Balcıoğlu Selçuk
Ardıyok Keki

Baseak CORE Papers No: 2

Citation: ARDIYOK Ş., AYTEKİN B., YÜKSEL B., DEMİRKAN H. (2020), Dünyada ve Türkiye'de Rekabet Hukukunda Dijital Delillerin Kullanılması Süreci ve Türkiye Bakımından Değerlendirmeler, Baseak CORE Papers No: 2, 2020

Dünyada ve Türkiye'de Rekabet Hukukunda Dijital Delillerin Kullanılması Süreci ve Türkiye Bakımından Değerlendirmeler

Şahin ARDIYOK, Burak AYTEKİN, Barış YÜKSEL, Hakan DEMİRKAN

***ÖZET**

Teknoloji alanında yaşanan hızlı gelişmeler toplumsal yaşamı direkt olarak etkilemektedir. Bu değişimin bir yansıması da halihazırda iş hayatında çalışanların kendi aralarındaki iletişimi neredeyse tamamen dijital ortamlar üzerinden gerçekleştirmesidir. Rekabet otoriteleri başta kartel olmak üzere diğer rekabet ihlallerine yönelik yoğun bir mücadele ortaya koymaktadır. Söz konusu mücadelenin en önemli ayaklarından birisi de teşebbüslerin iş yerlerinde gerçekleştirilen yerinde incelemelerdir. Mevcut durumda çalışanlar arası iletişimin büyük bir kısmının dijital ortamlar üzerinden gerçekleştirilmesi, rekabet hukukunda dijital delillerin kullanılmasının önemini arttırmıştır. Bu noktada fiziksel delillerden birçok farklı özelliğe sahip olan dijital delillerin kullanımının hukuki bir zemine oturtulması ihtiyacı ortaya çıkmıştır. Bu çalışmada ilk olarak rekabet hukukunda gözlenen fiziksel delillerden dijital delillere doğru olan geçiş süreci ele alınacaktır. Ardından rekabet hukukunda dijital delilin önemi tartışılacak bu kapsamda dijital delillerin geleneksel delillerle olan farklılıkları ortaya konulacaktır. Bu bölümde ayrıca uluslararası uygulamadan örneklere de yer verilecektir. Çalışmanın son bölümünde ise Türk rekabet hukukunda dijital delil konusu ilgili mevzuat çerçevesinde incelenecektir. Bu kapsamda dijital delil kullanılmasında dikkat edilmesi gereken hususlara dair değerlendirmeler sunulacaktır.

Anahtar kelimeler: Rekabet hukuku, rekabete aykırı anlaşmalar, hâkim durumun kötüye kullanılması, adli bilişim, dijital verilerin kopyalanması ve incelenmesi, özel hayatın gizliliği, kişisel verilerin korunması

JEL Kodları: K21, K24, K40

ABSTRACT

This paper aims at revealing elements of how digital data is handled by competition authorities around different jurisdictions. This paper evaluates the collection and evaluation of digital data in the Act on the Protection of Competition No: 4054. The primary conclusion of the paper suggests that the current competition law procedures are evolving along with technology but still needs clarification about how to handle personal and privileged data. It is evaluated that case handlers of the Turkish Competition Authority ("**TCA**") and competition law practitioners have similar approach with the practitioners in European Union but collection and examination of personal devices and personal data is a topic that is still much debated.

Keywords: Competition law, anti-competitive agreements, abuse of dominance, digital forensics, forensic imaging, right to privacy, data protection

JEL Codes: K21, K24, K40

* Balcıoğlu Selçuk Ardıyok Keki Avukatlık Ortaklığı, sardiyok@baseak.com, bayatekin@baseak.com

I. Giriş

Gelişen teknolojik gelişmeler ürün ve hizmetlerin sunuş yöntemini değiştirmekte, söz konusu değişim de toplumsal yaşama direkt olarak etki etmektedir. Bu kapsamda gün geçtikçe geleneksel iş ve işleyişler, alışılmış formlarının dışına çıkmakta, buna bağlı olarak söz konusu durumun hukuki bir zemine oturtulması ihtiyacı doğmaktadır. Bahsi geçen teknolojik gelişimin bir yansıması da günümüzde insanların neredeyse tamamen dijital ortamlar üzerinden iletişim kurmasıdır. Bu noktada özellikle iş yaşamında çalışanlar arasında gerçekleşen iletişim neredeyse sadece dijital ortamlarda gerçekleşmekte ve bunun kaydı da yalnızca bilgisayar, cep telefonu ve tablet gibi elektronik cihazlarda tutulmaktadır.

Bilindiği üzere, rekabet otoriteleri kartel başta olmak üzere diğer ihlallere yönelik olarak serbest piyasa ekonomisinin dinamiklerini sağlamak adına ciddi şekilde mücadele etmektedir. Söz konusu mücadele kapsamında rekabet otoriteleri tarafından teşebbüslerin işyerlerinde ve teşebbüslere ait taşınmazlarda gerçekleştirilen yerinde incelemeler büyük önem arz etmektedir. Rekabet otoritelerin teşebbüslere yönelik olarak kullandıkları bu yetkinin en etkin bir biçimde kullanılması rekabet ihlalleri ile mücadele etmek açısından elzemdir.

Günümüzde iletişimin çoğunlukla dijital ortamlarda gerçekleşmesi, rekabet hukuku bakımından dijital delillerin önemini arttırmıştır. Bu noktada her geçen gün geleneksel iş ve işleyişlerin değişmesi ve dijital gerçeklikte yerini alması, bunlara ilişkin hukuki anlaşmazlıkların, haksız fiillerin ve suçların sübuta erdirilmesinde daha çok başvurulmaya başlanılan elektronik delillere ilişkin uyarlamaların yapılması ihtiyacı ortaya çıkmaktadır. Bu nedenle, elektronik delillerin elde edilmesinden, Rekabet Kurulu'na sunulmasına kadar geçen süreçte başvurulan birtakım yerleşik uygulamaların, elektronik delillerin elde edilmesi sürecinde işlevsel kılınan genel kabul görmüş standartlar çerçevesinde değerlendirilmesi gerekmektedir. Nitekim delillerin gerçeğe uygunluğunun, delillerin ve delil zincirinin bütünlüğü koşulları sağlanarak elektronik delillerin kabul edilebilirliğine ilişkin şartların yerine getirilmesi, delil hukuku bakımından önem arz etmektedir[1].

Elektronik delil kavramı ve bunun rekabet hukukuna etkilerini konu edinen bu çalışmamızda ilk olarak dijital delillerin rekabet hukukundaki kullanım biçimleri ele alınacak ve bunların temel hak ve özgürlüklerle ilişkisi ortaya konulacaktır. Takip eden bölümde ise Türkiye'deki mevcut durum ele alınarak Türkiye'ye yönelik önerilerimiz sıralanacaktır.

I.1. Rekabet Hukukunda Dijital Delil

I.1.1. Dijital delil toplamanın geleneksel yöntemlere göre avantajları

Rekabeti engelleyici eylemlerde bulunanların, rekabet ihlallerinin niteliği gereği söz konusu eylemlerinin bilinmemesi için büyük çaba gösterdikleri söylenebilir. Bu nedenle rekabet otoritelerince gerçekleştirilen yerinde incelemeler söz konusu ihlallere ilişkin delillerin ortaya çıkarılmasının yegâne yolu olarak karşımıza çıkmaktadır. Bu kapsamda dünya genelinde birçok rekabet otoritesinin teşebbüslerin işyerlerinde rekabet ihlali olup olmadığının tespit edilmesi için yerinde inceleme gerçekleştirme yetkisine sahip oldukları göze çarpmaktadır. Rekabet otoritelerinin bu denli güçlü bir yetkiye sahip olmaları, ihlal içerisinde olan teşebbüslerin söz konusu ihlalin varlığını gösteren delilleri ortadan kaldırma şeklinde davranışlar içerisinde bulunmalarına da neden olabilmektedir[2].

Yukarıda ifade edildiği üzere elektronik ortamda iletişimin daha hızlı ve kolay olması, teşebbüslerin ticari faaliyetlerine yönelik iletişimlerini dijital ortamda gerçekleştirmelerine sebep olmaktadır. Bu yönüyle iddia konusu bir rekabet ihlali bakımından delil değeri taşıyan çoğu bilgi ve belge, elektronik ortam haricinde var olmamaktadır. Teşebbüslerin 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[3].

Bu çerçevede rekabet otoritelerinin yerinde inceleme esnasında odaklarını dijital delillere çevirmesi pek çok avantajı

[1] Yalçınkaya M. (2015), "Rekabet Hukuku Uygulamaları Kapsamında Elektronik Delil", Rekabet Kurumu Uzmanlık Tezleri Serisi No:142, s.2.

[2] OECD (2013), "Session III: Unannounced Inspections in Antitrust Investigations", s.6.

[3] Yalçınkaya (2015), s.12.

beraberinde getirmektedir. İlk olarak yukarıda da ifade ettiğimiz üzere hâlihazırda teşebbüsler ticari faaliyetlerine ilişkin iletişimlerini dijital ortam üzerinden gerçekleştirmeyi tercih etmektedirler. Bu yönüyle dijital deliller fiziksel delillerde hiç bulunmayan birtakım bilgiler içerebilmektedirler. Zira teşebbüsler ticari faaliyetlerine ilişkin ticari bilgi veya iletişimlerini saklama noktasında dijital ortamı tercih etmektedirler. Sonuç olarak dijital delillerin toplanması geleneksel yollardan delil toplanmasına kıyasla rekabet ihlalleri ile mücadele konusunda daha etkin bir çözüm sağlamaktadır.

Diğer yandan fiziksel delillerin yerinde inceleme sırasında veya öncesinde teşebbüsler tarafından imha edilmesi ihtimal dahilindedir. Bu çerçevede teşebbüsün ihlal içerisinde bulunduğunu gösteren bir fiziksel delilin yok edilmesi ve başkaca da bir delilin olmaması durumunda, teşebbüse karşı bir soruşturma başlatılmasının önüne geçilebilmektedir.

Oysa dijital deliller bakımından adli bilişim teknolojileri sayesinde, yerinde incelemelerde önceden silinen bazı dijital dokümanların yerinde incelemeyi gerçekleştiren raportörler tarafından ortaya çıkarılabilmesi mümkün olmaktadır. Diğer bir ifade ile dijital deliller kolaylıkla ortadan kaldırılamamaktadır. Bu noktada örneğin bilgisayarda bulunan bir elektronik verinin basit bir işlem ile silinmesi durumunda söz konusu veri tamamen ortadan kaldırılmış olmamakta, silinen elektronik verinin hard disk üzerinde kapladığı yer boşluk olarak işaretlenerek sonradan veri yazmaya uygun hale getirilmektedir. Bilgisayar tarafından silinmiş olarak işaretlenen bölüm üzerine başka yeni veri yazılmadığı müddetçe silinen verinin geri getirilmesi mümkün olmaktadır. Öte yandan, bir elektronik veri silindikten sonra arşiv ünitelerinde belirli bir süre için muhafaza edilebilmektedir. Bu sebeple kullanıcı tarafından bir elektronik delil silinmiş sanılsa da, uzmanlar tarafından uygulanabilecek veri kurtarma uygulamaları ile elektronik veriye ulaşılması söz konusu olabilmektedir[4].

Ayrıca, delillerin ortadan kaldırılması amacı ile hareket eden bir kimsenin söz konusu dijital delilin ortadan kaldırıldığından emin olması son derece zordur. Nitekim elektronik cihazlarda örneğin bilgisayarda silme de dahil tüm işlemler için ilgili sistem tarafından kayıtlar tutulmaktadır. Bu çerçevede bir bilgisayarda yapılan kaydetme veya silme gibi işlemlerin kapsamı, ne zaman yapıldığı vb. bilgilere bu sistemler üzerinden kolaylıkla ulaşılabilmektedir. Adli bilişim konusunda uzman olan bir kimse, bilgisayar üzerinde yapılan bu tür işlemleri kolaylıkla tespit edebilecektir[5]. Dolayısıyla kartele taraf olan teşebbüslerin aleyhe dijital delilleri ortadan kaldırması, fiziksel delillere kıyasla daha zordur.

Dijital delillerle geleneksel delillerin ayrıştığı bir diğer nokta ise söz konusu delillerin barındırdıkları içeriğe ilişkin olarak karşımıza çıkmaktadır. Buna göre her ne kadar fiziksel deliller önemli birtakım bilgileri ihtiva edebilseler de, dijital deliller çok daha fazla bilgi içerme kapasitesine sahiptir. Bu çerçevede geleneksel delillerde içerik o dokümanda bulunan bilgiler ile sınırlı iken, dijital deliller bünyesinde birtakım ilave bilgileri de ihtiva etmektedir. Bu kapsamda dijital delillerde yer alan metadata[6], ilgili doküman hakkında, oluşturulma tarihi, gönderici ve alıcının kimlik bilgileri, silinme tarihi ve belge üzerinde yapılan değişiklikler gibi kapsamlı bilgileri bünyesinde barındırmaktadır. Bu sebepten ötürü dijital dokümanlar, fiziksel dokümanlara kıyasla daha fazla bilgi taşıyabilmektedir. Son olarak, çok fazla miktarda dijital verinin incelenmesi gerektiği durumlarda, ilgili dokümanların tespitini ve incelemesini kolaylaştıran arama araçlarının varlığı rekabet otoritelerine büyük kolaylık sağlamaktadır. Dolayısıyla dijital deliller rekabet hukuku bakımından bir ihlalin olup olmadığı noktasında daha kesin sonuçlara ulaşılmasını sağlamaktadır[7].

I.1.2. Dijital Delil Toplamanın Dezavantajları

Dijital delillerin yukarıda sayılan avantajlarının yanı sıra birtakım dezavantajlarının da bulunduğunu ifade etmek gerekmektedir. Bu kapsamda dijital delillerin dezavantajı olarak sayılabilecek bir durum, özellikle blok halinde bulunan veriler bakımından gizli, şahsi ya da hukuki olarak ayrıcalıklı (ör: avukat ile müvekkil arasındaki yazışmalar) dokümanlar ile yürütülen inceleme ile ilişkili dokümanların herhangi inceleme yapmaksızın ayrıştırılmasının zorluğudur. Buna bağlı olarak, rekabet otoriteleri her türlü veriyi içinde barındıran elektronik cihazları incelediklerinde,

[4] 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, s.186.

[5] Zirve S. Ö.&Yıldız S. (2013), "Canlı Adli Bilişimin İhtiyaç ve Risk Bakımından Değerlendirilmesi", I. International Symposium on Digital Forensics and Security Proceeding Book, s.366.

[6] Metadata, bir veri hakkındaki verilerdir. Belirli bir veri setine ya da kaynak hakkında nasıl, ne zaman ve kim tarafından oluşturulduğu hakkında tanımlayıcı bilgiler içerir.

[7] ICN (2010), "Chapter on Digital Evidence Gathering", Cartel Enforcement Subgroup 2- ICN Cartels Working Group.

kaçınılmaz olarak gizli, şahsi ya da hukuki olarak ayrıcalıklı dokümanlar da dahil olmak üzere her türlü dokümana erişmektedir.

Bu durum ise, gerek Avrupa İnsan Hakları Sözleşmesinin (AİHS) 8. maddesi, gerekse pek çok ülkenin ulusal hukuku çerçevesinde temel hak ve özgürlükler arasında sayılan gizlilik hakkının orantısız olarak kısıtlanması sorununu beraberinde getirmektedir. Bu noktada şu hususun altını çizmek gerekir ki, rekabet hukukunun süjesinin teşebbüsler olması ve bu teşebbüslerin çok büyük çoğunlukla tüzel kişiliği haiz olması, gizlilik hakkının orantısız olarak kısıtlanmasından kaynaklanabilecek sorunları ortadan kaldırmamaktadır. Nitekim Avrupa İnsan Hakları Mahkemesi'nin (AİHM) *Colas Est* kararında[8], tüzel kişilerin de 8. madde kapsamında gizlilik hakkına sahip olduğu ortaya koyulmuştur. AİHM, AİHS'nin 8. maddesi ile konuta yönelik öngörülen korumanın tüzel kişilerin işyerleri için de geçerli olacağını, şirketin gerçek kişi olmamasının bu hakkın varlığını etkilemeyeceğini ve şirketlerin de devletlerin keyfi uygulamalarına karşı korunacağını açık biçimde ifade etmiştir. Öte yandan, aşağıda daha detaylı olarak izah edileceği üzere, rekabet otoriteleri bazı durumlarda teşebbüs çalışanlarının gizlilik hakkını kısıtlayabilecek uygulamalarda da bulunmaktadır. Dolayısıyla, rekabet otoritelerinin dijital delil toplama ihtiyacı ile teşebbüslerin ve teşebbüs çalışanlarının temel hak ve özgürlükleri arasındaki dengenin nasıl sağlanacağı hususu kritiktir.

Bu dengenin sağlanması noktasında AİHS'nin 8. maddesinde[9], gizlilik hakkının hukuka uygun biçimde sınırlanması için aranan kanunilik ve orantılılık şartlarının yol gösterici olabileceği değerlendirilmektedir. Bu ilkelere uygun bir hukuki çerçevenin oluşturulması için, ilk olarak rekabet otoritelerinin teşebbüslere ait elektronik cihazların incelenmesi bakımından kanun ile açık biçimde yetkilendirilmesi gerekmektedir. Bunun yanı sıra, söz konusu elektronik cihazlar gizli ve hukuki olarak ayrıcalıklı bilgiler içerebileceğinden, rekabet otoritelerinin kanun ile kendilerine tanınan bu yetkiyi keyfi biçimde kullanmaları da engellenmelidir. Teşebbüs çalışanlarına ait elektronik cihazların incelenmesi noktasında ise, bunlarda yer alabilecek bilgilerin hassasiyeti ile orantılı olarak, daha kapsamlı ve katı kurallara ihtiyaç duyulacağı düşünülmektedir.

Dijital delillerin değiştirilmeye son derece elverişli yapıları da söz konusu delillerin dezavantajlı bir yönü olarak karşımıza çıkmaktadır. Nitekim fiziksel belgelerin iradi olarak yok edilmeleri haricinde ancak yangın, sel gibi istisnai durumlarda yok olmaları söz konusuyken, elektronik deliller bilişim sistemlerinin günlük işleyişi içinde, inceleme esnasında, manyetik ortam, yüksek sıcaklık gibi fiziksel koşullar nedeniyle değişikliğe uğrayabilir ya da yok olabilir. Örneğin ağ üzerinde çalıştırılan bir uygulama kullanıcının bilgisi haricinde ağ üzerindeki kayıtları değiştirebilir, hatta yok edebilir. Yine benzer şekilde bir bilgisayarın çalıştırılması ya da bir dosyanın açılması sabit disk üzerinde değişikliğe yol açabilir[10].

Son olarak dijital verilerin saptanmasının zor olması da bu başlık altında ele alınması gereken bir durumdur. Bilindiği üzere dijital veriler bir yerden bir yere kolaylıkla aktarılabilme özelliğine sahiptir. Bu çerçevede boyutları ne kadar büyük olsa da dijital veriler belirlenen bir yerde kolaylıkla muhafaza edilebilmektedir. Özellikle büyük şirketler, ticari faaliyetlerine ait elektronik verileri belirli bir yerde muhafaza edebilmek için bulundukları yerde veya farklı bir ülkede sunucular bulundurabilmektedirler. Bu sebeple, dijital verilerin hem sanal ortamda herhangi bir yerde saklanabilmeleri ve bu verilere zaman ve mekân kısıdı olmadan erişilebilmesi, hem de çok büyük boyutlarda verilerin basit bir elektronik cihazın içine sığdırılabilmesi nedeniyle elektronik verilere ulaşılmasının fiziki dokümanlara göre daha zor olduğu savunulabilir[11].

I.1.3. Dijital delil toplanması esnasında uyulması gereken temel ilkeler ve uluslararası uygulamadan örnekler

Elektronik delillerin, delil niteliğini kaybetmeden, karar mercileri tarafından kabul edilebilirlik niteliğini haiz olarak dış dünyaya aktarılmaları açısından birtakım bilimsel

[8] Başvuru no: 37971/97, Societe Colas Est ve diğerleri Fransa'ya karşı, 16.4.2002.

[9] AİHS madde 8: (1) Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.
(2) Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir.

[10] Zheng J., "Email Evidence Preservation How to Balance the Obligation and the High Cost", Lex Electronica, Vol:14, s.4.

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

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[12].

Bilindiği üzere, dijital deliller değiştirilmeye son derece müsait bir yapıya sahiptir. Bu çerçevede elektronik deliller bilişim sistemlerinin günlük işleyişi içinde, inceleme esnasında, manyetik ortam, yüksek sıcaklık gibi fiziksel koşullar nedeniyle değişikliğe uğrayabilmektedir. Hemen ifade edilmelidir ki söz konusu değişikliklerin idari olarak yapılması ve yeni dijital belgeler yaratılması veya belgelerin değiştirilmesi de son derece kolaydır. Bu nedenle dijital delillere ilişkin bir diğer kritik husus delillerin gerçekliğinin araştırılmasıdır. Bu durum ise hukuki bir delil olarak kararlara dayanak yapılacak dijital delillerin mutlak suretle gerçekliğinin araştırılması ve tespit edilmesi (authentication) ihtiyacını doğurmaktadır.

Bu noktada, yukarıda değinildiği üzere dijital ortamda bulunan her türlü verinin ispat hukuku açısından delil niteliği taşıyacak şekilde elde edilmesi ve mahkemeye sunulmasına kadar geçen süreçler karşımıza adli bilişim kavramını çıkarmaktadır. Rekabet otoritelerinin tesis edecekleri kararlarda gerekçe olarak kullanacakları dijital deliller bakımından da adli bilişim alanında genel kabul gören bazı prensiplere uyulması faydalı olacaktır.

Ancak adli bilişim konusuna geçmeden önce dijital delil toplama sürecinde önem taşıyan bazı hususlara değinilmesi gerekir. Bilindiği üzere dijital delillerin toplanmasına yönelik getirilen başlıca iki eleştiri, söz konusu metodun temel hak ve özgürlükleri olması gerekenden fazla kısıtladığı ve dijital delillerin değiştirilmeye müsait olduğuna ilişkindir.

Öncelikle dijital delillerin gerçekliğine ve dijital delillerin toplanması esnasında temel hak ve özgürlüklerin orantısız olarak kısıtlanmasına ilişkin endişelerin giderilmesi için, bu hususlara dair kapsamlı ve şeffaf usul kurallarının geliştirilmesi gerekmektedir. Bu kurallar çerçevesinde dijital delillerin toplanması, saklanması, delil ve gözetim zincirlerinin (chain of evidence ve chain of custody) sağlanması, delillerin gerçekliğinin teyidi ve delil üzerinde yapılan her türlü işlemin kaydının tutulması gibi hususlar bakımından nasıl bir usul izleneceği açık bir biçimde tespit edilmelidir. Günümüzde, özellikle Avrupa Birliği ve Uluslararası Rekabet Otoriteleri Birliği (ICN) bünyesinde tüm bu hususlara ilişkin en iyi uygulama örneklerinin geliştiği görülmektedir[13].

Dijital delillerin hukuka uygun olarak toplanması bakımından temel kural, rekabet otoritelerinin dijital delil toplayabilme hususunda kanun ile açıkça yetkilendirilmiş olmasıdır. Ancak ifade edilmelidir ki bu yetkilendirme tek başına yeterli değildir. Bu yönde bir yetkilendirmenin yanı sıra, dijital delillerin toplanmasına ilişkin yetkinin keyfi ve temel hak ve özgürlükleri orantısız biçimde sınırlayacak şekilde kullanılmasını engellemeye yönelik bazı ilave tedbirlere de ihtiyaç duyulmaktadır. Özellikle rekabet otoritelerinin müdahale yetkisi arttıkça, keyfi uygulamaları engellemeye yönelik ilave tedbirler daha da önemli bir hale gelecektir. Çalışanların özel hayatına yönelik ciddi bir müdahalenin keyfi bir biçimde uygulanması hukuki açıdan büyük sorunlar doğuracaktır.

Mevcut durumda delil zincirinin sağlanmasına ve otoritelerin dijital belgelerin gerçekliğini kesin olarak güvence altına almasına özel bir önem atfedildiği görülmektedir. 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[14]. Rekabet otoritelerinin, dijital delillerin gerçekliğini teyit etmek için ise farklı uygulamalara başvurduğu görülmektedir. Bu açıdan en sağlıklı ve ağırlıklı olarak kullanılan yöntem; dijital delillerin toplanması veya bilgisayarlara veya benzer amaçla kullanılan cihazlara ait disklerin imajlarının alınması[15] (ilgili rekabet otoritesinin imaj alma bakımından yetkili olduğu varsayımı altında) aşamasında yazma koruma araçlarının[16] kullanılması ve

[12] Yalçınkaya (2015), s.15.

[13] Örneğin bknz. ICN (2010)

[14] Casey E. (2011), "Digital Evidence and Computer Crime Forensic Science, Computers and the Internet", s.20.

[15] Adli imaj (forensic image), veri taşıyıcılarının (CD, USB, sabit disk vs.), içinde bulunan tahsis edilmemiş ve kullanılmayan alanlar da dahil olmak üzere, her bir bit bazında aynı olan dijital kopyasını ifade etmektedir.

[16] Yazma koruma aracı (write blocker), sabit diskte yer alan dijital verilerin toplanması esnasında bunların içeriği üzerinde bir değişiklik yapılmasını engellemek için kullanılmaktadır.

tüm dijital belgelerin hash değerinin[17] alınmasıdır. Hash değerinin kıyaslanması veya kriptografik özet olarak da nitelendirilen bu yöntemde 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 kullanılmakta ve delillerin gerçek olup olmadığı tespit edilmektedir.

Bilindiği üzere rekabet otoritelerinin yalnızca dijital belgelerin fiziksel kopyalarını aldığı durumlarda, şirketi temsil ile yetkili kişilerden kurum uzmanları tarafından alınan fiziksel kopyaların belgelerin dijital ortamdaki orijinalleri ile aynı olduğuna dair bir beyan alınması yeterli olabilmektedir. Ancak özellikle incelenen verilerin boyutunun çok fazla olduğu ve tüm ilgili belgelerin fiziksel kopyasını almanın mümkün veya makul olmadığı durumlarda, adli bilişim araçlarından faydalanılması ve ilgili belgelerin dijital kopyalarının alınması gerekli olabilmektedir. Bunun yanı sıra, deliller toplandıktan sonra da, bunların fiziksel olarak nerede bulunduğunu sürekli olarak ortaya koyan bir kayıt tutulmalıdır.

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[18]. Bu durum ise karşımıza adli bilişim kavramını getirmektedir. Halihazırda rekabet otoritelerinin dijital delillerin toplanmasında kullanabileceği çeşitli adli bilişim araçları (yazılım ve donanım) araçları mevcuttur. Her ne kadar rekabet otoritelerinin amacına özel olarak geliştirilmiş bir yazılım bulmak zor olsa da, bu araçlar, disklerin imajının alınmasına ve her türlü elektronik cihazın (bilgisayar, mobil telefon, tablet bilgisayar vs.) incelenmesine olanak sağlamakta ve silinmiş olanlar da dahil (teknik olarak geri getirilmesi mümkün olduğu seviyede) tüm verilerin araştırılmasını mümkün kılmaktadır.

Özellikle bilgisayarların ve sunucuların incelenmesinde kullanılan çeşitli adli bilişim araçları olduğu bilinmektedir. Rekabet otoriteleri arasında en popüler adli bilişim araçlarından bir tanesi Nuix'tir[19]. Nuix, rekabet otoritelerinin çok geniş bir veri yelpazesine erişmesini sağlamaktadır. Öte yandan bu gibi adli bilişim araçlarından bazıları, "konsept" araması adı verilen bir yöntemi kullanmaktadır. Basit arama yöntemlerine göre çok daha gelişmiş olan konsept arama yönteminde, aranan anahtar kelimelerin eş anlamlıları, bunlara benzer diğer kelimeler ve hatalı yazımları da aramaya dahil edilmektedir. Ayrıca bu yöntem ile birbiri ile düzenli iletişim halinde olan, aralarındaki iletişimde aranan anahtar kelimelere ve bunun türevlerine sıkça rastlanan kişilerin otomatik olarak gruplanması mümkün olmakta ve bu kişiler arasında her türlü uygulama (örneğin Whatsapp veya Skype benzeri anlık mesajlaşma uygulamaları) üzerinden gerçekleştirilen iletişim incelenebilmektedir. Dolayısıyla bu tip araçlar, rekabet otoritelerinin incelemeleri ile ilişkili olabilecek dijital delillere ulaşmasını ciddi derecede kolaylaştırmaktadır. Adli bilişim araçlarının en önemli özelliklerinden bir tanesi de, bu araçların daima delil zincirini koruyacak biçimde çalışması ve elde edilen dijital dokümanların gerçekliğini teyit edebilmesidir. Mobil telefon ve tablet bilgisayar gibi farklı elektronik cihazların incelenmesinde de benzer araçlar kullanılmaktadır. Rekabet otoriteleri tarafından sıkça kullanılan Cellebrite[20] veya benzer özelliklere sahip olan DataPilot[21] bunlara örnek olarak gösterilebilir.

Her ne kadar rekabet otoritelerinin yerinde incelemeler sırasında adli bilişim araçları yardımıyla her türlü elektronik cihazı incelemesi ve her türlü dijital belgeye ulaşması teknik olarak mümkün hale gelmiş ise de, yukarıda izah edilen sebeplerden ötürü, söz konusu incelemelerin yürütülmesi bakımından nasıl bir hukuki çerçeve çizileceği de son derece önemlidir. Şu anda rekabet otoritelerinin yetkileri bakımından en çok tartışma yaratan konuların; teşebbüs çalışanlarına ait elektronik cihazların incelenip incelenemeyeceği, teşebbüse ait bilgisayar veya sunuculardaki disklerin imajının, daha sonra rekabet otoritesinin yerleşkesinde incelenmek üzere, alınıp alınamayacağı ve belli bir konuya yönelik inceleme yürütülürken farklı bir konuya ilişkin delillerin de toplanıp toplanamayacağı olduğu görülmektedir. Bu soruların cevaplanması bakımından en

[17] Hash değeri (hash value), bir dijital belge karşılığında oluşturulan matematiksel algoritmayı ifade etmektedir. Dijital belgeye ait hash değeri, söz konusu belgenin "parmak izi" olarak ifade edilebilir. Belgeye ait hash değerini değiştirmeden, belge üzerinde herhangi bir değişiklik yapılması kesinlikle mümkün değildir. Dolayısıyla orijinal belgenin hash değeri ile daha sonra kullanılan belgenin hash değeri aynı olduğu müddetçe, kullanılan belgenin orijinal belge ile birebir olduğu anlaşılmaktadır.

[18] Özocak G., "Ceza Muhakemesinde Elektronik Delillerin Tespiti ve Toplanması", İzmir 2. Uluslararası Bilişim Hukuku Kurultayı, 17-19 Kasım 2011 Bildiriler Kitabı, s.114.

[19] Detaylı bilgi için Bkz. http://www.nuix.com/

[20] Detaylı bilgi için Bkz. http://www.cellebrite.com/

[21] Detaylı bilgi için Bkz. https://datapilot.com/

kritik nokta, rekabet otoritelerinin dijital delil toplama ihtiyacı ile teşebbüslerin ve teşebbüs çalışanlarının temel hak ve özgürlükleri arasındaki dengenin nasıl korunacağıdır.

AİHM *Robathin* kararında[22] kolluk kuvvetlerinin, yürütülen bir soruşturma kapsamında bir avukata ait bilgisayarın sabit diskinin tamamının imajının alınmasını orantısız bir kısıtlama olarak değerlendirmiş ve bunun AİHS'nin 8. maddesine aykırı olduğuna hükmetmiştir. AİHM, avukata ait bilgisayarda, avukatlık mesleği gereği çok ciddi miktarda hukuki olarak ayrıcalıklı belge bulunacağına dikkat çekmiş ve Avusturya'nın iç hukukunda imaj alındıktan sonra bu tip belgelerin korunmasını sağlayacak yeterli düzenlemelerin var olmadığını vurgulamıştır. Bu karardan anlaşılacağı üzere, iç hukukta ilgililerin temel hak ve özgürlüklerini koruyacak ilave tedbirlerin bulunup bulunmaması da, rekabet otoritelerinin uygulamalarının hukuka uygun olup olmadığının tespiti bakımından son derece önemlidir. Örneğin, iç hukukta temel hak ve özgürlüklerin korunması için yeterli düzenlemelerin yapıldığı bir ülkede, rekabet otoritesinin teşebbüse ait bilgisayarların imajını alması ve bunu kendi yerleşkesinde incelemesi AİHS'ye uygun olarak nitelendirilebilecek iken, iç hukukunda yeterli koruma sağlanmayan bir ülkede aynı uygulamanın 8. maddeyi ihlal etmesi söz konusu olabilecektir.

Bu noktada, özellikle rekabet otoritesinin yerleşkesinde inceleme yapılmak üzere imaj alınması bakımından, AB Komisyonu tarafından geliştirilen "kapalı zarf (sealed envelope)" uygulamasına özel olarak dikkat çekmek gerekir. Kapalı zarf uygulaması çerçevesinde, teşebbüse ait bilgisayarın imajı Komisyon'a ait yerleşkede incelenmeden önce teşebbüsün temsilcileri davet edilmekte ve temsilcilere gizli veya hukuki olarak ayrıcalıklı belgeleri belirleme imkanı tanınmaktadır. Bu uygulama, imaj alınması yönteminin temel hak ve özgürlükleri orantısız biçimde kısıtlamasını engelleyecek ilave tedbirlere iyi bir örnek teşkil etmektedir.

AB Komisyonu, teşebbüs çalışanlarına ait cihazların incelenmesi bakımından benzer bir ilave tedbir benimsemiştir. Buna göre Komisyon uzmanlarının teşebbüs çalışanlarına ait cihazları inceleyebilmesi, ancak incelenen teşebbüsün "kendi cihazını getir (bring your own device)" politikasını benimsediğinin kesin olarak anlaşılması halinde mümkün olmaktadır. Kendi cihazını getir politikasını benimseyen teşebbüsler, çalışanlarının profesyonel amaçlarla kendilerine ait cihazları kullanmasını öngördüğünden, çalışanlara ait cihazlarda Komisyon tarafından yapılan inceleme ile ilişkili delil bulunma ihtimali ciddi derecede artmaktadır ve bu durum cihazların incelenmesini meşrulaştırmaktadır. Komisyon bunun yanı sıra, kendisine ait cihaz incelenen çalışanın incelemeyi takip etmesine ve gizli ya da hukuki olarak ayrıcalıklı bilgileri tespit etmesine de izin vermektedir.

Daha önce de bahsedildiği üzere, dijital belgelerin büyük çoğunlukla bir bütün olarak saklanması dolayısıyla, inceleme yapan raportörlerin yalnızca somut olayda inceledikleri konu ile doğrudan ilişkili belgeleri incelemesi genellikle mümkün olmamakta, uzmanlar ister istemez farklı belgelerin içerikleri hakkında da bilgi sahibi olmaktadır. Bazı durumlarda, uzmanların incelemenin kapsamı dışında kalan ancak farklı bir rekabet hukuku ihlaline işaret eden dijital belgelere rastlaması da söz konusu olabilmektedir. İşte böyle bir durumda, bu belgelere dayalı olarak incelemenin kapsamının genişletilmesinin ya da yeni bir inceleme başlatılmasının mümkün olup olmadığı son derece tartışmalıdır.

Bu tartışma bakımından Avrupa Birliği Adalet Divanı'nın (ABAD) *Deutsche Bahn*[23] *(DB)* ve *Nexans*[24] kararları son derece önemlidir.

ABAD, *DB* kararında, DB'nin hakim durumunu kötüye kullandığı iddiası ile yürütülen bir soruşturma kapsamında teşebbüsün merkezinde yerinde inceleme yürüten Komisyon uzmanlarının, DB'nin yine rekabet hukuku ihlali teşkil edebilecek farklı davranışlarına ilişkin deliller elde etmesinin ve buna dayalı olarak soruşturmanın kapsamını genişletmesinin hukuka uygun olup olmadığını incelemiştir. ABAD, somut olayda delillerin hukuka aykırı olarak elde edildiğine hükmetmiştir. Ancak yine aynı kararda, ABAD yerinde inceleme yapan uzmanların farklı ihlallere ilişkin belgelere "rastlamasının" kural olarak ihlal teşkil etmeyeceğinin, ancak somut olayda uzmanların bilinçli olarak bu belgeleri aradığına dair kuvvetli emarelerin bulunduğunun ve hukuka aykırılığın bundan kaynaklandığının altını çizmiştir.

Nexans kararında ise; Komisyon uzmanları incelemelerine Komisyon'a ait yerleşkede devam etmek üzere teşebbüsün

[22] Başvuru no: 30457/06, Robathin Avusturya'ya karşı, 03.07.2012.

[23] Case C 583/13 P, Deutsche Bahn AG ve diğerleri Avrupa Komisyonu'na karşı.

[24] Case C-37/13 P, Nexans SA ve Nexans France SAS Avrupa Komisyonu'na karşı.

sunucusuna takılı diskin tamamının imajını almış ve daha sonra yapılan incelemelerde Nexans'ın başlangıçta soruşturma kapsamına dahil edilmeyen ürün pazarlarında da rekabeti kısıtlayıcı uygulamalarda bulunduğuna dair deliller elde etmesinin hukuka uygunluğu incelenmiştir. ABAD burada da Komisyon uzmanlarının yerinde inceleme kararının kapsamını aşmayacak şekilde inceleme yapması gerektiğini vurgulamış ve somut olayda delillerin hukuka aykırı olarak elde edildiğine hükmetmiştir. *Nexans* kararı, Komisyon'un geniş inceleme yetkileri karşısında teşebbüslerin temel hak ve özgürlüklerinin korunmasına yönelik denge mekanizmasının oluşturulması bakımından oldukça önemlidir.

Türkiye'deki mevcut duruma ilişkin açıklamalarımıza geçmeden önce, henüz çok fazla gündeme gelmeyen, ancak gelecekte ciddi sorunlara yol açabilecek son bir hususa da değinmekte fayda olacaktır. Teknolojinin gelişmesi ile teşebbüsler dijital verilerini kendi yerleşkelerinden ziyade veri depolama hizmeti sunan diğer teşebbüslerin yerleşkelerinde saklamaya başlamışlardır. Veri depolama hizmeti sunan teşebbüsler, hizmeti alan teşebbüsle aynı ülkede olabileceği gibi, başka ülkelerde de bulunabilmektedir. Özellikle bulut bilişim (cloud computing) hizmeti sunan büyük teşebbüsler, müşterilerinin verilerini genellikle yurt dışındaki sunucularda depolamaktadır.

Bu durum, rekabet otoritelerinin inceleme yetkileri bakımından çok ciddi sorunlara yol açabilir. Nitekim bazı ülkelerde rekabet otoritelerinin inceleme yetkisinin coğrafi kapsamı teşebbüsün yerleşkesi ile sınırlıdır. ICN bu tip yetkilendirme yaklaşımını "lokasyon yaklaşımı (location approach)" olarak adlandırmaktadır. Lokasyon yaklaşımının benimsendiği durumlarda yerinde incelemeyi gerçekleştirecek uzmanların, teşebbüs yerleşkesi dışında depolanan verileri incelemek için yeni bir yetkilendirmeye ihtiyacı olacaktır. Veri depolama hizmeti sunan teşebbüsün yurt dışında olması durumunda ise tek çözüm farklı ülke rekabet otoriteleri arasında işbirliği yapılması olacaktır ki bu şekilde bir uluslararası işbirliğinin hukuki altyapısını oluşturmak hiç kolay olmayacaktır. Diğer bazı ülkelerde ise, incelenen teşebbüsün "erişebildiği" her türlü verinin, yerinde incelemeyi yürüten uzmanlarca incelenebileceği öngörülmektedir. ICN bu tip yetkilendirme yaklaşımını ise "erişim yaklaşımı (access approach)" olarak adlandırmaktadır. Erişim yaklaşımının benimsendiği ülkelerde, teşebbüslerin depolanan veriye erişimi olduğu müddetçe, verilerin farklı bir yerde depolanması herhangi sorun teşkil etmeyecektir.

I.2. Türkiye'deki Mevcut Durum ve Öneriler

4054 sayılı Rekabetin Korunması Hakkında Kanun'da **("Rekabet Kanunu")** rekabet ihlalleri bakımından delil kavramı ile ilgili bazı düzenlemeler bulunmaktadır. Bu kapsamda Rekabet Kanunu'nun "Önaraştırma" başlıklı maddesi *"Önaraştırma yapmakla görevlendirilen raportör 30 gün içinde elde ettiği bilgileri, her türlü delilleri ve konu hakkındaki düşüncelerini Kurul'a yazılı olarak bildirir"* hükmünü içermektedir.

Kanun'un "Delillerin Toplanması ve Tarafların Bilgilendirilmesi" başlıklı 44. maddesi ise Soruşturma safhasında, Rekabet Kanunu'nu ihlal ettiği iddia edilen kişi veya kişilerin, kararı etkileyecek her türlü bilgi ve delili Kurul'a sunabilecekleri ifade edilmiştir.

Yine aynı Kanun'un "İspat Yükü" başlıklı 59. maddesi şu şekildedir:

> *"Zarar görenlerin bir anlaşmanın varlığı ya da piyasada rekabetin bozulduğu izlenimini veren, özellikle piyasaların fiilen paylaşılması, uzun sayılacak bir süre piyasa fiyatında gözlenen kararlılık, fiyatın piyasada faaliyet gösteren teşebbüslerce birbirine yakın aralıklarla arttırıldığı gibi kanıtları yargı organlarına sunmaları halinde teşebbüslerin uyumlu eylem içerisinde bulunmadıklarını ispatlama yükü davalılara geçer.*
>
> *Rekabeti kısıtlayıcı anlaşma, karar ve uygulamaların varlığı her türlü delille ispatlanabilir."*

Rekabet Kanunu'nda yer alan düzenlemeler ışığında rekabet ihlallerinin her türlü delille ispatlanabileceğinin kabul edildiği göze çarpmaktadır. Bununla birlikte, nelerin delil niteliği taşıyacağı veya hangi konuların ne tür delillerle ispatlanabileceğine ilişkin özel bir hüküm bulunmamaktadır. Bu yönde bir düzenlemenin halihazırda olmaması nedeniyle, Rekabet Kanunu ile delil serbestisi ve delillerin serbestçe değerlendirilmesi ilkelerinin esas alındığı, bir vakıayı ispat edecek bütün delillerin ispat aracı olarak kullanılabileceği çıkarımında bulunmak mümkündür[25].

Halihazırda Rekabet Kurulu'nun, yerinde inceleme yetkisi ve bilgi isteme yetkileri kapsamında diğer ispat araçlarının

[25] Uyanık P. (2003), "Rekabet Hukuku Açısından Delil", Rekabet Kurumu Uzmanlık Tezleri Serisi, No:34, s.25.

yanı sıra elektronik delil de topladığı ifade edilmelidir. Dolayısıyla dünya genelinde teknolojik gelişmelere dayalı olarak dijital veri toplanmasının öneminin artması Türkiye'ye de yansımıştır. Buna bağlı olarak Haziran ayında Kanunun 15.maddesinde Kurumun incelediği ve topladığı dijital verilere doğrudan atıfta bulunulan bir değişiklik yapılmıştır ve ilgili maddenin (a) bendi takip eden şekilde güncellenmiştir: *"Defterlerini, fiziki ve elektronik ortam ile bilişim sistemlerinde tutulan her türlü verilerini ve belgelerini inceleyebilir, bunların kopyalarını ve fiziki örneklerini alabilir."*

Türk rekabet hukukunda, özellikle kartellerle mücadele noktasında dijital delillerin önemi giderek artmaktadır. Kurul'un yakın tarihli ihlal kararlarının büyük bir çoğunluğunda en önemli deliller rakipler arası iletişimi ortaya koyan dijital deliller olmuştur.

Diğer yandan yerinde incelemeler çerçevesinde dijital delil toplanması bakımından mevcut durumda sistematik bir uygulamanın olmadığını da vurgulamak gerekir. Bu durumun 8 Ekim'de yayınlanan, "Yerinde İncelemelerde Dijital Verilerin İncelenmesine İlişkin Kılavuz" (Kılavuz)[26] ışığında zamanla daha sistematik bir hale gelmesi beklenmektedir.

Kılavuza göre, Kurum bünyesindeki meslek personeli tarafından yürütülen yerinde incelemeler, teşebbüs yerleşkelerinde yapılabileceği gibi inceleme kapsamındaki verilerin çoğaltılması yoluyla teşebbüsün yerleşkesinin dışında Kurumun Ankara'daki adli bilişim laboratuvarında da gerçekleştirilebilecektir. Hali hazırda uygulanan, inceleme konusu açısından stratejik teşebbüs çalışanlarının belirlenmesi; bu kişilerin kullanımında olan bilgisayarlarda daha önceden belirlenmiş arama ibarelerinin dâhili arama imkânları ile aratılması ya da bilgisayar dosyaları arasında gezinilerek elektronik delillere ulaşmaya çalışılması devam etmektedir. Buna ek olarak, verilerin tutulduğu ortamların fiziksel ya da mantıksal imajının alınması de artık mümkündür. Bu durum, incelemelerde elektronik delillere ulaşılması bakımından adli bilişim araçlarının kullanımını da beraberinde getirmektedir.

Dolayısıyla AB Komisyonu ve bazı üye ülke otoritelerine benzer şekilde, Kurum'un raportörleri gerekli görmesi durumunda, incelemelerini kurum yerleşkesinde sürdürmek üzere teşebbüse ait dijital verileri adli bilişim yöntemleriyle kısmen veya tamamen ayrı veri depolayıcılarına kopyalayabilecektir.

Dijital belgelerin fiziksel kopyalarının alındığı durumlarda, söz konusu belgelerin gerçekliğinin teyit edilmesi için, teşebbüs yetkililerinden, yerinde inceleme sırasında alınan fiziksel belgelerin dijital belgeler ile aynı olduğuna dair yazı alınmaktadır. Dijital belgelerin doğrudan alındığı hallerde ise, veri taşıyıcılarının imajı alınarak hash değerleri hesaplanacak ve bu hash değerleri doğrulanacaktır. Şu an için Türkiye'de dijital delillerin gerçekliği bu yöntemlerle teyit edilmektedir.

Yayınlanan kılavuz ışığında Rekabet Kurumu'nun meslek personelinin yerinde incelemelerde yukarıda değinilen Nuix veya Cellebrite gibi harici adli bilişim araçlarından yararlanmasını, bunlara ek olarak teşebbüslerin benzer amaçlarla kullanılabilecek araçları da kullanmayı talep edeceğini söylemek mümkündür. Bununla birlikte, teşebbüslerin rekabet hukuku bilincinin hızla arttığı ve dolayısıyla dijital delillere ulaşmanın giderek zorlaştığı da bir gerçektir. Öte yandan teşebbüsler arası iletişimde bilgisayar dışındaki elektronik cihazların önemi de ciddi derecede artmıştır. Bu sebeplerden ötürü, Rekabet Kurumu'nun da yukarıda değindiğimiz daha gelişmiş adli bilişim araçlarından faydalanmanın yanı sıra mobil telefon veya tablet gibi diğer taşınabilir elektronik cihazları incelemek noktasında adımlar atacağı açıklanmıştır. Bu inceleme, gerekli görülmesi durumunda kişisel cihazları da kapsayabilecektir. Cihazın inceleme kapsamına alınmasındaki kıstaslar, cihazdaki veriler arasında teşebbüse ait bir bilgi olup olmadığı, cihazın teşebbüsün faaliyetleri doğrultusunda kullanılıp kullanılmadığı veya cihazın rekabet ihlaliyle ilişkili olup olmadığıdır. Dolayısıyla, cihazın çalışana veya teşebbüse ait olup olmaması, cihazın incelenmesi açısından önem teşkil etmemektedir. Kılavuzda, cihazların teşebbüse ait dijital veri içerip içermediğinin hızlı gözden geçirme işlemiyle tespit edileceği paylaşılmıştır.

Yayınlanan Kılavuzla Rekabet Kurumu'nun meslek personelinin yerinde incelemelerde inceleyebileceği elektronik cihazlara yönelik kanuni yetkileri daha net bir hale gelmiştir. Kanunda yapılan değişiklikten ve kılavuzun yayınlanmasından önce de Danıştay'ın Kurum raportörlerinin mevcut uygulamalarını hukuka uygun bulduğu pek çok karar

[26] Detaylı bilgi için Bkz. https://www.rekabet.gov.tr/Dosya/kilavuzlar/yerinde-inceleme-kilavuz1-20201009091644514-pdf

bulunmaktadır. Kanun da yapılan güncellemeler ve Kılavuz, Kurum personelinin yerinde incelemelerde sahip olduğu yetkilere dair hukuki zemini güçlendirmiştir. Bu noktada, Kurum'un dijital delilleri inceleme ihtiyacı ile teşebbüslerin temel hak ve özgürlükleri arasındaki dengenin ciddi derecede sarsıldığını söylemek ve Kurum uygulamalarının orantısız kısıtlamalara yol açtığını ileri sürmek zordur.

Diğer taraftan, özellikle Kılavuzda kişilere ait taşınabilir iletişim cihazlarının da inceleme kapsamına alınabileceğinin açıklanması sonrasında hem Türkiye Cumhuriyeti Anayasası hem de AİHS ile güvence altına alınan temel hak ve özgürlüklerin zedelenip zedelenmediği tartışılan bir konu haline gelmiştir.

Mevcut Kanun'un 15. maddesine, Kurum'un meslek personelinin "fiziki ve elektronik ortam ile bilişim sistemlerinde tutulan her türlü veri ve belgeleri" inceleme yetkisi olduğuna dair bir ekleme yapılmıştır. Bu ekleme ile raportörlerin dijital delil toplama yetkisi en nihayetinde açık bir kanuni dayanağa kavuşmuştur.

Bununla birlikte, ilgili Kanun hükmünün tüm yasal düzenlemeler gibi Anayasaya uygun olması gerektiği hususunda herhangi bir şüphe bulunmamaktadır. Bu kapsamda yukarıda da kısaca ifade ettiğimiz üzere Anayasanın 20. Maddesinde düzenlenen Özel Hayatın Gizliliği ile 22. Maddesinde düzenlenen Haberleşme Hürriyetinin ancak ve ancak Anayasada öngörülen şartlara uygun olarak kısıtlanabilmesi mümkündür[27]. Bu doğrultuda, Anayasanın 20. ve 22. maddelerinde bahse konu temel hak ve özgürlüklerin kısıtlanması bakımından tüm yasal düzenlemelerin iki şarta bağlı olduğu görülmektedir:

(i) Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak kısıtlama yapılabilir;

(ii) Ancak Kanun ile getirilebilecek olan kısıtlamanın usulüne göre verilmiş hakim kararı ile yapılması gerekmektedir. Gecikmesinde sakınca bulunan hallerde ise kanunla yetkili kılınmış merciin yazılı emri ile kısıtlamanın uygulanması mümkündür. Bu halde yetkili merciin kararı yirmidört saat içinde görevli hakimin onayına sunulur.

Gerçekten de Anayasanın 20 ve 22. maddelerinde güvence altına alınan temel hak ve özgürlüklerinin kısıtlanmasına yönelik birçok yasal düzenlemede anılan şartların gözetildiği görülmektedir. Örneğin, 5271 sayılı Ceza Muhakemesi Kanununun 134. maddesi kapsamında Cumhuriyet Savcısı tarafından verilecek dijital verilerin incelenmesi ve gerektiğinde bilgisayar kütüklerine el konulmasını da içeren "arama kararı"nın hakim onayına tabi olarak verilebileceği düzenlenmektedir. Aynı şekilde haberleşme hürriyetinin kısıtlanması sonucunu doğuracak olan iletişimin takibine ilişkin önleyici kolluk faaliyetleri bakımından düzenlenen 2559 sayılı Polis Vazife ve Selahiyet Kanununun Ek-7'nci maddesi ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanununun Ek-5'nci maddesi de ilgili kısıtlamalar bakımından "hakim kararı"nı gerekli kılmaktadır. Keza devletin güvenliği bakımından bile Milli İstihbarat Teşkilatı'nın yetkilerini düzenleyen 2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununun 6'ncı maddesinde aynı perspektifle düzenleme yapıldığı ve bahse konu kısıtlamalar bakımından yine "hakim kararı"nın arandığı görülmektedir.

Anayasanın açık hükmü ve düzenlemeleri kapsamında tüm kanunî düzenlemeler için zorunlu kılınan "hakim kararı"nın Rekabetin Korunması Hakkında Kanun'un 15. maddesi yönünden düzenlemeye konu edilmemesi isabetli bir yaklaşım olarak görülmemektedir.

Kanundaki değişiklik ve yayınlanan kılavuz ışığında, teşebbüse ait veri kayıt ortamlarının imajının alınmasına ve bunların Kurum yerleşkesinde incelenmesine olanak tanıyan bir ortam oluşmuştur. Öte yandan, bu yetkinin tanınması, özellikle gizli ve hukuki olarak ayrıcalıklı verilerin korunmasına yönelik ilave tedbirlerin de mutlaka alınmasını gerektirmektedir. Kurum bunu yerine getirmek için Komisyon'un "kapalı zarf" yaklaşımını benimsemiş ve durumu Kılavuzda açıklamıştır. Bu duruma ek olarak, incelemelerin teşebbüs sınırları dahilinde tamamlanmasının ön görüldüğü ve taşınabilir iletişim cihazlarında yapılacak incelemelerin teşebbüs sınırlarında tamamlanacağı ve ilgili

[27] Anayasa Mahkemesi'nin 17.09.2020 tarih ve 2016/13010 başvuru numaralı bireysel başvuru kararı Mahkeme'nin işçi-işveren ilişkisi kapsamında iş amaçlı e-posta yazışmalarının işveren tarafından denetlenmesinin Anayasaya uygunluğunu denetlediğini göstermektedir. Bu kapsamda, iş amaçlı da olsa işçi-işveren ilişkisinde dahi haberleşeme hürriyeti ile özel hayatın gizliliği korunmaktadır. İşyeri güvenliği ve düzeni ile iş amaçlı e-posta yazışmalarının incelenmesi arasındaki kuvvetli meşru menfaat ilişkisi karşısında dahi Anayasal hürriyetlerin kısıtlanmasını sınırlı ve dar tutulduğu görülmektedir. Bu yönüyle, kamu gücünü haiz idari otoritelerin yaptığı denetimlerde idari işlemlerin yasaya uygunluğu gereği Anayasada sayılı kısıtlama hallerinin dikkate alınması gerektiği kanaatindeyiz.

cihazlardan kopyalanan verilerin inceleme kapsamı dışında kalanlarının Kurum tarafından teşebbüs sınırları dışına çıkarılmayacağı belirtilmiştir. Bu, her ne kadar cihazdaki verilerin incelenmesini ölçülü bir hale getirse de, kişisel cihazlarda yapılacak hızlı gözdem geçirme işlemi ve bu cihazların incelenmesi sırasında denk gelinebilecek kişisel veriler olması, yukarıda da paylaştığımız özel hayatın gizliliği bakımından risk teşkil etmektedir.

Burada özel olarak teşebbüs verilerinin farklı bir teşebbüs yerleşkesinde depolanması sorununa da değinilecektir. Türkiye'de faaliyet gösteren pek çok teşebbüsün de yurt içi veya yurt dışında faaliyet gösteren teşebbüslerden veri depolama hizmeti aldığı bilinmektedir. Mevcut mevzuata bakıldığında, Rekabetin Korunması Hakkında Kanun'un 15. maddesinde *"Kurul, bu Kanunun kendisine verdiği görevleri yerine getirirken gerekli gördüğü hallerde, teşebbüs ve teşebbüs birliklerinde incelemelerde bulunabilir"* ibaresi yer almaktadır. Kurumun güncel yerinde incelemeleri ve bilgi talepleri doğrultusunda, şu anda ülkemizde erişim yaklaşımının benimsendiği söylenebilir. Bu yaklaşım, teşebbüslerin GDPR ve benzeri mevzuatlara uyum konusunda tereddüte düşmesine sebep olmaktadır.

Kanunda yapılan değişiklikler arasında ve yayınlanan Kılavuzda, alınan verilerin hash değerlerinin kontrol edilmesi dışında delil ve gözetim zincirine dair bir düzenleme olmaması da bir eksiklik olarak değerlendirilebilir Sonuç olarak kullanıcıların teknolojik gelişime paralel olarak dijital ortama olan artan eğilimi, rekabet hukuku bakımından dijital delil konusunun önemini arttırmıştır. Dijital delillerin kapsam ve nitelik olarak fiziksel delillerden ayrışması nedeniyle rekabet otoriteleri söz konusu delilleri değerlendirme noktasında çalışmalar yapmıştır. Bu kapsamda özellikle kartel gibi doğasında gizlilik unsurunu barındıran ihlaller bakımından dijital deliller hayati önem taşımaktadır ve kartelle mücadele çerçevesinde etkin bir çözüm sunmaktadır. Dijital delillerin söz konusu faydaları yanı sıra birtakım dezavantajlarından da bahsetmek gerekir. Bu bağlamda özellikle dijital delillerin temel hak ve özgürlüklerle ilişkisini dengeli tutacak bir hukuki zeminin kurulması büyük önem taşımaktadır. Ülkemiz açısından bir değerlendirme yapılacak olursa, rekabet hukukunda delil serbestisinin kabul edildiği ve dijital delillerin sıklıkla kullanıldığı ifade edilmelidir. Dolayısıyla ülkemizde dijital delil toplanmasına ilişkin usul ve esasların ortaya konması, ilgili süreçlerin yasal bir dayanağı olmasını sağlamıştır. Dijital delil toplama noktasında çağdaş uygulamalardan yararlanılması dijital delillerden beklenen maksimum faydanın sağlanmasına yardımcı olacak ve rekabet ihlallerinin önlenmesi noktasında büyük rol oynayacaktır.