilen kişisel e-posta hesaplarının kullanıcısından hesabını açması talep edilerek yetkililer tarafından inceleme gerçekleştirilmektedir. Kullanıcının bu talebi karşılıksız bırakması, yerinde incelemenin engellenmesi kapsamında değerlendirilebilmektedir.

Mobil telefonlara ilişkin Komisyon uygulaması teşebbüste elektronik delil ihtiva edebileceği öngörülen tüm cep telefonlarının incelenebilmesi şeklindedir. Komisyon uygulamasında, mülkiyet bir kıstas olarak dikkate alınmamaktadır. Bu doğrultuda mobil cihazlar üzerinde adli bilişim uygulaması için *Oxygen Forensic®* yazılımı kullanılmaktadır. Elde edilen veriler eğer gerekli görülürse *Nuix®*'e aktarılabilmektedir[42].

2.1.2. Amerika Birleşik Devletleri Uygulaması

Amerika Birleşik Devletleri'nde (ABD) federal rekabet hukuku kanunları ABD Adalet Bakanlığı Antitröst Birimi (DOJ) ve Federal Ticaret Komisyon'u (FTC) tarafından uygulanmaktadır. Ceza hukuku rejimi kapsamında ele alınan rekabet ihlallerini[43] *(Criminal cases)* soruşturmak münhasıran DOJ'un yetki

[41] Rekabet otoritelerinin teşebbüslerin bilişim altyapısı üzerinde gerçekleştirdikleri elektronik delil aramalarında, teşebbüse ait elektronik kayıtları inceleyip incelememe kararlarını verirken iki yaklaşıma göre hareket ettikleri görülmektedir. Bunlardan, ilki elektronik verilerin yer aldıkları sunucuların konumunun belirleyici olduğu, **yerleşim yaklaşımıdır**. İkincisi ise, teşebbüsten olağan iş akışı içinde erişilebilen her türlü veriye erişim sağlanabileceği noktasından hareket edilen **erişim yaklaşımıdır**.

[42] Komisyon'un yerinde incelemelerde mobil iletişim cihazları ve kişisel e-posta hesaplarına ilişkin uygulamasına ilişkin bilgiler Komisyon'un Adli bilişim projesi yöneticisi ve 2 numaralı kartel dairesi başkanı Dirk VAN ERPS ile iletişime geçilerek elde edilmiştir.

[43] "Ceza hukuku rejimi kapsamındaki rekabet ihlallerine yönelik yürütülen soruşturmalar" kast edilmektedir.

alanındayken, bu kapsamda olmayan ihlaller[44] *(Civil Cases)* ve birleşme-devralma işlemleri sektörel bazlı olarak DOJ ve FTC arasında paylaşılmaktadır.

Amerikan federal rekabet otoriteleri DOJ ve FTC tarafından, iki temel yetki çerçevesinde elektronik delil elde edilmektedir. Bunlar; DOJ ve FTC'nin hukuk soruşturmaları kapsamında başvurduğu bilgi ve belge isteme yetkisi ile DOJ[45] tarafından ceza soruşturmaları kapsamında Federal Ceza Usul Kanunu'nun[46] 41. maddesi uyarınca düzenlenen adli aramalardır. DOJ ve FTC'nin elektronik delil elde etme uygulamaları önce bilgi ve belge isteme yetkisi, ardından DOJ tarafından gerçekleştirilen adli aramalar kapsamında ele alınacaktır.

DOJ ceza soruşturmalarında, iddianamenin hazırlanmasından önce, kovuşturmaya yer olup olmadığına karar vermek için bir araya gelen tahkikat jürisinin celp kararı ile (tahkikat jürisi celbi "Grand Jury Subpoena") teşebbüsün talep edilen her türlü bilgi ve belgeyi üretmesini ve/veya tahkikat jürisi önünde ifade vermesini sağlayabilmektedir (Everett vd. 2012, 21). Benzer şekilde FTC de celp kararı ile teşebbüsü her türlü bilgi ve belgeyi sağlamaya ve/veya ifade vermeye zorlayabilmektedir[47].

Aynı zamanda gerek DOJ, gerekse de FTC tarafından Adli Soruşturma Talebi[48] (AST) yetkisi çerçevesinde teşebbüsleri talep edilen belgeleri üretmeye, ifade vermeye, inceleme konusu ile ilgili maddi eşyaları sağlamaya, yöneltilen soruları cevaplamaya zorlamaya yetkilidir[49] (Muyskens ve Fischer 2009, 1). DOJ ve FTC'nin celp kararları ve AST'ler kapsamında[50] elektronik delil elde etme sürecinin konumuz bakımından önem arz eden yönü; teşebbüslerin rekabet otoritesinin belirlediği kriterler doğrultusunda kendi bilişim sistemleri üzerinde

[44] Ceza Hukuku rejimi dışında ele alınan rekabet ihlalleri için "Civil Cases", türkçe karşılığı "Hukuk Davası" kavramı kullanılmaktadır. Fakat, türk hukuk literatüründe kullanılan hukuk davası terimi ile tam olarak uygun düşmediğini belirtmek gerekir.

[45] DOJ ceza soruşturmalarında arama emri ve tahkikat jürisi celbi'nin yanı sıra USA Patriot Improvement and Reauthorization Act of 2005 (Patriot Act) uyarınca iletişimin tespiti, dinlenmesi ve kayda alınması yoluyla da elektronik delil elde etme yetkisine sahiptir (Everett vd. 2012).

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

[47] 15 U.S.C. § 49 (FTC).

[48] Talep edilen bilgi veya belgenin ifşası için Tahkikat jürisi soruşturmasındaki (Grand Jury Investigation) celp ve Federal Usul Kuralları'ndaki "discovery" talebinin standardı ile korunuyorsa AST'ler aracılığıyla talep edilemeyecektir (Coşgun 2009, 6).

[49] 15 U.S.C. § 57b-1 (FTC); 15 U.S.C. §§ 1311-1314 (DOJ).

[50] FTC ve DOJ, celp ve AST'ler ayrı olarak karşı tarafın gereğine yerine getirmekle yükümlü olmadığı "Voluntary Regquest For Information" bilgi ve belge isteme yetkisini de kullanabilmektedir. Ayrıntılı bilgi için bkz. (Sims vd. 2014, 100).

oldukça kapsamlı olarak gerçekleştirdiği elektronik veri[51] üretme ve derleme faaliyetidir. Bu faaliyeti verilerin saklanması, üretilmesi ve değerlendirilmesi şeklinde üç aşamalı bir süreçte açıklamak mümkündür.

Birleşik Devletler uygulamasında teşebbüsler yasal soruşturma ihtimali ile karşı karşıya oldukları durumlarda; olağan veri saklama politikasını askıya alarak, inceleme konusuyla ilgisi kurulabilecek *"potentially relevant"* verilerin korunmasına ilişkin her türlü önlemi almak zorundadır[52] (Sims vd. 2014, 164). Bu zorunluluk hali, bilgi ve belge isteme yetkisinin Birleşik Devletler uygulamasındaki etkin kullanımına zemin hazırlayan unsurların başında gelmektedir. Zira delil niteliği taşıyabilecek elektronik verilerin yok edilmesi, değiştirilmesi ve gizlenmesi bu suretle önlenebilmektedir.

Verilerin korunmasına ilişkin teknik ve idari önlemlerin[53] alınmasının ardından ise elektronik verilerin üretilmesi ve derlenmesi süreci başlamaktadır. DOJ'un bazı soruşturmalarda bilgi talebi çerçevesinde yaklaşık bir milyon elektronik kayıt üretildiği bilgisi, sürecin ne denli geniş kapsamlı olduğu açısından anlamlıdır (Greer 2012, 1). Bu nedenle bilgi ve belgelerin üretilmesi sürecinde teşebbüslerin kendi bilgi işlem departmanları yetersiz kaldığı için genellikle, elektronik keşif konusunda uzmanlaşmış firmalardan hizmet alımı yoluna gidilmektedir. Şayet, bu bilgi ve belgelerin belirlenen spesifikasyonlarda (veri bütünlüğünün sağlanması, üst verilerin korunması, talep edilen formatta sunulması vs.) olmaması teşebbüsün aleyhine olarak sürecin uzamasına ve cezai yaptırım tehdidiyle karşı karşıya kalınmasına yol açabilecektir (Sims vd. 2014, 172).

Birleşik Devletler uygulamasının dikkat çeken tarafı, bizzat teşebbüsün rekabet otoritesi tarafından belirlenen kriterler çerçevesinde inceleme konusu ile ilgisi kurulabilecek belgeleri derleyerek otoriteye sağlıyor olmasıdır. Bu kapsamda; rekabet otoritesinin doğrudan bazı belgeleri talep etmek yerine, teşebbüsü inceleme

[51] Celp kararı ve AST'ler kapsamında elde edilen bilgi ve belgelerin %90'ından fazlasını elektronik kayıtlar oluşturmaktadır (Sims vd. 2014, 174).

[52] Amerika Birleşik Devletleri'nde teşebbüslere veri saklama ve veri koruma yükümlüğü getiren Sarbanes-Oxley Act'in (Sox) her ne kadar halka açık şirketler hedeflenerek çıkarılmış olsa da bazı hükümleri herkese uygulanabilir niteliktedir. Buna göre yasal bir soruşturma açısından delil niteliği taşıyabilecek her türlü bilgi ve belgenin değiştirilmesi, yok edilmesi, gizlenmesi suç sayılarak, 25 milyon dolar ve/veya 20 yıl hapis cezasına kadar yaptırım uygulanması öngörülmüştür (Sims vd. 2014, 669).

[53] Çalışanlara yasal soruşturma kapsamında veri saklama yükümlülüklerinin bulunduğunun duyurulması *"Legal Hold Notice*", aleyhlerine olan belgeleri yok etme riski bulunmayan çalışanlar ile soruşturma konusu belgelerin hazırlanmasına ilişkin görüşme gerçekleştirilmesi… Ayrıntılı bilgi için: Bkz. (Sims vd. 2014, 172).

konusuyla ilgisi kurulabilecek belgelere yönlendirecek kriterleri belirlediği görülmektedir. Örneğin, otorite tarafından arama ibareleri belirlenmekte ve teşebbüs bu çerçevede bilişim altyapısı üzerinde elektronik delil araması gerçekleştirerek, elde ettiği bulguları resmi bilgi talebinin gereği olarak otoriteye teslim etmektedir (Greer 2009, 6).

Literatürde resmi bilgi talebinin Komisyon'da uygulandığı şekli için *" Request For Information"* bilgi talebi kavramı kullanılırken, Birleşik Devletler uygulaması için mecburi keşif *"Compelled Discovery"* nitelemesi kullanılması esasında uygulamadaki farkı yansıtması bakımından önemlidir. Zira delil niteliği taşıyabilecek belgeler, rekabet otoritesi tarafından belirlenen kıstaslar ve yöneltilen sorular çerçevesinde bizzat teşebbüs tarafından elde edilmektedir.

Bilgi ve belge isteme yetkisinin Birleşik Devletler uygulamasında karşılık bulan halinde Komisyon uygulamasından farklı olarak, inceleme konusu ile ilgisi kurulabilecek bilgi ve belgelerin kapsamı çok daha geniş olarak belirlenmektedir. Dolayısıyla, Birleşik devletler uygulamasında çok daha büyük miktarda verinin değerlendirilmesi gerekliliği doğmaktadır (Sims vd. 2014, 180). Büyük miktarda elektronik verinin analiz edilmesi sorunu ise adli bilişim araçları ve öngörücü kodlama[54] *"Predictive Coding"* gibi ileri arama teknikleri kullanılarak aşılmaya çalışılmaktadır.

Birleşik Devletler uygulamasında belge ve bilgi isteme yetkisinin yanı sıra, DOJ tarafından gerçekleştirilen adli aramalar kapsamında da elektronik delil elde edilebilmektedir. Federal Soruşturma Bürosu (FBI) ajanları ile işbirliği içinde gerçekleştirilen adli aramalarda arama, kopyalama ve el koyma tedbirlerine başvurulabilmektedir (Everett vd. 2012, 23). DOJ tarafından yayımlanan ceza soruşturmaları kapsamında bilgisayarlar üzerinde arama ve el koyma tedbirlerinin uygulamasına ilişkin kılavuzdan[55] DOJ'un genel uygulamasının[56] elektronik delil araması yapılacak cihazlara el koyulması şeklinde olduğu ve el koyulan cihazların adli bilişim laboratuvarlarında standart adli bilişim süreçlerine tabi tutulduğu

[54] Predictive coding: rastgele istatiksel olarak anlamlı bir belge seti seçilerek, seçilen belge seti inceleme konusuyla ilgili olup olmamasına göre yazılıma kodlanır. Daha sonra veri madenciliği, kavramsal arama, oyun teorisini kullanarak geçmişte gerçekleşen olaylardan hareketle geleceğe dönük tahminde bulunma gibi kabiliyetlerle donatılmış özel yazılımlar aracılığıyla veri seti inceleme konusu ile ilgili olup olmamasına göre ayrıştırılır. Kaynak: http://www.insidecounsel.com/2013/08/13/e-discovery-the-value-of-predictive-coding-in-inte?t=e-discovery erişim tarihi: 06.03.2014.

[55] "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" Kaynak: http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

[56] Ibid.: s. 86.

anlaşılmaktadır. DOJ'un bu kapsamdaki elektronik delil elde etme faaliyeti, Komisyon uygulamasında olduğu gibi, standart uygulamanın dışına çıkmadığı için daha detaylı ele alınmasına gerek görülmemiştir.

DOJ tarafından gerçekleştirilen adli aramalar kapsamında elektronik delillerin elde edilmesine ilişkin dikkat çeken hususlardan biri de erişim yaklaşımının benimsenmiş olmasıdır. El koyma ya da imaj alma işleminin gerçekleştirilemediği durumlar açısından elektronik verilerin arama kararında belirtilen yerden farklı bir konumda yer alan bir sunucuyla ilişkilendirilmiş olmaları önemli bir sorun teşkil etmektedir[57]. Zira Birleşik devletler uygulamasında arama emrinde, aranacak unsurlar ve kişiler ile birlikte aramanın yapılacağı yerin de açıkça belirtilmesi gerekmektedir[58]. Delil araması gerçekleştirilecek ortamlar arama emrinde açıkça belirtilen yerler ile sınırlıdır [59]. Eğer elektronik veriler başka bir yerdeki sunucuda bulunuyorsa; bu sunucular üzerindeki verilerin incelenmesi, sunucuların yer aldığı yeri kapsayacak ilave bir arama emrinin alınması gerektirmektedir[60].

2.1.3. Almanya Uygulaması

Alman rekabet otoritesi (Bundeskartellamt-BKartA) tarafından, susma hakkının Alman hukukundaki yorumu, şüpheli teşebbüslerden bilgi ve belge talebinde bulunulmasına el vermediği için sadece yerinde incelemeler aracılığıyla elektronik delil elde edilebilmektedir. BKartA'nın el koyma ve imaj almayı kapsayan geniş yerinde inceleme yetkileri bulunmaktadır[61]. Alınan elektronik veri setini, komisyon'un aksine, teşebbüste ayrıştırma zorunluluğu bulunmayan BKartA, teşebbüslere ait sabit disklerin adli kopyalarını ve/veya e-posta kutularının basit kopyalarını kendi merkezinde inceleyebilmektedir. BKartA'nın düzenlediği yerinde incelemelerde elektronik delil araması, BKartA bünyesinde çalışan tam zamanlı adli bilişim uzmanları ve adli bilişim uzmanı polisler tarafından gerçekleştirilmektedir (Saller 2013, 84).

---

[57] Ibid: s.64 para.2.

[58] Ibid: s.69 *"The Particularity Requirement"*.

[59] Eğer üçüncü taraf internet servis sağlayıcısı (ISS) ise, devletin bilgi talebinin nasıl karşılanacağı the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2701-2712 ile düzenlenmiştir. Yasal bir inceleme kapsamında e-postalar, e-posta hesabına ait kayıtlar ya da erişim bilgileri talep edildiği takdirde bu talep ECPA'da belirlenen çerçevede karşılanır.

[60] Ibid: s.84 *"Multiple Warrants in Network Searches"*.

[61] Sec. 94-110 CCP The German Code Of Crımınal Procedure İngilizce versiyonu **için** Bkz: http://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html.

BkartA, teşebbüslerin olağan işleyişini aksatmamak amacıyla çoğunlukla inceleme konusu ile ilgisi bulunabilecek elektronik veri setlerinin kopyasını alarak, kendi merkezinde yer alan adli bilişim laboratuvarında elektronik delillerin elde edilmesi yolunu seçmektedir[62] (BKartA[63] 2010, 22). BKartA tarafından adli bilişim süreçlerinde genel maksatlı *FTK®, Encase®, Ilook®* gibi adli bilişim yazılımları ile spesifik bazı işlevleri yerine getiren *PRTK®* (Şifre kırma), *SecureClean®* (Veri silme) *Ontrack®* (veri kurtarma) adli bilişim yazılımları yoğun olarak kullanılmaktadır (Vollmer 2005).

BKartA Komisyon'un uygulamasına paralel olarak elde ettiği elektronik verileri elektronik formatta muhafaza etmektedir. BKartA buna ek olarak, basılı dokümanları da tarayarak dijital ortama aktarmakta ve adli bilişim araçları ile incelenebilmelerini sağlamaktadır. Bu suretle adli bilişim araçlarının da yardımıyla yazılı dokümanların elektronik veri seti ile birlikte taranması ve incelemenin daha hızlı bir şekilde gerçekleştirilmesi sağlanmaktadır. Aynı zamanda; kendi başlarına bir anlam ifade etmeyen bazı belgelerin diğer belgeler ile ilgisi kurularak delil değeri saptanabilmektedir (BKartA 2010, 22).

BKartA tarafından, elde edilen elektronik veri setleri genellikle inceleme öncesi sahip olunan bilgilerden, pişmanlık başvurularından, görüşmelerden yola çıkılarak belirlenen arama ibareleri aracılığıyla incelenmektedir. Ayrıştırma sırasında ihtiyaç duyulduğu takdirde yeni arama ibareleri de eklenebilmektedir. BKartA tarafından, belgelerin toplu olarak bir arada bulunduğu elektronik veri seti üzerinde, inceleme konusunun kapsamı dışındaki sonuçlara ulaştıracak arama ibarelerinin kullanılıp kullanılmadığı hususu ise tartışmaya açık değildir. BKartA tarafından elektronik veri seti üzerindeki inceleme bitirildikten sonra belirlenen elektronik deliller ve bu delillere ulaşırken kullandığı arama ibarelerinin listesi teşebbüse gönderilmektedir (Saller 2013, 85).

[62] Elektronik delile ulaşmak için başvurulan bu adli bilişim uygulamaları, elektronik delil araması yapılacak elektronik ortamların bulunduğu yerde *(on-site)* ya da elektronik ortama el koymak ya da adli kopya almak suretiyle adli bilişim laboratuvarında *(off-site)* gerçekleştirilmektedir (Maras 2012, 32).

[63] http://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Brosch%C3%BCren/Brochure%20-%20Effective%20cartel%20prosecution.pdf?__blob=publicationFile&v=11.

2.2. ELEKTRONİK DELİLLERİN ELDE EDİLMESİ SÜRECİNDE TEMEL HAK VE ÖZGÜRLÜKLER BAĞLAMINDA ORTAYA ÇIKAN PROBLEMLER

2.2.1. Elektronik Delillerin Elde Edilmesi Sürecine İlişkin Genel Tartışmalar

Klasik delillere nazaran soyut nitelik arz eden, ancak bir bilişim sistemi üzerinde var olabilen elektronik delillerin elde edilmesi süreci zorunlu olarak gerek iç hukukta gerekse uluslararası hukukta güvence altına alınan kişisel hayatın gizliliği ve haberleşme özgürlüğü gibi temel hak ve hürriyetler alanına müdahaleler içermektedir (Özocak 2011, 123).

AB Temel Haklar Şartı'nın[64] *"özel hayata ve aile hayatına saygı"* başlıklı 7. maddesinde herkesin, özel hayatına, aile hayatına, konutuna ve haberleşme özgürlüğüne saygı gösterilmesini isteme hakkına sahip olduğu belirtilmektedir. Avrupa İnsan Hakları Sözleşmesi'nin[65] (AİHS) 8. maddesinin ilk fıkrasında da[66] özel hayatın ve aile hayatının korunması düzenlenmekte, ikinci fıkrasında ise bu özgürlük alanına hangi durumlarda müdahale edilebileceğine açıklık getirilmektedir. Buna göre, ancak yasayla öngörülmüş olması halinde, ölçülülük ilkesine uygun biçimde ve toplumun ekonomik refahı, dirlik ve düzenin sağlanması gibi önemli toplumsal faydaların söz konusu olması veya başkalarının hak ve özgürlüklerinin korunması için gerekli olması durumunda bu tür bir müdahalenin hukuki meşruiyetinden söz edilebilecektir. Kişi hak ve özgürlüklerine müdahale için çizilen bu soyut sınırın idarenin keyfi ve ölçüsüz davranışlarına karşı belli bir koruma sağlamayı amaçladığı ifade edilebilir.

Bilişim sistemleri üzerinde gerçekleştirilen elektronik delil aramaları ve temel hak ve özgürlükler kesişiminde gündeme gelen problemlerin esası, aslında teşebbüse ait tüm kayıtların elektronik ortamda bir arada bulunuyor olmasına dayanmaktadır. Elektronik ortamdaki belgeler, klasik dokümanlara kıyasla çok daha büyük miktarda, çok daha kolay ve hızlı bir şekilde kopyalanabilmektedir. Kopyalanan veri miktarı arttıkça, incelemenin hukuki zeminini oluşturan inceleme kararının kapsamının dışında olan bilgi ve belgeler, avukat müvekkil arasındaki iletişimin gizliliğine ilişkin koruma kapsamındaki bilgi ve belgeler[67] ve kişisel

[64] Article 7 of the Charter of Fundamental Rights. http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[65] http://www.echr.coe.int/Documents/Convention_ENG.pdf.

[66] http://www.anayasa.gov.tr/files/bireysel_basvuru/AIHS_tr.pdf.

[67] Bu kavramın Türkçe karşılığı olarak Pınar, bu imtiyazın avukatlık mesleğinin icrasının bir sonucu

hayatın gizliliğine ilişkin korumadan yararlanan bilgi ve belgelerin ayrıştırılması zorunluluğu ortaya çıkmaktadır.

Burada kısaca AİHS'in 8. maddesi ile öngörülen çerçevenin teşebbüsler açısından da geçerliliği konusunda ABAD içtihadına değinmek gerekli görünmektedir. ABAD önceki kararlarında[68] AİHS'nin 8. maddesi ile getirilen hukuki himayenin bireylere ilişkin olduğunu ve işyerini kapsayacak şekilde genişletilemeyeceğini, Avrupa İnsan Hakları Mahkemesi'nin de (AİHM) aksi yönde bir kararının olmadığını ifade etmiştir. Ancak AİHM'nin *Colas Est*[69] kararından sonra bu içtihadından dönerek[70] teşebbüslerin de AİHS'nin 8. maddesinde öngörülen temel hak ve özgürlüklerin süjesi olarak kabulüne karar verdiği görülmektedir. Bu yorumun bir getirisi olarak, incelenen elektronik veri setinin içinde yer alan inceleme konusunun kapsamı dışındaki belgeler haricinde, haberleşme özgürlüğü, özel hayatın gizliliği gibi temel hak ve özgürlükler alanındaki korumadan yararlanan bilgi ve belgelere hassasiyetle yaklaşılması gerekmektedir. Eş deyişle, ceza yargılamasında olduğu gibi rekabet ihlalinin tespit edilmesiyle sağlanacak kamu yararı ile temel hak ve özgürlükler arasında sağlıklı bir denge kurulmalıdır.

Rekabet otoritelerine sabit disklere el koyma ya da imaj alma yetkisi tanınan ülke uygulamaları açısından da elektronik verilerin ayıklanması ile ilgili tartışmaların devam ettiği görülmektedir. Konunun bir yönü incelemenin el koyma tedbirini gerektirip gerektirmediğine, bir diğer yönü de inceleme, el koyma tedbiri gerektirmese dahi imaj alındığı takdirde alınan içeriğin ayrıştırılmasına ilişkindir. Bu sorunların ele alındığı, Birleşik Devletler'de *United States v. Upham*[71] ve AİHM'nin *Robathin*[72] kararlarında elektronik veriler üzerinde el koyma ya da adli kopya alma tasarrufunda bulunulurken ölçülülük/orantılılık prensibine riayet edilmesi gerekliliğinin vurgulandığı görülmektedir. İki örnek kararda da yargı erki tarafından, arama emrinde bilgisayara el konulması yetkisi tanınmışsa da eğer arama işlemi aramanın yapıldığı yerde de kolayca gerçekleştirilebilir nitelikteyse o takdirde el koyma tedbirine başvurulamayacağı vurgulanmıştır.

Öte yandan elektronik kayıtların kolay ve hızlı bir şekilde kopyalanabilir

olduğu ve bu imtiyazdan müvekkilin yaralandığı gerekçesiyle "avukatlık imtiyazı" kavramını tercih etmiştir. Bu gerekçeye iştirak edilerek söz konusu kavram tarafımızca da benimsenmiştir.

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

[69] Başvuru no: 37971/97, Societe Colas Est And Others v. France, 16.4.2002.

[70] Case C-94/00, Roquette Freres SA v. Commission, [2002] ECR I-9011, 22.10.2002 para. 29.

[71] *United States v. Upham* 168 F.3d 532 (1999).

[72] Başvuru no:30457/06, Robathin v Austria, 03.07.2012.

yapısı, rekabet otoritesini gerekli olandan ya da yetkisi olandan daha fazla bilgi ve belgeyi almaya, bilişim sistemi üzerindeki incelemesini de bu minvalde genişletmeye sevk edebilmektedir (Lang 2013, 2). Fakat temel hak ve özgürlükler alanına yapılan bir müdahale ile ulaşılmak istenen sonuç, karşı tarafın özgürlük alanını daha az kısıtlayıcı uygulamalarla da elde edilebiliyorsa idare tarafından genişletici tercih kullanılmamalıdır. İdarenin aksi yöndeki tercihleri için başvurulan uygulamanın idare açısından daha elverişli ve daha az külfetli olduğu savunması geçerli bir savunma sayılmamaktadır[73].

Genel olarak ülke uygulamalarına bakıldığında elektronik delillerin elde edilmesi süreci ve ispat hukuku içindeki yerine ilişkin hukukun bu alanına özgü spesifik düzenlemelerin yer almadığı görülmektedir[74]. Dolayısıyla klasik delillerin elde edilmesine ilişkin yasalardan yorum yoluyla devşirilen hükümler elektronik delillere uygulanmaktadır. Bunun bir sonucu olarak, geleneksel delillere kıyasen önemli farklılıklar gösteren elektronik delil elde edilmesi faaliyetinde önem sorunlar ortaya çıkmaktadır.

2.2.2. Elektronik Delil Aramalarında İmtiyazlı Bilgi ve Belgeler İle Özel Hayatın Gizliliği Kapsamındaki Bilgilerin Durumu

2.2.2.1. Hukuki İmtiyazdan Yararlanan Belgeler

Avukatlık imtiyazı kapsamında değerlendirilen belgeler, sadece el koymaya/suretini almaya ve ihlal kararında değerlendirmeye alınmaya karşı değil, okuyup öğrenilmeye[75] (göz atma) karşı da hukuki imtiyazdan yararlanmaktadır (Pınar 2011, 138). Soruşturmacı önyargısı olarak nitelendirebileceğimiz, soruşturmayı yürüten tarafın kendi görüşüne yakın sonucu daha çabuk ve kolay kabullenme eğiliminde olduğu göz önüne alındığında, avukatlık imtiyazından yararlanan belge karara esas alınmasa dahi soruşturma heyetinin kanaatini şekillendirmede büyük rol oynayacaktır. Bu açıdan teşebbüs tarafından avukatlık imtiyazından yararlandığı iddia edilen belgelerin içerik dışındaki başlık gibi bölümlerine bakılarak imtiyaz kapsamında olup olmadığına karar verilmesi gerekmektedir (Lang 2013, 10).

Basılı dokümanlar üzerinden inceleme yapıldığı dönemlerde, bir dokümanın imtiyazlı belge kapsamında olup olmadığını teşebbüste belirlemek ve buna göre ayrım yapmak mümkün olmaktaydı. Fakat kimi ülke uygulamalarında elektronik

[73] Case C-212/08, *Zeturf Ltd v. Premier ministr*e, [2011] ECR I, 30.06.2011, para. 48.

[74] ICN'nin elektronik delil elde edilmesine ilişkin çalışması kapsamında yaptığı ankete katılım sağlayan ülkelerin tamamına yakınında elektronik delil toplama yetkilerinin mevcut düzenlemelerden yorum yoluyla yapılan çıkarımlara dayandırıldığı ifade edilmektedir. (ICN 2010, 21).

[75] Case 155/79, *A.M. & S. v. Commission*, [1982] ECR 1575, 18.5.1982.

delillerin elde edilmesi sürecinde belgelerin teşebbüste ayrıştırılması söz konusu olmamaktadır (ECN 2012, 14). Özellikle, veri kütüklerinin adli kopyasının alındığı durumlarda veri kütüğünün nitelikli *(bit to bit)* kopyası alındığı için teşebbüste imtiyazlı belgelerin ve özel hayatın gizliliği kapsamındaki belgelerin ayrıştırılması işlemi gerçekleştirilmemektedir. Bu nedenle elektronik delillerin elde edilmesi sürecinde imtiyazlı belgeler ve özel belgelerin basılı dokümanlar üzerinde yürütülen incelemedekinden daha farklı ele alınması gerekmektedir.

Ülke uygulamalarının çoğunluğunda, rekabet otoriteleri imtiyazlı belgeleri ve özel hayatın gizliliği kapsamındaki bilgileri kopyalamaya ya da el koymaya yetkili değildir. Bu nedenle, ancak imtiyazlı belgeler ayrıştırıldıktan sonra elektronik verilerin kopyası alınabilmektedir. Özellikle, büyük hacimli veri kütüklerinin adli kopyasının alındığı durumlarda imtiyazlı belgeleri ya da özel hayata ilişkin belgeleri teşebbüste ayrıştırmak mümkün olmadığından bazı otoriteler için bu durum adli kopyaları almanın ya da daha büyük hacimli veri kütüklerinin kopyalanmasının önünde engel oluşturmaktadır.

Bazı ülke uygulamalarında, adli kopya alındığı durumlarda, teşebbüsün alınan içerik incelenirken, sürece dâhil olmasına imkân tanınmakta, böylece imtiyazlı belgelerin ayrıştırılması mümkün olabilmektedir. Örneğin, Hollanda uygulamasında, adli kopyası alınan sabit diskler incelenmeye başlanmadan önce teşebbüse hukuki imtiyaz kapsamında değerlendirilebilecek belgeleri belirlemesi için 10 gün mühlet tanınmakta, bu süre zarfında imaj dosyalarının incelenmesine başlanmamaktadır. Almanya ve Danimarka uygulamasında ise teşebbüs istediği takdirde, adli kopyası alınan sabit disklerin incelenmesi sürecine katılabilmektedir (Doury 2009, 6).

Kurum'un mevcut uygulamasında teşebbüslerin e-posta kutularında yapılan aramada çıkan sonuçların dosya konusu incelemeyle ilgili olup olmadığının saptanabilmesi için, sınırlı dahi olsa göz atılmakta, e-postanın kimden geldiğinden ziyade içeriği dikkati celb etmektedir. Dolayısıyla incelemeyi gerçekleştiren raportörler tarafından e-postanın hukuki imtiyazdan yararlandığı kabul edilerek bir sureti alınmadığı durumlar açısından da; belgenin içeriğinin öğrenilmiş olması soruşturmanın ilerleyen safhalarında objektifliği etkileme riskini ortaya çıkarmaktadır.

2.2.2.2. Özel Hayatın Gizliliğinden Yararlanan Kişisel Bilgiler

Günümüzde iş hayatı ile özel hayatın kesiştiği noktada çalışanlar işyerlerine ait ve yaptıkları işe özgülenmiş bilgisayarları, cep telefonları ve tablet bilgisayarları özel hayatlarına ilişkin iletişim için de kullanabilmektedir. Bazı durumlarda bunun

tersi de mümkün olabilmektedir. Yeni nesil cep telefonlarının gelişen özellikleri sayesinde iş yaşamı ile ilgili yazışmalar kişisel telefonlar, şahsın kendisine ait tablet bilgisayarlar üzerinden yapılabilmektedir.

Bu nedenle, rekabet otoriteleri tarafından incelenen ya da yetkilerinin sınırına bağlı olarak el konan veya adli kopyası alınan dijital veriler, özellikle de e-posta hesapları, kişilerin özel hayatına ilişkin bilgiler de içerebilmektedir. Zira e-postalara ilişkin olarak fiziki dokümanlarda olduğu gibi düzenli bir dosyalama sistemi bulunmamaktadır. Genel uygulama özel hayatın gizliliği kapsamında değerlendirilebilecek belgelerin tamimiyle özel hayat alanına ilişkin olması halinde kopyalama ve el koymaya konu edilmemesidir. Öte yandan, inceleme konusu kapsamında yer alan unsurları içeren belgeler açısından ülke uygulamalarına göre farklılaşan hassasiyette koruma sağlandığı görülmektedir (Doury 2009, 5).

Kurum uygulaması yerinde incelemelerde veri kütüklerinin adli kopyası alınmasını ya da veri kütüklerine el koyma yetkisinin kullanımını içermemektedir. Dolayısıyla, özel hayatın gizliliği kapsamında sağlanan korumadan yararlanan kişisel bilgiler teşebbüste ayrıştırılarak alınmasının önüne geçilmektedir.

2.2.2.3. İmtiyazlı Belgeler ve Kişisel Verilerin Korunmasına Yönelik Alınabilecek Önlemler

Elektronik verilerin teşebbüste ayrıştırılmadan alındığı durumlar açısından, alınan veri setinin inceleme konusuyla ilgisi bulunmayan, hukuki imtiyazlardan yararlanan ve kişisel hayatın gizliliği kapsamında yer alan belgeleri de içermesi nedeniyle, temel hak ve özgürlükler alanına ölçülülük ve öngörülebilirlik ilkelerini aşan bir müdahale söz konusu olmaktadır. Bu bakımdan rekabet otoriteleri tarafından girişilen ispat faaliyetinin uzantısı olarak temel hak ve özgürlüklere yapılan müdahalenin hafifletilmesi ve teşebbüslere hukuki koruma sağlanması amacına matuf bazı usullerin geliştirildiği görülmektedir.

Örneğin; Almanya, Avustralya, İngiltere gibi ülke rekabet hukuku uygulamaları ile idari rejimin öncüsü konumundaki Komisyon[76] uygulamasında bu amaca yönelik olarak *"Mühürlü Zarf Prosedürü"*nün uygulandığı görülmektedir (Doury 2009, 9). Mühürlü zarf prosedürü teşebbüste ayrıştırma işleminin gerçekleştirilemediği durumlar özelinde; ayrıştırılmadan alınan elektronik verilerin ayrıştırma işleminin daha sonra teşebbüsün de katılımına imkân tanınarak gerçekleştirilmesi şeklinde tanımlamak mümkündür.

[76] Mühürlü zarf prosedürüne yerinde incelemelerin %10'undan azında, sıklıkla da adli bilişim araçlarının kullanılmadığı yerinde incelemelerde başvurulmuştur.

Mühürlü zarf prosedürü, CMK'nın "Belge Veya Kâğıtları İnceleme Yetkisi" başlıklı 122. maddesinde düzenlenen sistematiğe oldukça benzemektedir. Anılan maddenin 1.fıkrasında hakkında arama tedbiri uygulanan kimsenin belge veya kâğıtlarını inceleme yetkisinin Cumhuriyet Savcısı ve hâkime ait olduğu, 2. fıkrasında el koyulan belge ve kâğıtların bir zarfa konularak mühürleneceği, eğer ileride mührün kaldırılmasına ve kâğıtların incelenmesine karar verilirse zilyede ya da temsilcisine çağrı yapılacağı düzenlenmektedir. Kanun koyucunun bu düzenlemeyle ilgilinin suçla ilişkisi olmayan ve onun özel hayat ve ilişkileri ile ilgili belge ve kâğıtlarının, ne suretle olursa olsun başkaları tarafından okunmamasını sağlamayı ve özel hayatın dokunulmazlığını güvence altına almayı amaçladığı görülmektedir. Bu nedenle kişiye ait kâğıtların incelenmesi, ayrıştırılması ve sonrasında sadece suçla ilgili olanlarının Cumhuriyet Savcısına teslim edilmesinde Hâkimler yetkili kılınmıştır. Kişinin özel hayatının korunmasına atfedilen önem nedeniyle, hâkim tarafından mühür kaldırılırken ve kâğıtlar incelenirken zilyet veya avukatının çağrılması öngörülmüştür.

Rekabet otoritesine elektronik verileri ayrıştırmadan alma yetkisi tanınmış ise, mühürlü zarf prosedürünün ayrıştırılmadan elde edilen elektronik veriler açısından belli bir hukuki koruma sağladığından söz edilebilir. Ancak, bu yetkinin tanınmadığı rekabet hukuku rejimlerinde mühürlü zarf prosedürü uygulaması mevcut olmayan bir yetkinin yaratılması ya da mevcut yetkinin genişletilmesi anlamına geleceği düşünülmektedir.

Nitekim Avrupa Birliği mevzuatında mühürlü zarf prosedürünün ve adli kopya alma yetkisinin düzenlenmemiş olması nedeniyle bu prosedüre ilişkin itirazlar yükselmektedir. AİHM'nin de bu itirazların haklılığına işaret eden, elektronik verilerin ayrıştırılmadan bir bütün halinde kopyalanmasının, inceleme konusundan çok daha geniş bilgilere erişim imkânı sağlaması bakımından özel hayata daha yoğun ve kapsamlı bir müdahale teşkil ettiği, dolayısıyla böyle bir yetkinin açık ve ayrıntılı kurallarla düzenlenmesi gerektiği yönünde anlaşılabilecek kararlarının[77] bulunduğu belirtilmelidir (Gündüz 2009, 26).

Topluluk İlk Derece Mahkemesi'nin (İDM) yakın tarihli *Nexan* kararında[78] Komisyon'un mühürlü zarf prosedürü kapsamında elektronik verileri ayrıştırmaksızın, daha sonra incelemek üzere almasının itiraza konu edildiği

[77] Başvuru no: 50882/99, *Sallinen v. Finland*, 27.9.2005, para. 89-90.

[78] Case T-135/09, *Nexans France* [2012] ECR II, 14.11.2012.

görülmektedir. İDM, Komisyon tarafından mühürlü zarf prosedürü kapsamında elektronik verilerin ayrıştırılmaksızın alınmasının teşebbüsün hukuki pozisyonunda belirgin değişikliğe yol açmadığı ve nihai karara giden yolda bir ara uygulama niteliği taşıdığını belirtmekle yetinerek[79] mühürlü zarf prosedürünün uygulanıp uygulanmayacağına ilişkin bağlayıcı bir karar vermemiştir. Bu açıdan ABAD'ın Nexan'ın temyiz başvurusu[80] neticesinde verecek olduğu karar mevcut uygulamanın hukuka uygunluğu bakımında belirleyici olacaktır.

Yukarıdaki değerlendirme bir bakıma Kurum'un mevcut yerinde inceleme yetkisi çerçevesinde mühürlü zarf prosedürüne başvurulup başvurulamayacağı sorusunun cevabını içermektedir. Bu noktada akla gelebilecek bir diğer soru ise teşebbüsün bu uygulamaya rıza göstermesinin veya gönüllü olmasının mühürlü zarf prosedürünü uygulanabilir kılıp kılamayacağıdır. Zira yerinde incelemeye muhatap olan teşebbüslerin de yerinde inceleme sürecinin bir an önce sonlanması adına böyle bir talepte bulunması mümkündür. Fakat Türk hukuk sistemi içinde ilgilinin arama tedbirine başvurulmasına rıza göstermesi hukuka uygunluk sebebi oluşturmadığından, (Türker 2009, 199) teşebbüsler bu uygulamaya rıza gösterseler dahi uygulanamayacağı düşünülmektedir.

Bir diğer yöntem ise soruşturma heyetinin imtiyazlı belgelere ve özel hayatın gizliliği kapsamında değerlendirilebilecek belgelere nüfuz etmesinin engellenmesi amacıyla; ayrıştırma işlemini gerçekleştirmek üzere soruşturma heyeti dışında yetkililerin görevlendirilmesi yoluna başvurulmasıdır. Örneğin; Birleşik Devletler ve Kanada uygulamasında soruşturma heyetine dâhil olmayan yetkililerce el konulan veri setinin incelemeye tabi tutularak, hukuki imtiyazdan yararlanmayan dokümanların soruşturma heyetine aktarılması suretiyle, soruşturma heyetinin inceleme konusu dışında yer alan bilgi ve belgeler ile avukatlık imtiyazından yararlanan belgelere temas etmesinin önüne geçilmektedir (Doury 2009,7).

2.2.3. Elektronik Delil Araması Yapılması Öncesinde Mahkeme Kararının Gerekliliği

Yerinde inceleme yetkisi idarenin aldığı karar doğrultusunda ve idare eliyle gerçekleştiriliyor olsa da uygulanması bakımından adli aramalara benzerlik göstermektedir (Devrim 2009, 63, Yolcu 2003, 48; Budak 2004, 147). Adli aramaların Anayasa'nın 20. ve 21. maddeleri ile CMK'nın 119. maddesi uyarınca

[79] Ibid. para 121,125.

[80] Case C-37/13 P,Nexans v Commission, 24.06.2013.

hâkim kararı ile ya da gecikmesinde sakınca bulunan hallerde kanunla yetkili kılınmış merciin yazılı emri ile gerçekleştirilebileceği düzenlenmiştir. Arama kararının alınması, kamu menfaati ile temel hak ve özgürlükleri alanına müdahale edilen kişinin özel menfaati arasındaki hassas dengenin gözetilmesini gerektiren zor bir karar olması dolayısıyla bağımsız ve tarafsız bir mahkemeye bırakılmıştır (Devrim 2009, 64).

Devrim (2009, 62) ideal olanının, bilişim sistemleri üzerinde gerçekleştirilen delil araması esnasında temel hak ve özgürlükler alanına yapılan yoğun müdahale nedeniyle yerinde incelemeler öncesinde mahkeme kararı alınması olduğunu fakat mevcut idari rejim bakımından mahkeme kararının alınmamasının meşru kabul edilmesi gerektiğini ifade etmektedir. Ancak yazar yerinde incelemelerin adli aramalara benzer nitelikte olması, kullanılan yetkinin kapsamı ve verilen cezaların ağırlığından hareketle yerinde inceleme öncesinde mahkemeden izin alınmasının, yapılan incelemenin meşruiyetini güçlendireceğini de eklemektedir (2009, 67).

Gerçekten de elektronik ortamdaki aramalarda, klasik dokümanların aksine aranan bilgi ve belgelerin mahiyetlerine göre ayrıştırılmamış olarak bulunmasından dolayı, soruşturmacı tarafından görülmemesi gerekli olan, gizliliği Anayasa ve yasalarla güvence altına alınmış belge ve bilgilere temas edilmektedir. Bu açıdan mahkeme kararı, klasik dokümanlar üzerinde gerçekleştirilen aramalara kıyasen daha büyük önem arz etmektedir (Doury 2009, 3). Bu durumu CMK'nın sistematiği içinde bilgisayar sistemleri üzerinde uygulanacak koruma tedbirlerinin ayrıca düzenlendiği ve ilave bir takım hukuki güvencelerin sağlandığı rasyonalitesi ile birlikte değerlendirdiğimizde, teşebbüsün bilişim sistemleri üzerinde arama tedbirinin uygulandığı yerinde incelemeler öncesinde mahkeme kararının alınmasının, uygulamanın meşruiyetini arttıracağı ve hukuki açıdan güvence sağlayacağı belirtilmelidir.

2.2.4. Elektronik Delil Elde Etme Sürecinin Şeffaflığı

AİHS'de idealize edilen demokratik toplum modelinin üzerinde yükseldiği hukukun üstünlüğü ilkesinin gereği olarak bu metin ile güvence altına alınan temel hak ve özgürlükler alanına yapılacak müdahaleye ilişkin hukuki güvencelerin kamu otoritelerince de sağlanması gereklidir[81]. Bu açıdan idareye tanınan takdir yetkisinin sınırları belirginleştirilmeli ve idarenin keyfi davranışlarına karşı kişinin hak ve özgürlükleri koruma altına alınmalıdır. Bu doğrultuda idarenin hak ve özgürlükler

[81] Başvuru No: 4158/05, *Gillan and Quinton v UK*, 12.01.2010, para. 77.

alanına müdahale içeren eylemlerine ilişkin olarak erişilebilir, öngörülebilir ve müdahaleden etkilenen kişiye idare karşısında hukuki pozisyonunu almasını sağlayacak düzenlemelerin yapılması gerekmektedir[82].

Teşebbüsler açısından elektronik delil elde edilmesi sürecinde başvurulan uygulamalar, imtiyazlı belgeler, özel hayatına gizliliğine ilişkin bilgi ve belgeler ile inceleme konusu kapsamı dışındaki belgelere ilişkin uygulamaların bir standarda bağlı olarak yürütülmesi, teşebbüsler açısından öngörülebilirlik sağlayacağı gibi hak arama hürriyetinin de daha etkin kullanılmasına imkân tanıyacaktır. Bu bağlamda; Hollanda rekabet otoritesinin doğrudan elektronik delil elde edilmesi uygulamalarına ilişkin kılavuzu,[83] Komisyon'un Bilgi Notu ve Kanada[84] rekabet otoritesinin teşebbüsün bilişim sistemi üzerindeki aramalarla ilgi detayları içeren yerinde inceleme prosedürü örnek olarak gösterilebilir. ABD'de ise DOJ tarafından ceza soruşturmalarında bilgisayarlarda arama ve el koyma ile elektronik delillerin toplanması hakkında yayımlanmış bir kılavuz[85] bulunmaktadır.

Bu noktada, Kurum uygulaması açısından da, Komisyon uygulamasında olduğu gibi genel yerinde inceleme prosedürü ve elektronik delil elde edilmesi uygulamalarına ilişkin unsurların birlikte yer aldığı, ya da teşebbüsün bilişim alt yapısı üzerinde gerçekleştirilecek aramalar esnasında başvurulacak uygulamalar özelinde bir metnin hazırlanması ve kamuoyu ile paylaşılmasının yerinde olacağı düşünülmektedir. Söz konusu çalışmanın kapsamı, bilgi işlem alt yapısı üzerinde yapılacak incelemede hangi adli bilişim araçlarının kullanılacağı, imtiyazlı belgelerin nasıl ele alınacağı, elde edilen elektronik delillerin nasıl muhafaza edileceği, verilerin kopyasının hangi yolla alınacağı (adli kopya, basit kopya) gibi detayları içerecek şekilde belirlenmelidir.

Bunun yanı sıra, bilgi işlem altyapısı üzerinde gerçekleştirilecek inceleme açısından teşebbüsün alması gereken önlemler ve işbirliği yapma yükümlülüğünün sınırlarına ilişkin genel bir çerçeve de oluşturulmalıdır. Örneğin, bazı çok uluslu şirketlerde, Türkiye'deki sistem yöneticisinin admin yetkileri sınırlı olduğundan, yurt dışı ile bağlantı kurulup sistem üzerinde gerekli yetkiler tanındıktan sonra

---

[82] Başvuru No: 30562/04, 30566/04; *S. and Marper v. UK*, 04.12.2008, para. 95.

[83] http://www.nmanet.nl/Images/80928%20NMa%20digitale%20werkwijze%202007%20%20vertaling_tcm16-120103.pdf

[84] "Section 15&16 Of The Competition Act" Kaynak: http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/eng/02660.html Erişim tarihi: 08.03.2014.

[85] *"Prosecuting Computer Crimes"* Kaynak: http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf Erişim tarihi: 08.03.2014.

inceleme gerçekleştirilebildiği vakidir. Bu açıdan, Kurum uygulamasının ana hatlarını belirleyen bir metin, bu gibi durumlar açısından teşebbüslerin olası problemleri öngörerek, çözümler üretmesi noktasında yarar sağlayabilecektir.

2.2.5. Sabit Disklerin Bütün Olarak Kopyalanması

Elektronik verilerin yer aldığı cihazlara el koyulması veya elektronik verilerin bir bütün olarak kopyalanması tedbiri temel hak ve özgürlükler alanına daha ağır bir müdahale içerdiğinden, bu tedbire başvurulabilmesi için öncelikle belli koşulların oluşması gerekliliği aranmaktadır. Bu gereklilikler ise genelde, kopyalama işleminin yeterli olmayacağı durumlar, örneğin bazı verilerin şifrelenmiş olması durumu ve zaman kısıtı veya birtakım teknik sebeplerle inceleme mahallinde teşebbüste kopyalama işleminin gerçekleştirilemiyor olması olarak karşımıza çıkmaktadır.

Elektronik delillerin elde edilmesi sürecinde ölçülülük ilkesine vurgu yapılan *Robathin*[86] kararında AİHM, avukatlık mesleğini icra eden bir kişinin bürosunda, bilişim sistemi üzerinde yapılacak aramayı, arama kararının konusu dahilinde sınırlandırma çabası gösterilmeden doğrudan imaj alınması işlemini değerlendirmiştir. Bu değerlendirmede AİHM, bütün veri setinin kopyalanması ve incelemenin soruşturma konusu iddialar ile ilgisi bulunmayan belgeleri de kapsayacak şekilde yapılmasının, kamu yararını gerçekleştirmek için gerekli olandan fazla olduğuna dolayısıyla idarenin ölçülülük ve gereklilik ilkesi dışında hareket ederek ve AİHS'nin 8. maddesinin ihlal edildiğine karar vermiştir.

Avukat bürosunda yapılan bir incelemeye ilişkin olması ve bilgisayarların adli kopyaları ile birlikte incelemeyle yakından uzaktan ilgisi bulunmayan üçüncü kişilere ait bilgilerin de alınmış olmasının bu karara zemin hazırladığı ifade edilebilir (Lang 2013, 6). Aynı nispette olmasa da bu durum yerinde incelemelerde gerçekleştirilen elektronik delil aramaları için de geçerlidir. İş yerinde bulunan belgelerin işle ilgili olduğu varsayımında hareket edildiği takdirde dahi, teşebbüse ait imtiyazlı belgeler ile inceleme gerçekleştirilen teşebbüsle iş ilişkisinde bulunan diğer teşebbüslere ait hassas bilgiler elektronik ortamda birlikte bulunabilmektedir.

2.2.6. İnceleme Kararı'nın Kapsamı ve Arama İbareleri

Elektronik veri seti üzerinde hangi arama ibarelerinin kullanacağı ve bu ibarelerin kapsamı, incelemenin kapsamını da belirleyeceği için önemlidir. Zira elde edilecek bilgi ve belgeler arama kararının kapsamı ile sınırlıdır (Lang 2013, 11). Arama ibarelerinin, arama kararından bağımsız olarak belirlenmesi,

[86] Başvuru no:30457/06, *Robathin v Austria*, 03.07.2012.

inceleme kararının kapsamı dışına çıkıldığı anlamını taşıyacaktır. Meselenin anlaşılması açısından İDM'nin inceleme kararının kapsamı dâhilinde hareket etme zorunluluğuna ilişkin *Nexan/Prysmian* kararındaki tespitler önemli görünmektedir.

Nexan ve Prysmian tarafından yerinde inceleme kararına ilişkin olarak; Komisyon'un elinde yerinde inceleme kararı almasını makul gösterecek yeterli done olmadığı, inceleme kararında rekabet ihlalinin olduğu düşünülen pazarın "elektrik kabloları ve malzemeleri tedariki pazarı, ek olarak sualtı ve yer altı yüksek gerilim kabloları" şeklinde oldukça geniş kapsamlı belirlendiği, oysa Komisyon'un sadece su altı yüksek gerilim kabloları pazarına ilişkin rekabetin ihlal edildiği şüphesini uyandırabilecek bilgiye sahip olduğu öne sürülmüştür. İDM, pişmanlık başvurusu kapsamındaki belgeler, Komisyon'un konuya ilişkin basın açıklaması ve Komisyon yetkililerinin yerinde incelemelerde özellikle yoğunlaştıkları çalışanların çalıştıkları alanlardan yola çıkarak bu itirazı yerinde bulmuş ve inceleme kararını kısmen iptal etmiştir.

İDM öncelikle, Komisyon'un yerinde inceleme kararında, yerinde incelemenin konusunu, amacını ve incelenen pazarı net bir şekilde belirtmesi gerektiğini ifade etmiştir. Yerinde inceleme kararında inceleme konusunun kapsamı elektronik delil aramasının da sınırlarını belirleyeceği[87] için İDM'nin *Nexan* ve *Prysmian*'ın yukarıda yer verilen itirazlarına ilişkin değerlendirmeleri önem taşımaktadır. Nitekim İDM kararında Komisyon'un yerinde incelemelerde aramalarını yerinde inceleme kararında belirtilen pazarlarla sınırlaması gerektiğini, inceleme kararında belirtilen pazarlarla ilgisi bulunmayan belgeleri kullanamayacağını belirtmiştir.

ABAD'ın *Hoechst*[88] kararında da belirtildiği üzere; incelemenin hangi pazara yönelik olduğunun net bir şekilde belirtilmesi, incelenen teşebbüsün Komisyon ile girişeceği işbirliğini Komisyon'un rekabet ihlali şüphesini destekleyecek ön bulgulara sahip olduğu pazarlar ile sınırlayabilmesi ve savunma hakkının etkin kullanılması bakımından önem taşımaktadır.

İnceleme kararları, elektronik delil aramasında kullanılacak anahtar kelimeleri ve diğer arama ibarelerini içermez; dolayısıyla uygulamada elektronik veri seti üzerinde hangi anahtar kelimeler ve ibarelerin aranacağı incelemeyi gerçekleştiren yetkililer tarafından belirlenir. Kullanılan arama ibarelerinin inceleme kararında belirtilen konunun kapsamında olması gereklidir. Kullanılan arama ibaresi inceleme konusu kapsamında değilse, o arama ibaresi üzerinden yapılan sorgulama

[87] Bkz. 1/2003 Sayılı tüzüğün 12/2. ve 28/1. maddeleri.

[88] Cases 46/87 and 227/88, *Hoechst AG v. Commission*, [1989] ECR 2859, 21.9.1989, para. 29.

sonucunda ortaya çıkan içeriğin kopyalanması hukuka aykırılık arz edecektir. Bunun önüne geçebilmek adına Birleşik Devletler uygulamasında inceleme ekibi ile teşebbüs avukatları mümkün olan en uygun çerçeveyi belirleyebilmek adına kullanılacak arama ibarelerini müzakere etmektedir (Lang 2013, 11) .

Arama ibareleri ne kadar özenle seçilirse seçilsin, arama ibareleri ile örtüşen fakat inceleme konusuyla ilgisi bulunmayan, delil ya da emare niteliği taşımayan verilerin kopyalanmasının söz konusu olması muhtemeldir. Bu kapsamdaki verilerin teşebbüsten alınması, AB Temel Haklar Şartı'nın 7. maddesi kapsamında başlı başına bir ihlal teşkil etmese de, ölçülülük ilkesinin aykırı davranılmış olacaktır. Özellikle, adli bilişim araçları yardımıyla, içerisinde inceleme konusu kapsamı dışında da çok sayıda elektronik verinin yer aldığı veri seti üzerinden arama ibareleri kullanılarak yapılan aramada, sorgulama sonuçlarının doğrudan alınması durumunda ölçülülük unsuruna aykırı bu türden bir problem ortaya çıkabilecektir (Lang 2013, 11).

Türkiye uygulaması için ise şu aşamada böyle bir riskten bahsedilemeyecektir. Zira, dahili arama imkanları ile arama ibareleri taranmakta ve sorgulama sonuçları, incelemeyi gerçekleştiren raportör tarafından ön incelemeye tabi tutulduktan sonra çıktısının alınıp alınmamasına karar verilmektedir. Sınırlı sayıda alınan çıktılar arasında bariz şekilde inceleme ile ilgisi kurulamayacak belgeler de tutanak hazırlanırken gerekirse ayrıştırılabilmektedir.

2.2.6.1. Arama İbarelerinin Teşebbüsle Paylaşılması

Elektronik delil arama faaliyetinin özellikle adli bilişim araçları ile yürütüldüğü bir düzende arama ibarelerinin teşebbüsten gizlenmemesi yerinde olacaktır[89]. Kurum'un mevcut uygulamasında daha önce de ifade edildiği gibi alınan belgeler tutanağa geçirilirken detaylı bir ayrıştırma sağlanmaktadır. Ayrıca, teşebbüs temsilcisi incelemeye refakat ederken kullanılan arama ibarelerini öğrenebilmektedir. Bu nedenle arama ibareleri gizlenmediği gibi gizlendiği durumda dahi ortaya çıkabilecek sorunların önüne geçilmiş olmaktadır.

Fakat sabit disklerin imajının alınarak büyük hacimli bir veri setinin üzerinden taramanın yapıldığı durumlar farklı özellikler arz etmektedir. İncelemenin hangi kapsamda ele alındığını kullanılan arama ibarelerinin çerçevesi belirleyecek olduğundan, teşebbüsün hangi arama ibarelerinin kullandığı bilgisine sahip olması gerekliliği ortaya çıkmaktadır. Çünkü teşebbüsün inceleme konusunun kapsamını

[89] Bu tespit soruşturma gizliliği açısından ifşa edilmesi sakıncalı olmayacak arama ibareleri açısından geçerlidir. Bkz. Case 145/83, *Adams v. Commission*, [1985] ECR 3539, 7.11.1985.

açık ve net olarak bilmesi savunma hakkının daha etkin kullanılabilmesi ve inceleme kararına karşı muhtemel itirazlarını şekillendirebilmesi açısından önemlidir. Gerçekten de, eğer teşebbüs hangi arama ibarelerinin kullandığını bilmezse inceleme ekibinin inceleme kararında yer alan kapsama sadık kalıp kalmadığından emin olamayacaktır.

Öte yandan, teşebbüs ile kullanılacak arama ibarelerinde mutabık kalınması, yetkililer tarafından alınacak belgelerin seçilim aşamasını hızlandıracaktır. Geniş bir arama ibaresi listesi kullanılması durumunda, yapılan sorgulama sonucunda çok sayıda belgenin gözden geçirilmesi zorunluluğu ortaya çıkacaktır. Ayrıca, rekabet otoritesinin bazı konularda eksik ya da yanlış malumatının olması mümkündür. Bu gibi nedenlerle arama ibarelerinin teşebbüsle kısmen de olsa müzakere edilmesi incelemenin kapsamının gereksiz olarak genişlemesini önleyeceği gibi, ölçülülük ilkesine uygun hareket edilmiş olmasını sağlayacaktır. Bu gerekçelerle arama ibarelerinin incelemeye muhatap olan tarafla paylaşılması yerinde incelemenin etkin ve hızlı bir şekilde gerçekleştirilmesine katkı sağlayabilecek niteliktedir.

2.2.7. Elektronik Delillerin Elde Edilmesi Uygulamalarına İlişkin Yargısal Denetim

AİHM'nin *Smirnovv* kararında[90], yerinde inceleme öncesinde mahkeme kararı alınmamasının idareye geniş bir takdir yetkisi tanıdığı belirtilmiştir. Ardından inceleme sonrasında etkili bir yargısal denetimin varlığının bu olumsuzluğu belirli ölçüde giderebileceği, fakat buna rağmen idarenin inceleme kararı verilmesi için uygun ve yeterli gerekçelerin oluşup oluşmadığını tayin etme konusunda yetersiz kaldığı ifade edilmektedir. AİHM'nin *Ravon* kararında[91] ise yerinde inceleme kararına ve yerinde inceleme kararına dayanarak uygulanan tedbirlere ilişkin olarak etkili bir yargısal denetimin olması gerektiği ifade edilmektedir (Gündüz 2009, 25).

Yerinde inceleme öncesi mahkeme kararının alındığı ülke uygulamalarında, gerek kararın kendisinin gerekse de kararın icrası esnasındaki uygulamaların yargısal denetimi mümkün olabilmektedir. Fakat mahkeme kararının gerekli olmadığı, rekabet ihlallerinin idari rejim içinde ele alındığı ülke uygulamalarında, yerinde inceleme kararını ve kararın gereğini yerine getiriliş şeklini kısa vadede denetleyecek etkin hukuki mekanizmaların bulunmadığı görülmektedir (Doury 2009, 8). Örneğin; İDM'nin *Nexan* kararında[92], Komisyon'un teşebbüsün

[90] Başvuru no: 71362/01, *Smirnovv v. Russia*, 7.7.2007, para. 45, 47.

[91] Başvuru no: 18497/03, *Ravon v. France*, 21.2.2008, para. 28.

[92] Case T-135/09, *Nexans France v. Commission* [2012] ECR II, 14.11.2012.

bilişim alt yapısı üzerinde elektronik delil arama yetkilerine dair itirazlara ilişkin değerlendirmesi, itiraza konu edilen inceleme kararının ara karar niteliğinde olduğu[93] ve teşebbüsün hukuki pozisyonunda değişiklik meydana getirmediği,[94] bu sebeple ancak nihai kararla birlikte temyiz edilebileceği yönünde olmuştur. Öte yandan, teşebbüsün Komisyon'un adli kopyaları almasına izin vermemesi durumunda, Komisyon tarafından 1/2003 sayılı Tüzüğün 23(1) (c) ve (d) maddeleri uyarınca idari para cezası uygulanması kararının, nihai karar beklenmeksizin temyiz edilebileceği ifade edilmiştir[95].

Teşebbüsün, yerinde inceleme uygulamalarına engel olmak için, hakkında yerinde incelemenin engellenmesine ilişkin yaptırım kararı uygulanmasına neden olduktan sonra bu kararı temyiz etmesi seçeneğinin makul bir yaklaşım niteliği taşımadığı açıktır. Zira bu seçenek, yerinde incelemenin engellenmesi sebebiyle maruz kalabileceği yaptırım ortadayken, inceleme sırasındaki bir uygulamaya karşı çıkması halinde elde edebileceği kazanımların belirsiz olması nedeniyle, teşebbüsü önemli bir risk almaya mecbur bırakmaktadır (Dietzel vd., 2012). Bu risk faktörü ise adil yargılanma hakkının bir parçası olarak iç hukukta ve uluslararası hukukta güvence altına alınmış olan adalete erişim hakkını kısıtlar niteliktedir[96].

Öte yandan, yerinde inceleme kararı ve inceleme sırasındaki uygulamaların yargısal denetimini gerçekleştirecek hukuki mekanizmaların olmayışı, itirazların ancak nihai karar ile birlikte temyiz edilebilmesinin de yeterli hukuki koruma sağlamayacağı söylenebilecektir. Soruşturma heyeti tarafından görülmemesi gerekli imtiyazlı belgelerin ya da inceleme kararının kapsamı dışında yer alan belgelerin soruşturma dosyasında yer almasının, karara esas alınmasa dahi, karara ne ölçüde etki ettiğinin belirlenmesi mümkün olmayacaktır (Doury 2009, 3). Bu bakımdan, yerinde inceleme kararı ve yerinde inceleme sırasındaki uygulamalara ilişkin olarak, nihai karardan bağımsız yargısal denetim yolunun açık olması önem kazanmaktadır.

Türkiye uygulaması açısından da Kurul'un bilgi isteme ve yerinde inceleme kararları nihai karara ulaşmada hazırlayıcı işlem niteliğinde olduğu için, ancak nihai kararla birlikte yargıya başvurulabilecektir (Eğerci 2005, 167). O halde Kurul'un esasında bir idari işlem olan idari para cezası uygulanmasına ilişkin kararlarının, cezalandırma iradesi ve potansiyel cezanın ağırlığı da göz önüne

[93] Ibid. para.116.

[94] Ibid. para.115.

[95] Ibid. para.126.

[96] http://www.yargitay.gov.tr/abproje/belge/sunum/conf4/yaseminCag_adaleteerisim.pdf.

alındığında, diğer idari işlemlerden farklı olarak ceza hukukuna ilişkin bir takım güvencelerden yararlanması gerektiği kabul edilmelidir. Ceza yargılamasında suçun cezalandırmasındaki toplum yararı ile sanık hakları arasındaki dengeyi muhafaza ederek maddi gerçeğin ortaya çıkarılması amacına yönelik olarak, delillerin elde edilmesi aşamasında etkinen tarafa bir takım hak ve güvenceler de sağlandığı görülmektedir (Özbek 2001, 181). Bu açıdan, nihai tahlilde toplum refahını amaçlayan rekabet hukuku uygulamaları kapsamında teşebbüslerin temel hak ve özgürlükler alanına ciddi bir müdahale söz konusu olduğundan (Eğerci 2005, 165), kamu yararını hedefleyen rekabet uygulamaları ile bu uygulamalardan etkinen teşebbüslerin temel hak ve özgürlükleri arasında dengenin sağlanması gerekmektedir.

BÖLÜM 3

4054 SAYILI KANUN ÇERÇEVESİNDE ELEKTRONİK DELİL

3.1. GENEL OLARAK 4054 SAYILI KANUN ÇERÇEVESİNDE ELEKTRONİK DELİL

4054 Sayılı Kanun'da "delil" kavramına yer verilerek, rekabeti sınırlayıcı anlaşma, karar ve uygulamaların varlığının her türlü bilgi ve delille ispatlanabileceğinden (md.40, 44, 59) bahsedilmektedir. Bununla birlikte, nelerin delil olabileceği ve hangi hususların hangi delillerle ispatlanabileceğine ilişkin sınırlayıcı bir hüküm öngörülmemektedir. Böyle bir hüküm olmayışı nedeniyle, rekabet hukukunda delil serbestîsi ve delillerin serbestçe değerlendirilmesi ilkelerinin esas alındığı, bir vakıayı ispat edecek bütün delillere ispat vasıtası olarak başvurulabileceği çıkarımında bulunmak mümkündür (Uyanık 2003, 25).

Mevcut uygulamada da, Kurul'un yerinde inceleme yetkisi ve bilgi isteme yetkisi çerçevesinde diğer ispat vasıtalarının yanı sıra elektronik delil de elde ettiği görülmektedir. Bundan başka, taraf savunmaları ve pişmanlık başvuruları ile üçüncü kişilerce yapılan şikâyet ve ihbar başvuruları bağlamında da elektronik delil sunulabilmektedir. Bu kapsamda, çalışmanın devamında, elektronik delillerin elde edilmesi bağlamında Kurul'un yerinde inceleme ve bilgi isteme yetkilerinin ele alınarak; taraflarca sunulan elektronik delillerin kabulüne ilişkin nasıl bir yaklaşım geliştirileceğinin irdelenmesine gerek görülmüştür.

3.2. YERİNDE İNCELEME YETKİSİ KAPSAMINDA ELEKTRONİK DELİL

3.2.1. Yerinde İncelemelerde Elektronik Delil Toplanması Bakımından Yetki Tartışması

Elektronik delillerin elde edilmesi bakımından mevcut uygulamanın yasal altyapısını oluşturan Kanun'un 15. maddesinde, teşebbüsün bilgi işlem altyapısı üzerinde inceleme gerçekleştirilebileceğine ilişkin açık bir hüküm yer

almamaktadır. Bunun bir uzantısı olarak, Kurum'un 17 yıllık uygulama geçmişine rağmen teşebbüsün bilişim sistemlerinin incelenmesine ilişkin sınırın ne olduğu sorusu hala güncelliğini korumaktadır. Bu belirsizlik durumu, hukuken kişisel eşya olan mobil iletişim araçları, tablet bilgisayarlar gibi elektronik cihazlar üzerinde de inceleme gerçekleştirme gerekliliği ortaya çıktıkça daha da artmaktadır.

Kanunun 15. maddesinin lafzında "inceleme" olarak nitelenen eylemin sınırı, uygulanması itibarıyla benzerlik gösterdiği, adli makamlarca bilgisayarlarda arama, kopyalama ve el koyma yöntemini düzenleyen CMK'nın 134. maddesi ile ilişkilendirilerek belirlenebilir. Ancak öncelikle, terminolojik açıdan "arama" ve "inceleme" arasındaki ayrıma değinmek gerekir. Bu açıdan bilhassa bir idari otorite tarafından bu yetkilerin ne şekilde kullanılabileceği noktasında yol gösterici olması düşünülerek, iki kavramın aynı hüküm içerisinde yer aldığı 6362 Sayılı Sermaye Piyasası Kanunu'nun (6362 Sayılı Kanun) 89. maddesi[97] dikkate değerdir. 6362 Sayılı Kanun'un 89/1. maddesinde "*yetkililerin ilgili gördükleri bilgi ve belgeleri istemeye, tüm defter ve belgeler ile elektronik ortamda tutulanlar dâhil tüm kayıtlar ve sair bilgi ihtiva eden vasıtaları, bilgi sistemlerini incelemeye, bunlara erişim sağlanmasını istemeye ve bunların örneklerini almaya yetkili oldukları"* belirtilmiştir. Anılan Kanun'un 89/3. maddesinde ise istenilen kayıt ve belgelerin gizlenmesi durumunda sulh ceza hâkiminin kararı üzerine gerekli yerlerde kolluk yardımı ile arama yapılabileceği düzenlenmektedir. Böylece kanun koyucu, idari otoritenin 6362 Sayılı Kanun'un kendinse tanıdığı yetki çerçevesinde temin edemediği bilgi ve belgelere, yargı yerince kendisine sağlanan bir arama emri ve kolluk yardımı ile ulaşmasının önünü açmıştır.

4054 sayılı Kanun kapsamında gerçekleştirilen yerinde incelemeler açısından bir çıkarımda bulunulacak olursa, mevcut uygulamanın arama faaliyetine yakın olduğu söylenebilecektir. Zira rekabeti ihlal eden teşebbüslerin,

[97] M. 89 – *(1) Denetim, bu Kanun kapsamındaki tüm kurum ve kuruluş ile ilgili diğer gerçek ve tüzel kişilerin bu Kanun ve ilgili diğer mevzuatın sermaye piyasasına ilişkin hükümleriyle ilgili faaliyet ve işlemlerini kapsar. Denetimle görevlendirilen personel, 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 elektronik 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.…*
(3) Kurul Başkanının talepte bulunması ve sulh ceza hâkiminin kararı üzerine gerekli yerlerde kolluk yardımı ile arama yapılabilir. 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.

pek tabii ihlalin gizli kalması için her türlü önlemi alması ve gizlilik kaidesiyle hareket etmeleri beklenecektir. Bu nedenle, inceleme kavramı nispeten edilgen bir faaliyeti nitelemekte; mevcut uygulamada daha etken mahiyetteki arama yetkisine başvurularak teşebbüslerin mahremiyet alanına nüfuz edilmektedir. Zira bu gizlilik öngörüsü, delil elde etmek için temel hak ve özgürlükler bağlamında koruma altına alınan alanlara erişimi gerekli kılmaktadır.

Badur ve Ertem'e (2010, 121) göre ise 4054 sayılı Kanun'daki inceleme ibaresinin; teşebbüsleri yerinde incelemeyi gerçekleştiren Kurul uzmanlarının talep ettikleri defter, evrak ve belgeleri sağlamakla sınırlı olarak yükümlü kıldığını, bunun dışında Kurul uzmanlarının arama yetkisinin bulunmadığını ifade etmektedir. Kurul'un yerinde incelemenin engellenmesi nedeniyle ceza uyguladığı bazı kararlarda da bu doğrultuda itirazların gündeme geldiği görülmektedir.

Örneğin, *Konya MTSK Birliği Derneği kararında*[98] dernek başkanı tarafından, sadece ismiyle talep edilen belgelerin verilebileceği, raportörlerin dolapları ve çekmeceleri arayamayacağının ifade edildiği görülmektedir. Bu karar temyiz edilmediği için, Danıştay'ın konuya ilişkin ne yönde bir değerlendirmede bulunacağını bilmek mümkün olmamıştır. *Reysaş*[99] kararında, ise savcılık kararı bulunmaksızın bir çalışma ofisine girilemeyeceği, Rekabet Kurulu yetki belgelerinin bu kapsamda bir inceleme için yeterli olmadığı iddiaları yer almaktadır. Danıştay konuyu ele aldığı kararında[100], söz konusu iddialara ilişkin doğrudan bir değerlendirmede bulunmazken, inceleme gerçekleştirilecek odanın kilitlenerek, teşebbüs sahibi inceleme mahalline intikal edene kadar incelemenin geciktirilmesini, yerinde incelemenin engellenmesi kapsamında değerlendirdiği görülmektedir.

Yerinde inceleme yetkisi ile karşılaşılan bir başka argüman ise, yerinde incelemelerde bilişim sistemleri ile kişinin her türlü evrak ve belgeleri üzerinde arama gerçekleştirilmesine imkan veren 4054 sayılı Kanun'un 15. maddesinin, Anayasa 21. maddesi ile güvence altına alınan konut dokunulmazlığı ve özel hayatın gizliliği haklarını ihlal ettiği yönündedir. Bu iddianın gündeme geldiği Danıştay kararlarında[101] Anayasa'ya aykırılık sorununun ciddi görülmediği

[98] 15.11.2006 tarih 06-84/1081-313 sayılı Kurul kararı.

[99] 11.11.2009 tarih, 09-54/1320-M sayılı Kurul kararı.

[100] Danıştay 13. Dairesinin 26.03.2013 tarih E: 2010/543 K: 2013/844 sayılı Reysaş kararı.

[101] Örnek olarak; Danıştay 13. Dairesinin 26.03.2013 tarih, E: 2009/5890, K: 2013/847 sayılı Koçak Petrol kararı, 13.12.2006 E: 2005/8957 K: 2006/4722 sayılı Denizli Çimento ve Modern Beton Kararı.

anlaşılmaktadır. Bu çerçevede, Danıştay'ın mevcut uygulamayı teyit ettiğini ifade etmek mümkündür.

Esasında yerinde incelemenin engellenmesine ilişkin Kurul kararlarının çoğu zaman bilgisayarların incelenmesinin engellenmesi odaklı olduğu görülmektedir. Kurul'un Turkcell genel müdürünün odasında ve bilgisayarında yapılmak istenilen yerinde incelemenin, genel müdürün yurt dışında olması ve bilgisayarının şifresinin mevcut olmaması gerekçesiyle engellenmesi nedeniyle ceza uygulanmasına ilişkin kararı, Danıştay 10. Dairesi tarafından hukuka uygun bulunmuş[102] ve Danıştay İdari Dava Daireleri Kurulu (İDDK) tarafından da onanmıştır[103]. Kurul'un *Koçak Petrol* kararında[104] da, teşebbüsün yerinde incelemenin engellenmesi anlamını taşıyacak diğer davranışlarla birlikte, incelemenin başladığı andan itibaren bilgisayara müdahale edilmemesi gerektiği belirtilmesine rağmen, bilgisayardan bir klasörün silinmesi nedeniyle yerinde incelemenin engellendiği sonucuna ulaşılmış; anılan karar Danıştay tarafından da hukuka uygun bulunmuştur[105]. *Reysaş* kararında ise, şirket yetkilisinin taşınabilir bilgisayarı ile birlikte raportörlerin bilgisi dışında 10-15 dakikalığına ortadan kaybolması, diğer gerekçelerle birlikte, yerinde incelemenin engellenmesi ya da zorlaştırılması olarak kabul edilmiş, Danıştay da Kurul'un bu değerlendirmesini hukuka uygun bulmuştur[106]. Bu kararlarından yola çıkarak Danıştay'ın, Kurul'un bilişim sistemleri üzerinde inceleme yapma yetkisini tasdik ettiği sonucuna varmak mümkündür.

Özellikle; yerinde incelemelerde elektronik delil elde edilmesi bakımından ortaya çıkan tartışmaların yetki tartışmalarının, yetkinin dayanağı ve uygulamanın genel niteliği hakkında olduğu ifade edilebilir. Mevcut Kanun tasarısı yasalaştığı takdirde, bilgisayarlar üzerinde inceleme yapma yetkisi yasal zemine kavuşmuş olacaktır. Fakat mevcut uygulamanın genel niteliği hakkındaki belirsizliğe ilişkin olarak, idari rejimin genel sınırları da zorlanarak 15. maddenin yeniden düzenlenmesi bir seçenek olarak sunulabilir.

3.2.1.1. Yerinde İncelemelerde Elektronik Delil Elde Edilmesi Açısından Kanun Tasarısı

Yerinde inceleme yetkisinin içeriğine ilişkin itirazların da etkisiyle, 4054 Sayılı Rekabetin Korunması Hakkında Kanun'da Değişiklik Yapılmasına Dair

[102] Danıştay 10. Dairesi'nin 25.11.2002 tarih ve E:2000/5592, K:2002/4506 sayılı Turkcell kararı.

[103] İDDK'nın 16.06.2005 tarih ve E:2003/315, K:2005/21 77 sayılı Turkcell kararı.

[104] 05.088.2009 tarih, 09-34/837-M sayılı Kurul kararı *(Koçak Petrol Kararı)*.

[105] Danıştay 13. Dairesinin 26.03.2013 tarih, E: 2009/5890, K: 2013/847 sayılı Koçak Petrol kararı.

[106] Bkz. dipnot 100.

Kanun Tasarısı (Kanun Tasarısı) ile Kanun'un 15/1. maddesinin 1. fıkrasının 2. cümlesinde yer alan *"teşebbüs veya teşebbüs birliklerinin*" ibaresinden sonra gelmek üzere *"ve bunların yöneticilerinin ve çalışanlarının"* ibaresi eklenmektedir. Ayrıca, Kanun'un 15. maddesinin a bendinin *" defterlerini veya her türlü ortamda tutulan veri ve belgelerini inceleyebilir"* şeklinde değiştirilmesi, c bendinden sonra gelmek üzere ise *"İncelemenin gerektirdiği hallerde, teşebbüsün temel faaliyetlerini aksatmayacak şekilde büro, dolap ve benzeri yerleri, veri ve bilgi içeren vasıtayı en fazla yirmi dört saat için mühürleyebilir"* bendi eklenmesi öngörülmektedir.

Kanun tasarısı ile *"...her türlü ortamda tutulan veri ve belgelerini"* ibaresiyle, bilişim sistemi üzerinde gerçekleştirilen elektronik ortamda delil aramasının zemini oluşturulmuş olmaktadır. Aynı şekilde birinci fıkrasının ikinci cümlesinden sonra *"... yöneticilerinin ve çalışanlarının"* ibaresinin eklenmiş olması, kişilerin kendisine ait mobil iletişim araçları ve tablet bilgisayar gibi cihazların incelenip incelenemeyeceğine ilişkin belirsizliği ortadan kaldıracaktır.

Kanun tasarısındaki değişikliğin madde gerekçesinde; *"... veya her türlü elektronik ortamda tutulan verilerin, bilgi ve belgelerin incelenebilmesi, bunların bulunduğu* ***elektronik ortamların imajlarının alınması dahil*** *her türlü kopya ve çıktılarının alınabilmesi..."* ifadesine yer verilmesi dikkat çekmektedir. Zira madde metninde imaj alınabilmesiyle ilgili hiçbir düzenleme bulunmazken, gerekçede imaj alınması yetkisini de kapsayan bir düzenlemeden bahsedilmektedir.

Bu noktada imaj alınması bakımından iki olasılıktan söz edilebilir. Bunlardan biri, Komisyon uygulamasında olduğu gibi geçici olarak sabit disklerin imajının alınmasıdır ki bunun mümkün olması gerektiği düşünülmektedir. Bir diğeri, sabit disk imajlarının teşebbüste ayrıştırılmadan alınmasıdır. Ancak ilgili Kanun değişikliğinin lafzından böyle bir anlam çıkarmak güç görünmektedir. Örneğin, CMK 134/5. madde'de *"...verilerin tamamının veya bir kısmının kopyası alınabilir"* denilerek verilerin ayrıştırılmadan alınabileceği düzenlenmiştir. Oysa 4054 Sayılı Kanun bakımından bu türden bir hüküm söz konusu değildir. Ayrıca, imaj alma yetkisinin temel hak ve özgürlükler alanına daha kapsamlı bir müdahale içerdiği için mahkeme kararı olmadan kullanılıp kullanılamayacağı konunun bir başka boyutudur. Öte yandan Kanun'un buna cevaz verdiği varsayılsa bile, daha detaylı olarak düzenlenmesi gereken imaj alma yetkisine ilişkin herhangi bir hükmün yer almaması, bir eksiklik olarak değerlendirilebilir.

Bir diğer önemli yenilik ise, Komisyon'a paralel olarak[107] mühürleme yetkisinin Kanun'da düzenlenmesidir. Süregelen uygulamada 4054 sayılı Kanun ile açıkça

[107] Komisyon'a inceleme süresince mühürleme yetkisi tanınırken, mühürleme süresinin 72 saati aşmaması gerektiği kabul edilmiştir. Bkz. 1/2003 Sayılı Tüzük giriş bölümü para. 25.

öngörülmemiş olmasına rağmen, mühürleme yetkisinin kullanıldığı görülmektedir (Kekevi 2008, 120). Bu açıdan, değişiklik ile düzenlemenin uygulamadan türemiş olacağı ifade edilebilir. Mühürleme yetkisinin elektronik delil açısından önemine gelince, verilerin şifreli olması, adli bilişim araçlarına uyumlu olmayan özel yapım *(custom made)* donanım ve yazılımlar ile karşılaşılması gibi durumlarda incelemeye ara verilmesi gerektiğinde kullanılabilecek bu yetki, elektronik delillerin tahrif edilmesi riskini ortadan kaldırmak adına olumlu bir düzenlemedir. Öte yandan, Komisyon'un uygulamasında olduğu gibi, bilgisayarların geçici olarak imajının alınması gereken bir adli bilişim süreci benimsenirse; bu halde yerinde incelemelerin daha uzun süre gerektirecek olması, mühürleme yetkisinin daha aktif kullanımı anlamına gelecektir.

3.2.1.2. Kişisel Mailler ve Mobil İletişim Araçları Üzerinde Delil Araması Yapılması

3.2.1.2.1. Mobil İletişi Araçlarının İncelenmesi

Artan işlem kapasiteleri ile neredeyse bir bilgisayara denk işlevleri yerine getirebilen mobil iletişim araçları, iş hayatında yoğun olarak kullanılmaktadır. Teşebbüs çalışanları, işle ilgili bir çok işlemi; özellikle de e-posta hesapları arasında senkronizasyon sağlayarak yazışmalarını mobil iletişim araçları üzerinden de yapabilmektedir. Yerinde incelemelerde ağırlıklı olarak e-posta hesapları üzerinde elektronik delil araması yapıldığı düşünüldüğünde, mobil iletişim araçlarının elektronik delil arama süreci dışında tutulması, yerinde incelemelerden beklenilen etkinliğin sağlanmasını büyük ölçüde engelleyecektir.

Komisyon, daha önce genel çerçevesine yer verilen adli bilişim araçlarından yararlanarak gerçekleştirdiği elektronik delil araması sistematiği içinde, mobil iletişim araçları üzerinde delil incelemesi yapmaktadır. Birleşik Devletler uygulamasında da, hâkim kararıyla gerçekleştirilen yerinde incelemelerde, mobil iletişim araçları adli bilişim araçları vasıtasıyla incelenmekte ya da bunlar hakkında el koyma işlemi uygulanabilmektedir.

Kurum uygulaması açısından bu konuya ilişkin bir standart bulunmamakla birlikte genellikle, mobil iletişim araçları teşebbüs tarafından sağlanmışsa inceleme gerçekleştirilmektedir. Yerinde inceleme yetkisini düzenleyen Kanun'un 15. maddesinde inceleme gerçekleştirilebilecek taşınır ve taşınmazların teşebbüs ve teşebbüs birliklerine *ait olanlarla* sınırlandırıldığı görülmektedir. Bu bakımdan mevcut düzenleme çerçevesinde kişilerin mülkiyetinde olan mobil iletişim araçları üzerinde inceleme gerçekleştirilemeyeceği düşünülmektedir.

Esasında, mobil iletişim araçlarının ulaştığı fonksiyonellik seviyesi ve herkesçe erişilebilir olmaları göz önüne alındığında, teşebbüs tarafından tahsis edilmiş olması ya da kişinin kendi mülkiyetinde olması, uygulama açısından bir farklılık yaratmamalıdır. CMK'nın 134. maddesinde yer alan *"...şüphelinin kullandığı"* ibaresine bakılarak, en azından ceza hukuku alanında Kanun koyucunun da bu açıdan bir fark gözetmediği anlaşılmaktadır. Nitekim bu hüküm elektronik delil araması yapılan elektronik cihazın kime ait olduğundan bağımsız olarak arama tedbirinin uygulanmasına imkan vermektedir. Kanun değişikliği tasarısında da, 4054 sayılı Kanun'un 5/1. maddesinin 2. cümlesinde yer alan *"teşebbüs veya teşebbüs birliklerinin"* ibaresinden sonra gelmek üzere *"ve bunların yöneticilerinin ve çalışanlarının"* ibaresinin eklenmesi öngörülmüştür. Tasarının yasalaşması halinde, teşebbüs çalışanlarına ait kişisel olduğu iddia edilen cep telefonlarının da incelenebileceği izlenimi uyanmaktadır.

Öte yandan, bilgisayar işlevi gören mobil iletişim cihazlarının teşebbüsün bilişim altyapısıyla uzak ya da yakın ilişkili olduğu konusundan ayrı olarak; bu cihazlar üzerinde yapılacak incelemenin kişisel hak ve özgürlükler alanına kapsamlı bir müdahale anlamına geleceği açıktır. Mevcut uygulama çerçevesinde sadece dâhili arama imkânları ile gerçekleştirilecek incelemenin yetersiz olması bir yana, gerekenden fazla kişisel bilgiye temas edilmesi sonucunu doğuracak olmasından hareketle, ölçülülük ilkesine aykırılık teşkil edeceği belirtilmelidir.

Komisyon uygulamasında, mobil iletişim araçları da diğer bilgisayarlarla birlikte adli kopyaları alınarak, adli bilişim araçları vasıtasıyla incelenmektedir. Böylece, sadece inceleme kararı kapsamında arama ibareleri kullanılarak kişisel bilgilerin gizliliği korunabilmektedir. Bu açıdan, Kurum'un adli bilişim araçlarını aktif olarak kullanmaya başlaması, mevcut uygulama açısından özel hayatın gizliliği bağlamında ortaya çıkacak sorunları ve genel olarak mobil iletişim araçları üzerinde gerçekleştirilecek incelemenin etkinliğinin arttırılması açısından fayda sağlayacaktır.

3.2.1.2.2. Kişisel E-Posta Hesaplarının İncelenmesi

Günümüzde kişiler, çoğunluğu ücretsiz olarak hizmet veren ağ tabanlı e-posta hizmetlerinden (Gmail, Yahoo Mail vb.) yoğun olarak yararlanmaktadır. Kişisel kullanıma hitap eden bu tür e-posta hesaplarının iş ile ilgili yazışmalar için de kullanılması, hatta sadece iş ile ilgili yazışmalar için kullanılan ağ tabanlı e-posta hesaplarının da bulunması olasıdır. Bu açıdan ilk olarak; ağ tabanlı e-posta

hesaplarının her zaman kişisel kullanıma ait olacağı yanılgısını bir kenara bırakmak gerekmektedir.

Ağ tabanlı e-posta hesaplarının bu şekliyle kullanımının mümkün olması, yerinde incelemelerde teşebbüste ağ tabanlı e-posta hesaplarına erişim sağlanıp sağlanmadığının tespit edilmesini gerektirmektedir. Burada ağ tabanlı e-posta hesaplarının tespit edilmesi gerekliliği ile ifade edilmek istenen, incelenen tarafa bu yönde kullanımda olan bir hesabının olup olmadığının sorulması ve erişim talebinde bulunulması değildir. Zira incelemeyi gerçekleştirenler tarafından **doğrudan bilişim sistemi üzerinde bir tespitte bulunulamamışsa,** karşı tarafın böyle bir e-posta hesabının varlığını gizlemesi halinde, hatta var olduğu fakat erişim izni vermeye yanaşmadığı bir durumda yapılabilecek bir şey yoktur.

Kanımızca, kişinin kullanımında olan ağ tabanlı e-posta hesabına erişim izni vermeye zorlanıp zorlanamayacağı tartışması, sadece bu teşebbüsten o e-posta adresine erişim sağlandığının tespit edilebildiği durumlar için geçerlidir. Bu tartışmaya geçmeden önce, bu tespitin nasıl gerçekleştirileceğine değinilmesi gerekmektedir. Ağ tabanlı e-posta hizmetlerinde e-postalar, hizmet sağlayıcısının (Google, Yahoo vs.) e-posta sunucularında tutulur; kullanıcı internet aracılığıyla tarayıcı üzerinden hesabına erişerek e-posta alma ve gönderme işlemlerini gerçekleştirir. Bu nedenle, tarayıcı üzerinden (tarayıcı geçmişi, çerezler[108]) ve önbellekten[109] ağ tabanlı e-posta hesabına erişim sağlandığına dair emareler elde edilebilir. Ayrıca, "pagefile.sys" ve "hiberfil.sys." gibi sistem dosyalarından da, yararlanılan ağ tabanlı e-posta hizmetinin tespit edilmesine ilişkin emareler elde edilebilecektir[110].

Ağ tabanlı e-posta hizmetlerinin özü itibariyle çevrim içi sağlanan bir bilişim hizmeti olduğundan hareketle, bulut bilişim teknolojisine de dikkat çekmek gerekmektedir. Uygulamada, sadece sabit disk üzerinde yer alan elektronik delillere odaklanılmaktadır. Oysa hızla gelişen ve yaygınlaşan bulut bilişim teknolojilerinin

---

[108] "Çerez (İng. cookie), herhangi bir İnternet sitesi tarafından bilgisayara bırakılan bir tür tanımlama dosyası. Çerez dosyalarında oturum bilgileri ve benzeri veriler saklanır." Kaynak: http://tr.wikipedia.org/wiki/%C3%87erez_(internet) Erişim: 11.03.2014.

[109] Özellikle önbellekten okunan e-postalara ilişkin kısımlar elde edilebilir. Eğer, gönderilen e-postalar daha sonra konumuş ise aynı şekilde bunların belli kısımlarına erişilebilir. Örneğin Windows XP kullanılan bir bilgisayarda Chrome'dan erişilen e-posta hesaplarına ilişkin bilgiler şu dosyalarda tutulmaktadır: WinXP%root%/DocumentsandSettings/%userprofile, %/LocalSettings/Application, Data/Google/Chrome/User Data/Default/Cache.

[110] Kaynak: http://www.magnetforensics.com/webmail-forensics-digging-deeper-into-the-browser/ Erişim: 11.03.2014.

yaygınlaşmasıyla e-posta hizmetlerinden, veri depolamaya kadar birçok bilişim hizmeti, ağ üzerinden tedarik edilecektir. Bilişim teknolojilerindeki bu dönüşümün, delile erişilmesini engellemek üzere kullanılması ihtimali karşısında, adli bilişim araçları kullanılarak teşebbüsün sanal ortamdaki izlerinin takip edilmesi gerekliliği ortaya çıkmaktadır.

Ağ tabanlı e-posta hesabının kullanıldığında dair tespit işlemi gerçekleştirildikten sonra, elektronik verilere ulaşılmasında erişim yaklaşımına göre hareket eden Kurum, kişiden söz konusu e-posta hesabına erişim izni vermesini talep edilebilecektir. Bu noktadan sonra, kişinin bu talebi geri çevirirken öne sürebileceği en önemli argüman, söz konusu e-posta hesabında, özel hayatın gizliliği kapsamındaki yazışmaların yer aldığı olacaktır.

Yetkililerin bu yazışmaların içeriğine bakmaksızın e-posta başlıkları, alıcı ve gönderici adreslerini incelemek kaydıyla yazışmaların genel niteliğine ilişkin fikir sahibi olması mümkündür. Nitekim okunmasında ve öğrenilmesinde sakınca görülen imtiyazlı belgelere ilişkin olarak genel rekabet hukuku uygulaması da bu yöndedir. Bu açıdan kişisel e-posta hesaplarının iş ile ilgili yazışmaları içerip içermediğini belirlemeye yetecek nispette yapılacak inceleme, idarenin ölçülülük ilkesine aykırılık teşkil etmeyeceği ve bunun özel hayatın gizliliğine müdahale anlamına gelmeyeceği düşünülmektedir. Aksi takdirde, rekabet ihlallerinin ortaya çıkarılmasında yoğun olarak e-posta hesaplarından elde edilen delillere dayanıldığı da düşünüldüğünde, ağ tabanlı e-posta hesaplarına "kişisel" adı altında imtiyaz alanı yaratılarak uygulamanın etkinliği azaltılabilecektir. Bu bakımdan, mevcut yetki çerçevesinde kişilerin teşebbüsten erişim sağladığı tespit edilen e-posta hesaplarının incelenmesi noktasında, işbirliğinde bulunmaya zorlanabileceği, karşı tarafın işbirliğine yanaşmamasının yerinde incelemenin engellenmesi kapsamında değerlendirilebileceği düşünülmektedir.

3.2.2. Yerinde İncelemelerde Elektronik Delil Toplanması Bakımından Mevcut Durum

Mevcut durumda, elektronik delil elde edilmesine yönelik sistematik bir uygulamanın varlığından söz etmek mümkün değildir. Genellikle, inceleme konusu açısından stratejik teşebbüs çalışanları belirlenmekte; bu kişilerin kullanımında olan bilgisayarlarda daha önceden belirlenmiş arama ibareleri dâhili arama imkânları ile aratılarak ya da bilgisayar dosyaları arasında gezinilerek elektronik delillere ulaşmaya çalışılmaktadır. Elektronik delil araması büyük ölçüde kişilere ait e-posta kutularında gerçekleştirilmektedir. Yerinde incelemelerde elektronik delillere ulaşılması bakımından herhangi bir adli bilişim aracının kullanımı söz konusu

olmamaktadır. Bu başlık altında, Kurum'un kişisel e-posta hesapları, mobil iletişim araçları gibi elektronik ortamlardan delil elde edilmesine ilişkin uygulamalarına, daha önce bu konulara ilişkin tartışmaların ele alındığı başlıklar altında yer verildiği için tekrardan kaçınmak adına değinilmemiştir.

Arama ibareleri ile yapılan sorgulamalar ile ya da başka şekilde ulaşılan elektronik kayıtlar, çıktıları alınmak suretiyle, kâğıda yazdırılamayacak nitelikteyse elektronik veri taşıyıcısına kaydedilerek alınmaktadır. Bilgisayar çıktılarının delil niteliğine ilişkin itirazların önüne geçilebilmesi için, teşebbüsçe alınan her belgenin onaylanması temin edilmektedir. Öte yandan elektronik formatta alınan veriler açısından genellikle; bu verilerin değişmediğinin, alındığı haliyle muhafaza edildiğinin ortaya konabilmesi adına herhangi bir önlemin alınmadığı görülmektedir. Verilerin elektronik formatta alındığı durumlar açısından, daha sonra elektronik formatta alınan verinin doğruluğuna ilişkin ortaya çıkabilecek itirazların önüne geçilebilmesi için, verilerin kriptografik özetinin alınarak tutanağa yazılması fayda sağlayacaktır.

Mevcut uygulamada elektronik delillerin çıktısının alınması bazı yönleri itibariyle eleştirilebilir. Zira bizzat elektronik deliller, kâğıt üzerinde ya da ekrandaki görünümlerinden daha kuvvetli delillerdir. Bunun sebeplerinden biri, elektronik formatta muhafaza edilen elektronik delillerin, çıktılardan farklı olarak, elektronik delilin değerinin saptanmasını sağlayacak üst verileri de birlikte barındırmasıdır (Göksu 2011, 30). Öte yandan belgelerin elektronik formatta alınmasının, fotokopi ve taşıma külfetini ortadan kaldırmak, dokümanların gözden geçirilmesi ve tasnif edilmesini kolaylaştırmak gibi pratik faydaları da olduğu bir gerçektir.

Bu gerekçelerle, Kurum uygulamasının elektronik delillerin, elektronik ortamda muhafaza edilmesine imkan tanıyacak şekilde geliştirilmesi önem arz etmektedir. Bu yönde atılacak bir adımın, bütüncül bir yaklaşım geliştirilmesini gerektirdiği de hatırlatılmalıdır. Kurum politikalarını oluşturanlar tarafından elektronik delil elde etme süreçlerine ilişkin böyle bir gereklilik tespit edilirse, birbirini tamamlayacak uygulamalardan oluşan bir prosedür geliştirilmesi uygun olacaktır. Aksi takdirde, elektronik verilerin doğruluğunun ve teşebbüse ait verilerin güvenliğinin nasıl sağlanacağı gibi sorunlar gündeme gelecektir.

3.3. BİLGİ İSTEME YETKİSİ ÇERÇEVESİNDE ELEKTRONİK DELİL

Kurum'un 4054 Sayılı Kanun'un 14. maddesi çerçevesinde elektronik delil elde edip edemeyeceğine ilişkin kesin bir hüküm bulunmamaktadır. Esasında,

elektronik delillerin, geleneksel delillerin elektronik ortamdaki halini yansıttığı noktasından hareket edilirse, bu türden bir ayrıma gerek olmadığı da ifade edilebilir. Keza bilgi isteme yetkisi çerçevesinde elektronik belgelerin istenip istenemeyeceğine ilişkin esaslı bir tartışma da bulunmamaktadır.

Bununla birlikte, Kekevi'nin (2011, 109) bu konuya ilişkin yaklaşımı kayda değerdir. Yazar, Kurul'un bilgisayarlar üzerinde gerçekleştirilecek elektronik delil aramasının engellendiği gerekçesiyle aldığı *Turkcell, Koçak Petrol* ve *Reysaş* kararlarına karşılık Danıştay ve İDDK'nın tutumunun Kurum'un bilgisayarlar üzerinde elektronik delil araması yapması yetkisini teyit eder nitelikte olduğunu değerlendirmektedir. Ardından kıyasta bulunmak suretiyle; Kanun'un 14 ve 15. maddelerinin paralellik arz ettiği, dolayısıyla eğer bilgisayarlar üzerinde inceleme yapılabiliyorsa, bilgi isteme yetkisi çerçevesinde elektronik belgelerin de talep edebileceği yönünde bir çıkarımda bulunmaktadır.

Mevcut uygulamada, bilgi isteme yetkisi aracılığıyla iki genel çerçevede elektronik delil elde edildiği söylenebilir. İlk çerçevede, teşebbüslerin ortaklık yapıları, pazar payları, mali tabloları, her türlü ticari sözleşmeleri gibi dosya konusu inceleme açısından iddia konusu ihlalin anlaşılmasına yardımcı olabilecek fakat tali öneme sahip bilgiler elde edilmektedir.

İkinci olarak ise, teşebbüste hazırda bulunmayan fakat bilgi isteme yazısının içeriğinde yer alan ayrıntılı sorulara cevaben hazırlanan bilgilerin elde edilmesi için kullanılmasıdır. Bu kapsamda teşebbüsten, belli zaman aralıkları için, teşebbüsün müşteri/bayi/sağlayıcı gibi iş ilişkisinde bulunduğu taraflar özelinde, bölge ve satış kanalı gibi ayrımları da gözeterek, alım ve satım miktarlarının, bunlara ilişkin fiyat hareketlerinin, uyguladığı indirimlerin/indirim sistemlerinin, her türlü satış koşulunun yer aldığı tabloları/dokümanları hazırlaması talep edilebilmektedir.

Buradan hareketle; bilgi isteme yetkisinin genellikle dosya konusu inceleme açısından destekleyici, tali bilgi ve belgeleri kapsayacak şekilde kullanıldığı, fakat iç yazışmalar, rakiplerle yapılan yazışmalar, toplantı tutanakları gibi tutulması zorunlu olmayan kayıtlar için kullanılmadığı ifade edebilir. Öte yandan, Kanunda inceleme konusuyla ilgili olmak kaydıyla, istenilebilecek bilgilere ilişkin bir sınırlama getirilmediği görülmektedir. Bu noktada bilgi isteme yetkisinin belli çalışanların e-posta hesaplarında yer alan e-postaların ya da bir müşteri ile yapılan yazışmaların talep edilmesine imkân verecek şekilde kullanılıp kullanılamayacağı sorusu akla gelmektedir. Kekevi, rakiplerle yapılan toplantılar hakkında, toplantıya ilişkin hazırlanmış her türlü bilgi ve belgenin talep edilebildiği Komisyon

uygulamasını örnek göstererek, Kurum uygulamasında genellikle bu tür doğrudan delillerin talep edilmemesini bilgi isteme yetkisinin bu yönde kullanımına ilişkin bir ilke geliştirilmemiş olmasını göstermektedir (2008, 119).

Bununla birlikte her ne kadar Kurum uygulaması daha farklı bir yönde gelişmiş olsa da bilgi isteme yetkisinin belirtilen çerçevede kullanıldığı da vakidir. Örneğin; Kurul'un *Doğu Anadolu, Güneydoğu Anadolu, Adana ve Doğu Karadeniz Çimento kararında*[111] bilgi isteme yetkisi çerçevesinde; Kars Çimento'dan elde edilen bir toplantı notunda adı geçen teşebbüslerden bilgi ve belge talebinde bulunulduğu görülmektedir. Bu kapsamda; toplantı notunda adı geçen diğer teşebbüslerden toplantı notunun ait olduğu tarihte gerçekleştirilen bir toplantıya katılım olduysa, katılımcıların adları, soyadları ve görevleri, toplantı gündemi ve toplantıda alınan kararlar, toplantıya ilişkin belgeler ve iş seyahatlerinin kayıtları talep edilmiştir. Cevabi yazılarda teşebbüsler adına teşebbüs çalışanları tarafından belirtilen tarih ve yerde herhangi bir toplantıya katılım olmadığı ifade edilmiştir. Bunu karşın, söz konusu teşebbüslerde yapılan yerinde incelemelerde bazı kişilerin o tarihte Ankara'ya iş seyahati yaptığını gösteren harcama bildirimleri ve faturalara ulaşılmıştır.

Söz konusu kararda, yerinde inceleme gerçekleştirilerek mevcut olmadığı öne sürülen belgelere erişilmiştir. Fakat talep edilen belgelere başka suretle erişilemediği durumlar için, teşebbüslerce talep edilen bilgi ve belgelerin mevcut olmadığının öne sürülmesi karşısında, bilgi isteme yetkisinin işlevi büyük ölçüde ortadan kalkacaktır.

Nitekim, AİHM'nin ABAD'ın *Orkem*[112] kararında vardığı yargıların sorgulandığı *Funke*[113] kararında AİHM, Fransız gümrük otoritesinin varlığından emin olmadığı belgelerin, var olduğu ihtimalinden hareketle[114] ceza uyguladığı, bu nedenle kişinin adil yargılanma hakkının ihlal edildiği sonucuna ulaşılmıştır (Aslam ve Ramsdem 2008, 68). Bu nedenle teşebbüsün, talep edilen belgelerin mevcut olmadığını ileri sürmesi halinde, eğer örnek Kurul kararında olduğu gibi belgeler ortaya çıkarılamazsa, teşebbüse yaptırım uygulanabilmesi söz konusu olmayacaktır.

---

[111] 06.04.2012 tarih, 12-17/499-140 sayılı Kurul kararı *(Doğu Anadolu, Güneydoğu Anadolu, Adana ve Doğu Karadeniz Çimento kararı)*.

[112] Case 374/87, *Orkem v. Commission*, [1989] ECR 3283, 18.5.1989.

[113] Başvuru no: 10828/84, *Funke v. France*, 25.02.1993.

[114] Ibid. para. 44.

Bu bakımdan bilgi isteme yetkisi çerçevesinde daha amaca yönelik, belli çalışanlara ait e-posta yazışmaları gibi, elektronik veri talebinde bulunulsa dahi, teşebbüslerin soruşturma konusuyla ilgili elektronik verileri muhafaza etme yükümlüğü ve delillerin tahrif edilmesi durumunda caydırıcı ceza tehdidi söz konusu olmadığı için istenilen sonuca ulaşılamayacaktır. Zira teşebbüs kendi aleyhine kullanılabilecek her türlü bilgi ve belgeyi gizleme yolunu seçecektir.

Aslında, teşebbüsün kendisi aleyhine kullanılabilecek bilgi ve belgeleri gizlemesi veya çarpıtarak vermesi bilgi isteme yöntemiyle elde edilen diğer bilgi ve belgeler için de geçerlidir. Fakat bilgi ve belgelerin gereği gibi sağlanmasında ceza tehdidi belirleyici unsur olduğu için eğer talep edilen bilgi, tutulması gerekli olan kayıtlarda mevcut ise güvenilirlik problemi daha düşük olacaktır (Devrim 2009, 18). Çünkü bu bilgilere sonradan erişme veya başka kaynaklardan teyit etme imkânının bulunması cezai yaptırım tehdidini arttıracaktır. Buna karşın, E-posta yazışmaları gibi tutulması gerekli olmayan, fiziksel varlığı bulunmayan elektronik veriler açısından güvenilirlik unsuru oldukça düşük olacaktır. Bu yüzden; bilgi isteme yetkisi daha kapsamlı ve doğrudan ihlale ilişkin elektronik verilerin elde edilmesinde amaçlanan faydayı sağlamayacaktır.

3.3.1. Bilgi İsteme Yetkisi Çerçevesinde Elektronik Delillerin Elde Edilmesi Açısından Kanun Tasarısı

Kanun Tasarısı'nın 7. maddesiyle, Kanunun *"Bilgi İsteme Yetkisi"* başlıklı 14 maddesinin *"Bilgi ve Belge İsteme"* başlığı altıda yeniden düzenlendiği görülmektedir. Bu çerçevede yapılması öngörülen değişikliklerden biri de bilgi isteme yetkisinin *bilgi ve belge isteme* şeklinde genişletilerek, belge isteme yetkisinin de tanınmış olmasıdır. Bu değişikliğin bilgi isteme yetkisinin kullanımı açısından ne ifade ettiği önem arz etmektedir.

4982 Sayılı Bilgi Edinme Kanun'un 3/d maddesinde tanımlanan[115] ve yine bir üst kavram olarak HMK'da esas alınan belge kavramını ele aldığımızda belgenin yazılı, basılı veya çoğaltılmış dosya, evrak, broşür vb. ile elektronik ortamda kaydedilen her türlü bilgi, haber ve veri taşıyıcısı olduğu ifade edilmektedir. Bu kapsamda; eğer belge kavramı salt olarak; bilginin saklanabildiği her şey olarak ele alınırsa, ki elektronik ortamda oluşturulan bu veriler genel anlamda belgedir, mevcut yetki çerçevesinde de "belge" talebinde bulunulabildiğinden bahsedilebilir. Dolayısıyla söz konusu değişikliğin sadece uygulama ile mevzuatın

[115] **Belge:** Kurum ve kuruluşların sahip oldukları bu Kanun kapsamındaki yazılı, basılı veya çoğaltılmış dosya, evrak, kitap, dergi, broşür, etüt, mektup, program, talimat, kroki, plân, film, fotoğraf, teyp ve video kaseti, harita, elektronik ortamda kaydedilen her türlü bilgi, haber ve veri taşıyıcılarını ifade eder.

uyumlaştırılmasını sağlayacağı sonucuna varılabilir. Nitekim madde gerekçesinde de revizyondan bahsedilmekte, esaslı bir değişiklik yapıldığına ilişkin herhangi bir ibare yer almamaktadır.

3.4. REKABET HUKUKUNDAKİ TARAFLAR AÇISINDAN ELEKTRONİK DELİLLERE BAŞVURULMASI

3.4.1. Kendi Elindeki Elektronik Delillere Başvurma Açısından

4054 sayılı Kanun'un "delillerin toplanması ve tarafların bilgilendirilmesi" başlıklı 44. maddesinde, Kanunu ihlal ettiği iddia edilen kişi veya kişilerin, kararı etkileyebilecek her türlü bilgi ve delili, soruşturma süresince Kurul'a sunabileceği belirtilmektedir.

Bu çerçevede, Kurul savunma makamı tarafından lehte sunulan delillerin doğruluğunu ve delil değerini, diğer takdiri delillerde olduğu gibi, vicdani kanaatine göre serbestçe değerlendirebilecektir. Ne var ki, delillerin vicdani kanaate göre serbestçe değerlendirilebilmesi keyfi hareket edilebileceği anlamına gelmemektedir. Delillerin akla ve mantığa uygun bir değerlendirmeye tabi tutularak, hangi delillerin neden değerlendirmeye alınıp, neden alınmadığının açıklanması gerekmektedir (Özocak 2011, 111).

Bu açıdan Kurul, tarafça sunulan delillerin gerçek olmadığını ileri sürüyorsa, bunu kanıtlaması gerekecektir. Türk hukukunda genel kural, mahkemeye sunulan bir delilin ancak itiraza konu olması durumunda doğru olup olmadığının incelenmesi şeklindedir. Fakat ülkemiz rekabet hukuku uygulamasındaki taraf kavramı medeni usul hukukundan farklılık arz ettiğinden, sunulan delilin kabul edilebilir olup olmadığı Kurul'un re'sen inceleyebileceği bir meseleye dönüşmektedir.

Eğer Kurul, kararında söz konusu delillerin gerçek olmadığını ileri sürmeden başka delillere dayanıyorsa, bu durumda tarafın sunduğu delillerin doğruluğunu ortaya koyma gerekliliği ortadan kalkacaktır. Bu gereklilik ile ifade edilmek istenen, savunma makamı tarafından sunulan elektronik delillerin ispat edilmek istenen hususun ispatına ne ölçüde muktedir olduğunun değil, elektronik delillerin yargılamaya kabul edilip edilemeyeceğinin (admissibility) ortaya konulmasıdır. Yani Göksu'nun ifadesiyle, "delilin, delili getirenin iddia ettiği "şey" olup olmadığının tespitidir" (2011,170).

Elektronik delillerin yapıları itibariyle değişmeye ve taklide açık olmaları, karara esas alınmadan önce karar mercileri tarafından doğrulanmalarını zorunlu kılmaktadır (Göksu 2011, 169). Zira bilgisayar çıktıları ya da delil zinciri ve doğruluğu sağlanmamış elektronik formattaki kayıtların içeriklerinin kolayca değiştirilebilme ihtimali, bunların tek başına delil olma gücünü zayıflatmakta,

hatta ortadan kaldırmaktadır. Bir belgenin gerçek olmadığı iddia edilirse, artık bu belgenin delil niteliği gerçekliğinin ispat edilmesine bağlı hale gelecektir.

Esasında, yazılı belgeler açısından da değiştirilmiş olma riski söz konusudur. Fakat HMK'nun 211. maddesinde de tarif edilen çerçevede, yazılı belgeler üzerindeki el yazısı ve imza gibi nesnel unsurlar üzerinden belgenin gerçekliği, elinden çıktığı iddia edilen kişiye ait olup olmadığı, belge üzerindeki tahrifat iz bırakacağı için değiştirilip değiştirilmediği kolayca anlaşılabilmektedir. Ancak, elektronik deliller açısından gerekli önlemler alınmaması halinde bu unsurlara ilişkin tespitte bulunmak neredeyse olanaksızdır (Özbek 2001, 187). Buradan hareketle savunma makamının kendi uhdesindeki delillerin doğrulanması açısından nasıl bir yaklaşımın geliştirileceği önem kazanmaktadır.

Tarafın kendi kendisinde bulunan elektronik delillere başvurabilmesinin değerlendirilmesi adına, 6762 sayılı Türk Ticaret Kanunu'nda "ticari defterlerin ispat kuvveti" başlığı altında ticari defterlerin sahibinin hem lehinde hem de aleyhinde delil olarak kullanılabilmesi düzenlemesi yol gösterici olabilir. Zira bu Kanun ile elektronik ortamda tutulan defterler açısından, elektronik belgelere delil niteliği kazandırılmıştır.

Delil bütünlüğünün sağlanması açısından ticari defterler için getirilen, usulüne uygun tutulmuş olma ve parçalarının birbirini teyit etmesi şartı, elektronik delillerin karar mercileri önünde değerlendirilmesi aşamasında aranacak kriterler bakımından önemlidir (Göksu 2011, 72). Kendi elindeki elektronik kayıtlara başvurmak isteyen savunma makamının, öncelikle bu kayıtları düzgün olarak tuttuğunu ortaya koyması gerekir. Bu kapsamda, teşebbüsün veri saklama ve veri güvenliği politikası incelenebilir. Bununla birlikte, eğer bilişim hizmetleri dışarıdan temin ediliyorsa, hizmet sağlayıcısının tanıklığına da başvurulabileceği ifade edilebilir.

Ayrıca; öne sürülen delillerin birbirini teyit eder nitelikte olması ve iddia edilen ihlalin süresinin tamamını ya da önemli bir kısmını kapsayacak şekilde sunulması yerinde olacaktır. Buradan hareketle, elektronik kayıtların tutarlılığı ve güvenilirliğine ilişkin çıkarımda bulunabilir.

Delillerin ağırlığı ve delillerin mahkemece kabul edilmesi arasındaki ayrımın önem kazandığı jürili yargılamanın (Göksu 2011, 103) geçerli olduğu Birleşik Devletler'deki *Lorraine v. Markel American Insurance Co.*[116] davasında da

[116] *Lorraine v. Markel American Ins. Co*., 2007 U.S. Dist. LEXIS 33020 (D. Md May 4, 2007) http://www.mdd.uscourts.gov/opinions/opinions/lorraine%20v.%20markel%20%20esiadmissibility%20opinion.pdf

benzer usuller geliştirildiği görülmektedir. Söz konusu davada, taraflar birbirlerinin beyanlarını içeren e-posta yazışmaları mahkemeye sunmuştur, mahkeme tarafların sunduğu e-postaların kabul edilebilir olması için gerekli olan şartları taşımadığı, bu açıdan kabul edilemeyeceğine karar vermiştir. Bu süreçte elektronik delilin değişikliğe uğramadan elde edildiğine ilişkin uzman bilirkişi ifadesine başvurulması, gerçekliği kanıtlanmış deliller ile öne sürülen delillerin kıyaslanması böylece tutarlı olup olmadığının saptanması, delil üzerinden elde edilecek üst veri ve delilin içeriğinde yer alan emarelerden hareketle doğruluğunun sınanması gibi yöntemlere başvurulduğu görülmektedir.

3.4.2. Şikâyetçi Tarafından sunulan Elektronik Deliller Açısından

4054 sayılı Kanun'un 44. Maddesinde, haklarında soruşturmaya başlandığı bildirilen tarafların, sözlü savunma hakkını kullanma taleplerine kadar mümkünse elde edilmiş olan her türlü delilin bir nüshasının kendilerine verilmesini isteyebileceği, Kurul'un tarafları bilgilendirmediği ve savunma hakkı vermediği konuları kararlarına dayanak yapamayacağı düzenlenmiştir. Bu açıdan elektronik delillerin kabul edilebilirliği, şikâyetçi tarafından ya da pişmanlık başvurusu kapsamında sunulan bazı elektronik delillerin inkâr edilmesi halinde de gündeme gelecektir.

Kurul'un, yukarıda değerlendirilen teşebbüsün kendi lehine elektronik deliller sunduğu durumda yönelebileceği yaklaşımın yanı sıra uzman görüşü müessesesi seçeneği ortaya çıkmaktadır. Nitekim ceza yargılamasında bazen delilleri değerlendirme aracı olarak, bazen de doğrudan delil olarak bilirkişilik müessesinin işlevsel kılındığı, bu kapsamda CMK'nın 67/6. maddesinde yargılama konusu olaya ilişkin olarak ya da bilirkişi raporunda değerlendirilmek üzere uzman mütalaasına başvurulabileceğinin düzenlendiği görülmektedir (Dönmez 2007, 1148). Yine bu paralelde HMK'nun 293. maddesinde dava dosyasındaki teknik ve hukuki açıklamaları güçlendirme amacına yönelik "uzman görüşü" müessesine başvurulabileceği düzenlenmiştir.

Birleşik Devletler uygulamasına baktığımızda da bu çerçevede Federal Medeni Usul Kanunu'nun 53. Maddesi ve Federal Delil Kanunu'nun 706. Maddesi uyarınca hakim tarafından, elektronik delil aramalarına ilişkin olarak, uzman kişi atanabildiği görülmektedir (Weithers 2000, 13). Uzman görüşü, elektronik delillerin elde edildiği adli bilişim aşamalarının başından sonuna kadarki teknik süreçler, uygulanan yöntemler, elektronik delilin güvenilirliği konusunda karar mercilerinin bilgilendirilebilmeleri, bu suretle elektronik delillerin karar mercileri tarafından kabul edilebilirliğinin arttırılması açısından önemlidir.

Türk rekabet hukuku mevzuatında "uzman görüşü"ne ilişkin hükme "Rekabet Kurulu Nezdinde Yapılan Sözlü Savunma Toplantıları Hakkında Tebliğ'de (Sözlü Savunma Tebliği) rastlanmaktadır[117]. Kurul'un bu hükmü işleterek, elektronik delillere ilişkin adli bilişim uzmanlarının görüş ve değerlendirmelerini alması mümkündür. Böylece, Uzman kişi değerlendirmesinden sonra elektronik delillerin güvenilirliğine ikna olunursa, söz konusu elektronik delillerin değerlendirmesine geçilebilecektir.

Uzman görüşü Kurul tarafından belirlenen kişi veya kişilerce hazırlanacağı için, uzmanlığına başvurulan kişinin taraflardan biri tarafından getirilmesi durumunda ortaya çıkabilecek taraflı davranma sorunu[118] da bertaraf edilmiş olacaktır. Öte yandan, ülkemizde henüz adli bilişim alanında kullanılan araçlara ilişkin standartların gelişmemiş olmaması, ayrıca elektronik delillerin elde edilmesine ilişkin adli bilişim süreçlerine dair genel kabul görmüş uygulamaları barındıran iyi uygulama rehberlerinin de bulunmaması, ilk aşamada bir sorun olarak ileri sürülebilir. Bu nedenle hâlihazırda uzman görüşü müessesinin etkinliği sınırlı olsa da, eksikliklerin giderilmesiyle karar mercilerinin elektronik delillerin güvenilirliği hakkındaki endişelerini ortadan kaldırmak üzere elektronik delillerin kabul edilebilirliği artabilecektir

3.5. TÜRKİYE İÇİN ÖNERİLER

3.5.1. Politika Önerileri

Öncelikli olarak ifade edilmesi gereken, yerinde incelemelerin etkinliğinin arttırılması için alışılagelmiş inceleme tekniklerinin yetersiz kaldığı ve adli bilişim araçlarının etkin olarak kullanılmaya başlanması gerekliliğidir. Gelişmiş ülkelerdeki rekabet otoritelerinin bu paralelde hareket ettiği göz önüne alındığında Kurum'un bu alana yönelik hukuki ve teknik altyapıyı bir an önce oluşturmasının gerekli olduğu düşünülmektedir. Bu bakımdan, Komisyon'un merkezinde adli bilişim araçlarının yer aldığı, elektronik delillerin tespit, analiz ve açığa çıkartılmasının adli bilişim

[117] Sözlü Savunma Tebliği m. 13:
"(1) Taraflar, dosya konusu olayla ilgili olarak, konunun uzmanlarından bilimsel görüş alabilirler.
(2) Kurul, talep üzerine veya resen, kendisinden görüş alınan uzman kişinin Toplantıda dinlenmesine karar verebilir.
(3) Savunmasında uzman görüşüne başvuracak olan taraf, uzman görüşü ile birlikte, eğer görüş niceliksel analizler de içeriyorsa bu analizlerin dayandığı her türlü veriyi ve analizi 11 inci maddenin ikinci fıkrasında belirtilen süre içinde Kurula sunar."

[118] Göksu (2011, 150), uzman görüşü müessesine ilişkin en büyük tehlike olarak görüş verecek uzmanı tarafın getirecek olmasına dikkat çekmekte, fakat elektronik delilin teknik ve bilimsel yönüne atıfta bulunarak hakimin yanlış yönlendirilmesinin çok sınırlı olacağını ifade etmektedir.

araçları ile gerçekleştirildiği, birbirini tamamlayan aşamalardan oluşan elektronik delil elde etme prosedürü somut ve başarılı bir örnek olarak gösterilebilir.

Teknolojik gelişmelere paralel olarak elektronik delillerin yer aldığı cihazlarda ve elektronik veri saklama yöntemlerindeki yenilikler ortaya çıkmaktadır. Bu nedenle, elektronik delil araması yapan personelin yenilikleri yakından izlemesi, elektronik delil elde etmek için yeni yöntemlere adapte olması ve en etkin yöntemleri seçebilme hususunda kabiliyetler geliştirmesi Kurum'un da kaynak ayırarak bu çabaya destek olması gerekmektedir.

Kurum'un son yıllarda bilişim alanından meslek personeli alımı yapması, yerinde incelemelerde teşebbüsün bilişim alt yapısı üzerinde gerçekleştirilecek delil aramasının etkinliğini arttırılması bakımından önemlidir. Fakat bu durum diğer meslek personelinin de adli bilişim alanında eğitilmesi gerekliliğini ortadan kaldırmamaktadır. Meslek personelinin sadece aramanın gerçekleştirildiği elektronik ortama entegre basit arama araçları üzerinde arama yapmaya ilişkin temel bilgiye sahip olması, bu konudaki asgari yeterliliği sağlamaktan uzak kalacaktır. Keza Komisyon'un bu konudaki yapılanmasına baktığımızda az sayıda adli bilişim uzmanı istihdam edilirken, yaklaşık 50 kadar meslek personelinin adli bilişim araçlarını kullanacak seviyede adli bilişim konusunda birikim sahibi olduğu görülmektedir.

Komisyon ve Almanya uygulaması incelendiğinde; her iki rekabet otoritesinin yapılanması içinde de adli bilişim uzmanları ve adli bilişim konusunda eğitim almış personelden müteşekkil yerinde inceleme destek birimi olduğu görülecektir. Bu açıdan; Kurum yapılanması içinde yerinde incelemelere sistematik olarak destek sağlayabilecek, yerinde inceleme uygulamasının teknik ve prosedürel açıdan gelişmesine ilişkin çalışmalar yürütecek bir birim ya da çalışma grubu nevinden bir yapı ihdas edilmesinin fayda sağlayacağı ifade edilebilir.

3.5.2. Düzenleme Önerileri

Daha önce de dikkat çekildiği üzere 4054 Sayılı Kanun'da elektronik ortamlar üzerinde delil araması yapılabileceğine ilişkin açık bir hüküm yer almamaktadır. Bu kapsamda mevcut durumdaki belirsizliği nihayete erdirecek, aynı zamanda da teknik gelişmeler ile birlikte elektronik delil elde etme uygulamaları açısından ortaya çıkabilecek gereksinimlere karşılık verebilecek bir düzenleme yapılmasının yerinde olacağı ifade edilebilir.

Bilişim sistemleri üzerinde gerçekleştirilen incelemenin geleneksel delil aramasına göre, temel hak ve özgürlükler adına daha kapsamlı bir müdahale niteliği

taşıdığı göz önüne alındığında; olması gereken hukuk bakımından, uygulamanın sınırları ve bu uygulamaya ilişkin öngörülen hukuki güvencelerin yasayla düzenlenmiş olmasının yerinde olacağı düşünülmektedir. Bu kapsamda; CMK 134. maddede şüpheliye tanınan hukuki güvenceler misal teşkil etmesi bakımından önemlidir.

İlave olarak; Kanunda Kurum'un, bilişim sistemleri üzerinde elektronik delil araması yapma yetkisine dair açık bir hüküm yer almadığı için, bu yetkinin kullanımına ilişkin 4054 Sayılı Kanun'un 27. maddesi uyarınca yapılacak ikincil düzenlemeler, hukuksal açıdan sağlam bir zemine oturmayacaktır. Zira ancak kanun ile düzenlenmesi esas olan temel hak ve özgürlükler alanı, ikincil düzenlemeler ile müdahale edilmiş olacaktır. Bu nedenle, Kanunda bilişim sistemleri üzerinde inceleme yapılabileceğine dair açık bir hükmün yer alması, konuya ilişkin olarak gereksinim duyulan ikincil düzenlemelere hukuki zemin sağlaması bakımında da önem taşımaktadır.

Kurul tarafından hukuka aykırılığın tespit edilmesi amacına yönelik yürütülen idari soruşturmalarda, soruşturma sürecinde izlenen yargı benzeri süreçler de göz önüne alınarak yargılama hukukunda benimsenen temel kaideler esasında delil elde etme yetkilerine ilişkin olarak belirlilik, saydamlık, açıklık esasına uygun idari usullerin geliştirilmesi gerekmektedir. İdarenin takdir yetkisinin çerçevesini net bir şekilde belirleyen, idareyi keyfi ve ölçülülük ilkesine aykırı davranışlardan alıkoyacak, idarenin eylemlerini öngörülebilir kılan düzenlemeler hak arama hürriyetinin etkin kullanımı hukuk devleti anlayışının işlerlik kazanması açısından elzemdir (Koç 2012, 238).

Bu açıdan, öncelikli olarak ilgili kanun maddesinin bilişim sistemleri üzerinde inceleme gerçekleştirilip gerçekleştirilemeyeceği tereddüdünü ortadan kaldıracak şekilde revize edilmesi gerektiği düşünülmektedir. Ardından ise, Kurum'un elektronik delil elde etme sürecinde başvurduğu uygulamalar, kullanılabilecek yetkinin genel çerçevesi, teşebbüslerin işbirliği yükümlülükleri gibi konuları açıklığa kavuşturan, Kurum uygulamasının tutarlılığını arttırılmasına katkı sağlayacak ikincil bir düzenleme yapılmasının yerinde olacağı düşünülmektedir. Bu türden bir mevzuat geliştirme çabasına girişilmesi hukukun temel ilkeleri açısından bir gereksinim, hatta zorunluluk hali olduğu gibi Kurum uygulamasının hukukilik, öngörülebilirlik ve saydamlık gibi modern yönetim ilkelerine yaklaştıracak olması bakımından da önem arz etmektedir.

3.5.3. Yerinde İnceleme Yönergesinin Gözden Geçirilmesi

Bir iç metin olarak yürürlükte olan, *4054 Sayılı Kanun'un Uygulanması çerçevesinde Rekabet Kurumunca Yapılacak Yerinde İncelemelere İlişkin Usul ve Esaslara Dair Yönerge*'de (Yönerge) yerinde inceleme süreçlerine ilişkin oldukça geniş kapsamlı düzenlemelere yer verilmiştir. Yönerge'nin amaçları arasında yerinde incelemelerin hukuki belirlilik, nesnellik ve tutarlık ilkelerine uygun olarak gerçekleştirilmesi, yerinde incelemeye muhatap olan teşebbüslerin haklarının azami ölçüde gözetilmesi, yerinde inceleme işlemleri ve uygulamalarında mümkün olduğunca yeknesaklık sağlanması gösterilmektedir.

Bu bakımdan ilk akla gelen soru Yönerge'nin daha önce gerekliliğine değinilen, yerinde inceleme davranışları ve bilişim sistemleri üzerinde gerçekleştirilecek incelemeye ilişkin ikincil bir düzenlemenin yerini tutup tutmayacağıdır. Öncelikli olarak; gerekliliğine vurgu yapılan ikincil düzenlemenin amaca hizmet etmesini sağlayacak en önemli unsur kamuya açık olmasıdır. Zira yerinde incelemeye muhatap olan teşebbüsler ancak bu sayede hak ve yükümlülüklerini tam olarak bilebilecek, idarenin keyfi veya usulsüz müdahaleleri karşısından hak arama özgürlüğünü daha etkin kullanabilecektir. Dolayısıyla, idarenin davranışları bu doğrultuda disipline edilerek, idarenin uygulamalarının yeknesaklık içinde yürütülmesi sağlanabilecektir. Bu bakımdan, Yönerge'nin bir iç metin olmasının amaçlanan faydayı büyük ölçüde engellediği ifade edilebilir.

Bu noktada, Yönerge'nin mevcut haliyle kamuoyuna açık hale getirilmesi ile amaçlanan faydalara ulaşılıp ulaşılamayacağı sorusu gündeme gelecektir. Yönergenin mevcut haliyle kamuoyu ile paylaşılması, Yönerge'de yerinde incelemeyi gerçekleştirecek uzmanlar açısından anlam ifade eden yerinde incelemeye hazırlık unsurlarının da yer alması, ayrıca nispeten uzun bir metnin hem meselelerin özünün yakalanması hem de gerekli pratikliğin sağlanması açısından etkin bir seçenek oluşturmamaktadır.

Bununla birlikte; Yönergede bilişim sistemleri üzerinde gerçekleştirilecek elektronik delil aramalarına ilişkin her hangi bir düzenleme yer almaması da önemli bir eksiklik olarak ortaya çıkmaktadır. Bu nedenle; oldukça ayrıntılı düzenlemelerin yer aldığı Yönerge'nin mevcut haliyle kamunun dikkatine sunulmasındansa Yönerge temel alınarak hazırlanacak; Yönerge'ye **göre** daha kısa, Komisyon'un Bilgi Notu'na benzer nitelikte yerinde inceleme öncesinde teşebbüse sunulabilecek bir metnin amaçlanan faydaya ulaşılması bakımından daha etkin bir seçenek oluşturduğu düşünülmektedir.

SONUÇ

Geleneksel dokümanlara has yazılılık ve cisim bulma niteliği elektronik deliller bakımında geçerli değildir. Dolayısıyla, elektronik delillerin tespit edilmesi, aranması, karar mercileri tarafından geçerliliği kabul edilecek şekilde elde edilmesi belli süreçlerin takip edilmesini ve bazı kurallara uyulması gerekliliğini doğurmaktadır. Bu nedenle, elektronik delillerin kendilerine özgü niteliklerinin dikkate alınarak yerinde inceleme prosedürünün oluşturulması gerekmektedir.

Karteller başta olmak üzere rekabet ihlallerinin ortaya çıkarılması için girişilen ispat faaliyeti, çoğunlukla teşebbüslerin bilişim sistemleri üzerinden elde edilecek delillere bağlı olarak gerçekleştirilmektedir. Bu nedenle daha etkin elektronik delil araması yapılması, yerinde incelemelerin etkinliğine ve rekabet ihlalleri ile girişilen mücadelenin başarısına doğrudan etki edecektir. Komisyon ve ABD başta olmak üzere birçok rekabet hukuku rejiminde bu amaca matuf olarak adli bilişim yazılımlarının etkin olarak kullanıldığını görülmektedir. Kurum'un da bu çerçevede uygun adli bilişim altyapısını oluşturup, elektronik delil aramasını, eksikliklerine daha önce dikkat çekilen mevcut uygulamanın ötesine taşıması gerekmektedir.

Kurum'un ekonomik kolluk görevini ifa ederken kullandığı yetkilerin, karşı tarafın temel hak ve özgürlükler alanına müdahale içerdiği açıktır. Bu müdahalenin hukukun temel prensipleriyle uyumlaştırılması, bu doğrultuda etkinen taraf açısından hukuki güvencelerin öngörüldüğü, hak arama hürriyetinin etkin kullanımına olanak sağlayan düzenlemelerin yapılması gerekmektedir. Bu bağlamda, bilişim sistemleri üzerinde yapılacak incelemenin yasal zeminin sağlamlaştırılması; bilişim sistemleri üzerinde yapılacak delil aramasına ilişkin uygulamaların, kullanılan yetkinin kapsamının, teşebbüsün işbirliği yapma yükümlülüğünün çerçevesinin belirleneceği açıklayıcı metinlerin oluşturulması önem taşımaktadır.

ABSTRACT

As a consequence of advancements in information technologies, traditional business tasks have been transferred to the digital realm. Therefore; today vast majority of the documents created throughout the bussiness operations are being stored and distributed by electronic means. Because of this transition, electronic evidence gathering has become a standard tool for competition authorites in their fight against competition law infrigments. On the other hand, due to the lack of spesific norms for electronic evidence in competition regimes, there are ongoing debates over legal aspects of electronic evidence. In addition to that, especially for non criminal competition law regimes there are problems related to insuffcient technical capabilities in electronic evidence gathering processes. Throughout the thesis both legal and technical aspects of electronic evidence have been analyzed from competition law perspective. By analyzing Turkish Competition Authority's electronic evidence gathering processes and comparing it to the other competition law regimes, it has been emphasized that technical capacity for electronic evidence gathering should be increased. Moreover, there are uncertainities related to legal base of Turkish Competition Authority's electronic evidence gathering authority. By reviewing the current Turkish Competition Law and projected Draft Law, boundaries of authority have been discussed in detail.

KAYNAKÇA

AKARSLAN, H. (2012), *Bilişim Suçları*, Seçkin Yayınları, Birinci Baskı, ANKARA.

MAINI, A. (2007), *Digital Electronics Principles, Devices and Applications,* 1. Baskı John Wiley & Sons Ltd, West Sussex/İNGİLTERE.

ARTHUR K.K., VENTER H.S. (2004), "An Investigation Into Computer Forensic Tools", http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/060.pdf .

ASLAM, I. ve M. RAMSDEN (2008), "EC Dawn Raids: A Human Rights Violation?", *The Competition Law Review,* Vol. 5, Issue 1, 61-87.

AVŞAR B. Z., G. ÖNGÖREN (2010), *Bilişim Hukuku*, Türkiye Bankalar Birliği, 1. Basım, İSTANBUL.

BADUR E.,ERTEM B. (2010), "Rekabet Kurulu'nun Denetim Yetkisini Kullanma Araçları -Geçici Tedbir, Bilgi İsteme ve Yerinde İnceleme Kararları", *TBB Dergisi,* 2010 (90), 103-121.

BADUR E., ERTEM B., (2008), "Rekabeti Sınırlayıcı Uygulamalara İlişkin İnceleme ve Araştırma Usulü", *Rekabet Dergisi* Sayı 33, s. 3-59.

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

BRAID, M. (2001), "Collecting Electronic Evidence After a System Compromise", http://www.auscert.org.au/render.html?it=2247 .

BUDAK, A. C. (2004), "AT Konsey ve Komisyonu'nun Yeni Rekabet Tüzükleri ve Rekabet Kanunu'nda Yapılan Değişiklikler Işığında Delillerin Toplanması ve İspat", *Rekabet Kurumu Perşembe Konferansları*-18, ANKARA.

BUI S., ENYEART M., LUONG J. (2003), "Issues in Computer Forensics", http://www.cse.scu.edu/~jholliday/COEN150sp03/projects/Forensic%20Investigation.pdf

CASEY E. (2011), *Digital Evidence and Computer Crime Forensic Science, Computers and the Internet*, 3. baskı, Elsevier Inc., Birleşik Devletler.

CHUNG. C. S., BYER D. J. (1998), "The Electronic Paper Trail: Evidentiary Obstacles to Discovery and Admission of Electronic Evidence", *Boston University Journal of Science & Technology Law*, 179-199.

COSIC J., COSIC Z. (2012), "Chain of Custody and Life Cycle of Digital Evidence", *Computer Technology and Application,* 3, 126-129.

CYBEX INITIATIVE (2006), "THE ADMISSIBILITY OF ELECTRONIC EVIDENCE IN COURT: Fighting Against High-Tech Crime", http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/libro_aeec_en.pdf

ÇAKMAK M. (2005), "İdare Hukuku Ve İnternet", *Gazi Üniversitesi Hukuk Fakültesi dergisi*, cilt: IX s.1-2, 299-328.

ÇETİN E. H. (2011), "Hakim Tarafından Elektronik Belgelerin Delil Olarak Değerlendirilmesi", *Terazi Aylık Hukuk Dergisi,* Sayı:54.

ÇETİNKAYA E. (2013), "Medeni Usul Hukukunda Hukuka Aykırı Yoldan Elde Edilen Delillerin İspat Hukukundaki Değeri", *Genç Hukukçular Hukuk Okumaları,* Birikimler 4, 175-185.

ÇOLAK H., M. TAŞKIN (2007), *Ceza Muhakemesi Kanunu Şerhi*, İkinci Baskı, Seçkin Yayıncılık Ankara.

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

DIETZEL K., POUNCEY C., FOUNTOUKAKOS K., HERRON M., SMITH H. (2012), "Fishing Expeditions, Forensic Imaging and Fines: Important Developments Relating to European Commission Dawn Raids", *Freehills Competition eBulletin*, http://awa2013.concurrences.com/business-articles-awards/article/the-eu-general-court-rules-on

DOKURER S. (2013), "Adli Bilişim İncelemelerinde Veri Kurtarma", *1. Internatıonal Symposium On Digital Forensics And Security Proceding Book*, 362-364.

DOURY N. J. (2013), "Digital Evidence Gathering: An Up-Date", *Concurrences*, N° 2-2013, 216-219.

DOURY N. J. (2009) "Digital Evidence Searches in Competition Investigations: Best Practices For Effective Fundamental Rights, Results of an International Survey Among Defense Lawyers", *Concurrences*, N ° 4–2009, 1-9.

DÖNMEZ B. (2007), "Yeni CMK'da Bilirkişi Kavramı", *DEÜ Hukuk Fakültesi Dergisi,* Cilt: 9, Özel Sayı, s.1145-1177.

ECN Working Group Cooperatıon Issues And Due Process, Investigative Powers Report, October 2012, http://ec.europa.eu/competition/ecn/investigative_powers_report_en.pdf .

EĞERCİ, A. (2005), *Rekabet Kurulu Kararlarının Hukuki Niteliği ve Yargısal Denetimi*, Rekabet Kurumu Lisansüstü Tez Serisi, No 12, Ankara.

ERPS D. V. (2013), "Digital Evidence Gathering: An Up-Date", *Concurrences,* N° 2-2013, 213-215.

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

GHOSH A. (2004), "Guidelines for the Management of IT Evidence" http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan016411.pdf

GIOVA G. (2011), "Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems", *IJCSNS International Journal of Computer Science and Network Security*, VOL. 11 No. 1, 1-9.

GREER T. (2012), "Electronic Discovery at the Antitrust Division: An Update", http://www.justice.gov/atr/public/electronic_discovery/281388.htm

GÖKSU M. (2011), "6100 Sayılı Hukuk Muhakemeleri Kanunu Çerçevesinde Senetle İspat Kuralları ve Bunların İstisnaları", *Hacettepe Hukuk Fak. Dergisi,* 1(1) 53–65.

GÖKSU M. (2011), Hukuk Yargılamasında Elektronik Delil, Seçkin Yayınları, 1. Baskı, Ankara.

GÜNDAY M. (2007), "Rekabet Kurulu'nun İdari Para Cezalarına İlişkin Kararlarının Yargısal Denetimi Ve Karşılaşılan Sorunlar", *Rekabet Hukukunda Güncel Gelişmeler Sempozyumu-V, 6-7 Nisan 2007 Kayseri* içinde, 3-10, Ankara.

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

HENKOĞLU T. (2011), *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi*, Pusula Yayınları, 1. Baskı, İSTANBUL.

HOSMER C. (2002), "Proving the Integrity of Digital Evidence with Time", *International Journal of Digital Evidence*, Volume 1, Issue 1 1-7.

ICN (2010), "Anti-Cartel Enforcement Manual, Cartel Working Group, Subgroup 2: Enforcement Techniques, Chapter 3: Digital Evidence Gathering", http://www.internationalcompetitionnetwork.org/uploads/library/doc627.pdf .

KEKEVİ, H. G. (2011), "Bilgi İsteme Yetkisine ve Eksik, Yanlış, Yanıltıcı ya da Geç Bilgi Verilmesine İlişkin Rekabet Kurulu Ve Danıştay Kararlarının Değerlendirilmesi", *Rekabet Hukuku İle İlgili Kurul ve Yargı Kararları Sempozyumu Bildiriler-Tartışmalar*, II. Cilt, Banka ve Ticaret Hukuku Araştırma Enstitüsü Yayınları, 67-145 Ankara.

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

KESER BERBER L. (2008), "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El Koyma", Ankara Barosu Bilişim Kurulu, Sempozyum metni içinde, http://trdocs.org/docs/index-33384.html?page=4 .

KOÇ E. (2012), "4054 Sayılı Rekabetin Korunması Hakkında Kanun'da Düzenlenen İdari Para Cezaları İçin Öngörülen İdari Usul", *TBB Dergisi*, 2012 (98), 231-282.

KONURALP, H. (2007), "Rekabet Hukukunda Deliller ve Değerlendirilmesi", *Rekabet Hukukunda Güncel Gelişmeler Sempozyumu-V, 6-7 Nisan 2007 Kayseri* içinde, s. 11-21, ANKARA.

KOZUSHKO H. (2003) , "Digital Evidence", http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/DigitalEvidencePaper.pdf .

LANG J. T. (2013), "Legal Problems of Digital Evidence, Journal of Antitrust Enforcement", *Journal of Antitrust Enforcement*, 1–25.

MALKOÇ, İ., M. YÜKSEKTEPE (2008), *Açıklamalara ve Yorumlarla 5271 sayılı Yeni Ceza Muhakemesi Kanunu*, 1. Cilt, Malkoç Kitabevi, ANKARA.

MARAS M. H. (2012), *COMPUTER FORENSICS Cybercriminals, Laws and Evidence*, Jones and Bartlett Learning Publications, 1. Basım ABD.

MASON S. (2008), "Rethinking Concepts In Virtual Evidence", *Ankara Barosu Uluslararası Hukuk Kurultayı 8-11 Ocak 2008*, Ankara, Cilt II, 176-182.

MUYSKENS N. J., FISCHER D. (2009), "Digital Evidence In Competition Investigations: National Comparisons United States". http://www.shb.com/newsevents/2009/DigitalEvidenceinCompetitionInvestigations.pdf

National Center for Justice and the Rule of Law University of Mississippi School of Law, "COMBATING CYBER CRIME: Essentıal Tools And Effectıve Organızatıonal Structures A Guıde For Polıcy Makers And Managers" (2007), http://www.olemiss.edu/depts/ncjrl/pdf/CyberCrimebooklet.pdf .

OECD (2013), "Latin American Competition Forum Session III: Unannounced Inspections in Antitrust Investigations", http://search.oecd.org/officialdocuments/displaydocumentpdf/?cote=DAF/COMP/LACF(2013)2&docLanguage=En

ÖZBEK O. (2008), "Hukuk Devletinde Bireysel Güvenlik Ekseninde Bilişim Teknolojileri", http:// http://tredocs.com/tw_files2/urls_25/63/d-62577/7z-docs/6.pdf .

ÖZBEK V. Ö. (2001), "Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği Ve Değerlendirilmesi", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, Cilt 59, Sayı 1-2 s.181-202.

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

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

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

PAUL G. L. (2008), *Foundations of Digital Evidence, American Bar Association Publications*, 1. Baskı, Amerika Birleşik Devletleri

PIAZZA L. (2013), "The Revision of the Commission Explanatory Note on European Commission Surprise Inspections", *Journal of European Competition Law & Practice*, Volume 4, Issue 5, 421-422.

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

RICHTER J., KUNTZE N., RUDOLPH C. (2010), "Securing Digital Evidence", *Fifth International Workshop on Systematic Approaches to Digital Forensic Engeneering*, 119-130.

SALLER M. (2013), "Digital Evidence Gathering in German Cartel Investigations", *Europrean Competititon Law Review*, Volume 34 Issue 2, 84-85.

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

STANLEY, A.(2008), "The Continuing Evolution of Consent and Authority in Digital Search and Seizure", *Fordham Intellectual Property, Media & Entertainment Law Journal,* Vol. XIX, Autumn 2008, Number 1, s. 179-218.

SIMS J., K. M. FENTON, D. P. WALES, (2014), *Antitrust Law answer Book, Practising Law Institute, Practising Law Institute Publications*, New York City.

SIMONSSON I. (2013), "Digital Evidence Gathering in Dawn-Raids Judicial Review: Up-Front or Retrospective?", *20th St. Gallen Competition Law Forum*, http://ssrn.com/abstract=2327122.

UYANIK, P. (2003), *Rekabet Hukuku Açısından Delil*, Rekabet Kurumu Uzmanlık Tezleri Serisi, No.34, Ankara

VOLLMER C.(2005),"Bundeskartellamt Gathering Electronic Evidence in Searches/ Raids, ICN Cartel Workshop", http://www.internationalcompetitionnetwork.org/uploads/library/doc691.pdf

WITHERS K. J. (2000), "Computer-Based Discovery in Federal Civil Litigation", http://www.fjc.gov/public/pdf.nsf/lookup/ElecDi01.pdf/$file/ElecDi01.pdf .

YILMAZ, E. (2004), "Rekabet Hukukunda Deliller, Delillerin Toplanması ve Değerlendirilmesi Üzerine Düşünceler", *Rekabet Hukukunda Güncel Gelişmeler Sempozyumu-II*, Rekabet Kurumu Yayınları, ANKARA.

YILMAZ E. (2011), "Hukuk Muhakemeleri Kanununun Getirdikleri", *Ankara Barosu Dergisi*, 2011/2 214-253.

YOLCU, İ. A. (2001); *4054 sayılı Rekabetin Korunması Hakkında Kanun'da Yer Verilen Soruşturma Prosedürünün ve Uygulamada Karşılaşılan Usul Sorunlarının AB Hukuku Bağlamında Değerlendirilmesi*, Rekabet Kurumu Uzmanlık Tezleri Serisi, No:93, Ankara.

ZHENG J. (2009), "Email Evidence Preservation How to Balance the Obligation and the High Cost", *Lex Electronica*, Vol. 14 n°2, 1-16.

ZİRVE S. Ö.,YILDIZ S. (2013), "Canlı Adli Bilişimin İhtiyaç ve Risk Bakımından Değerlendirilmesi", *1. International Symposium On Digital Forensics And Security Proceding Book*, 365-371.

AİHM Kararları

Başvuru no: 50882/99, *Sallinen v. Finland*, 27.9.2005
Başvuru No: 4158/05, *Gillan and Quinton v UK*, 12.01.2010
Başvuru no: 30457/06, *Robathin v Austria*, 03.07.2012
Başvuru No: 30562/04, 30566/04; *S. and Marper v. UK*, 04.12.2008
Başvuru no: 10828/84, *Funke v. France*, 25.02.1993
Başvuru no: 37971/97, *Societe Colas Est And Others v. France*, 16.4.2002
Başvuru no: 18497/03, *Ravon v. France*, 21.2.2008
Başvuru no: 71362/01, Smirnovv. Russia, 7.7.2007

ATAD KARARLARI

Case C-94/00, Roquette Freres SA v. Commission, [2002] ECR I-9011, 22.10.2002
Case 374/87, Orkem v. Commission, [1989] ECR 3283, 18.5.1989
Cases 46/87 and 227/88, Hoechst AG v. Commission, [1989] ECR 2859, 21.9.1989
Case 155/79, A.M. & S. v. Commission, [1982] ECR 1575, 18.5.1982
Case C-212/08, Zeturf Ltd v. Premier ministre [2011] ECR I, 30.06.2011
Case 145/83, Adams v Commission, [1985] ECR 3539, 07.11.1985
Case 89/11 P, E.ON Energie v. Commission, [2012] 22.11.2012

İDM Kararları

Case T-135/09, Nexans France v. Commission [2012] ECR II, 14.11.2012.

Yargıtay Kararları

Yargıtay 9. Dava Dairesi, Esas No: 2012/11543, Karar No: 2013/3370, Karar Tarihi: 06.03.2013

Komisyon Kararları

Case COMP/B-1/39.326-E.ON Energie AG, 30.01.2008.
Case COMP/39.796-Suez Environnement, 24.05.2011.
Case COMP/39793-EPH and others, 28.03.2012.
Cartonboard, [1994]. OJ L 243/1.

Danıştay Kararları

Danıştay 13. Dairesinin 26.03.2013 tarih, E: 2010/543, K: 2013/844 sayılı Reysaş kararı
Danıştay 13. Dairesinin 26.03.2013 tarih, E: 2009/5890, K: 2013/847 sayılı Koçak Petrol kararı,
Danıştay 13. Dairesinin 13.12.2006 tarih, E: 2005/8957, K: 2006/4722 sayılı Denizli Çimento ve Modern Beton Kararı
Danıştay 10. Dairesi'nin 25.11.2002 tarih, E:2000/5592, K:2002/4506 sayılı Turkcell kararı.
İDDK'nın 16.06.2005 tarih ve E:2003/315, K:2005/21 77 sayılı Turkcell kararı

Kurul kararı

18.07.2013 tarih ve 13-46/601-M sayılı Kurul kararı (*TTNET)*
15.11.2006 tarih ve 06-84/1081-313 sayılı Kurul kararı *(Konya Mtsk)*
05.08.2009 tarih ve 09-34/837-M sayılı Kurul kararı *(Koçak Petrol)*
11.11.2009 tarih ve 09-54/1320-M sayılı Kurul kararı *(Reysaş)*
06.04.2012 tarih ve 12-17/499-140 sayılı Kurul kararı *(Doğu Anadolu çimento*)

EKLER

EK-1 Uygulamada Karşılaşılan Sorunlar

Elektronik deliller geride iz bırakmadan değiştirilebilir nitelikte oldukları için, CMK'da koruma tedbirlerini uygulayan kolluğun, elektronik deliller üzerindeki tasarrufunu mümkün olduğunca azaltan, diğer yandan etkinen tarafa hukuki güvence sağlayan hükümler tesis edildiği görülmektedir (Sevimli 2007, 997). Fakat uygulamada CMK 134. maddede ihdas edilen bu hukuki çerçevenin gerçekleşmediğine şahit olunmaktadır. Bu bağlamda CMK 134. Madde de öngörülen arama rejiminin aksayan yönlerinin irdelenmesi, gelecekte Kurum uygulamasını geliştirmeye dönük düzenlemeler açısından yol gösterici olabileceği düşünülmektedir.

CMK 134. madde de kişi temel hak ve özgürlüklerine daha kapsamlı bir müdahale anlamı taşıyan el koyma tedbirinin hangi durumlarda başvurulabileceğinin ve el koyma işlemi sırasında hangi şartlara uyulması gerektiğinin çerçevesi çizilmiştir. Bunlar; CMK maddede el koyma tedbirinin şifre engeli ile karşılaşılması veya gizlenmiş bilgilere ulaşılamaması halinde uygulanabileceği, inceleme tamamlandıktan sonra el konulan cihazların gecikme olmaksızın iade edileceği (134/2.), el koyma işlemi esnasında bütün verilerin yedekleneceğidir (134/3. madde).

Uygulamada el koyma tedbirine verilerin şifrelenmiş olması veya sisteme şifre engeli nedeniyle ulaşılamamasından ziyade adli bilişim uygulamalarının zaman alması, detaylı inceleme yapabilmek için laboratuvar ortamına ihtiyaç duyulması, inceleme mahallinin uygulamaya müsait olmaması gibi gerekçelerle başvurulduğu görülmektedir. Zira vasat bir sabit diskin incelenmesi 4,5-5 saat kadar sürerken daha kapsamlı bir sabit diskin Kolluk tarafından incelenmesi 12-13 saat alabilmektedir (Berber 2008, 5). Bu nedenle, zaman gerektiren imaj alma işlemi, özellikle de çok sayıda bilgisayarla karşılaşma ihtimali yüksek olan örgütlü suçlar bakımından, olay yerinde incelemenin gerçekleştirilmesi yerine el koyma tedbirine başvurulması sonucunu doğurmaktadır. Kolluk kuvvetleri tarafından bu yönde inisiyatif kullanılmasında olay yerinin maddi şartları, inceleme için gerekli teknik araç, gereçlerin eksikliği ve incelemenin olay yerinde makul sürenin ötesinde kalınması gerekliliği gibi nedenler de etkili olmaktadır[1].

El konulan cihazların gecikme olmaksızın iade edileceği şeklindeki madde hükmünün ise adli bilişim personeli ve laboratuvarının yetersizliği, sadece belli

[1] http://www.dijitaldeliller.com/cmk134.htm erişim tarihi: 04.03.2013

illerde adli bilişim laboratuvarlarının olması nedeniyle uygulamada karşılık bulamamaktadır. El koyulan cihazlara aylar sonra inceleme sırası gelmesi nedeniyle uygulamada el koyulan bilgisayarların ve veri kütüklerinin kısa sürede iadesi mümkün olmamaktadır[2].

CMK'nın 134/3. maddesinde el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklenmesi gerektiği, 134/4. maddesinde ise istenmesi halinde bu yedekten bir kopyanın şüpheliye veya vekiline verileceği düzenlenmektedir. Yedekleme işleminin önündeki en büyük engel ise yine zaman problemi ve malzeme eksikliği olarak karşımıza çıkmaktadır. Kolluk kuvvetleri tarafından yedekleme işlemi için gerekli harici disklerin tedarik edilmesinde yaşanan sıkıntılar nedeniyle çoğu zaman kopyanın talep edilmesi halinde dahi bu talebi karşılamak mümkün olmamaktadır. Ayrıca, bilgisayar dışında da dijital veri barındıran sim kart, navigasyon, akıllı telefon gibi farklı nitelikteki birçok elektronik cihazın yedeklemesi teknik nedenlerle yapılamamaktadır. Dolayısıyla, bu durumda da teknik imkansızlıklar nedeniyle yapılan yedeklemenin bir kopyasının şüpheliye veya vekiline vermek mümkün olmamaktadır[3]. Ayrıca, eğer soruşturma bulundurulması yasak olan bir içerik dolayısıyla yürütülmekteyse, bu içeriğin yer aldığı yedeğin şüpheliye verilmesi hukuki bir garabet oluşturacaktır.

CMK'nın 134/5. maddesinde beşinci fıkrasında bilgisayar veya bilgisayar kütüklerine el koyulmadığı hallerde de, kopyası alınan verilerin kâğıda yazdırılacağı belirtilmektedir. Alınan bazı dijital verilerin basılı kopyalarının bir anlam ifade etmemesi, ortalama büyüklükte bir dijital veri setinin dahi yazdırılamayacak kadar çok kâğıt sayfası gerektirebileceği gibi teknik imkânsızlıklar nedeniyle bu madde hükmünün pratikte uygulanabilirliği tartışmalıdır.

Akıllı cep telefonu teknolojisinde kaydedilen gelişmeler, cep telefonlarını nerdeyse bir bilgisayar tarafından gerçekleştirilebilecek her türlü işlevi yerine getirebilecek noktaya taşımıştır. Bu itibarla cep telefonları da elektronik delillerin öncelikli olarak bulunabileceği ortamlardan biri haline gelmiştir. Durum böyleyken, CMK 134. maddedeki özel arama ve el koyma rejiminin sadece bilgisayar ve bilgisayar programları ile bilgisayar kütükleri için geçerli olması, bu kapsamda yer almayan cep telefonlarına CMK'nın 116-129 maddeleri çerçevesinde niteliksiz suç eşyasıyla aynı muamelenin yapılmasına neden olmaktadır (Özocak 2011, 116).

Bu doğrultuda, CMK'nın "El koyma Kararını Verme Yetkisi" başlıklı 127. maddesi uyarınca, 134. maddesinde ki el koymanın sadece hakim kararı

[2] http://www.dijitaldeliller.com/cmk134.htm erişim tarihi: 04.03.2013

[3] http://www.dijitaldeliller.com/cmk134.htm erişim tarihi: 04.03.2013

ile yapılabilmesinin aksine, gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının, Cumhuriyet savcısına ulaşılamadığı hallerde ise kolluk amirinin yazılı emri ile kolluk görevlileri tarafından el koyma işlemi gerçekleştirebilmektedir.

Cep telefonlarının özel hayatın gizliliği kapsamında korunması gerekli olan birçok kişisel bilgiyi barındırmasına karşılık hâkim kararı olmaksızın el koyulabilmekte ve bilgisayarlara el konmasına ilişkin rejimi düzenleyen 134. maddenin sağlanan hukuki güvencelerden şüpheli yararlanamamaktadır. Bu bakımdan; temel hak ve özgürlükler bağlamında sorun yaratmakta, kişisel verilerin ve özel hayatın gizliliğine yapılan müdahaleyi evrensel hukukun çizdiği sınırların dışına çıkarmaktadır (Özocak 2011, 116).

134. madde metninde tahdidi olarak bilgisayar, bilgisayar kütükleri ve programlarında arama yapılabileceğinin belirtilmesi dar yorumlandığında cep telefonlarına bu maddede öngörülen arama rejiminin uygulanamayacağı sonucu çıkarılabilir. Fakat, kanımızca bilişim teknolojilerinin gelişimine bağlı olarak elektronik aygıt çeşitliliğindeki sürekli artışı göz önüne aldığımızda, cep telefonları dâhil üzerinde elektronik delil araması yapılabilecek her türlü elektronik aygıtın bilgisayar kavramı içinde değerlendirilebilmelidir. Örneğin, Birleşik Devletler Temyiz Mahkemesi (United States Court of Appeals*) U.S. k. Kramer* kararında[4] bilgisayar kavramının oldukça geniş tanımlandığı[5] görülmektedir. Birleşik Devletler Bilgisayar Dolandırıcılığı ve Kötüye Kullanma Yasası'nın[6] (e)(1) maddesine istinaden internete erişim sağlamayan sadece arama ve SMS gönderme fonksiyonuna sahip bir cep telefonunu[7] dahi bilgisayar kavramı içinde değerlendirmiştir.

Bu bakımdan, bilişim sistemleri üzerinde gerçekleştirilecek aramalara ilişkin hükümlerin hem hukuki ve hem teknik perspektifinin birbirini tamamlayıcı nitelikte olması gerekliliği önem kazanmaktadır. CMK 134. madde hukuk sistematiği açısından temel hak ve özgürlükleri önceleyen yapısı itibariyle olumlu özellik arz etmektedir. Öte yandan bir takım teknik imkânsızlıklar nedeniyle birçok hükmünün uygulama alanı bulmamasının amaçlanan yararın aksine sonuçlara yol açabildiği görülmektedir.

---

[4] *U.S. v. Kramer*, 631 F.3d 900 (Şub 8, 2011)

[5] Bilgisayar kavramı mantıksal, aritmetik veya depolama fonksiyonlarına sahip elektronik, manyetik, elektrokimyasal yahut yüksek hızda veri işleme kapasitesine sahip cihazlar ile veri depolama ya da iletişim olanağı sunan cihazlar veya bu tür cihazlarla birlikte çalışan cihazları kapsayacak şekilde, el ile çalışan hesap makinesi, daktilo gibi cihazlar hariç tutularak tanımlanmıştır. *Bkz. 18 U.S.C. § 1030(e)(1)*

[6] http://energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf

[7] *Motorola Motorazr V3*

REKABET KURUMU

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