T.C.
SAKARYA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

CEZA YARGILAMASINDA ELEKTRONİK DELİL

DOKTORA TEZİ

Yusuf BAŞLAR

Enstitü Anabilim Dalı: Siyaset Bilimi ve Kamu Yönetimi
Enstitü Bilim Dalı : Kamu Yönetimi

Tez Danışmanı: Prof. Dr. Halil KALABALIK

MAYIS-2015

T.C.

SAKARYA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

CEZA YARGILAMASINDA ELEKTRONİK DELİL

DOKTORA TEZİ

Yusuf BAŞLAR

Enstitü Anabilim Dalı: Siyaset Bilimi ve Kamu Yönetimi
Enstitü Bilim Dalı : Kamu Yönetimi

"Bu tez 26/05/2015 tarihinde aşağıdaki jüri tarafından Oybirliği / ~~Oyçokluğu~~ ile kabul edilmiştir."

JÜRİ ÜYESİ	KANAATİ	İMZA
Prof. Dr. Halil Kalabalık	Başarılı	
Doç. Dr. İsa DİNER	Başarılı	
Yrd. Doç. Dr. Meral EKİCİ SAHİN	Başarılı	
Yrd. Doç. Dr. Kökal SAHİN	Başarılı	
Yrd. Doç. Dr. Murat SERDEM	Başarılı	

BEYAN

Bu tezin yazılmasında bilimsel ahlak kurallarına uyulduğunu, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, tezin herhangi bir kısmının bu üniversite veya başka bir üniversitedeki başka bir tez çalışması olarak sunulmadığını beyan ederim.

Yusuf BAŞLAR

26.05.2015

ÖNSÖZ

Bu tezin yazılması aşamasında, çalışmamı sahiplenerek titizlikle takip eden danışmanım Prof. Dr. Halil Kalabalık'a değerli katkı ve emekleri için içten teşekkürlerimi ve saygılarımı sunarım. Yrd. Doç. Dr. Murat Erdem ve Yrd. Doç. Dr. Köksal Şahin bütün süreç boyunca her anlamda yanımda olmuş, desteklerini ve katkılarını esirgememişlerdir. Savurma sınavı sırasında jüri üyeleri Doç. Dr. İsa Döner ve Yrd. Doç. Dr. Meral Ekici Şahin de çalışmamın son haline gelmesine değerli katkılar yapmışlardır. Bu vesileyle tüm hocalarıma ve tezimin son okunmasında yardımlarını esirgemeyen meslektaşım Hasan Dursun'a teşekkürü borç bilirim. Son olarak bu günlere ulaşmamda emeklerini hiçbir zaman ödeyemeyeceğim anneme ve aileme şükranlarımı sunarım.

Yusuf BAŞLAR

26.05.2015

İÇİNDEKİLER

KISALTMALAR

AİHM : Avrupa İnsan Hakları Mahkemesi

AİHS : Avrupa İnsan Hakları Sözleşmesi

AKSSS : Avrupa Konseyi Siber Suç Sözleşmesi

AÜEHFD : Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi

Bkz : Bakınız

C : Cilt

CGK : Ceza Genel Kurulu

CHD : Ceza Hukuku Dergisi

CMA : Computer Misuse Act

CMK : Ceza Muhakemesi Kanunu

CMUK : Ceza Muhakemeleri Usulü Kanunu

FSEK : Fikir ve Sanat Eserleri Kanunu

MAR-HAD : Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi

PACE : Police and Criminal Evidence Act

PC : Personel Computer

PVSK : Polis Vazife ve Selahiyet Kanunu

RIPA : Regulation of Investigatory Powers Act

s : Sayfa

S : Sayı

TAAD : Türkiye Adalet Akademisi Dergisi

TBMM : Türkiye Büyük Millet Meclisi

TCK : Türk Ceza Kanunu

UYAP : Ulusal Yargı Ağı Projesi

ÖZET

SAÜ, Sosyal Bilimler Enstitüsü **Doktora Tez Özeti**

Tezin Başlığı: Ceza Yargılamasında Elektronik Delil

Tezin Yazarı: Yusuf BAŞLAR **Danışman :** Prof. Dr. Halil KALABALIK

Kabul Tarihi: 26 Mayıs 2015 **Sayfa Sayısı:** ix (ön kısım) + 313 (tez)

Anabilimdalı: Siyaset Bilimi ve Kamu Yönetimi **Bilimdalı:** Kamu Yönetimi

Ceza muhakemesi hukukunun amacı maddi gerçeği ortaya çıkartmaktır. Bu amaç ise soruşturma ve kovuşturma evrelerinde elde edilecek delillerle gerçekleştirilebilir. Delil serbestîsi ilkesi gereğince delil olma vasıflarını taşıyan ve özellikle hukuka uygun şekilde elde edilen her şey ceza yargılamasında delil olarak değerlendirilebilir. Bu bağlamda teknolojik ilerlemeye bağlı olarak son yıllarda ortaya çıkan ve gelecekte fiziksel deliller kadar baskın bir delil türü olacağından şüphe duyulmayan elektronik delilin de ceza yargılamasında kullanıldığı görülmektedir. Gerçekten de, belge delilleri arasında değerlendirilen elektronik delil, bilişim suçlarının yanı sıra birçok klasik suçun aydınlatılmasında önemli bir yere sahiptir. Bu bakımdan bu delil türünün ceza yargılamasındaki öneminin ortaya konması önem arz etmektedir.

Elektronik delil, yürütülmekte olan bir soruşturma veya kovuşturmaya esas olmak üzere bilişim sistemleri ve veri depolama aygıtlarından elde edilen delil türünü ifade etmektedir. Elektronik delilin geçerliliği hukuken bir delilde olması gereken özellikleri bulundurmasının yanı sıra teknolojik anlamda da bazı özelliklere sahip olmasına bağlıdır. Hukuken ve teknolojik bakımdan geçerliliği denetlenen bir elektronik delilin ceza yargılamasında kullanılmasında bir sakınca bulunmamaktadır.

Elektronik delilin hukuken geçerliliği her şeyden önce onun hukuka uygun biçimde elde edilmiş olmasına bağlıdır. Bu husus mukayeseli hukuk ve iç hukukumuz bakımından önemli bir konuma haizdir. Mukayeseli hukukta bazı ülkeler elektronik delilin elde edilmesi hususunda genel arama ve elkoyma tedbirlerini kullanmalarına karşın bazı ülkeler ise bilişim sistemlerinde yapılacak arama ve elkoyma tedbirlerini özel olarak düzenlemişlerdir. Ülkemizde ise bu husus Ceza Muhakemesi Kanunu'nun 134. maddesinde özel olarak düzenlenmiştir.

Elektronik delilin özellikle teknolojik anlamda denetimi ise onun adli bilişim kurallarına bağlı elde edilip edilmemesine bağlıdır. Adli bilişim, elektronik delile ilk temas edildiği andan itibaren onun toplanması, muhafazası, incelenmesi, analizi ve raporlanarak adli makamlara sunulması sürecinin bütününü ifade etmektedir. Adli bilişim, elektronik delilin yapısından kaynaklı bazı potansiyel sorunların yanı sıra adli bilişimin ilke ve standartlarının henüz belirlenmemesi, yeterli kaynak aktarımının sağlanmaması gibi bazı sorunları da barındırmaktadır. Bu durum, adli bilişim sürecinin etkin şekilde yürütülmesine ve dolayısıyla elektronik delilin geçerliliğine olumsuz biçimde tesir etmektedir. Bu tezde elektronik delilin ceza yargılamasındaki önemi, elektronik delilin elde edilmesinde adli bilişimin gerekliliği, mukayeseli hukuk ve Türk hukukunda elektronik delil elde etmek amacıyla bilişim sistemlerinde yapılacak arama ve elkoyma tedbirlerine ilişkin hukuki düzenlemeler incelenecektir.

Anahtar Kelimeler: Elektronik Delil, Dijital Delil, Adli Bilişim, Bilişim Sistemleri, Arama ve Elkoyma

SUMMARY

Sakarya University Institute of Social Sciences **Abstract PhD Thesis**

Title of the Thesis: Electronic Evidence in Criminal Proceedings	
Author	**:** Yusuf BAŞLAR **Supervisor:** Prof. Dr. Halil KALABALIK
Date	**:** 26 May 2015 **Nu. of pages:** ix (pre text) + 313 (main body)
Department : Political Science and Public Administration	**Subfield:** Public Administration

The aim of criminal procedure law is to reveal material facts. This objective can be accomplished by evidence obtained during the investigation and prosecution. In accordance with the principle of circumstantial evidence, everything that is especially obtained in compliance with the rule of law and has evidential value can be evaluated as evidence in criminal proceedings. In this context, it is observed that electronic evidence, which has emerged in recent years and is believed will be a strong evidence type like physical evidence in the future, is used in criminal proceedings depending on technological progress. Indeed, electronic evidence rated among document evidence has an important place in solving many classic crimes as well as cybercrimes. In this regard, it is important to present the significance of this type of evidence in criminal proceedings.

Electronic evidence is the type of evidence obtained from information systems and data storage devices based on a continuing investigation or prosecution. The validity of electronic evidence which meets the requirement of being legal evidence depends on a number of technological features. There are no drawbacks to electronic evidence which is legally and technologically validated in criminal proceedings.

The legal validity of electronic evidence first depends on whether it was obtained in accordance with the rule of law. This issue has an important position in terms of comparative law and domestic law. In comparative law, some countries apply the general search and seizure measures regarding the obtaining of electronic evidence whereas some countries have special measures regulated for carrying out the search and seizure in their information systems. In our country, on the other hand, those measures are stipulated specifically in the art. 134th of Criminal Procedure Code.

In particular, the technological audit of electronic evidence is connected to whether it is obtained based on computer forensic rules. Digital forensics represents the whole processes of collection, storage, inspection, analysis, and submission of a report to judicial authorities from the first contact with the electronic evidence. It also has some problems such as unsettled legal principles and standards of informatics and the failure to provide adequate resource allocation as well as some potential problems stem from the nature of the electronic evidence. These problems negatively affect the efficient execution of the forensic computing process and the validity of electronic evidence. This thesis has examined the importance of electronic evidence in criminal proceedings, informational legal requirements in obtaining electronic evidence, and legal regulations relating to search and seizure measures in information systems in order to obtain electronic evidence in comparative law and Turkish law.

Keywords: Electronic Evidence, Digital Evidence, Computer Forensic, Information Systems, Search and Seizure

GİRİŞ

Çalışmanın Konusu ve Önemi

Teknoloji ve bunun bir sonucu olarak yeni iletişim sistemlerinin gelişimi hayatın tüm aşamalarındaki bilgi ve ürün değişim sürecini etkilemiştir. Kişiler ve kurumlar arasındaki elektronik posta gönderiminin yıllık bazda trilyonlarla ifade edildiği, kişi ve kurumlarca oluşturulan belgelerin tamamına yakınının elektronik ortamda oluşturulduğu ve bunların ancak üçte birinden daha azının yazılı çıktısı alınarak fiziksel boyut kazandığı bir dijital çağda yaşamaktayız. Elektronik medya[*] ve sanal ortamın bu şekilde muazzam biçimde kullanıldığı bir hayatta kişiler ve kurumlar arasında ihtilaflar çıkması ve hatta suç teşkil edecek eylemlerin meydana gelmesi kaçınılmazdır.

Teknolojinin gelişmesi ve hayatın her alanında insanlarla bütünleşmesi, dolandırıcılık ve hırsızlık suçları başta olmak üzere birçok klasik suç tipinin yeni teknolojik gelişmelere göre yeniden tanımlanmasına ve bilişim suçları gibi yeni suç tiplerinin ortaya çıkmasına neden olmuştur. Bununla birlikte gerek yeni teknolojik ortama uyarlanan klasik suçların gerekse teknolojinin gelişmesine bağlı olarak hayatımıza giren bilişim suçlarının soruşturulmasında ve bu suçları işleyen kişi veya kişilerin tespitinde geleneksel fiziksel deliller yeterli gelmemektedir. Bu durum bu suç tiplerinin ortaya konması ve faillerinin cezalandırılması için elektronik delile müracaat etme zorunluluğunu ortaya çıkarmıştır.

Gerçekten de bilişim ve iletişim cihazları işlenen suçlarla ilgili olarak kimi zaman suçun işlenmesinde kullanılan bir nesne, kimi zaman ise -suçun işlenmesinde doğrudan doğruya etken olmamakla birlikte- suç delillerinin saklanıldığı bir ortam olarak karşımıza çıkmaktadır. Bu durumda elektronik delil söz konusu suçun ve bu suça ilişkin fail veya faillerin tespitinde çoğu zaman tek delil türü olarak karşımıza çıkmaktadır.

Tezin Amacı

Bu çalışma ile elektronik delil kavramı, elektronik delilin ceza yargılamasındaki önemi ve kullanılabilirliği, elektronik delilin araştırılma ve toplanma süreci incelenmek

[*] Elektronik medya; insanların elektronik olarak iletişim kurdukları farklı platformlara verilen addır.

suretiyle ülkemizde ve mukayeseli hukuktaki mevzuat ve uygulamada dikkat çeken sorunların tespit edilmesi ve özellikle iç hukukumuz bakımından bu sorunlara yönelik çözüm önerilerinin ortaya konulması amaçlanmaktadır.

Çalışma Yöntemi

Tez çalışmamızın yazımında öncelikle yerli ve yabancı kaynak araştırması yapılmış, ayrıca tez konusuyla ilgili içtihatlar ayrıntılı biçimde taranmış, sonrasında elde edilen yerli ve yabancı kaynaklar ile içtihatların değerlendirilmesi aşamasına geçilmiştir. Yapılan değerlendirilme sonucunda tez yazımına başlanmıştır.

Çalışmanın İçeriği

Suç, bir kimsenin, kanunda unsurları tanımlanan ve karşılığında ceza veya güvenlik tedbiri uygulanan hukuka aykırı eylemini ifade etmektedir. Suç ve suçlunun tespiti ile cezalandırılması ise ayrı bir yargılama faaliyetini gerekli kılmaktadır. Bir kimsenin suç işlediği şüphesi üzerine başlatılan ve bu şüphe giderilinceye kadar devam eden süreç ise ceza muhakemesi hukukunun faaliyet alanına girmektedir.

Ceza muhakemesi hukukunun amacı maddi gerçeğe ulaşmaktır. Bununla birlikte maddi gerçek her ne pahasına olursa olsun elde edilmesi gereken bir hedef değildir. Bu bakımdan, suç işleyen kişileri toplum adına cezalandırmakla görevli devlet, maddi gerçeğe ulaşmak için kat etmesi gereken yolda temel hak ve özgürlüklere saygılı ve hukuk devleti prensiplerine uygun davranmak zorundadır. Hukuk devleti olmanın gereği bir taraftan kişilerin özgürce yaşamalarını sağlamakken diğer taraftan da toplum nazarında adalet ve güveni tesis etmek için suç ve suçlularla mücadele etmektir. Bunu sağlayamayan bir devlet, hukuk devleti olma yolunda önemli bir mesafe alamamış demektir.

Bir taraftan kişilerin özgürce yaşamalarının sağlanmasına diğer taraftan da toplum nazarında adalet ve güvenin tesis edilmesine katkı sunmak amacıyla üzerinde çalışmaya karar verdiğimiz ceza yargılamasında elektronik delil isimli tezimiz dört bölümden oluşmaktadır. Tezimizin birinci bölümünde öncelikle ceza yargılamasında delilin ne anlama geldiği, delillerde bulunması gereken özelliklerin ve delillerin fonksiyonun neler olduğu, ceza yargılamasında kaç çeşit delilin varlığının kabul edildiği ve elektronik

delilin bu delil çeşitlerinden hangisi içerisinde değerlendirilmesi gerektiği hususları irdelenecektir.

Diğer taraftan birçok ülke hukukunda olduğu gibi ceza muhakemesi sistemimizde de delil serbestîsi ilkesinin kabul edildiği ve fakat gerek mukayeseli hukukta gerekse iç hukukumuzda delil serbestîsi ilkesinin mutlak olmadığı, bu anlamda delil serbestîsi ilkesinin hukuka uygun elde edilmiş delillerle sınırlandırıldığı bilinmektedir. Bu nedenle delil serbestîsi ilkesi ve hususiyle delil serbestîsi ilkesi içerisinde değerlendirilemeyecek hukuka aykırı deliller (delil yasakları) konusu da incelenecektir.

Modern hukuk sistemlerinde hukuka aykırı elde edilen delillerin yargılamada kullanılamayacağı hususunda genel bir kanaat birliği bulunmaktadır. Bununla birlikte bu uygulamanın istisnasız bir biçimde uygulanıp uygulanmayacağı hususunda farklı görüş ve yaklaşımlar bulunmaktadır. Bu bağlamda Türk hukuk sisteminde hukuka aykırı biçimde elde edilen delillerin yargılamaya esas alınmaması prensibinin mutlak olup olmadığı ya da her hukuka aykırılığın elde edilen delili yargılamada kullanılmayacak biçimde hukuka aykırı delil konumuna sokup sokmadığı hususu ile hukuka aykırı delilin uzak etkisi ve hukuka aykırı delillerin dosyadan çıkartılıp çıkartılmayacağı meselelerinin iç hukukumuz bakımından uygulamasının öğretideki farklı görüşler, Yargıtay ve Anayasa Mahkemesi'nin içtihatları ışığında açıklığa kavuşturulması, bundan sonra da elektronik delil konusunun incelenmeye başlanması gerekmektedir.

Bu bakımdan tezimizin birinci bölümünde ceza yargılaması anlamında her geçen gün önemini artıran ve baskın bir delil türü haline gelen elektronik delilin yakından ele alınması, öneminin vurgulanması, ne şekilde oluşturulduğu, hangi ortamlardan elde edilebileceği, hangi niteliklere sahip olması gerektiği, fiziksel delillerle arasında ne gibi farklılıkların bulunduğu, hangi hallerde geçerli delil olarak kabul edilebileceği, elektronik delille ilgili ortaya çıkan sorunların neler olduğu, hangi suç tiplerinin kanıtlanmasında kullanılabildikleri ve en önemlisi de ceza yargılaması açısından kabul edilebilir bir delil türü olup olmadığı hususları da ortaya konacaktır.

Gerçekten de, elektronik delilin hassas, kolay değiştirilebilir ve silinebilir yapısı, elde edilmesi veya korunması sırasında dahi bozulabilme özelliği ve hatta elde edilmesi için

kimi temel hak ve özgürlüklerin göz ardı edilmesi gerekliliği, elektronik delilin ceza yargılaması bakımından kabul edilebilir bir delil türü olup olmadığı, kabul edilebilir olduğunun benimsenmesi durumunda da tek başına, başka delillerle desteklenmediği müddetçe, kişilerin mahkûmiyeti için yeterli olup olmadığı hususlarının tartışılması zorunluluğunu doğurmaktadır. Nitekim mukayeseli hukukta ve iç hukukumuzda bu husus tartışma konusu edilmiş ve konuyla ilgili farklı görüşler ortaya konulmuştur.

Elektronik delilin ceza yargılamasında kabul edilip edilmeyeceği, kabul edilse de mahkûmiyet için tek başına yeterli olup olmayacağı hususlarında tartışmalar bulunmakla birlikte tartışma bulunmayan bir husus elektronik delilin kabul edilebilirliğinin benimsenmesi halinde de bu elektronik delilin her türlü şüpheden uzak, kesin ve inandırıcı bir delil türü olarak hükme esas alınabilmesi için hukuka uygun şekilde elde edilmesi ve yapısal olarak herhangi bir değişikliğe veya bozulmaya maruz kalmadığının incelenmesi zorunluluğudur. Bunun sağlanması ise elektronik delilin usule uygun arama ve elkoyma kararıyla elde edilmesi ve adli bilişim sürecinden geçerek hâkim huzuruna getirilmesine bağlıdır.

Ceza muhakemesi hukukunun en temel prensiplerinden birisi de maddi gerçeğin ortaya çıkartılmasıdır. Maddi gerçeğe ulaşarak adaleti sağlama ise özellikle soruşturma evresinde delillerin iyi bir şekilde elde edilmesine bağlıdır. Bunu sağlamak için de koruma tedbirlerine müracaat edilmektedir. Ancak, özellikle elektronik ortamda saklı bulunan delillerin hassas ve kırılgan yapıları ile çok kısa sürede karartılabilir olma özellikleri bu delillerin bütünlüğünün korunarak yargı makamlarının önüne getirilmesi imkânını sağlayacak koruma tedbirlerini gerekli kılmaktadır. Bunun sağlanamaması bilişim sistemleri aracılığı ile işlenen suçlar başta olmak üzere elektronik ortamda bulunması muhtemel delillerle aydınlatılacak suçların ve bu suçları işleyen kişilerin suçluluk hallerinin ispatlanamaması sonucunu doğurabilir.

Bununla birlikte, elektronik delilin elde edilmesi sırasında şüpheliye veya şüphelilere ait bilişim sistemleri üzerinde uygulanacak koruma tedbirlerinin kişilerin temel hak ve özgürlüklerine müdahale anlamını taşıdığı da bir gerçektir. Zira bu koruma tedbirleriyle kişilerin özel hayatlarına doğrudan müdahale edildiği gibi kişisel verilerinin de ortaya çıkmasına neden olunmaktadır. Bu bakımdan bir taraftan elektronik ortamda bulunan delillerin elde edilmesi ve bu delillerin karartılmasının engellenmesi amacıyla gerekli

koruma tedbirlerinin uygulanması diğer taraftan da bu koruma tedbirlerinin uygulanması sırasında temel hak ve özgürlüklerin ihlal edilmemesi amacıyla uluslararası hukukta ve iç hukukumuzda düzenlemeler yapılmak suretiyle söz konusu koruma tedbirlerinin belirli bir düzen ve disiplin içerisinde uygulanması amaçlanmıştır.

Bu bağlamda bilişim sistemlerinden elektronik delil elde etme amacıyla uygulanan koruma tedbirleri üzerinde durulması gerekmektedir. Bu hususta değinilmesi gereken en önemli koruma tedbirleri ise şüphesiz arama ve elkoyma koruma tedbirleridir. Bununla birlikte bazı hukuk sistemlerinde tartışma konusu olan uzaktan arama koruma tedbirlerine de değinmek gerekmektedir.

Bu kapsamda tez çalışmamızın ikinci bölümünde mukayeseli hukukta bilişim sistemlerinde yapılan arama ve elkoyma tedbiri üzerinde durulacaktır. Mukayeseli hukukta bilişim sistemlerinde bulunan elektronik delilin elde edilmesi amacıyla uygulanması gereken koruma tedbirlerine ilişkin en önemli düzenlemelerden birisi Avrupa Konseyi Siber Suç Sözleşmesi'dir. Türkiye'nin de taraf olduğu ve "Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun"un 02.05.2014 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe girmesiyle iç hukukumuzun da bir parçası haline gelen Sözleşmenin bu kapsamda ele alınması bir kat daha önem arz etmektedir.

Bununla birlikte iç hukukumuzdaki farklılıkları ortaya koyma adına mukayeseli hukukta Amerika Birleşik Devletleri başta olmak üzere İngiltere, Almanya, Fransa ve İtalya hukuk sistemlerinde bilişim sitemlerinde yapılan arama ve elkoyma koruma tedbirlerinin mevzuat, öğreti ve mahkeme içtihatları bakımından incelenmesi ve sonrasında iç hukukumuzdaki uygulamaya bakılması gerekmektedir.

Tez çalışmamızın üçüncü bölümde ise Türk hukukunda elektronik delilin elde edilmesi ve korunması sürecinde uyulması gereken usul hükümlerini düzenleyen yasa ve yönetmeliklerin ilgili hükümleri incelenecektir. Bu bağlamda 5271 sayılı Ceza Muhakemesi Kanunu'nun 134. maddesinde düzenlenen bilişim sistemlerinde arama, kopyalama ve elkoyma koruma tedbiri ayrı bir öneme sahiptir.

Koruma tedbirlerinin genel olarak temel hak ve özgürlüklere müdahale eden yapısı bulunmaktadır. Bununla birlikte bir suç soruşturması kapsamında kişilerin bilişim sistemlerinde yapılan arama sırasında suçla ilgisi olmayan birçok kişisel verinin ifşa olma olasılığının bulunması, bilişim sistemlerinde uygulanacak koruma tedbirlerinin temel hak ve özgürlükler bakımından daha sıkı uygulama şartına bağlanması zorunluluğunu doğurmaktadır.

Diğer taraftan fiziksel delillerin elde edilmesinde kullanılan klasik arama ve elkoyma tedbirlerinin, özellikle bilişim suçlarının soruşturulmasında gerekli olan ve kendine mahsus yapısal özelliklere sahip bulunan elektronik delilin elde edilmesi ve olayların aydınlatılması hususlarında yetersiz kaldığı görülmektedir. Bu bakımdan bilişim sistemleri üzerinde aranacak elektronik delilin elde edilmesi ve bu delilin adli bilişim kurallarına uygun biçimde korunarak yargı makamları önüne getirilmesini sağlayacak ayrıksı koruma tedbirlerinin düzenlenmesinde gereklilik bulunmaktadır.

Bu nedenlerle iç hukukumuzda, birçok ülke hukukundan farklı olarak, genel arama ve elkoyma koruma tedbirlerinden ayrı bir koruma tedbirinin düzenlenmesi yoluna gidilmiştir. CMK'nın 134. maddesinde düzenlenen söz konusu koruma tedbirinin, 21.02.2014 tarihli ve 6526 sayılı Kanunla maddenin birinci fıkrasında yapılan değişiklik de dikkate alınarak, koruma tedbirinin amacı, kapsamı, uygulanma koşulları, her bir fıkra hükmünün uygulanma biçimi, genel hükümlerle ilgisi bakımından ayrıntılı bir incelemeye tabi tutulması yerinde olacaktır.

Diğer taraftan temel hak ve özgürlüklere birçok koruma tedbirine nazaran daha ağır biçimde müdahale eden bu koruma tedbirinin temel hak ve özgürlükler bakımından ayrıca ele alınması, mevcut düzenlemenin gerek Anayasa'da gerekse Avrupa İnsan Hakları Sözleşmesi'nde belirtilen temel hak ve özgürlükler ve bunların kısıtlanması hallerinde gerekli olan temel kıstaslar bakımından uygun olup olmadığı noktaları ile olması gereken hukuk bakımından nelerin yapılması gerektiği hususlarının değerlendirilmesi gerekir.

Avrupa Konseyi Siber Suç Sözleşmesi'nin 19. maddesinde "Saklanan Bilgisayar Verileri Hakkında Arama ve Elkoyma" konusu düzenlenmiştir. Buna göre; Avrupa Konseyi Siber Suç Sözleşmesi'ne imza atan ve bu Sözleşmeyi onaylayıp iç hukuklarının

bir parçası haline getiren pek çok ülkenin bilişim sistemlerinde yapılacak arama ve elkoyma tedbirine ilişkin ayrı bir düzenleme yapmadıkları ve elektronik delillerin elde edilmesinde genel arama ve elkoyma tedbirlerini uyguladıkları görülmektedir. Bu bakımdan ayrı bir öneme sahip CMK m. 134 hükmünün Avrupa Konseyi Siber Suç Sözleşmesi ve hususiyle bu sözleşmenin 19. maddesi bakımından değerlendirilmesi önem arz etmektedir.

Bilişim sistemlerinde yapılacak arama, kopyalama ve elkoyma tedbiri esasen CMK m. 134 uyarınca yerine getirilmekte ise de bu maddeyle büyük ölçüde uyumlu ve fakat madde metninde eksik kalan veya uygulamada izaha muhtaç olan bir iki hususun Adli ve Önleme Aramaları Yönetmeliği'nin 9. maddesi ve Suç Eşyası Yönetmeliği'nin 17. maddesi kapsamında düzenlendiği görülmektedir. Bu bakımdan arama, kopyalama ve elkoyma tedbirinin uygulanması ve elde edilen elektronik delillerin muhafazası konusunda bu yönetmelik hükümlerine de değinmek gerekmektedir.

Ayrıca, iç hukukumuzda düzenlemeye konu olmamakla birlikte gerek iç hukukumuzda gerekse mukayeseli hukukta uygulanabilirliği tartışmaya açılmış uzaktan erişimle arama ve bulut bilişimde arama konularına da kısaca değinmek suretiyle bu tür aramaların iç hukukumuzdaki yasal düzenleme çerçevesinde uygulama alanlarının olup olmadığı hususunu ortaya koymaya çalışacağız.

Elektronik delilin görünür ve anlaşılır hale getirilmesi, elde edilmeden önce veya sonra değişikliğe uğrayıp uğramadığının saptanması, elde edildikten sonra yargı makamlarına herhangi bir değişikliğe uğramadan teslim edilmesinin sağlanması elektronik delilin kabul edilebilirliği bakımından hayati öneme sahip olması nedeniyle bu sürecin bütün halde ele alınarak kurallara bağlanması adli bilişim sürecinin bir bilim dalı olarak ele alınması sonucunu doğurmuştur.

Bu bakımdan son olarak tez çalışmamızın dördüncü bölümünde, elektronik delilin bütünlüğünün korunması ve ceza yargılamasında bir delil türü olarak kabul edilebilirliğinin sağlanması bakımından önemli bir yere sahip olan adli bilişim süreci incelenecektir. Buna göre; adli bilişim sürecinin ilk aşamasında elektronik delilin bulunduğu elektronik medyadan toplanması, toplama aşamasında gerekli hukuki ve teknolojik alt yapının gerekliliği, elektronik delilin bütünlüğünün korunması için bu

aşamada yapılması zorunlu işlemlerin neler olduğu, hukuken ve teknolojik anlamda usulüne uygun elde edilen elektronik delilin paketlenmesi, uygun ortamlarda taşınması ve muhafaza altına alınması hususlarının ne şekilde gerçekleştirilmesi gerektiği açıklanacaktır.

Adli bilişim sürecinin ikinci aşaması ele alınırken elde edilen birçok elektronik verinin incelenerek bunlardan hangilerinin delil mahiyetinde veriler olabileceğinin ortaya konulması, bunların yapılması sırasında hangi metotların kullanıldığı, gizlenmiş veya silinmiş verilerin geriye getirilip getirilemeyeceği hususlarının aydınlığa kavuşturulması sağlanacaktır.

Adli bilişimin üçüncü aşamasında bütün halde elkonulan elektronik veriler üzerinde yapılan inceleme neticesinde ortaya çıkartılan ve soruşturma veya kovuşturmaya konu olayda delil olabilecek nitelikteki veriler üzerinde analiz işleminin yapılması ve söz konusu suç ile bu suçun faili arasındaki ilginin kurularak bu verilerin artık bir delil olarak ortaya konulması, bunun sağlanması için ise hangi işlemlerin yapılması gerektiği hususları ortaya konacaktır.

Adli bilişimin son aşamasında ise adli bilişim sürecinde toplanan, paketlenerek uygun şekilde taşınan ve muhafaza edilen elektronik verilerin incelenerek bunlardan suça konu olaya temas eden delil niteliğindeki verilerin analizi de yapıldıktan sonra olayla ilgili olduğu tespit edilen elektronik delilin yargı makamlarına anlaşılır bir dilde raporlanması ve sunulması işlemleri ile bu aşamada adli bilişim uzmanlarının dikkat etmesi gereken hususlar açıklanacaktır.

Adli bilişim sürecinin aşamaları açıklandıktan sonra ise halen gelişmekte olan bir bilim dalı olan adli bilişim süreciyle ilgili mukayeseli hukukta da görülen ve fakat özellikle iç hukukumuzda sıklıkla karşılaşılan gerek elektronik delilin yapısından gerekse mevzuatımızda ve uygulamada var olan eksikliklerden kaynaklı sorunlara değinilecektir.

BÖLÜM 1: CEZA YARGILAMASINDA DELİLLER

1.1. Ceza Yargılamasında Delil Kavramı

Ceza yargılaması, geçmişte yaşandığı iddia olunan bir olayın gerçekten meydana gelip gelmediğini, meydana gelmiş ise ne şekilde ve kim tarafından meydana getirildiğini ortaya çıkartmak ve bu olayın hukuk kuralları karşısındaki durumunu tespit etmek amacıyla işleyen bir süreçtir. Gerçekleştiği iddia olunan olay hakkında belli bir vicdani kanaate sahip olabilmek için ise geçmişte ne olduğunu ve nasıl oluştuğunu bilmek gerekmektedir[1].

Ceza yargılamasında ispat, suçun cezalandırılmasında toplumun sahip olduğu menfaat ile sanık hakları arasındaki dengeyi korumak suretiyle maddi gerçeği ortaya çıkarmaya yarayan faaliyet olarak tanımlanabilir[2]. Başka bir ifadeyle ispat, ceza yargılamasında fiilin fail tarafından işlenip işlenmediği hususunda, hukuka uygun araçlarla, yargılama makamının tam bir kanaate ulaşma faaliyeti ve sürecini ifade etmektedir[3]. İspatın konusunu, suçluluğu veya yaptırımı doğrudan doğruya ilgilendiren olaylar ile bunların ispatı bakımından önem taşıyan yardımcı olay oluşturur. Ayrıca, ceza yargılamasına ilişkin bir işlem de ispatın konusunu oluşturabilir. Ancak, doğa olayları veya tarihsel olayların ispatı gerekmez[4].

İspat faaliyeti sonucunda oluşan bir inanç ve zan yeterli olmayıp hâkimin tam bir kanaate ulaşması gerekmektedir. İspat hususunda şüpheler giderilemiyorsa, bu konuda kesin bir kanaate varılamıyorsa, şüpheden sanık yararlanır (in dubio pro reo) ilkesi uyarınca, sanık lehine bir değerlendirme yapmak gerekecektir[5]. Diğer bir ifadeyle, "iddianın sabit olması ilkesi" gereğince sanığın mahkûm edilebilmesi için, hâkimin

[1] Vahit Bıçak, **Suç Muhakemesi Hukuku**, 2. Basım, Ankara: Seçkin Yayıncılık, 2013, s. 423.

[2] Veli Özer Özbek, "Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt. 59, Sayı. 1-2, (2001), s. 181.

[3] Bahri Öztürk, Mustafa Ruhan Erdem ve Veli Özer Özbek, **Uygulamalı Ceza Muhakemesi Hukuku**, 7. Basım, Ankara: Seçkin Yayıncılık, 2002, s. 410.

[4] Bahri Öztürk (Ed.), **Nazari ve Uygulamalı Ceza Muhakemesi Hukuku Ders Kitabı**, 7. Basım, Ankara: Seçkin Yayıncılık, 2014, s. 296.

[5] Faruk Turhan, **Ceza Muhakemesi Hukuku**, Ankara: Asil Yayınları, 2006, s. 152.

iddianın sabit olduğu hususunda kanaate varması gerekmektedir. Aksi halde sanık hakkında beraat kararı verilmelidir. Dolayısıyla, beraat kararı için suçsuzluğun sabit olması gerekmeyip, suçluluğun sabit olmaması yeterlidir[6].

Bir olayın ispatlanması, yargıya varma konumunda olan hâkimin o olayın varlığı konusunda ikna edilmesi, hâkimdeki olaya ilişkin şüphenin giderilmesini ifade eder. Mahkeme, bir olayı ancak yeteri kadar delil değerlendirmesi yaptıktan sonra kanıtlanmış sayabilir. Hangi olgunun hangi tür ve sayıdaki delille ispatlanmış sayılacağını önceden söylemek mümkün değildir. Bu durum, ispatlanacak olgunun özelliğine göre değişebilir. Önemli olan, mahkemenin bir olguyu kanıtlanmış sayarken mantık kurallarından sapmamış olmasıdır[7].

İspat, geçmişte yaşanmış olayların hukuki sonuçlarının belirlenmesi amacıyla yapılan çalışmada çok önemli bir işleve sahiptir. Ceza hukuku, hangi fiillerin suç teşkil ettiğini düzenleyen bir hukuk dalı olduğuna göre, bir fiilin cezalandırılması veya cezalandırılmamasının temelini oluşturması bakımından ispat çok önemlidir. Diğer taraftan hüküm, hukuka uygun biçimde mahkeme önüne getirilip tartışılan deliller üzerine inşa edilmelidir. Yargılama aşamasında suçun sübutuna veya unsurlarına etki edecek pek çok ayrıntılı olayın ispatlanması gerekmektedir. Zira bu olaylar doğrudan ve dolaylı olarak sanığın hukuki durumunu etkileyebilmektedir[8].

Diğer taraftan, daha önce ispat edilmiş bir olayın tekrar ispat edilmesine de gerek bulunmamaktadır. Bu durum, kesin hüküm (muhkem kaziye) otoritesinin sonuçlarından biridir. Bunun istisnası ise, daha önce karar veren mahkemenin ceza mahkemesi olmaması durumudur. Zira şekli gerçekle yetinen bir yargılama sonucunda verilen bir kararın, yargılamaya konu olayı, maddi gerçeği arayan ceza hâkimi gibi belirlememiş

---

[6] Nevzat Toroslu ve Metin Feyzioğlu, **Ceza Muhakemesi Hukuku**, 7. Basım, Ankara: Savaş Yayınları, 2009, s. 173-174; Bununla birlikte suç işlediği iddia olunan kişinin aleyhinde mahkeme huzuruna çıkartılmayı gerektirecek derecede delilin bulunması gerekir. Eğer bu nispette delil yoksa şüpheli hakkında dava dahi açılmaz ve şüphelinin sıfatı sanık olarak da değişmez. Bkz. Doğan Soyaslan, **Ceza Muhakemesi Hukuku,** 4. Basım, Ankara: Yetkin Yayınları, 2010, s. 195.

[7] Neval Okan ve Diğerleri (Ed.), **Ceza Muhakemesi Hukuku**, Eskişehir: Anadolu Üniversitesi Yayınları, 2005, s. 129.

[8] Mehmet Yavuz, "Ceza Muhakemesinde İspat Sorunu", **Türkiye Adalet Akademisi Dergisi (TAAD),** Sayı. 9, (Nisan 2012), s. 155.

olması imkân dâhilindedir. Bu durumda diğer mahkemenin kararı ceza mahkemesini bağlamayacaktır[9].

Soruşturma aşamasında yapılan en önemli faaliyet, olayı temsil eden delillerin araştırılması ve koruma altına alınmasıdır. Kural olarak, soruşturma evresinde[*], olayı temsil eden deliller araştırılır, kovuşturma evresinde[**] ise deliller değerlendirilir. Bu bağlamda, ceza yargılamasının adalete ve maddi gerçeğe ulaşmadaki başarısı delillerin soruşturma evresinde ne derece iyi toplandığına bağlıdır[10]. Ancak, ceza yargılamasında amaç gerçeğe ulaşmak olunca, bu amaca matuf hukuka uygun her türlü olanağın kullanılması da mümkündür. Bu nedenle de ceza yargılamasında her şey delil olabilir, hâkim de delil toplayabilir ve hatta toplamak zorunda olup önüne gelen delillerle yetinmek durumunda değildir[11].

Delil kavramı hukukta ispat aracı olarak kullanılmaktadır. Bu bağlamda, bir hukuki ihtilafı çözmeye veya suç fiilini ispata yarayan ve ikamesi hukuk tarafından yasaklanmamış her şeye (canlı-cansız, yazılı-sözlü) delil veya ispat vasıtaları denilmektedir. Delil, meydana gelen bir suçun aydınlatılması ve suç faillerinin tespitine yarayan her türlü ispat vasıtalarını kapsar[12].

Ceza yargılamasında önemli olan, tarafların tatmin edilmesi olmayıp gerçeğin ortaya çıkartılmasıdır[13]. Maddi gerçeğin arandığı ceza yargılaması delille başlar ve başka

---

[9] Toroslu ve Feyzioğlu, s. 174.

[*] Suç haberinin alınmasıyla başlayıp esas olarak Cumhuriyet savcısı ve onun yardımcısı sıfatıyla kolluk tarafından yerine getirilen ve kamu davasının açılıp açılmamasını amaç edinen, kural olarak yazılı ve gizli gerçekleştirilen bir dizi adli nitelikteki faaliyete soruşturma; bu faaliyetin yapıldığı safhaya da soruşturma evresi denir. Bkz. Bahri Öztürk (Ed.), Nazari ve Uygulamalı Ceza Muhakemesi Hukuku Ders Kitabı, 7. Basım, s. 578.

[**] İddianamenin kabulüyle başlayıp, iddia ve savunma ışığında yargılama neticesinde verilen bir hükümle sona eren ve duruşma hazırlığı, duruşma ve son karar aşamalarından ibaret olan ceza yargılaması safhasına kovuşturma evresi; bu evrede yapılan işlemlere de kovuşturma denir. Bkz. Bahri Öztürk (Ed.), Nazari ve Uygulamalı Ceza Muhakemesi Hukuku Ders Kitabı, 7. Basım, s. 606.

[10] Nur Centel ve Hamide Zafer, **Ceza Muhakemesi Hukuku**, 9. Basım, İstanbul: Beta Yayınevi, 2012, s. 197.

[11] Yener Ünver ve Hakan Hakeri, **Ceza Muhakemesi Hukuku**, 1. Cilt, 8. Basım, Ankara: Adalet Yayınevi, 2013, s. 11.

[12] Mustafa Kaygısız, **Kriminalistik Olay Yeri İnceleme Suç Yeri ve Olay Güvenliği**, Ankara: Adalet Yayınevi, 2007, s. 35.

[13] Toroslu ve Feyzioğlu, s. 173.

delillerin elde edilmesiyle de ilerler. İspatı sağlamaya yönelik tüm araçlar delillerden ibarettir. Bununla birlikte, her ispat aracı soyut olarak bir delil olmakla birlikte, deliller yargılama aşamasında bir değerlendirmeye tabi tutulurlar ve gerekirse delil olarak kabul edilmezler. Bu bakımdan bir şeyin delil olabilmesi ile delil olarak kabul edilebilmeleri farklı şeylerdir[14].

Delil, geçmişte meydana gelen olayın objektif (maddi) ve sübjektif (manevi) öğeleri, ağırlatıcı ve hafifletici nedenleri ile nedensellik bağı üzerinde hâkimi aydınlatmaktadır. Bu bakımdan, delilin, suç ile ilgisinin bulunması gerekir. Delilin, suç ile ilgisinin bulunması ise, doğrudan veya dolayısıyla olabilir. Suç ile ilgisi bulunmayan deliller ceza yargılamasında gözetilemez[15].

Delil, vicdani kanaate ulaşma aracıdır. Karar verme konumundaki hâkimin, yargılama konusu olay hakkındaki vicdani kanaatini delile dayandırması, kararın keyfi verilmesi önündeki en büyük engeldir. Kararın gerekçesinde vicdani kanaatin dayandığı delillerin gösterilmesi zorunluluğu, vicdani kanaatin deliller dışında başka faktörlerin etkisiyle oluşmasını engellemeye yöneliktir. Vicdani kanaatin delile dayandırılması zorunluluğu, basın, siyasi ortam, toplumda hâkim olan genel anlayış gibi dış etkenlerden hâkimi korur. Benzer şekilde, bu zorunluluk, bir hâkimin yetişme biçimi, genel kültürü, eğitim düzeyi ve yaşam deneyimi gibi iç etkenlerin yönlendirmesiyle karar vermesi riskine karşı da güvence oluşturur[16].

1.2. Delillerin Ortak Özellikleri

Ceza yargılaması sürecinde maddi gerçeğe ulaşmayı sağlayacak ve iddia edilen olayla ilgili vicdani kanaatin oluşmasına katkı verecek her şey delil olabilir. Bununla birlikte bu serbesti sınırsız olmayıp delil adı altında sunulan şeylerin bazı özelliklere sahip olması gerekmektedir. Bu özelliklerin olmaması durumunda delilin varlığından söz edilemeyecektir.

---

[14] Nurullah Kunter ve Feridun Yenisey, **Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku**, 11. Basım, İstanbul: Beta Yayınevi, 2000, s. 503.

[15] Ali Rıza Çınar, "Hukuka Aykırı Kanıtlar", **Türkiye Barolar Birliği Dergisi**, Sayı. 55, (Kasım-Aralık 2004), s. 34.

[16] Bıçak, s. 424.

Nitekim Yargıtay Ceza Genel Kurulu da delillerde sahip olunması gereken özelliklerin çerçevesini çizdiği bir kararında *"Ceza yargılamasının amacı, hiçbir duraksamaya yer vermeden maddi gerçeğin ortaya çıkarılmasıdır. Bu araştırmada, yani gerçeğe ulaşmada mantık yolunun izlenmesi gerekir. Gerçek; akla uygun ve realist, olayın bütününü veya bir parçasını temsil eden kanıtlardan veya kanıtların bütün olarak değerlendirilmesinden ortaya çıkarılmalıdır. Yoksa bir takım varsayımlara dayanılarak sonuca ulaşılması, ceza muhakemesinin amacına kesinlikle aykırıdır. Ceza yargılamasında, kuşkunun bulunduğu yerde, mahkûmiyet kararından söz edilemez. Bu ilke evrenseldir*[17]*."* hükmüne yer vermiştir.

1.2.1. Gerçekçilik

Delilin gerçekçi olması, onun beş duyu organla öğrenilebilir ve algılanabilir olmasını, diğer bir ifadeyle delilin, insanların iç dünyalarının bir parçası değil, nesnel ve elle tutulabilir dış dünyanın bir parçası olması ve duyu organlarla algılanabilir olmasını ifade eder. Gerçekçilik, delilin düşünülen, tasarlanan ve hayal edilen şeyler olmayıp gerçekte var olan şeyler olmasıdır. Yargılama konusu olayın tüm derinliğine ve karmaşıklığına rağmen bozulmadan, çarpıtılmadan ve değiştirilmeden ortaya konulmasına delillerin gerçek olması imkân sağlar[18].

1.2.2. Akılcılık

Delilin akılcı olması, akla ve mantığa uygun olmasını, bilime aykırı olmamasını ifade eder. Delilin maddi gerçeği akla uygun, gerçekçi ve objektif niteliklere dayanan verilerle ispat edebilir özellikte olması gerekmektedir. Bu bakımdan insan aklının, mantığının ve bilim düzeyinin kabul edemeyeceği şeyler delil olamazlar[19].

Delilin akılcılık özelliği, bilimsel açıdan kabul edilebilir bir nitelik taşımasını da beraberinde getirir. Hâkimin kararına temel teşkil eden delili bir falcının kehanetine

---

[17] Yargıtay C.G.K. 19.04.1993. E. 1993/6-79, K. 1993/108 (**Yargıtay Kararları Dergisi,** Cilt. 19, Sayı. 10, Ekim 1993), s. 1565.

[18] Bıçak, s. 429.

[19] Cumhur Şahin ve Neslihan Göktürk, **Ceza Muhakemesi Hukuku II**, 2. Basım, Ankara: Seçkin Yayıncılık, 2013, s. 19; Gürkan Özocak, "Ceza Muhakemesinde Elektronik Delillerin Tespiti ve Toplanması", **İzmir 2. Uluslararası Bilişim Hukuku Kurultayı,** İzmir, 17-19 Kasım 2011, s. 111.

veya yaygınca kabul edilen asılsız inançlara dayandırması delilin akılcılığı özelliği ile bağdaşmaz. Zira gerek falcının kehaneti gerekse toplumun benimsediği asılsız inançlar akıl yoluyla izah edilemez[20].

1.2.3. Erişilebilirlik

Delilin erişilebilir olması, somut olarak elde edilerek mahkemenin takdirine sunulabilir olmasını ifade eder. Ulaşılması hiçbir şekilde veya belirsiz bir süre için mümkün olmayan bir delil ceza yargılamasında kullanılamaz. Buna göre sanığın suç ortağının veya olay tanığının ölmesi, akıl hastalığına tutulmuş olması veya bulunduğu yerin öğrenilememesi, bu kişilerin herhangi bir engel nedeniyle duruşmada hazır bulunmasının belirsiz bir süre için imkânsız olması gibi durumlarda sanığın suç ortağının veya olay tanığının beyanını duruşmada elde etmek mümkün olmayacaktır[21].

1.2.4. Olayı Temsil Edicilik

Delil, olayı temsil edici nitelikte olmalıdır. Buna göre ispat aracının olayın bir parçası olması veya olayı yansıtması gerekmektedir. Olayı herhangi bir boyutuyla temsil etmeyen deliller, yargılama konusuna ilgisiz olmaları nedeniyle reddedilirler. Olayı temsil edicilik, geçmişte yaşanmış olayı anlatabilme ve canlandırabilme özelliğini ifade etmektedir. Delilin sağlam ve güvenilir olması da yine olayı temsil ediciliğin bir unsurudur[22].

Temsil edicilik hususu, yargılama konusu olayın tamamı esas alınarak karara bağlanmalıdır. Dolaylı delillerin olayı temsil ediciliği tek başlarına düşünüldüğünde zayıf görülebilir, ancak, sair delillerle birlikte ele alındığı takdirde olayın ispatına yardımcı olabilecekleri kanaatine varılır. Bazen dolaylı bir delil tek sonuca değil, birden fazla sonuca götürebilir. Bu durum, o delilin temsil edici olmamasıyla ilgili olmayıp

[20] Bıçak, s. 429.

[21] Şahin ve Göktürk, s. 19-20; Özocak, s. 111.

[22] Şahin ve Göktürk, s. 20.

sonuca götürmek için yetersiz oluşuyla ilgilidir. Zira delilin temsil ediciliği, delilin ikna ediciliğinden farklıdır[23].

1.2.5. Müştereklik

Delilin muhtevasını sadece hâkimin öğrenmesi yeterli olmayıp tarafların da öğrenmesi ve mütalaa niteliğindeki hükümleri ile kolektif hüküm verme faaliyetine katılabilmeleri gerekmektedir[24]. Bu bakımdan müştereklik, ceza yargılamasında öne sürülen delillerin, davanın bütün taraflarınca bilinir ve tartışılabilir olmasını ifade eder. Davaya bakan hâkimin, özel yollardan kişisel olarak edindiği ve mahkeme önüne getirilmeyen bir veri delil olarak değerlendirilemez[25]. Aksi halde, tarafların bilmediği bir delile itiraz etmeleri ve etkin bir savunma yapma imkânını bulabilmeleri söz konusu olamaz[26].

Nitekim CMK m. 217/1'de *"Hâkim, kararını ancak duruşmaya getirilmiş ve huzurunda tartışılmış delillere dayandırabilir. Bu deliller hâkimin vicdani kanaatiyle serbestçe takdir edilir."* hükmüne yer verilerek delillerin müşterekliğine vurgu yapılmaktadır.

Bu itibarla delilin kendisi, kaynağı ve muhtevasının iddia, savunma ve yargılama makamlarının tümü tarafından bilinmesi, öğrenilmesi ve tartışılması delillerin müştereklik özelliğinin bir gereğidir. Yargılama konusu bir olay hakkında hâkimin sahip olduğu şahsi delillere dayanarak karar vermesi ise delillerin müşterekliğinin ihlalidir[27].

1.2.6. Hukuka Uygunluk

Hukuka uygunluk, delilin hukuka uygun elde edilmiş olmasını, ikame ve değerlendirme yasağı içermemesini ifade etmektedir. Suç, ancak hukuka uygun olarak elde edilmiş

---

[23] Bıçak, s. 427.

[24] Nurullah Kunter, Feridun Yenisey ve Ayşe Nuhoğlu, **Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku**, 18. Basım. İstanbul: Beta Yayınevi, 2010, s. 1332.

[25] Ali Şafak ve Vahit Bıçak, **Ceza Muhakemesi Hukuku ve Polis**, 6. Basım, Ankara: Roma Yayınları, 2005, s. 281.

[26] Bülent Bayraktar, "Muhakemelerde Delillerin Önemi", **Kırgızistan-Türkiye Manas Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, Sayı. 25, (2011), s. 14-15.

[27] Bıçak, s. 429.

delillerle ispatlanabilir. Hukuka aykırı bir şekilde elde edilmiş delillerin ikamesi ve değerlendirilmesi ise yasaktır[28].

Ceza yargılamasına ilişkin her işlem esasen Anayasa'da korunan temel bir hakka müdahale anlamını taşımaktadır. Dolayısıyla bu tür işlemlerin belirlenen kurallara uygun yapılmaması, çoğu zaman anayasal bir hakkın ihlali sonucunu doğuracaktır. Ceza yargılaması bu şekilde bir hakkın ihlal edilmesi neticesinde ulaşılan maddi gerçekle ilgilenmemektedir. Bu bakımdan ceza yargılamasının ulaştığı maddi gerçeğe, süreci düzenleyen hukuk kurallarına uygun davranılarak ulaşılması gerekmektedir[29].

Belirtmek gerekir ki; ceza yargılamasının tek amacı maddi gerçeği ortaya çıkartmak da değildir. Bu doğrultuda adil yargılamanın gerektirdiği kamu barışının sağlanması, ihkak-ı hakkın önlenmesi ve cezanın infaz niteliğinin güvenceye alınması ve sanık haklarının korunması gibi çok önemli başka amaçlar da bulunmaktadır. Nitekim ceza muhakemesi kanunlarındaki koruma tedbirleriyle ilgili kuralların esas işlevi de sanık haklarının korunmasına yöneliktir[30].

Bu bakımdan günümüz ceza yargılama sistemine göre maddi gerçeğin aranması her ne pahasına olursa olsun gerçekleştirilemez. Günümüzde insan temel hak ve özgürlüklerinin maddi gerçeğin bulunmasından daha önemli olduğu kabul edilmektedir. Bu nedenle de hukuka aykırı olarak elde edilen delil kaynak ve araçları yargılamada kullanılamazlar[31].

1.3. Delillerin Fonksiyonları

Ceza yargılamasının amacı, adil yargılama kurallarına uyularak ve bu arada sanığın, suçu kesin hükümle sabit olana kadar suçsuz kabul edildiği (masumiyet karinesi) dikkate alınarak, maddi sorunun çözümlenmesi, bu şekilde maddi gerçeğin ortaya

[28] Şahin ve Göktürk, s. 20.

[29] Mesut Bedri Eryılmaz, **Ceza Muhakemesi Hukuku Dersleri,** Ankara: Seçkin Yayıncılık, 2012, s. 31-32.

[30] Ünver ve Hakeri, 1. Cilt, s. 12.

[31] Eralp Özgen, "Askeri Yargıtay Kararlarına Göre Delil Değerlendirmesi ve Savunma Hakkı", **Askeri Yargıtay'ın 80'inci Kuruluş Yıl Dönümü Sempozyumu**, Ankara, 6-7 Nisan 1994, s. 80-81.

çıkartılması ve sonrasında hukuki sorunun yine adil yargılama kurallarına saygı duyularak çözüme kavuşturulmasıdır[32].

Bu bakımdan ceza yargılamasında delillerin öncelikli fonksiyonu maddi gerçeğin ortaya çıkartılmasını sağlamaktır[33]. Nitekim CMK m. 160/2'de *"Cumhuriyet savcısı, maddi gerçeğin araştırılması ve adil bir yargılamanın yapılabilmesi için, emrindeki adli kolluk görevlileri marifetiyle, şüphelinin lehine ve aleyhine olan delilleri toplayarak muhafaza altına almakla ve şüphelinin haklarını korumakla yükümlüdür."* hükmüne yer verilmiştir.

Delillerin bir fonksiyonu da masumiyet (suçsuzluk) karinesinin işlerliğini sağlamaktır. Nitekim Anayasa'nın 38/4 maddesinde *"Suçluluğu hükmen sabit oluncaya kadar, kimse suçlu sayılamaz."* hükmüne yer verilerek masumiyet (suçsuzluk) karinesini anayasal güvenceye bağlamıştır.

Delillerin başka bir fonksiyonu ise Latince "in dubio pro reo" olarak ifade edilen ve masumiyet (suçsuzluk) karinesinin bir uzantısı olan "şüpheden sanık yararlanır" ilkesinin işlemesini sağlamaktır. Nitekim sanığın cezalandırılması için yeterli kuvvette bulunmayan deliller yargılama sonucunda sanığın beraat etmesine neden olacaktır.

1.4. Delil Çeşitleri

1.4.1. Beyan Delili

Ceza yargılamasının konusunu oluşturan olayla ilgili herhangi bir bilgisi veya kanaati olan kişilerin bu durumu yazılı veya sözlü olarak ifade etmeleri beyan delilini oluşturmaktadır. Beyan delili sanık, tanık, mağdur, vekil, kanuni mümessil, malen sorumlu, bilirkişi gibi ceza yargılamasının öğelerine ilişkin olabilir. Beyanın delil olarak nitelendirilebilmesi için mutlaka soruşturma veya kovuşturma aşamasında ifade edilmiş

[32] Metin Feyzioğlu, **Ceza Muhakemesinde Vicdani Kanaat**, Ankara: Yetkin Yayınları, 2002, s. 69-70.

[33] Veysel Dinler, "Ceza Muhakemesinde Delillerin Toplanması", (**Yayınlanmamış Yüksek Lisans Tezi**, Polis Akademisi GBE, 2009), s. 12.

olması gerekmeyip henüz soruşturma başlamadan önce yapılmış açıklamalar da beyan delilini oluşturabilmektedir[34].

Buna karşın öğretide, olaya ilişkin açıklamaların ancak kovuşturma aşamasında mahkeme önünde yapılmaları durumunda beyan delili özelliği gösterebilecekleri, soruşturma evresinde savcı veya kolluk önünde yapılan sözlü açıklamalara "ifade" denildiği, soruşturma evresinde beyan delili özelliği gösteren açıklamaların kovuşturma aşamasında mahkeme önünde tekrarlanmaları halinde bu evre için de beyan delili özelliğini taşıyabilecekleri, bununla birlikte, Cumhuriyet savcısı veya kolluk tarafından alınan ifadeye ilişkin tutanakların duruşmada okunması durumunda ise beyan değil belge delilinden söz edilebileceği savunulmuştur[35].

Beyan delili, suça ilişkin olayın aydınlatılması bakımından günümüzde de en çok başvurulan delil türü olmakla birlikte, güvenilirliği bakımından daima ihtiyatla yaklaşılması gereken bir delil çeşididir. Sanık ve mağdur olayı bizzat yaşayan kişiler olmaları nedeniyle gerçeği en iyi bilen kimselerdir. Buna karşın bu kişilerin olayın tarafı olmaları nedeniyle olayı kendi lehlerine olacak şekilde aktarmaları kuvvetle muhtemeldir. Bu yüzden bu kimselerin beyanlarının şüphe ile karşılanması doğaldır. Tanık ise, her ne kadar olayın taraflarından birisi değilse de çeşitli nedenlerle yanlış veya yalan beyanda bulunma ihtimali bulunmaktadır. Bu bakımdan, beyan delilinin olayın bütünlüğü bakımından değerinin hâkim tarafından dikkatlice takdir edilmesi gerekmektedir[36].

1.4.1.1. Şüpheli/Sanık Beyanı

Şüpheli veya sanığın olaya ilişkin açıklamalarının dinlenmesi ifade alma ve sorgu işlemi olarak tanımlanmaktadır. Bu bağlamda, CMK m. 2'ye göre, şüphelinin kolluk görevlileri veya Cumhuriyet savcısı tarafından soruşturma konusu suçla ilgili olarak dinlenmesi ifade alma olarak tanımlanırken, sorgu, şüpheli veya sanığın hâkim veya

[34] Bıçak, s. 436.

[35] Centel ve Zafer, s. 201.

[36] Mahmut Koca, "Ceza Muhakemesi Hukukunda Deliller", **Ceza Hukuku Dergisi (CHD)**, Sayı. 2, (Aralık 2006), s. 216.

mahkeme tarafından soruşturma veya kovuşturma konusu suçla ilgili olarak dinlenmesini ifade etmektedir[37].

Ceza yargılamasının amacı maddi gerçeğe ulaşmak olup bu amaca ulaşmayı mümkün kılmak için de ceza yargılamasında delil serbestîsi ilkesi benimsenmiştir. Bununla birlikte kanunun delillerin ile sürülmesi, toplanması ve değerlendirilmesi konularında bir sıralama yapma yolunu benimsediği görülmektedir. Bu sıralama çerçevesinde, yargılama sonucunda verilecek kararda, şahsi delillerin maddi delillere (belge ve belirti delillerine) ve ayrıca duruşmada ortaya konulan delillerin duruşma haricinde ileri sürülen delillere karşı bir önceliğinin olduğu görülmektedir[38].

Gerçekten de, şüpheli ve sanığın olay hakkında doğrudan doğruya bilgi sahibi olan yegâne kişi olduğu, birçok suçta, mağdurun dahi olaya ilişkin doğrudan bilgisinin bulunmadığı dikkate alındığında şüpheli veya sanık beyanının olayın aydınlatılması açısından son derece önemli olduğu ortadadır[39].

1.4.1.2. Tanık Beyanı

Ceza yargılamasına konu olan uyuşmazlığın taraflarından birisi olmayan, ancak uyuşmazlık konusu maddi sorunla ilgili, duyu organlarının bir veya birkaçı aracılığı ile bilgi edindiği varsayılan ve sahip olduğu bilgileri adli makamlara bildiren üçüncü kişilere tanık, tanığın yaptığı açıklamalara ise tanık beyanı denilmektedir[40].

Tanık, kendisi hakkında yürütülmeyen bir yargılamada bildiklerini anlatan herhangi bir kişidir. Tanığın kendisi delil kaynağıdır. Delil olan ise tanığın açıklamalarıdır[41]. Tanık denildiğinde suça konu olayı doğrudan gören ve/veya duyan kişi akla gelmektedir[42].

---

[37] Centel ve Zafer, s. 201.

[38] Şahin ve Göktürk, s. 22-23.

[39] Centel ve Zafer, s. 201.

[40] Metin Feyzioğlu, **Ceza Muhakemesi Hukukunda Tanıklık**, Ankara: Ankara Üniversitesi Hukuk Fakültesi Yayınları, 1996, s. 28.

[41] Şahin ve Göktürk, s. 24.

[42] Süheyl Donay, **Ceza Yargılama Hukuku,** İstanbul: Beta Yayınevi, 2010, s. 67.

Bununla birlikte ceza yargılamasının süjelerinden olan ihbar eden kişiler ile bilirkişiler de tanık olarak kabul edilmektedirler.

Tanık, ceza yargılamasında ilk akla gelen ve yaygın olarak kullanılan delil kaynaklarındandır. Tanıksız bir yargılama faaliyetiyle karşılaşmak oldukça güçtür. Ancak, ceza yargılama sisteminin, tanık deliline aşırı derecede bağımlı olması, hata ihtimalini de artırır. Zira olayın şoku altındaki tanığın, algılama, hatırlama ve ifade edebilme görevlerini tam anlamıyla yerine getirememesi, tanığın güvenilirliğinin sorgulanmasına neden olacaktır[43].

Nitekim Yargıtay bir kararında; *"Ölüm ve yaralanma ile sonuçlanan olayda, sanığın kullandığı midibüsle içinde köylüler olduğu halde köye dönerken ölenin kullandığı mobilete çarptığı iddiasıyla dava açılmıştır. Olayın köyler arasında meydana gelmesi, sanığın kullandığı araç içinde düğünden dönen 15-20 kişinin bulunduğu, bu kişiler tarafından olay sırasında ileri sürülmüş bir beyan olmadığı, aynı araçta bulunan tanıklardan bazılarının olaydan 5 yıl sonra sanığın mobilete çarptığını, bazılarının ise hiç kaza olmadığını ve böyle bir olayı görmediklerini söyledikleri, köy yerindeki 15-20 kişinin bulunduğu midibüsün yolda mobilete çarpmasını görüp olaya seyirci kalmaları veya olayı hemen akabinde ilgililere bildirmemeleri yahut olayla ilgili bir şey söylememeleri hayatın olağan akışına ve beşeri özelliklere uygun olmayıp, hükme esas alınan tanık beyanları arasındaki çelişkiler de nazara alındığında sanığın atılı suçu işlediğine ilişkin her türlü kuşkudan uzak kesin ve inandırıcı delil elde edilemediği gözetilmeden yazılı şekilde mahkûmiyetine karar verilmesi nedeniyle hükmün bozulmasına[44]"* hükmetmiştir.

Tanık, olay hakkında öğrendiklerini açıklamaktadır. Olay hakkındaki bilgi, uyuşmazlık konusu olayın beş duyu organ aracılığı ile algılanması şeklinde olabileceği gibi, olayın başka kişilerden duyulması şeklinde de olabilir. Birinci durum doğrudan tanıklığı ifade ederken, ikinci durumda ise dolaylı tanıklıktan söz edilir[45]. Buna göre, tanık beyanı, ispat konusu olan olayı temsil ettiği nispette değer kazanmaktadır. Yargılama

[43] Bıçak, s. 251.

[44] Yargıtay 9. CD. 06.04.2009. E. 2009/1380, K. 2009/3904 (UYAP).

[45] Şahin ve Göktürk, s. 24.

sonucunda verilecek karar bakımından olay hakkında doğrudan bilgi sahibi olan tanığın beyanı, olayı daha iyi temsil etmesi nedeniyle, olayı başkalarından öğrenen tanığın beyanından daha değerli olacaktır[46].

1.4.1.3. Diğer Kişilerin Beyanları

Beyan delilleri şüpheli/sanık ve tanık beyanı şeklindeki ayrım ile tam olarak karşılanamamaktadır. Bu bakımdan diğer kişilerin açıklamaları ile ilişkili olarak üçüncü bir alt başlığa yer verilmektedir. Kanunda sadece suç şüphesi olan kişilerin yani şüpheli ve sanık ile tanığın açıklamalarının nasıl elde edileceğine dair müstakil düzenlemeler bulunmaktadır. Buna karşın, şüpheli ve sanık ile tanık dışında kalan kişilerin beyanlarının elde edilişine yönelik ayrıntılı düzenlemelere yer verilmemekte, daha çok atıf yoluyla konunun düzenlenmeye çalışıldığı görülmektedir[47].

Bu bağlamda, CMK m. 236'da mağdur ve şikâyetçinin beyanına ilişkin hükümlerde -yemin hariç- tanıklığa ilişkin hükümlerin uygulanacağı belirtilmektedir. Ancak olayın tarafı olmaları nedeniyle bu kişilere ait açıklamaların ihtiyatla değerlendirilmesi gerekmektedir. Esasen suçtan zarar gören kişi (mağdur/şikâyetçi), pek çok durumda olayı bizzat yaşadığı için konuyu en iyi bilen kişidir. Bu kişinin, olayı tarafsız şekilde anlatması durumunda soruşturma ve kovuşturma makamlarının işi kolaylaşacaktır. Ancak, insan tabiatı gereği, genellikle kendisini haklı görme eğiliminde olabileceğinden suçtan zarar görenlerin açıklamaları objektif olamayabilir. Suçtan zarar görenin kamu davasına katılarak "katılan" sıfatını alması durumunda da değişiklik olmayacaktır[48].

Mağdur, şikâyetçi veya katılanın soyut iddialarının başka delillerle doğrulanmaması durumunda genellikle mahkûmiyet kararı verilememektedir. Mahkemenin soyut iddia üzerine vermiş olduğu mahkûmiyet kararında ise mağdur beyanındaki iddiaları inandırıcı bulma nedenlerini açıklaması gerekmektedir[49].

---

[46] Toroslu ve Feyzioğlu, s. 178.

[47] Şahin ve Göktürk, s. 43.

[48] Bahri Öztürk (Ed.), Nazari ve Uygulamalı Ceza Muhakemesi Hukuku Ders Kitabı, 7. Basım, s. 324.

[49] Bıçak, s. 441-442.

Nitekim Yargıtay bir kararında; *"Suça sürüklenen Aydın ve annesi tanık Gülten ile katılan Sevim'in, komşu oldukları, aralarında uzun süredir husumet bulunduğu, suça sürüklenen Aydın'ın, katılana ait kömürlüğün kilidini kırdığı, suça sürüklenen çocuk Aydın'ı evinin önünde oynarken gören katılanın, onun yanına gittiği ve kendisine; 'burada oynamayacaksın!' dediği, bunun üzerine Aydın'ın, katılana; 'ben seni geçen sene dövdüm, dayak yedin, şimdi seni yine döveceğim, senin ölümün gelmiş!' şeklinde tehdit içeren sözleri söyleyip bağırdığı şeklinde tanımlanan olayda; suça sürüklenen çocuğun, atılı suçları işlediğine dair, aralarında husumet bulunan katılanın soyut beyanı dışında, cezalandırılmasını gerektirir her türlü şüpheden uzak kesin ve inandırıcı delil elde edilemediğinden.....verilen beraat kararında bir isabetsizlik görülmemiştir[50]."* hükmüne yer vermiştir.

Diğer taraftan soruşturmanın henüz başında, özellikle de olay mahallinde bazı kişilerin vermiş oldukları bilgilerin hangi sıfatla verildiği konusunda tereddüt yaşandığı için "ifade sahibi" şeklinde bir kategori de oluşturulmakta ve "bilgi toplama" şeklinde bir beyan delili şekli ortaya çıkmaktadır[51].

Bütün bu kişilerin beyanları gerçeğin oraya çıkartılmasında yardımcı olabilir ve dolayısıyla delil niteliğindedir. Ancak bu kişiler tanık olmadıklarından ve yeminli dinlenmediklerinden dolayı yalan beyanda bulunmaları halinde yalan tanıklıktan değil katılan gibi, iftira suçundan veya başka bir suçtan dolayı cezalandırılabilirler[52].

1.4.2. Belge Delili

Belge, somut bir olayla ilgili bilginin bir kâğıda veya benzer nitelikte kayıt özelliği taşıyan bir eşyanın üzerine aktarılmış halini ifade eder[53]. Belge, somut bir olayı temsil eden ve insanlar tarafından oluşturulan bir ispat aracıdır. Belgede genellikle olayın belirli şekillerle bir nesne üzerine aktarılması söz konusudur. Belge içerik itibariyle beyandan daha güvenilirdir. Zira belge genellikle olay anında ve kişilerin huzurunda

[50] Yargıtay 15. CD. 02. 07. 2013. E. 2013/11647, K. 2013/12277 (UYAP).

[51] Şahin ve Göktürk, s. 43.

[52] Toroslu ve Feyzioğlu, s. 194.

[53] Mesut Bedri Eryılmaz, s. 644.

yapıldığından hata olasılığı daha azdır. Bu nedenle, sahte olmayan, şekil itibariyle de güvenilir nitelikteki belgeler ceza yargılamasında önem arz etmektedirler. Belgenin güvenilirliği, onu hazırlayanın güvenilirliği ile orantılıdır. Bu bakımdan resmi belgenin ispat gücü özel belgeden daha fazladır[54].

İmzasız mektup gibi, tanzim edeni belli olmayan belgeler ise ispat bakımından değersizdir. Bu belgelerin ispat fonksiyonunu taşıyabilmesi, yazı sahibinin tespit edilebilmesine bağlıdır. Belgenin güvenilirliğini sağlamak için kimi zaman imza da yeterli olmayabilir. Nitekim mahkeme ilamı, tapu senedi ve nüfus cüzdanı gibi bazı resmi belgelerin gerçekliği bu belgelerin mevzuatta belirtilen usule uygun şekilde tanzim edilmelerine bağlı kılınmıştır[55].

Belge delilleri yargılama sürecinde çeşitli işlemlere tabi tutulabilir. Belgenin üzerinde tahrifat yapıldığı iddia edildiğinde, bu durumun anlaşılması özel ve teknik bir bilgiyi gerektirdiğinden belge delili bilirkişi incelemesinin konusunu teşkil eder. Bilirkişi, teknik bilgisini kullanarak belge üzerindeki işaretlerden bunun sahte olup olmadığını anlamaya çalışmaktadır. Belgenin üzerindeki yazıların tamamen silindiği iddia olunduğunda ise bunun araştırılması özel ve teknik bir bilgiyi gerektirmediğinden hâkim bu belgeyi bizzat inceleyebilir. Bu durumda belge teknik anlamda bir keşif faaliyetinin konusunu oluşturur[56].

Belgeler, fikri bir muhtevaya sahiptirler ve muhtevalarıyla delili değerlendiren kişiye ışık tutup ona bugünde dünü yaşatır, olay hakkında karar vericilerin bir kanaate ulaşmasına yardımcı olurlar[57].

İspatı gerekli olan bir hususun hem tanığı hem de belgesi varsa, bu durumda hâkim doğrudan doğruyalık, sözlülük ve mahkemenin gerçeği bulma yükümlülüğü ilkeleri doğrultusunda hangi tür delili tartışmaya açacağına kendisi karar verecektir. Bununla

[54] Şahin ve Göktürk, s. 44.

[55] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1384.

[56] Centel ve Zafer, s. 245.

[57] Bıçak, s. 454.

birlikte, bir olayın ispatında kullanılması mümkün olan tüm delillerin, soruşturma evresinde ayrım yapılmaksızın toplanması ve koruma altına alınması gerekmektedir[58].

Belge delili denildiğinde genellikle yazılı belge akla gelmekte ise de belge delili sadece yazılı belgeden ibaret değildir. Bu bakımdan belge delili yazılı belge, şekil tespit eden belge, ses ve görüntü tespit eden belge ve bilişim verisi şeklindeki belge olmak üzere dört alt başlıkta incelenebilir.

1.4.2.1. Yazılı Belge

Yazılı belge, bir olayı nakleden veya bir irade beyanını içeren her türlü yazıyı ifade etmektedir[59]. Yazılı belge, adından da anlaşılacağı üzere yazılı olması zorunlu olan belgedir. Yazılı belgenin ceza hukukunda delil olarak değerlendirilebilmesi, olayın bir parçası olması ve olayı temsil amacıyla düzenlenmesine bağlıdır[60].

1.4.2.2. Şekil Tespit Eden Belge

Bu tür belgeler fotoğraf, resim, kroki, plan gibi belli bir olayı temsil etmek üzere düzenlenen belgelerdir[61]. Bu tür belgelerin hileli olup olmadığına dikkat edilmesi gerekmektedir. Özellikle resmin gerçeği temsil gücü oldukça şüphelidir. Zira resmin yapılmasında bunu yapanın hayal gücünün katkısı çok fazladır[62].

1.4.2.3. Ses ve Görüntü Tespit Eden Belge

Ses ve görüntünün kaydedilmesi sonucunda oluşturulan belgeye ses ve görüntü tespit eden belge denilmektedir. Ses ve görüntü kaydeden araçlarla yapılan tespitlerin ceza yargılamasında hangi durumda delil olarak kullanılacağı ve kullanıldığı takdirde ne tür bir delil olduğu hususu ceza muhakemesi hukukunun önemli bir sorununu teşkil etmektedir.

---

[58] Centel ve Zafer, s. 247.

[59] Toroslu ve Feyzioğlu, s. 196.

[60] Özgün Öztunç, "Ceza Muhakemesinde Hukuka Aykırı Deliller", (**Yayınlanmamış Doktora Tezi**, Marmara Üniversitesi SBE, 2010), s. 36.

[61] Bahri Öztürk (Ed.), Nazari ve Uygulamalı Ceza Muhakemesi Hukuku Ders Kitabı, 7. Basım, s. 644.

[62] Toroslu ve Feyzioğlu, s. 196.

Ses ve görüntü kayıtlarının delil olarak kullanılıp kullanılamayacaklarına ilişkin sorun bu ses ve görüntülerin tahrifata uğrama veya sahte olarak oluşturulabilme olanağının yüksek olmasından kaynaklanmaktadır. Bununla birlikte ses ve görüntü kayıtlarının bu denli suiistimale açık olmalarına karşın günümüz teknolojisinin gelişmişlik düzeyi dikkate alındığında söz konusu kayıtlarda olması muhtemel tahrifat veya sahteciliklerin tespiti mümkün görünmektedir.

Yıldız'a göre; güvenilir olmadıkları gerekçesiyle, genel ve soyut bir şekilde ses ve görüntü kayıtlarının delil olarak kullanılamayacakları biçiminde bir yargıda bulunmak doğru bir yaklaşım tarzı değildir. Nitekim diğer delillerde de her zaman bir gerçeğe aykırılığın bulunması mümkündür. Bu bağlamda, ses ve görüntü kayıtlarında yapılabilecek sahtecilik diğer delillerden daha fazla değildir. Dolayısıyla, diğer delillerin ses ve görüntü kaydına göre daha güvenilir olduğunu söylemek mümkün değildir. Bu nedenle, hukuka uygun elde edilmiş bir ses veya görüntü kaydının tahrifata uğradığı veya sahte olarak oluşturulduğu konusunda herhangi bir tereddütün bulunmadığı hallerde bu kayıtların ispatta kullanılabileceği açıktır[63].

Benzer görüşte olan Centel ve Zafer'e göre ise; hukuka uygun yollardan elde edilmiş ve teknik açıdan sağlamlığı ispatlanmış olan ses ve görüntü kayıtlarının diğer delillerden bir farkı bulunmamakta olup, bunlar ispat gücü bakımından diğer delillerle aynı durumdadır[64].

Değirmenci'ye göre, ses ve görüntü kayıtları, ilgili kayıtların sahihliği ve tahrif edilmediği hususları diğer delillerle desteklendiği sürece tek başına mahkûmiyete esas olacaktır. Bununla birlikte, ses ve görüntü kayıtlarının tek başına bir olayı ispata yeterli olup olmayacağı hususu, ceza yargılamasına konu maddi olayı doğrudan mı, yoksa dolaylı olarak mı işaret ettiği ile ilgili bir durumdur. Bu hususun belirlenmesi ise mahkemeye bırakılmalıdır[65].

---

[63] Ali Kemal Yıldız, "Ses ve/veya Görüntü Kayıtlarının İspat Fonksiyonu, **Ceza Hukuku Dergisi (CHD)**, Sayı. 2, (Aralık 2006), s. 256; Aynı doğrultuda bkz. Levent Bayram, "Ses ve Görüntü Kayıtlarının Türk Hukukundaki Yeri", **Polis Bilimleri Dergisi**, Cilt. 6, Sayı. 3-4, (2004), s. 10.

[64] Centel ve Zafer, s. 245.

[65] Olgun Değirmenci, **Ceza Muhakemesinde Sayısal (Dijital) Delil**, Ankara: Seçkin Yayıncılık, 2014, s. 396.

Koca'ya göre de; günümüzün teknolojik gelişmeleri sayesinde esasen bir bant kaydındaki sesin kime ait olduğu veya bu kayıt üzerinde tahrifat yapılıp yapılmadığı kolaylıkla tespit edilebilmektedir. Bu bakımdan bu araçların hukuka uygun şekilde elde edildikleri ve içeriğinin de gerçek olduğu, herhangi bir tahrifata maruz bırakılmadığı kesin olarak belirlendikten sonra bunların yargılamada tek başlarına dahi delil olarak kullanılabilmeleri mümkündür. Buna karşın ses veya görüntü kayıtlarının hukuka aykırı şekilde elde edilmeleri veya bunlar üzerinde tahrifat şüphesinin varlığı halinde belirti delili olarak dahi kullanılmaları mümkün değildir[66].

Bununla birlikte, Öztürk ise; ses ve görüntü kayıtlarının usulüne uygun elde edilmiş ve muhafaza altına alınmış olmaları durumunda bile tek başlarına mahkûmiyet kararı verilmesine yetmeyeceğini ve bunların başka delillerle desteklenmesi gerektiğini savunmuştur[67].

Anayasa Mahkemesi de bir kararında *"Ses alma alanındaki ilerleme ve gelişmeler bugün o evrededir ki bir sesin belirli bir kişiye ilişkin bulunduğunun hala parmak izlerinde olduğu gibi kuşkusuzca ve kesinlikle saptanamamasına karşılık birtakım montaj yollarıyla ve gerekirse ses taklit etmede usta kişilerin yardımlarından da yararlanılarak bantlar istenildiği gibi doldurulabilmektedir. Bir toplantıda hazır bulunanlar, zamanında ve usulünce tutanaklarla saptanarak o toplantıya ilişkin bulunduğu ileri sürülen ses bantlarına böylece destek ve güç kazandırılmadıkça bant çevirilerine hukuk yönünden tam bir güvenle bağlanıp dayanılamayacağı ortadadır. ....Yukarıdan beri açıklananlarla varılan sonuç şudur: Başkaca inandırıcı ve pekiştirici kanıtlar bulunmadıkça yalnızca ses bantlarının...*[68]*"* delil olarak kullanılmasının hukuk devletinde düşünülemeyeceğine hükmetmiştir

Bununla birlikte Anayasa Mahkemesi görüntü kayıtlarıyla ilgili verdiği bir kararında ise *"video bantların, yasa dışı yollarla sağlanmadığı ve konuşmaların da görüntü ve içerik bakımından bunları yaptığı iddia edilen kişilere ait olduğu dosyada bulunan belgeler ve*

[66] Koca, Ceza Muhakemesi Hukukunda Deliller, s. 218.

[67] Bahri Öztürk (Ed.), Nazari ve Uygulamalı Ceza Muhakemesi Hukuku Ders Kitabı, 7. Basım, s. 328.

[68] Anayasa Mahkemesi 19.08.1971. E. 1971/41. K. 1971/67 (UYAP).

bilirkişilerce yaptırılan çözümle sabit olduğundan, video bantlar delil olarak kabul edilmiştir[69]*."* hükmüne yer vermiştir.

Yargıtay konuya ilişkin bir kararında; *"Teyp bantlarının tek başlarına delil vasfını haiz olamayacağı düşünülmeden ve dosyada sanıkların suç konusu sözleri sarf ettiklerine dair banttan başka hiç bir delil bulunmadığı gözetilmeden mahkûmiyet hükmü kurulması bozmayı gerektirmiştir*[70]*."* hükmüne yer vermiştir.

Buna karşın Yargıtay'ın daha yeni bir kararında ise; *"Telefon konuşmalarına ilişkin çözüm tutanaklarının aslı veya onaylı örneklerinin getirtilerek dosya içine konması; belirtilen tutanakların sanıklara okunarak konuşmaların kendilerine ait olup olmadığının sorulması; kendilerine ait olmadığını söylemeleri halinde ses kayıtları dinletilerek seslerin kendilerine ait olup olmadığının sorulması; seslerin de kendilerinin olmadığını belirtmeleri halinde ses örnekleri alınarak, kayıtlardaki seslerin sanıklara ait olup olmadığı konusunda Adli Tıp Kurumu Fizik İhtisas Dairesi veya uzman bir kurum veya kuruluştan rapor alınması; ses kayıtlarının sanıklara ait olduğunun belirlenmesi halinde, telefon konuşmalarının somut olayla ve gerçekleşen olgularla örtüşüp örtüşmediğinin ayrı ayrı irdelenip değerlendirilmesi, sonucuna göre tüm deliller birlikte tartışılarak sanıkların hukuki durumlarının belirlenmesi gerekirken…*[71]*"* hükmüne yer verilerek ses kaydının sanığa ait olduğu ve olayla ilgili bulunduğu hususlarının kesin olarak tespiti durumunda delil vasfına haiz olduğu kabul edilmiştir.

Kanaatimizce, CMK m. 217/2 hükmü uyarınca hukuka uygun biçimde elde edilmeyen bir ses ve/veya görüntü kaydı delil olarak kullanılamaz. Bu bakımdan kişilerin özel hayatları ve kişilik hakları ihlal edilerek elde edilen bu neviden verilerin delil niteliğinden bahsedilemez. Buna karşın her şeyin delil olabildiği ve delil hiyerarşisinin bulunmadığı ceza muhakemesinde, CMK m. 135 vd. maddelerine uygun olarak kaydedilen ve herhangi bir tahrifat ve sahteciliğe maruz kalmayan ses ve görüntü kayıtlarının tek başlarına bile delil olarak kullanılabileceği açıktır.

---

[69] Anayasa Mahkemesi 16.01.1998. E. 1997/1. K. 1998/1 (UYAP).

[70] Yargıtay 9. CD. 05.10.1984. E. 1984/1835, K. 1984/2346 (Yılmaz Güngör Erdurak, **En Son Değişiklikleriyle Notlu-İçtihatlı Ceza Muhakemeleri Usulü Kanunu,** Ankara: Sevinç Matbaası, 1985, s. 239).

[71] Yargıtay 10. CD. 03.06.2013. E. 2011/8204, K. 2013/4982 (UYAP).

Bununla birlikte CMK m. 135 hükmü uygulanmaksızın elde edilen bazı ses kayıtlarının delil niteliğine sahip olup olmadığı hususu üzerinde de durulması gerekir. Bu bağlamda telefon vasıtasıyla işlenen bir suçun mağdurunun, aranması üzerine telefonunu açması sonrasında yaptığı görüşmeyi kaydetmesi halinde bu kayıtların da hukuka uygun elde edilmiş delil değeri kazanabileceği, ayrıca mağdurun meşru savunma çerçevesinde hareket etmesinden mütevellit mağdurun eyleminin haberleşmenin gizliliğini ihlal veya kişiler arasındaki konuşmaların kayda alınması ya da benzeri başka bir suça vücut vermeyeceği ileri sürülmektedir[72].

Gerçekten de, çocuk kaçıran bir kişinin telefonla şantaj yapması örneğinde olduğu gibi meşru müdafaa halinin varlığı durumunda, bu kişinin konuşması yasada belirtilen kurallara uyulmadan kayda alınmış olsa da bu kaydın yargılamada delil olarak kullanılabilmesi gerekmektedir[73].

Öğretide ileri sürülen farklı bir görüşte ise, bir kişinin, bir başka kişiyle yaptığı konuşmaları, kendisine yönelik işlenen haksız bir fiilin ispatı amacıyla kaydetmesi durumunda, kayıt altına alınan seslerin kişisel veri olarak nitelendirilemeyeceği, bu verinin, artık kişisel olmaktan çıkmış ve bir başka kişi tarafından algılanabilir mahiyet kazanmış bir veri olduğu, bu nedenle de böyle bir durumda, karşı tarafın konuşmasını kayıt altına alan kişinin eyleminin, CMK m. 135 kapsamında değerlendirilemeyeceği, bu eylemin özel hayata ilişkin TCK'da düzenlenmiş suçlardan herhangi birine de uymayacağı, bu itibarla eylemin meşru müdafaa hukuka uygunluk sebebi olarak da değerlendirilemeyeceği gerekçesiyle bu şekilde elde edilen kayıtların delil olarak kullanılamayacağı ifade edilmektedir[74].

Yargıtay Ceza Genel Kurulu yakın tarihli bir kararında ise; "*Kişinin kendisine karşı işlenmekte olan bir suçla ilgili olarak, bir daha kanıt elde etme olanağının bulunmadığı*

[72] Ali İhsan Erdağ, "İletişimin Denetlenmesi Kapsamında İki Önemli Sorun Olarak: Mağdurun İletişimin Tespiti ve İletişimin Mağdur Tarafından Kaydedilmesi", **Türkiye Barolar Birliği Dergisi**, Sayı. 92, (Mart-Nisan 2011), s. 49-54.

[73] Bahri Öztürk, **Yeni Yargıtay Kararları Işığında Delil Yasakları (Hukuka Aykırı Olarak Elde Edilen Deliller, Yasak Kanıtlar)**, Ankara: Ankara Üniversitesi Siyasal Bilimler Fakültesi İnsan Hakları Merkezi Yayınları, 1995, s. 114.

[74] Yusuf Yaşar, "Bir Suçun İspatı Amacıyla İletişimin Kayda Alınmasının Hukuki Niteliği", **Türkiye Adalet Akademisi Dergisi (TAAD),** Sayı. 14, (Temmuz 2013), s. 383, 391.

ve yetkili makamlara başvurma imkânının olmadığı ani gelişen durumlarda karşı tarafla yaptığı konuşmaları kayda alması halinin kanıtların kaybolması ve bir daha elde edilememesi söz konusu olacağından hukuka uygun olduğu, kişinin bu eyleminin özel hayata ve hayatın gizli alanına karşı suçlar kapsamında da değerlendirilemeyeceği[75]*"* hükmüne yer vermiştir.

Öğreti ve uygulamada kabul edilen ve tarafımızca da benimsenen söz konusu uygulama, Amerikan hukukunda var olan üçüncü taraf (third party) öğretisine benzemekte ve kişilerin kolluk makamlarının yönlendirmesi veya talebi olmaksızın, hükümetin de bir görevlisi gibi davranmaksızın elde etmiş oldukları delillerin sınırlı şartlarda kabul edilebilirliğini sağlamaktadır. Bununla beraber, Türk hukukunda üçüncü kişiler tarafından elde edilen delillerin hukuka uygunluğu değerlendirmesi, sadece kişilerin kendilerine karşı işlenen suçlar bakımından kabul edilmesi nedeniyle Amerikan hukukunda mevcut olan üçüncü taraf öğretisine göre daha sınırlıdır[76].

Ceza muhakemesi hukukunda ses ve görüntü kaydeden araçlarla yapılan tespitlerin deliller içerisindeki yeri ile ilgili çeşitli görüşler ileri sürülmüştür. Öğretide bizim de katıldığımız görüşe göre; usulüne uygun şekilde doldurulup muhafaza altına alınmış ve yine usulüne uygun şekilde mahkemeye delil olarak sunulmuş bulunan ses ve görüntü kayıtları yazılı açıklamalardır ve belge delili niteliğindedirler[77].

Kunter, Yenisey ve Nuhoğlu'na göre ise, ses ve görüntü kaydının belge delili olarak nitelendirilmesini süjenin ses ve görüntü kaydı yapılacağı hususunda bilgilendirilmesi ve bundan sonra kaydın yapılması şartına bağlıdır. Buna göre, CMK m. 147/1-h uyarınca ifade alma sırasında ses ve görüntünün kayda alınması halinde "irade açıklamalarının tespit edildiği belge"nin varlığından söz edilmesi gerekir. Kanun bu tür ses ve görüntü kaydının ceza yargılaması amacıyla yapılmasını birkaç yerde kabul etmiştir. Buna karşın bu görüşe göre, iletişimin denetlenmesindeki ses kayıtları (CMK m. 135) veya teknik araçlarla izleme yöntemi ile gizlice yapılan ses ve görüntü kayıtları

[75] Yargıtay CGK. 21.05.2013. E. 2012/5MD-1270, 2013/248 (UYAP).

[76] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 437-438.

[77] Bahri Öztürk (Ed.), Nazari ve Uygulamalı Ceza Muhakemesi Hukuku Ders Kitabı, 7. Basım, s. 327.

(CMK m. 140)'nın hukuki anlamda "belge" delilini oluşturmayıp "belirti" delili nevinden kabul edilmesi gerekmektedir[78].

Centel ve Zafer'e göre ise, teknik anlamda sağlamlıkları kabul edildikten sonra ve kişinin özel hayatının çekirdek alanına tecavüz edilmeden elde edilmeleri şartıyla ses ve görüntü kayıtlarının keşfe konu belirti delilini oluşturacağı kabul edilmelidir[79]. Özbek ve diğerleri ise belge delilleri arasında inceledikleri ses ve görüntü kayıtlarının tek başlarına mahkûmiyet için yeterli olmadıklarının kabul edilmesi durumunda belirti deliline yakın olduklarını vurgulamışlardır[80].

Yıldız'a göre de; ses ve görüntü kayıtları belge niteliğinde olmayıp esas olarak keşif konusudurlar. Mahkeme söz konusu kayıtları mahkemede dinlemek veya seyretmek suretiyle bunların duruşmada ortaya konulmasını ve bu suretle yargılamaya katılan diğer süjelerin de tartışma olanağını sağlamalıdır. Bundan elde edilen sonuca göre de vereceği hükümde bu kayıtları değerlendirmelidir. Bununla birlikte, duruşmada bu tür bir değerlendirme yoluna gidilmeyip de bu kayıtların içeriğinin yazıya dökülerek bunların duruşmada okunması cihetine gidilirse, bu durumda belge delilinden söz etmek mümkün olacaktır[81].

Koca'ya göre ise; esasen ceza muhakemesi hukuku bakımından, ses ve görüntü kaydının deliller içerisindeki yerinin tespit edilmesinden ziyade bunların ne kadar güvenilir ve hukuka uygun oldukları önem taşımaktadır. Zira bunların hukuka uygun şekilde elde edilmeleri durumunda, yargılamada delil olarak kullanılabileceklerinde kuşku bulunmamaktadır[82].

[78] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1387.

[79] Centel ve Zafer, s. 245.

[80] Veli Özer Özbek ve Diğerleri, **Ceza Muhakemesi Hukuku,** 5. Basım, Ankara: Seçkin Yayıncılık, 2013, s. 652.

[81] Ali Kemal Yıldız, Ses ve/veya Görüntü Kayıtlarının İspat Fonksiyonu, s. 258.

[82] Koca, Ceza Muhakemesi Hukukunda Deliller, s. 218.

1.4.2.4. Bilişim Verisi Şeklindeki Belge

6100 sayılı Hukuk Muhakemesi Kanunu m. 199'da elektronik veriler hukuken birer belge olarak kabul edilmelerine karşın[83] Ceza Muhakemesi Kanunu'nda bu şekilde açık bir hüküm bulunmamaktadır. Bununla birlikte CMK'nın çeşitli hükümlerinde bilişim sistemlerinden ve elektronik cihazlardan elde edilebilecek delillerden söz edilmektedir.

Bilişim sisteminde yer alan elektronik verilerin ne tür bir delil olduğu hususu ceza muhakemesi hukukunun önemli bir sorununu teşkil etmektedir. Özbek'e göre, elektronik veriler, yazılı olmamaları ve okunma kabiliyetleri bulunmamaları nedeniyle belge niteliğini haiz değildir. Elektronik ortamda kayıtlı bulunan verilerin tespitinin bilgisayar disketi veya CD ile yapılmakta olması hatta bir yazıcı ile yazdırılarak yazılı belge haline dönüştürülmesi ve böylece somut hale getirilmesi mümkün ise de bu durum elektronik verilere belge niteliği kazandırmamaktadır. Zira elektronik verilerin içeriğinin değiştirilebilmesine karşın bu verilerin değiştirilip değiştirilmediğinin anlaşılması mümkün değildir. Bu bakımdan, elektronik veriler, sadece kayıtlı olan aktüel içeriğin ispatını ortaya koydukları için bir belge delili olmayıp keşif konusu olan bir belirti delilidir[84].

Değirmenci, elektronik verinin niteliğine göre bir ayrım yapmaktadır. Buna göre; elektronik veri, bilişim sisteminin suçun işlenmesinde araç olarak kullanılması veya bilişim sisteminin suçun hedefi olması durumlarında belirti delilidir. Buna karşın elektronik veri, -hakaret içeren bir metnin bilgisayarda yazılması ve kaydedilmesinde olduğu gibi- bilişim sisteminin suçun delilini muhafaza etmekte kullanıldığı durumlarda ise belge delili niteliğindedir[85].

Kunter, Yenisey ve Nuhoğlu'na göre ise; bilişim sisteminde yer alan elektrik yükleri cihazlarla okunarak anlamlandırılabilmektedir. Bilişim teknolojisi içerisinde irade

---

[83] 6100 sayılı Hukuk Muhakemeleri Kanunu m. 199'da; "Uyuşmazlık konusu vakıaları ispata elverişli yazılı veya basılı metin, senet, çizim, plan, kroki, fotoğraf, film, görüntü veya ses kaydı gibi veriler ile elektronik ortamdaki veriler ve bunlara benzer bilgi taşıyıcıları bu Kanuna göre belgedir." hükmüne yer verilmiştir.

[84] Veli Özer Özbek, "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Cilt. 4, Sayı. 1, (2002), s. 143-144; Veli Özer Özbek, Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi, s. 186-188.

[85] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 393-394.

açıklaması içeren ve düzenleyeni teknik yöntemlerle tespit edilebilen bu tür veri grupları teknik anlamda "belge" niteliğindedir. Bu tür belgeler özellikle bilgisayarlardan yararlanarak ve bilgisayar programları (word, exel vb.) kullanılarak düzenlenir ve belli bir isim altında kaydedilerek bilgisayarın içinde saklanabilirler[86]. Bize göre de; çalışmamızın konusunu teşkil eden elektronik veriler, belge delili kategorisi içerisinde değerlendirilmelidir.

1.4.3. Belirti Delili

Belirti, ispat edilecek olayın dolaylı olarak ispatına yardımcı olan ve olaydan geriye kalan her türlü iz ve eseri ifade etmektedir[87]. Maddi gerçeğin araştırılması, her şeyin delil olması ve hâkimin delilleri serbestçe takdir edebilmesi ilkelerinin hâkim olduğu ceza muhakemesi hukukumuzda belirti, tartışmasız bir delil türüdür ve fevkalade bir önemi haizdir[88].

Bununla birlikte suç mahallinde bulunan ve atılı suça konu olabileceği değerlendirilen belirtilerin usulüne uygun biçimde toplanması, muhafaza edilmesi ve inceleme yapacak birime gönderilmesi gerekmektedir. Zira yalnızca güvenliği sonuna kadar sağlanabilmiş belirtilerin incelenmeleri doğru ve sağlıklı sonuçlar verebilir ve hâkime yargılamada yol gösterebilir. Aksi halde toplanmasından mahkeme huzuruna getirilmesi anına kadarki aşamalardan herhangi birinde güvenliğinden şüphe edilen belirti, diğer delillerde olduğu gibi, hâkime kanaat vermede yardımcı olamayacaktır[89].

Beyan ve belge delilleri somut olaya özgü olup bu somut olayı doğrudan doğruya temsil ve ispat eden delillerdir. Buna karşın, belirti delili ise olayı genel nitelikte temsil eden, somut olayın yanı sıra başka hususları da ispat edebilecek özellikteki dolaylı delillerdendir. Bununla birlikte olayı dolaylı olarak ispat edebilmeleri nedeniyle belirti

[86] Nurullah Kunter, Feridun Yenisey ve Ayşe Nuhoğlu, **Açıklamalı Ceza Muhakemesi Kanunu**, Cilt. I, İstanbul: Beta Yayınevi, 2013, s. 1324.

[87] Koca, Ceza Muhakemesi Hukukunda Deliller, s. 219.

[88] Bahri Öztürk, Yeni Yargıtay Kararları Işığında Delil Yasakları, s. 5.

[89] Cemal Öztürk, **Ceza Muhakemesinde İz Bilimi Kriminalistik Gerçeği,** Ankara: Seçkin Yayıncılık, 2006, s. 52.

delilinin ispat gücünün zayıf olduğundan söz edilemez. Bunun aksine, kriminalistik* biliminin verilerine göre değerlendirilecek olan belirti delili ispat gücü yüksek bilimsel delillerden kabul edilirler. Ancak, olayı doğrudan ispat etmediklerinden dolayı, bu delillerin her zaman tek başlarına kullanılmayıp genellikle başka delillerle desteklenmeleri gerekmektedir[90]. Ancak, belirtinin başka delillerle desteklenmesi yasal bir zorunluluk olmayıp mantık kurallarının bir sonucudur. Bu bakımdan hâkimin, belirti delili ile vicdani kanaatini oluştururken dikkatli olması gerekmektedir[91].

Belirti tabii ve sun'i olmak üzere iki şekilde nitelendirilebilir. Tabii belirti, olayın bir parçası olan ve suçu işleyenin iradesi dışında olayı doğal bir şekilde temsil eden delildir. Tabii belirtinin somut olayı temsil edip etmediği dikkatli bir şekilde araştırılmalıdır. Örneğin olay yerinden elde edilen parmak izi veya kan lekesi suçtan önce veya sonra meydana gelmiş olabilir. Bu bakımdan belirti delilinin bu gibi hallerde tek başına ispat gücü bulunmayabilir[92].

Tabii belirti, insan iradesi dışında olduklarından objektiftir. Bu itibarla, insan eseri olan beyan ve belge gibi delillere nazaran daha önemlidir. Ancak, bu sağlamlık, belirtinin şekil bakımından gerçekliği ile kaimdir. Diğer taraftan belirti, istenilerek veya istenilmeyerek değişebilir. Bu nedenle adli kolluğun bu durumu engellemek için gerekli tedbirleri alması gerekmektedir[93].

---

* Kriminalistik, suç ve suçlunun bilimsel yöntem ve araçlar kullanılarak tespit edilmesi, belirlenmesi, suçun aydınlatılması ve suç analizinin yapılmasını ifade eder. Bkz. Kaygısız, s. 2; Kriminalistik, bir bilim olmayıp bir tekniktir ve fizik, kimya ve biyoloji bu tekniğin temelini teşkil eder. Kriminalistiğin kendi değişmez kanunları yoktur. Uygulanacak kurallar ve teknolojideki gelişmeler kriminal incelemelerde büyük değişiklikler meydana getirir. Bkz. Hamit Hancı, Ayşim Tuğ ve Yeşim Doğan, "Kriminalistik Kriminoloji Değildir", **Türkiye Barolar Birliği Dergisi,** Sayı. 48, (2003), s. 262.

[90] Şahin ve Göktürk, s. 46; Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 125; Belirtinin ispata ulaşmakta tek başına yeterli olamayacağı ve mutlaka başka delillerle desteklenmesi gerektiği hususunda ayrıca bkz. Metin Feyzioğlu, "Belirtilerin Şüphenin Yenilmesindeki İşlevi ve Benzer İsnadlara Ait Delil Araçlarının Somut Olayın Çözümünde Birlikte Değerlendirilmesi", **Ankara Barosu Dergisi**, Sayı. 1, (2000), s. 21; Veli Özer Özbek, Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi, s. 182.

[91] Centel ve Zafer, s. 248.

[92] Toroslu ve Feyzioğlu, s. 196-197.

[93] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1393.

Sun'i belirti ise, failin iradesiyle veya bir insan tarafından belirli bir amaçla hazırlanmış olan nesnelere denir. Olay yerinde bulunan düğme, tabanca, bıçak veya taşınan şapka gibi nesneler sun'i belirti niteliğindedirler[94]. Tabii belirti ispat gayesi ile meydana getirilmediği halde sun'i belirtide gaye ispattır[95]. Bu bakımdan tabii belirtiye nazaran ispat gücü daha sınırlıdır[96].

1.5. Delil Serbestîsi İlkesi

Ceza yargılamasının konusu, geçmişte yaşandığı iddia olunan bir olaydır. Olayın gerçekleşip gerçekleşmediği, gerçekleşmişse ne şekilde meydana geldiği, olayla ilişkili kişiler, olayın ve kişilerin ceza hukuku bakımından durumu ceza yargılaması sürecinde araştırılmaktadır. Ayrıca, diğer bazı hukuk alanlarından farklı olarak ceza hukukunda ispat araçları önceden hazırlanmaz ve hatta genellikle suç gizlilik içinde işlenir ve deliller yok edilmek istenir[97].

CMK m. 217/1'e göre hâkim, kararını ancak duruşmaya getirilmiş ve huzurunda tartışılmış delillere dayandırabilir. Bu deliller hâkimin vicdani kanaatiyle serbestçe takdir edilir. Bu bakımdan ceza yargılamasında hangi durumda hangi delilin ispat aracı olarak kullanılacağı hususu belirli kurallara tabi kılınmamıştır. Hâkim, hangi delillere başvuracağını belirlemede ve bu delillerin takdirinde vicdani kanaatine göre hareket edecektir. Bu durum ülkemiz hukuk sistemi bakımından da geçerli olan vicdani delil sisteminin bir tezahürüdür.

Vicdani delil sisteminin iki sonucu ya da unsuru bulunmaktadır. Bunlardan birincisi, ceza yargılamasında kural olarak her şeyin delil olabilmesi, başka bir ifadeyle, kanuni ispat ve delil sisteminin bulunmaması; ikincisi ise, hâkimin, duruşmada ortaya

[94] Centel ve Zafer, s. 247-248.

[95] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1393.

[96] Yener Ünver ve Hakan Hakeri, **Ceza Muhakemesi Hukuku**, 2. Cilt, 7. Basım, Ankara: Adalet Yayınevi, 2013, s. 126.

[97] Şahin ve Göktürk, s. 17-18.

konulmuş olan delillerin serbestçe değerlendirilmesi sonucunda, vicdani kanaatini oluşturmasıdır[98].

Vicdani delil sisteminin özünde delillerin somut olayın ispatı bakımından, değerini hâkimin serbestçe takdir edecek olması yatmaktadır. Hâkim duruşmada tartışılan delillerin bazılarına daha çok değer vermek, bazılarına ise hiç değer vermemek serbestîsine sahiptir[99]. Bununla birlikte, hâkimin delilleri serbestçe değerlendirmesi ve vicdani kanaatine göre karar vermesi, keyfi hareket edebileceği anlamını taşımamaktadır. Hâkimin yapacağı değerlendirme akla ve mantığa uygun bir değerlendirme olmalıdır. Hâkim toplanan hangi delillere neden inanıp neden inanmadığını ve hangi delilleri hükme neden esas alıp almadığını açıklamak zorundadır[100]. Zira hâkimin delilleri isabetli değerlendirip değerlendirmediği hususu kanun yolu mercii tarafından denetime tabidir[101].

Bu bağlamda, ceza yargılamasında her şey delil olabilmekte, hâkim belli bir durumun sübuta erdiği yönündeki hükmünü, delilleri değerlendirerek, tam bir inanışla ve vicdani bir kanıya vararak verebilmektedir. Nitekim günümüzde de çağdaş ülkeler tarafından ceza yargılamasında vicdani delil sistemi benimsenmiş, belli durumların kanunlarda gösterilen delillerle ve hâkimi bağlayacak biçimde ispat edilmesi sistemini ifade eden kanuni ispat sistemi terk edilmiştir[102].

Kanuni ispat sisteminin geçerli olduğu dönemde, hâkimin delilleri değerlendirme serbestîsi bulunmamaktaydı. Kanunlarda hangi suçun hangi delillerle ispat edileceğine ve delillerin ispat gücüne ilişkin hükümler bulunmaktaydı. Ancak, hâkim, çoğu zaman sanığın suçu işlediği hususunda bir kanaate sahip olmasına rağmen kanunun öngördüğü sayı ve nitelikte delil bulunmaması nedeniyle mahkûmiyete hükmedememekteydi. Bugün ise, vicdani delil sisteminin bir sonucu olarak hâkim, soyut kanuni kurallarla

[98] Ali Kemal Yıldız, Ses ve/veya Görüntü Kayıtlarının İspat Fonksiyonu, s. 254.

[99] Öztunç, s. 89.

[100] Feyzioğlu, Ceza Muhakemesinde Vicdani Kanaat, s. 49.

[101] Ali Parlar, Muzaffer Hatipoğlu ve Erol Güngör Yüksel, **Açıklamalı-İçtihatlı Ceza Muhakemesi Hukukunda Deliller Çapraz Sorgu ve İspat,** Ankara: Yayın Matbaacılık, 2008, s. 9.

[102] Çınar, s. 39.

bağlı olmaksızın delilleri ve bunların olayı ispat gücünü serbestçe değerlendirebilmektedir[103].

Ceza yargılamasında, hukuk yargılamasının aksine, bazı hususların sadece bazı delillerle ispat edilmesi zorunluluğu kabul edilmemiştir. Ceza yargılamasında, ispat edilecek somut olay geçmişe ilişkin olduğundan ve bu olayların ortaya çıktığı zamanın ve şartların önceden bilinmesi mümkün olmadığından, bu nedenle de hukuk yargılamasında olduğu gibi deliller önceden hazırlanamadığından vicdani delil sisteminin bir sonucu olarak delil serbestîsi ilkesi benimsenmiştir[104].

Delil serbestîsi, kural olarak; ceza yargılamasında her şeyin delil olmasını, her şeyin her şeyle ispatlanabilmesini, her zaman delil ileri sürülebilmesini, delillerin serbestçe değerlendirilebilmesini ifade eder. Gerçekten de, ceza yargılamasında maddi gerçeğin araştırılıyor olması, vereceği kararın sorumluluğunu üstlenecek olan yargılama makamının delilleri serbestçe değerlendirmesini de zorunlu kılmaktadır. Böylece hâkim, kendisini gerçeğe götürecek yolda serbestçe yürüyebilmektedir[105].

Ceza yargılamasında, sadece duruşmanın akışının ispatıyla ilgili olarak kanuni delil sistemi benimsenmiş; kanunda, duruşmanın nasıl yapıldığının, kanunda belirtilen usul ve esaslara uygun olarak yapılıp yapılmadığının ancak tutanakla ispat olunabileceği kabul edilmiştir. Duruşmanın akışına ilişkin bir iddianın, duruşma tutanağı dışında başka bir delille ispat edilmesi mümkün değildir. Duruşma tutanağına karşı ise sadece sahtecilik iddiası ileri sürülebilir (CMK m. 222). Ancak, duruşmanın akışına ilişkin ispat konusu ceza yargılamasının konusunu teşkil eden ceza uyuşmazlığının ispatıyla ilgili bir konu değildir. Bu nedenle, bu husus, delil serbestîsinin bir istisnası olarak kabul edilemez[106].

Buna karşın, delil serbestîsinin istisnası olarak, hukuki uyuşmazlıklarla bağlantılı olan ceza uyuşmazlıklarının ispatı gösterilebilir. Zira boş çekin alacaktan fazla olarak

[103] Ali Kemal Yıldız, "Ceza Muhakemesinde İspat ve Delillerin Değerlendirilmesi", (**Yayınlanmamış Doktora Tezi,** İstanbul Üniversitesi SBE, 2002), s. 142-143.

[104] Toroslu ve Feyzioğlu, s. 170.

[105] Şahin ve Göktürk, s. 18-19.

[106] Centel ve Zafer, s. 191.

doldurulması sonucu oluşan güveni kötüye kullanma gibi bir takım hukuki uyuşmazlıklarla ilgili suçların ispatı için yazılı delil aranmaktadır[107].

Diğer taraftan, vicdani delil sistemini zayıflatacak ve zamanla onun yerini alacak olan bir sistem olarak bilimsel delil sistemi gösterilebilir. Gerçekten de, ceza yargılamasında kullanımı günden güne artan bilimsel deliller, delil serbestîsi ilkesinin sınırlarını zorlamaya başlamıştır. Belirti delili bunların başında gelmektedir. Nitekim öldürülen bir kişinin tırnakları arasında bulunan deri parçasının sanığa ait olduğu bilimsel olarak ispatlandığı bir durumda hâkimin bu durumu reddetmesi kolay olmayacaktır. Bununla birlikte, bilimsel incelemelerin bunun sanığa ait olabileceği yönünde ihtimale dayalı bir sonuç verdiği durumda ise hâkim sadece böyle bir delile dayanarak mahkûmiyet kararı veremeyecektir[108].

1.6. Hukuka Aykırı Deliller (Delil Yasakları)

1.6.1. Genel Olarak

Hukuk devleti ilkesinin temelinde yatan düşünce kolluk güçlerinin hukukun süjesi olması ve hukuk uyarınca sorumlu tutulabilmeleridir. Bunu başarmanın yolu ise, kontrol ve denge sistemi altında yetki dağılımı yapmaktan geçer. Ceza davası, yargı makamlarının hüküm ve ceza yoluyla ceza kanununu uygulamakla sorumlu tutulduğu sistemin önemli bir unsurunu teşkil etmektedir. Mahkemenin rolü ise bu işin hukuka uygunluğunu araştırmaktır[109].

Ceza mevzuatında suç olarak nitelendirilen eylemler, vatandaşların sahip oldukları en önemli hakları ihlal etmektedir. Bir hukuk devleti, insan haklarını korumanın yanı sıra adaleti tesis etmek ve güvenliği sağlamak ve de bu suretle suçlulukla mücadele etmek mecburiyetindedir. Bununla birlikte, birçok olayda suç faillerinin kimler olduğunun

---

[107] Öztunç, s. 90.

[108] Hikmet Şen, "Bilimsel Yöntemlerle Elde Edilen Delillerin Hukuka Aykırılığı Sorunu ve Bağlayıcılığının Değerlendirilmesi", **Adalet Dergisi,** Sayı. 34, (Mayıs 2009), s. 115; Bahri Öztürk (Ed.), Nazari ve Uygulamalı Ceza Muhakemesi Hukuku Ders Kitabı, 7. Basım, s. 384.

[109] Hock Lai Ho, "Ceza Davasında Hukuka Aykırı Elde Edilen Delilin Yasaklanması Kuralı", Doruk Özgündüz (Çev.), Yener Ünver (Ed.), **Ceza Muhakemesi Hukukunda Delil ve İspat** içinde (85-111), Ankara: Seçkin Yayıncılık, 2014, s. 108.

bilinmemesi yüzünden suçlularla mücadele çerçevesinde alınan bazı tedbirler olayla hiç bağlantısı olmayan kişileri de doğrudan veya dolaylı şekilde etkilemesi nedeniyle suç ve suçlularla mücadelede kişilerin haklarını ihlal edebilmektedir. Bu bakımdan suç ve suçlularla mücadelede devletin zor kullanma yetkisi ve görevinin icrası sırasında özenli ve ölçülü davranılması gerekmektedir. İşte delil yasakları, bu ölçünün belirlenmesinde kullanılan araçların başında gelir. Bu nedenle delil yasakları insan hakları ile iç içe olan önemli ve teknik bir konudur[110].

Ceza yargılaması, fert çıkarları ile toplum çıkarlarının birbirleriyle çatışma halinde oldukları bir alanda işlev görmektedir. Bireyi toplum adına cezalandıran devlet, delil toplama ve değerlendirme faaliyeti sırasında bireyin temel haklarına saygılı olmak ve hukuka uygun davranmak zorundadır. Bir hukuk devletinde devletin bütün işlemlerinin hukuka uygun olması gerektiği gibi ceza yargılamasında kullanılacak delillerin de hukuka uygun elde edilmesi gerekmektedir. Bu nedenlerle, insan hakları ihlallerinin önlenmesi ve bazı kişisel ve toplumsal değerlerin korunması amacıyla devletin delil toplama ve değerlendirme faaliyetine bazı sınırlamalar getirilmesi ihtiyacı duyulmuştur[111].

Delillerin sınırsız ve değişik usul, yol ve yöntemlerle elde edilmesi ve uyuşmazlıkların bu delillerle çözülmesi, birçok bireysel ve toplumsal değerin ihlali sonucunu doğurabilir. Bu bakımdan, ancak hukuka uygun yol ve yöntemlerle elde edilmiş delillere dayanılarak bir sonuca ulaşılması gerekmektedir. Başka bir ifadeyle, delil elde edilmesi ve değerlendirilmesi işlemlerine ceza yargılamasında sınır getirilmekte ve bu sınırlamalara ise delil yasakları denilmektedir[112].

Delil yasakları, etkin bir cezai tatbikat amacıyla kullanılan her aracın meşru olup olmadığı veya bir hukuk devletinde somut olayın soruşturulmasının herhangi bir sınırı olup olmadığı hususunu ilgilendirdiğinden dolayı adalet duygusuna doğrudan temas

[110] Bahri Öztürk (Ed.), Nazari ve Uygulamalı Ceza Muhakemesi Hukuku Ders Kitabı, 7. Basım, s. 392.

[111] Öztunç, s. 135.

[112] Şahin ve Göktürk, s. 74-75.

eden az sayıdaki ceza muhakemesi kurumlarından birisidir [113] . Delil yasakları müessesesi, insan hakları ile temel hak ve hürriyetleri korumak amacıyla oluşturulmuştur. Delil elde etmenin sınırları, hukukun genel ilkeleri ve yasalarla kabul edilmiştir[114].

Nitekim Yargıtay Ceza Kurulu'nun bir kararında da *"1412 sayılı Ceza Muhakemeleri Usulü Kanununun 254. maddesinin birinci fıkrasında; 'Mahkeme irat ve ikame edilen delilleri, duruşmadan ve tahkikattan edineceği kanaate göre takdir eder.' denilmekle, yargılama sürecinde sunulan ve toplanan kanıtlardan çıkarım yapılması yargıçların takdirine bırakılmıştır. Ancak hem 'delil serbestîsi' hem de 'delillerin yargıçların kanaatine göre takdir edilmesi' ilkelerinin belli sınırları bulunmaktadır. Bunlardan biri de, mahkemenin, ancak hukukun izin verdiği yöntemlerle elde edilen delilleri dikkate alabilecek olmasıdır. Başka bir deyişle, hukuk düzeninin yasakladığı yöntemlerle toplanan deliller mahkemece dikkate alınamazlar[115]."* hükmüne yer verilmiştir.

Bu bakımdan delil yasakları kavramı, hem hukuka aykırı şekilde delil elde etme yasağını, hem de bu şekilde elde edilen delilin kovuşturma makamlarına sunulması ve değerlendirilmesi yasaklarını ihtiva etmektedir.

1.6.2. Hukuka Aykırı Delillerin Değerlendirilmesi

Ceza yargılamasında usulüne uygun olarak elde edilmeyen delillerin ortaya konması, değerlendirilmesi ve hükme esas alınması hususlarının kabul edilmemesi prensibine delil değerlendirme yasağı denilmektedir. Hukuka aykırı delillerin ceza yargılamasında değerlendirmeye alınıp alınmayacağı ise delil yasakları ile ulaşılmaya çalışılan amacın tespiti ile doğrudan bağlantılıdır.

Delil yasaklarının amacının ne olduğuna ilişkin iki temel görüş mevcuttur. Birinci görüşe göre, delil yasaklarının amacı, Anglo-Amerikan hukuk sisteminin de kabul ettiği

---

[113] Sabine Gless, "Delil Yasakları ve Uzak Etki", Kerem Öz (Çev.), Yener Ünver (Ed.), **Ceza Muhakemesi Hukukunda Delil ve İspat** içinde (345-359), Ankara: Seçkin Yayıncılık, 2014, s. 345.

[114] M. Serhat Kaşıkara, "Ceza Muhakemesi Hukukunda Delil Elde Etme Yasakları", **Ceza Hukuku Dergisi (CHD),** Sayı. 10, (Ağustos 2009), s. 188.

[115] Yargıtay CGK. 29.11.2005. E. 2005/7-144, K. 2005/150 (**Yargıtay Kararları Dergisi,** Cilt. 32, Sayı. 3, Mart 2006), s. 468.

üzere, kolluğu disiplin altına almaktır. İkinci görüşe göre ise delil yasaklarının amacı temel hak ve özgürlükleri korumaktır[116].

Delil yasaklarının amacının kolluğu disiplin altına almak olduğu kabul edildiğinde, kolluğun tekrar hukuka aykırı yöntemlere başvurmasının önüne geçmek amacıyla hukuka aykırı şekilde elde edilen tüm deliller yargılamada değerlendirilmeyecektir. Ancak, delil yasaklarının amacının temel hak ve özgürlükleri korumak olduğu kabul edildiği takdirde hukuka aykırı şekilde elde edilen deliller sadece bu nedenle ve peşinen değerlendirme dışı tutulmayacaktır[117].

Bu bağlamda, elde edilen delillerin hukuka aykırı olduğu belirlendikten sonra, bu delillerin değerlendirme yasağı kapsamında olup olmadığının tespitinde üç yaklaşım tarzı benimsenmektedir. Bunlar kesin kabul yaklaşımı, kesin ret yaklaşımı ve esnek yaklaşımdır.

1.6.2.1. Kesin Kabul Yaklaşımı

Kesin kabul yaklaşımı, hukuka aykırı şekilde elde edilen delillerin akıbeti hakkında kabul edilen en eski görüştür. Bu yaklaşım, elde edilen delilin yargılamaya konu olan uyuşmazlıkla ilgili ve olayın açıklığa kavuşturulmasında yararının bulunması halinde bu delilin nasıl elde edildiğini araştırma ihtiyacı duyulmaksızın hükme esas alınabilmesini kabul eden yaklaşım tarzını ifade etmektedir[118].

1.6.2.2. Kesin Ret Yaklaşımı

Kesin ret yaklaşımı, sanığın önceden belirlenmiş kurallar çerçevesinde yargılama hakkının bulunması nedeniyle önceden belirlenmiş kurallara uyulmaksızın ve usule uygun olmayan yöntemlerle elde edilen delillerin hiç bir şekilde hükme esas alınmaması gerektiğini ifade eden yaklaşım biçimidir.

---

[116] Bahri Öztürk, Yeni Yargıtay Kararları Işığında Delil Yasakları, s. 9.

[117] Seydi Kaymaz, **Uygulama ve Teoride Ceza Muhakemesinde Hukuka Aykırı (Yasak) Deliller**, Ankara: Seçkin Yayıncılık, 1997, s. 249.

[118] Şafak ve Bıçak, s. 139.

Kesin ret yaklaşımına yöneltilen en büyük eleştiri, bu yaklaşım kabul edildiğinde sanığın mahkûmiyetine yol açabilecek delillerin reddine ve dolayısıyla mahkûmiyetle sonuçlanabilecek kimi suçların aklanmasına neden olmasıdır. Ancak bu konuda Amerika Birleşik Devletleri'nde yapılan bir araştırmada, kesin ret yaklaşımının uygulandığı davaların sayısının toplam davaların %1'i gibi bir orana isabet ettiği ve dolayısıyla kesin ret yaklaşımının çok ciddi olumsuz sonuçlar doğurmadığı ileri sürülmüştür[119].

Kesin ret yaklaşımı, katı bir biçimde uygulanması durumunda çok basit, teknik bazı usulsüzlükler sonucunda sanıkların serbest kalmasına yol açacağı, bu durumun halkın hukuk ve yargı sistemine olan saygısını azaltacağı ve hukuk sisteminin itibarının zedeleneceği, diğer taraftan basit bir hukuka aykırılık nedeniyle yargılamanın kilitlemesinin yalnızca şüpheli veya sanığın haklarının korunması açısından değerlendirilmesi durumunun kamu yararı ile fert yararı arasında kurulması gereken dengenin gözetilmemesi sonucunu doğuracağı gerekçeleriyle eleştirilmektedir[120].

1.6.2.3. Esnek Yaklaşım

Esnek yaklaşım, hukuka aykırı olarak elde edilen delilin kabul edilebilirliğine karar vermede, kabul etme ya da reddetme şeklinde sabit bir kural kabul etmek yerine, mahkemenin her davada birey ve toplumun yarışan menfaatlerini göz önünde tutmak suretiyle bu iki alternatif arasında karar vermesi gerektiğini benimsemektedir. Bu yaklaşıma göre; mahkemelere açıkça takdir hakkı tanınmalıdır[121].

Kesin kabul ve kesin ret çözümleri ceza yargılamasında iki farklı yaklaşımı yansıtmaktadır. Bunlardan birincisi maddi gerçeğin bulunmasının ve suçluların cezalandırılmasının ceza yargılamasının en önemli amacı olduğunu vurgulayan faydacı yaklaşımdır. İkincisi ise delil elde etmek amacıyla düzenleyen normların korunmaları

---

[119] İbrahim Şahbaz, "Karşılaştırmalı Hukukta ve Avrupa İnsan Hakları Mahkemesi Kararlarında Hukuka Aykırı Deliller", **Ankara Barosu Dergisi**, Sayı. 1, (2006), s. 105-106.

[120] Timur Demirbaş, **Sanığın Hazırlık Soruşturmasında İfadesinin Alınması**, İzmir: Dokuz Eylül Üniversitesi Döner Sermaye İşletmesi Yayınları, 1996, s. 259 vd.; Bıçak, s. 530.

[121] Mahmut Koca, "Ceza Muhakemesinde Hukuka Aykırı Delilleri Değerlendirme Yasağı", **Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi (AÜEHFD)**, Cilt. IV, Sayı. 1-2, (2000), s. 116.

gerektiğinin ve bu ihtiyacın suçluların cezalandırılması gibi diğer birtakım amaçların önüne geçebileceğini vurgulayan moral yaklaşımdır. Kesin kabul ve kesin ret yaklaşımları arasındaki uyuşmazlığın tam olarak çözülememiş olması ve hukuk sistemlerinin bu iki yaklaşımdan birini diğerine tercih edememeleri, sorunun ancak hâkime takdir hakkı veren esnek yaklaşımla çözülebileceği kanaatinin ağırlık kazanmasına neden olmaktadır[122].

Nitekim Avrupa İnsan Hakları Mahkemesi'nin de takdir hakkını hâkime veren çözüm yolunu benimsediği görülmektedir. Buna göre; Avrupa İnsan Hakları Sözleşmesi'nde hukuka aykırı delillerin değerlendirilmesi hususunda herhangi bir düzenleme bulunmamaktadır. Avrupa İnsan Hakları Mahkemesi'nin vermiş olduğu kararlarda ise hukuka aykırı elde edilmiş delillerin hukuki değerlendirmesi konusunda ilke teşkil edecek genel bir kural koymadığı görülmektedir.

Avrupa İnsan Hakları Mahkemesi'nin bu konuyla ilgili vermiş olduğu bir kararında (Kostovski/Fransa, 20.11.1989); *"Mahkemeye göre sunulan delillerin gerekliliği konusunda karar yetkisi öncelikle bir iç hukuk sorunudur ve toplanan delillerin ispat gücünü takdir de, ilke olarak, ulusal mahkemelerin yetkisindedir. Mahkemenin işlevi ise, ispat araçlarının sunuluş tarzı da dâhil olmak üzere, yargılamanın, bütünü bakımından, adil olup olmadığını araştırmaktır[123]"* hükmüne yer verilmiştir.

Avrupa İnsan Hakları Mahkemesi'nin başka bir kararında (Schenk/İsviçre, 12.07.1988); "*Sözleşmenin 6. maddesi ile adil yargılama hakkının güvenceye alındığını, 6. maddede yer alan hak ve özgürlüklerin doğrudan çiğnenmemesi koşulu ile Sözleşmede delillerin hukuki geçerliliği konusunda herhangi bir hükmün bulunmadığını ve bunun yerel mahkemelerin görevi olduğunu (paragraf 46)"* belirtmiş ve "*başvurucunun savunma hakkının da kısıtlanmadığı somut olayda adil yargılama ilkesinin doğrudan ihlalinin söz konusu olmadığına (paragraf 47-49)"* hükmetmiştir. Mahkemenin konuyla ilgili verdiği başka bir kararda (Khan/İngiltere, 12.05.2000) ise; *"yerel polisin uygulamış olduğu gizli dinleme tedbirinin, 'yasa ile öngörülmüş olma' koşulunu içermemesi nedeniyle*

[122] Bıçak, s. 530-531.

[123] A. Şeref Gözübüyük ve Feyyaz Gölcüklü, **Avrupa İnsan Hakları Sözleşmesi ve Uygulaması Avrupa İnsan Hakları Mahkemesi İnceleme ve Yargılama Yöntemi**, 9. Basım, Ankara: Turhan Kitabevi, 2011, s. 306.

Sözleşme'nin özel hayata saygı hakkını koruyan 8. maddesinin ihlal edildiğine (paragraf 27-28)" ancak *"bu yolla elde edilen delilin kullanılması açısından genel olarak bütün yargılama sürecinin adil olması gerektiğini belirterek bu yönde bir ihlal bulunmadığı gerekçesiyle 6. maddeye ilişkin başvurunun reddine (paragraf 38-40)*[124] *"* karar vermiştir.

İngiliz hukuk sisteminde hukuka aykırı elde edilen delillerin değerlendirmeye esas alınıp alınmayacağı konusunda esnek yaklaşımı benimsediği görülmektedir. Ortak hukuk (common law) sistemi de hukuka aykırı elde edilen delilin değerlendirme dışında bırakılması hususunun hâkimin takdirinde olması gerektiğini benimsemekteydi. Bununla birlikte, 1984 tarihli Polis ve Suç Delili Kanunu (Police and Criminal Evidence Act-PACE) hukuka aykırı elde edilen delilin kabul edilebilirliği hususunu düzenlemiştir. Bu düzenlemede konuya ilişkin üç hüküm bulunmaktadır. PACE m. 76 itirafların kabul edilebilirliğine ilişkindir. PACE m. 78 genel olarak dürüst olmayan delilin değerlendirme dışı tutulmasını ele almaktadır. PACE m. 82 ise Ortak hukuk sisteminin delili değerlendirme dışı tutma konusundaki takdirilik kuralını muhafaza etmektedir[125].

Alman Federal Mahkemesi'nin geliştirmiş olduğu "Haklar çevresi" teorisinin de esnek yaklaşımı benimsediği söylenebilir. Buna göre; hukuka aykırı delillerin değerlendirilmesinde öncelikle ihlal edilen hakkın niteliğine bakmak gerekmektedir. Delilin elde edilmesi sırasında uyulması gereken kurallar yüzünden sanığın önemli hakları ihlal edilmişse, hukuka aykırı deliller değerlendirilmeyecektir. Buna karşın, kuralların ihlali sanığın hakları bakımından önem taşımıyorsa, delil hukuka aykırı olmasına rağmen yargılamada kullanılacaktır. Bu hususta bir değerlendirme yapılırken ihlal edilen kuralın koruduğu hukuki çıkarın, yani yasal düzenlemenin kimin menfaati için yapıldığı da değerlendirilmelidir[126].

[124] Güçlü Akyürek, "Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu", **Türkiye Barolar Birliği Dergisi**, Sayı. 101, (Temmuz-Ağustos 2012), s. 69.

[125] Koca, Ceza Muhakemesinde Hukuka Aykırı Delilleri Değerlendirme Yasağı, s. 119-120.

[126] Kaymaz, s. 261.

1.6.2.4. Türk Hukuk Sistemindeki Durum

Türk hukuk sisteminde yürütülmekte olan bir yargılamada hukuka aykırı delillerin değerlendirmeye esas alınıp alınmayacağına ilişkin hangi yaklaşımın benimsendiği hususunda mevzuatta bulunan bazı hükümler dikkate alınarak bir kanaate varmak mümkündür. Buna göre; Anayasa m. 38/6'da kanuna aykırı elde edilmiş bulguların delil olarak kabul edilmeyeceği öngörülmektedir. Diğer taraftan, CMK m. 206/2-a'da kanuna aykırı olarak elde edilen delillerin duruşmada ortaya konamayacağı, CMK m. 217/2'de isnat edilen bir suçun ancak hukuka uygun şekilde elde edilmiş delillerle ispat edilebileceği, CMK m. 230/1'de ise mahkûmiyet hükmünün gerekçesinde, delillerin tartışılması ve değerlendirilmesi, hükme esas alınan ve reddedilen delillerin belirlenmesi; bu kapsamda dosya içerisinde bulunan ve hukuka aykırı yöntemlerle elde edilen delillerin ayrıca ve açıkça gösterilmesi gerektiği düzenlenmiştir.

Öğretide, Anayasa'da "kanuna aykırı" kavramının kullanılmış olması nedeniyle esnek yaklaşımın benimsendiği ileri sürülmüş, bu bağlamda, kanun dışında kalan diğer hukuksal metinlerde yer alan delil elde etmeye ilişkin normların (uluslararası sözleşme, kanun hükmünde kararname, tüzük, yönetmelik hatta genelge ve tebliğ) ihlali durumunda elde edilen delillerin değerlendirme dışı kalacağı ifadesinin bulunmaması nedeni ile Anayasa'daki düzenlemenin kesin ret yaklaşımını benimsemediği belirtilmiştir[127].

CMK'da kullanılan kavramlar da Türk hukukunda kesin ret yaklaşımının benimsendiği sonucunu doğurmamaktadır. "Kanuna aykırı" kavramıyla ilgili yukarıdaki Anayasal normla ilgili belirtilen hususlar CMK açısından da geçerlidir. CMK'da ifade edilen "hukuka aykırı" kavramı, usulsüz elde edilen bir delilin otomatik olarak hukuk düzeninin bütününe aykırı elde edildiği sonucuna götüremeyecek niteliktedir. "Hukuka aykırılık" kavramı, bünyesinde "hukuka uygunluk nedenlerini" de barındırmaktadır. Delil elde etmeye yönelik herhangi bir normun ihlali hukuk düzeninin bütününe aykırılık teşkil etmeyebilir. Bir başka ifadeyle, esnek yaklaşımda dikkate alınması

[127] Bıçak, s. 540; Soyaslan'a göre ise; "kanun" teriminden anlaşılması lazım gelen teknik anlamda kanundan başka, Anayasa, usulüne göre onaylanmış uluslararası sözleşmeler, kanun hükmünde kararnameler, kararlar ve yönetmeliklerdir. Bu bağlamda kanun teriminde kastedilen şekli anlamda kanun, yani yazılı kurallar olup maddi anlamda kanun değildir. Bkz. Doğan Soyaslan, "Hukuka Aykırı Deliller", **Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi (AÜEHFD)**, Cilt. 7, Sayı. 3-4, (Aralık 2003), s.12.

gereken faktörler olarak ortaya konulan hususlar, usulsüz ulaşılan deliller açısından "hukuka uygunluk nedenleri" görevini ifa edebilir. Bu bakımdan, "mevzuata aykırı elde edilen deliller hükme esas alınamaz" veya "usulsüz ulaşılan deliller hükme esas alınamaz" şeklinde bir hüküm ancak kesin ret kuralının benimsendiği sonucunu doğurabilir. Bu bakımdan Anayasa ve yasalardaki mevcut hükümler Türk hukukunda kesin ret yaklaşımın benimsendiğini iddia etmeye imkân tanımamaktadır[128].

Gerçekten de, soruşturma evresinde kolluk tarafından gerçekleştirilen ve herhangi bir temel hak ve özgürlüğe zarar vermeyen basit bir hukuka aykırılığın yargılamayı kilitlemesi muhakeme tekniğine uygun değildir. Zira muhakeme tekniği bakımından tek taraflı düşünülerek sadece sanığın korunmaya çalışılması, bir hukuk devletinde yargılamanın yapılabilmesinde bulunması gereken kamu yararı ile fert yararı arasındaki oranlılık (ölçülülük) ilkesi[*] esaslarına göre belirlenmesi gereken makul oranın göz ardı edildiği anlamını taşıyacaktır[129].

Diğer taraftan, herhangi bir hakkın ihlal edilmediği her türlü basit şekli hukuk ihlalinin mutlak bozma sebebi sayılması uzun vadede son derece ağır sonuçların doğmasına da neden olabilir. Delil elde edilirken soruşturma ve kovuşturma makamlarınca yapılan basit şekli aykırılıklar güçlükle elde edilen ve son derece önemli olan başka delilleri de kullanılamaz hale sokarak yargılamanın akim kalmasına neden olabilir. Bu durum, insan haklarını ihlal etmeden maddi gerçeğe ulaşmaya çalışan ceza yargılaması tekniğine uygun düşmemektedir[130].

Bir hukuk devletinde, devletin tüm işlem ve eylemlerinin hukuka uygun olması gerekmekte ise de; hata yapmanın insanlara özgü bir durum olmasının gereği insanlar tarafından yerine getirilen bu işlem ve eylemlerde hata yapılması normal bir durumdur. Ceza yargılaması uygulamasında da, özellikle delil elde edilirken zaman zaman hukuka

---

[128] Bıçak, s. 540.

[*] Ceza muhakemesi hukukunda oranlılık (ölçülülük) ilkesi, bir ceza muhakemesi işleminin yapılması ile sağlanması beklenen yarar ve ortaya çıkması olası zarar arasında makul bir oranın (ölçünün) bulunmasını, oransızlık durumunda ise işlemin yapılmamasını ifade etmektedir. Bkz. Veli Özer Özbek, **Ceza Muhakemesi Hukukunda Koruma Tedbiri Olarak Arama**, Ankara: Seçkin Yayıncılık, 1999, s. 33.

[129] Bahri Öztürk, Yeni Yargıtay Kararları Işığında Delil Yasakları, s. 10.

[130] Bahri Öztürk (Ed.), Nazari ve Uygulamalı Ceza Muhakemesi Hukuku Ders Kitabı, 7. Basım, s. 402.

aykırılıklar yapılabilmektedir. Adli kolluğu bulunmayan ülkelerde bu hukuka aykırılıklar daha sık ve yaygın şekilde görülebilmektedir. Temel hak ve özgürlükleri ihlal etmeyen basit bir hukuka aykırılık nedeniyle elde edilen önemli delillerin kullanılamaması veya bu delillerin hükme esas alınmaması, insan haklarını fiilen gerçekleştirmek yanında suçlarla mücadele etmek, sosyal disiplini ve hukuki barışı sağlamak mecburiyetinde olan bir hukuk devletinde kabul edilemez[131].

Bu bağlamda, Anayasa ve CMK'da belirtilen hükümlerin kesin bir yasak şeklinde değerlendirilmesi çok da olası gözükmemektedir. Zira hukuka aykırı şekilde delil elde etme hususu çok kapsamlı bir mesele olup bu konuda doğrudan bir ilke konulması zordur. Bu nedenle, yüksek mahkemelerinin ilk safhada ampirik yöntemlerle söz konusu hükümleri her olaya göre yorumlayarak uygulamaları, daha sonraki safhada ise bu uygulamadan hareketle bir ilkeye varmaları gerekmektedir[132].

Yargıtay Ceza Genel Kurulu bir kararında; *"CMUK'un 254/2 maddesi ile CMUK'un yasak sorgu yöntemleri kullanılarak elde edilen deliller dışında kalan diğer hukuka aykırı deliller için genel bir değerlendirme yasağı getirilmiştir. Ancak bu hüküm, delilin elde edilmesindeki her türlü hukuka aykırılığın, o delilin değerlendirme kapsamı dışında tutulmasını gerektireceği biçiminde yorumlanmamalıdır. Zira insan haklarını korumak amacıyla gerçekleştirildiği anlaşılan CMUK'un 254/2 maddesindeki değişiklik, hukuk devleti ilkesinin diğer iki unsuru olan adaleti ve hukuki güvenliği gerçekleştirmeyi engellememelidir. Nitekim doktrinde de, elde edilen delillerin basit hukuka aykırılıklar nedeniyle değerlendirme dışında tutulmasının, haksız beraat kararlarının verilmesine ve yargılamanın kilitlenmesine neden olabileceği ifade edilmiştir. O halde, anılan hükmün uygulanmasında yargıcın takdir yetkisini kullanabilmesi mümkündür. Yargıç, yasaklanmış deliller dışında, takdir yetkisini kullanıp değerlendirme yaparken, delil elde edilmesi faaliyeti sırasında ihlal edilen kurallar nedeniyle sanığın haklarının ihlal*

[131] Bahri Öztürk, Yeni Yargıtay Kararları Işığında Delil Yasakları, s. 29.

[132] M. Tevfik Odman, "Askeri Yargıtay'ın Hukuka Aykırı Deliller Korusunda Verdiği Kararlar", **Askeri Adalet Dergisi,** Sayı. 95, (Ocak 1996), s. 31.

edilip edilmediğine bakmalı, sanığın haklarının ihlal edilmediği hallerde, hukuka aykırı şekilde elde edilen delilleri yargılamada kullanabilmelidir[133]*."* hükmüne yer vermiştir.

Yargıtay Ceza Genel Kurulu'nun Cumhuriyet savcısı hazır olmaksızın bir iş yerinde yapılan aramada o yer ihtiyar heyeti veya komşulardan iki kişi bulundurulmaksızın yapılan bir aramada elde edilen delillerin hukuka aykırı olup olmayacağına ilişkin verdiği bir kararında ise; *"Usulüne göre alınmış arama kararına istinaden, herhangi bir hak ihlaline neden olunmadan yapılan arama sonunda ele geçen delillerin, sırf arama sırasında bulunması gereken kişilerin orada bulundurulmaması suretiyle şekle aykırı hareket edildiğinden bahisle hukuka aykırı olarak elde edilmiş delil sayılmaları ve mahkûmiyet hükmüne dayanak teşkil edilmemeleri kabul edilemez*[134]*."* şeklindeki gerekçeyle sanığın mutlak delil yasakları kapsamındaki temel hak ve hürriyetlerinin ihlal edilmediği, şekli aykırılıkların varlığı halinde ise hâkimin oranlılık ilkesi çerçevesinde kamu yararı açısından bir değerlendirme yapması gerektiği, elde edilen delillerin sadece şekli aykırılıkların varlığı nedeniyle hukuka aykırı olarak elde edilmiş delil sayılmalarının kabul edilemeyeceği vurgulanmıştır.

Anayasa Mahkemesi'nin ise delil yasakları konusunu daha katı bir biçimde değerlendirdiği görülmektedir. Buna göre Anayasa Mahkemesi delil yasaklarının amacına vurgu yaptığı bir kararında *"Söz konusu delil yasağı artık sadece içtihadi bir ilke veya kural olmayıp yasal bir hükümdür. Hukuka aykırı delillerin davalarda kullanılmasına yasak getirilmesinin amacı, sanığın Anayasa teminatı altına alınmış olan haklarının ihlal edilmemesidir. ..... Özet olarak, Türk hukuk sisteminde 'hukuka aykırı şekilde' elde edilen deliller hiçbir şekilde kullanılamaz. Hukuka aykırılıktan kasıt ise tüm pozitif hukuk kuralları ile birlikte hukukun kabul edilmiş evrensel ilkelerine aykırılıktır. Bu anlamıyla 'hukuka aykırı şekilde elde edilen deliller', 'yasal olmayan yöntemlerle elde edilen deliller' kavramından yani 'yasa dışılıktan' da geniş bir içeriğe sahiptir.*[135]*"* hükmüne yer vermiştir.

---

[133] Yargıtay CGK. 15.03.2005. E. 2005/10, K. 2005/15 (UYAP).

[134] Yargıtay CGK. 26.06.2007. E. 2007/7-147, K. 2007/159 (UYAP), Yargıtay CGK 13.03.2012. E. 2011/8-278, K. 2012/96 sayılı Kararında da aynı sonuca varılmıştır (UYAP).

[135] Anayasa Mahkemesi. 22.06.2001. E. 1999/2, K. 2001/2 (Anayasa Mahkemesi Kararlar Dergisi, Cilt. 2, Sayı. 37, 2002, s. 983, 985).

Bununla birlikte Anayasa Mahkemesi daha yeni tarihli bir kararında ise; "*Ceza yargılamasının temel amacı maddi gerçeğe ulaşmaktır. Çağdaş hukuk sistemlerinde, hukuka aykırı delillerin ceza yargılamasında hükme esas alınıp alınamayacağı hususunda iki ayrı görüş bulunmaktadır. Bunlardan birincisine göre, maddi gerçeğin ortaya çıkarılmasındaki kamu yararı ile kişinin hukuka aykırı olarak delil toplanması sırasında ihlal edilen hakkının dengelenmesi, kamu yararının ağır basması hâlinde hukuka aykırı olarak toplanmış olan delillerin hükme esas alınması, aksi hâlde bunların hükme esas alınmaması gerekir. İkinci görüşe göre ise delillerin hukuka aykırı olarak toplanması sırasında kişilerin temel hak ve hürriyetlerinin ihlal edilip edilmediği, maddi gerçeğin araştırılmasındaki kamu yararının ağırlığı dikkate alınmaksızın elde edilen hukuka aykırı deliller hükme esas alınmamalıdır.*

Anayasa'nın 38/6 maddesinde, 'Kanuna aykırı olarak elde edilmiş bulgular delil olarak değerlendirilemez.'; 5271 sayılı Kanun'un 217/2 maddesinde, 'Yüklenen suç, hukuka uygun bir şekilde elde edilmiş her türlü delille ispat edilebilir' denilmiştir. Aynı Kanun'un 206/2 maddesinde, ortaya konulması istenilen bir delilin kanuna aykırı olarak elde edilmiş olması hâlinde reddolunacağı; 230/1 maddesinde ise mahkûmiyet hükmünün gerekçesinde hükme esas alınan ve reddedilen delillerin belirtileceği, bu kapsamda dosya içerisinde bulunan ve hukuka aykırı yöntemlerle elde edilen delillerin ayrıca ve açıkça gösterileceği kurala bağlanmıştır. Söz konusu kurallar dikkate alındığında, hukukumuzda toplanmaları sırasında kişilerin temel hak ve özgürlüklerinin ihlal edilip edilmediğine bakılmaksızın hukuka aykırı delillerin ceza yargılamasında kullanılması yasaklanarak ikinci görüşün benimsendiği anlaşılmaktadır. Bununla birlikte doktrinde ve kimi Yargıtay Ceza Genel Kurulu kararlarında belirtildiği üzere, delillerin toplanması için yapılan işlemlerin geçerliliğini etkilemeyen şekle ilişkin basit usul hatalarının bu kapsamda değerlendirilmemesi gerekir[136]*."* hükmüne yer vermek suretiyle basit usul hatalarının delil yasakları kapsamında değerlendirilemeyeceği görüşünü benimsemiştir.

Gerçekten de, kanun koyucunun delil elde edilmesi amacıyla arama tedbiri hakkında yapmış olduğu düzenlemede kolluğun iradi olarak bu arama tedbirinde eksik kişi

[136] Anayasa Mahkemesi (Yüce Divan). 19.12.2012. E. 2011/1, K. 2012/1, http://www.anayasa.gov.tr/files/yuce_divan_2011.doc (08 Aralık 2014).

bulundurması düşünülemez. Nitekim usulüne uygun alınmış bir hâkim kararı ile arama yapan kolluğun hukuka aykırı olarak delil elde etmek kast ve iradesiyle hareket ettiği de düşünülemez. Bu bakımdan kolluğun soruşturma için önem arz edecek nitelikteki bir delili iradi olarak hukuka aykırı elde etmek istediği söylenemez. Ancak şüphelinin kaçacak olması, delillerin kaybolma olasılığının bulunması, zaman darlığı gibi çeşitli nedenler ile kolluğun arzu etmemesine rağmen delilin elde edilişinde kusurlu davrandığı söylenebilir[137].

Bu bağlamda, hukuka aykırı elde edilen delillerin değerlendirilmesinde, söz konusu deliller istisnasız olarak değerlendirme dışı tutulmamalıdır. Hâkim, yasada açıkça yasaklanmış deliller dışında, takdir yetkisini kullanıp değerlendirme yaparken delil elde edilmesi faaliyeti sırasında ihlal edilen kurallar sebebiyle sanığın haklarının ihlal edilip edilmediğine bakmalı, sanığın haklarının ihlal edilmediği sonucuna varıldığında hukuk kurallarına aykırı biçimde elde edilen deliller yargılamada kullanılmalıdır[138].

Bu bakımdan kanun koyucunun iradi bir kavram kullanmasından hareketle, her türlü hukuka aykırılığı değerlendirme yasağı kapsamında görmediği, ifade alma ve sorguda yasak usulleri belirleyen CMK m. 148'de mutlak değerlendirme yasağına giren durumların özel olarak belirtildiği, bunun dışındaki hukuka aykırılıklarda ise hâkime takdir hakkı bıraktığı sonucuna varılmalıdır[139]. Buna göre; hukuka aykırı delillerin değerlendirilmesi meselesi adil yargılama ilkesiyle bağlantılı bir konudur[140]. Tüm bu belirtilenler ışığında Türk hukuk sisteminde esnek yaklaşımın benimsendiği söylenebilir.

---

[137] Ali Eryılmaz, "Ceza ve Disiplin Muhakemesinde Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu", (**Yayınlanmamış Yüksek Lisans Tezi**, Polis Akademisi GBE, 2011), s. 63; Mesut Orta, "Bilişim Suçlarında İspat", **1. Polis Bilişim Sempozyumu**, Ankara, 21-22 Ekim 2003, s. 291.

[138] Kaymaz, s. 263; Yazara göre; sanığın haklarının ihlal edilmesi halinde ise, suçun topluma vermiş olduğu zarar ile devlet görevlilerinin sanığa ait hakları ihlal etmeden doğan kişisel ve toplumsal zarar karşılaştırılmalı, sanığın topluma verdiği zarar daha fazla ise hukuka aykırı elde edilen deliller yargılamada kullanılmalı, aksi halde ise elde edilen deliller hüküm verilirken değerlendirilmemelidir. Bkz. Kaymaz, s. 271.

[139] Ali Eryılmaz, s. 291.

[140] Özgür Biyan, **Türk Vergi Hukukunda İspat – Delil,** Ankara: Adalet Yayınevi, 2012, s. 93; Hasan Tahsin Gökcan, "Gizli Kamera Kaydı Delil Olarak Kabul Edilebilir mi?", **Terazi Hukuk Dergisi,** Cilt. 5, Sayı. 42, (Şubat 2010), s. 74.

Buna karşın öğretide, CMK m. 217 hükmünün çok açık olup, hukuka aykırılığı keyfi veya olayın koşullarına göre derecelendirip bazı hukuka aykırı delilleri ispat yasağı kapsamı dışına çıkartılamayacağı, belirtilen madde metninin hukuka aykırı delillerin kullanılamayacağını ve hükmün yalnızca hukuka uygun delillere dayandırılabileceğini belirttiği gibi madde gerekçesinde bazı hukuka aykırı delillerin kullanılması için esnek bir yaklaşıma işaret etmediği belirtilerek[141] esnek yaklaşımı benimsemeyen görüşlerin de varlığı görülmektedir.

Aynı görüşteki Erol'a göre de; "hukuka uygun delil" ceza kanunlarının yanı sıra bütün hukuk kurallarına uygun olarak elde edilen delildir. Ancak delilin, ne olduğu, elde edilme ve yargılamada kullanılma usulü ceza muhakemesi hukukunda ayrıntılı olarak düzenlenmiş olduğundan bir delilin hukuka uygun olup olmadığı öncelikle ceza muhakemesi normlarına bakılarak tespit edilmelidir. Eğer delil ceza muhakemesi hukukunda belirtilen koşullara aykırı olarak elde edilmişse bu delil kanuna aykırı elde edildiğinden yargılamada kullanılamayacaktır[142].

Değirmenci'ye göre ise, gerek Anayasa'nın 38/6 maddesi gerekse CMK'nın hukuka aykırı delilleri düzenleyen hükümleri dikkate alındığında, kanun koyucunun hak ihlallerinden hareket etmediği, hak ihlali olmasa da hukuk kuralına aykırı hareketin delili hukuka aykırı hale getireceği görüşündedir. Bu nedenle de bir hak ihlali olup olmadığına bakmaksızın hukuk kurallarına aykırı elde edilen deliller, hukuka aykırı delil olarak kabul edilecek ve hükme esas alınamayacaktır[143].

Şen'e göre ise, insan haklarını ihlal eden etmeyen, önemli önemsiz, büyük-küçük hukuka aykırılıklar gibi ayrımlar yapmak ve bu sayede bazı delilleri yargılamada kullanılabilir hale getirmek yanlış olup hukukla bağdaşmamaktadır. İnsan hak ve hürriyetleri bahane edilerek ve önemli olanın gerçeğe ulaşmak olduğunu söyleyerek

[141] Yener Ünver, "Ceza Muhakemesinde İspat, CMK ve Uygulamamız", **Ceza Hukuku Dergisi (CHD),** Sayı. 2, (Aralık 2006), s. 134.

[142] Mehmet Erol, "Ceza Muhakemesi Hukukunda Delil Olarak Telefon Dinleme", (**Yayınlanmamış Yüksek Lisans Tezi,** Kocaeli Üniversitesi SBE, 2010), s. 55.

[143] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 422.

bazı hukuka aykırı delilleri yargılamada kullanılabilir hale getirmek, aslında hukuku, insan hak ve hürriyetlerini çiğnemekten başka bir anlam taşımamaktadır[144].

1.6.3. Hukuka Aykırı Delillerin Uzak Etkisi Sorunu

Hukuka aykırı delillerin uzak etkisi meselesi, yasak yollarla elde edilen delillere dayanılarak ortaya çıkartılan yeni delillerin ceza yargılamasında değerlendirilip değerlendirilemeyeceği sorunu ile ilgilidir. Zehirli ağacın meyveleri olarak da tanımlanan bu mesele zehirli ağacın meyvelerinin de zehirli olup olmayacağı noktasında tartışılmaktadır.

Zehirli ağacın meyveleri terimi, Anglo-Amerikan ortak hukukunda kullanılan bir dizi terimdir. Bu terim, yasa dışı soruşturma, arama, yakalama ve sorgulamalara dayanan, tarafsız olup olmadığı belli olmayan, hukuka aykırı bir şekilde toplanmış delillerin mahkemede kabul edilip edilmeyeceği hususuna dayanır. Bu metaforun mantığı, eğer ispatın kaynağı (ağaç) kusurlu ise ondan kaynaklanan bir şeyin (meyve) de aynı kusuru taşıyacağıdır[145].

Zehirli ağacın meyveleri doktrini, Amerikan kolluk kuvvetlerinin endişe verici araştırma yöntemlerini engellemek ve kolluk kuvvetlerini disipline etmek amacıyla ortaya çıkmıştır. Buna göre, Anglo-Amerikan hukuk sisteminde, delil yasaklarının görevi, kolluğu disiplin altına almak iken, Kıta Avrupa'sı hukuk sisteminde ise insan haklarını korumaktır. Bu nedenle Anglo-Amerikan hukuk sisteminde, delil toplayan kolluğun neden olduğu her türlü hukuka aykırılık, delil yasakları ile karşılanmakta ve elde edilen deliller, ceza yargılamasında kullanılamamaktadır. Oysa Kıta Avrupa'sı hukuk sisteminde, ister kasti, ister taksirli olsun, delilin elde edilmesi esnasında kolluk tarafından gerçekleştirilen hukuka aykırılık, eğer herhangi bir temel hak ve hürriyeti ihlal etmemiş ise bu deliller ceza yargılamasında kullanılabilmektedir[146]. Ancak,

---

[144] Ersan Şen, **Türk Hukuku'nda Telefon Dinleme-Gizli Soruşturmacı-X Muhbir**, 6. Basım, Ankara: Seçkin Yayıncılık, 2013, s. 37.

[145] Florian Geyer, "Zehirli Ağacın Meyvesi", Burcu Başak Uluçay ve Barış Hocaoğlu (Çev.), Yener Ünver (Ed.), **Ceza Muhakemesi Hukukunda Delil ve İspat** içinde (457-485), Ankara: Seçkin Yayıncılık, 2014, s. 458.

[146] Aysun Altunkaş, "Hukuka Aykırı Delil Teorisi Işığında İfade Alma ve Sorgu", (**Yayınlanmamış Yüksek Lisans Tezi,** İstanbul Bilgi Üniversitesi SBE, 2006), s. 210.

işkence veya acımasız, insanlık dışı ya da onur kırıcı davranış sonucu elde edilen itiraflardan kaynaklı fiziksel meyveler bu durumun istisnasını oluşturmaktadır[147].

Alman hukuk sistemi, hukuka aykırı delillerin uzak etkisi hususunda genel bir kural koymaktan çekinmekte, somut olayın özelliklerine ve delil elde etme yasağının niteliğine göre karar verilmesini tercih etmektedir. Bu doğrultuda da, Alman mahkemelerinin değerlendirme yasağının uzak etkisini genişletmeyi kabul etmediği ve polis tarafından yapılan usule ilişkin hataların, elde edilen diğer delilleri değerlendirme kapsamı dışında bırakmaya yol açmasının açıkça haksız nitelikteki beraat kararlarına neden olabileceğinden çekindiği görülmektedir[148].

İtalyan hukuk sistemi, ceza yargılamasının temel prensiplerinin ihlali sonucunda elde edilen delillerin kullanımını engelleyici katı dışlama kurallarına sahip olmasına karşın İtalya'da geleneksel olarak kabul edilen maddi gerçeği bulma prensibi ceza yargılamasında bu kuralların önemini azaltmıştır. Buna göre; zehirli ağacın meyvesi hakkında içtihat bulunmayan İtalya'da kaynağına bakmaksızın güvenilir ve temsil edici maddi deliller hala kabul edilmektedir[149].

Türk hukukunda ise hukuka aykırı olarak elde edilen delillere dayanılarak ulaşılan yeni delil araçlarının, yargılamada değerlendirmeye esas alınıp alınmayacağı, başka bir ifadeyle hukuka aykırı delillerin uzak etkisinin kabul edilip edilmeyeceği hususunda görüş birliği bulunmamaktadır.

Hukuka aykırı delillerin uzak etkisini kabul eden yazarlardan Öztürk'e göre, mülga CMUK m. 254'deki "hukuka aykırı şekilde elde edilen delillerin hükme esas alınmayacağını" mutlak bir şekilde öngören düzenleme karşısında uzak etki meselesi

[147] Stephen C. Thaman, "Karşılaştırmalı Hukukta Yasak Ağacın Meyveleri", Ahmet Emrah Geçer (Çev.), Yener Ünver (Ed.), **Ceza Muhakemesi Hukukunda Delil ve İspat** içinde (361-407), Ankara: Seçkin Yayıncılık, 2014, s. 406.

[148] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1478; Alman doktrininde, azınlıkta kalan görüşe göre ise, yasaklanmış deliller konusundaki kuralların eksiksiz olarak uygulanabilmesi için, yasak ağacın meyvelerinin de değerlendirme dışında kalması gerekmektedir. Bkz. Öztunç, s. 192, dp. 413.

[149] Thaman, s. 406.

Türk ceza muhakemesi hukuku bakımından halledilmiş durumdadır[150]. Anayasa m. 36/8 ve 5271 sayılı CMK m. 217/2 de bu kanaati büsbütün pekiştirmektedir. Mevzuattaki bu düzenlemeler karşısında hukuka aykırı delillerin elde edilişlerinin doğrudan doğruya veya dolaylı olmasının hiçbir önemi bulunmamaktadır. Burada, önemli olan husus delil veya delillerin elde edilmesi sırasında herhangi bir hukuka aykırılığın yapılmış olmasıdır[151].

Bu bağlamda, örneğin işkence ile elde edilen ikrar sonucu suç aletinin ele geçirildiği bir durumda, bu ikrarın kurulan hükümle nedensellik ilişkisi bulunması ve hükmü etkileme gücü olmasa da elde edilen suç aletinin hukuka aykırı yöntemlerle elde edilmesi nedeniyle ceza yargılamasında kullanılabilmesi ve hükme esas alınabilmesi kesinlikle mümkün değildir[152].

Benzer görüşe sahip yazarlardan İpekçioğlu'na göre; hukuka aykırı yöntemlerin kanunda yasaklanması, insan haklarına karşı duyarlılığın bir sonucudur. Her ne kadar CMK m. 148'de, hukuka aykırı delil araçlarının dolaylı etkisi açıkça yasaklanmamışsa da, yine de bu delil araçlarının yargılamada kullanılamayacağı ve hükme esas alınamayacağı sonucuna varmak mümkündür. Nitekim hukuka aykırı delil araçlarının doğrudan etkisini yasaklama için yeterli görüp de dolaylı etkisini bu kapsamda değerlendirmemek bir çelişkidir[153].

Özboyacı'ya göre, Anayasa'nın 38/6 maddesinde 2001 yılında yapılan değişiklik sonrasında Türk hukuk sisteminde hukuka aykırı delillerin uzak etkisine ilişkin tartışmanın sona ermiş olması gerekmektedir. Anayasa'nın ilgili maddesinde "kanuna aykırı olarak elde edilmiş bulgular, delil olarak kabul edilmez" hükmüne yer

[150] Bahri Öztürk (Ed.), **Nazari ve Uygulamalı Ceza Muhakemesi Hukuku Ders Kitabı**, Ankara: Seçkin Yayıncılık, 2009, s. 373.

[151] Bahri Öztürk (Ed.), Nazari ve Uygulamalı Ceza Muhakemesi Hukuku Ders Kitabı, 7. Basım, s. 417.

[152] Bahri Öztürk, Yeni Yargıtay Kararları Işığında Delil Yasakları, s. 33, 43.

[153] Pervin Aksoy İpekçioğlu, "Gözaltında Alınan İfadenin Önemi ve Delil Değeri", **Ankara Üniversitesi Hukuk Fakültesi Dergisi,** Cilt. 57, Sayı. 3, (2008), s. 63.

verilmektedir. Buna göre, Anayasa'ya göre hukuka aykırı deliller vasıtasıyla elde edilen bulgular meşru delil olarak kabul edilemezler[154].

Koca'ya göre; hukuka aykırı yöntemlerle elde edilen deliller bakımından değerlendirme yasağının uzak etkisi kabul edilmelidir. Buna göre, zehirli ağacın meyveleri de mutlak şekilde zehirlidir. Aksi bir düşünce, işkence gibi yasak yöntemler kullanılmasına rağmen, elde edilen ifade sayesinde ulaşılan delilleri yargılamaya sokmak anlamına gelir ki bu durumda, yasak sorgu yöntemlerinin bir anlamı kalmaz[155].

Avcı'ya göre; hukuka aykırı delillerin elde edilişlerinin doğrudan doğruya veya dolaylı olmasının herhangi bir önemi bulunmamaktadır. Burada önemli olan delil veya delillerin elde edilişi sırasında bir şekilde herhangi bir hukuka aykırılığın yapılmış olmasıdır. Bu bakımdan hukuka aykırı şekilde elde edilen bir delilin yardımıyla ulaşılan diğer delillerin yargılamada değerlendirmeye alınması durumunda hukuka aykırı deliller kapsamında kabul edilen kural ve ilkeler bozulmuş olacağından kendisinden beklenen fonksiyonu icra edemeyecektir[156].

Şen'e göre; esas itibariyle, hukuka aykırı biçimde uygulanan bir tedbirden hareketle ulaşılan diğer delillerin de yargılamada kullanılabilmeleri mümkün değildir (zehirli ağacın meyvesi de zehirlidir). Bu nedenle de hakkında elde edilen delillerin hukuka aykırı olduğu konusunda değerlendirme yapabilme olanağı bulunmayan şüpheliden alınan beyanların da yargılamada kullanılamayacağı açıktır[157].

Erol'a göre; bir delilin elde edilmesindeki hukuka aykırılığı, o delilden ayrı tutup, delil gerçek diyerek kullanmaya çalışmak hukuken doğru görülemez. Çünkü delil ne kadar gerçekçi olursa olsun, yine de hukuka aykırı elde edilmiş bir delildir. Bu delile yapışık

---

[154] Alper Özboyacı, **Ceza Muhakemesi Hukukunda Delil Yasakları (Yargıtay İçtihatları İle),** İstanbul: Kazancı Hukuk Yayınevi, 2008, s. 22.

[155] Koca, Ceza Muhakemesinde Hukuka Aykırı Delilleri Değerlendirme Yasağı, s. 135.

[156] Feyzullah Avcı, "Ceza Yargılamasında Özel Hayatın Gizliliği Hak ve Hürriyetinin Hukuka Aykırı Olarak Elde Edilen Deliller Nedeniyle İhlali", (**Yayınlanmamış Yüksek Lisans Tezi,** Selçuk Üniversitesi SBE, 2006), s. 96-97.

[157] Ersan Şen, "Ceza Yargılaması Süreci", **Türkiye Barolar Birliği Dergisi,** Sayı. 97, (Kasım-Aralık 2011), s. 282.

olan hukuka aykırılığı, o delilin gerçek ve doğru olduğu savunmasıyla gidermek mümkün değildir[158].

Değirmenci'ye göre de, hukuka aykırı delillerin ceza yargılamasında kullanılamamasının bir sonucu olarak hukuka aykırı delilden hareketle elde edilen diğer deliller de hukuka uygun olarak değerlendirilemez ve yargılamada kullanılamaz. Hukuka aykırı delillerin ceza yargılamasında kullanılamaması; ceza yargılamasının sağlıklı işlememesi, işlenen suçların ortaya çıkartılamaması, suç işleyen kişilerin cezasız kalması gibi sonuçların doğmasına sebebiyet verecek ise de, söz konusu sonuçların, yargı kararlarında istisnalar oluşturulmak suretiyle giderilebilmesi mümkündür[159].

Öğretide yasak delillerin uzak etkisini kabul etmeyen Kaymaz'a göre, hukuka aykırı delillerin değerlendirilmemesi için delilin doğrudan doğruya elde edilmesi ile dolaylı olarak elde edilmesi arasında bir fark bulunmamaktadır. Fakat haksız beraat kararlarının önlenebilmesi, yargılamanın basit hukuka aykırılıklar nedeniyle kilitlenmemesi için bir ayrım yapmak gerekmektedir. Buna göre; işkence gibi mutlak delil yasakları ihlal edilerek elde edilen dolaylı delillerin gerek soruşturmanın başlatılmasına esas başlangıç şüphesine temel teşkil etmemesi gerekse yargılama aşamasında değerlendirilmemesi gerekir. Ancak, elde edilmesi sırasında uyulması gerekli kurallara riayet edilmemesi nedeniyle hukuka aykırı hale gelen deliller aracılığıyla elde edilen diğer delillerin ise istisnasız bir şekilde değerlendirme dışında tutulması doğru değildir. Hukuka aykırı şekilde elde edilen delillerin yargılamada kullanılıp kullanılmayacağının belirlenmesinde, ihlal edilen hakkın niteliği, anayasal bir hak olup olmadığı, sanığın haklarının ne ölçüde etkilendiği, oranlılık ilkesi, suçun meydana çıkarılmasındaki kamu yararı ile sanığın hukuka aykırılık sebebiyle uğradığı zarar kıyaslanarak, sonucuna göre bir karar verilmesi gerekmektedir[160].

Eryılmaz'a göre, delil yasaklarının uzak etkisi hususunda yasada takdir yetkisini ortadan kaldıran mutlak manada yasaklayıcı bir hüküm bulunmamaktadır. Bu husus nazara alındığında, hukuka aykırı delil ile ulaşılmak istenen amaç, delillerin elde edilmesi

[158] Erol, s. 69.

[159] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 434-435.

[160] Kaymaz, s. 274.

aşamasında sanığın temel hak ve özgürlüklerinin ihlal edilmemesini sağlamaktır. Bu anlamda, sınırlamayı mutlak olarak yorumlamayıp, ihlal edilen kural ile korunan hukuki değerin kıyaslamasının yapılarak oranlılık ilkesi doğrultusunda denge aranması gerekmektedir. Buna göre, genel bir kural koymanın zorluğu dikkate alındığında, uzak etki meselesinin kendi hususiyeti içerisinde hâkim tarafından değerlendirilmesi, sorunun çözümü bakımından daha yerinde olacaktır[161].

Darende'ye göre, uzak etki sadece bir tek hal için dikkate alınabilir. Buna göre, uzak etki değerlendirmesinin konusu olan delil, başka yolla elde edilme imkânı olmayıp yalnızca hukuka aykırı delil sonucunda elde edilebilmişse, yani hukuka aykırı delilin zorunlu sonucu niteliğini taşıyorsa, bu durumda söz konusu delili de geçersiz kabul etmek gerekir. Buna karşın, kasıtlı olmayan ihlallerde, uzak etkiden bahsetmek mümkün değildir. Bu bağlamda, sanığın evinde yapılacak aramayla kolayca ele geçirilebilecek bir silah ve üzerindeki izler, sadece yasak sorgu yöntemi sırasında öğrenildiği için hukuka aykırı delil olarak nitelendirilmemelidir. Zira bu delil, yasak sorgu yöntemine başvurulmamış olsaydı da elde edilebilecek niteliktedir[162].

Demirbaş'a göre, sadece hukuka aykırı biçimde elde edilen ilk delilin yargılamada kullanılması mümkün değildir. Bununla birlikte, bu delile dayanarak elde edilen diğer delil veya delillerin yargılamada kullanılması gerekir. Nitekim kendisine yapılan işkence neticesinde sanığın suçu ikrar etmesi ve bu esnada suç aletinin yerini göstermesi durumunda işkence sonucu elde edilen ikrar yargılamada kullanılamayacak ve fakat ikrar sayesinde elde edilen suç aleti yargılamada geçerli bir delil olarak kullanılabilecektir[163].

Yaşar'a göre ise hukuka aykırı olarak elde edilen delillerin, hükme esas alınamayacağı hükmü CMK m. 148'de öngörülen yasak sorgu yöntemi doğrultusunda düzenlenmiştir. Buna göre, yasak sorgu yöntemleri kullanılarak delil elde eden soruşturma ve kovuşturma görevlilerinin ceza sorumlulukları olduğu gibi disiplin soruşturmasına da tabi olacakları açıktır. Hukuka aykırı delilin hükme dayanak yapılması durumunda

[161] Ali Eryılmaz, s. 73.

[162] M. İhsan Darende, "Hukuka Aykırı Delil", http://www.turkhukuksitesi.com/makale_622.htm (28 Ocak 2014).

[163] Demirbaş, s. 298-300.

kararın bozulması gerekmektedir. Ancak hükümle hukuka aykırı delil arasında illiyet bağı yoksa veya hükme etki etmemişse bir sorun bulunmamaktadır[164].

Yargıtay Ceza Genel Kurulu tarafından verilen bir kararda da uzak etkinin benimsenmediği görülmektedir. Sanığın ikametgâhında kenevir bitkisi olduğu ihbarı alınması üzerine il merkezinde, gecikmesinde ne tür bir sakınca olduğu belirtilmeden, hâkim kararı veya yetkili amir tarafından verilen yazılı emir de alınmadan ve sanığın aramaya muvafakat ettiği de belirtilmeden yapılan aramada bulunan 50 kök kenevir bitkisi ve sonrasında sanığın ikrara dayalı elde edilen delille mahkûmiyet kararı verilen olayda;

"*Yerel Mahkeme, iddia ve sanığın ikrarı dışında, olayla ilgili olarak düzenlenen tutanaklar, ekspertiz raporu ve emanette bulunan uyuşturucu madde gibi diğer kanıtlara da dayanmak suretiyle, sanığın uyuşturucu niteliğindeki esrar maddesi elde edebilmek amacıyla evinin damında 50 kök hint keneviri dikip yetiştirdiğini kabul ederek bu suçtan cezalandırılmasına karar vermiş, Yargıtay Özel Dairesi, hukuka aykırı gerçekleştirilen arama sonucunda elde edilen delilin hükümde esas alınamayacağını, başkaca delille desteklenmeyen soyut ikrarın da mahkûmiyet için yeterli bulunmadığını belirterek hükmü bozmuştur. Yargıtay C. Başsavcılığı ise; somut olayda sanığın soruşturma ve kovuşturma evrelerinde hâkim önündeki ikrarının özgür iradesine dayanması ve bu ikrarın başkasının suçunu üstlenmeye yönelik olduğunun ileri sürülmemesi karşısında kabule değer bir delil niteliğinde bulunduğunu, dolayısıyla sanığın suçunun sabit olduğunu belirterek itiraz yasa yoluna başvurmuştur.....*

Açıklanan pozitif hukuk normları ve uygulamayı yansıtan yargısal kararlar karşısında belirtmek gerekir ki; 'hukuka aykırı biçimde' elde edilen deliller, Türk Ceza Yargılaması Hukuku sisteminde dikkate alınamaz. Bu itibarla; sanığın konutunda hukuka aykırı olarak gerçekleştirilen arama işleminde elde edilen maddi delil ile buna ilişkin düzenlenen ekspertiz raporlarının Yerel Mahkemece hükme esas alınmasında isabet bulunmamaktadır. Esasen somut olayda; aramanın hukuka aykırı olduğu ve sonucunda elde edilen delilin hükme esas alınamayacağı hususunda Yargıtay Özel

[164] Osman Yaşar, **Ceza Muhakemesi Kanunu Yeni İçtihatlarla Uygulamalı ve Yorumlu,** II. Cilt, 5. Basım, Ankara: Seçkin Yayıncılık, 2011, s. 2609.

Dairesi ile Yargıtay C. Başsavcılığı arasında bir görüş farklılığı söz konusu değildir. Çözümü gereken uyuşmazlık, hukuka aykırı aramada elde edilen maddi delil dışındaki diğer delillerin, bu bağlamda hakkındaki ihbar ile sanığın mevcut ikrarının somut olayda mahkûmiyet için yeterli olup olmadığı hususunda toplanmaktadır.....

Tüm bu hususlar birlikte değerlendirildiğinde, hakkındaki ihbar üzerine başlatılan soruşturma ve kovuşturma evrelerinde sanığın ihbarla uyumlu ve hayatın olağan akışına da uygun düşen özgür ve samimi ikrarı karşısında, uyuşturucu madde elde etmek amacıyla izinsiz hint keneviri ekme suçu sübuta ermiştir[165]*.*" hükmüne yer verilmiştir.

Bizce de delil yasaklarının uzak etkisi konusunda Anayasa'da ve Ceza Muhakemesi Kanunu'nda hâkimin takdir yetkisini ortadan kaldıran sınırlayıcı bir hüküm bulunmaması karşısında Kıta Avrupa'sı hukuk sistemini benimseyen iç hukukumuz bakımından bu hususun somut olayın özelliklerine göre hâkim tarafından değerlendirilmesi gerekmektedir. Bununla birlikte işkence, insanlık dışı veya onur kırıcı davranış sonucu yapılan itiraflar üzerine elde edilen delillerin ise istisna tutularak yargılamada değerlendirmeye alınmaması gerektiği kanaatindeyiz.

1.6.4. Hukuka Aykırı Delillerin Dosyadan Çıkartılması Sorunu

Türk hukuk sisteminde hukuka aykırı delillerin dosyadan çıkartılıp çıkartılmayacağı hususu tartışmalı bir konudur. Odman'a göre, hukuka aykırı delillerin dosyadan çıkartılması en uygun görünen yoldur. Zira bu gibi delillerin vicdani kanaatine göre karar verecek hâkimleri etkilemesi mümkündür. Bununla birlikte, hukuk sistemimizde delillerin dosyadan çıkartılmasına ilişkin bir hüküm olmaması nedeniyle mahkemelerin

[165] Yargıtay C.G.K. 29.11.2005, E. 2005/7-144, K. 2005/150 (**Yargıtay Kararları Dergisi,** Cilt. 32, Sayı. 3, Mart 2006), s. 465-472; Buna karşın söz konusu Ceza Genel Kurulu Kararındaki çoğunluk görüşüne katılmayan iki kurul üyesinin karşı oy yazılarında ise, *"Hukuka aykırı şekilde elde edilen delil dolayısı ile ulaşılan deliller ister hukuka aykırı, isterse hukuka uygun yolla elde edilsin, hukuka aykırı deliller olacaktır. Öğretide baskın görüşün bu yönde olduğunu görüyoruz. Bu duruma 'hukuka aykırı delillerin dolaylı etkisi, uzak etkisi' ya da 'zehirli ağacın meyvesi de zehirlidir' denilmektedir.....Bu değerlendirmelerle birlikte olayımıza tekrar döndüğümüzde, sanığın ikrarının hukuka aykırı arama ile elde edilen delile dayanılarak alındığını, dolayısıyla bu ikrarın da hukuka aykırı delil olduğunu ve yargılamada kullanılamayacağını son kez vurgulamak istiyoruz. Zehirli ağacın meyvesi de zehirlidir"* denilmektedir. s. 473-485.

bir ara karar ile delillerin dikkate alınmamalarına ve daha sonra da hükme esas alınmamalarına karar vermeleri gerekmektedir[166].

Yıldız'a göre; bir delilin hukuka aykırı yollardan elde edildiği ve hukuken yasak olan delillerden olduğu saptandığı takdirde bunların esasa ilişkin dava dosyası içerisinde tutulması ve yargılama süjelerinin bu delillerle temasının engellenmesi gerekmektedir[167].

Öztürk'e göre ise, yargılama aşamasında hukuka aykırı delillerin varlığının tespiti halinde asıl uyuşmazlığı yargılayan "delil yasakları davası" olarak anılabilecek bir tali davanın açılabilmesi mümkündür. Ancak bu durumda da delillerin dosyadan çıkartılabilmesi mümkün değildir. Zira bu durum ceza yargılama tekniğine aykırıdır. Delil yasakları davası sonucunda hukuka aykırı olduğuna karar verilen delilin gerçekten hukuka aykırı olup olmadığının denetlenmesi gerekmektedir. Diğer taraftan, maddi gerçeği, insan haklarını ihlal etmeden arayan bir ceza yargılamasında hiçbir delil dosyadan çıkartılamaz. Kaldı ki, delil yasakları ihlal edilerek elde edilen delilin dosyada muhafaza edilmesi hâkimi etkilemez; etkilememelidir[168].

Karşı görüşe sahip Kaymaz'a göre, delilleri serbestçe değerlendirme yetkisine sahip olan ve vicdani kanaatine göre hüküm verme durumunda olan mahkemenin bazı delilleri hükme esas almaması mümkündür. Ancak, mevcut hukuk sistemimiz içerisinde henüz daha yargılama devam ediyorken mahkemenin bir ara karar ile de olsa delilin hukuka aykırı olduğuna karar vermesi mümkün değildir. Bununla birlikte, hukuka aykırı olduğu değerlendirilen delillerin bir zarfa konulup mühürlenerek dosyada muhafaza edilmesi mümkündür[169].

Gökcan'a göre ise; soruşturma dosyasına sunulan delillerin dosyaya alınmaması veya kovuşturma aşamasında delillerin dosyadan çıkartılması şeklinde bir uygulama kanuna uygun değildir. Zira CMK m. 230/1-b hükmünde, hukuka aykırı yöntemlerle elde

[166] Odman, s. 32.

[167] Ali Kemal Yıldız, Ceza Muhakemesinde İspat ve Delillerin Değerlendirilmesi, s. 203.

[168] Bahri Öztürk, Yeni Yargıtay Kararları Işığında Delil Yasakları, s. 45.

[169] Kaymaz, s. 278.

edildiği için reddedilen delillerin de hüküm gerekçesinde belirtilmesi gerekmektedir. Bu bakımdan, şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi veya kamu davası açılmasına karşın bazı delillerin reddedilmesi durumunda, kararda bunların da gerekçeleriyle birlikte açıklanması kanuna uygun bir yöntem olacaktır. Karara karşı temyiz yoluna başvurulması durumunda da ilgili delilin hukuka uygun olup olmadığına ilişkin iddialar temyiz mercii tarafından değerlendirilmelidir[170]. Ancak, hukuka aykırı elde edilen delil kullanılmayıp yalnızca dosyada kalmışsa, bu durumda hükmün bozulmaması gerekecektir[171].

Ünver ve Hakeri'ye göre de, yeni hükümler hukuka aykırı delillerin ilke olarak dosyaya girmesine imkân vermemektedir. Bu hükümler dosyada bulunan delilin dosyadan çıkartılamayacağına da işaret etmektedir. Zira delilin bilahare değerlendirilmesi, özellikle hukuka aykırılık bakımından ele alınması, kanun yolu aşamasında gözetilmelidir. Bu bakımdan hukuka aykırı bir delil bir defa dosyaya girince yasa hükümleri bu delilin dosyadan çıkartılmasını engellemektedir[172].

Ceza Muhakemesi Kanunu'nda hukuka aykırı şekilde elde edilen delillerin dosyadan çıkartılmasına ilişkin herhangi bir hüküm bulunmadığı gibi CMK m. 206, 230/1-b, 289 ve 302/3-4 hükümleri de hukuka aykırı şekilde elde edilmiş delillerin dosyada muhafaza edilmesi gerektiğine işaret etmektedir. Bu bakımdan bizce de, hukuka aykırı şekilde elde edildiği iddia olunan delillerin varlığı halinde dahi bu delillerin dosyadan çıkartılması hukuk sistemimiz açısından mümkün değildir.

1.7. Elektronik Delil ve Kullanıldığı Suç Tipleri

1.7.1. Elektronik Delil

Son yıllarda mevcut teknolojinin gerek nitelik gerekse nicelik olarak akıl almaz derecede ilerleyişine şahit olunmaktadır. Çok az insan, hayatı oldukça kolaylaştıran teknolojiden kendini uzak tutmayı başarabilmektedir. Bununla birlikte insanlar

[170] Hasan Tahsin Gökcan, "Cumhuriyet Savcısının Delilleri Değerlendirme Yetkisi ve Yargıtay Uygulaması", **Ankara Barosu Dergisi,** Sayı. 1, (2012), s. 200-201.

[171] Osman Yaşar, II. Cilt, s, 2609.

[172] Ünver ve Hakeri, 2. Cilt, s. 192; Aynı görüş için bkz. Özboyacı, s. 25.

teknolojinin birçok olumlu yönünden istifade etmesine rağmen zaman zaman olumsuz taraflarıyla da yüzleşebilmektedir. Teknolojinin olumsuz taraflarının başında ise onun kötüye kullanılması gelmektedir.

Teknolojinin gelişmesiyle kâğıt yerine elektronik belgenin kullanılması, iletişim için elektronik ortamın tercih edilir olması ve günlük işlerde bilişim sistemlerinin hayatın vazgeçilmezi haline gelmesi sonucunda oluşan yeni ortam ve felsefenin hukuka uygunluğu, güvenilirliği ve kuralların belirginliği tüm hukuk sistemini etkileyen tartışmanın öncülüğünü yapmaktadır.

Suçların soruşturulmasının etkin bir şekilde yürütülmesinde delillerin önemi yadsınamaz bir gerçektir. Özellikle, yargılama sürecinde, suçun sanık tarafından işlendiğinin şüpheye yer verilmeyecek şekilde ispatı için fiziksel delillerin yanı sıra fiziki varlığı olmayan soyut nitelikte delillerin de kullanıldığı ve hatta hâkim bir delil türü olduğu görülmektedir[173].

Bununla birlikte elektronik delilin bu özelliğine rağmen, elektronik delille ilgili teknik, kanıtsal ve yasal konularda pek az kişi gerçekten tecrübe sahibidir. Bu nedenle elektronik delilin, genellikle hâkim bir delil türü olduğu hususunun göz ardı edildiği, yanlış toplandığı veya etkisiz biçimde analiz edildiği görülmektedir[174].

Diğer taraftan, günümüzde elektronik delil lehine yaşanan dönüşüme rağmen, avukatların, hukuk akademisyenlerinin, hâkim ve savcıların dahi büyük oranda elektronik delilin hâkim bir delil türü olduğunu fark edemedikleri görülmektedir. Hukukun sosyal istikrarı sağlama aracı olarak görev gördüğü bir dünyada hukuk sistemindeki katılımcıların elektronik delillere aşina olmamaları, ceza mahkemelerinde yargılanan pek çok kişinin katı bir adaletle yüzleşmesine sebep olabilmektedir[175].

---

[173] Mesih Gözüşirin, "5237 Sayılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları ile Mücadeleye İlişkin Model Önerisi", (**Yayınlanmamış Yüksek Lisans Tezi**, Kara Harp Okulu SBE, 2011), s. 89.

[174] Eoghan Casey**, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet**, Third Edition, California: Academic Press, 2011, s. 8.

[175] Stephen Mason, "Bilişim Hukukunda Delillerin Toplanması", **Ankara Barosu Uluslararası Hukuk Kurultayı**, Cilt. 2, Ankara, 08-11 Ocak 2008, s. 171.

Elektronik delil hakkında pek çok savcı ve hâkimin kolaylıkla anlayamadığı temel nokta, konunun karmaşıklığı ve elektronik delil özelliklerinin doğasıdır. Konu hakkında temel bilgilere dahi sahip olmayarak bir atılı suçun soruşturmasından ve şahsa karşı ceza davası açılıp açılmamasından sorumlu olan savcılar ve soruşturma sürecinde savcılara teknik anlamda yardımcı olan adli bilişim uzmanları ciddi hatalar yapma tehlikesiyle karşı karşıyadırlar. Bu bakımdan savcıların, hâkimlerin ve hatta hukuk akademisyenlerinin elektronik delilleri anlamaya başlamaları hayati önem arz etmektedir[176].

Elektronik delil, ceza yargılamasında maddi olayı kısmen veya tamamen açığa çıkartacak nitelikte, bilişim sisteminde saklanan ve ortaya çıkartılması hukuki ve teknik süreci gerektiren bir veridir[*]. Bu bakımdan söz konusu verinin saklandığı ortam, delile elektronik delil niteliğini vermektedir[177].

Bu bağlamda, elektronik delili incelerken elektronik delile ilişkin temel kavramların öncelikle irdelenmesi gerekmektedir. Zira elektronik delilin tam manasıyla algılanabilmesi temel kavramların yeterince iyi anlaşılmasına bağlıdır. Temel kavramlar anlaşılamadığı sürece elektronik delilin yapısı ve ceza yargılamasındaki önemi de gerektiği şekilde algılanamayacaktır.

1.7.1.1. Elektronik Delile İlişkin Temel Kavramlar

1.7.1.1.1. Elektronik ve Dijital Kelimeleri

Elektronik delil, birden fazla disiplini ilgilendiren bir delil türüdür. Delilin elde edilmesi süreci, bilgisayar bilimi, iletişim bilimi, hukuk bilimi gibi birçok bilimin alanına girmektedir. Bu bağlamda, disiplinler arası bir konu olduğundan dolayı, farklı disiplinlerde aynı kavramı ifade etmek için farklı terminolojinin kullanıldığı

[176] Mason, Bilişim Hukukunda Delillerin Toplanması, s. 183.

[*] Veri; bilişimde, olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimini ifade etmektedir. Bkz. Türk Dil Kurumu. http://www.tdk.gov.tr/tdksozluk/sozbul.ASP?kelime (02 Ekim 2014).

[177] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 31.

görülmektedir[178]. Bu delil türü için en çok kullanılan kavramlar ise "elektronik delil" ve "dijital delil" kavramlarıdır.

"Elektronik" ve "dijital" kelimeleri, bilgisayar ve bilişim konusunda en çok kullanılan kelimeler olup genellikle birbirlerinin yerine ve gerekli özen gösterilmeksizin kullanılmaktadır. Bu bakımdan da elektronik delil kavramının kimi zaman dijital delil olarak da ifade edildiği görülmektedir.

"Elektronik" kavramı eksi yüklü elektronların hareketlerinden yararlanarak çeşitli donanımları yapma bilimini ifade etmektedir. "Elektronik", serbest elektron hareketinin denetimini konu edinir ve bu yapı; radyo, televizyon, bilgisayar gibi pek çok aygıtın temelini oluşturmaktadır[179].

"Dijital" kavramı ise dilimizdeki "sayısal" kelimesinin karşılığına tekabül etmektedir. Elektronik cihazlar içerisinde bulunan dijital veriler temelde ikili sayı sistemi ile kaydedilmektedir. İkili sayı sistemi 1 ve 0 değerlerinden oluşmakta olup bu sayı sistemi ise dijital verilerin temelini oluşturmaktadır. Bilgisayar ekranında görülen metin arka arkaya kaydedilen bu birler ve sıfırların anlamlandırılmasını sağlayan programlar sayesinde okunabilir duruma gelmektedir[180].

Adli bilişim çalışmaları kapsamında bir suçun aydınlatılmasına yönelik delil elde etme çalışmaları dijital ortamdaki verilerin okunmasına dayanır. Başka bir ifadeyle olay mahallinde bulunan bir USB bellek yerine bu bellek içerisindeki sayısal veriler yapılan işin ana konusunu oluşturur. Bununla birlikte bir kolluk personeli olay mahalline gittiğinde ilk olarak temas edeceği ve toplayacağı deliller içerisinde sayısal verileri de barındıran elektronik cihazlar da olacaktır. Bu anlamda ilk müdahale sırasında elde

[178] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 453.

[179] Ali Karagülmez, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, 2. Basım, Ankara: Seçkin Yayıncılık, 2011, s. 38.

[180] Hakan Aydoğan, "Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri", (**Yayınlanmamış Yüksek Lisans Tezi**, Polis Akademisi GBE, 2009), s. 30; Kubilay Say, "Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi", (**Yayınlanmamış Yüksek Lisans Tezi**, Ankara Üniversitesi SBE, 2006), s. 47.

edilen ve suç ile ilişkisi araştırılacak olan USB belleği bir elektronik delil niteliğindedir[181].

Bu bakımdan "elektronik delil" ifadesinin hem elektronik cihazı hem de bu cihaz içerisinde bulunan dijital verileri kapsaması ve dijital delil ifadesine göre daha üst bir anlamı içermesi nedenleri ile biz de bu çalışmamızda elektronik delil kavramının kullanılmasının daha isabetli olacağı kanaatindeyiz.

1.7.1.1.2. Elektronik Veri ve Elektronik Delil Kavramları

5070 sayılı Elektronik İmza Kanunu'nun 3-a maddesinde yapılan tanıma göre *"Elektronik veri, elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları"* ifade etmektedir. Buna göre, elektronik ortamda var olan her türlü veri elektronik veridir. Bu verinin nerede, kim tarafından ve nasıl oluşturulduğunun hiçbir önemi yoktur. Verinin herhangi bir aşamada elektronik ortamda yer almış olması yeterlidir[182].

Elektronik veri, Avrupa Konseyi Siber Suç Sözleşmesi'nin 1. maddesinde bilgisayar verisi olarak ifade edilmiştir. Sözleşmede "bilgisayar verisi" terimi ise, *"bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlar da dâhil olmak üzere, bir bilgisayar sisteminde işlenmeye uygun nitelikteki her türlü bilgi ve konsept"* şeklinde tanımlanmıştır.

Elektronik veriler bilgisayarda olabileceği gibi diğer bilişim sistemlerine ait cihazlarda da olabilir. Bu bağlamda bilişim sisteminde tutulan her türlü bilgi, ister sistem tarafından üretilmiş olsun ister kullanıcı tarafından oluşturulmuş olsun bilişim sistemlerinde veri olarak depolanmaktadır. Bu bakımdan, bilişim sistemlerinde delil aramanın amacı yargılamaya konu maddi olayı herhangi bir şekilde tespit eden elektronik verilere ulaşmak[183] ve elektronik delilleri elde etmektir.

---

[181] Aydoğan, s. 30.

[182] Mustafa Göksu**, Hukuk Yargılamasında Elektronik Delil**, Ankara: Adalet Yayınevi, 2011, s. 13.

[183] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 50.

Bu bağlamda, elektronik veri ile elektronik delil arasındaki ilişkinin bir fonksiyon ilişkisi olduğu, elektronik delilin mutlaka elektronik veri niteliğinde bulunması gerektiği, buna karşın sadece maddi olayla irtibatlı olan elektronik verinin elektronik delil olarak nitelendirilebileceği söylenebilir[184].

Bir bilgi veya veri, elektronik ortamda tutulabilir. Elektronik ortamda tutulan söz konusu bilgi veya veri, ceza yargılamasında delil olma niteliğine sahip olduğunda, başka bir ifadeyle, yargılamaya konu olan maddi olayı temsil edici ve gerçek olduğu durumlarda elektronik delil olacaktır. Belirtmek gerekir ki; elektronik verinin delil olabilmesi, delillerin sahip olması gereken ortak özelliklere haiz olmasına bağlıdır[185].

Bir elektronik verinin elektronik delil olarak nitelendirilmesi ayrıca onun güncel olarak erişilebilen bir yerde depolanmış olmasına ve adli bilişim uzmanlarınca geri getirilebilir olmasına da bağlıdır. Gerçekten de, günümüzün en büyük sorunlarından birisi, elektronik delilin var olup olmadığı hususu olmayıp, onun nerede saklandığı, ona erişilip erişilemeyeceği ve sonuçta geri getirilip işleme tabi tutarak suç eylemlerini aydınlatmada kullanılıp kullanılamayacağı hususudur[186].

Bu bağlamda elektronik delil; yürütülmekte olan bir soruşturma veya kovuşturmaya esas olmak üzere, bilişim sistemleri (bilgisayar, mobil telefon, dijital fotoğraf makineleri, dijital videolar, dijital faks makineleri vs.) ve bu özellikteki depolama aygıtları üzerinden elde edilen adli delilleri ifade etmektedir[187]. Elektronik delil, bilişim teknolojisi içeren her türlü donanım, bu donanım üzerinde çalışan ve her türlü yazılım tarafından kullanılan veya üretilen her türlü veri ile bilişim teknolojisi tarafından kullanılan her türlü elektronik sinyali kapsamaktadır[188].

---

[184] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 60.

[185] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 127.

[186] Larry Daniel and Lars Daniel, **Digital Forensics For Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom**, Waltham: Syngress Publishing, 2012, s. 4.

[187] Türkay Henkoğlu, **Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi**, İstanbul: Pusula Yayıncılık, 2011, s. 5.

[188] Mustafa İlker Öztürk, "Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri", (**Yayınlanmamış Yüksek Lisans Tezi**, Ankara Üniversitesi SBE, 2007), s. 38.

Başka bir tanıma göre ise elektronik delil; herhangi bir cihaz, bilgisayar sistemi ile oluşturulan, işlenen, depolanan veya iletilen ya da iletişim sistemi ile aktarılan, hüküm süreci ile ilgili olan verileri ifade etmektedir. Bu veriler, dijital formattaki veriler ile analog cihaz* çıktılarını da kapsamaktadır[189].

Casey'e göre elektronik delil, bir suçun nasıl meydana geldiği ile ilgili teoriyi destekleyen veya çürüten, bilgisayar kullanılmak suretiyle saklanan veya taşınan veridir[190]. Carrier'e göre ise; elektronik delil, dijital olay veya dijital verinin durumu hakkındaki bir varsayımı destekleyen veya reddeden veriye denir[191].

Hargreaves'e göre; Casey'in elektronik delil tanımı bir suç soruşturmasına odaklıdır. Ayrıca bu tanım yasal bir amaca matuf yapılmıştır. Oysa elektronik delilin kullanımı bir suçun ispatına yönelik olarak kısıtlanamaz. Carrier'in tanımı ise elektronik delil ifadesini daha genel manada kullanan ve elektronik delilin hukuki veya cezai soruşturmanın dışında kullanılabileceği hususunu da dikkate alan içeriği basit bir inanç veya düşüncenin doğruluğunu belirlemek için kullanılmış daha uygun bir tanımdır[192].

Elektronik delilin temelini, bilgisayar veya bilgisayar sistemlerinde bulunan ve suç veya uyuşmazlıkla ilgili olan dijital veriyi ifade eden her türlü bilgi veya değer oluşturmaktadır. Bilişim sistemlerinde veya veri saklama birimlerinde, suçun ispat

* Analog cihazdan elde edilen deliller analog delilleri oluşturmaktadır. Bu delil türünün örnekleri arasında mekanik cihaz ürünü ve otomatik kayıt, fotoğraflar, bant kayıtları, radarla takip edilen ve otomatik olarak filme kaydedilen bir geminin hareketleri, nefes testi makinesinde yapılan bir testin sonuç çıktısı ve video kayıtları bulunmaktadır. Anolog sistemler ya da ürünler kalıcı biçimde meydana getirilebilen veri şeklinde delil oluşturabilmektedir. Bkz. Mason, Bilişim Hukukunda Delillerin Toplanması, s. 172; Anolog, devamlı değişken bir akış halinde bulunan verileri ifade eder. Bilgisayarlar doğrudan anolog veriyi işleyemezler. Bunun için gelen anolog verileri dijitale çeviren arabirimlerin kullanılması gerekir. Bkz. http://analog.nedir.com/ (21 Nisan 2015).

189 Mason, Bilişim Hukukunda Delillerin Toplanması, s. 173.

190 Casey, Digital Evidence and Computer Crime, s. 7.

191 Brian D. Carrier, "A Hypothesis-Based Approach to Digital Forensic Investigations", (**PhD Thesis**, Purdue Üniversity, 2006), s. 11.

192 Christropher James Hargreaves, "Assessing The Reliability Of Digital Evidence From Live Investigations Involving Encryption", (**PhD Thesis**, Cranfield University, 2009), s. 16.

edilmesini sağlayacak ve çok farklı şekillerde saklanabilen dijital veriler ve bununla bağlı olarak da deliller bulunabilir[193].

Bu bakımdan, elektronik delil, bir suç işlenmesinde kullanılan ya da bir suç ve onun mağduru veya faili arasında bağlantıyı sağlayan[194] her çeşit veri kaydı, dosya, kaynak kodu, yazılım, veri saklama birimi ve buna benzer pek çok birimi kapsamaktadır[195].

Elektronik delilde bulunması gereken ortak hususlara ilişkin bir tespit yapmak gerekirse; elektronik delil her şeyden önce elektronik ortamda tutulan veriyi ifade eder. Söz konusu verinin amacı, herhangi bir hukuki uyuşmazlıkta bir hususu ispatlamak veya çürütmektir. Veri, elektronik cihaz tarafından oluşturulabileceği gibi, söz konusu cihaz tarafından saklanabilir veya aktarılabilir. Bu anlamda veri; durağan veya akış halinde olabilir[196].

Belirtmek gerekir ki; elektronik delilin birinci derecede kullanıldığı -bilişim suçlarını konu alan- davalarda faile atfedilen suçun ortaya çıkartılabilmesi ve iddiaların ispatlanabilmesi, çoğu zaman elde edilen elektronik delilin ispat gücüne ve hukuka uygunluğuna bağlıdır[197].

1.7.1.1.3. Bilgisayar

Elektronik delilin bulunduğu ortamların başında bilgisayar gelmektedir. Bilgisayarın dışındaki diğer bilişim sistemi araçlarında da elektronik delil bulunmasına karşın "elektronik delilin elde edilmesi" kavramı genellikle bilgisayarlarda yapılan aramayı hatıra getirmektedir. Bu nedenle de iç hukuk sistemimizde olduğu gibi birçok hukuk

[193] Basri Aktepe, "Emniyet Personelinin Bilgisayar ve Bilgisayarla İlintili Suçlarla Mücadelede Dikkat Etmesi Gereken Hususlar (Adli Tıp Esaslarına Uygun Olarak Delillendirme)", Ankara, **1. Polis Bilişim Sempozyumu**, 21-22 Ekim 2003, s. 67.

[194] Harvey Kozushko, "Electronic Evidence", 2003, http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/DigitalEvidencePaper.pdf (12 Kasım 2013).

[195] Aktepe, s. 67.

[196] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 129.

[197] Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, 2. Basım, Ankara: Seçkin Yayıncılık, 2012, s. 665.

sisteminde elektronik delilin aranması, bilgisayarlarda arama kavramı ile ifade edilmektedir[198].

Bu bakımdan elektronik delil için büyük öneme sahip olan bilgisayarın ifade ettiği anlamın ve sınırlarının belirlenmesi gerekmektedir. Buna göre bilişim sisteminin en temel bileşenlerinden birisini oluşturan bilgisayar, çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin olarak tanımlanmaktadır[199].

Bilgisayar, dış ortamdan aldığı verileri, üzerine yüklenen programlar aracılığıyla depolayan, işleyen, yeni sonuçlar üreten, veri iletişimini sağlayan makineler şeklinde de tanımlanmaktadır[200]. Bilgisayarı, benzer diğer aygıtlardan ayıran en önemli özelliği ise belirli bir amaca özgülenmemesi, uygun programın üzerine yüklenmesi kaydıyla genel olarak belirlenmiş bir işlevi yerine getirebilmesidir[201].

1.7.1.1.4. Bilişim ve Bilişim Sistemi

Bilişim, teknik, ekonomik ve toplumsal alanlardaki iletişimde kullanılan ve özellikle elektronik aletler aracılığı ile düzenli bir biçimde işlenmeyi ön gören bilimi ifade etmektedir[202]. Bilişim, insanların teknik, ekonomik, siyasal ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle bilgisayar aracılığı ile düzenli ve akılcı biçimde işlenmesi, her türden fikri sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarlarda toplanması ve kullanıcıların erişimine açık bulundurulması bilimi şeklinde de tanımlanmıştır[203].

---

[198] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 31.

[199] Türk Dil Kurumu. http://www.tdk.gov.tr/tdksozluk/sozbul.ASP?kelime (02 Ekim 2014).

[200] Bahaddin Alaca, "Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutu İle)", (**Yayınlanmamış Yüksek Lisans Tezi**, Ankara Üniversitesi SBE, 2008), s. 5-6.

[201] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 35.

[202] Türk Dil Kurumu. http://www.tdk.gov.tr/tdksozluk/sozbul.ASP?kelime (02 Ekim 2014).

[203] Dülger, s. 61; Serhat Koç ve Selva Kaynak, "Bilişim Suçları Bağlamında Yeni Medya Olarak İnternet ve Kişisel Güvenlik", **Akademik Bilişim'10-XII. Akademik Bilişim Konferansı Bildirileri,** Cilt.1, Muğla, 10-12 Şubat 2010, s. 72.

Bilgisayara göre daha geniş bir alanı kapsayıp bu nedenle daha üst bir kavram olan bilişim sistemi ise, en basit şekliyle, veri veya bilgileri alan, bu verileri işleme tabi tutabilen, sonuçları ya da verileri çıktı şeklinde verebilen elektronik makineler şeklinde tanımlanmıştır[204].

Başka bir deyişle bilişim sistemi, verilerin otomatik makineler aracılığıyla ve otomatik olarak işlenmesini sağlayan sistemleri ifade etmektedir[205]. Yargıtay ise bilişim sistemini *"verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemler[206]"* şeklinde tanımlamıştır.

Teknolojinin gelişimine bağlı olarak, maddi olayla ilgili verilerin sadece bilgisayarlarda değil, diğer bilişim sistem aygıtlarında da bulunacağı görülmüştür. Özellikle özel hukuk kaynaklı olarak elektronik delil kavramının doğuşu, bu şekilde gerçekleşmiştir. Özel hukukta kullanılan elektronik delil ve delile ilişkin düzenlemeler ise zamanla ceza yargılaması için de genişletilerek uygulamaya konulmuştur[207].

Bu bakımdan biz de tez çalışmamızda bilgisayar terimine nazaran daha üst bir kavram olması ve daha geniş bir anlamı içermesi nedenleriyle elektronik delilin bulunduğu ortamlardan bahsederken -Avrupa Konseyi Siber Suç Sözleşmesi ve ülkemiz mevzuatında genellikle kullanılan bilgisayar teriminden daha ziyade- bilişim sistemleri terimini kullanmayı uygun gördük.

1.7.1.1.5. Bilgisayar Ağı

Bilgisayar ağı, bilgisayarların belirli bir protokol altında iletişimde bulunmasını sağlayan sisteme denir. Ağ üzerindeki bilgisayarlar birbirlerinden çok uzakta olsalar dahi aynı protokol sayesinde karşılıklı çalışabilirler[208].

---

[204] Behçet Altaylı, **Bilgisayarlar ve Basic ile Programlama,** İstanbul: Filiz Kitabevi, 1985, s. 17.

[205] Muammer Ketizmen, **Türk Ceza Hukukunda Bilişim Suçları,** Ankara: Adalet Yayınevi, 2008, s. 11.

[206] Yargıtay 15. C.D. 23.09.2013, E. 2013/17302, K. 2013/13703 (UYAP).

[207] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 60.

[208] Ali Osman Özdilek, **İnternet ve Hukuk**, İstanbul: Papatya Yayıncılık, 2002, s. 14.

Ağlar, yayıldıkları alan göz önüne alındığında ikiye ayrılmaktadırlar. Bilişim araçlarının birbirlerine daha yakın ve belirli bir bölgede toplandıkları ve de bir kablo veya ağ kartı (ethernet kartı) ile bağlandıkları ağ sistemine LAN (Local Area Network-Yerel Alan Ağı) denilmektedir[209]. Yerel alan ağları, dar çerçevede tutulurlar ve diğer ağlara sınırlı bağlantı içinde olabilirler. Uzak mesafedeki bağlantılardan oluşan diğer ağ çeşidi ise WAN (Wide Area Network-Geniş Alan Ağı) şeklinde tanımlanmaktadır[210].

1.7.1.1.6. İnternet

Çeşitli ağların birleşmesi sonucunda teşekkül etmesi bakımından "ağların ağı" olarak da tanımlanan internet, "international" ve "network" kelimelerinin birleşmesinden oluşmaktadır. Buna göre internet, dünya üzerinde bulunan bilişim ağlarının ve bilgisayarların dünya çapında birbirleriyle bağlanarak belli esaslar dâhilinde kendine özgü bir dille iletişimlerinin sağlanmasını ifade etmektedir[211].

Başka bir ifadeyle internet, birden fazla haberleşme ağının (network) birlikte oluşturdukları metin, resim, müzik, grafik vb. dosyalar ile bilgisayar programlarını kısaca tüm insanlık bilgisinin paylaşıldığı ve bilgisayarlar arasında karşılıklı olarak iletildiği, bilgisayarlar arasında kurulmuş bir ağ olarak da tanımlanabilir[212].

İnternetin sağlamış olduğu birçok kolaylık ve avantaj bulunmasına karşın bunların kötüye kullanılması da söz konusu olabilmektedir. İnternetin diğer iletişim araçlarına göre daha az izlenebilmesi onun suç faillerince daha yoğun biçimde kullanılması sonucunu doğurmuştur. Vergi, sigorta kodları, askeri bilgiler gibi devlet için önemli birçok veriye ulaşabilme imkânının bulunması da suç failleri için cazip bir görüntü arz etmektedir. İnternet üzerindeki her verinin ulaşılıp imha edilmeye açık olması da ayrı bir sorundur. Bilişim alanının en önemli unsuru sayılan internetin sağladığı inanılmaz kolaylık ve imkânlar bu sahayı aynı zamanda geniş bir suç alanı haline de getirmiştir.

---

[209] Esra Yaycı, "Bilişim Suçları", (**Yayınlanmamış Yüksek Lisans Tezi**, Gazi Üniversitesi SBE, 2007), s. 10.

[210] A. Caner Yenidünya ve Olgun Değirmenci, **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul: Legal Yayıncılık, 2003, s. 35-36.

[211] Yenidünya ve Değirmenci, s. 36-37.

[212] Özdilek, İnternet ve Hukuk, s. 13.

Sahanın sınır tanımazlığı ölçüsünde bu ortamda işlenen suçlar da sınır tanımaz hale gelmiş, ortaya çıkardığı yıkım da büyük boyutlu olmuştur[213].

1.7.1.1.7. İletişim Kontrol Protokolü/İnternet Protokolü (TCP/IP)

Bilgisayarlar arasında veri iletişimini sağlamak amacıyla protokollere ihtiyaç duyulmaktadır. Protokoller iletişimdeki eşler arasında olan mesaj trafiğinin kurallarını oluşturup daha etkin bir iletişimin gerçekleşmesini sağlarlar. İnternette kullanılan ve kabul gören protokol TCP/IP (Transmission Control Protocol/Internet Protokol)'dir. TCP/IP bağlantılı yönlendirilmiş bir protokoldür. TCP/IP'nin bu yapısı sayesinde bilgisayarlardan gönderilen bir verinin yerine ulaşıp ulaşmadığı veya doğru ulaşıp ulaşmadığının kontrolü sağlanır[214].

IP adresi, belirli bir ağa bağlı bilişim sistemlerinin birbirlerini tanımak, birbirleriyle iletişim kurmak ve veri alışverişinde bulunmak için kullandıkları İnternet Protokolü standartlarına göre verilen adresi ifade etmektedir[215]. Başka bir deyişle IP adresi, bir ağa bağlı bilişim sistemlerinin birbirleriyle haberleşebilmeleri için gerekli olan sanal adrese verilen isimdir[216].

IP adresi numaralardan oluşmaktadır. Bu numaralar, internet hizmeti kullanımı nedeniyle kullanıcılara tahsis edilen numaralardır. İnternete bağlı her bilişim sisteminin 32 bitten oluşan bir formatta IP numarası bulunmaktadır. Bu IP numarası servis sağlayıcı* tarafından boşta olan bir numaranın verilmesi suretiyle her bağlantıda

---

[213] Levent Kurt, **Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Yeri,** Ankara: Seçkin Yayıncılık, 2005, s. 46.

[214] Özdilek, İnternet ve Hukuk, s. 16.

[215] Burcu Erdoğan, "Bir Kişiyi Suçlamak İçin IP Adresi Yeterli midir?", (t.y.), http://www.bilisimhukuk.com/2010/02/bir-kisiyi-suclamak-icin-ip-adresi-yeterli-midir/ (10 Ocak 2015).

[216] Cengiz Tanrıkulu, **Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma**, Ankara: Adalet Yayınevi, 2014, s. 25.

* Servis sağlayıcı; kullanıcılarının internete erişimini sağlayan doğrudan internet bağlantısına sahip olmanın yanı sıra başkaları tarafından hazırlanan verileri, kendi sunucularında depolayarak siber uzay ortamına aktarma işlevini de yerine getiren internet süjesini ifade eder. Bkz. Hasan Sınar, **İnternet ve Ceza Hukuku,** İstanbul: Beta Yayınevi, 2001, s. 87.

değişebileceği gibi, erişim sağlayıcılar* tarafından, ADSL abonelerine verilenlerde olduğu şekliyle statik de olabilir. Bu bakımdan IP numaraları sayesinde bağlı bulunan aboneliğin tespiti ile yer bilgisi ve adresleri içeren abone bilgilerine ulaşabilmek mümkündür[217].

IP numarasının sanal âlemde bilişim sistemi kullanıcılarını tanımlayan en önemli ayırt edici unsur olması, onun önemini bir kat daha artırmaktadır. Zira sanal âlemde yapılan her işlemde IP numarasının kullanılması ve ayrıca bu numaranın kullanılması suretiyle gerçekleştirilen her işlemden IP numarası sahibinin sorumlu tutulması bu durumu açıklamaktadır[218]. Nitekim bilişim suçları ile ilgili yürütülen bir soruşturma sırasında internet bağlantısı tespit edilen IP numarası ile bağlantıyı yapan telefonun bağlı olduğu erişim santralinin de dijital santral olması, hangi telefonun bağlantı yaptığını tespit etmede büyük kolaylık sağlamaktadır[219].

IP numarası önemli bir elektronik delil vasfını haizdir. Bununla birlikte IP numarası özellikle bilişim suçları bakımından bir başlangıç noktası niteliği taşımakta ise de -zaman damgalı haliyle- yetkilendirilmiş faaliyet belgesine sahip kurum veya kişilerce yargı makamlarına sunulmadığı ve başka delillerle desteklenmediği sürece tek başına sonuca götürücü özelliği bulunmamaktadır.

Nitekim Yargıtay da bir kararında *"…. sanığın, bir süre duygusal boyutta arkadaşlık ilişkisi içerisinde olduğu şikayetçinin müstehcen fotoğraflarını, onun bilgisi dışında bir sosyal paylaşım sitesine koyduğu iddiasına konu olayda, şikayetçinin beyanında geçen sosyal paylaşım sitesine onun adına üyelik işlemlerinin yapıldığı bilgisayarın internet servis sağlayıcısı ve internet servis sağlayıcısı tarafından verilen IP adresinin tespit edilmesi, tespit edilen IP adresinin belirtilen tarih ve saatte hangi abone tarafından*

* Erişim sağlayıcı; kullanıcılarına internet ortamına erişim olanağı sağlayan her türlü gerçek veya tüzel kişileri ifade eder. (5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun m. 1-e).

[217] Burcu Erdoğan, http://www.bilisimhukuk.com/2010/02/bir-kisiyi-suclamak-icin-ip-adresi-yeterli-midir/ (10 Ocak 2015).

[218] Huzeyfe Önal, "Bilişim Suçlarında IP Adresi Analizi-Adli Bilişim Açısından IP Adresleri", 2010, http://www.bga.com.tr/calismalar/ip_forensic.pdf (18 Ocak 2015), s. 4.

[219] İsmail Tulum, "Bilişim Suçları ile Mücadele", (**Yayınlanmamış Yüksek Lisans Tezi**, Süleyman Demirel Üniversitesi SBE, 2006), s. 90.

kullanıldığının ve o abonenin kimlik ve açık adres bilgilerinin belirlenmesi, IP adresini kullanan abonenin sanıkla bağlantısı araştırılıp, gerektiğinde sanığın iş yerinde ve evinde kullandığı bilgisayarlar üzerinde bilişim uzmanı üç kişilik bilirkişi marifetiyle inceleme yapılarak, söz konusu üye profilinin, sanığın kullanımında olan bilgisayar aracılığıyla oluşturulup oluşturulmadığı hususunun belirlenmesi; şikayetçinin 31.08.2009 tarihli şikayet dilekçesi de göz önüne alınarak, iddia olunan suç tarihinde şikayetçi ve sanığın abonesi olduğu telefon hatları araştırılıp, bu tarihten önceki ve sonraki altı aylık görüşme detaylarını gösterir HTS raporları istenilerek, toplanan tüm deliller birlikte değerlendirilerek, iddia ve savunmanın doğruluk derecesi açıklığa kavuşturulduktan sonra sanığın hukuki durumunun takdir ve tayini gerekirken, eksik incelemeye dayalı olarak….,[220]*"* hükmüne yer vererek yeterli bir soruşturma için IP adresinin tespitinin dışında araştırılması gereken hususları sıralamıştır[221].

1.7.1.2. Elektronik Delilin Önemi

Günümüzde, olay yerinde bulunması muhtemel delillerin arasında kıl, kan, tırnak gibi biyolojik; eroin, kokain, barut gibi kimyasal; parmak izi, ayakkabı izi, alet izi gibi fiziksel; kovan, kovan çekirdeği, tabanca gibi balistiksel; senet, para, broşür gibi belgesel nitelikte fiziksel delillerin olmasının yanı sıra son yıllarda bilişim teknolojisinin insan hayatının her alanında sıkça kullanılmasıyla birlikte olay yerlerinde karşılaşılabilinen deliller arasına bilgisayarlar, disketler, optik diskler, manyetik kasetler, cep telefonları, bellek kartları vs. gibi elektronik delil niteliğindeki bilişim ve iletişim cihazları da girmiştir[222].

Gündelik yaşamda sıklıkla kullanılan bilişim ve iletişim cihazları, insanoğlunun kullandığı suç araçları arasında önemli bir yer teşkil etmektedir. Değişmeyen bir kural olarak, bir kişinin işlemiş olduğu suçtan sonra bahse konu suçla alakalı delil niteliğinde

[220] Yargıtay 12 CD. 17.06.2013. E. 2013/7154, K. 2013/16476 (UYAP).

[221] Yargıtay başka bir kararında da; *"….IP numarasının kullanılan bilgisayarı göstermeyip internetle olan bağlantıyı göstermesi, sanığın bilgisayarlarında yapılan incelemede, bu bilgisayar kütüğünden marma- riskoleji-k12.com adresine bağlantı yapıldığının tespit olunamaması "hack" programına rastlanmasının şikâyetçiye ait siteye müdahale edildiğini göstermeyeceği, kesin delil bulunmadan varsayımlarla hüküm kurulamayacağı cihetle tebliğnamedeki bozma düşüncesine katılınmamıştır."* hükmüne yer vermiştir. Bkz. Yargıtay 8. CD. 24.10.2013. E. 2012/21817, K. 2013/25428 (UYAP).

[222] Kubilay Say, "Data İncelemeleri", Oğuz Karakuş (Ed.), **Kriminalistik** içinde (510-531), Ankara: Adalet Yayınevi, 2009, s. 511.

herhangi bir iz ve emare bırakmaması kendi elinde olmadığı gibi, bilişim sistemleri ile işlenen suçlarda da o suç ile ilgili deliller, işlenen suç sonrasında farklı şekil ve boyutlarda elektronik delil olarak elde edilebilmektedir[223].

Gerçekten de, elektronik delil niteliğindeki bilişim ve iletişim cihazlarının adli bir olayla ilgili olarak bazen bir suçun işlenmesinde kullanıldığı bazen ise klasik suçlarda işlenen suça yönelik, yardımcı bir unsur olarak önemli bilgiler bulundurduğu görülmektedir. Başka bir ifadeyle bilişim ve iletişim cihazları bir suçun işlenmesinde temel unsur olabildiği gibi suçun işlenmesinde doğrudan kullanılmamakla birlikte suçun aydınlatılmasında birer delil kaynağı niteliğinde karşımıza çıkabilmektedir[224].

Dijital bilgi, elektrik gelince görülen, elektrik kesildiğinde de yok olan sanal bilgidir. Bu bakımdan, dijital bilginin hukuki olarak delil niteliği taşımasında da bazı problemlerle karşılaşılmaktadır. Ancak bu bilgiler ispat edilemeyecek nitelikte bilgiler değildirler. Esasen elektronik medyalarda bulunan verileri oluşturan 1 ve 0 değerlerini tanımlamak için kullanılan yöntemlerden biri manyetik alanlardır. Disk yüzeyinde oluşturulan pozitif ve negatif yönlü manyetik alanlar 1 ve 0 değerlerini, bu 1 ve 0 değerleri de verileri oluşturmaktadır. Bu yüzden bilimsel yöntemlerle yerine getirilen adli bilişim incelemeleri hukuken sonuç doğurabilmektedir. Bilişim sistemlerinin çok hızlı işlem yapabilme kapasiteleri sayesinde veriler üzerindeki bazı görsel işlemler sanal olarak yapılıyor gibi görünse de aslında bu işlemlerin arkasında her zaman bilimsel olarak ispatlanabilen bir alt yapı bulunmaktadır[225].

Dijital işlemler ister yazılımlar yoluyla isterse elektronik mantık kapıları ile yapılıyor olsun neticede yüksek teknoloji bilgisi ile gerçekleşmektedir. Bu dijital işlemlerin bir suçun işlenmesinde kullanılmış olmaları durumunda ise incelenmeleri de aynı seviyede

[223] Hüseyin Çakır ve Ercan Sert, "Bilişim Suçları ve Delillendirme Süreci", Örgütlü Suçlar ve Yeni Trendler, **Uluslararası Terörizm ve Sınıraşan Suçlar Sempozyumu (UTSAS 2010),** Oğuzhan Ömer Demir ve Murat Sever (dr.), Ankara, 2011, s. 145-146; A. Hakan Ekizer, "Adli Bilişim (Computer Forensics)", http://www.ekizer.net/adli-bilisim-computer-forensics (10 Nisan 2014).

[224] Aydoğan, s. 2.

[225] Semih Dokurer, "Adli Bilişim", **2. Polis Bilişim Sempozyumu,** Ankara, 14-15 Nisan 2005, s. 227.

bir teknoloji bilgisini gerektirmektedir. Bu konuda uzmanlar tarafından incelenmesi gereken deliller ise adli bilişimin materyallerini oluşturan elektronik delillerdir[226].

Sonuç olarak; elektronik delil kavramı, genellikle bilişim suçları ile birlikte kullanılmakta ise de; teknolojinin hayatımızda önemli bir rol oynadığı günümüzde klasik suçların aydınlatılmasında da hayati bir önem arz etmekte ve bilişim suçlarına mahsus bir olgu olmaktan da çıkmış bir vaziyettedir.

1.7.1.3. Elektronik Delilin Oluşturulması

Günümüz sosyal dünyasında elektronik delilin normal bir insan yaşantısının her yönüne nüfuz ettiği görülmektedir. Bu günlerde gerçekleştirilen pek çok eylemde elektronik delilin farklı şekillerini içeren bir parmak izi oluşmaktadır. Nitekim elektronik posta gönderme, bir doküman çıktısı alma, dijital bir kamerayla fotoğraf çekme, internet kullanma ve hatta GPS özelliğe sahip bir otomobil kullanma gibi davranışların tümü bir elektronik delil oluşumuna sebebiyet vermektedir[227].

Sosyal medyanın çok geniş bir kitle tarafından yoğun bir biçimde kullanılması yaygın ve kalıcı nitelikteki elektronik delillerin oluşması için yeni alanlar açmaktadır. Zira günümüzde insanlar günlük etkinliklerini, düşüncelerini, kişisel fotoğraflarını hatta kaldıkları yerlerle ilgili ayrıntıları Twitter, Facebook ve MySpace gibi sosyal medya siteleri aracılığıyla paylaşmaktadırlar[228].

Bu bakımdan kişilerin günlük yaşamda kullanmış oldukları bilişim sistemlerinin donanım ve yazılımları arasındaki komut alış verişi, elektronik verileri üretmekte veya yüklenen verileri çeşitli formatlara dönüştürmektedir. Bu verilerin geçiş yollarına ve saklandığı alanlara elektronik ortam denilmektedir. Her elektronik veri kullanıldığı veya saklı bulunduğu elektronik aygıtta iz bırakmaktadır. Bu izler yazılımlarla sağlanan

[226] Dokurer, Adli Bilişim, 2. Polis Bilişim Sempozyumu, s. 227.

[227] Daniel and Daniel, s. 3.

[228] Daniel and Daniel, s. 4.

komutlar nedeniyle oluşabildiği gibi kullanıcıların isteğe bağlı kayıt ve işlemleriyle de oluşabilmektedir[229].

Bununla birlikte insanlar günlük yaşantılarında çoğu zaman yaptıklarının farkında olmadan da birçok elektronik delil üretmektedirler. Bir kimsenin bir arkadaşıyla internet ortamınla oyun oynaması veya internette video izlemesi, sanal âlemdeki binlerce alışveriş mağazasından herhangi birinden alışveriş yapması ve hatta iş yerinde fotokopi makinesini kullanması gibi pek çok davranışı hep yeni bir elektronik delilin üretilmesi sonucunu doğurmaktadır.

Günümüzün teknoloji dünyasında insanların dijital parmak izi oluşumuna sebebiyet vermediği bir gün geçirmesi neredeyse imkânsızdır. Hatta kişiler, günlük yaşantımızın vazgeçilmezlerinden olan bilgisayar ve cep telefonlarından kendilerini tecrit etseler bile söz konusu durumu değiştirebilmeleri çok da mümkün görünmemektedir. Zira bir kimsenin trafikte kırmızı ışık ihlalinde bulunması bile polis kamerasının bu ihlali kaydetmesi, bunun üzerine kişinin yerleşim yerinin tespit edilerek kimi zaman elektronik posta ortamında ceza makbuzu gönderilmesi, kişi bilgilerinin gelişen olaya göre dijital ortamda yeniden kayıt altına alınması gibi zincirleme birçok elektronik delil oluşumuna sebebiyet verecektir.

1.7.1.4. Elektronik Delilin Bulunduğu Ortamlar

Gerek insan müdahalesi sonucunda gerekse bilişim sistemi tarafından otomatik olarak üretilen her elektronik veri yargılamaya konu olayı temsil ettiği müddetçe elektronik delil niteliğini haizdir. Bu bakımdan, elektronik delilin kaydedilmesi ve depolanması, elektronik delile erişebilmek açısından çok önemlidir.

Bilişim suçlarının yanı sıra birçok klasik suç bakımından da elde edilmesi muhtemel deliller elektronik nitelikte olabilir. Elektronik delillerin bu yapısı dış dünyaya görsel ve işitsel şekilde yansıyabilmektedir. Bu nedenle elektronik delillerin bulunabileceği yerlerin iyi bilinmesi ve pek çok olasılık üzerinde dikkatle durulması gerekmektedir. Aşağıda elektronik delillerin bulunması muhtemel yerler ayrıntılı olarak incelenecektir.

[229] Murat Kızılyar, "Ceza Yargılamasında Dijital Verilerin Delil Değeri", **Adalet Dergisi,** Sayı. 50, (Eylül 2014), s. 80-81.

1.7.1.4.1. Bilgisayar İç Donanımları

Elektronik delilin bulunduğu bilgisayar iç donanımlarının başında sabit disk (hard disk) ve RAM gelir. Sabit disk, manyetik olarak verileri kaydedebilen sert metal plakalardan ve elektronik devrelerden oluşan cihazdır. Sabit disk bilgisayar içerisinde olabildiği gibi harici olarak da kullanılabilir[230].

Sabit diskin üzerinde dokümanlar, kelime işlemci dosyaları, resimler, ses ve video dosyaları, veri tabanı dosyaları, veri tabanı erişim kayıtları, e-mail ve chat kayıtları, internet geçmişi, erişim şifreleri ve kullanıcı adları, silinmiş dosyalar ve silinmiş disk alanları, şifrelenmiş veya kriptolanmış dosyalar, dosya yetkileri ve tarihleri, sistem tarafından verilen hizmetler, Virüs, Trojan, SpyWare vs. gibi zararlı yazılımlar, sistem üzerinde yüklü yazılımlar, sanal disk alanları ve RAM bilgileri gibi elektronik deliller bulunabilmektedir[231].

Türkçeye "rastgele erişimli bellek" olarak çevrilen RAM, merkezi işlem birimine yardımcı olan yongalar olup bilgisayar içinde işletim sistemi, uygulama programları ve işlenen verinin tutulduğu ve de işlemci tarafından hızlı bir şekilde erişimin sağlandığı bellektir. Merkezi işlem birimi tarafından kullanılan veriler geçici olarak bu bellekte tutulur ve veri üzerindeki işleme faaliyeti bitince yeniden asıl depolandıkları yere geri dönerler. Yani bellekteki veriler burada kalıcı olarak bulunmazlar. "Rastgele erişim" denilmesinin nedeni ise işlemcinin, RAM'in herhangi bir bölümündeki veriyi istediği yerinden okumaya veya yazmaya başlayabilmesinden kaynaklanmaktadır. Bu geçişler ardışık, sıralı veya belirli zamanlarda da olabilir[232].

Uçucu veriler, failin bilgisayarının internete bağlı olduğu durumlarda bilgisayarın internet protokol adresini, bağlı bulunduğu diğer bilgisayarları ve açılmış olan portlar (bağlantı kapıları) gibi bilgileri ifade eder. Bu bilgilerin tespit edilmesi mümkündür ve bunlar delil niteliğindedirler. Bağlı şekli ne olursa olsun geçerli kullanıcı, geçerli gün ve saat, bilgisayarın ne kadar süre ile açık konumda olduğu, işletim sisteminin kurulma

[230] Dülger, s. 665-666.

[231] Kaygısız, s. 300.

[232] Aysan Şentürk (Ed.), **Bilgisayar Kullanımı ve İnternet**, Ankara: Ekin Yayınevi, 2007, s. 17-18.

tarihi ve kayıtlı sahibinin kim olduğu tespit edilebilir. Uçucu veri sabit diske depolanmayıp RAM'da depolanmaktadır. Uçucu olarak nitelendirilmesinin nedeni ise bilgisayara güç akışının kesilmesi durumunda bu verilerin anında siliniyor ve kurtarılamıyor olmasıdır[233].

RAM üzerindeki sistem saati ve tarihi, sistemde bulunan geçerli kullanıcının adı, sistemde açık olan portlar (bağlantı noktaları) ve hizmetler, sistemde yürürlükte olan geçerli işlemler, sistemde açık olan dosyalar, hali hazırda veya daha önce sisteme bağlanmış olan diğer sistemler, bütün dosyaların oluşturma, düzeltme ve erişilme saatleri, PAGEFILE. sys dosyası vs. gibi uçucu veriler RAM'den elde edilebilecek elektronik delillere örnek olarak gösterilebilir[234].

Elektronik delil, bilgisayarın herhangi bir bileşeninde bulunabilir. Bilgisayarın her bir bileşeninde bulunan elektronik delile, gerek ispat açısından işlevi gerekse elde ediliş biçimi bakımlarından yaklaşım yöntemi farklı olacaktır. Nitekim sabit disk bünyesinde bulunan verilerin elde edilmesi ile RAM üzerinde bulunan uçucu verilerin elde edilmesine ilişkin yöntemler birbirinden farklıdır. Bu durum da bilgisayar donanımlarının tespiti hususunu önemli kılmaktadır[235].

1.7.1.4.2. Floppy ve CD/DVD/BluRay

Floppy disketler ve CD/DVD/BluRay formatındaki kayıt ortamları, taşınabilir depolama araçları olarak kullanılır ve manyetik alan veya lazer işleme yöntemi ile üzerlerine veri kaydedilebilir. Floppy disketlerde ve RW uzantılı CD/DVD/BluRay'ler üzerinde veri değişikliği yapılabilmesine karşın diğer CD/DVD/BluRay kayıt ortamlarında yazma işleminin oturumu kapatıldıktan sonra veri değişikliği yapılamamaktadır[236].

Floppy disketlerde ve CD/DVD/BluRay'ler üzerinde dokümanlar, kelime işlemci dosyaları, resimler, ses ve video dosyaları, veri tabanı dosyaları, veri tabanı erişim

---

[233] Dülger, s. 666.

[234] Cem Günal, "Adli Bilişim ve Delillerin Toplanması", **Özyeğin Üniversitesi Hukuk Fakültesi Bilişim Hukuku Sertifika Programı Sunumu**, İstanbul, 18 Şubat-11 Mart 2012, s. 24.

[235] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 46.

[236] Dülger, s. 666.

kayıtları, şifrelenmiş ve kriptolanmış dosyalar, floppy disketler ve CD/DVD/BluRay'lerin oluşturulma tarihleri gibi elektronik deliller elde edilebilir[237].

1.7.1.4.3. Hafıza Kartları

Hafıza kartları, bilgisayarlar, dijital kameralar, dijital fotoğraf makineleri, cep telefonları, el bilgisayarları, dijital not defterleri, müzik/video oynatıcılar, video oyun konsolları ve benzeri elektronik cihazlarla beraber kullanılan küçük veri depolama aygıtlarıdırlar[238].

Boyutları her geçen gün artan hafıza kartları, karttan güç kesildiğinde bile bilgilerin kaybedilmediği elektronik kayıt cihazlarındandır. Silinmiş ancak üzerine yeni veri kaydedilmemiş kayıp verilerin hafıza kartlarından kurtarılması da mümkündür[239].

Hafıza kartlarında, ses, video ve fotoğraf dosyaları, dokümanlar, kelime işlemci dosyaları, küçük veri tabanı dosyaları, veri tabanı erişim kayıtları, şifrelenmiş veya kriptolanmış dosyalar, USB hard disk ve flash disklerde silinmiş dosyalar ile disk alanları ve mevcut dosyaların alanları gibi elektronik deliller elde edilebilir[240].

1.7.1.4.4. Taşınır Bellekler (Flash Memory)

Taşınır bellekler, flash bellek ve parmak disk gibi farklı isimlerle de kullanılan, USB ara birimi üzerinden bilgisayara bağlanan, küçük ve hafif veri depolama aygıtlarıdır. Taşınması ve gizlenmesi en kolay veri depolama birimleridir[241]. Yonga (çip) içinde bilgi tutmak için elektriğe gereksinim duymaz. Bilgisayarlarda kullanılan RAM kadar hızlı olmamakla birlikte yüksek hızda veri okuma özelliğine sahiptir. Sarsıntılara karşı sabit disklerden daha fazla direnç göstermelerinden dolayı kullanımı oldukça yaygındır.

[237] Kaygısız, s. 300-301.

[238] Henkoğlu, s. 229.

[239] Dülger, s. 666.

[240] Kaygısız, s. 302.

[241] Henkoğlu, s. 228.

Bu nedenle de elektronik delil tespitinde başvurulan en önemli araçlardır[242]. Hafıza kartlarından elde edilebilen elektronik deliller taşınır bellekler için de söz konusudur.

1.7.1.4.5. Cep Telefonları ve SIM Kartlar

Günümüzde cep telefonları bilgisayarların fonksiyonunu icra edebilen bir niteliğe sahip olmuştur. Bu bakımdan cep telefonları elektronik delillerin çokça rastlandığı cihazlardan olduğu söylenebilir. Cep telefonunun konuşmak, elektronik posta göndermek, mesaj atmak, ses veya görüntü kaydı yapmak amacıyla kullanılması bir yönüyle daha sonra kullanılması muhtemel elektronik delillerin oluşturulması anlamını taşımaktadır[243].

Günlük kullanımda önemi her geçen gün artan ve teknolojik gelişmelere paralel olarak bilgisayarlarda bulunan birçok özelliği de bünyesinde barındıran cep telefonları, gerek mevcut gerekse silinmiş kısa mesajlar (SMS), telefon rehberi kayıtları, son aramalar listesi gibi elektronik delilleri barındırırlar. Ayrıca kapasitelerine bağlı olarak, müzik ve fotoğraf dosyaları, videolar, kelime işlemci program ve belgeleri de depolayabilmektedirler. Akıllı telefonlar her yönüyle bilgisayarlarla benzerlik gösterdikleri için bilgisayar incelemelerinde kullanılan inceleme ve yöntemler bu cihazlar bakımından da geçerlidir[244].

SIM kartlar ise, bir cep telefonunun GSM şebekesinden hizmet alabilmesi için gerekli olan abone kartı olarak tanımlanabilir. SIM kartlar dâhili bir belleğe sahip olup bu bellekte adli bilişim açısından önemli elektronik delilleri barındırabilmektedirler. Bu deliller arasında telefon rehber bilgileri, son arama bilgileri (arayan, aranan ve cevapsız çağrı bilgileri), kısa mesajlar (SMS) ve GSM şebekesine ait bilgiler bulunmaktadır[245].

---

[242] Burak Çekiç, "İnternet Aracılığı İle İşlenen Suçlar", (**Yayınlanmamış Yüksek Lisans Tezi**, Marmara Üniversitesi SBE, 2006), s. 12.

[243] Daniel and Daniel, s. 8.

[244] Günal, s. 29.

[245] Aydoğan, s. 80.

1.7.1.4.6. Dijital Kamera ve Fotoğraf Makineleri

Dijital kamera, görüntüler ve videolar için dijital kayıt yapabilen, ayrıca saklama aracı ve sohbet donanımı ile birlikte görüntüleri ve videoları bilgisayarlara aktarabilen aygıtlardır. Dijital kameralar görüntüleri ve/veya videoları dijital formatta kaydetmekte ve bunları daha sonra izlemek veya düzenlemek amacıyla bilgisayar, televizyon gibi araçlarla transfer edebilmektedir. Dijital kameralar ve fotoğraf makinelerinde yer alan görüntüler, video kayıtları, tarih ve zaman damgası[246], ses kayıtları, hafızalarındaki silinmiş veriler bu cihazlardan elde edilebilecek en önemli elektronik delillerdir[247].

1.7.1.4.7. Mp3 Çalar/IPod

Mp3 çalarlar hafıza kapasitelerine bağlı olarak birçok elektronik delili bünyesinde barındırabilmektedirler. Mp3 çalarların çoğunun aynı zamanda taşınabilir bellek olarak da kullanıldıkları görülmektedir. Ayrıca bu cihazlar gelişen teknolojiye bağlı olarak çeşitli fonksiyonlara sahiptirler. Mp3 çalarların radyosunun bulunması, depolanmış fotoğrafı ve videoları oynatabilme özellikleri ve internete bağlanabilmeleri, bu cihazlardan elektronik delil elde etme imkânını artırmaktadır[248].

MP3 çalarların gerek kendi hafızaları gerekse ek hafıza kartları flash bellek olarak kullanılabildiklerinden incelemenin bu doğrultuda geliştirilmesi gerekmektedir. MP3 çalarlardan elde edilen en önemli elektronik deliller ses kayıtları, olması muhtemel sair dosyalar ve silinmiş verilerdir[249].

1.7.1.4.8. El Bilgisayarları (PDA, PLAM, Pocket PC)

El bilgisayarları gün geçtikçe yaygınlaşmakta ve özellikle iş hayatında tercihen kullanılır hale gelmektedir. Bu cihazlar, üzerlerinde küçük ve kendilerine has işletim sistemleri bulunan cihazlardır. Bu cihazlar, içerlerinde bir işletim sistemi barındırdıklarından dolayı bilgisayar statüsünde değerlendirilerek adli bilişim uzmanları

[246] Günal, s. 30.

[247] Kaygısız, s. 301.

[248] Günal, s. 31.

[249] Kaygısız, s. 301.

tarafından incelenmeleri gerekir. Bu bakımdan el bilgisayarlarının harici ve dâhili depolama birimlerinde elektronik delil niteliğinde çeşitli dijital veriler bulunabilir[250].

Diğer taraftan el bilgisayarları, ajanda işlevi gören, çeşitli ofis programlarını (MS Word, MS Excel v.b) kullanma hizmeti verebilen ve hatta kablosuz ağlar aracılığıyla internete girebilme özelliğine sahip cihazlar olduklarından bu cihazlarda bilgisayarda rastlanan türde elektronik delile rastlamak imkân dâhilindedir[251].

1.7.1.4.9. Yazıcı ve Fakslar

Günümüzde bazı yazıcı ve faks cihazları oldukça gelişmiş özelliklere sahiptirler. Bu cihazların bünyelerinde kapasiteleri sınırlı da olsa veri depolama (hafıza) üniteleri bulunmaktadır. Bazı yazıcı ve fakslar hafızalarında son işlenen belgelerin kopyalarını, işlenme tarihlerini ve cihazın özelliğine göre daha pek çok bilgiyi tutabilmektedirler. Bu bakımdan yazıcılar üzerinde, son yazdırılan belgeler, yazdırma tarihi ve adedi, kullanıcıya ait kullanım kayıtları, faks cihazları üzerinde ise son gönderilen ve son alınan belgenin kopyası, gönderilme ve alınma tarih ve saatleri, gönderilme ve alınma adedi ile kayıtlı kullanıcı bilgileri gibi elektronik delillerin elde edilmesi mümkündür[252].

1.7.1.4.10. Oyun Konsolları

Gençlerin önceleri atarilerde sonraları ise bilgisayar sistemlerinde oynadıkları oyunların yerlerini, ses kalitesi ve neredeyse gerçek zamanlı görüntü hizmeti nedeniyle, oyun konsollarına bıraktığı görülmektedir. PlayStation ve XBOX isimleriyle bilinen bu oyun konsollarındaki gelişmeler sonucunda bünyelerinde bilgisayar sistemlerinde bulunan işlemciler ve veri depolama birimi niteliğindeki sabit diskler yer almaya başlamıştır. Özellikle XBOX gibi cihazlarda bazı modifikasyonlar ile cihazın veri depolama birimi üzerinde Linux işletim sistemi yüklenebilmektedir. Bu şekilde neredeyse bir PC* özelliğini alan oyun konsolları üzerinde her türlü elektronik delili bulmak mümkündür. Bu bakımdan soruşturma sırasında elde edilen oyun konsollarının elektronik delil ihtiva

[250] Ekizer, http://www.ekizer.net/adli-bilisim-computer-forensics (06 Nisan 2014).

[251] Dülger, s. 667.

[252] Kaygısız, s. 304-305.

* Personal Computer (PC): Kişisel Bilgisayar

edebilecekleri göz ardı edilerek sadece bir oyun cihazı olarak değerlendirilmesi soruşturmada bulunabilecek muhtemel delillerin elde edilememesine neden olabilecektir[253].

1.7.1.4.11. Ağ (Network) Cihazları

Birçok ağ (network) cihazı (router, switch, hardware firewall vs.) üzerlerinde ağ aktivesi, erişim denetimi ve ağ yapılandırması gibi verileri barındırabilmektedir. Bu cihazların incelenmesi sonucunda adli bilişim uzmanı ağ sistemlerini ileri düzeyde bilmek zorundadır. Ağ cihazları üzerinde bulunabilecek veriler yine cihazın özelliklerine göre oldukça farklılık gösterebileceğinden incelenecek cihazı tanımak, cihazın fabrika verilerini ve özelliklerini bilmek, incelemeye başlamadan önce yol haritası çizilmesi bakımından oldukça önemlidir[254].

Ağ cihazlarının üzerinde ağın yapılandırma şekli, erişim ve yönlendirme bilgileri, erişim denetim listeleri, donanım tabanlı cihaz listeleri (MAC ID), ağ üzerinde oluşmuş bazı arıza bilgileri, ağın performans ve kullanım bilgileri ve ağ üzerinde yetkisiz erişim bilgileri gibi elektronik deliller elde edilebilir[255].

1.7.1.4.12. İnternet ve Ağ (Network) Ortamları

Önceleri yalnızca bilişim sistemleri üzerinden elektronik delil elde etmeye yönelik araştırmalar söz konusuyken, günümüzde birbiriyle bütünleşmiş sistemlerden oluşan bilgisayar ağlarının ve bu ağların gelişmesiyle ortaya çıkan internetin bilişim aktivitelerinin temelini teşkil etmesi sonucunda, internet ve ağ ortamları üzerinden de elektronik delil elde etmeye yönelik çalışmalar yoğunlaşmıştır[256].

İnternet ve ağ ortamlarında elektronik veriler sürekli akışkanlık sağlamaktadırlar. Bu bakımdan bu ortamlarda da elektronik delil elde etmek mümkündür. Bilişim sistemlerinde bulunması gereken birçok elektronik veri bu ortamlardan elde edilebilirse

---

[253] Ekizer, http://www.ekizer.net/adli-bilisim-computer-forensics (06 Nisan 2014).

[254] Kaygısız, s. 305.

[255] Kaygısız, s. 305.

[256] Yusuf Uzunay, "Bilgisayar Ağlarına Yönelik Adli Bilişim", **İzmir Yüksek Teknoloji Enstitüsü Adli Bilişim Çalıştayı**, İzmir, 19-20 Mayıs 2005, s. 1.

de bu verilerin delil olarak geçerliliğini sağlayabilmesi için teknik seviyeden anlaşılabilir seviyeye iyi bir şekilde dönüştürülerek açıklanmaları gerekmektedir[257].

Bununla birlikte, ağ ortamı üzerinden elde edilen elektronik verilerinin analizi, bilişim sistemlerinden elde edilen verilerin analiz işleminden farklıdır. Zira bilişim sistemi veya depolama aygıtlarında bulunan veriler (RAM üzerindeki veriler hariç), cihazlar kullanılmadığı zaman halen incelenebilir durumda olmasına karşın ağ üzerindeki veriler devamlı olarak değişmektedir. Canlı bir ağ analizi ise, sadece belirli bir zamana ilişkin trafiğin yakalanarak (snapshot) daha sonra detaylı olarak incelenmesi ile mümkündür[258].

İnternet ve ağ ortamları üzerinde birçok yerden elektronik delil elde etmek mümkündür. Bu bağlamda internet ve ağ ortamlarındaki başlıca elektronik delil kaynakları, istemci bilgisayar sistemleri, sunucu bilgisayar sistemleri, ağ aktif cihazları, güvenlik sistemleri ve gömülü sistemlerdir[259].

Kullanıcıların web istekleri ve elektronik postaları gibi belirli bir incelemeye yönelik bilgiler, girişim tespit cihazlarında olduğu gibi sadece saldırı olarak tanımlanacak alarm bilgileri, tek başına anlam ifade etmeyen ve fakat diğer bilgilerle birlikte analiz edildiğinde önem arz eden bilgiler ve ağ üzerinde bulunan bütün sunuculardaki her türlü bilgi bu ortamlarda bulunması muhtemel elektronik deliller olarak sayılabilir[260].

1.7.1.4.13. GPS (Global Positioning System) Cihazları

GPS, düzenli olarak kodlanmış bilgi transferi sağlayan bir uydu ağıdır. Uydular arasındaki mesafenin ölçülmesi suretiyle dünya üzerindeki yerin tespit edilmesi işlemi gerçekleştirilmektedir. Farklı uydulardan gelen farklı sinyalleri navigasyon cihazı üçlü kestirme yapmak suretiyle, üzerinde yüklü bulunan haritadaki kesin yeri bulabilmektedir. GPS verileri, kişilerin kamuya açık olan yollar üzerindeki güzergâhlarını tespit etmesi nedeniyle kişilerin yer bilgileri üzerinde mahremiyet

[257] Kaygısız, s. 305.

[258] Tuncay Ercan ve Doğukan Nacak, "Kablosuz Ağlardaki Paket Trafiğine Adli Bilişim Yaklaşımı", **Journal of Yaşar University**, Cilt. 4, Sayı. 13, (2009), s. 1911-1912.

[259] Uzunay, Bilgisayar Ağlarına Yönelik Adli Bilişim, s. 7-8.

[260] Ercan ve Nacak, s. 1912.

beklentisinin bulunmayacağı genel olarak öne sürülmektedir. Bununla birlikte, GPS verilerinin sıkça kullanıldığı Amerikan hukukunda, GPS takip sistemlerinin kullanılmasının kişinin mahremiyet beklentisini ihlal etmediği ileri sürülmekteyse de kişinin belirli bir zaman diliminde sürekli yer tespiti işleminin mahkeme kararı gerektireceği de ifade edilmektedir[261].

1.7.1.4.14. Bulut Bilişim

Teknolojik gelişmelere ve bilişim hizmetlerinin internet erişimine açık hale gelmesine bağlı olarak elektronik verilerin yalnızca yerel bilişim sistemlerinde saklanması yerine uzak bilişim sistemlerinde saklanarak ve belirli bir mekâna bağlı kalmaksızın ihtiyaç duyulan her yerde ve zamanda erişim sağlama yolunu olanaklı kılmaya yönelik bulut bilişim modeli oluşturulmuştur.

Bu bağlamda, basit tanımlamayla bulut bilişim, kurumların işlerini yürütürken yararlandıkları bilişim sistemlerine ilişkin hizmetleri üçüncü taraflardan internet üzerinden alınmasını ifade etmektedir. Bulut bilişim sayesinde, bir kurumda bulunan bilişim sisteminden beklenen hemen hemen her türlü hizmet (uygulama, veri saklama, yedekleme, bilgi işleme, uygulama geliştirme, iletişim vb.) sağlanabilmektedir[262].

Bulut bilişim uygulamasında istenilen bilgiye her yerden ve her nevi bilgi iletişim cihazı (PC, Mac, iPhone, Android ve BlackBerry) kullanmak suretiyle erişim mümkün olduğundan dolayı donanım kaynaklı sorunlar yaşanmamakta, fiziksel sunuculardan daha hızlı çalışan sanal bilgisayar ile yüksek erişebilirlik imkânı sunulmakta, bellek ve disk değişikliği gerekmeksizin esnek yapı kullanılabilme imkânı sunulmaktadır. Bütün bu avantajlı yönleri dikkate alındığında, bilgi teknolojilerindeki gelişimin yansıması olarak ortaya çıkan bulut bilişimden uzak durmak ya da alternatif yöntemlerde ısrarcı olmak akılcı bir çözüm olarak görünmemektedir[263].

---

[261] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 152.

[262] Özcan Rıza Yıldız, "Bilişim Dünyasının Yeni Modeli: Bulut Bilişim (Cloud Computing) ve Denetim", **Sayıştay Dergisi**, Sayı. 74-75, (Temmuz-Aralık 2009), s. 7.

[263] Türkay Henkoğlu ve Özgür Külcü, "Bilgi Erişim Platformu Olarak Bulut Bilişim: Riskler ve Hukuksal Koşullar Üzerine Bir İnceleme", **Bilgi Dünyası Dergisi**, Cilt.14, Sayı.1, (Nisan 2013), s. 64.

Kamu veya özel sektör ayırımı yapmaksızın eski sorunlara yeni çözümler sunan bulut bilişim sayesinde tüm kurumlar, iş yapma sistemlerinde değişime gitmektedirler. Bu kapsamda, daha az maliyet, daha az nitelikli bilişim personeli, daha esnek ve daha az karmaşık bir yapıyla çok daha iyi ve kaliteli hizmet verilmesi kamu kurumlarının önceliği olmaktadır. Ülkemizde kamu kurumları için henüz böyle bir çalışma bulunmamakla birlikte, bazı uygulamaların belirli merkezlerde tutulmaya başlandığı görülmektedir. Bulut bilişime tam uymamakla birlikte Say2000i uygulaması, Ulusal Yargı Ağı Projesi (UYAP) ve MERNİS bu modele örnek teşkil etmektedir[264].

Bulut bilişimde, diğer bilişim sistemleri ve bağlı donanımlarından elde edilmesi muhtemel ses, video ve fotoğraf dosyaları, dokümanlar, kelime işlemci dosyaları, küçük veri tabanı dosyaları, veri tabanı erişim kayıtları, şifrelenmiş veya kriptolanmış dosyalar, silinmiş dosyalar gibi pek çok elektronik delil elde edilebilme olanağı bulunmaktadır.

1.7.1.4.15. Diğer Donanımlar

Elektronik delilin bulunduğu ortamlar yukarıda sayılanlardan ibaret değildir. Sayıları her geçen gün artmakta olan ve elektronik delil ihtiva edebilecek elektronik cihazların arasına modemler, kredi kartı kopyalama cihazları, telesekreterler ve bunun gibi pek çok cihazı eklemek mümkündür.

1.7.1.5. Elektronik Delilin Özellikleri

Amerika Birleşik Devletleri Adalet Bakanlığı Ulusal Adalet Enstitüsü'nün yayınlamış olduğu "Elektronik Olay Yeri Soruşturması" kılavuzunda elektronik delilin yapısal özellikleri açıklanırken dört husus üzerinde durulmaktadır. Buna göre elektronik delil;

- DNA ve parmak izi delilleri gibi gizlidir (latent yapıdadır);
- Kolaylıkla değiştirilebilir, bozulabilir veya yok edilebilir;
- Dünya çapında bir alana dağılmış olabilir;

[264] Özcan Rıza Yıldız, s. 6, 13.

- Zamana bağlı olabilir[265].

Elektronik delilin gizli (latent) bir yapıda olduğu ifadesiyle bu delil türünün ortaya çıkartılabilmesi için özel cihaz ve yazılımlarla incelenmesi gerektiği vurgulanmaktadır. Belirli yöntemler dâhilinde incelemesi yapılmayan elektronik delilin ortaya çıkartılabilmesi mümkün değildir[266].

Gerçekten de elektronik delil soruşturma kapsamında elektronik cihazlarda saklanan veya bu cihazlardan aktarılan veri ve bilgiyi ifade etmektedir. Bu anlamda elektronik delil aynen DNA ve parmak izi gibi gizli yapıya sahip delil türlerindendir. Bu bakımdan elektronik cihaz içerisinde saklı bulunan elektronik delilin doğal halleriyle görülmeleri mümkün değildir. Bu delillerin görünür hale getirilebilmesi için bazı yazılım ve donanıma ihtiyaç duyulmaktadır. Kimi zaman analiz süreci veya herhangi bir sürecin açıklanmasına yönelik tanık beyanı da gerekebilir[267].

Bu bağlamda elektronik delillerin içerisindeki dijital verileri anlayabilmek için mutlaka alet ve cihazlar ile nicel gözlem yapılmalıdır. Zira genellikle makine dili ile kodlanmış olan bilgilerin yine bir makine tarafından[268] özel teknik ve yöntemlerle, delil niteliğini kaybetmeden toplanmaları, analiz edilmeleri ve mahkemeye sunulmaları gerekmektedir[269].

Elektronik delilin değiştirilmesi ve bozulması diğer fiziksel delillerin tahrip edilmelerinden daha kolay ve daha kısa zamanda gerçekleşebilmektedir. Elektronik delilin yapısında, özellikle elde edilmesi sırasında, kolayca ve kimi zaman tespiti mümkün olmayan değişiklikler yapılması söz konusu olabilmektedir. Bu bakımdan

[265] John Ashcroft (Ed.), "Electronic Crime Scene Investigation: A Guide for First Responders", Washington: PhotoDisc, Inc, 2001, https://www.ncjrs.gov/pdffiles1/nij/187736.pdf (09 Eylül 2014), s. 6.

[266] Aydoğan, s. 31.

[267] Ashcroft (Ed.), s. 2.

[268] Say, Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi, s. 29.

[269] Henkoğlu, s. 2.

elektronik delilin elde edilmesi aşamasında çok daha fazla hassasiyet gösterilmesi gerekir[270].

Elektronik delilin içerisinde bulunan veriler dijital formatta kaydedilmektedir. Verilerin dijital formatta kaydedilebilmeleri için ise elektrik enerjisine ihtiyaç duyulmaktadır. Elektrik enerjisinin kesilmesi nedeniyle verilerin kaybolmaması için sabit disk gibi dijital depolama medyalarında manyetik saklama teknolojisinin kullanılması, verilerin silinmesini engellememektedir. Elektronik yöntemlerle yazılan veriler yine elektronik yöntemlerle silinebilir. Bu nedenle elektronik delil içerisinde bulunan dijital veriler, elektrik enerjisine maruz kaldıkları zamanlarda silinme olasılığıyla yüz yüzedirler. Uzmanlar tarafından, uygun aletlerle yapılmayan müdahalelerde elektronik delilin silinmesi veya değiştirilmesi kaçınılmazdır. Elektronik delil, bu hassas yapılarından dolayı mutlaka uzmanlar tarafından incelenmelidir[271].

Bilişim ve iletişim teknolojileri, özellikle de günümüzde küresel ağ halinde dünyayı kaplayan internet [272] ile elektronik veriler, sınırları kolaylıkla aşabilmektedir. Bu bakımdan elektronik ortamda işlenen suçlarda, mekân ve mesafe kavramlarının anlamını yitirdiği görülmektedir. Bu tip suçlarda suçun işlenmiş olduğu yer, bilgisayar sistemleri, elektronik veri saklama ortamları, bilgisayar ağları ve internetin sanal sonsuzluğudur.

Gerçekten de, özellikle internet üzerinden gerçekleşen bir iletişimde artık coğrafi sınırların anlamının kalmadığı görülmektedir. Sınır aşan ihlaller bu yolla işlenen suçların en belirgin özelliğini oluşturmaktadır. Bu şekilde işlenen suçlarda, klasik suçlarda olduğu gibi fail ile mağdurun göz göze gelmesi söz konusu değildir[273].

---

[270] Karagülmez, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, s. 394; Servet Yetim, "Dijital Kanıt Araştırma Yöntemleri", **İstanbul Barosu Dergisi**, Cilt. 82, Sayı. 3, (Mayıs-Haziran 2008), s. 1208.

[271] Say, Data İncelemeleri, s. 513.

[272] Özgür Uçkan ve Yasin Beceni, "Bilişim-İletişim Teknolojileri ve Ceza Hukuku", **İnternet ve Hukuk**, Yeşim Atamer (drl.), İstanbul: Bilgi Üniversitesi Yayınları, 2004, s. 364.

[273] Özgür Kamışlık, "Bilişim Hukukunda Delillerin Toplanması", **Ankara Barosu Uluslararası Hukuk Kurultayı**, Cilt. 2, Ankara, 08-11 Ocak 2008, s. 159.

Suç işlemeye meyilli kişilerin internet aracılığı ile dünyanın diğer ucundaki bilgisayar sistemlerini zarara uğratmaları mümkündür. Bu tür sınır aşan suçlarda incelenmesi gereken bilgisayarlar dünyanın öbür ucunda olabilir ve hatta suçta kullanıldığı düşünülen bilgisayar gerçekte kolluğu yanıltmak için kullanılan ve suçla ilgisi bulunmayan bir kimsenin bilgisayarı dahi olabilir[274]. Şüphesiz ki bu durum delil elde etmeyi zorlaştıran önemli bir etkendir.

Yazılım endüstrisinin gelişmesiyle birlikte bilgisayar yazılımları çeşitli alanlarda kullanılmaya başlanmıştır. Nitekim günümüzde bilgisayar yazılımlarının sayısı sayılamayacak düzeydedir. İnternet üzerinden serbestçe dağıtılabilen ve indirilebilen yazılımlardaki güvenlik açıkları ise bilgisayarları sürekli tehdit eder boyuttadır. Zira bilgisayar üzerinde çalışan ve güvenilir kaynaklardan elde edilmemiş yazılımların arka planda ne türlü işlemler yürüttüğünü tespit etmek kolay değildir. Bu bağlamda, bilgisayar monitöründe herhangi bir işlem yapıyor gibi görünen bir programın esasen aynı anda bilgisayarın sabit diski üzerinde saklanan suç unsuru verileri siliyor olması muhtemeldir. Bu durum, elektronik delilin zamana bağlı olduğunu göstermektedir. Bu tip durumlarda elektronik delil derhal elde edilemezse bu delilin değişmesi veya kaybolması sonucuyla karşılaşılabilir.

1.7.1.6. Elektronik Delil İle Fiziksel Delil Arasındaki Farklar

Elektronik ortamda milyarlarca bilgi ve belgeyi saklayabilmek çok kolaydır. Fiziksel delil bakımından böyle bir imkân söz konusu değildir. Örneğin bir kütüphane dolusu kitaba karşılık gelebilecek elektronik veri 1-2 cm büyüklüğüne dahi ulaşmayan hafıza kartlarında taşınabilmektedir[275].

Ceza yargılamasında kullanılan fiziksel delil somut nitelikte olup üzerinde elkoyma ve muhafaza altına alma kararı verilerek kolayca elde edilebilir nitelikte bir delil olmasına karşın elektronik delil ise soyut niteliğe sahiptir. Her ne kadar elektronik delilin içerisinde yer aldığı somut bir donanım aygıtı mevcut ise de, ceza yargılaması

[274] Kubilay Say, "Bilişim Suçlarında Olay Yeri İncelemesinin Hukuki Boyutu", Levent Bayram (Ed.), **Ses Görüntü ve Data İncelemeleri** içinde (251-260), Ankara: Adalet Yayınevi, 2008, s. 257.

[275] Yavuz Erdoğan, **Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa Konseyi Siber Suçlar Sözleşmesi ve Yargıtay Kararları İle)**, İstanbul: Legal Yayıncılık, 2012, s. 405.

bakımından esas teşkil eden bu donanım aygıtının kendisi olmayıp içerisinde yer alan dijital nitelikteki verilerdir[276]. Bu bakımdan bilgisayar ve diğer elektronik cihazlarda gözle görülemeyecek şekilde saklı bulunan elektronik delilin görülebilmesi için mutlaka bir işlemden geçirilmesi gerekmektedir. Bunun için ekran veya yazıcı gibi yardımcı cihazlara da ihtiyaç duyulur[277].

Elektronik delile ulaşılması ve böyle bir delilin toplanarak muhafaza altına alınması kendine mahsus özellikler arz eder. Elektronik delil somut aygıtın içerisinde bulunan soyut verilerden ibarettir. Bu bakımdan içerisinde delil bulunduğu şüphesiyle muhafaza altına alınan bir elektronik aygıtta suç delilinin bulunup bulunmadığı net olarak belli değildir. Dolayısıyla elektronik delilin toplanmasında delil olarak düşünülen aygıtın suça ulaşmada vasıta olup olmayacağı fiziksel delile nazaran daha belirsiz bir konumdadır[278].

Elektronik delilin incelemesi, değerlendirilmesi ve analizi fiziksel delile nazaran daha karmaşık, teknik uzmanlık gerektiren ve masraflı bir iştir. Elde edilen elektronik verilerin bir hukuki delile dönüştürülmesi süreci belli bir prosedürü takip eder. Uygulanan bu prosedür sonucunda da elektronik delil kendisini bir hukuki delil olarak ortaya koyar[279].

Fiziksel delil genellikle sabit bir yapıdadır ve yapısal olarak değiştirilmesi zordur. Oysa elektronik delil, bilgisayar ve uzun iletişim hatları içerisinde her an yapısı değiştirilebilir. Bununla birlikte fiziksel delilde mümkün olan değişiklik yapıldığında bunun fark edilebilmesi kolaydır. Oysa elektronik delilin yapısında tespiti her zaman kolay olmayan değişiklik yapılabilmesi mümkündür. Elektronik delil elde edilme

[276] Özocak, s. 114; Aydoğan Tan, Adli Bilişim (Computer Forensic), 2009, http://mbasic.facebook.com/notes/gazi-%C3%BCniversitesi-adli-bili%C5%9Fim-anabilim-dal%C4%B1/adli-bili%C5%9Fim-computer-forensic-aydo%C4%9Fan-tan/502561823148516/?refid=17 (06 Nisan 2014).

[277] Göksu, s. 30.

[278] Özocak, s. 117.

[279] Tan, http://mbasic.facebook.com/notes/gazi-%C3%BCniversitesi-adli-bili%C5%9Fim-anabilim-dal%C4%B1/adli-bili%C5%9Fim-computer-forensic-aydo%C4%9Fan-tan/502561823148516/?refid=17 (06 Nisan 2014).

aşamasında da kolaylıkla değişikliğe uğrayabilir. Bu bakımdan, elektronik delilin elde edilmesi sırasında çok daha fazla özen gösterilmelidir[280].

Fiziksel delilin şüpheden uzak olmasını sağlamak çoğu zaman kolayken, elektronik delilin şüpheden uzak olmasını sağlamak her zaman mümkün değildir. Sanığın mahkûmiyeti için ise her türlü şüpheden uzak, kesin ve inandırıcı delilin elde edilmesi gerektiğinden şüpheden arındırılmamış bir delil mahkûmiyet hükmü kurulurken kullanılamaz[281].

1.7.1.7. Elektronik Delilin Nitelikleri

Elektronik delil mahkeme önünde etkin şekilde kullanılabilir nitelikte olabilmesi için diğer maddi delillerde olması gereken ve aşağıda belirtilen bazı niteliklere sahip olması gerekmektedir[282].

- Elektronik delil öncelikle kabul edilebilir olmalıdır. Bu delilin mahkemede kullanılabilir olması anlamına gelir. Bu kurala uyulmaması kanıtların olay yerinden toplanmaması ve soruşturma giderlerinin gereksiz yere artması anlamına gelir.

- Elektronik delil gerçek olmalıdır. Delil olayla bağlı olmalıdır ve ispatı sağlamaya yönelik ilişkiyi gösterebilmelidir.

- Elektronik delil eksiksiz, tam olmalıdır. Delil toplarken olayın sadece tek bir açıdan değerlendirilmesi yeterli değildir. Delil sadece failin eylemlerini ortaya çıkarmak adına toplanmamalı, ayrıca failin masumiyetini de ortaya çıkartabilir nitelikte olmalıdır.

- Elektronik delil güvenilir olmalıdır. Özellikle delil toplama ve analiz süreci delillerin gerçeklik ve güvenilirliğine gölge düşürmemelidir.

- Elektronik delil inandırıcı olmalıdır. Mahkemeye sunulan delil hâkim tarafından anlaşılabilir ve inanılabilir nitelikte olmalıdır.

---

[280] Karagülmez, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, s. 393-394.

[281] Yavuz Erdoğan, Türk Ceza Kanunu'nda Bilişim Suçları, s. 406.

[282] Kozushko, http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/DigitalEvidencePaper.pdf (12 Kasım 2013).

Yukarıda belirtilenlerin dışında elektronik delilin yasal kurallara uygun olması gerekir. Buna göre; elektronik delil yasada veya uyulması gerekli genel bir düzenlemede ayrıca açıklanmış olan (elektronik) delille ilgili kurallara da uygun olmak zorundadır. Bu bağlamda 5271 sayılı CMK m. 134'e aykırı olarak bilgisayarlarda arama, kopyalama veya elkoyma işlemi yapılması durumunda elde edilen elektronik delil yukarıda belirtilen niteliklere haiz olsa bile yasaya uygun sayılmayacaktır[283].

1.7.2. Elektronik Delille İlgili Karşılaşılan Sorunlar

Bir kanıt türü olarak elektronik delil, suç soruşturmasının uygulayıcıları bakımından birçok sorunu ihtiva etmektedir. Öncelikle son derece dağınık ve kaygan yapıya sahip bir kanıt türü olan elektronik delili elde etmek oldukça zordur. Örneğin, bir sabit disk, bilgi parçaları birbirine karışmış ve zaman içinde katmanlaşmış dağınık bir veri alaşımını içermektedir. Bu alaşımın ise sadece küçük bir kısmı soruşturmayla ilgili bulunmaktadır. Bu bakımdan, bu verilerden kullanışlı olanlarını çıkartarak onları bir arada, uygun ve yorumlanabilir bir biçime sokmak gerekir[284].

Bu durum ise elektronik verileri, delil haline getirecek kişilerin bu hususta uzmanlaşmasıyla mümkündür. Uzmanlaşmanın yanı sıra zaman faktörü de elektronik verinin elektronik delil haline dönüştürülmesi sürecini etkileyen önemli bir faktördür. Elektronik delilin elde edilmesi ayrıca zaman alıcı bir faaliyet olarak karşımıza çıkmaktadır[285].

Elektronik delil, dijital verilerden oluşmaktadır. Bu veriler ise bilişim sistemleri üzerinde kaydedilmiş 1 ve 0 değerlerine verilen anlam sonucunda ortaya çıkarlar. Dolayısıyla doğrudan elle tutulabilen ve gözle görülebilen bir yapının olmayışı dijital verileri soyut hale getirmektedir. Soyut kavramlardan kesinlik çıkartmak ise oldukça zordur. Bununla birlikte delillerin, işlevleri itibariyle bir suçu ispat edici nitelikte kesin

[283] Karagülmez, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, s. 395.

[284] Casey, Digital Evidence and Computer Crime, s. 25.

[285] Olgun Değirmenci, "Bilgi Toplumunun Delil Türü: Sayısal Deliller ve Bilimselliği", **Terazi Hukuk Dergisi,** Cilt. 9, Sayı. 97, (Eylül 2014), s. 22.

bulgular barındırmaları gerekir. Bu bakımdan, dijital verilerin yüzde yüz delil olarak kullanılması hususunda büyük sorunlar ortaya çıkabilmektedir[286].

Olay yerinden elde edilen elektronik verilerin, mahkemeye sunulana kadar muhafazasının sağlanması, hâkimin vicdani kanaatinin tam ve doğru delillere dayanarak oluşturulması açısından önemlidir. Bu bakımdan, elektronik delilin bütünlüğünün sağlanabilmesi, mevcut teknolojik gelişmelere rağmen karşılaşılan sorunlardan birini teşkil etmektedir[287].

Gerçekten de, elektronik delilin oldukça kolay manipüle edilebilir yapıda olması soruşturma uygulayıcıları bakımından yeni sorunları gündeme getirmektedir. Elektronik delil, kötü niyetli suçlular tarafından veya elde edilişi sırasında yanlışlıkla, bozulmaya ilişkin belirgin herhangi bir işaret bırakmaksızın değiştirilebilir. Bununla birlikte, elektronik delil bu sorunu hafifletecek birçok özelliğe de sahiptir. Şöyle ki;

- Elektronik delil, aynen çoğaltılamaz ve kopyası asıl delilmiş gibi incelenebilir. Nitekim söz konusu elektronik delil olduğunda onun kopyasının incelenmesi yaygın bir uygulamadır. Bu sayede orijinal delilin zarar görme riski önlenmiş olmaktadır.

- Elektronik delilin değiştirilmesi veya tahrif edilmesi durumunda, doğru araçlar kullanılarak orijinal delil ile karşılaştırma yapılması halinde bu durumun tespit edilmesi oldukça kolaydır.

- Elektronik delili yok etmek son derece zordur. Bir dosya silinse veya bir sabit disk formatlansa bile elektronik delil yine de kurtarılabilir.

- Suçlular elektronik delili yok etmeye çalıştıklarında, farkında olmadan elektronik delilin kopyasını veya onunla bağlantılı kalıntılarını yerlerinde bırakabilirler[288].

---

[286] Yusuf Uzunay ve Kemal Bıçakçı, "A3D3M: Açık Anahtar Altyapısı Destekli Dijital Delilleri Doğrulama Modeli", **Ağ ve Bilgi Güvenliği Ulusal Sempozyumu**, İstanbul, 9-11 Haziran 2005, http://www.emo.org.tr /ekler/ 4843973f9b66701ek. pdf. (31 Ekim 2014).

[287] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 188-189.

[288] Casey, Digital Evidence and Computer Crime, s. 26.

Bilişim sisteminde yer alan elektronik veri ile doğrudan bilişim sisteminin maliki arasındaki ilişkiyi her zaman kurmak mümkün değildir. Özellikle kötü niyetli veya casus amaçlı yazılımların (malware) kullanılması suretiyle herhangi bir bilişim sisteminin suçun işlenmesinde araç olarak kullanılması olasıdır. Bu gibi durumlarda suçun gerçek fail veya faillerine ulaşmak ancak bilişim sisteminde yer alan veri ile fail veya failler arasındaki bağlantının sağlanmasıyla mümkün olacaktır[289].

Bu nedenle elektronik delil, yürütülmekte olan münferit bir soruşturmanın yalnızca bir bileşeni (cüzü) olabilir. Eğer bir olgu, bilgisayar dosyalarının tarih-zaman damgaları gibi tek bir şekil veya katı bir soruşturma kaynağına dayandırılmış ise bu olgunun daha sonra beklenmedik şekilde zayıflatılması soruşturmayı olumsuz biçimde etkileyecektir. Mevcut elektronik delilin dışında ek bir delilin olmadığı durumlarda, suçun işlendiği sırada bilgisayarın başkası tarafından kullanıldığı tezi makul bir savunma olarak ileri sürülebilecektir[290].

Yukarıda da belirtildiği gibi günümüzde kötü niyetli veya casus amaçlı yazılımlar kullanılarak özgün mekanizması güvenli bilgisayarların devre dışı bırakılabilmelerinin yanı sıra herhangi bir şifreye ihtiyaç duymaksızın dahi birçok bilgisayara izin istenmeksizin erişim sağlanabilmektedir. Diğer taraftan, sanık, beraatını sağlayacak kimi delillerin sistemden toplanmadığını iddia etmesi durumunda, toplanan elektronik delil, sadece suçun varlığını destekleyen zayıf bir delil niteliğinde kalabilmektedir[291].

Benzer şekilde, truva atları gibi bazı zararlı programlar, bir bilgisayarı suçun işlenmesinde araç olarak kullandıktan sonra, geriye yönelik tüm izleri silebilmektedir. Maddi olaya, bu nitelikteki bir yazılımın neden olduğunun ortaya çıkartılması, sorumluların hukuki yaptırımla muhatap olmaları, ceza hukukunun özel ve genel önleyici amacının yerine getirilmesi bakımından gereklidir[292].

[289] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 176.

[290] Casey, Digital Evidence and Computer Crime, s. 26.

[291] Casey, Digital Evidence and Computer Crime, s. 26.

[292] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 188.

Diğer taraftan elektronik verilerin internet sayesinde kolaylıkla yer değiştirebilmesi, yine internet sayesinde verilere müdahale edilebilmesi, internet yoluyla işlenebilen ve bilişime mahsus suçların dünyanın herhangi bir yerinden kolaylıkla yapılabilmesi, karşımıza elektronik delillerin elde edilmesi ile ilgili ülkesellik ve yetki sorunlarını çıkarmaktadır. Dolayısıyla, dünyanın herhangi bir yerinde yapılan hareketle işlenen bir suçun Türkiye'de sonuç doğurması durumunda veya tam tersi bir durumda elektronik delil elde edebilmek oldukça güçtür. Bu soruna uluslararası sözleşmelerle ve adli yardımlaşmayla çözüm üretilmeye çalışılmaktadır. Ancak, bu konudaki kavramların, standartların ve suç tanımlarının ülkeden ülkeye değişken olması sebebiyle, sorunun bir süre daha devam edeceği gözükmektedir[293].

Son alarak belirtmek gerekir ki; elektronik delil çoğu zaman kişilerin atılı suç ile hiçbir ilgisi olmayan kişisel verilerinin de saklandığı bilişim sistemlerinde bulunmaktadır. Bu nedenle söz konusu bilişim sistemi içerisinde çok küçük bir alanda saklı bulunan soruşturmaya konu elektronik verinin tespiti ve elde edilmesi sürecinde şahısların kişisel verileri ifşa olmakta ve dolayısıyla özel hayatlarının gizliliğine müdahalede bulunularak mağduriyetlere neden olunmaktadır. Elektronik delile ulaşılamayan arama faaliyetlerinde ise bu mağduriyet daha da artmaktadır. Bu bakımdan elektronik delilin elde edilmesi sürecinde soruşturmanın aydınlatılması ile özel hayatın gizliliğinin korunması arasındaki menfaat dengesinin gözetilerek uygulamanın buna göre tesis edilmesi gerekmektedir.

1.7.3. Elektronik Delilin Geçerliliğinin Denetlenmesi

Hukuken elde edilen delillerin geçerli sayılabilmesi için gerekli bazı prosedürlerin yerine getirilmesi ve uluslararası standartları taşıması büyük önem arz etmektedir. Özellikle elektronik delil yapısı itibariyle, diğer suçlarda elde edilen fiziksel delillere nazaran daha hassas ve kolay bozulabilir nitelikte olduğu için birçok sorunu bünyesinde barındırmaktadır. Nitekim elektronik delilin elde edilmesi sırasında olay yerinde

[293] M. Gökhan Ahi, "Adli Bilişim Nedir ?", http://www.bilisimhukuk.com/2009/07/adli-bilisim-nedir/ (04 Mayıs 2014).

yapılacak en küçük hata, verilerin zarar görmesine veya yok olmasına neden olabilmektedir[294].

Bu bakımdan elektronik delilin elde edilmesi sürecinde olaya ilk müdahale eden ekipten, incelemenin uzman birim ve laboratuvarlarda yapılmasına ve bundan sonra da elde edilen sonuçların mahkemeye sunulması aşamasına kadar devam eden her aşama büyük önem taşımaktadır[295].

1.7.3.1. Hukuki Geçerliliğin Denetlenmesi

Elektronik delilin hukuki geçerliliğinin denetlenmesinde öncelikle hukukun temel gerekleri olan ve diğer delillerde bulunması gereken özellikler olan gerçeklik, akılcılık, erişebilirlik, olayı temsil edicilik, müştereklik ve hukuka uygunluk özelliklerine sahip bulunması zorunludur. Yukarıda bu özelliklerle ilgili bilgiler verildiğinden bu kısımda bu özelliklerin sadece elektronik delillerle ilişkisine temas edilecektir.

Delilin müştereklik özelliğinin gereği olarak, bir ceza yargılamasında öne sürülen elektronik delilin, davanın bütün taraflarınca bilinir ve tartışılabilir olması gerekmektedir. Elektronik delil, delillerin müşterekliği ilkesi bakımından diğer delillere nazaran daha avantajlı bir konumdadır. Zira daha soruşturma aşamasında dahi elektronik delilleri içeren ve kopyası alınan elektronik verilerin bir kopyası şüpheliye verilmektedir. Bu durum, çoğaltılabilme özelliğine sahip elektronik delil açısından bir avantaj niteliğindedir[296].

Gerçekten de, soruşturma veya kovuşturma makamlarında bulunan bir fiziksel delilin fail veya mağdur tarafından temin edilerek kendi istedikleri bir uzmana inceletmeleri mümkün değilken elektronik delil açısından böyle bir imkân bulunmaktadır. Örneğin, aleyhe delil niteliği arz eden bir bilgisayar diski, şüpheli tarafından başka bir uzmana incelettirilebilir ve buradan elde edilin yeni bilgiler şüpheli lehine kullanılabilir[297].

---

[294] Yusuf Uzunay , "Dijital Delil Araştırma Süreci", **2. Polis Bilişim Sempozyumu**, Ankara, 14-15 Nisan 2005, s. 46-47.

[295] Çakır ve Sert, s. 148.

[296] Hüseyin Akarslan, **Bilişim Suçları**, Ankara: Seçkin Yayıncılık, 2012, s. 132-133.

[297] Akarslan, s. 133.

Bununla birlikte ülkemiz uygulamasında kriminal laboratuvarlar dışında uzman mütalaası olarak getirilen ve yargı makamlarına sunulan raporların çoğu zaman dikkate alınmaması müştereklik ilkesini zedelemektedir[298].

Elektronik delil, akılcı, izah edilebilir ve rasyonel olmalıdır. Bu nedenle öngörüler ve zihin okuma araçlarıyla elde edilen elektronik veriler delil olarak kabul edilemezler[299]. Delilin akılcılık özelliği, bilimsel açıdan kabul edilebilir bir nitelik taşımasını da beraberinde getirir[300]. Delilin bilimsel olması ise özellikle bilişim sistemlerinden elde edilen elektronik deliller bakımından ayrı bir özellik arz etmektedir. Adli bilişim uzmanı, bilişim sisteminde yer alan veriyi elde etmekte ve analiz etmek suretiyle suçla ilgisini ortaya koymaktadır. Bu bağlamda bilirkişi niteliği bulunduğundan şüphe duyulmayan adli bilişim uzmanının elektronik delili elde etme ve yorumlama yöntemi, mahkemeyi etkileyecek ve kararın oluşmasına katkı sağlamaktadır. Her ne kadar adli bilişim uzmanının delil elde etme sürecine uyarak elde ettiği delil, mahkeme açısından bağlayıcı olmasa da maddi gerçeğin ortaya çıkartılması açısından oldukça önemlidir[301].

Elektronik delilin bilimselliği, delilin elde edilmesi aşamasında genel kabul gören yöntemlerin kullanılmasının yanı sıra elektronik delili elde eden soruşturma personelinin ehliyetiyle de doğrudan ilgilidir. Elektronik delili elde edecek personel, kolluk kuvveti veya savcılık/mahkeme tarafından atanan bilirkişi, adli bilişim konusunda sertifikayla da desteklenen bilgi düzeyine sahip olmalıdır[302].

Bununla birlikte, elektronik delilin bilimsel yöntemlerle elde edilmesi, onun delil değerini taşıması için gerekli ve fakat yeterli olan bir özellik değildir. Bilimsel yöntemlerle elde edilmeyen bir elektronik delil, geçerli bir delil olup olmadığı hususunda kuşku uyandıracaktır. Elektronik delilin bilimsel yöntemlerle elde edildiğinin

[298] Halid Özkan, "Ceza Muhakemesinde Ekran Görüntüsü Çıktılarının Delil Niteliği", Yener Ünver (Ed.), **Ceza Muhakemesi Hukukunda Delil ve İspat** içinde (265-287), Ankara: Seçkin Yayıncılık, 2014, s. 268.

[299] Özkan, s. 269.

[300] Bıçak, s. 429.

[301] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 117.

[302] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 121.

tespit edilmesi durumunda ise bu elektronik delilin hukuka uygun biçimde elde edilip edilmediği hususu da ayrıca değerlendirilecektir.

Ceza yargılaması bakımından delillerin en önemli özelliği olan "hukuka uygun elde edilmiş olma" hususu elektronik delil bakımından da büyük öneme sahiptir[303]. Nitekim elektronik delilin hassas yapısı, yığın halinde bulunabilme özelliği, sosyal hayatın elektronikleşmesi sonucunda ceza yargılamasında elektronik delile başvurma lüzumu hissedilmesine binaen hukuk kurallarına uyulmaksızın elde edilecek deliller özel hayatın gizliliği, kişisel verilerin ifşası gibi bazı hak ihlallerine yol açacaktır[304].

Bu bakımdan, hukuk düzenince belirlenen koşullara uyulmaksızın veya söz konusu koşulların sınırlarının aşılarak hareket edilmesi durumunda elde edilen elektronik delilin hukuka aykırılığı gündeme gelecektir[305]. Bu durumda ise elektronik delilin hukuken geçerliliğinden söz edilemeyecektir.

1.7.3.2. Teknolojik Geçerliliğin Denetlenmesi

Elektronik delilin geçerliliği bakımından hukuken denetlenmesi kadar teknolojik bakımdan da denetlenmesi gerekmektedir. Elektronik delilin teknolojik geçerliliğinin denetlenmesinde ise bütünlük, doğrulanma, inkâr edilememe, doğruluk ve daha sonra ele alınabilirlik ilkelerine uygunluğunun denetlenmesiyle sağlanmaktadır.

1.7.3.2.1. Elektronik Delilin Bütünlüğü İlkesi

Elektronik delil bakımından karşılaşılan en büyük sorunlardan birisi onun elde edilmesi ve yargılama sonuna kadar muhafazası sürecinde bütünlüğünün korunması hususudur. Bu durum aynı zamanda elektronik delille fiziksel deliller arasındaki en temel farklardan birini teşkil etmektedir.

Cumhuriyet savcısı, elektronik medyadan elde edilen verilerin ilk alındığı haliyle temsil edildiğini, elektronik medyanın tamamen kolluk güçleri ya da kısmen veya tamamen

[303] Akarslan, s. 133.

[304] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 389.

[305] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 389.

tanık veya sanık tarafından elde edildiği hususlarına bakmaksızın, mahkeme önünde doğru ve kesin olarak ortaya koymak zorundadır[306].

Elektronik delilin bütünlüğü ilkesi, elektronik delile ilk ulaşıldığı andan itibaren hem fiziken hem de elektronik bakımdan koruma altına alınmak suretiyle delilin değişmediğinin tespit edilmesini ifade etmektedir[307]. Elektronik delilin yapısı gereği kasten ya da yanlışlıkla silinmesi, değiştirilmesi veya bozulması kolay ve mümkündür. Bu durum elektronik delilin bütünlüğünü sağlamayı oldukça zorlaştırmaktadır. Bu nedenle elektronik delilin bütünlüğüne herhangi bir zarar gelmemesi son derece önemlidir[308].

Elektronik delilin bütünlüğünün sağlanması işlemi genellikle kriptografi* teknikleri kullanılmak suretiyle gerçekleştirilmektedir. Bununla birlikte elektronik delilin fiziksel olarak da korunması gerekir. Fiziksel koruma ise delillerin incelenecek yere bozulmadan taşınması, yargılama başlayıncaya kadar uygun ortamlarda saklanması ve yine mahkemeye getirilişi sırasında herhangi bir bozulmaya uğramamasını ihtiva etmektedir[309].

1.7.3.2.2. Elektronik Delilin Doğrulanması İlkesi

Elektronik delil kullanımının yaygınlaşmasıyla birlikte ceza soruşturması yeni bir boyut kazanmıştır. Kolluk güçleri, daha önceden kullanılmayan birçok soruşturma yöntemini kullanma yolunu benimsemişlerdir. Bu kapsamda elektronik deliller, olay faillerinin arkalarında bıraktıkları dijital izler olarak takip edilmiş ve birçok soruşturma sonuçlandırılabilmiştir. Bununla birlikte, kovuşturma aşamasında ceza hâkimi

[306] John. D. Nilsson (Ed.), **Digital Evidence in the Courtroom,** New York: Nova Science Publishers, Inc., 2010, s. 21.

[307] Gözüşirin, s. 91.

[308] Mustafa İlker Öztürk, s. 39.

* Kriptografi, kriptoloji (şifre bilimi)'nin bir dalı olup, şifreleme yöntemi kullanılmak suretiyle bilgi güvenliğini koruma bilimi ve sanatını ifade etmektedir. Cryptography Defined/Brief History, http://www.laits.utexas.edu/~anorman/BUS.FOR/course.mat/SSim/history.html (18 Ocak 2015).

[309] Gözüşirin, s. 92.

tarafından elektronik delille ilgili göz önünde bulundurulması gereken temel ilke, elektronik delilin doğası gereği yeterince kişiselleştirilememiş olmasıdır[310].

Elektronik delilin elde edilmesinden sonra adli soruşturma sürecinde gerçekten iddia olunan suçla veya şüpheliyle alakalı olup olmadığının ispatı gerekmektedir. Zira soruşturma sürecinde elde edilen elektronik verilerin aynısının herhangi bir kişi tarafından oluşturulması mümkündür. Hatta bu elektronik verilerin sonradan kolluk tarafından üretildiği de iddia olunabilir. Bu bakımdan soruşturma sürecinde elektronik verilerin olay ve şüpheli ile ilişkisi teyit edilmelidir[311].

Elektronik delilin bulunduğu suç tiplerinde karşılaşılan en sorunlu konulardan birisi, bir olayda elde edilen elektronik delilin mahkeme esnasında kabul edilebilirliği hususudur. Gerçekten de, elektronik delilin gerçek delil özelliği gösterebilmesi için ilk toplandığı andan itibaren hiçbir biçimde değiştirilmediğinin, kim veya kimler tarafından nerede ve ne zaman toplandığının doğrulanması gerekmektedir. Bugüne kadar bahse konu mesele alıcı ve gönderici arasında iletilen veriler üzerinde belirli matematiksel işlemler gerçekleştirilmek suretiyle güvenlik için çeşitli mekanizmaları sağlayan kriptografi bilimi altında incelenmiş olmasına karşın mevcut çözümler içerisinde elektronik delile kesinlik kazandıracak entegre bir mekanizma bulunamamıştır[312].

Elektronik delilin yargılama sırasında kabul edilebilirliğini sağlamak için yalnızca doğrulamada kullanılacak teknik yöntemler yeterli değildir. Delillerin inceleme ve analiz işlemlerine tabi tutulduğu laboratuvar standartlarının bu işlemleri yerine getirmek için uygun olup olmadığı, kullanılan araç, gereç ve yöntemlerin yerindeliği gibi başka birçok konunun da değerlendirilmeye alınması gerekmektedir. Bu bakımdan adli bilişim süreci için gerekli uluslararası standartların belirlenerek, bu standartların uygulamaya konulması çok büyük öneme sahiptir[313].

---

[310] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 404.

[311] Mustafa İlker Öztürk, s. 39.

[312] Yusuf Uzunay ve Mustafa Koçak, "Bilişim Suçları Kapsamında Dijital Deliller", **AB'05 Akademik Bilişim Konferansı**, Gaziantep, 31 Ocak - 4 Şubat 2005, http://ab.org.tr/ab05/tammetin/134.pdf (30 Ekim 2014).

[313] Uzunay ve Bıçakçı, http://www.emo.org.tr /ekler/ 4843973f9b66701ek. pdf. (31 Ekim 2014).

1.7.3.2.3. Elektronik Delilin İnkâr Edilememesi İlkesi

Elektronik delillendirme işlemindeki elektronik delilin sahibi, bu delili elde eden kolluk birimi, delilin alındığı elektronik medya, delilin içeriği gibi bütün unsurların daha sonradan inkâr edilememesi gerekmektedir[314]. Bu bakımdan, elektronik delilin elde edilmesi sırasında kullanılan bilgi ve tekniklerin doğruluğunun gerektiğinde adli sürecin tüm aşamalarında ispatı gereklidir[315].

CMK m. 169/2 her soruşturma işleminin tutanağa bağlanmasını, tutanağın adli kolluk görevlisi, Cumhuriyet savcısı veya sulh ceza hâkimi ile hazır bulunan zabıt kâtibi tarafından imzalanmasını, CMK m. 134/3 ise bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında sistemdeki bütün verilerin yedeklemesinin yapılmasını hükme bağlamıştır. Bu bakımdan, adli bilişim sürecinde elde edilen elektronik verilerin tutanağa bağlanarak imza altına alınması elektronik delilin inkâr edilememesi açısından büyük önemi haizdir.

1.7.3.2.4. Elektronik Delilin Doğruluğu İlkesi

Delillerin elde edilme sürecinde, elektronik delilin kişisel veya kurumsal sahibi, onu elde eden kolluk birimi, delilin elde edildiği elektronik ortam, elektronik delilin elde edildiği zaman, elektronik delilin içeriği gibi bütün unsurların doğruluğunun daha sonradan inkâr edilemeyecek şekilde belgelenmesi gerekmektedir.

Gerçekten de elektronik delil ister insan müdahalesi ile oluşturulan bir delil niteliğinde olsun, isterse sistem tarafından otomatik olarak oluşturulan bir delil olsun, doğruluğunun mutlaka kontrol edilmesi gerekmektedir. Bu bakımdan, bilişim sistemlerinin girdi, süreç ve sonuç şeklinde çalışan sistemler olduğu göz önünde bulundurulmamalı ve elektronik delil bakımından girdi, delillerin işlem görmesi durumunda işlemlerin doğruluğu ve çıktının girdi, işlem süreçleri ile uygunluğu kontrol edilmelidir[316].

---

[314] Uzunay ve Bıçakçı, http://www.emo.org.tr /ekler/ 4843973f9b66701ek. pdf. (31 Ekim 2014).

[315] Mustafa İlker Öztürk, s. 39-40.

[316] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 139.

Özellikle, belli bir verinin kayıt öncesindeki kayda hazırlık usulleri, programdaki yapısal hatalar, veri girişim ayrıntıları, bilişim sistemine verilen komutlarda yapılan hatalar, kaydedilerek saklanan verideki hasar ve bozukluklar, bilişim sisteminin çalıştığı sırada elektrik kesintisinin olup olmadığı, bilişim sisteminin hata verip vermediği, veri içerisinde kelime araması veya belli bölümlerin kesilmesi, verinin başka bir karaktere çevrilmesi gibi işlemler yapılırken sıradan, kişiye özgü hatalar yapılıp yapılmadığı, kullanılan bilişim sisteminin standart tipte olup olmadığı, bilişim sisteminin hassas çalıştığına güvenilip güvenilemeyeceği gibi teknik hususların da bilirkişi tarafından incelenerek hazırlanan verinin belli bir kişinin ürünü olup olmadığının teknik yönden bilirkişi marifetiyle belirlenmesi gerekir[317].

1.7.3.2.5. Elektronik Delilin Daha Sonradan Ele Alınabilirliği İlkesi

Bilimsel bir yöntemin en önemli özelliği yapılan herhangi bir deney veya gözlemin doğruluğunu kanıtlamak için tekrar edilebilir niteliğe sahip olmasıdır. Bu bakımdan elektronik delilin elde edilmesi sürecinde bir uzman tarafından yapılan inceleme ve bulgular başka bir uzman tarafından daha sonra tekrar ele alınabilir olmalıdır[318]. Nitekim bu durum elektronik delilin sonradan ele alınabilirliği ilkesinin bir gereğidir.

Bu bağlamda elektronik delilin sonradan ele alınabilirliği ilkesi, elde edilen ve mahkemeye delil olarak sunulan tüm bulgulara farklı kişiler tarafından, farklı yer ve zamanlarda da aynı yöntem ve metotlar kullanılarak ulaşılabilmesini ifade etmektedir. Sonuçların tekrar elde edilebilir olması, elektronik delile olan güvenilirliğin en önemli göstergesidir. Genel kabul gören tekniklerin ön plana çıkmasındaki en önemli etken, farklı kişiler tarafından uygulanan bu tür yazılımların her defasında aynı sonucu vermeleridir[319].

Bu bakımdan elektronik delil incelemesinde elde edilen verilerin doğruluğunu kanıtlamak için delilin elde edilme ve inceleme süreci yeterince detaylandırılarak kayıt altına alınmalıdır. Başka bir uzman aynı yol ve yöntemler neticesinde aynı sonuca

[317] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1104.

[318] Adli Bilişim Prensipleri Nelerdir ?. 2014, http://www.teknospaper.com/2014/04/adli-bilisim-prensipleri/ (25 Ekim 2014).

[319] Henkoğlu, s. 2, 7; Özkan, s. 268.

varıyorsa delilden elde edilen sonuçların ve uygulanan yöntemin geçerliliği ispat edilmiş olacaktır[320].

1.7.4. Elektronik Delilin Ceza Yargılamasında Kabul Edilirliği

1.7.4.1. Genel Olarak

Bilişim sistemlerinde bulunan elektronik deliller ceza yargılaması sürecinde üç şekilde ortaya çıkmaktadır. Öncelikle bilişim sistemleri vasıtasıyla işlenen bir suçta, olay yeri olarak bilişim sistemi, suça, faile, mağdura ve olayın niteliğine ilişkin elektronik delil barındırabilmektedir. İkinci olarak, bilişim sistemi, suçun hedefi olabilmektedir. Bu durumda, faile veya fiile ilişkin delil veya emareler bilişim sisteminden elde edilebilecektir. Üçüncü olarak ise, bilişim sistemi, suçta araç veya hedef olmamasına rağmen, herhangi bir suça ilişkin delillerin depolandığı yer olarak kullanılabilmektedir.

Ceza yargılamasında birçok davanın elektronik delille ilgili olduğu ve bu delil türünün söz konusu yargılama bakımından büyük öneme sahip olduğu hususlarında genel bir uzlaşı bulunmasına karşın elektronik delilin mahkemede delil olarak kullanılıp kullanılmayacağı hususu halen tartışmalı bir konudur. Bu durum, genellikle bireysel olarak hâkimin sahip olduğu tecrübe, inanç ve anlayışa göre farklılık arz edebilmektedir [321] . Elektronik delilin güvenilirliği ile ilgili olarak bazı hâkimler, elektronik delilin hassas ve nesnel yapısı nedeniyle onun fiziksel delile göre daha güvenilir olduğuna inanmaktadırlar. Buna karşın bazı hâkimler ise elektronik delilin orijinalliğini doğrulamak için araçların yetersiz olmasının bu delilin güvenilirliğini zayıflattığını bu nedenle de bu delil türünün fiziksel delile göre daha az güvenilir olduğuna inanmaktadırlar[322].

Elektronik delil, ceza yargılamasını yürüten hâkimde suçun işlendiğine ilişkin aksine ihtimal vermeyecek şekilde tam bir kanaat oluşturmalıdır. Ayrıca suçun o fail tarafından

---

[320] Adli Bilişim Prensipleri Nelerdir ?. http://www.teknospaper.com/2014/04/adli-bilisim-prensipleri/ (25 Ekim 2014).

[321] Gary Craig Kessler, "Judges' Awareness, Understanding, and Application of Digital Evidence**", PhD Thesis**, Nova Southeastern University, 2010, s. 31.

[322] Fredesvinda Insa, "The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime-Results of a European Study**", Journal of Digital Forensic Practice**, Vol. 1, No. 4, 2006, s. 286.

işlenip işlenmediğine ilişkin delillerin aksine şüphe bırakmayacak şekilde gösterilmesi gerekir. Aksi halde "şüpheden sanık yararlanır" ilkesi gereğince sanığın beraatına hükmedilmesi gerekecektir[323]. Nitekim Yargıtay birçok kararında sanığın atılı suç nedeniyle cezalandırılması için her türlü şüpheden uzak, kesin ve inandırıcı delil elde edilememiş olmasını beraat nedeni olarak kabul etmektedir[324].

1.7.4.2. Mukayeseli Hukukta Durum

Mukayeseli hukukta elektronik delil ile fiziksel deliller arasındaki ilişki açısından, elektronik delili fiziksel delile eşdeğer sayma yönünde bir eğilim bulunmaktadır. Bu eşdeğer durum özellikle üç alanda özellik göstermektedir. Öncelikle ve en yaygın eşdeğerlik, elektronik belgenin, kâğıt bazlı belgeye eşdeğer sayılması bakımındandır. İkinci olarak, elektronik delil olarak kabul edilen elektronik imzanın, el ile atılan imzaya eşdeğerliği hususudur. Üçüncü olarak ise elektronik postanın, klasik posta usullerine eşdeğer sayılması durumudur[325].

Amerikan hukuk sisteminde ceza yargılamasında elektronik delilin kabul edilebilirliğine ilişkin özel delil kuralları bulunmamaktadır. Federal mahkemelerde yürütülen davalar bakımından uygulanan Federal Delil Kuralları (Federal Rules of Evidence) elektronik delil de dâhil her türlü delil için geçerlidir. Bununla birlikte geleneksel kuralların yeni bir kanıt türü olan elektronik delil bakımından uygulanması her zaman kolay olmamakta ve kimi zaman mahkemeler elektronik delilin değerlendirilmesinde temkinli davranmaktadırlar. Bu bakımdan uygulamada Federal Delil Kurallarından özellikle elektronik deliller hakkında güvenilir olma, tanık beyanı dinlenmesi ve en geçerli delil olma kuralları üzerinde hassasiyetle durulduğu görülmektedir[326].

---

[323] Orta, s. 290.

[324] *"Sanığın üzerine atılı müsnet suçu işlediğine dair müşteki ve tanık M.. Y...'nın görgüye dayanmayan soyut beyanları haricinde her türlü şüpheden uzak kesin ve inandırıcı delil elde edilemediği gibi şüpheden sanık yararlanır ilkesi gereğince beraatına karar verilmesi gerekirken yazılı şekilde mahkûmiyetine karar verilmesi bozmayı gerektirmiş..."* Yargıtay 13. CD. 23.11.2013. E. 2011/21334, K. 2011/6227 (UYAP).

[325] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 129.

[326] Linda L. Listrom ve Diğerleri, "The Next Frontier: Admissibility of Electronic Evidence", ABA Annual Meeting, Summer 2007, http://www.mccarthyfingar.com/files/20110129123145-A%20B%20A%20(00276545).PDF (19 Ocak 2015), s. 1-2.

Avrupa ülkeleri mevzuatında elektronik delil, etkinliği, kullanılırlığı ve meşruiyeti bakımından ülkeden ülkeye farklı bir role sahiptir. Delil elde edilmesinde şeffaflık ve ifade özgürlüğüne saygı, Avrupa standartlarını yansıtan ilkeler olmakla birlikte bu ilkelerin delilin kabul edilebilirliği söz konusu olduğu durumlarda ikincil bir konuma sahip olduğu görülmektedir. Elektronik delilleri etkileyen bu ilkeler de verilerin korunması standartları, haberleşmenin gizliliği ve ifade özgürlüğü hakkına saygı temelinde kendini göstermektedir[327].

Uygulama bakımından da Avrupa öğretisi, elektronik delilin etkinliği, kullanılırlığı ve meşruiyetinin daha büyük öneme sahip olduğunu belirtmektedir. Teknik uzmanlarda -elektronik delilin elde edilmesi sürecinde- bireysel haklara saygı prensibine uygun davrandıklarını vurgulamaktadırlar. Örneğin, Almanya ve Yunanistan ülkelerinin adli bilişim uzmanları verilerin korunması standartlarından söz ederlerken Fransa, Lüksemburg ve İrlanda ülkelerinin adli bilişim uzmanları gizliliğin korunmasına vurgu yapmaktadırlar. İtalya ve Birleşik Krallık uzmanları ise söz konusu temel ilkelerin işlevlerini geliştirmek için şifreli malzemeleri tercih etmektedirler[328].

Elektronik delilin ceza yargılamasında kabul edilebilirliğine ilişkin olarak yargı içtihatlarının da belirleyici bir role sahip olduğu görülmektedir. Bu bağlamda; Alman hukukunda elektronik delilin ceza yargılamasında delil olarak kullanılıp kullanılmadığı hususuna bakıldığında; burada delil serbestîsi ilkesi geçerli olup mahkemeye her türlü delil sunulabilmektedir. Buna göre elektronik delilin de yaygın bir delil türü olarak kabul edildiği görülmektedir. Nitekim elektronik delilin, daha gerçekçi yapısı nedeniyle hâkimi yargılama sürecinde daha kolay ikna etme özelliğine sahip olduğu değerlendirilmektedir[329].

İngiltere'de bilişim sistemlerinden elde edilen elektronik delil ceza yargılama sisteminde yaygın olarak kabul edilmekte ve birçok davada da kullanılmaktadır. Bu ülkedeki genel kanaate göre, elektronik delil, diğer kanıtlarla aynı kurallara göre değerlendirilmesi

[327] Insa, s. 287-288.

[328] Insa, s. 288.

[329] Rand Europe & Lawfort, "Update to the Handbook of Legal Procedures of Computer and Network Misuse In Eu Countires For Assiting CSIRT, D: 15 Final Report", 2005, ftp://ftp.cordis.europa.eu/pub/ist/docs/directorate_d/trust-security/ec-csirt-d15.pdf, (01 Ocak 2015), s. 115.

gerekmektedir [330] . Bununla birlikte İngiltere'de elektronik delilin özgünlüğünü ispatlamak ve elektronik delilin elde edildiği anda bilişim sisteminin uygun çalıştığının ispatını sağlamak için bilişim sistemini işleten teknik personelin mahkemede tanık olarak dinlenildiği görülmektedir[331].

Birçok Avrupa ülkesi hukuk sistemlerinde olduğu gibi Fransız hukuk sistemi de delil serbestîsi ilkesini benimsemiştir. Bununla birlikte ceza yargılamasında delil serbestîsinin bazı istisnaları bulunmaktadır. İlk olarak delillerin toplanması sırasında temel hak ve özgürlüklerin orantısız biçimde ihlal edilmemesi gerekir. İkinci olarak, deliller yasal yollarla elde edilmelidir. Üçüncü olarak ise delillerin toplanması sürecinde hukukun genel prensiplerinin ihlal edilmemesi gerekmektedir [332] . Bu bakımdan, yukarıdaki istisnalara uyulmak kaydıyla suçlar elektronik delil de dâhil olmak üzere her türlü ispat aracıyla kanıtlanabilir ve hâkim delil değeri konusunda kendi vicdani kanaatine göre karar vermede özgürdür[333].

1.7.4.3. Türk Hukukundaki Durum

Türk Hukukunda elektronik delilin ceza yargılamasında bir delil türü olarak kabul edilip edilmeyeceği, kabul edildiği takdirde ise elektronik delilin tek başına mahkûmiyet kararı vermek için yeterli olup olamayacağı hususu öğretide tartışma konusu olmuş ve bu hususta farklı görüşler ileri sürülmüştür.

Elektronik delilin ceza yargılamasındaki rolüne mesafeli olan bir görüşe göre; soruşturma sırasında delil olarak elde edilen elektronik verilerin bilgisayar ortamında tutulmalarından dolayı silinebilir, değiştirilebilir veya yenilenebilir nitelikte olmaları nedeniyle hukuki anlamda çok da sağlam delil kategorisinde değerlendirilmemeleri gerekmektedir[334].

---

[330] Rand Europe & Lawfort, s. 268.

[331] Tanrıkulu, s. 199.

[332] Olivier Leroux, "Legal Admissibility of Electronic Evidence", **International Review of Law, Computers & Technology**, Vol. 18, No. 2, (July 2004), s. 208.

[333] Rand Europe & Lawfort, s. 108.

[334] İsmail Ergün, **Siber Suçların Cezalandırılması ve Türkiye'de Durum**, Ankara: Adalet Yayınevi, 2008, s. 44.

Buna karşın elektronik ortamda bulunan verilerin ortadan kaldırılması kolay gibi gözükse de bilginin kolay bir şekilde kaybolmadığı, hemen hemen her bilginin yedeğinin bulunduğu, bir bilgisayar diskindeki bilgilerin silmeyle, formatlamayla kaybolmadığı, hatta deprem gibi doğal afetlerden sonra bile adli bilişim uzmanları tarafından yapılan çalışmalar sonucunda verilere tekrar ulaşılabildiği bilinen bir gerçektir. Bu bakımdan elektronik verilerin delil niteliği taşıması için sağlam ve değiştirilemez bir yapıya sahip olması şart değildir[335].

Gerçekten de elektronik delilin tahrife açık niteliğe sahip olması delil olarak kabul edilmelerinin önüne geçmemelidir. Bu bakımdan elektronik delilin tahrif edildiği ispatlanmadığı sürece ceza yargılamasına konu olan bir olayda bir iddiayı ispatlayabileceği veya çürütebileceği kabul edilmelidir[336]. Bununla birlikte elektronik delilin sağlamlığının ortaya konulması bilirkişi incelemesini gerekli kılmaktadır[337].

Bu bakımdan öğretide büyük ölçüde uzlaşma sağlanan hususa göre ceza yargılamasında delil serbestîsi ilkesinin bir gereği olarak her türlü şeyin delil olabileceğinin kabulü karşısında, elektronik ortamda elde edilen ve ceza yargılamasında maddi gerçeği aydınlatmaya yarayan elektronik verilerin delil olma niteliğinde herhangi bir sorun görünmemektedir[338]. Nitekim Avrupa Birliği çalışma raporlarına göre de; bilişim sistemlerindeki elektronik veriler önemli delil niteliğini haiz olabilmekte ve bu deliller aracılığıyla işlenen suç açığa kavuşturulabilmektedir[339]. Bu bakımdan tartışılması gereken konu bu verilerin tek başına mahkûmiyete yetecek kuvvette olup olmadığı hususudur[340].

Elektronik delilin ceza yargılamasında tek başına mahkûmiyete yetecek kuvvette olmadığı yönünde görüşe sahip olan Özbek'e göre; elektronik verilerin içeriğinin

---

[335] Orta, s. 290-291.

[336] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 135.

[337] Kunter, Yenisey ve Nuhoğlu, Açıklamalı Ceza Muhakemesi Kanunu, Cilt. 1, s. 1323.

[338] Orta, s. 289.

[339] Leyla Keser Berber, "Adli Bilişimle İlgili Olarak AB ve ABD'deki Yasal Düzenlemeler ve Kişisel Verilerin Korunması" **Bilişim Hukuku Konferansı-YARGITAY**, Ankara, 09-10 Ekim 2008, s. 29.

[340] Orta, s. 289.

değiştirilebilir nitelikte olması, bu verilerin tek başlarına delil olma gücünü zayıflatmakta ve hatta ortadan kaldırmaktadır. Bilgisayar belleğinde veya veri depolama aygıtlarında saklanan bilgilerin yazılı metinler haline dönüştürülmesi de bir irade açıklamasının tam olarak ortaya konulup ispatlanmasını ifade etmemektedir. Zira bu şekildeki bir irade açıklaması, orijinal şekilde belgelenmemekte, sadece bilgilerin sunulması anlamını taşımaktadır. Bu durumda, bu şekilde elde edilen verilerin tek başına mahkûmiyet kararı verilmesi için yeterli olmayıp başka delillerle ispatlanması gerekmektedir. Bu bağlamda elektronik veriler, tanık beyanı gibi doğrudan doğruya değil, bir belirti türü olarak dolaylı ispatın konusunu teşkil etmektedir[341].

Özbek'e göre, elektronik verilerin delil olarak kullanılabilmesi özel hayatın gizliliği ilkesi bakımından da değerlendirmeye tabi tutulmalıdır. Zira özel hayatın gizli alanı gerek ceza yargılaması gerekse insan haysiyetinin dokunulmazlığı ilkesinin koruması altında bulunduğu için hiçbir şekilde müdahaleye imkân tanımaz. Bu bakımdan, hayatın gizli alanına ilişkin olan, örneğin bireyin cinsel hayatını konu alan verilerin delil olarak değerlendirilebilmesi mümkün değildir. Buna karşın, elde edilen veriler, cinsel saldırı gibi cinsel dokunulmazlığa karşı işlenmiş olan suçların aydınlatılması bakımından önem arz etmesi durumunda oranlılık ilkesi çerçevesinde sınırlı olarak kullanılabilmelidir[342].

Kızılyar'a göre fiziksel delillerden farklı olarak elektronik delilin tespiti, elde edilmesi ve delil olarak mahkeme huzuruna getirilmesi birçok prosedürü gerektirmekte ve teknik zorlukları barındırmaktadır. Bu durum elektronik verilerin delil olarak kullanılmasında bazı sorunları da beraberinde getirmektedir. Başta delilin kaynağının doğrulanması olmak üzere tahrifata uğrayıp uğramadığı, usulüne uygun elde edilip edilmediği, delil değerinin bulunup bulunmadığı, kişilere yönelik isnadı doğru biçimde ispatlayıp ispatlayamadığı gibi hususlar uygulamada tartışma konusu olmaktadır. Bu bakımdan elektronik verilerin delil olarak kullanılması, çoğu zaman ek delillerle desteklenmesini veya başka araştırmalar yapılmasını gerekli kılmaktadır[343].

---

[341] Veli Özer Özbek, Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi, s. 185-186.

[342] Veli Özer Özbek, Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi, s. 189.

[343] Kızılyar, s. 79.

Orta'ya göre de elektronik verilerin kolaylıkla değiştirilebiliyor olmaları onların delil niteliğini ortadan kaldırmamakla birlikte şüpheye yol açmayacak şekilde başka delillerle de desteklenmesini gerekli kılmaktadır[344].

Elektronik delilin kolay değiştirilebilir olma özelliği, uzman kişilerce bu değişikliklerin tespit edilebilir olmasına rağmen, elektronik delilin ceza yargılamasında doğrudan delil olarak kullanılmalarına yönelik ciddi eleştirileri beraberinde getirmektedir. Elektronik delil, kesin ve delil bütünlüğü teknik yöntemlerle sağlanabilir nitelikte ise de, teknik standartlara ve kurallara uyulmadan elde edilen elektronik deliller bakımından söz konusu eleştiriler yerindedir. Özellikle bilişim bağlantılı suçlarda çok daha önemli olan adli bilişim süreci iyi eğitim almış deneyimli teknik uzmanlar tarafından yürütülmelidir. Zira bilişim bağlantılı suçlarda elektronik deliller "doğrudan delil" niteliğinde oldukları için bu delillerin bozulması yargılama sürecinin ciddi şekilde sekteye uğramasına neden olabilir[345].

Değirmenciye göre, elektronik delilin diğer delillerle desteklenmesi ihtiyacı, elektronik delilin niteliğine göre belirlenmesi gereken bir meseledir. Elektronik delil, insan tarafından oluşturulan ve bilişim sisteminde muhafaza edilen bir delil niteliğinde ise doğruluğu diğer delillerle desteklenerek sağlanmalıdır. Elektronik delil, bilişim sistemi tarafından insan müdahalesi olmaksızın oluşturulan bir delil ise sistemin uygun şekilde işleyip işlemediği göz önüne alınması gerekir. Bu durumda bilişim sisteminde yer alan verinin, fail ile bağının kurulması ve değiştirilmemiş olması önemlidir[346].

Öğretide elektronik delilin ceza yargılamasında başkaca delillerle desteklenmeksizin mahkûmiyete esas olabileceği de ileri sürülmüştür. Bu bağlamda; elektronik delilin tek başına yeterli bir delil olabilmesini adli bilişim sürecine uygun elde edilmesi kaydına bağlayan Ünal'a göre elektronik verilerin değiştirilebilir olmalarına karşın teknolojinin geldiği nokta dikkate alındığında bu verilerin değiştirilip değiştirilmediği hususu tespit edilebilmektedir. Adli bilişim sürecinin uygulanması veya bu süreç uygulanmadığında da elde edilen verilerin bütünlüğü ve güvenliği teknik bir inceleme sonucunda ispat

[344] Orta, s. 290.

[345] Akarslan, s. 133-134.

[346] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 392.

edilebildiği durumlarda elektronik verilerin delil olarak kullanılabilir olduğu aşikârdır. Bununla birlikte, teknik inceleme yapılırken elektronik veriler üzerinde yapılan işlemlerin ayrıntılı bir şekilde kaydedilmesi gerekmektedir[347].

Gerçekten de, elektronik delilin orijinal hali ile muhafazası ve yapılan tüm teknik işlemlerin ayrıntılı olarak raporlanması ve kişisel yorumlar yerine teknik bilgi temelli değerlendirmelerin yapılması hukuki açıdan geçerli bir delil sayılmasında etkili olacaktır [348] . Bu bakımdan elektronik verilerin ceza yargılamasında delil olarak kullanılabilmesi, üzerinde çok kolay oynama yapılabilen ve fakat bu tür oynamaların da teknik olarak belirlenmesi mümkün olan verilerin sağlamlığı CMK m. 66 uyarınca bilirkişi tarafından inceleme yapılarak kontrol edildikten ve gerektiğinde belgenin hazırlanması süreci ile ilgili tanık beyanı alındıktan sonra hiçbir şekilde değişikliğe uğramadan mahkeme huzuruna getirilmesine bağlıdır[349].

Buna karşın adli bilişim süreci tamamlanmaksızın veya teknik inceleme yapılmaksızın soruşturma veya kovuşturmada ortaya konan elektronik veriler sadece belirti hükmünde kalacaklardır. Bu bakımdan, bu nitelikteki elektronik veriler kullanılarak mahkûmiyet hükmü verildiği hallerde başka delillerle de desteklenmeleri gerekmektedir. Elektronik verilerin elde edilmesi aşamasında hukuka aykırılık durumunun varlığı veya elektronik verilerin bütünlüğünün bozulması hallerinde ise bu verilerin belirti delili olarak da kullanılmaları da mümkün değildir[350].

Ceza yargılaması bakımından delillerin en önemli özelliği olan "hukuka uygun elde edilmiş olma" hususu elektronik delil ve aşağıda ayrıntısıyla inceleyeceğimiz adli bilişim süreci açısından büyük önem arz etmektedir. Zira elektronik delilin elde edilmesi sürecinde hukuka uygun davranmanın yanı sıra bu süreçteki teknik hususlara

---

[347] Osman Gazi Ünal, "Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma" (**Yayınlanmamış Yüksek Lisans Tezi,** Gazi Üniversitesi SBE, 2011), s. 20.

[348] Mustafa İlker Öztürk, s. 40.

[349] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1109.

[350] Ünal, s. 20.

da riayet etmek gerekmektedir. Nitekim elektronik delilin bozulmaya müsait yapısı adli bilişim sürecinde bu tekniklere uymayı zorunlu kılmaktadır[351].

Bununla birlikte, ceza hâkimi tarafından yargılamayı sona erdiren hükme esas teşkil edebilmesi için elektronik delilin yalnızca hukuka uygun yöntemlerle elde edilmiş olması yeterli değildir. Bunun yanı sıra söz konusu delilin tarafların bilgisine sunulması, duruşmaya getirilip tartışılması gerekmektedir. Nitekim CMK m. 217 uyarınca hâkim, ancak duruşmaya getirilen ve huzurunda tartışılan delillere dayanarak karar verebilir[352].

Belirtmek gerekir ki; esasen elektronik delille ilgili tartışmanın tek başına bu delil türünün mahkûmiyet için yeterli olup olmadığı noktasında değil, dava dosyasında bulunan bir elektronik delilin suçun işlendiği konusunda hâkimde vicdani kanaati oluşturup oluşturmadığı noktasında toplanması gerekmektedir. Bu bakımdan, bir delilde bulunması gereken, hukuka uygun yöntemlerle elde edilmiş, gerçek, değiştirilmemiş, dava konusu olayla ilgili ve temsil kabiliyeti olma özelliğine sahip her veri, elektronik delil olarak hükme esas teşkil edebilecektir[353].

Kanaatimiz;

Yukarıdaki değerlendirmeler ışığında belirtmek gerekir ki; elektronik delilin tek başına delil olarak kullanılabilip kullanılamayacağı hususundaki tartışmanın genelde delilin sahihliği ve tahrif edilebilirliği noktasında toplandığı görülmektedir. Bununla birlikte, bu husus diğer deliller bakımından da geçerli olup sahih olmayan veya tahrif edilmiş durumda bulunan diğer deliller de ceza yargılamasında delil olarak kullanılamazlar. Bu bakımdan bilişim sistemlerinden elde edilen elektronik delilin her şart altında güvenilir olmadıkları iddia edilemez. Bu anlamda elektronik delilin en az fiziksel deliller kadar güvenilir olduğunu düşünmekteyiz.

Nitekim Yargıtay da bir kararında; *"Dijital delilin yapısı gereği manipülasyona açık olduğu bilinmektedir. Diğer delil türlerine göre özellik arz eden bazı yönleri olmakla birlikte dijital delil de sonuçta, deliller hiyerarşisinin kabul edilmediği, delil*

[351] Akarslan, s. 133.

[352] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 390.

[353] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 396.

serbestîsinin benimsendiği ceza muhakemesi sistemimizde bir ispat aracıdır. İspat aracı olan delilin değerlendirilmesinde, Ceza Muhakemesi Hukuku'nda bir delil için öngörülen nitelikleri taşıyıp taşımadığı nazara alınıp, genel olarak; somut olayın özellikleri, yüklenen suçun işleniş biçimi, dosyadaki diğer deliller gibi hususlar gözetilip, özel olarak da; delilin temsil ettiği olayın niteliği, ele geçiriliş yeri, şekli ve zamanı, bu delilin sair karakteristik özellikleri gibi hususlar göz önünde bulundurulmalıdır[354]*."* hükmüne yer vermiştir.

Elektronik delilin ceza yargılamasında tek başına mahkûmiyete yetecek kuvvette olup olmayacağı hususunda ise; esasen elektronik delilin başkaca delil olmadan mahkûmiyet hükmü için yeterli kuvvette olmadığı ve bu nedenle başka delillerle desteklenmesi gerektiğine ilişkin yasal bir zorunluluk bulunmamaktadır. Özellikle bilişim suçlarında fiziksel delillere müracaat etme olanağının bulunmadığı hallerde böyle bir zorunluluk getirme bilişim suçlarının sonuçlandırılması bakımından büyük sorunlara neden olacaktır. Bu bakımdan hukuki ve teknolojik geçerliliği konusunda tereddüt bulunmayan hallerde elektronik delilin tek başına mahkûmiyet hükmü kurmak için yeterli kuvvette bir delil türü olduğunu düşünmekteyiz.

Bununla birlikte elektronik delilin mahkûmiyet kararına esas olması için başka delillerle birlikte kullanılması gerektiğine ilişkin yasal bir zorunluluğun bulunmamasına karşın yapılarından kaynaklanan hassasiyet nedeniyle çoğu zaman savunma tarafının elektronik delilin hukuki ve teknolojik geçerliliğine yönelik itirazlarda bulunduğu, bu itirazların yargılama sürecinde sanık lehine şüpheli bir durumun oluşmasına sebebiyet verdiği, bu nedenle yargılama faaliyeti sırasında sair delillerle bu şüpheyi yenme zorunluluğunun gündeme geldiği, dolayısıyla da yasal bir zorunluluk olmasa da yapıları gereği çoğu zaman elektronik delilin kullanımının diğer delillerle birlikte gerçekleştiği de fiili bir durum olarak ortaya çıkmaktadır.

Gerçekten de kimi zaman elektronik delilin düzgün bir adli bilişim sürecinden ve bilirkişi incelemesinden geçirilerek doğruluğu konusunda herhangi bir şüphe duyulmaksızın mahkeme huzuruna getirilmesine rağmen yine de savunma tarafından elektronik delilin tahrifata uğradığı ve güvenilirliği konusunda şüphe uyandırdığı

[354] Yargıtay 9. CD. 09.10.2013, E. 2013/9110, K. 2013/12351 (UYAP).

iddiasına muhatap olduğu görülmektedir. Ancak bu hallerde elektronik delilin güvenilirliğine itiraz eden savunma tarafının elektronik delilin hangi açıdan güvenilir olmadığını ortaya koyması gerekmektedir. Bu itirazların açıkça ortaya konması halinde ise savunmanın söz konusu itirazlarının araştırılması ve ortaya konan şüphenin giderilmesi gerekir.

Nitekim Anayasa Mahkemesi, bireysel başvuru hakkına konu olan 18.06.2014 tarihli bir kararında; İstanbul 10. Ağır Ceza Mahkemesinde yürütülen yargılama ve yargılama sonunda verilen mahkûmiyet kararı ile ilgili olarak *"dijital delillerin değerlendirilmesine ilişkin şikâyetlerin giderilmediğine dair iddiaların"* kabul edilebilir olduğundan bahisle Anayasa'nın 36. maddesinde güvence altına alınan adil yargılama hakkının ihlal edildiğine, bu nedenle ihlalin ve sonuçlarının ortadan kaldırılması için yeniden yargılama yapılması gerektiğine hükmetmiştir[355].

Belirtmek gerekir ki; Anayasa Mahkemesi'nin söz konusu kararı elektronik delilin bizatihi güvenilir bir delil türü olup olmadığına veya bahse konu yargılamada kullanılan ve karara etkisi olan elektronik delillerin usule uygun elde edilmedikleri ya da değerlendirilmediklerine ilişkin değildir. Nitekim Anayasa Mahkemesi'nin bu yönde bir karar vermesi de düşünülemez. Zira bu nitelikteki bir karar onu süper bir temyiz mercii konumuna sokacaktır. Anayasa Mahkemesi'nin söz konusu kararı yalnızca elektronik delillerin değerlendirilmesine ilişkin şikâyetlerin tam olarak giderilmemesinin adil yargılama ilkesiyle bağdaşmayacağına ilişkindir.

Elektronik verinin bizzat kendisi insan duyu organlarıyla algılanabilir olmadıkları için bu verilerin kullanılması görünür hale getirilmesine bağlıdır[356]. Bu anlamda ceza yargılamasında elektronik delilin yazıcıdan çıktı alınması halinde hukuki niteliğinin ne olduğu hususuna da değinmek gerekmektedir. Nitekim uygulamada sıklıkla rastlanan hakaret ve tehdit suçlarında sosyal ağ ve video sitelerinin ekran görüntüsü yazıcı

[355] Anayasa Mahkemesi. 18.06.2014. BN. 2013/7800, http://www.kararlaryeni.anayasa.gov.tr/BireyselKarar/Content/de3fd0d1-cced-4a35-8377-750ed661dd6b?wordsOnly=False (15 Ekim 2014).

[356] Oğuz Atalay, "Elektronik Belgelerin Delil Değeri", **Bilişim Hukuku,** Mete Tevetoğlu (drl.), İstanbul: Kadir Has Üniversitesi Yayınları, 2006, s. 139.

çıktıları doğrudan delil olarak kabul edilmekte ve tek başına mahkûmiyete esas alınarak hükümler verilebilmektedir[357].

Bir elektronik verinin birden fazla çıktısının alınması halinde, bu durum orijinal metnin fotokopilerine benzetilebilir. Ancak bu çıktıları fotokopiden ayıran özellik asıl metnin kâğıda yazılı bir şekilde değil, ancak elektronik ortamda görülebilir olmasıdır. Oysa kâğıda yazılı orijinal bir metnin çoğaltılmasında elde bulunan kâğıda dayalı bir orijinal metin ve fotokopi yoluyla çoğaltılan kopyaları bulunmaktadır. Bu kopyalar ise kural olarak aslın yerine geçemezler[358].

Bu bakımdan elektronik verilerin yazıcı çıktılarının ceza yargılamasında delil niteliğini haiz olması yazıcı çıktılarının mutlak şekilde doğrulanması ve kabul edilebilirliğinin ispatlanmasına bağlıdır[359]. Bu bağlamda dijital ortamda saklanan verinin çıktısı alınan nüsha ile aynı olması durumunda, çıktısı olarak alınan elektronik veri de delil niteliğine sahip olacaktır. Bununla birlikte çıktı olarak alınan elektronik verinin gerçekliğini yitirmesi, temsil ediciliğini kaybetmesi durumunda ise delil olarak değerlendirilmesi mümkün olmayacaktır[360].

Belirtmek gerekir ki; elektronik verilerin yazıcı çıktılarının ceza yargılamasında delil olarak ileri sürülmesi durumunda orijinal veri ile yazıcı çıktılarının birbirlerinin aynısı olup olmadıklarının tespiti, başka bir ifadeyle yazıcı çıktılarının doğruluğunun ve kabul edilebilirliğinin sağlanması, bilirkişi incelemesi yaptırılması ve tespiti halinde olay tanıklarının dinlenilmesi gibi ek usul işlemlerinin yerine getirilmesini zorunlu kılmaktadır. Bu işlemler gerçekleştirilmeden yalnızca yazıcı çıktıları ile mahkûmiyet hükmü kurulmasının mümkün olmadığı kanaatindeyiz.

---

[357] Özkan, s. 282.

[358] Mine Erturgut, **Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi,** Ankara: Yetkin Yayınları, 2004, s. 40-41.

[359] Özkan, s. 282.

[360] Değirmenci, Bilgi Toplumunun Delil Türü, s. 20.

1.7.5. Elektronik Delilin Kullanıldığı Suç Tipleri

Ceza yargılamasına konu olan bir olayın aydınlatılması ve suç faillerinin tespit edilmesi, yakalanması ve cezalandırılması, soruşturma ve kovuşturma sürecinde elde edilecek delillerin ispat gücü ile doğrudan ilgili hususlardır. Bu bakımdan soruşturmaya konu bir olayın aydınlatılmasında günden güne kullanımı ve önemi artan elektronik delilin incelenmesi sırasında bu delil türünün hangi suçlarda kullanıldığına da değinmek gerekmektedir.

Elektronik delil kullanımında ilk akla gelen suç tipi şüphesiz bilişim suçlarıdır. Nitekim bilişim ve hukuk kavramları en çok bilişim suçu kavramı üzerinde kesişmektedirler. Psikolojik, sosyolojik ve ekonomik yönü itibariyle son yılların en önemli araştırma konularından birisi haline gelen bilişim suçları, soruşturma dosyaları içerisinde en sık rastlanan suç tiplerinden biri halini almıştır. Mahiyeti ve yapısı itibariyle farklılıklar arz eden bilişim suçlarının soruşturulması da, klasik suçlara nazaran ayrı bir eğitim, disiplinler arası uzmanlık alanı ve yeni yöntemlere gereksinim duymaktadır.

Bilişim suçu kavramı teknolojiyi kullanan tüm ülkelerin ortak problemi haline gelmiştir. Bilişim teknolojilerindeki gelişmeler bilgisayar ağları sayesinde ulusal sınırların ötesine ulaşmıştır. Bu nedenle ulusal düzenlemeler ve ulusal hukuklar bilişim suçları ile mücadelede yetersiz kalmaktadırlar. Bilişim suçları ile ideal bir mücadele, teknolojik gelişmelerle küreselleşen dünyada, bu suçlara karşı uluslararası çapta bir iş birliği ile mümkündür[361].

Yukarıda da değinildiği üzere bilişim, teknik, ekonomik ve toplumsal alanlardaki iletişimde kullanılan ve özellikle elektronik aletler aracılığı ile düzenli bir biçimde işlenmeyi öngören bilimi ifade etmektedir. Bilişim teknolojisi ise, bilişimde kullanılan bütün araç ve gereçlerin oluşturduğu sisteme denir[362].

Bilişim suçu, bilişim sistemleri ve internet kullanımının yaygınlaşmasıyla birlikte ortaya çıkmış, tanımı ve yapısı üzerinde tam bir uzlaşı sağlanamamış bir suç tipi olarak kendini

[361] Mehmet Özdemir, "Bilişim Suçları ve Mücadelede Taşra Teşkilatında Karşılaşılan Problemler ve Çözüm Önerileri", **1. Polis Bilişim Sempozyumu**, Ankara, 21-22 Ekim 2003, s. 284.

[362] Türk Dil Kurumu. http://www.tdk.gov.tr/tdksozluk/sozbul.ASP?kelime (02 Ekim 2014).

göstermektedir. Özellikle elektronik ortamda işlenmesi ve bu ortam içerisinde genel anlamda hukuka aykırılık unsurunun bulunması, bu suç tipinin en belirgin unsurlarıdır. Bilişimin doğal yapısı, sağlamış olduğu özgür iletişim imkânının yanı sıra bireylere yönelik ihlaller bakımından gerçekleştirilmesi çok kolay, kontrol edilmesi ise oldukça güç olan bir ortamın çıkmasına, dolayısıyla da bilişim suçunun kolay ve yaygın biçimde işlenmesine neden olmuştur[363].

Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu Mayıs 1983 tarihli toplantısında bilişim suçunu bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış şeklinde tanımlamıştır[364].

Bilişim suçu daha geniş bir anlamda ise; her türlü teknolojik cihazın kullanılması suretiyle yasal olmayan yollarla kişisel veya kurumsal nitelikteki bilişim sistemlerinde zarar verici etki bırakma şeklinde de tanımlanabilir. Bilişim teknolojilerinde suçun meydana gelebilmesi için mutlaka teknolojinin kullanılması gerekmektedir. Bu teknoloji, bilgisayar, kredi kartı, telefon, pos makinesi gibi cihazlar olabilir[365].

Türk Ceza Kanunu'nda bilişim suçlarının "bilişim alanında suçlar", "mal varlığına karşı suçlar" ve "kişisel verilerin korunmasına ilişkin suçlar" bölümlerinde düzenlendikleri görülmektedir.

Bilişim alanında suçlar bölümünde; hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma (m. 243), bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi (m. 244/1-2), bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama (m. 244/4) ve banka veya kredi kartlarının kötüye kullanılması (m. 245) suçları düzenlenmiştir.

---

[363] Halil İbrahim Dilek, "Bilişim Suçları ve Türk Hukuk Sistemindeki Yeri", (**Yayınlanmamış Yüksek Lisans Tezi**, Diyarbakır Üniversitesi SBE, 2007), s. 11.

[364] Orta, s. 288.

[365] Dilek, s. 10.

Malvarlığına karşı suçlar bölümünde; bilişim sisteminin kullanılması yoluyla işlenen hırsızlık (m. 142/2-e) ve bilişim sistemlerinin kullanılması yoluyla dolandırıcılık (m. 158/1-f) suçları düzenlenmiştir.

Kişisel verilerin korunmasına ilişkin suçlar bölümünde ise; kişisel verilerin kaydedilmesi (m. 135), verileri hukuka aykırı olarak verme veya ele geçirme (m.136) ve verileri yok etmeme (m. 138) suçları düzenlenmiştir.

Ceza mevzuatımızda Fikir ve Sanat Eserleri Kanunu (FSEK) ve Elektronik İmza Kanunu'nda da bilişim suçlarının düzenlendiği görülmektedir. Buna göre; Fikir ve Sanat Eserleri Kanunu'nda, koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri suçu[366] (m. 72) düzenlenmiştir. Elektronik İmza Kanunu'nda ise, elektronik imza oluşturma verilerinin izinsiz kullanımı (m. 16) ve elektronik sertifikalarda sahtekârlık (m. 17) suçlarının düzenlendiği görülmektedir.

Belirtmek gerekir ki; bilişim suçlarıyla mücadele kanun koyucu açısından oldukça zor bir alandır. Suçun faillerinin araştırılması, yakalanması ve yargılanarak cezalandırılması hususiyet arz eden konulardır. Ayrıca, siber uzayın tek bir devletin kontrolünde olmaması da bilişim suçlarıyla mücadeleyi zorlaştırmaktadır. Nitekim yeterli teknik alt yapıya sahip birisi için bilişim suçları, işlenmesi çok kolay ve fakat doğurabileceği sonuçlar bakımından ağır nitelikli suçlardandır. Bilişim suçları, yakınlık, ölçek, fiziki kısıtlamalar ve yöntemler açısından klasik suçlardan farklı olarak faillere çeşitli avantajlar sunmakta, bu avantajlar ise faillerin tespitinde sorunlara neden olmaktadır. Bu bakımdan bilişim suçlarıyla mücadelede üzerinde durulması gereken en önemli konulardan birisi adli bilişim yöntemlerinin geliştirilerek bu alanda uzman personelin yetiştirilmesidir[367].

Bilişim suçlarının soruşturulmasında ve bilişim suçunun faillerinin tespit edilmesinde genellikle bilişim sistemlerinde yer alan delillerden istifade edilmektedir. Bununla birlikte elektronik delil yalnızca bilişim suçlarının ispatlanmasında değil, bilişim

[366] Bu suç tipi ile ilgili ayrıntılı bilgi için bkz. Yusuf Başlar, "Koruyucu Hakları Etkisiz Kılmaya Yönelik Hazırlık Hareketleri Suçu", **Uyuşmazlık Mahkemesi Dergisi**, Cilt. 1, Sayı. 1, (Mayıs 2013), s. 243-259.

[367] Hayati Pallı, "Türk Ceza Kanununda Yer Alan Başlıca Bilişim Suçları", **Adalet Dergisi,** Sayı. 33, (Ocak 2009), s. 132-133.

sistemlerinin suçun işlenmesinde araç veya hedef olarak kullanılmadığı klasik suçlar bakımından da ispat vasıtası olarak kullanılabilmektedir[368].

Gerçekten de, günümüzde elektronik veri depolama birimlerinin yaygınlaşması nedeniyle elektronik delil, sadece bilgisayar sistemlerinin veri depolama birimlerinde yer almamakta, çok değişik elektronik veri depolama cihazlarında da bulunabilmektedir. Bu durum, elektronik delilin bilişim suçları ya da bilişim yoluyla işlenmiş suçların yanı sıra klasik suçlar açısından da önemli bir konuma sahip olmasını sağlamaktadır[369].

Bu bağlamda; TCK'da düzenlenen kasten öldürme (m. 81), organ ticareti (m. 91/6), cinsel taciz (m. 105), tehdit (m. 106), şantaj (m. 107), haberleşmenin engellenmesi (m. 124), hakaret (m. 125), haberleşmenin gizliliğini ihlal (m. 132), özel hayatın gizliliğini ihlal (m. 134/2), müstehcenlik (m. 226), uyuşturucu ve uyarıcı madde kullanılmasını kolaylaştırma (m. 190/2), halk arasında korku ve panik yaratmak amacıyla tehdit (m. 213), suç işlemeye tahrik (m. 214), suçu ve suçluyu övme (m. 215), halkı kin ve düşmanlığa tahrik veya aşağılama (m. 216), yasalara uymamaya tahrik (m. 217), suç işlemek amacıyla örgüt kurma (m. 220/8), göreve ilişkin sırrın açıklanması (m. 258), iftira (m. 258), gizliliği ihlal (m. 285), Cumhurbaşkanına hakaret (m. 299), devletin egemenlik alametlerini aşağılama (m. 300), Türklüğü, Cumhuriyeti, devletin kurum ve organlarını aşağılama (m. 301), halkı askerlikten soğutma (m. 318) suçları ile özel ceza kanunlarında bulunan daha birçok suçun çözümünde elektronik delilin göz ardı edilemez duruma geldiği görülmektedir.

Nitekim kasten öldürme olayına ilişkin dijital fotoğraflar, twitter, facebook vs. sosyal paylaşım siteleri aracılığı ile kişilerin birbirlerine yönelik hakaret ve tehdit içerikli yazışmaları, masumiyeti bilinen bir kişi hakkında BİMER aracılığı ile yapılan iftira niteliğindeki suç ihbarı içeriği, çocuk pornografisi veya kişilerin cinsel mahremiyetine ilişkin fotoğraf ve video kayıtları gibi yukarıda sayılan suçlara dair elektronik delil teşkil edebilecek verilerin bir bilgisayarın sabit diskinde veya bağlı donanımlarında bulunması artık istisnai bir durum olmaktan çıkmıştır.

---

[368] İbrahim Keskin, "Bilişim Suçları", **Adalet Dergisi,** Sayı. 29, (Eylül 2007), s. 116; Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 70.

[369] Ekizer, http://www.ekizer.net/adli-bilisim-computer-forensics (06 Nisan 2014).

BÖLÜM 2: MUKAYESELİ HUKUKTA BİLİŞİM SİSTEMLERİNDE ARAMA VE ELKOYMA

2.1. Genel Olarak

Günümüzde dijital cihazlar, kullanıcılarına, şaşırtıcı miktarda kişisel bilgiyi ve her türlü veriyi saklama imkânı tanımaktadır. İnsanlar artık, klasik mektup ve dosya dolapları yerine elektronik posta ve sabit diskleri tercih etmektedirler. Bugünün yüksek teknoloji dünyasında ceza soruşturmaları yürütülürken, soruşturma makamları, fiziksel delillerden ziyade elektronik delille karşılaşmaktadırlar. Kolluk görevlilerinin ise, suç faaliyetine ilişkin delilleri elde etmek amacıyla herhangi bir dijital cihazı incelemeden önce -tıpkı şüphelinin ev, iş yeri ve aracında arama yapılmadan önce olduğu gibi- arama kararı almaları gerekmektedir[370].

Geleneksel arama ve elkoyma kuralları özel hayatın gizliliği hakkını tehdit eden genel ve keşif mahiyeti taşıyan aramaları önlemekte başarısız kalmaktadır. Bu sorunu fark eden mahkemeler dijital ortam aramaları için "özel yaklaşımlar" benimsemektedir. Bu yaklaşım tarzı, özel hayatın gizliliğini önemli ölçüde korumasına karşın, kolluğun yasal çerçevede yaptığı arama işlemlerini ise çoğu zaman ciddi şekilde engellemektedir. Bu nedenle hem özel hayatın gizliliği hakkını hem de adaletin yerine getirilmesini korumak amacıyla yasama organları dijital ortamda yapılacak arama ve elkoyma işlemlerine yönelik yasalar çıkartmak zorundadırlar[371].

Bu bağlamda Avrupa Konseyi Siber Suç Sözleşmesi (AKSSS) başta olmak üzere Amerika Birleşik Devletleri, İngiltere, Almanya, Fransa ve İtalya hukuk sistemlerinde elektronik delil elde etmeye yönelik bilişim sistemlerinde yapılan arama ve elkoyma koruma tedbirlerinin incelenmesi yerinde olacaktır.

[370] Lily R. Robinton, "Courting Chaos: Conflicting Guidance from Courts Highlights The Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence", **Yale Journal of Law and Technology**, Vol. 12, (2010), s. 311.

[371] Robinton, s. 311.

2.2. Avrupa Konseyi Siber Suç Sözleşmesi Kapsamında Bilişim Sistemlerinde Arama ve Elkoyma

2.2.1. Genel Olarak

Bilişim teknolojilerinin hızlı bir şekilde gelişmesi nedeniyle ceza muhakemesi hukuku, işlenen suçların etkin şekilde soruşturulması bakımından uyumluluk gösterme zorunluluğu içerisinde bulunmaktadır. Özellikle elektronik ortamda bulunan delillerin saniyeler içerisinde karartılabilir olma nitelikleri, söz konusu delillerin karartılabilme olasılığını en aza indirgeyecek ceza muhakemesi hukuku koruma önlemlerini oluşturmayı gerekli kılmaktadır. Aksi takdirde, elektronik ortamda işlenen suçların faillerinin ve bu suçların ispatı için aranan delillerin elde edilememesi durumu ile karşı karşıya kalınabilmektedir[372].

Bilişim teknolojilerinin ve internetin getirmiş olduğu yenilikler ve kolaylıklara karşın bunların suç işlemek için de kullanılmaları ve işlenen suçların -terör ve pornografik yayınlarda olduğu gibi- ülke sınırlarını aşacak nitelikte olmaları, devletleri bilişim alanında işlenen suçların etkin şekilde soruşturulması ve bu suçlarla mücadele edilmesi hususlarında iş birliği yapma noktasına getirmiştir[373].

Bu bağlamda, Avrupa Konseyi Bakanlar Komitesinin 4 Şubat 1997 tarihli toplantısında alınan karar ile oluşturulan "Siber Uzay Suçları Uzmanlar Komitesi (PC-CY)", Nisan 1997'de toplanarak siber suçlara ilişkin uluslararası bir anlaşma taslağını görüşmeye başlamıştır. Görüşmelerden sonra, gözden geçirilmiş ve son halini almış konvansiyon taslağı ve gerekçe niteliğine sahip açıklayıcı notası (memorandumu) Haziran 2001'de genel kurulda onaylanmak üzere Avrupa Suç Sorunları Komitesine ve ardından kabul edilip imzaya açılmak üzere Bakanlar Komitesine sunulmuştur[374].

---

[372] Serap Keskin, "Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt. 59, Sayı. 1-2, (2001), s. 155.

[373] Fatih Selami Mahmutoğlu, "Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt. 59, Sayı. 1-2, (2001), s. 40.

[374] Kayıhan İçel, "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, Cilt. 59, Sayı. 1-2, (2001), s. 5-6.

Uluslararası alanda ortak bir ceza politikasının oluşturularak toplumun siber suçlara karşı korunması, ortak suç tanımlarının getirilmesi, soruşturma yöntemlerinin tanımlanması (veriyi saklama, trafik verisini arama, toplama ve elkonulması ile iletişim yetkisi) ve uluslararası işbirliğinin geliştirilmesi amacını taşıyan Avrupa Konseyi Siber Suç Sözleşmesi 23 Kasım 2001 günü Budapeşte'de 26 üye ülke ile 4 üye olmayan ülke (ABD, Japonya, Kanada ve Güney Afrika) olmak üzere toplam 30 ülke tarafından imzalanmıştır[375].

2004 yılında yürürlüğe giren ve Avrupa Konseyi Siber Suç Sözleşmesi olarak bilinen bu sözleşmenin giriş bölümünde, sözleşmenin toplumun elektronik ortamda işlenen suçlara karşı korunması için gerekli yasal düzenlemelerin yanı sıra uluslararası işbirliğinin geliştirilmesi yollarıyla ortak bir ceza politikasının kabul edilmesi, bilgisayar ağlarının dijital hale gelmesinin, tek bir noktaya yönelmesinin ve sürekli küreselleşmesinin beraberinde getirdiği önemli değişikliklerin ortaya çıkması, bilgisayar ağlarının ve elektronik bilgilerin suç işlenmesi amacıyla kullanılabilmesi, bu tür suçlara ilişkin delillerin ise bu ağlarda saklanabileceği gibi bu ağlar aracılığıyla aktarılabilmesi riskinin ortaya çıkması sonucunda elektronik ortamda işlenen suçlarla mücadelede ülkelerle özel sektör arasında işbirliğinin sağlanması, bilgi teknolojilerinin kullanımı ve geliştirilmesine ilişkin meşru hakların korunması ve de bu tip suçlara karşı etkin mücadelede uluslararası işbirliğini gerçekleştirme bilinciyle imzalandığı belirtilmektedir.

Bu bağlamda bu sözleşmenin temel amacı, "gerekli mevzuatın kabul edilmesi ve uluslararası işbirliğinin geliştirilmesi yoluyla siber suçlara karşı toplumun korunmasını amaçlayan ortak bir ceza politikasının izlenmesi" olduğu söylenebilir. Ayrıca Sözleşmede, "siber suçların ortak tanımlarının yapılması, cezai soruşturma ve kovuşturma yöntemlerinin belirlenmesi, siber suçlara karşı uluslararası işbirliği yollarının oluşturulması" hedeflenmektedir. Sözleşme, taraf olan ülkelere, tanımlanan suçların işlenmesini ve söz konusu suçların işlenmesine yardım veya yataklık yapılmasını ulusal mevzuatta cezai bir suç olarak tanımlanma ve gerekli yasama işlemlerini ve diğer işlemleri yapma yükümlülüğü getirmektedir. Sözleşme, söz konusu

[375] Mustafa İlker Öztürk, s. 47.

suçlara yönelik soruşturma ve kovuşturmaların yanı sıra işlenen suçlara delil teşkil edebilecek verilerin toplanması, saklanması, araştırılması ve elkonulması gibi ulusal düzeyde alınması gereken tedbirleri de içermektedir[376].

Elektronik ortamda özgürlüklerin, insan haklarının ve güvenliğin korunması ile risklerin azaltılmasına ilişkin kabul edilmiş tek uluslararası rehber ve hükümetlerin vatandaşlarını korumasına yönelik önemli bir araç niteliğinde olan bu sözleşmede, özellikle telif hakları ihlalleri, bilgisayarlarla bağlantılı sahtecilik eylemleri, çocuk pornografisi, ağ güvenliğine ilişkin suçlar tanımlanmakta ve bu suçlarla mücadele etmede işbirliği öngörülmektedir. Bununla birlikte Sözleşmede ceza muhakemesi hukukuna ilişkin hükümlerin ceza yargılaması sürecinde elektronik delillerin elde edilmesi ve korunmasına yönelik koruma tedbirleriyle ilgili olduğu da görülmektedir. Bu hükümler ise Sözleşmenin 14-21. maddeleri arasında düzenlenmiştir.

Avrupa Konseyi bünyesinde hazırlanmış olup internet ve bilgisayar ağları aracılığıyla işlenen suçlara ilişkin uluslararası nitelikteki ilk belge olma özelliği taşıyan Sözleşmede öngörülen koruma tedbirleri, elektronik ortamda işlenen suçu ve bu suçun fail veya faillerini ortaya çıkartabilmek için delil elde edebilmek amacıyla ceza muhakemesi hukukunun klasik koruma tedbirlerinden olan arama ve elkoyma tedbirlerinin elektronik ortamdaki özel bir türünü teşkil etmektedir. Sözleşmede ayrıca, arama tedbirinde elektronik delili özgün niteliği ile elde etmek bakımından geç kalınması tehlikesinin varlığı halinde elektronik verileri arama işlemi öncesinde aramayı olanaklı kılacak, veriler üzerinde ön koruyucu niteliğe sahip tedbirlere de yer verilmiştir[377].

2.2.2. Sözleşmenin Usul Hukukuna İlişkin Hükümleri

Elektronik ortamında gerçekleşen suçlarla mücadelede karşılaşılan en önemli sorunlardan birisi failin teşhis edilmesi ve suçu oluşturan fiilin kapsamını ve etkilerini değerlendirmektir. Karşılaşılan sorunlardan bir diğeri ise saniyeler içerisinde değişebilen, taşınabilen veya silinebilen elektronik verilerin geçici niteliğidir. Bu bağlamda Sözleşmenin arama ve elkoyma gibi geleneksel koruma tedbirlerini yeni

[376] Bilişim Ajandası, "Nihayet Türkiye de 'Sanal Suçlar Sözleşmesi'ni İmzaladı", **Bilişim Kültür Dergisi**, 2010, http://www.bilisimdergisi.org/s127 (04 Mart 2014), s. 12.

[377] Serap Keskin, s. 156.

teknoloji ortamına uyumlu hale getirme ve bu koruma tedbirlerinin teknolojik ortamda etkinliklerini sürdürmeleri için verilerin hızlı bir biçimde korunmasına ilişkin yeni yöntemler belirlediği görülmektedir[378].

2.2.2.1. Usul Hükümlerinin Kapsamı

Sözleşmenin 14. maddesi taraf ülkelerden her birinin ulusal mevzuatına ve hukuki çerçevelerine uygun olarak Sözleşmede tanımlanan yetki ve usulleri tesis etmek amacıyla gerekli olan özel ceza soruşturma ve işlemleri ile ilgili yasama işlemlerini yapmasını öngörmüştür[379].

Sözleşmenin 14. maddesine göre, 20. ve 21. maddelerde öngörülen tedbirler hariç Sözleşmede belirtilen sair tüm tedbirler Sözleşmede öngörülen suçlar ile Sözleşmede öngörülmese de bilgisayar sistemleri* aracılığıyla işlenen diğer suçlar ve cezai bir suça ilişkin olarak elektronik ortamda delil toplamak amacıyla kullanılabilecektir.

Sözleşmenin aynı maddesine göre, Sözleşmenin 2. kısmında belirlenen yetkiler ve usuller yoluyla herhangi bir suça ilişkin olarak elektronik ortamda delil elde edilebilmesi güvence altına alınmaktadır. Böylece bilgisayar verilerini elde etmek için elektronik olmayan veriler için de klasik yetkiler ve usuller çerçevesinde mevcut olanlara paralel imkânlar sağlanmıştır. Ayrıca, Sözleşmede, tarafların, kovuşturulan suçun niteliğinden bağımsız olarak elektronik ortamda bulunan bilgilerin ceza yargılamalarında delil olarak kullanılmasının imkân dâhilinde olduğu hususunu ülke mevzuatlarına sokmak zorunda oldukları belirtilmektedir[380].

---

[378] Sevil Yıldız, "Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi", (**Yayınlanmamış Doktora Tezi**, Selçuk Üniversitesi SBE, 2006), s. 188.

[379] Oğuz Turhan, "Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar)", (**Yayınlanmamış Planlama Uzmanlığı Tezi**, Başbakanlık Devlet Planlama Müsteşarlığı Hukuk Müşavirliği, Ankara, 2006), s. 116.

* AKSSS'nin hazırlık süreci yıllarında "bilgisayar" kavramı çok fazla ön planda olduğu için Sözleşmede "bilgisayar sistemi" ve "bilgisayar verisi" kavramlarının kullanıldığı görülmektedir. Bununla birlikte Sözleşmede "bilgisayar sistemi ve " bilgisayar verisi" kavramları çok geniş kapsamlı olarak tanımlandıklarından dolayı günümüzde herhangi bir şekilde veri iletimine izin veren her türlü teknoloji bilgisayar olarak tanımlanabilir. Yasin Beceni, "Avrupa Siber Suçlar Sözleşmesi", **Bilişim Hukuku**, Mete Tevetoğlu (drl.), İstanbul: Kadir Has Üniversitesi Yayınları, 2006, s. 97.

[380] Oğuz Turhan, s. 117.

Bununla birlikte, yukarıda da değinildiği üzere, usul hükümlerinin uygulama alanı gerek özel hayatın gizliliğini gerekse iletişim özgürlüğünü ihlal edici özellikleri göz önüne alınarak Sözleşmenin 20. maddesinde düzenlenen içerik bilgilerinin gerçek zamanlı olarak toplanması ve 21. maddede düzenlenen içerikle ilgili bilgilere müdahale edilmesi tedbirleri bakımından istisna tutulmuşlardır.

2.2.2.2. Şartlar ve Önlemler

Sözleşmenin 15. maddesine göre, sözleşmeyi imzalayıp onaylayan devletler, Sözleşme hükümleri doğrultusunda öngörülen koruma tedbirleri arasında denge kuran ve temel hak ve özgürlüklere yeterli güvence öngören düzenlemeler yapmak zorundadırlar. Söz konusu dengeyi sağlayıcı unsurlar Sözleşmede gösterilmemekte, bunları belirleme işi taraf devletlere bırakılmaktadır. Bununla birlikte, devletler için ortak standartların da bulunduğu, devletlerin söz konusu düzenlemeleri yaparken bu ortak standartları temel almak zorunda oldukları da vurgulanmaktadır[381]. Sözleşmede belirtilen yetki ve usullerin bu şekilde kullanılmasıyla "hakkaniyet ilkesinin tesis edilmesi" de sağlanmış olacaktır. Hakkaniyet, her bir taraf ülke tarafından iç hukuklarındaki ilgili ilkeler uyarınca uygulanacaktır[382].

Ceza muhakemesi hukukunda her koruma tedbirinde olduğu gibi Sözleşmede öngörülen bilişim koruma tedbiri ile işlendiği iddia edilen suç arasında da bir dengenin olması gerekmektedir. Hafif bir koruma tedbiri ile delile ulaşmak mümkün iken daha ağır nitelikteki bir bilişim koruma tedbirine başvurulmaması gerekmektedir. Bu durum ceza muhakemesi hukukunda koruma tedbirlerinin ortak özelliklerinden biri olan oranlılık ilkesinin bir tezahürüdür. Bu bakımdan, taraf devletler, Sözleşmede öngörülen koruma tedbirlerini iç hukuklarında düzenlerken, her bir koruma tedbiri için başvurma koşullarını ve usulünü oranlılık ilkesi doğrultusunda belirlemek zorundadırlar[383].

Sözleşmenin 15. maddesinde ayrıca, taraf devletlerin kamu yararını ve adaletin sağlıklı şekilde yürütülmesini de dikkate almaları, bu bağlamda kamu yararı ile tutarlı olduğu

[381] Serap Keskin, s. 160.

[382] Oğuz Turhan, s. 117.

[383] Serap Keskin, s. 160-161.

ölçüde belirtilen koruma tedbirlerinin uygulanmaları sonucunda hizmet sağlayıcılar dâhil üçüncü kişilerin hak, sorumluluk ve haklı yararları üzerindeki etkiyi ve bu etkinin hafifletilmesi yollarını da değerlendirmeleri gerekmektedir[384].

2.2.2.3. Saklanan Bilgisayar Verilerinin Hızlı Bir Biçimde Korunması

Avrupa Konseyi Siber Suç Sözleşmesi'nin en önemli özelliği siber suçlarla ilgili uluslararası ortamda ortak bir yaklaşım belirlemiş olmasıdır. Birçok ülkede elektronik verinin korunması yeni bir kavram olmakla birlikte, elektronik veriler bilgisayarla ilgili suçlara yönelik soruşturmalarda önemli bir rol oynamaktadır. Bu bağlamda, suça yönelik fiil ve faili tespit etmede, uluslararası ortamda ortak bir tutum belirlemek amacıyla depolanmış verilerin korunması konusuna açıklık getirilmiştir[385].

Elektronik delilin önem arz ettiği suçlarda yapılması gereken ilk ve en önemli iş elde edilerek saklanan elektronik verilerin değişmeden muhafaza edilmesini sağlayacak bir şekilde koruma altına alınması hususudur [386] . Bilgisayar verilerinin korunması, depolanmış olan bir verinin, kalitesini veya durumunu değiştirecek veya bozacak her türlü şeyden korunması anlamına gelmektedir. Bilgisayar verilerinin korunmasını gerekli kılan üç temel neden bulunmaktadır. Birincisi, bilgisayar verilerinin kolaylıkla değiştirilebilmesidir. İkincisi, bilgisayarlarla ilişkili suçların büyük çoğunluğunun bilgisayar sistemleri aracılığı ile yapılan iletişim yayınlarından kaynaklanmasıdır. Üçüncüsü ise, kanunsuz içerik veya suça yönelik fiilin kanıtını taşıyan iletişimin muhafazasının soruşturmalarda da delil niteliği taşımasıdır[387].

Sözleşmenin 16/1 maddesinde belirtilen depolanmış verilerin hızlı bir biçimde korunması tedbiri, bilgisayar verileri üzerinde gelecekte uygulanması planlanan arama ve elkoyma tedbirlerini gerçekleştirebilmeyi mümkün kılmak amacıyla öngörülmüş bir koruma tedbiridir. Bu sayede, bilgisayar verilerinin silinmeden, değiştirilmeden, bozulmadan, özgün niteliğiyle korunabilmesi amaçlanmaktadır. Koruma, zorunlu olarak

[384] Serap Keskin, s. 161.

[385] Aslı Deniz Helvacıoğlu, "Avrupa Konseyi Siber Suç Sözleşmesi Temel Hükümlerinin İncelenmesi", **İnternet ve Hukuk**, Yeşim Atamer (drl.), İstanbul: Bilgi Üniversitesi Yayınları, 2004, s. 289-290.

[386] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1094.

[387] Helvacıoğlu, s. 290.

koruma altına alınan verilerin ya da kopyalarının haklı kullanıcılar tarafından erişilememesi anlamına gelmemektedir. Bu durum "verilerin dondurulması" şeklinde ifade edilmektedir. Bununla birlikte, Sözleşme verilerin dondurulup dondurulmaması, başka bir ifadeyle verilerin erişilmez kılınıp kılınmaması hususunun takdirini taraf devletlere bırakmıştır[388].

Bu koruma tedbiri "veri içeriği" ve "bu veriye ilişkin sinyal bilgisi"nin kaybolmasını ve değiştirilmesini önlemeye ve böylece muhafaza altına almaya yönelik olup elektronik verinin içeriğine girmeyi ve bir anlamda bunu okumayı kapsamamaktadır. Bu koruma tedbirinin amacı, delil olabilecek nitelikteki bir verinin içeriğinin nasıl oluştuğu, ne şekilde değiştirildiği, hangi yolları izleyerek o bilgisayara ulaştığı gibi hususların kuşkuya yer bırakmayacak şekilde güven altına alınması ve bu veri içeriğinin delil olarak sonraki bir tarihte mahkeme önünde tartışmasız bir şekilde ortaya konmasını sağlamaktır. Bu tedbirde sinyal bilgileri de muhafaza altına alınacağından verinin naklinde rol oynamış olan servis sağlayıcıların da belirlenmesi gerekmektedir[389].

Sözleşmenin 16/2 maddesinde ayrıca, tarafların korumayı bir emir yoluyla yürürlüğe sokmaları halinde, koruma emrinin, bu emri alan kişinin kontrolü altında bulunan veya sahip olduğu belirtilen depolanmış bilgisayar verisi ile ilişkili olmasının gerektiği belirtilmektedir. Emri alan kişi, bu bilgisayar verisinin bütünlüğünü, asgari 90 gün olmak üzere gerekli olduğu sürece sağlamak ve muhafaza etmek zorundadır[390].

Ayrıca, taraf devletlerin bilgisayar verilerini koruması gereken görevlinin veya başka bir kişinin bu hususa ilişkin usulleri iç hukukta belirtilen süre boyunca gizli tutması için gerekli önlemleri almaları gerekmektedir (m. 16/3). Hâkimin verdiği bu kararlara uymayan kişi hakkında ise Sözleşmenin 14. ve 15. maddeleri uyarınca yaptırım uygulanabilecek ve ilgili hakkında muhakeme hukuku garantileri öngörülebilecektir (m. 16/4).

[388] Serap Keskin, s. 161-162.

[389] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1094.

[390] Helvacıoğlu, s. 290.

2.2.2.4. Trafik Verilerinin Hızlı Bir Biçimde Korunması ve Kısmen Açıklanması

Bilgisayarın içinde olan veya internet üzerinde dolaşan elle tutulamayıp gözle görülemeyen elektronik veriler, ceza muhakemesi hukukunda kendine özgü bir delil hukuku oluşturmuştur. Bu nedenle, internete giren bilgisayarlar arasında yapılan iletişim bilgileri ile ağa giren bilgisayarın o sırada nerede bulunduğunun tespit edilmesine ilişkin bilgilerin, servis sağlayıcıları tarafından belli bir süre saklanması zorunluluğu bulunmaktadır[391].

Bu bağlamda Sözleşmenin 17. maddesiyle de taraf devletlere 16. madde uyarınca korunması gereken trafik bilgilerine ilişkin olarak bu bilgilerin korunması işleminin kolaylaştırılması hususunun söz konusu bilgilerin bir ya da birden fazla hizmet sağlayıcı tarafından iletilmiş olmasına bakılmaksızın sağlanması ve ayrıca taraf devletin yetkili merciye veya bu merciin belirlediği bir kişiye söz konusu servis sağlayıcıları ve bilgilerin iletildiği yolu belirleyebilmesini sağlayacak ölçüde açıklama yapılması işleminin kolaylaştırılması zorunluluğu yüklenmektedir.

Sözleşmenin 1/d maddesine göre trafik bilgileri terimi, bir bilgisayar sistemi kullanılarak yapılan bir iletişime ilişkin olarak, söz konusu iletişim zincirinin bir halkası konumunda bulunan bir bilgisayar sistemi tarafından üretilen ve iletişimin başlangıç noktasını, varış noktasını, izlediği yolu, saatini, tarihini, boyutlarını, süresini veya bu iletişimde kullanılan hizmetin tipini gösteren herhangi bir bilgisayar verisini ifade etmektedir.

Bu bağlamda, sözleşmenin 17. maddesinde öngörülen koruma tedbiri ile 16. maddede düzenlenen koruma tedbiri çerçevesinde trafik bilgilerinin hızlı biçimde korunması ile ilgili somut zorunluluklar getirilmekte ve iletişim sürecinde birden fazla hizmet sağlayıcının da bulunabileceği göz önünde tutularak, bunları ve iletinin izlediği elektronik yolu belirleyebilmek için bazı trafik verilerinin açığa vurulması sağlanmaktadır[392].

[391] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1093.

[392] Serap Keskin, s. 165.

Depolanmış trafik verileri, geçmişte yapılmış olan iletişimlerin kaynağının veya varış noktalarının tespit edilmesinde ve böylece suçu işleyen kişilerin tespitinde büyük öneme sahiptir. İletişimin yayınlanmasında genellikle birden çok hizmet sağlayıcı rol oynamaktadır. Bunlardan her biri trafik bilgilerinin bir kısmına sahip olabilir ve bu bilgilerin toplanması ile sonuca ulaşılabilir. İşte Sözleşmenin 17. maddesinde birden fazla hizmet sağlayıcının, iletişimin yayınında yer aldığı durumlarda, trafik verisinin hızlandırılmış muhafazasının tüm hizmet sağlayıcılar bakımından geçerli olduğu ifade edilmektedir[393].

Bununla birlikte, bu işlemin nasıl yapılacağı Sözleşmede belirtilmemiş ve taraf devletlerin hukuk ve ekonomi sistemiyle uyumlu bir yol seçmek üzere iç hukuklarına bırakılmıştır. Taraf devletlerin yetkili idarecileri her hizmet sağlayıcısına muhafaza emrini ayrı ayrı gönderebileceği gibi iletişimin iletimine katıldıkları belirlenen tüm hizmet sağlayıcılar için geçerli olacak tek bir talimat göndermeleri de mümkündür[394].

2.2.2.5. Üretim Emri

Sözleşmenin 18. maddesi, taraf devletlerin yetkili makamlarının ulusal sınırlar içerisinde bulunan bir kişiyi, kendi mülkiyetinde veya kontrolünde bulunan bir bilgisayar sisteminde ya da başka bir cihazda saklanan verileri verme ve ayrıca yine ulusal sınırlar içerisindeki bir hizmet sağlayıcının mülkiyetinde ya da kontrolünde bulunan sözü geçen hizmete ilişkin abone bilgilerini verme yönünde talimat verme konusunda yetkili kılacak yasal düzenlemelerde bulunmasını öngörmektedir.

Sözleşmenin 18. maddesi ile "veriyi teslim etme yükümlülüğü" doğuran ve "production order" adı verilen bir karar tipi oluşturulmuştur. Bu karar ile hâkim, nezdinde, zilyetliğinde veya denetimi altındaki bir bilgisayar ortamında saklanan veriyi bulunduran bir kişiye veya servis sağlayıcısına "ileride delil olabilecek nitelikte bilgiler taşıyan bir veriyi" teslim etme mecburiyetini yükleyebilmektedir. Bu madde ile klasik ceza muhakemesi hukukunda mevcut bulunan, elinde delil olabilecek bir şey bulunduran kişiye, bunu devlete teslim etmesi anlamında bir "muhafaza altına alma

[393] Helvacıoğlu, s. 290-291.

[394] Sevil Yıldız, s. 192.

kararı", rıza ile vermezse "elkoyma kararı" veya tanığı tanıklık yapmaya mecbur etmek için kullanılan "zorlama hapsi" gibi tedbirlere benzeyen yeni bir karar tipi oluşturulmuştur[395].

Sözleşmenin 18. maddesinde düzenlenen üretim emri, söz konusu yasal düzenlemelerin uygulanmasına esneklik kazandırmakta ve özellikle hizmet sağlayıcılarının yetkililere kontrolleri altındaki verileri gönüllü olarak vermeleri hususunda yasal bir dayanak sağlamaktadır[396].

Üretim emrinin konusunu oluşturan veriler depolanmış konumda bulunan verilerdir. Bu bakımdan şimdiki zamanda akış durumunda bulunan bilgisayar verileri üzerinde üretim emrinin verilebilmesi olanak dâhilinde değildir. Üretim emri, ancak kişi ya da hizmet sağlayıcının söz konusu verileri depoladığı hallerde önem arz etmektedir. Bununla birlikte, Sözleşme, kişi ya da kurumlara verileri depolama yükümlülüğü veya depolamaları halinde verilerin doğruluğunu güvenceye bağlama yükümlülüğü getirmemektedir. Eğer hizmet sağlayıcı, hizmet verdiği abonelerin kayıtlarını tutmuyorsa bu koruma tedbiri kullanılamayacaktır[397].

Abonelik bilgileri terimi, bilgisayar verisi şeklinde ya da başka şekillerde saklanan ve hizmet sağlayıcının elinde bulunan ve verilen hizmetlere ilişkin olan trafik ya da içerikle ilgili bilgilerinin haricindeki bilgileri ifade etmektedir. Bu bilgiler kullanılarak sağlanan iletişim hizmetinin türü, teknik imkânlar ve hizmet süresi, abonenin kimliği, posta ya da bulunduğu yerin adresi, telefon numarası ve aboneye ulaşılabilecek diğer numaralar, hizmet sözleşmesi veya düzenlemesi esas alınarak verilen fatura ve ödeme bilgileri, hizmet sözleşmesi veya düzenlemesi esas alınarak verilen ve iletişim ekipmanının kurulduğu bölgeye ilişkin olan diğer bilgiler belirlenebilmektedir.

Başka bir ifadeyle abonelik bilgileri, bir hizmet sağlayıcının idari bölümü tarafından hizmetlere abone olan kişilerle ilgili tutulan bilgileri ifade etmektedir. Abonelik bilgisi, bilgisayar verileri biçiminde olabileceği gibi kâğıt üzerine tutulmuş kayıtlar gibi başka

[395] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1095.

[396] Helvacıoğlu, s. 291.

[397] Serap Keskin, s. 167.

biçimlerde de bulunabilirler. Soruşturmada abone bilgisine ya abonenin hangi hizmetlerden istifade ettiğinin tespit edilmesi ya da teknik adresin bilinmesi halinde kişinin tespit edilmesi için ihtiyaç duyulmaktadır[398].

Sözleşmenin 18. maddesinde belirtilen, "mülkiyetinde ya da kontrolünde" ifadesiyle verilerin üretim emrini veren ülkenin sınırları içerisinde fiziksel mülkiyet dâhilinde bulunması ya da fiziksel mülkiyetin dışında ise kişinin ya da hizmet sağlayıcının üretim emrini veren ülkenin sınırları içinden verilerin üretimini serbestçe kontrol edebilme olanağı anlatılmaktadır. Bu bağlamda, uzaktaki bir online depolama hizmeti yoluyla hesabında depoladığı bilgiler için kendisine üretim emri verilen kişi ile başka bir şirketin sağladığı veri depolama olanağından yararlanıp, abone bilgilerini uzakta depolayan hizmet sağlayıcı söz konusu abone bilgilerini üretmek zorunda kalacaktır. Sözleşmede geçen "hizmete ilişkin" ibaresiyle ise üretim emrini veren ülkenin sınırları içinde sunulan hizmetlerle ilgili abonelik bilgileri anlatılmak istenmektedir[399].

Hâkimin verdiği bu kararlara uymayan kişi hakkında ise Sözleşmenin 14 ve 15. maddeleri uyarınca yaptırım uygulanabilecek ve ilgili hakkında muhakeme hukuku garantileri öngörülebilecektir (m. 18/3).

2.2.2.6. Saklanan Bilgisayar Verileri Hakkında Arama ve Elkoyma

Sözleşmenin 19. maddesinde belirtilen koruma tedbiri ile somut bir ceza soruşturmasında, delil elde edebilmek amacıyla depolanmış durumda bulunan bilgisayar verilerinin aranması ve bu verilere elkoyma işlemleri düzenlenmektedir. Bu koruma tedbiri, elektronik olmayan ortamdaki arama ve elkoyma koruma tedbirlerinin elektronik ortamda uygulama alanı bulan bir görünümüdür[400].

Bu bakımdan, hükmün amacının, maddi varlığa sahip nesneler üzerinde uygulanan arama ve elkoyma tedbirine ilişkin geleneksel soruşturma yetkilerini bilişim sistemleri ve buralarda depolanmış elektronik veriler bakımından genişletmek ve ayrıca siber suçlarla ilgili yürütülen soruşturmalarla alakalı elektronik delillerin toplanmasına olanak

[398] Oğuz Turhan, s. 120.

[399] Serap Keskin, s. 167.

[400] Serap Keskin, s. 169.

sağlamak olduğu söylenebilir. Nitekim birçok ülkede depolanmış bilgisayar verisi maddi varlığa sahip nesne olarak kabul edilmediğinden kolluk teknolojik ortamdaki verilerin elde edilmesi bakımından geleneksel tedbirleri uygulayamamaktadır[401].

Yukarıda da belirtildiği üzere, saklanan bilgisayar verilerinin aranması ve bunlara elkonulmasına yönelik koruma tedbiri depolanmış vaziyetteki bilgisayar verilerine ilişkindir. Sözleşmede, elektronik posta kutusunda bekleyen ancak henüz bilgisayar sistemine yüklenmemiş durumdaki elektronik posta mesajının depolanmış bilgisayar verisi mi yoksa transfer edilecek bir elektronik veri mi olduğuna ilişkin bir açıklık bulunmamaktadır. Bu hususu açıklamaya yönelik yapılması gereken düzenlemeler taraf devletlerin iç hukuklarına bırakılmıştır[402].

Sözleşmenin 19/1 maddesinde taraf devletler, yetkili makamlarını kendi ulusal sınırları içinde, bir bilgisayar sistemi veya sistemin bir parçasında ya da veri saklama cihazlarında arama yapma veya benzer şekilde erişim yapma konusunda yetkilendirmeleri gerekmektedir. Bu yetkilendirmenin ulusal sınırların dışında gerçekleştirilmesi mümkün değildir. Bunun için taraf ülkelerin karşılıklı iş birliği yolunu seçmeleri gerekmektedir.

Bu madde hükmünde "arama veya benzer şekilde erişim" ifadesinin kullanıldığı görülmektedir. Buna göre, verileri bulmaya çalışma, okuma, denetleme ve inceleme anlamlarına gelen klasik "arama" ifadesi devlet tarafından cebri yetkilerin kullanılması fikrini işaret etmektedir. "Erişim" kelimesi ise, bilgisayar terminolojisini daha iyi yansıtan, belli bir yargıyı içermeyen bir ifadedir. Bu bakımdan Sözleşmede klasik kavramlarla modern terminolojiyi uzlaştırmak amacıyla her iki ifade de kullanılmıştır.

Diğer taraftan bu hükme göre, bilgisayarda arama yapmak için ya bilgisayar sistemine girmek ya bilgisayarda kayıtlı bulunan verinin içine girmek ya da bilgisayar verisi saklanan bir ortama girmek gibi üç ayrı işlem tipi düzenlenmektedir. Bilgisayar

[401] Lorenzo Picotti and Ivan Salvadori (hzl.), **National Legislation Implementing the Convention on Cybercrime-Comparative Analysis and Good Practices**, Strasbourg: Discussion Paper, 2008, s. 55.

[402] Sevil Yıldız, s. 195.

sisteminde arama yapma kararı veren hâkimin hangi işlemin yapılacağını kararında belirtmesi gerekmektedir[403].

Sözleşmenin 19/2 maddesinde, bir önceki fıkra uyarınca yapılan arama veya erişim sırasında aranan verilerin ulusal sınırlar içerisindeki başka bir bilgisayar sisteminde ya da bu sistemin bir parçasında saklandığına dair gerekçelerin varlığı halinde söz konusu arama ve erişim işlemlerinin bu sistemleri de kapsayacak şekilde genişletilebilmesine izin verilmektedir.

Sözleşmenin 19/3 maddesinde, 19/1 ve 19/2 maddeleri uyarınca yapılan arama sonucunda erişilen bilgisayar verilerine elkoyma veya bunları başka şekillerde koruma altına alma hususunda izin verilmesi öngörülmektedir. Bu madde uyarınca herhangi bir bilgisayar sistemine ya da bu sistemin bir parçasına veya bilgisayar verilerinin saklandığı cihazlara elkonulması ya da bunların benzer şekilde koruma altına alınması, bu bilgisayar verilerinin kopyalanıp alıkonulması, söz konusu saklı bilgisayar verilerinin doğruluğunun muhafaza edilmesi, erişilen bilgisayar sistemindeki söz konusu verilerin erişilemez, kullanılamaz hale getirilmesi ya da silinmesine izin verilmektedir.

Sözleşmenin 19/4 maddesi ise, elektronik ortamda arama yapma ve elkoyma işlemini gerçekleştirme konusunda teknik bilgiye sahip kişilere, yetkili mercilerin işini kolaylaştırmak amacıyla yardım etme zorunluluğunun getirilebilmesini düzenlemektedir. Bu bağlamda, bilgisayar sisteminin işleyişi ya da bu sistem içindeki bilgisayar verilerinin korunması için kullanılan önlemler hakkında bilgi sahibi olan herhangi bir kişinin arama ve elkoyma konusunda yardımcı olmaya zorlanmasına izin verilmektedir. Ancak, bu yardım yükümlülüğü, "makullük" ölçütü ile sınırlandırılmıştır. Buna göre, bilgi sağlama, bir şifrenin ya da başka bir güvenlik önleminin açığa vurulmasının diğer kullanıcıların gizliliğini ya da aranması için yetki verilmeyen verileri tehdit ediyorsa makul olmayabilir[404].

[403] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1096.

[404] Serap Keskin, s. 171.

2.2.2.7. Trafik Verilerinin Gerçek Zamanlı Olarak Toplanması

Sözleşmenin 20. maddesinde, taraf devletlerin yetkili makamlarının bir bilgisayar sistemi üzerinden aktarılan ve ulusal sınırlar içerisinde kalan özel iletişim niteliğindeki trafik bilgilerini yine ulusal sınırlar içinde bulunan teknik imkânlar kullanılmak suretiyle gerçek zamanlı (anlık) olarak toplanması ya da kaydedilmesi hususunda yetkili kılınması ve servis sağlayıcıların söz konusu trafik bilgilerinin toplanması ve kaydedilmesi işlemleriyle ilgili olarak yetkili makamlarla iş birliği yapması ve onlara bu konuda yardımcı olmaları hususunda yasal düzenlemelerde bulunması öngörülmektedir.

Trafik verilerinin gerçek zamanlı yani anlık olarak toplanması, iletişimi şimdiki zamanda gerçekleştirilen iletiye ait trafik verilerinin de anlık olarak toplanması anlamına gelmektedir. Veriler, ses ya da elektronik sinyallerin iletilmesi biçiminde maddi olmayan verilerdir. Verilerin toplanması işlemi, verilerin bir kopyasının üretilmesi şeklinde gerçekleştirilir. Trafik verileri, anlık olarak toplanırken, verilerin iletişim sürecindeki akışına engel olunmaz ve veri iletişim sürecinde ulaşması istenen yere ulaşır. Bu noktada, iletişim hizmetlerinin kamusal ya da özel kuruluşlarca sağlanması veya kamuya açık ya da kapalı bir kullanıcı grubuna veya özel kişilere sunulmuş olması arasında herhangi bir fark bulunmamaktadır. Başka bir ifadeyle, her türlü iletişime ait trafik verilerinin anlık olarak toplanmasına karar verilebilecektir[405].

Sözleşmenin 20. maddesine göre bilgisayar verisinin gerçek zamanlı toplanması koruma tedbiri her suç bakımından uygulanabilir niteliktedir. Bununla birlikte "usul hükümlerinin kapsamı"nın belirlendiği 14. maddede taraf devletlere bu koruma tedbirini belirli suçlarla sınırlı tutma hakkı verilmiştir. Bu hakkın sınırı ise; Sözleşmenin 21. maddesinde düzenlenen "içerikle ilgili bilgilere müdahale edilmesi" koruma tedbirinin uygulanabileceği suçlardan daha kısıtlı olmamasıdır.

Sözleşmenin 20. maddesiyle devletlere, hazır teknik imkânları elverdiği ölçüde hizmet sağlayıcılarının, trafik verilerinin anlık olarak toplanması işleminde soruşturma organlarıyla işbirliği yapma ve onlara yardımcı olma yükümlülüğünün yanı sıra verilen karar uyarınca bu toplama işlemini bizzat yapma yükümlülüğünü getirmelerini

[405] Serap Keskin, s. 173.

öngörmektedir. Bununla birlikte, taraf devletlerin söz konusu işlemi gerçekleştirebilecek ya da yardım isteyebilecek teknik imkânlara ve bilgiye sahip olmaları gerekmektedir[406].

Diğer taraftan, trafik verilerinin gerçek zamanlı olarak toplanması koruma tedbirinin ceza soruşturmasında etkin olabilmesi gizli yapılabilmesine bağlıdır. Bu bakımdan, Sözleşmede, trafik verilerinin anlık olarak toplanması işleminin gizli yapılması öngörülmektedir. Bu çerçevede, müdahalenin, iletişimin taraflarının algılayamayacakları bir şekilde yürütülmesi gerekmektedir. Ayrıca, işbirliği yapan ya da yardım eden hizmet sağlayıcılarının ve bilgisi bulunan çalışanlarının taraf devletlerin iç hukuklarınca belirlenecek bir süre boyunca sır saklama yükümlülüğü getirilmektedir[407].

2.2.2.8. İçerikle İlgili Bilgilere Müdahale Edilmesi

Sözleşmenin 21. maddesinde, taraf devletlerin yetkili makamlarının ulusal yasalarca belirlenecek ciddi nitelikteki suçlara ilişkin olarak bir bilgisayar sistemi üzerinden aktarılan ve ulusal sınırlar içinde özel iletişim sayılan içerik bilgilerini gerçek zamanlı olarak teknik imkânların kullanılması suretiyle toplanması ya da kaydedilmesi hususunda yetkili kılınması ve servis sağlayıcıların söz konusu içerik bilgilerinin toplanması ya da kaydedilmesi işlemleriyle ilgili olarak yetkili makamlarla iş birliği yapması ve onlara bu konuda yardımcı olmaları hususunda yasal düzenlemelerde bulunması öngörülmektedir. Aynı madde hükmüne göre yukarıda belirtilen hususlarla ilgili kendilerine yetki verilen servis sağlayıcılar söz konusu yetki hakkındaki esasları ve bilgileri gizli tutmakla yükümlüdürler.

Sözleşmede içerik bilgilerinin ne olduğu hususunda herhangi bir tanım bulunmamaktadır. Bununla birlikte madde metninde içerikle ilgili söz konusu bilgilerin bir bilgisayar sistemi üzerinden aktarılan ve taraf ülkenin ulusal sınırları içinde kalan özel iletişim sayılan bilgiler olduğundan bahsedilmektedir.

Bu bağlamda içerik bilgileri kavramı ile anlatılmak istenenin, trafik bilgileri dışında kalan, iletişimin içeriği, bu anlamda iletişimin anlamı ve niyeti ya da iletişimle taşınan mesaj veya bilgiden ibaret olduğu söylenebilir. İçerikle ilgili bilgilere müdahalede ise

[406] Serap Keskin, s. 175.

[407] Serap Keskin, s. 175.

iletişim sürecinde bulunan içeriğe anında ulaşılmaktadır. Bu özelliği nedeniyle iletişim özgürlüğü ve özel yaşamın dokunulmazlığı hakkında en ağır biçimde müdahale edici nitelikte bir koruma tedbiri bulunmaktadır. Bununla birlikte, bazı durumlarda içerik bilgilerine anında erişilmeden iletişimin niteliği keşfedilememektedir. Trafik bilgilerinin anında toplanması koruma tedbirinde olduğu gibi, bu tedbirde de iletişimin varış noktasına ulaşması engellenmemekte, bilgilerin bir kopyası üretilmektedir. Burada da yine kamusal ya da özel hizmet sağlayıcı veya kamuya açık ya da kapalı iletişim ayrımı bulunmamaktadır[408].

2.2.3. Avrupa Konseyi Siber Suç Sözleşmesinin İç Hukukumuzdaki Yeri

Avrupa Konseyi Siber Suç Sözleşmesinde, gerek taraf ülkelerin siber suçlarla mücadelede birbirlerine yakın bir uygulama benimsemeleri gerekse zaman içerisinde mevzuatlarda ve uygulamalarda oluşması muhtemel farklılıkların önüne geçilmesi amacıyla bilgisayar ve bilgisayar verileri ile ilgili ayrıntılı bir düzenleme yolunun benimsendiği görülmektedir. Diğer taraftan sözleşmede ayrıntılı bir teknik terim kullanımı ile ülkeler arasında terim birliği sağlanmasının hedeflendiği anlaşılmaktadır. Bununla birlikte zengin bir ayrıntıya (331 maddelik memoranduma) sahip olan Sözleşmenin taraf ülkelere birçok yükümlülük yüklemesi nedeniyle bazı devletlerin Sözleşmeyi imzalamakla birlikte kendi iç hukuklarında yürürlüğe sokmadıkları da görülmektedir[409].

2001 yılında imzaya açılan ve 2004 yılında yürürlüğe giren Avrupa Konseyi Siber Suç Sözleşmesi 10 Kasım 2010 tarihinde Türkiye tarafından da onaylanmıştır. Ancak Anayasa'nın 90/1 maddesine göre Türkiye Cumhuriyeti adına yabancı devletlerle ve milletlerarası kuruluşlarla yapılacak andlaşmaların onaylanması, Türkiye Büyük Millet Meclisi'nin onaylamayı bir kanunla uygun bulmasına bağlıdır. Bu nedenle TBMM tarafından bir kanunla uygunluğu sağlanmayan Sözleşme uzunca bir süre yürürlüğe girememiştir. Nihayet 22.04.2014 tarih ve 6533 sayılı "Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun" ile onaylanması uygun bulunan Sözleşme, Kanun'un 02.05.2014 tarihinde Resmi Gazete'de

[408] Serap Keskin, s. 175-176.

[409] Ünal, s. 46.

yayımlanmasıyla yürürlüğe girmiştir. Bu bakımdan Sözleşmenin Türkiye açısından bağlayıcılık durumu bulunmaktadır.

Bilişim teknolojilerinin işleyiş biçimi çoğu zaman bazı suç tiplerinin birden fazla ülkeyi ilgilendirmesi sunucunu doğurmaktadır. Bu nedenle Avrupa Konseyi Siber Suç Sözleşmesinde, özellikle bilişim suçlarının ulusal sınırları aştığı durumlarda, elektronik delillerin toplanması bakımından hızlı, etkin ve özel bir adli yardım öngörülmektedir[410].

Türkiye'nin, yakın bir zamana kadar bu sözleşmeye taraf olmaması söz konusu özel adli yardım taleplerine cevap verilmemesine neden olmaktaydı. Bu anlamda, Siber Suç Sözleşmesinin Türkiye açısından da yürürlüğe girmiş olması özellikle ulusal sınırları aşan bilişim suçlarının takibinde uluslararası işbirliğinin sağlanması bakımından büyük öneme sahiptir. Zira sınır aşan ve uluslararası işbirliğinden faydalanılamayan bilişim suçu soruşturmalarında, suç faillerine ulaşılamamakta, bu durum ise suçtan zarar gören kişilerin mağduriyetlerinin giderilememesi sonucunu doğurmaktadır.

2.3. ABD Hukuk Sisteminde Bilişim Sistemlerinde Arama ve Elkoyma

2.3.1. Genel Olarak

Tüm ceza soruşturma ve kovuşturmalarında, delillerin elde edilmesi sürecine ilişkin karşılaşılması muhtemel temel sorun, kolluk güçlerinin suça konu delille ilgili yaptığı arama ve elkoyma işlemi için yasal hakka sahip olup olmadığı hususudur[411]. ABD ceza yargılama sisteminde arama ve elkoyma, tutuklama tedbirinde olduğu gibi, kararı veren mahkemenin gösterdiği sınırlar içerisinde kolluk güçleri tarafından yerine getirilmektedir[412].

[410] Ünal, s. 41.

[411] Fred Galves and Christine Galves, "Ensuring the Admissibility of Electronic Forensic Evidence and Enhancing Its Probative Value at Trial", **Criminal Justice Magazine**, Vol. 19, No. 1, Spring 2004, http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust_cjmag_19_1_electronic.html (16 Aralık 2014).

[412] Tanrıkulu, s. 155.

ABD Anayasa'sındaki Dördüncü Değişiklik ve onun Amerikan içtihat hukuku tarafından yapılan yorumları arama ve elkoyma işlemine ilişkin sınırı belirlemektedir[413]. Buna göre, Amerikan Devrimi sırasında idari makamların verdiği arama ve elkoyma kararlarına tepki olarak ABD Anayasa'sına ilave edilen Dördüncü Değişiklik [414] soruşturma makamlarının arama kararı olmadan arama ve delillere elkoyma yetkisini sınırlandırmaktadır[415]. Zira makul olmayan arama ve elkoyma işlemlerine karşı kişilerin kendilerini, evlerini ve dokümanlarını koruma hakları bulunmaktadır[416].

Dördüncü Değişiklik, makul olmayan arama ve elkoymalara karşı vatandaşı korumaya yönelik iki hüküm içermektedir. Birincisi, bir arama yapmak için arama kararının gerekli olmasıdır (Johnson United States Davası, 1948). İkincisi ise, bazı durumlarda geçerli bir arama kararı olmaksızın arama yapılmaya imkân sağlanmasıdır (Illinois v. Rodriguez Davası, 1990). Dördüncü Değişiklik taslağının hazırlanmasından bu yana mahkemeler, arama kararının gerekliliği hususunda çok az istisnaya izin vermişlerdir. Bununla birlikte, her istisnai durumda, elde bulunan arama kararının söz konusu olaya uygulanabilir olmadığı veya delillerin kayıp olacağı ya da zarara uğrayacağı gibi gerekçelerin bulunması gerekmektedir (Parkhurstv. Trapp Davası, 1996)[417].

2.3.2. Bilişim Sistemlerinde Arama Kararına Bağlı Olarak Arama

Amerika Birleşik Devletleri, Avrupa Konseyi Siber Suç Sözleşmesi'ni 23.11.2001 tarihinde imzalamış, 29.09.2006 tarihinde onaylamış ve bu sözleşme 01.01.2007 tarihinde iç hukukta yürürlüğe girmiştir[418]. Buna karşın Amerikan hukukunda saklanan

---

[413] Galves and Galves, http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust_cjmag_19_1_electronic.html (16 Aralık 2014).

[414] Tanrıkulu, s. 155.

[415] H. Marshall Jarrett and Michael W. Bailie, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf (21 Aralık 2014), s. 1.

[416] Hasan Tahsin Arslan, "Anlaşma Çerçevesinde Bilişim Suçlarının İzlenmesi", **1. Polis Bilişim Sempozyumu,** Ankara, 21-22 Ekim 2003, s. 208.

[417] Robert Moore, "To View or Not to View: Examining the Plain View Doctrine and Digital Evidence", **American Journal of Criminal Justice**, Vol. 29, No. 1, (2004), s. 59-60.

[418] Member States of the Council of Europe, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (01 Ocak 2015).

bilgisayar verilerinin aranması ve bunlara elkonulmasına ilişkin Siber Suç Sözleşmesi'nin 19. maddesindeki düzenlemeye uygun herhangi bir iç hukuk düzenlemesinin yapılmadığı görülmektedir. Buna göre; A.B.D'de bilişim sistemlerinde arama yapılması ve buradan elde edilecek elektronik verilere elkonulmasına ilişkin özel bir düzenleme bulunmamaktadır. Bu ortamlarda yapılacak arama ve elkoyma işlemleri normal arama ve elkoyma kurallarına göre tesis edilmektedir.

Amerikan hukuk sisteminde Dördüncü Değişiklik uyarınca kolluğun şüpheliye ait bilişim sistemlerini aramadan ve incelemeye tabi tutmadan önce bu konuda hâkimden arama kararı alması gerekmektedir. Mahkemeler bilgisayarları adeta kişiye posta yoluyla gelen bir mektup veya koliye benzetmektedirler. Buna göre; böyle bir durumda nasıl ki kişinin veya yetkili merciin izni olmaksızın, haberleşme özgürlüğü ve özel hayatın gizliliği haklarını ihlal etmemek için ve kişilerin bilgisi olmaksızın bu eşyalar açılamıyorsa, bilişim sistemleri de sahip oldukları veriler nedeniyle kişilerin özel hayatlarının bir uzantısını teşkil ettiklerinden bunların da yetkisiz ve izinsiz biçimde, adli bir soruşturmanın konusu olsalar bile, arama ve elkoymaya konu edinmemeleri gerekir. Aksi bir davranış kişilerin temel hak ve özgürlüklerine saygı göstermemek anlamına gelir ve kişilerin de bu haklarına saygı gösterilmesini beklemeleri tabii bir beklentidir[419].

Bununla birlikte Dördüncü Değişiklik, makul olmayan arama ve elkoymalara karşı da koruma sağlamaktadır [420] . Buna göre; Dördüncü Değişiklik, soruşturmalarda uygulanacak arama ve elkoymalarda bulunması gereken şüphe derecesini makul şüphe olarak belirlemiştir. ABD'de soruşturmalarda makul şüphe olmaksızın arama ve elkoyma kararı verilemeyecektir. Makul şüphenin varlığı durumunda ise, diğer yasal ve anayasal şartların da bulunması ile bilişim sistemlerinde de arama ve elkoyma tedbiri uygulanabilir[421].

[419] Hüseyin Çeken, "Amerika Birleşik Devletlerinde İnternet Yolu İle İşlenen Suçlara İlişkin Düzenlemeler", **Askeri Adalet Dergisi,** Sayı. 114, (Mayıs 2002), s. 73-74.

[420] Moore, s. 59.

[421] Tanrıkulu, s. 162.

Bu bağlamda bir arama, ancak, bir kimsenin makul ve meşru olan özel hayat beklentisini ihlal etmiyorsa anayasal sınırlar içerisindedir. Bununla birlikte, bu aramada, iki somut sorunun karşılanması gerekmektedir. Bunlardan birincisi, kişinin davranışının özel hayat beklentisini sübjektif olarak yansıtıp yansıtmadığı, ikincisi ise, kişinin sübjektif özel hayat beklentisinin toplum tarafından "makul" olarak tanınmaya hazır olup olmadığı hususlarıdır[422].

Mahkemeler elektronik bilgilerin elde edilmesi sürecinde de makul özel hayat beklentisi kriterini aramaktadırlar. Bu kriter, bir kimsenin özel bilgisayarındaki dosyaları araştırmayı amaçlayan ve fakat arama yapmak için makul bir nedene sahip olmayan kolluk güçlerini kısıtlamaktadır. Nitekim, arama için makul bir nedenin olmaması, elde edilen delilin, bu kriter karşısında dışlanması sonucunu doğuracaktır[423].

Bir bilişim sisteminde saklanan bilgilerin bir kimsenin özel hayatının makul beklentisi sayılıp sayılmadığını belirlemek için, bilişim sistemlerini evrak çantası veya dosya dolabı gibi kapalı bir kap gibi değerlendirmek gerekmektedir. Bu bağlamda, Dördüncü Değişiklik, aynı durumdaki bir kapalı kabın açılması ve içeriğinin incelenmesinin yasaklanabilir olduğu durumlarda, genellikle, kolluk güçlerinin, bilişim sistemlerinde depolanmış bilgilere erişimini ve bunları görüntülemesini yasaklamaktadır[424].

Bu yüzden, kolluk güçlerinin, suç veya suç faaliyetlerine ilişkin teknolojik cihazlar ve elektronik verileri analiz etmeye yönelik arama yapmak için öncelikli olarak, makul bir nedene dayalı geçerli bir arama kararı almaları gerekmektedir. Aksi halde, kolluk güçleri, arama kararı olmaksızın arama yapılabileceğine ilişkin istisnai durumun olduğunu gösteren dikkatli ve geçerli bir saptamada bulunmak zorunda kalacaklardır[425].

ABD hukuk sisteminde arama kararının hem arama yapılacak yer hem de elkonulacak kişisel eşya bakımından açık ve belirgin olması gerekmektedir (Kyllo v. United States

[422] Jarrett and Bailie, s. 2.

[423] Galves and Galves, http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust_cjmag_19_1_electronic.html (16 Aralık 2014).

[424] Jarrett and Bailie, s. 3.

[425] Galves and Galves, http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust_cjmag_19_1_electronic.html (16 Aralık 2014).

Davası, 2001). Ancak, arama kararını uygulayacak olan polisin gerçekte sınırının ne olduğunun tespiti gerekmektedir. Klasik durumlarda, arama kararının uygulanmasına ilişkin kurallar, arama ve elkoyma sürecinin nispeten dar kapsamda uygulanmasını sağlamaya yöneliktir. Buna göre, arama kararında aranacak yerin ve ele geçirilecek eşyanın spesifik olarak belirtilmesi gerekmektedir. Elkoyma işlemi de arama kararında belirtilen delil ile sınırlı kalmalıdır (Maryland v. Garrison Davası, 1987). Nitekim bu kurallar, arama kararına istinaden gerçekleştirilen bir arama işleminin şüphelinin eşyalarını rastgele karıştırma şeklinde yapılacak bir genel aramaya dönüşmesini engellemeye yardımcı olur[426].

Bununla birlikte, elektronik delil için bu kuralları uygulamak bir bulmaca serisini kurmak gibidir. Elkoyma sürecinin ilk adımı soruşturma görevlilerinin şüphelinin bilgisayarını olay yeri dışında yapılacak arama (off site arama) için alması ile başlamaktadır. Bilgisayarın tamamına elkoyma pratik nedenlerden dolayı gereklidir ancak bu durumu geleneksel kurallara dayalı olarak haklı kılmak oldukça güçtür. Birçok durumda, bilgisayar donanımı, delilin kendisinden ziyade yalnızca delili depolayan bir aygıt konumundadır. Delil, polisin aradığı bir dosyadır ve bu sadece bilgisayar donanımı içerisinde birçok zararsız dosya arasında saklı bulunmaktadır (Davis v. Gracey Davası, 1997). Zaman içerisinde, geleneksel kurallara göre bir avuç dosyayı elde etmek için bilgisayar donanımına elkoymak geniş kapsamlı görünmüştür (United States v. Tamura Davası, 1982). Bu durum kabaca, bir suç delili için tüm bir eve ve onun içerisindekilere elkoymaya benzemektedir ki Dördüncü Değişiklik bu durumu yasaklamaktadır (Kremen v. United States Davası, 1957)[427].

Geleneksel kurallar, fiziksel delil için uygulanabilir olan ve fakat elektronik delil için uygulanabilir olmayan yüksek bir hassasiyet seviyesi gerektirmektedir. Bir kimsenin fiziken bir bankayı soyması durumunda polis bankadan çalınan bonoların bulunması için bu kişinin evinde birkaç saatlik bir arama kararı alabilir. Zira bu evin içindeki her şeyi bir laboratuvara götürüp burada arama yapma zorunluluğu bulunmamaktadır. Polisin arama kararında belirtilen bonolarla sınırlı arama yapmasını gerektiren bir kural,

[426] Orin S. Kerr, "Digital Evidence and the New Criminal Procedure", **Columbia Law Review**, Vol. 105, (January 2005), s. 299.

[427] Kerr, Digital Evidence and the New Criminal Procedure, s. 299-300.

böylesi bir ortamda mantıklı bir kuraldır. Buna karşın, bilgisayar aramalarının daha fazla zaman alması ve teknik uzmanlık gerektirmesi gibi önemli farklılıkları bulunmaktadır. Bu bakımdan, fiziksel delil elde edilmesinde işleyen geleneksel yaklaşım, elektronik delil elde edilmesi bakımından o kadar da iyi işlememektedir[428]. Bu durum, bilişim sistemleri üzerinde yapılan aramalar bakımından farklı uygulamaları gerekli kılmaktadır.

ABD Ceza Muhakemesi Kanunu'nun 41/b maddesi arama ve elkoyma tedbirinin talep ve karar makamını belirlemiştir. Buna göre; arama ve elkoyma kararları federal ceza infaz görevlileri ve savcı tarafından istenebilecektir. Arama ve elkoyma kararlarını vermeye yetkili kişi ise bir il ve ilçe mülki sınırları içerisindeki yetkili hâkimlerdir. Yetkili hâkimlerin haklı bir nedenden dolayı bu kararı vermeye uygun olmaması durumunda bölgede bu konuda yetkilendirilmiş başka bir hâkim, arama ve elkoyma konusunda karar vermeye yetkilidir. İl veya ilçe sınırları dışında bulunan kişi veya eşya için de bir ilçe veya il sınırındaki yetkili hâkim, belirli şartların bulunması halinde arama ve elkoyma kararı vermeye yetkilidir. Soruşturma konusu olayın terör ile bağlantılı bir suç olması durumunda ise bir ilçe veya il hâkimi, bu yetki sınırları dışındaki yerlerde bulunan kişi veya eşyalar için de arama veya elkoyma kararı verebilecektir[429].

ABD uygulamasında bilişim sistemlerinde yapılacak bir aramanın ABD Ceza Muhakemesi Kanunu'nun 41/e-2-i maddesi uyarınca sulh hâkimi tarafından verilen bir arama kararına istinaden ve en geç ondört gün içerisinde yerine getirilmesi gerekmektedir. Bu hükmün 2009 yılından önceki hali (m. 41/e-2-a-i) mahkemeler arasında söz konusu sınırlayıcı sürenin sadece fiziksel delil için mi yoksa elektronik medya üzerinde yapılacak inceleme/analiz sürecini de kapsayıp kapsamadığı hususunda fikir ayrılıklarına neden olmaktaydı. Söz konusu değişiklik sonrasında ondört günlük sürenin arama ve elkoyma işleminin ilk uygulandığı süreç için geçerli olduğu, bilişim

[428] Kerr, Digital Evidence and the New Criminal Procedure, s. 300.

[429] Tanrıkulu, s. 165-166.

sistemi ve donanımları ile bunlardan alınan imaj üzerinde yapılacak sonraki inceleme/analiz işlemi için ise bu sürenin söz konusu olmadığı netlik kazanmıştır[430].

Bununla birlikte ABD Ceza Muhakemesi Kanunu'nun 41/e-2-i maddesinde bilişim sistemleri ve donanımları ile bunlardan alınan imaj üzerindeki inceleme/analiz faaliyetine ilişkin herhangi bir süre sınırlaması getirmemesi Kanunun sulh hâkimlerinin arama kararı vermeleri, kolluk güçlerinin arama emrini yerine getirmeleri ve hâkimlerin arama sonucunda elde edilen delilin kabul edilebilir olup olmadığını belirlemeleri hususlarında rehber olma özelliğini sınırlamıştır. Bu belirsizlik, elektronik medyada yapılan inceleme/analiz işleminin zamana bağlı olup olmadığı hususunda da mahkemeler arasında uyum eksikliği sonucunu doğurmuştur[431].

Nitekim United States v. Mutschelknaus davasında hâkim tarafından verilen arama ve elkoyma kararı sonucunda kolluk güçlerinin on gün içerisinde klasik arama ve elkoyma işlemini yerine getirmelerine karşın bilgisayar donanımında yapılan inceleme/analiz işlemini altmış günlük bir süre zarfında sonuçlandırmaları üzerine mahkeme 41. maddede herhangi bir süre kısıtlaması olmamasına rağmen altmış günlük bir gecikmeyi anayasal açıdan makul olup olmadığı hususunu incelemiş ve kolluk güçlerinin bu inceleme/analiz işlemini altmış gün boyunca sürdürmesini gerektirecek makul bir neden olmaması nedeniyle elde edilen verilerin delil olarak kullanılamayacağına karar vermiştir (United States v. Mutschelknaus Davası, 2010)[432].

2.3.3. Bilişim Sistemlerinde Arama Kararı Olmaksızın Arama

2.3.3.1. Genel Olarak

Zaman ve koşullar izin veriyorsa, kolluk görevlilerinin, bir istisnanın geçerli olup olmadığı hususunda kişisel hukuki değerlendirmelerine dayanmak zorunda kalmamaları adına başvurmaları gereken en ihtiyatlı yol arama kararı almalarıdır. Ancak, kolluk, makul özel hayat beklentisinin var olduğu bir durumda, arama kararı olmaksızın arama

[430] Kaitlyn R. O'Leary, "What the Founders Did See Coming: The Fourtyh Amendment, Digital Evidence, and the Plain View Doctrine", **Suffolk University Law Review**, Vol. 46, (2013), s. 212.

[431] O'Leary, s. 218.

[432] O'Leary, s. 218-219.

yapmaya karar vermişse, birkaç istisnadan birine başvurmalı veya delilleri yok etmelidir[433].

2.3.3.2. Rıza

Kolluğun arama kararı olmaksızın arama yapabilmesine ilişkin istisnalardan en belirgin olanı kişinin rızasının bulunması durumudur. Kolluk bu durumda arama kararı veya makul şüphe sebebi olmadan arama yapabilir. Eğer elektronik bilgiler üzerinde yetkili olan kişinin arama yapılması hususunda gönüllü bir rızası bulunmaktaysa, böyle bir durumda, yalnızca sözlü rıza beyanı ile yetinmek yerine açıkça rızanın kapsamını da belirten yazılı bir izin formunun kullanılması, şüphesiz daha iyi bir uygulama olarak kabul edilecektir. Burada rıza yetkisinin kontrol edilmesi de önemlidir. Özellikle bir aile üyesinin başka bir aile üyesinin elektronik bilgileri üzerinde yapılacak aramalarda rıza beyanında bulunması durumunda bu husus daha da önem arz etmektedir. Aynı durum, bir işveren veya sistem yöneticisinin bir çalışanın bilgisayar kayıtları üzerinde yapılacak aramada gösterdiği rıza beyanında da söz konusu olacaktır[434].

Mahkemeler çoğu zaman eşlerin verdiği rıza üzerine yapılan aramaları geçerli kabul etmektedir. Buna karşın rızanın geçerli olmadığı durumlar da söz konusu olabilmektedir. *"United States v. Smith"* davasında, Smith isimli birisi Ushman ve onun iki kızı ile birlikte yaşamaktadır. Smith hakkında iddia edilen çocuk tacizi olayında, Ushman, evdeki ebeveyn odasında bulunan Smith'e ait bilgisayarda yapılan aramaya rıza göstermiştir. Ushman bu bilgisayarı nadiren kullanıyor olmasına rağmen yerel mahkeme onun Smith'e ait bilgisayarda yapılan arama için verdiği rızayı geçerli saymıştır. Mahkeme gerekçesinde, Ushman'ın ebeveyn odasına girişinin yasak olmaması ve Smith'in bilgisayarın şifre ile korumaması nedeniyle Ushman'ın rıza yetkisinin bulunduğunu belirtmiştir (United States v. Smith Davası, 1998)[435].

---

[433] Galves and Galves, http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust_cjmag_19_1_electronic.html (16 Aralık 2014).

[434] Galves and Galves, http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust_cjmag_19_1_electronic.html (16 Aralık 2014).

[435] Jarrett and Bailie, s. 22-23.

Buna karşın, bir eşin bilişim sistemine erişim yetkisinin bulunmadığı hallerde vermiş olduğu rıza üzerine yapılan aramalarda mahkemeler genellikle bu rızanın geçerli olmadığına karar vermektedir. Nitekim Trulock v. Freeh davasında, bir eşin kolluğa bilişim sistemindeki dosyalara giriş için gerekli şifreyi bilmediğini belirttiği bir olayda vermiş olduğu rıza üzerine yapılan aramada, mahkeme, eşin beraber yaşadığı kişinin bilgisayar dosyaları üzerinde yapılan arama için vermiş olduğu rızayı geçersiz kabul etmiştir (Trulock v. Freeh, 2001)[436].

Diğer taraftan ABD hukukunda ebeveynin on sekiz yaşından küçük çocuklarının bilişim sistemleri üzerinde yapılan aramalar bakımından göstermiş oldukları rıza geçerli kabul edilmektedir. Çocukların on sekiz yaşından büyük olmaları durumunda gösterilen rızanın ise geçerli olup olmayacağı hususu somut olaya göre değişmektedir. Buna göre, evin ortak alanlarında yapılan aramada failin yaşına bakılmaksızın ebeveynin rıza hakkı tanınmaktadır. Nitekim Mahkeme, bir annenin, oğlunun bodrumda muhafaza ettiği bilgisayar ve dosyaları üzerinde yapılan aramada gösterdiği rızayı kabul etmiştir (United States v. Lavin Davası, 1992). Buna karşın, kolluğun, yetişkin çocuğun odasında veya diğer özel alanlarında arama yapmak istemesi durumunda, kolluk ebeveynin rıza yetkisinin olduğunu varsayarak arama yapamaz. Mahkemeler, farklı yaklaşım tarzlarını benimsemekle birlikte genellikle üç faktörün olup olmadığına özellikle bakmaktadırlar. Bunlar, şüphelinin yaşı, kira ödeyip ödemediği ve ebeveyninin kendi bilgisayarına erişimini yasaklayıp yasaklamadığı hususlarıdır. Şüpheli yetişkinse, kira ödemekteyse ve/veya ebeveyninin bilgisayarına erişimini yasaklamışsa -*"United States v. Whitfield"* davasında olduğu gibi[437]- mahkemeler genellikle ebeveynin rıza hakkının olmadığına karar vermektedirler[438].

ABD uygulamasında, kolluğun, bilgisayar tamircilerinin bilgisayarda yaptığı özel aramalar aracılığıyla ortaya çıkan bilgileri, mahkemeden alınacak tam bir arama kararına temel teşkil etmesi için kullandıkları çokça görülmektedir. Ancak, kolluğun bazı olaylarda, tamircinin rızasına dayanarak, arama kararına esas olacak şekilde olan

[436] Jarrett and Bailie, s. 22.

[437] Bkz. United States v. Whitfield, 939 F.2d 1071, 1075 (D.C. Cir. 1991).

[438] Jarrett and Bailie, s. 23-24.

ilk özel arama kapsamını aşacak biçimde uygulamayı genişlettikleri görülmüştür. Yerel mahkemeler, bilgisayar tamircilerinin aramalarda rıza yetkisinin bulunup bulunmadığı hususunda ikiye bölünmüş durumdadırlar. Yerel bir mahkeme tamircilerin bilgisayara erişim yetkileri olduğundan, tamir için getirilen bilgisayarların aranması hususunda "gerçek ve belirgin" bir rıza yetkilerinin bulunduğuna karar vermiştir (United States v. Anderson Davası, 2007). Buna karşın, bir başka yerel mahkeme ise, sanık, sabit diski tamirciye, arama yapılan dosyalarla ilgisi olmayan ve yalnızca sınırlı amaç ve süre için verdiğinden, tamircilerin harici bellekte arama yapma konusunda "gerçek ve belirgin" bir yetkilerinin bulunmadığına karar vermiştir (United States v. Barth, 1998)[439].

2.3.3.3. Zaruret Hali

Bilişim sistemlerinde arama kararı olmaksızın arama yapılabilmesine ilişkin bir başka istisna ise zaruret halidir. Eğer derhal yapılacak bir aramanın, fiziksel bir zararı, bir delilin yok olmasını veya kolluğun yasal çerçevedeki çalışmalarını engelleyecek başka bir sonucu önlemek için gerekli olduğu görülürse, kolluk arama kararı olmadan da arama ve/veya elkoyma işlemini gerçekleştirebilir[440].

Başlangıçta var olan duruma yeni bilgilerin eklenmesi sonucu ortaya çıkan yeni durumda zaruret halinin varlığından söz edilebilecektir. Örneğin, kolluğun, şüphelinin aracında arama yapmak için herhangi bir sebep olmaması nedeniyle araçta arama talep etmeksizin arama kararını sadece evde yapılacak arama ile sınırlı tuttuğu bir durumda, evde gerçekleştirilen arama işlemi sırasında güvenilir bir tanığın şüphelinin suç unsuru bulunabilecek CD ve DVD'leri aracının bagajında sakladığını ihbar etmesi durumunda[441] delillerin derhal elde edilememesi halinde şüphelinin bu delilleri yok etmesi söz konusu olacaksa zaruret halinden söz edilebilecektir.

Nitekim sanığın, bilgisayarındaki dosyaları sildiğini gören kolluğun bilgisayara derhal elkoyduğu bir olayda yerel mahkeme vermiş olduğu kararında, sanığın eylemlerinin zaruret durumu koşullarını oluşturması nedeniyle kolluğun herhangi bir arama kararı

[439] Jarrett and Bailie, s. 24-25.

[440] Galves and Galves, http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust_cjmag_19_1_electronic.html (16 Aralık 2014).

[441] Jacqueline J. DeGaine, "Digital Evidence", **The Army Lawyer**, (May 2013), s. 12.

olmaksızın bilgisayara elkoyabileceğine hükmetmiştir (United States v. David Davası, 1991)[442].

Bununla birlikte, zaruret halinde de, söz konusu olan aciliyet ve zaruret alanının ötesinde bir arama yapılamaz. Bu bağlamda, kolluk, imha edilmek üzere olan bir dizüstü bilgisayara derhal elkoyabilecek ve fakat güvenliği sağlanan dizüstü bilgisayar üzerinde detaylı bir arama yapabilmek için yine de arama kararı alması gerekecektir[443].

2.3.3.4. Yakalama Sonrası Arama Yapma Doktrini

Usule uygun bir yakalama işlemi uyarınca kolluk, herhangi bir arama kararı olmaksızın, yakalanan kişi üzerinde tam bir arama ve bu kişiyi çevreleyen alanda da daha sınırlı ölçüde bir arama gerçekleştirebilir (United States v. Robinson Davası, 1973)[444]. Bu durum özellikle, şüphelinin çağrı cihazları, taşınır bellekler, cep telefonları, kişisel dijital cihazlar ya da dizüstü bilgisayar taşıdığı durumlarda daha da büyük öneme sahip olabilir[445].

Çağrı cihazlarıyla başlayan ve sonraları cep telefonları ve kişisel dijital cihazlara kadar uzanan bu tip aramalar ile ilgili olarak da mahkemeler genellikle yakalama sonrası arama yapma doktrininin taşınabilir elektronik cihazlar için geçerli olduğuna karar vermişlerdir. İlk önceleri, yakalama sonrasında yapılan birçok çağrı cihazı araması işlemini onaylanmıştır (Bkz. United States v. Brookes Davası, 2005; Yu v. United States Davası, 1997; United States v. Thomas Davası, 1997; United States v. Reyes Davası, 1996; United States v. Lynch, Davası, 1995; United States v. Chan Davası, 1993). Daha yakın zamanlarda ise birçok mahkeme, yakalama sonrası gerçekleşen cep telefonu aramalarını da onaylamıştır (Bkz. United States v. Finley Davası, 2007; United States v. Valdez Davası, 2008; United States v. Curry Davası, 2008; United States v. Mercado-Nava Davası, 2007; United States v. Dennis Davası, 2007; United States v.

[442] Jarrett and Bailie, s. 28.

[443] Galves and Galves, http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust_cjmag_19_1_electronic.html (16 Aralık 2014).

[444] Jarrett and Bailie, s. 31.

[445] Galves and Galves, http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust_cjmag_19_1_electronic.html (16 Aralık 2014).

Mendoza, 2005; United States v. Brookes Davası, 2005; United States v. Cote Davası, 2005). Ayrıca bir temyiz mahkemesi, bu kapsamda yapılan bir elektronik adres defterinin aranmasını da onaylamıştır (Bkz. United States v. Goree Davası, 2002)[446].

2.3.3.5. Hemen Görünür Olma Doktrini (Plain View Doctrine)

Dördüncü Değişiklik, makul olmayan arama ve elkoyma işlemlerini yasaklamaktadır. Buna göre, kolluk, arama kararı alabilmek için makul bir neden göstermek zorundadır. Bu karar, kapsam itibariyle dar, nitelik itibariyle ise özeldir. Bu arama kararı, sadece kolluğun arayacağı delilin türü itibariyle sınırlı olmayıp kolluğun arama yapacağı alan itibariyle de kısıtlıdır. Ancak, kolluk yapmış olduğu arama sırasında başka bir suça ait delille karşılaşması durumunda hemen görünür olma doktrini (plain view doctrine) uyarınca bu delile de elkoyabilme imkânına sahiptir[447].

Bu bağlamda hemen görünür olma doktrini, kamu güvenliğinin korunması ile devlet gücünün kötüye kullanılmasının önlenmesi arasındaki dengeyi sağlayan hukuki bir kuraldır. Buna göre, suç unsuru eşyanın elkonulabilir olma niteliği belirgin ise hemen görünür olma doktrini, polise geçerli bir arama işlemi sırasında tespit ettiği sair delile elkoyma yetkisini vermektedir[448].

ABD yüksek mahkemesi üç önemli kararında hemen görünür olma doktrinin varlığını ele almıştır. Bunlar; Coolidge v. New Hampshire Davası (1971), Arizonay v. Hicks Davası (1987) ve Horton v. California Davası (1990) kararlarıdır. Bu kararlar, yasal çerçevede yapılan bir arama sırasında, bu aramada bulunan görevlinin başka bir suça ilişkin delil olabilecek bir içeriğin farkına varması durumunun, bu delillere elkoyması bakımından makul bir neden olarak kabul edilebileceğini saptamaktadır[449].

Mahkemeler başlangıçta fiziksel delillerin elde edilmesinde uyguladıkları hemen görünür olma doktrinini zamanla dijital veriler bakımından da uygulamaya

[446] Jarrett and Bailie, s. 32.

[447] Andrew Vahid Moshirnia, "Separating Hard Fact From Hard Drive: A Solution for Plain View Doctrine in the Digital Domain", **Harvard Journal of Law & Technology**, Vol. 23, No. 2, (Spring 2010), s. 611.

[448] Orin S. Kerr, "Searches and Seizures in a Digital World", **Harvard Law Review**, Vol. 119, (2005), s. 568.

[449] Moore, s. 61.

başlamışlardır[450]. Bu bakımdan hemen görünür olma doktrininin uygulandığı pek çok olayda, başka suçların kanıtlanmasını sağlayan elektronik delile rastlanmaktadır. Çocuk pornografisi niteliğindeki görseller, hemen görünür olma doktrini kapsamında bilişim sistemlerinde yapılan aramalar sırasında elde edilen en yaygın elektronik delil türünü teşkil etmektedir[451].

Bilişim sistemlerinde elde edilecek elektronik delil bakımından hemen görünür olma doktrini iki şekilde ortaya çıkmaktadır. Birinci durum, kolluğun hukuka uygun bir arama işlemi sırasında açık vaziyette bulunan bir bilgisayar ekranı üzerinde unutulmuş suç delilini görmesi durumudur. İkinci durum ise, kolluğun bilişim sistemi üzerinde bir suç delili elde etmek amacıyla yaptığı hukuka uygun bir arama sırasında farklı bir suça ilişkin delil bulması durumudur[452].

Belirtmek gerekir ki, kolluk hemen görünür olma doktrini uyarınca yapmış olduğu bilişim sistemleri üzerindeki aramada tüm dosyaları inceleyemeyecek, başka şekilde açmalarına imkân tanınmayan içerikleri sırf bu doktrine dayanarak açamayacaktır. Bu doktrinden yararlanmak için arama yapılan dosyada açıkça suç içeriği barındırdığını belli eden isimlendirmeler gerekmektedir[453].

2.4. İngiltere Hukuk Sisteminde Bilişim Sistemlerinde Arama ve Elkoyma

İngiltere ortak hukuk sistemini (common law) benimsemiş ülkelerdendir. Ortak hukuk sistemini benimseyen ülkelerin en belirgin özelliği hâkimlerin emsal kararlarının en önemli hukuk kaynağı olmayı sürdürmesidir. Bu durum hukuklarını yazılı hale getirmeleri sonucunda kanunların tek hukuk kaynağı olarak görülen Kıta Avrupa'sı hukuk sistemini (civil law) benimseyen ülkelerin tam tersidir. Bununla birlikte İngiliz

[450] "Hemen görünür olma (plain view) istisnası dijital aramalar bakımından da uygulanabilir." (United States v. Williams Davası, 592 F.3d 511, 514, 4th Cir. 2010), Bkz. Moshirnia, s. 610, dp. 1.

[451] Robinton, s. 333.

[452] DeGaine, s. 11.

[453] Tanrıkulu, s. 175.

hukukunda birçok alanın yazılı hale getirildiği ya da açık yasal düzenlemelerle içtihat hukukunun geçersiz sayıldığı da görülmektedir[454].

Bu anlamda, İngiltere'de bilişim sistemlerinde arama ve elkoyma tedbirini düzenleyen üç ayrı kanun mevcuttur. Bunlar, genel arama ve elkoymayla ilgili düzenlemeyi içeren 1984 tarihli Polis ve Suç Delili Kanunu (Police and Criminal Evidence Act-PACE), 1990 tarihli Bilgisayarın Kötüye Kullanılması Kanunu (Cumputer Misuse Act-CMA) ve Soruşturma Yetkileri Düzenleme Kanunu (Regulation of Investigatory Powers Act-RIPA)'dur[455].

İngiltere'de kolluk bir yerde arama yapmak ve burada bulduğu delillere elkoymak için yasal bir yetkiye sahip olmalıdır. Bu bağlamda, Polis ve Suç Delili Kanunu (PACE) arama ve elkoyma yetkisini düzenleyen bir yasal çerçeve ortaya koymaktadır[456]. Buna göre PACE on bir bölümden oluşmakta olup polisin arama ve elkoyma yetkisi birinci ve ikinci bölümde düzenlenmiştir. PACE'nin birinci bölümünde yer alan 1. maddesinde kolluğun kişi ve araçları durdurma ve arama yapma yetkisi düzenlenmiştir[457]. Aynı bölümde yer alan 4. maddesinde ise polisin yol kontrolü yapma yetkisi düzenlenmiştir[458].

PACE'nin ikinci bölümünde yer alan 8. maddesi binaya giriş ve burada arama yapma yetkisini düzenlemektedir. Buna göre arama kararı verme yetkisi sulh hâkimine aittir[459]. Polisin arama kararı talebinde bulunurken hukuka aykırı davranışın ne olduğunu da içeren ve bir arama yapmayı gerektiren makul nedenleri göstermesi gerekmektedir. Ayrıca, Amerika Birleşik Devletleri'nde olduğu gibi, aramanın ev ve eklentileri, eşyalar ve kişiler yönünden kapsamı mümkün olduğunca belirgin biçimde belirtilmelidir[460].

---

[454] Rand Europe & Lawfort, s. 261.

[455] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 293.

[456] Casey, Digital Evidence and Computer Crime, s. 77.

[457] http://www.legislation.gov.uk/ukpga/1984/60/section/1 (03 Ocak 2015).

[458] http://www.legislation.gov.uk/ukpga/1984/60/section/4 (03 Ocak 2015).

[459] http://www.legislation.gov.uk/ukpga/1984/60/section/8 (03 Ocak 2015).

[460] Casey, Digital Evidence and Computer Crime, s. 77.

PACE uyarınca arama yapılabilmesi için makul nedenlerin varlığının yanında aramaya konu eylemin, hakkında iddianame tanzim edilerek dava açılabilen bir suçu oluşturması gerekir. Bina ve eklentilerinde yapılacak aramalarda önemli bir hukuki yararın varlığı da söz konusu olmalıdır. Ayrıca, arama sonucu elde edilmesi muhtemel eşyanın delil olma olasılığı veya delili barındırma ihtimalinin yüksek olması gerekir. Diğer taraftan arama yapılacak yerin yasal ayrıcalığa sahip bir yer olmaması veya yasal olarak arama yapılacak yere ya da elkonulacak eşya ile ilgili olarak herhangi bir imtiyaz tanınmamış olması yahut özel bir usule tabi olmaması gerekmektedir[461].

PACE'nin ikinci bölümünde yer alan 19. maddesinde binada yapılacak elkoyma işlemine ilişkin genel hükümlere yer verilmiştir. Bu bağlamda, maddenin 2. ve 3. fıkralarına göre; bina içerisinde bulunan herhangi bir eşyanın bir suçun işlenmesi sonucunda elde edildiği veya bir soruşturmanın ya da başka herhangi bir suçun delili olduğu hususunda ve bu nitelikteki eşyanın gizlenmesi, kaybolması, zarar görmesi, değiştirilmesi veya yok edilmesinin önlenmesi için gerekli olduğu yönünde makul nedenlerin varlığı halinde kolluk bu eşyaya elkoyabilecektir[462].

İngiltere, Avrupa Konseyi Siber Suç Sözleşmesi'ni 23.11.2001 tarihinde imzalamış, 25.05.2011 tarihinde onaylamış ve bu sözleşme 01.09.2011 tarihinde iç hukukta yürürlüğe girmiştir[463]. Buna göre İngiltere Hukukunda saklanan bilgisayar verilerinin aranması ve bunlara elkonulmasına ilişkin Siber Suç Sözleşmesi'nin 19. maddesindeki düzenleye uygun bir iç hukuk düzenlemesinin varlığı dikkat çekmektedir.

Bu bağlamda PACE'de elektronik delilin toplanmasının özel olarak düzenlendiği görülmektedir[464]. PACE'nin 19/4 maddesinde elektronik ortamda saklanan bilgiden özellikle bahsedilmiştir. PACE'nin 20. maddesinde ise kolluğun elektronik delili toplama yetkisi düzenlenmiştir[465].

---

[461] Tanrıkulu, s. 203.

[462] http://www.legislation.gov.uk/ukpga/1984/60/section/19 (03 Ocak 2015).

[463] Member States of the Council of Europe, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (01 Ocak 2015).

[464] Insa, s. 287.

[465] Casey, Digital Evidence and Computer Crime, s. 77-78.

PACE'nin 19/4 maddesinde kolluğun soruşturma konusu veya diğer bir suçla ilgili delile veya suçun işlenmesi suretiyle elde edilen elektronik veriye; gizlenmesi, kaybolması, zarar görmesi, değiştirilmesi veya yok edilmesinin önlenmesi için gerekli olduğu yönünde makul nedenlerin varlığı halinde elkonulabilecektir. Buradaki elkoyma işlemi, elektronik ortamda saklanan ve bina içerisinde ulaşılan veri veya bilgi üzerinde gerçekleştirilebilecektir [466] . Bu maddeye göre söz konusu veri veya bilginin görüntülenebilir veya okunabilir olması gerekmektedir. Bu anlamda veri veya bilginin o an için görünebilir veya okunabilir olmasa da uygun araçlarla görüntülenebilir veya okunabilir olması da elkoyma işleminin yerine getirilebilmesi için yeterlidir[467].

PACE'nin 20. maddesinde ise elkoyma yetkisinin bilgisayarda saklanan elektronik veri bakımından uygulanması düzenlenmiştir. Bu madde, bilgisayar kaynaklı elektronik verilerin elde edilmesi yetkisinin genişletilmiş bir halini ihtiva etmektedir. Buna göre, polis, kanunun verdiği yetkiye dayanarak yalnızca bilgisayardaki verileri değil, bilgisayara bağlanabilen birimlerin de araştırılmasını isteyebilir[468].

Belirtmek gerekir ki; İngiltere'de kolluk usulüne uygun bir arama kararına dayalı olarak bir yerde arama yapması durumunda PACE'nin 19. ve 20. maddelerinde belirtilen makul nedenlerin varlığı halinde arama kararı kapsamında kalan eşyaya elkoyabilecektir. Bunun için hâkim tarafından usulüne uygun olarak verilen arama kararının dışında herhangi bir elkoyma kararına ihtiyaç bulunmamaktadır.

İngiltere'de bilişim sistemlerinde arama ve elkoyma tedbiri ile ilgili diğer bir kanun olan Bilgisayarın Kötüye Kullanılması Kanunu (CMA), bilişim sistemlerinin kötüye kullanılmasına ilişkin olaylarda İngiltere mevzuatının temel parçasını oluşturmaya devam etmektedir. Bu kanun, bilgisayar korsanlığı ve kasıtlı olarak virüs yayılması gibi suçları içermektedir ve bilişim sistemlerine yetkisiz erişim ve bu sistemlerde değişiklik yapılmasını önlemek, bilgisayar kullanılarak suç örgütlerine yardımcı olan suç unsuru

[466] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 294.

[467] Tanrıkulu, s. 201.

[468] Ünal, s. 49.

eylemlerin önünü almak ve bilgisayarlarda saklanan verilere erişimi engellemek veya zayıflatmak için düzenlenmiştir[469].

CMA'nın 14. maddesinde kanun kapsamındaki bilişim suçları ile ilgili arama kararı düzenlenmekteydi. Ancak, söz konusu madde, 2006 yılında Polis ve Adalet Kanunu (Police and Justice Act)'nun 15. cetvelinin 4. bölümü ile yürürlükten kaldırılmıştır[470].

İngiltere'de bilişim sistemlerinde arama ve elkoyma tedbiri ile ilgili bir diğer kanun olan Soruşturma Yetkilerinin Düzenlenmesi Kanunu (RIPA) soruşturma organlarına yargı kararı alma ihtiyacı duymaksızın son derece geniş yetkiler bahşetmektedir. Bu kanun Avrupa İnsan Hakları Sözleşmesiyle uyumlu olmasına karşın* soruşturma organlarına vermiş olduğu bu geniş yetkiler nedeniyle bazı sorunlara kapı aralamaktadır[471].

Bununla birlikte Kanun kapsamında hâkim kararı ile verilen yetkiler de önemli bir yer teşkil etmektedir. Bu bağlamda Kanun'un konumuzla ilgili noktası, ikinci kısımda yer alan trafik verilerinin gerçek zamanlı olarak toplanması ile üçüncü kısımda yer alan ve 49 ila 56. maddeler arasında düzenlenen şifre ile koruma altına alınan bilgilerin ifşası ve ortaya konulması için bildirimde bulunma zorunluluğuna ilişkin düzenlemelerdir. Buna göre; makul nedenlerin varlığı halinde verilerin araştırılması amacıyla hâkim tarafından verilen "uygun izin" ile bir kimsenin mülkiyeti altındaki şifreli olan ve bu şifre nedeniyle ulaşılması, o an erişilmesi veya anlaşılır biçime dönüştürülmesi mümkün olmayan elektronik verilerin araştırılması amacıyla uygun izne sahip kişi korunan

[469] Rand Europe & Lawfort, s. 262.

[470] http://www.legislation.gov.uk/uksi/2008/2503/article/2/made (03 Ocak 2015).

* RIPA'nın, bireylerin hak ve hürriyetlerinin korunması bakımından öngörmüş olduğu en büyük teminat hiç şüphesiz 4. Bölüm içerisinde düzenlenen ve bağımsız ve adli bir mahkeme niteliği taşıyan ve bu kanun kapsamındaki işlemlerin denetlenmesi ve tedbirin hukuka aykırı icra edildiği yönündeki şikâyetler hakkında karar verme yetkisine sahip olan, Soruşturma Güçleri Mahkemesi'dir (Inevstigatory Powers Tribunal-IPT-). Soruşturma Güçleri Mahkemesi'nin ihdas edilmesine ilişkin hükümlerin ve genel olarak kanunun, bireylerin hak ve hürriyetlerini korumayı amaç edinen güvence sistemi, 2010 tarihli Kennedy-Birleşik Krallık Kararı'nda, gizli tedbirler bakımından öngörülen kanuni şartlar, kötüye kullanılmaya karşı öngörülen tedbirler ve nihayet denetime ilişkin İletişim Komisyonu ve Soruşturma Güçleri Mahkemesi'nin adli yargılama (denetim) sistemi bir bütün halinde değerlendirildiğinde RIPA'nın, bireylerin temel hak ve hürriyetleri bakımından orantılı bir müdahale niteliği taşıdığını onaylanmıştır. Fatih Birtek, "İstihbarat Amacıyla İletişim Özgürlüğüne Müdahale Edilmesi Ve Müdahaleden Elde Edilen Materyallerin Delil Olarak Kabul Edilebilirliği", (t.y.), http://www.turkhukuksitesi.com/makale_1284.htm (05 Ocak 2015).

[471] Emanuel Gross, "The Struggle of a Democracy Against the Terror of Suicide Bombers: Ideological and Legal Aspects", **Wisconsin International Law Journal**, Vol. 22, No. 3. (Fall 2004), s. 671.

bilgiye sahip olan kişiye bu korunan bilgiyi açabilecek şifreyi açıklama yükümlülüğünü içeren bir bildirimde bulunur. Şifrenin açıklanması sadece uygun izne sahip olan veya uygun izin kararında belirtilen kişilere yapılır[472].

RIPA'nın 50. maddesinde bu bildirimle ilgili olarak elde edilen şifrenin korunan bilgiyle ilgili olup olmadığının tespiti ve bunun sonuçları üzerinde durulurken tedbirin ulusal güvenlik, suçun belirlenmesi, önlenmesi ve İngiltere'nin ekonomik çıkarlarının korunmasının amaçlandığı görülmektedir. Bu bağlamda RIPA'nın 49 ila 56. maddeleri arasında düzenlenen şifrelenmiş elektronik verinin elde edilmesine ilişkin bu tedbirde maliyetinden, teminatına ve kimler tarafından uygulanacağına kadar birçok konuya değinilmiştir. Bu bakımdan PACE'de düzenlenen bilgisayarlara yönelik tedbirlerle karşılaştırıldığında RIPA'da düzenlenen söz konusu tedbirin daha özel bir düzenleme olduğu kolaylıkla anlaşılabilir. Bu özel düzenleme şifrelerin çözümüyle ilgili olması nedeniyle elektronik yapıdaki iletişim araçlarında da uygulanabilmektedir[473].

RIPA'ya genel olarak bakıldığında maddelerde bilgisayar, bilişim sistemi, veri saklayan araç gibi hiçbir tanımlamanın yapılmaması ve söz konusu kavramlara yer verilmemesi dikkat çekmektedir. Buna göre RIPA'da, doğru bir yaklaşım tarzıyla, veri üzerine odaklanılmış ve verinin bulunduğu yer sınırlayıcı bir biçimde düzenlenmemiştir. Nitekim bilişim sistemlerinde veri aramayı, klasik arama tedbirlerinden farklı kılan hususlar verinin kendine mahsus yapısıdır. Verinin kendine mahsus yapısı dikkate alınarak düzenlemeler yapıldıktan sonra söz konusu verinin nerede bulunacağı teknolojik gelişmeler ile ortaya çıkartılacak bir hususdur[474].

İngiltere'de uzaktan erişimle arama yapılıp yapılamayacağı hususu üzerinde de durmak gerekmektedir. Bir bilgisayar üzerinde uzaktan erişimle arama yapmanın amacı, inceleme yapacak görevlinin, sabit disk ve rastgele erişimli bellek (RAM) üzerinde bulunan verilere erişimini sağlamak, elektronik posta trafiğini kesme ve internet arama alışkanlıkları ile anlık mesajlaşmaları izleme imkânlarını tanımaktır. Bunu gerçekleştirmek için şüphelinin bilgisayarına özel bir yazılım yüklenir. Bu yazılım daha

[472] Ünal, s. 50-51.

[473] Ünal, s. 51.

[474] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 294-295.

sonra bilgisayarda depolanan tüm verileri kopyalamak ve sonradan değerlendirme yapılmak üzere soruşturma makamına transfer eder. Bu tür bir yazılım kimi zaman şüphelinin ziyaret etmesi muhtemel internet adresine veya bilgisayarına indireceği bir programın parçasına yüklemek suretiyle de aynı fonksiyonu icra edebilmektedir[475].

İngiltere'de henüz uzaktan erişimle arama (remote forensic software-RFS) araçlarının kullanımının yasallığı veya uzaktan arama yöntemi ile elde edilen delillerin kabul edilebilirliğine ilişkin bir mahkeme kararı bulunmamaktadır. Ancak Avrupa Konseyi'nin tavsiyesi üzerine ülkede bilişim sistemlerinin uzaktan aranması resmen bir soruşturma yöntemi olarak tanınmıştır. Bu kapsamda İngiltere İçişleri Bakanlığı da polis memurları ve gizli servis elemanlarının mahkeme kararı olmaksızın şüphelilerin bilgisayarlarına uzaktan ve gizli bir şekilde arama yapabilmelerine izin veren bir planı kabul etmiştir. Bununla birlikte uzaktan erişimle arama İngiltere'de tamamen yeni bir soruşturma yöntemi değildir[476].

Nitekim İngiltere'de uzaktan erişimle arama yapma 1994 yılından beri yasal bir zemine oturtulmuştur. Buna göre, CMA'da yapılan bir değişiklikle devletin bilişim sistemlerine uzaktan erişim sağlaması mümkün hale gelmiştir. Bununla birlikte bu nitelikte bir yaklaşım RIPA altında da düzenlenmiştir. RIPA'nın ikinci kısmında yönlendirilmiş gözetim (directed surveillance) tedbirine yer verilmiştir. Yönlendirilmiş gözetim, bir kişi hakkında özel bilgiler elde edilmesi ve ciddi bir suçun tespiti veya önlenmesi amacıyla yürütülen özel nitelikte bir soruşturma kapsamında gerçekleştirilen gizli izleme faaliyetini ifade etmektedir. RFS araçları, belirli bir kimse hakkında bilgi edinmek, suç ve terör eylemlerini önlemek gibi amaçlarla bilgisayarda saklanan elektronik verileri aramakta ve şüphelinin çevrimiçi etkinliklerini izlemektedir. Bu bakımdan, RFS araçlarının kullanımı bu Kanun'a tabidir[477].

[475] Wiebke Abel, "Agents, Trojans and Tags: The Next Generation of Investigation", **International Review of Law, Computers & Technology**, Vol. 23, No. 1&2, (March-July 2009), s. 100.

[476] Abel, s. 101.

[477] Abel, s. 103.

2.5. Almanya Hukuk Sisteminde Bilişim Sistemlerinde Arama ve Elkoyma

Almanya, Avrupa Konseyi Siber Suç Sözleşmesi'ni 23.11.2001 tarihinde imzalamış, 09.03.2009 tarihinde onaylamış ve bu Sözleşme 01.07.2009 tarihinde iç hukukta yürürlüğe girmiştir[478]. Almanya, Sözleşmenin yürürlüğe girmesinden sonra Sözleşmeye uygun olarak iç hukukta bazı düzenlemeler yapmıştır. Buna göre Avrupa Konseyi Siber Suç Sözleşmesi'nin 1. maddesinde geçen "bilgisayar verisi" kavramı Alman Ceza Kanunu'na girmiş; bu kapsamda Alman Ceza Kanunu'nun 202a maddesinde verilerin depolandığı ve işlendiği bilişim sistemleri ağına girmek ve burada bulunan verileri ele geçirmek suç olarak düzenlenmiştir[479]. Buna karşın Alman hukukunda saklanan bilgisayar verilerinin aranması ve bunlara elkonulmasına ilişkin Siber Suç Sözleşmesi'nin 19. maddesindeki düzenlemeye uygun herhangi bir iç hukuk düzenlemesinin yapılmadığı görülmektedir.

Bu bağlamda Alman Ceza Muhakemesi Kanunu'nda bilişim sistemlerinde arama yapılması ve buradan elde edilecek elektronik verilere elkonulmasına ilişkin özel bir düzenleme bulunmamaktadır. Bu ortamlarda yapılacak arama ve elkoyma işlemleri normal arama ve elkoyma kurallarına göre tesis edilmektedir[480].

Buna göre, Alman hukuk sisteminde bilişim sistemlerinde arama ve elkoyma işlemleri; Alman Ceza Muhakemesi Kanunu'nda elkoymayı düzenleyen 94, elkoyma kararını verecek mercii düzenleyen 98, şüpheli kişiler için aramayı düzenleyen 102, diğer kişiler bakımından aramayı düzenleyen 103, arama emri ve icrasını düzenleyen 105, bilgi toplama ve soruşturmayı düzenleyen 161, adli kolluk görevlerini düzenleyen 163 ve belgelerin incelenmesini düzenleyen 110. madde hükümleri uyarınca gerçekleştirilmektedir[481].

---

[478] Member States of the Council of Europe, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (01 Ocak 2015).

[479] Sacit Yılmaz, "5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar", **Türkiye Barolar Birliği Dergisi**, Sayı. 92, (Mart-Nisan 2011), s. 66.

[480] Leyla Keser Berber, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El Koyma", **Ankara Barosu Avukatlık Akademisi Bilişim Hukuku Sertifika Programı 13. ve 14. Gruplar Sertifika Töreni**, Ankara, 9 Temmuz 2008, s. 8.

[481] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 290.

Bu bağlamda bilişim sistemlerinde bulunan verilere Alman Ceza Muhakemesi Kanunu m. 94 uyarınca elkonulabilir. Bu maddeye göre ceza soruşturması ile ilgili olarak anlamı bulunan her nesne muhafaza altına alınabilmekte, ancak ceza muhakemesi için gerekli bilişim sisteminin sahibi kendi isteği ile bu nesneyi soruşturma makamlarına teslim etmezse bu durumda bu nesneye zorla elkonulabilmektedir[482].

Alman Ceza Muhakemesi Kanunu m. 98 uyarınca elkoyma işlemi hâkim kararıyla gerçekleştirilir. Ancak, -basımevleri, matbaalar ve yazım ofisleri ile bunları eklentileri hariç- acele hallerin varlığı durumunda savcı ve diğer adli görevliler de elkoyma kararı verebilirler. Hâkim kararı olmadan yapılan elkoyma işlemi en geç üç gün içerisinde hâkim onayına sunulmak zorundadır. Hâkim ise elkoymadan itibaren üç gün içerisinde karar vermek durumundadır. Elkoyma ile ilgili kişiler elkonulan eşyanın kendilerine verilmesi için her zaman itirazda bulunabilirler[483].

Bilişim sistemlerinde yapılacak arama bakımından Alman Ceza Muhakemesi Kanunu m. 102 ve m. 103 hükümleri uygulama alanı bulacağına göre şüpheli haricindeki diğer kişilerce kullanılan ve diğer kişilere ait bilişim sistemlerinde de delil elde etmek amacıyla arama yapılabilecektir. Arama işleminden sonra arama işlemine tabi tutulan kişinin talebi üzerine aramanın sebebi ve aramaya neden olan suçu gösteren yazılı bir belge verilmelidir. Ayrıca, istek halinde yakalanan ve elkonulan eşyanın listesi hakkında arama tedbiri uygulanan kişiye verilecektir. Arama sonucunda herhangi bir şey bulunamaması durumunda ise bu durumu gösteren bir belge verilecektir (m. 107)[484].

Alman Ceza Muhakemesi Kanunu m. 110 uyarınca arama sonucu ele geçirilen belgeleri inceleme yetkisi, savcılık makamına veya savcılık makamı tarafından yetkilendirilen görevlilere aittir. Ancak, polise şüpheli verileri doğrudan inceleme yetkisi verilmemiştir[485]. Aramaya tabi tutulan kişinin meskeninde bulunan elektronik veri depolama cihazlarının incelenmesi, muhafaza ettiği verilerin kaybolma riskinin söz

[482] Tanrıkulu, s. 231.

[483] Ünal, s. 54-55.

[484] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 290.

[485] Rand Europe & Lawfort, s. 116.

konusu olduğu durumlarda, veri depolama cihazından elde edilebildiği ölçüde fiziksel olarak ayrı bir inceleme işlemini de kapsamaktadır (m. 110/3)[486].

Alman Ceza Muhakemesi Kanunu m. 161'de savcılığın bilgi toplaması ve araştırma yapması düzenlenmiştir. Bu bağlamda, savcı, bilgi toplayabilmek için kamu makamlarıyla yazışma yapabilir, bizzat kendisi veya polis aracılığıyla bilgi toplayabilir. Alman Ceza Muhakemesi Kanunu m. 163'te ise polisin görevlerinden söz edilmekte olup suçla ilgili bütün delillerin elde edilmesi ve delillerin karartılmasının engellenmesi yükümlülüğü düzenlenmiştir. Bu iki madde bilişim sistemlerine yönelik arama ve elkoyma tedbirleri bakımından uygulanabilir niteliktedir[487].

Elektronik posta trafiği ile ilgili tüm soruşturma tedbirlerinin Alman Anayasası m. 10 uyarınca haberleşmenin gizliliğine uygun olması zorunludur. Bu nedenle, elektronik posta trafiğinin izlenmesine ancak Alman Ceza Muhakemesi Kanunu m. 100'de açıkça belirtilen cinayet, soykırım, hırsızlık, ulusal güvenlik ve savunmaya karşı işlenen suçlar gibi ağır cezalık suçlarla ilgili yürütülen soruşturmalar bakımından izin verilir. Bu durumda hâkim veya acele hallerde savcı tarafından alınacak bir arama kararı gerekmektedir (m. 100)[488].

Bilişim sistemleri üzerinde yapılacak arama ve elkoyma işlemlerinde savcı bilişim sistemleri ile ilgili çalışma hakkında bilgi sağlamak veya elektronik verilere erişim sağlamak amacıyla gerekli uzmanlığa sahip bir kimseyi görevlendirebilir. Örneğin ağ yöneticisinin şifre istemesi veya sistem için güvenlik tekniğine ilişkin bilgi sağlama durumlarında olduğu gibi uzman yardımına ihtiyaç duyulduğu durumlarda bu türden bir görevlendirme söz konusu olabilecektir[489].

Uzaktan erişimle arama ile ilgili Almanya uygulamasına bakıldığında; bu tür bir aramanın Alman hukuk sisteminde hukuka uygun bulunmadığı değerlendirilmektedir. Nitekim savcılık makamının şüphelinin bilgisayarının uzaktan erişimle aranmasına

[486] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 291.

[487] Ünal, s. 55.

[488] Rand Europe & Lawfort, s. 116.

[489] Rand Europe & Lawfort, s. 116.

ilişkin bir kararı 25 Kasım 2006 tarihinde Bundesgerichtshof Federal Mahkemesi tarafından kaldırılmıştır. Bu olayda savcılık Ceza Kanunu'nun 94, 102 ve 110 maddeleri uyarınca söz konusu aramaya izin verilmesi hususunda itiraz etmiş ancak mahkeme kararında; konutta yapılan klasik aramalarla bir aygıt aracılığıyla gerçek zamanlı internet trafik verilerine ilişkin uzaktan erişimle bilgisayar aramasının aynı türden bir arama biçimi olmadığı ve o tarihte Almanya'da kolluğun uzaktan arama yapma yetkisini kullanabileceği herhangi bir yasal düzenlemenin bulunmadığı gerekçesiyle itirazı reddetmiştir[490].

Nordrhein – Westfalen eyaleti 30 Aralık 2006 tarihinde Anayasayı Koruma Kanununun (Verfassungsschutzgesetz) 5/2 maddesine 11. paragraf olarak yapmış olduğu ek bir düzenleme ile internet üzerinden yapılan haberleşmelerde internet üzerinden gizli izleme ve inceleme yapma imkânı tanınmıştır. Bu düzenleme aynı zamanda, Anayasayı Koruma Kuruluna şüphelinin özel bir bilgisayarı veya dizüstü bilgisayarında uzaktan erişimle arama yapmasına ilişkin bir yasal dayanak olma vasfını da taşımaktaydı[491].

Alman hukuk sistemine göre; devlet, eylem ve işlemleriyle Anayasanın ilk bölümünde belirtilen temel hak ve özgürlüklere müdahale ettiği hallerde anayasal şikâyet hakkının varlığı kabul edilmektedir. Bu kapsamda da söz konusu yasal düzenlemenin Anayasaya aykırılığı hususunda anayasal şikâyet başvurusunda bulunulmuştur[492]. Alman Federal Anayasa Mahkemesi (Bundesverfassungsgericht) 27 Şubat 2008 tarihinde vermiş olduğu kararla da bu yasa hükmünün Anayasa'ya aykırılığına hükmetmiştir. Federal Anayasa Mahkemesi iptal kararında yasal düzenlemedeki soruşturma biçiminin Anayasaya uygun olmadığı noktasında bir değerlendirmeye gitmeyip kararını, yeni bir

[490] Scritto da Wiebke Abel and Burkhard Schafer, "The German 'Federal Trojan' – Challenges Between Law and Technology", 2009, http://www.teutas.it/societa-informazione/prova-elettronica/634--the-german-federal-trojan-challenges-between-law-and-technology-wiebke-abel-llm-university-of-edinburgh-script-wabelsmsedacuk-burkhard-schafer-university-of-edinburgh-joseph-bell-centre-1-introduction-the-council-of-the-european-uni.html (21 Kasım 2014).

[491] Abel and Schafer, The German 'Federal Trojan' – Challenges Between Law and Technology, http://www.teutas.it/societa-informazione/prova-elettronica/634--the-german-federal-trojan-challenges-betweenlaw-and-technology-wiebke-abel-llm-university-of-edinburgh-script-wabelsmsedacuk-burkhard-schafer-university-of-edinburgh-joseph-bell-centre-1-introduction-the-council-of-the-european-uni.html (21 Kasım 2014).

[492] Wiebke Abel and Burkhard Schafer, "The German Constitutional Court on the Right in Confidential and Integrity of Information Technology Systems - A Case Report on BVerfG, NJW 2008, 822", **Scripted,** Vol. 6, Issue. 1, (April 2009), s. 109-110.

insan hakkı olarak bilgi teknolojisi sistemlerinin gizliliğinin ve bütünlüğünün korunması temeline dayandırılmıştır. Mahkeme kararı bu yönüyle de bir ilk olma özelliği taşımaktadır[493].

2.6. Fransa Hukuk Sisteminde Bilişim Sistemlerinde Arama ve Elkoyma

Fransa'da arama, elkoyma, bilirkişilerin belirlenmesi usulü gibi özel soruşturma işlemleri Ceza Muhakemesi Kanunu'nda (Code de Procédure Pénale) düzenlenmiştir. Buna göre, bir olayın ihbar edilmesi veya soruşturma organları tarafından re'sen tespit edilmesinden sonra genellikle bir soruşturma hâkimi (juge d'instruction) atanmaktadır. Soruşturma hâkimi gerekli görmesi durumunda Fransız polis teşkilatı içerisinde ihtisaslaşmış birimler yardımıyla ön soruşturma işlemlerini yerine getirmektedir. Arama emirleri gibi özel soruşturma tedbirleri bakımından sorgu hâkimi münhasır yetkiye sahiptir. Bazı durumlarda ise savcı veya hâkimin soruşturma işlemlerini yürütmek üzere sivil nitelikte bir bilirkişi kullandığı da görülmektedir[494].

Fransa, Avrupa Konseyi Siber Suç Sözleşmesi'ni 23.11.2001 tarihinde imzalamış, 10.01.2006 tarihinde onaylamış ve Sözleşme 01.05.2006 tarihinde iç hukukta yürürlüğe girmiştir[495]. Buna göre Fransız hukukunda saklanan bilgisayar verilerinin aranması ve bunlara elkonulmasına ilişkin Siber Suç Sözleşmesi'nin 19. maddesindeki düzenlemeye uygun iç hukuk düzenlemelerinin varlığı dikkat çekmektedir.

Fransız Ceza Muhakemesi Kanunu'nun 94. maddesi 1991 ve 2004 yıllarında iki defa değişikliğe uğramıştır. Buna göre, maddi gerçeğin ortaya çıkartılması için faydalı olacağı durumlarda, eşya veya elektronik verinin elde edilebileceği her yerde bu madde

[493]Abel and Schafer, The German 'Federal Trojan' – Challenges Between Law and Technology, http://www. teutas. it/societa-informazione/prova-elettronica/634--the-german-federal-trojan-challenges-betweenlaw-and-technology-wiebke-abel-llm-university-of-edinburgh-script-wabelsmsedacuk-burkhard-schafer-university-of-edinburgh-joseph-bell-centre-1-introduction-the-council-of-the-european-uni.html (21 Kasım 2014).

[494] Rand Europe & Lawfort, s. 108.

[495] Member States of the Council of Europe, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT= 185&CM=&DF=&CL=ENG (01 Ocak 2015).

uyarınca arama yapılabilecektir. Bu durum, bilgisayar sistemleri ve ağlar üzerinde yapılacak aramaları da kapsamaktadır[496].

Bununla birlikte bilgisayar dışında belge, bildiri ve diğer nesnelerden de söz edilmesine karşın Fransız Ceza Muhakemesi Kanunu'nun 56. ve 97. maddelerinde düzenlenen arama ve elkoyma prosedürünün de genel olarak Avrupa Konseyi Siber Suç Sözleşmesi'nin 19. maddesiyle uyumlu olduğu görülmektedir[497].

Ceza Muhakemesi Kanunu'nun 56. maddesinde "elektronik veri" ibaresine açık bir şekilde yer verilmek suretiyle bilişim sistemlerinde yapılacak arama işlemi düzenlenmiştir. Bu madde uyarınca maddi gerçeğin ortaya çıkartılması için elektronik verilere elkoyma, elektronik verinin saklandığı aygıta elkonulması veya elektronik verinin ilgili kişinin huzurunda kopyalanması ile mümkün olacaktır. Kopyalama yapılması durumunda, bulundurulması veya kullanılması yasa dışı veya zararlı olan elektronik verinin silinmesi söz konusu olabilecektir[498].

Ceza Muhakemesi Kanunu'nun 97. maddesi ise 94. madde uyarınca yapılacak aramaların ne şekilde gerçekleştirileceğine ilişkin ayrıntılı bilgiler sunmaktadır. Buna göre, ele geçirilen eşya, belge veya verinin tamamının derhal envanterinin çıkartılması ve bunların hepsinin mühürlenmesi gerekmektedir. Verilere elkoyma işlemi ya verilerin içerisinde bulunduğu depolama aygıtı (örneğin sabit disk) ile birlikte elkoyma veya verilerin bir kopyasının alınması suretiyle gerçekleştirilir. Kanunun 56. maddesinde belirtildiği gibi burada da verinin kopyasının alınması durumunda, eğer verinin bulundurulması veya kullanılması yasadışı veya zararlı ise orijinal veri silinebilecektir[499].

Ceza Muhakemesi Kanunu'nun 99-3 maddesinde elektronik delilin elde edilmesine ilişkin bilirkişi görevlendirilmesi prosedürü düzenlenmektedir. Buna göre; soruşturma

[496] Rand Europe & Lawfort, s. 108.

[497] Picotti and Salvadori (hzl.), s. 56.

[498] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 292-293.

[499] Rand Europe & Lawfort, s. 108.

hâkimi, herhangi bir kişi veya kuruma soruşturmayla ilgili bilgileri ortaya çıkartacak nitelikteki spesifik elektronik verilere elkoymaları hususunda emir verebilir[500].

Fransız hukukunda uzaktan erişimle arama hususu üzerinde de durmak gerekir. Buna göre; Ceza Muhakemesi Kanunu'nun 57/1. maddesi uyarınca adli kolluk görevlileri, devam eden soruşturma ile ilgili bilgisayarlarda saklanan herhangi bir veriye erişim konusunda yetkilidir. Adli kolluk görevlilerinin, arama sırasında meskende bulunan bilgisayar üzerinden erişilebilen diğer bilgisayar sistemleri üzerinde bulunan veri üzerinde de arama yapabileceği kabul edilmektedir. Bununla birlikte 57. maddenin 2. fıkrası ile birlikte değerlendirildiğinde, burada bahsedilen uzaktan erişimli aramanın ancak Fransa'nın yargı yetkisi içinde kalan bilgisayarlar bakımından sınırlı olduğu görülmektedir. Diğer taraftan madde kapsamındaki uzaktan erişimli arama, herhangi bir bilgisayardan başlatılabilen bir uzaktan erişimle arama olmayıp aramanın icrası sırasında sisteme bağlı ilk bilgisayardan başlatılan aramadır[501].

2.7. İtalya Hukuk Sisteminde Bilişim Sistemlerinde Arama ve Elkoyma

İtalya'da polis iddia edilen suçların ön soruşturmasını yapmak, delilleri toplamak ve toplanan delilleri muhafaza etmekle görevlidir. Şüpheli, polis tarafından sorgulanması sırasında savunma avukatını hazır bulundurma hakkına sahiptir. Polis re'sen kovuşturmayı gerektiren tüm suçları adli makamlara bildirmekle yükümlüdür. Adli işlemler bir ön soruşturmayla başlar. Alenen işlenen suçlarda, şüpheli suçu ikrar eder veya suç açık delillerle ortaya konursa soruşturma işlemleri bir sulh hâkimi tarafından yerine getirilir. Diğer tüm hallerde soruşturma işlemleri soruşturma hâkimi tarafından yürütülür[502].

İtalyan Ceza Muhakemesi Kanunu (Codice di Procedure Penale) delillerin elde edilmesine ilişkin kontrol ve arama tedbiri olmak üzere iki araçtan bahsetmektedir. Kontrol tedbiri, bilgisayar ve telekomünikasyon sistemleri de dâhil olmak üzere, suçun kişiler, yerler ve nesneler üzerindeki iz ve diğer etkilerinin belirlenmesini

[500] Rand Europe & Lawfort, s. 108.

[501] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 292.

[502] Rand Europe & Lawfort, s. 152.

hedeflemektedir. Arama tedbiri ise bir suçun oluştuğuna ilişkin somut delilleri veya bir şüphelinin tutuklanmasına temel teşkil edecek suça ilişkin diğer öğeleri bulmak amacıyla yapılan arama işlemidir. Uygulamada ise kontrol ve arama tedbirleri arasında çok ince bir çizginin bulunduğu görülmektedir[503].

Kontrol tedbiri Ceza Muhakemesi Kanunu'nun 244-246 maddeleri arasında düzenlenmektedir. Kanun, kişiler (m. 245), yerler ve nesnelere (m. 246) ilişkin kontrol tedbirine dair farklı disiplinlere yer vermektedir. Özellikle belirtmek gerekir ki; her iki madde de belirli garanti hükümleri düzenlenmiştir. Kanunun 245. maddesinde kişilere yönelik düzenlenen kontrol tedbirine ilişkin olarak; kişilere uygulanan kontrol tedbiri sırasında hakkında tedbir uygulanan kişinin güvendiği bir kimseden yardım alma hakkının olduğu öngörülmektedir. Ayrıca, söz konusu tedbirin kişinin onur ve haysiyetine saygı gösterilerek yerine getirilmesi gerekmektedir. Kanunun 246. maddesinde düzenlenen yer ve nesnelere ilişkin kontrol tedbirinde ise bunlara sahip kişiye yönelik bir kontrol emrinin olması zorunluluğu bulunmaktadır[504].

Diğer taraftan Ceza Muhakemesi Kanunu'nun 247-250. maddeleri arasında arama tedbirinin uygulanışına ilişkin hükümlere yer verilmiştir[505]. Buna göre; Kanunun 247. maddesinin 1. paragrafı bilişim sistemleri ile ilgili yapılacak arama işlemini düzenlemektedir. Bu bağlamda suça ilişkin veri, bilgi veya yazılımın bir bilgisayar veya bilgisayar sisteminde saklanıyor olduğuna inanmayı gerektirecek bir nedenin varlığı halinde, bu bilgisayar veya bilgisayar sistemi bir şifre veya diğer bir güvenlik önlemi ile korunuyor olsa bile, arama işleminin bir şekilde yerine getirilmesi ve gerekli teknik önlemler alınarak orijinal verinin korunması ve değişikliğe maruz kalmasının önlenmesi gerekmektedir. Kanunun 247. maddesinin 2. paragrafında ise -kontrol tedbirinde uygulanan garanti hükümlerinde olduğu gibi- gerekçeli karar üzerine verilen arama emirleri bakımından bazı garanti hükümlerine yer verilmiştir[506].

---

[503] Astolfo Di Amato, **Criminal Law in Italy**, The Netherlands: Kluwer Law International, 2011, s. 206.

[504] Amato, s. 206.

[505] Rand Europe & Lawfort, s. 152.

[506] Amato, s. 206-207.

Ayrıca Ceza Muhakemesi Kanunu'nun 250. maddesinde de hâkimin suça ilişkin somut delil veya sair öğelerin gizleneceğine kanaat getirdiği durumlarda aramanın devam ettiği yere gelen veya halen orada olan kişilerin de aranabileceği düzenlenmektedir. Kanunun 251. maddesi, aramanın kişinin ikametinde gerçekleştirilmesi durumlarını ve bu işlemlerin belirli zaman dilimiyle sınırlı olarak yerine getirilmesini öngörmektedir[507].

İtalyan hukuk sisteminde güvenlik amacıyla kanıt toplama aracı olarak ayrıca düzenlenen elkoyma tedbirinin yanı sıra Ceza Muhakemesi Kanunu'nun üçüncü kitabında düzenlenen konumuzla alakalı elkoyma tedbiri ise yalnızca suçla ilgili gerçek durumu tespit etmeye yönelik gerekli görülen somut delil veya diğer öğeleri elde etmeye ilişkindir[508].

Buna göre; Ceza Muhakemesi Kanunu'nun 253. maddesinin 1. paragrafı genel elkoyma tedbirini düzenlemektedir[509]. Aynı maddenin 2. paragrafı ise somut delilin tanımını içermektedir. Bu anlamda somut delil, gerçekleşmesiyle ortaya çıkan ve söz konusu suça ait olan ürün, kazanç veya fiyattır[510].

Ceza Muhakemesi Kanunu'nun 254. maddesinde ise kişiler arasındaki yazışmalarla ilgili elkoyma tedbirine ilişkin hükümlere yer verilmiştir[511]. Bu madde kapsamında elektronik haberleşmeye ilişkin yazışmalar, telekomünikasyon ve internet servis sağlayıcıların elkonulmasına ilişkin detaylı düzenleme de bulunmaktadır[512].

İtalya, Avrupa Konseyi Siber Suç Sözleşmesi'ni 23.11.2001 tarihinde imzalamış, 05.06.2008 tarihinde onaylamış ve bu sözleşme 01.10.2008 tarihinde iç hukukta yürürlüğe girmiştir[513]. Buna karşın İtalyan hukukunda saklanan bilgisayar verilerinin

[507] Amato, s. 206-207.

[508] Amato, s. 207.

[509] Rand Europe & Lawfort, s. 152.

[510] Amato, s. 207.

[511] Rand Europe & Lawfort, s. 152.

[512] Amato, s. 207.

[513] Member States of the Council of Europe, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (01 Ocak 2015).

aranması ve bunlara elkonulmasına ilişkin Siber Suç Sözleşmesi'nin 19. maddesindeki düzenlemeye uygun ayrıksı bir iç hukuk düzenlemesinin bulunmadığı görülmektedir.

Ancak, yukarıda belirtilen hususlar dikkate alındığında İtalyan Ceza Muhakemesi Kanunu'nun 247. maddesinin genel olarak Siber Suç Sözleşmesi'nin 19/1 maddesiyle, Ceza Muhakemesi Kanunu'nun 250 ve 254. maddelerinin ise Siber Suç Sözleşmesi'nin 19/3 maddesiyle uyumlu oldukları, bununla birlikte Ceza Muhakemesi Kanunu'nda Siber Suç Sözleşmesi'nin 19/2 ve 19/4 maddelerine temas eden herhangi bir düzenlemenin bulunmadığı söylenebilir[514].

Diğer taraftan, İtalyan hukuk sisteminde bilişim sistemleri üzerinde yapılacak arama ve elkoyma işlemlerinin yukarıda belirtilen yasa hükümlerinin yanı sıra esasen yargı içtihatları ile şekillendiği de görülmektedir. Nitekim bu konuda birçok yargı kararı bulunmaktadır. En önemli yargı kararlarından birisinde (Sent Cass. Sez. III, n. 1778/03) ise mahkeme, elektronik veri depolama aygıtları üzerinde elkoyma işleminin uygulanabileceğine ve fakat bu işlemin yazıcı, tarayıcı ve ekranları kapsamayacağına ve bunlardan elde edilen verilerin delil olarak kabul edilemeyeceğine hükmetmiştir[515].

Belirtmek gerekir ki; İtalyan hukuk sisteminde adli sürecin tüm aşamalarında (soruşturma, kovuşturma ve temyiz aşamalarında) hâkim, savcı veya savunma avukatı Ceza Muhakemesi Kanunu'nun 220. maddesi uyarınca delillerin değerlendirilmesi hususunda bilirkişi tayin edebilirler. Bununla birlikte bu konuda adli süreçle ilgili temel sorun elektronik delilin hukuken değerlendirmesine ilişkin kaygılarla ilgili çözüm arayışlarının halen devam ediyor olmasıdır[516].

Son olarak İtalyan hukuk sisteminde uzaktan erişimle arama hususuna da değinmek gerekmektedir. Bu konuyla ilgili olarak İtalyan Yüksek Mahkemesi savcılık tarafından Ceza Muhakemesi Kanunu'nun 234. maddesi uyarınca şüphelinin kamuya açık ofisinde kullanmış olduğu bilgisayarındaki verileri elde etmek amacıyla şüphelinin haberi olmaksızın korsan bir yazılım yüklemesine yetki veren bir arama kararının İtalyan

[514] Picotti and Salvadori (hzl.), s. 56.

[515] Rand Europe & Lawfort, s. 152.

[516] Rand Europe & Lawfort, s. 152.

Anayasasına uygun olduğuna hükmetmiştir. Yüksek Mahkeme gerekçeli kararında söz konusu yazılımın şüphelinin iletişimini takip etmediğini ve sadece bilgisayarında hâlihazırda bulunan bilgileri toplamaya elverişli olduğunu belirtmiştir[517].

Ayrıca, Yüksek Mahkeme, söz konusu davada uygulanan, korsan yazılım yüklemek suretiyle delil toplama metodunun bahse konu verinin aslını bozmaksızın ve orijinal dosyaya herhangi bir zarar vermeksizin kopyalamadan ibaret olması sebebiyle tekrar edilebilen bir eylem olduğuna da değinmiştir. Yüksek Mahkemenin belirtilen gerekçesi karşısında İtalya'da korsan yazılım kullanmak suretiyle uzaktan erişimle arama sonucunda elde edilen delillerin ulaşılabilir, denetlenebilir olmaları nedenleriyle, diğer tüm delil toplama metotlarının tabi olduğu geçerlilik koşullarına tabi olduğu söylenebilir[518].

[517] Giuseppe Vaciago, "Remote Forensics and Cloud Computing: An Italian and European Legal Overview", **Digital Evidence and Electronic Signature Law Review,** Vol. 8, (2011), s. 126.

[518] Vaciago, s. 116-127.

BÖLÜM 3: TÜRK HUKUKUNDA BİLİŞİM SİSTEMLERİNDE ARAMA VE ELKOYMA

3.1. Genel Olarak

Elektronik delilin elde edilmesine yönelik koruma tedbirlerinin uygulanması kişilerin özel hayatlarını kısıtlaması nedeniyle bu koruma tedbirlerinin Anayasa m. 13 uyarınca ancak kanunla düzenlenerek yürürlüğe konulmaları gerekmektedir. Zira devlet kişilerin temel hak ve özgürlüklerini kısıtlarken Anayasa m. 13 uyarınca Anayasa'da belirtilen amaçlar doğrultusunda bir kanuni düzenleme yoluna gitmelidir. Bu nedenle, bilişim sistemlerinden elektronik delil elde etmekle bağlantılı olan yetkilerin kanunla ve ayrıntılı olarak düzenlenmiş olmaları gereklidir[519].

Nitekim Türk hukukunda da Ceza Muhakemesi Kanunundaki klasik arama ve elkoyma koruma tedbirlerinden ayrı olarak bilişim sistemlerine ilişkin arama, elkoyma ve kopyalama koruma tedbiri düzenlenerek hem elektronik delilin aranması ve elde edilmesinde farklı bir yöntem izlenmesi hem de böyle bir yöntem izlenirken temel hak ve özgürlüklere müdahalede daha sınırlı ve hassas davranılması hedeflenmiştir.

Bu bakımdan Türk hukukunda bilişim sistemlerinde yapılacak arama, kopyalama ve elkoyma koruma tedbirinin düzenlendiği CMK'nın 134. maddesi ile bu koruma tedbiriyle bağlantılı olan Adli ve Önleme Aramaları Yönetmeliği'nin 17. maddesi ve Suç Eşyası Yönetmeliği'nin 9. maddesindeki hükümlerin ele alınması, bu arada hukuk sistemimizde yasal bir düzenlemeye konu olmayan uzaktan erişimle arama ve bulut bilişimde arama konularına da iç hukukumuz açısından değinilmesi yerinde olacaktır.

3.2. Ceza Muhakemesi Kanunu'nda Arama, Kopyalama ve Elkoyma Tedbiri

3.2.1. Genel Olarak

Koruma tedbirleri, ceza yargılamasının gereği gibi yapılabilmesi veya hükmün infazının mümkün kılınabilmesi amacıyla soruşturma ve kovuşturma sürecinde başvurulabilen ve hükümden önce, gerektiğinde zor kullanmak suretiyle bazı temel hak ve özgürlüklere

[519] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1094.

geçici müdahaleyi gerektiren işlemlerdir[520]. Koruma tedbirleri, adil yargılamanın en önemli bölümünü kapsamasının yanı sıra özellikle kişilerin hak ve özgürlüklerini sınırlama ihtimaline binaen hem anayasal haklar hem de temel hak ve özgürlüklerin korunması ile en sıkı ilişkisi olan tedbirlerdir[521].

Koruma tedbirlerinin amacı, ceza yargılamasında maddi gerçeğin ortaya çıkmasını sağlamak ve yargılama sonucunda verilecek hükmün uygulanabilirliğini güvence altına almaktır. Zira toplumsal barışın devamlılığı, toplumun ceza normlarına aykırı hareket eden failden korunması ve failin ıslah edilmesi suretiyle toplumsal normlara uygun hareket etmesinin sağlanması ancak maddi gerçeğin ortaya çıkartılmasıyla mümkündür. Konumuz bakımından da koruma tedbiri uygulanarak elektronik delile tam ve doğru bir şekilde ulaşılması, maddi gerçeğin ortaya çıkartılmasına hizmet edecektir[522].

5271 sayılı CMK'da "koruma tedbirleri" başlığı altında ve olabildiğince sistematik bir tarzda düzenlenen bu konu ile 1412 sayılı CMUK düzenlemesindeki terim karışıklığına son verilmiştir. Buna göre; CMK sistematiği altında koruma tedbirleri, yakalama ve gözaltı, tutuklama, adli kontrol, arama ve elkoyma, telekomünikasyon yoluyla yapılan iletişimin denetlenmesi, gizli soruşturmacı ve teknik araçlarla izleme ve koruma tedbirleri nedeniyle tazminat başlıkları altında düzenlenmiştir.

Günümüzde bilgisayar teknolojisinin hızla ilerlemesi ve birçok işlemin bilgisayar aracılığı ile gerçekleştirilmesi, yapılan işlerde büyük kolaylık ve verim artışı sağlamasına karşın bilgisayarların işlenen birçok suçta daha yaygın şekilde kullanılması dikkat çekici boyutlara ulaşmıştır[523].

Diğer taraftan, bilişim teknolojisinin kullanılması suretiyle işlenen suçlarda, fiziksel delil elde etme yöntemlerinin yetersiz kaldığı görülmektedir. Zira soruşturmanın konusunu oluşturan elektronik veriler elle tutulan ve gözle görülen nesneler değildir. Bu veriler, her gün gelişen ve yenilenen teknoloji kullanılarak saklanmakta ve bir yerden

[520] Cumhur Şahin, **Ceza Muhakemesi Hukuku I**, 4. Basım, Ankara: Seçkin Yayıncılık, 2013, s. 217.

[521] Donay, s. 74.

[522] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 84.

[523] Aslan Ölmez, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Kopyalama ve Bunlara El Koyma", **Terazi Hukuk Dergisi**, Cilt. 4, Sayı. 30, (Şubat 2009), s. 45.

başka bir yere kolaylıkla gönderilebilmektedir. Hatta bu veriler bazen şifrelenmekte bazen de hiçbir özellik göstermeyen resim veya ses içeren veriler içerisine gizlenerek kullanılabilmektedir[524].

Elle tutulamayan, gözle görülemeyen ve elektrik devrelerinden oluşan bilgisayar verilerinin ceza yargılamasında delil olarak değerlendirilmesi yeni bir olgudur. Bununla birlikte devletin "koruma tedbirleri" çerçevesinde bilgisayar programlarında bulunan verileri elde edip saklayarak yargılamada delil olarak kullanması artık yaygın şekilde görülmektedir. Bununla birlikte CMK'nın 116 vd. ile 127. maddelerinde arama ve elkoyma tedbirlerine ilişkin genel hükümler bulunmasına rağmen bu tür verilerin elde edilmesi özel bir arama ve elkoyma kararını gerekli kılmaktadır. Zira bir bilgisayarın içerisinde veya birbirlerine ağ şeklinde bağlanmış olan bilgisayarların bağlı bulunduğu sistem içerisinde delil aranması ve bunlara elkonulması ayrı bir işlem niteliğindedir.

Gerçekten de, bilgisayar veya bilgisayarın bağlı bulunduğu sistemlerde bu tedbirin uygulanması klasik arama ve elkoyma tedbiriyle benzerlik gösterse de kendine mahsus farklılıkların bulunması da doğaldır. Bu farklılıklar elektronik ortamın veya elektronik delilin kendilerine özgü niteliğinden kaynaklanmaktadır. Elektronik verinin bilgisayarın soyut tarafında yer alması düşünüldüğünde klasik arama ve elkoyma tedbiriyle bu verilerden anlaşılır bir şekilde delil elde edilmesi her zaman mümkün olmamaktadır[525].

Diğer taraftan, koruma tedbirinin amacının gerçekleştirilebilmesi tedbirin teknik boyutuyla ele alınmasına bağlıdır. Bu bakımdan, tedbire disiplinler arası bir çalışma ile hayat verilmesi gerekmektedir. Olayın teknik boyutunun yanı sıra hukuk normlarına uyulması olmazsa olmaz bir unsurdur. Olayın teknik boyutuna uyulmaması delile erişilememesine, olayın hukuki boyutunun göz ardı edilmesi ise elde edilen delilin hukuka aykırı olması nedeniyle mahkemede kullanılamamasına neden olacaktır[526].

Bu bağlamda, elektronik delilin kolaylıkla değiştirilebileceği, manipüle edilebileceği, çok fazla iz bırakmadan silinebileceği ve sıfırdan oluşturulabileceği hususları karşısında

[524] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1092.

[525] Ünal, s. 84-85.

[526] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 311.

elektronik delilin hukuki ve teknolojik anlamda usulüne uygun biçimde toplanarak analiz edilmesi işlemlerinin ne kadar önemli olduğu ortadadır. Ayrıca, suçu aydınlatmaya yönelik olsa da kişisel, ailevi ve mesleki kaygıların bulunduğu bilgisayar incelemelerinde uluslararası sözleşmeler ve Anayasa ile teminat altına alınan özel hayatın gizliliğinin ihlal edilebilmesi de muhtemeldir[527].

Bu bakımdan hem tedbirin elektronik ortamda gerçekleştirilmesi hem de müdahale edilen temel hak ve özgürlüklerin etkin bir şekilde korunması amacıyla CMK m. 134'de genel nitelikteki arama ve elkoyma tedbirinin özel bir şeklini ifade eden bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbiri düzenlenmiştir. Genellikle arama tedbiri bina ve eklentileri, araç ve kişiler üzerinde gerçekleşmesine karşın söz konusu tedbirde arama ve elkoymanın konusunu bilgisayarlar, bilgisayar programları ile bilgisayar kütükleri oluşturmaktadır[528].

Buna karşın öğretide bir görüşe[529] göre; CMK m. 134 hükmünün bir elkoyma hükmü olmayıp arama koruma tedbirinin bilgisayar kütük ve programlarında icrasıyla ilgili özel bir düzenleme olduğu, burada arama sonrasında bir şeye elkoyma değil, yalnızca verilerin örnek çıktılarının veya kopyalarının alınmasının yani delil tespitinin söz konusu olduğu, çok istisna hallerde delillere ulaşılamaması durumlarında ise yine bilgisayara elkoymuş olmak için değil, orada olabileceği değerlendirilen delillere ulaşmak için bu amaçla sınırlı ve geçici şekilde bilgisayarlar ve programlarında inceleme yapmak üzere elkonulmasına izin verildiği, bunun bir elkoyma olarak algılanması ve kolluğun da menkul bir mala elkoyma kararı varmış gibi muamelede bulunmasının yanlış olacağı ileri sürülmüştür.

Diğer taraftan insan yaşamının her alanında kullanılan bilişim sistemleri ve veri depolama aygıtları, kişilerin iz bıraktıkları delil kaynaklarından olmaları nedeniyle adli bilişimin temel konusunu teşkil etmektedirler. Bu bakımından söz konusu koruma

[527] Ahi, "Adli Bilişim Nedir ?", http://www.bilisimhukuk.com/2009/07/adli-bilisim-nedir/ (04 Mayıs 2014).

[528] Veli Özer Özbek, **Ceza Muhakemesi Hukuku,** Ankara: Seçkin Yayıncılık, 2006, s. 359.

[529] Ünver ve Hakeri, 1. Cilt, s. 578.

tedbirinin aynı zamanda adli bilişim kapsamına giren bir çalışmayı da içerdiği söylenebilir[530].

3.2.2. Tedbirin Amacı

Bilişim sistemlerinde yapılan aramada elde edilmesi amaçlanan bilgi, formatlanmış ve sistem tarafından okunabilir hale gelmiş bilgidir. Söz konusu formatlanmış bilgi ise elektronik veri olarak tanımlanmaktadır. Bu elektronik veri, yargılama sırasında maddi olayın ispatı hususunda kullanılabilmesi durumunda delil niteliği kazanacak ve elektronik delil ortaya çıkmış olacaktır[531].

CMK m. 116'da genel arama işleminin amacı, şüpheli veya sanığın yakalanması ya da suç delillerinin elde edilmesi olarak belirtilmiştir. CMK m. 123'te düzenlenen genel elkoyma tedbirinin amacı ise genellikle arama sonucunda elde edilen ve suç delili konumundaki eşyanın iade ve müsadere edilinceye kadar bir bütün halinde korunmasıdır. CMK m. 134'de düzenlenen arama, kopyalama ve elkoyma tedbirinde ise şüphelinin veya sanığın yakalanması tali bir amaç olarak gözetilebilir ise de tedbirin asıl amacı suç delillerinin elde edilmesi ve korunmasıdır. Bu bakımdan tedbirin öncelikli amacının elektronik delil elde etmek ve onun aslının ve/veya adli kopyasının muhafaza altına alınmasını sağlamak olduğu söylenebilir.

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma özellikle bilişim suçlarına ilişkin elektronik delillerin elde edilmesinde büyük önem arz etmektedir. Bununla birlikte söz konusu tedbir klasik suçların soruşturulmasında da kullanılmaktadır. Ceza Muhakemesi Kanunu'ndaki klasik arama tedbirine ilişkin hükümlerin bilgisayar ortamına uygulanması mümkün olmadığı için hukukumuzda bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbiri ayrıca düzenlemiştir.

[530] Yusuf Yaşar ve İsmail Dursun, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi (MAR-HAD),** Cilt. 19, Sayı. 3, (2013), s. 7-8.

[531] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 59-60.

Ceza muhakemesi sürecinde elde edilen delillerle maddi olay adeta tekrar inşa edilmektedir. Bu bakımdan, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbiri ile bilişim sistemlerinde bulunan elektronik delilin elde edilerek hâkimin yargılamaya konu olayda vicdani kanaatinin oluşması sağlanmaktadır.

3.2.3. Tedbirin Kapsamı

CMK m. 134/1'de tedbirin kapsamı şüphelinin kullandığı bilgisayar, bilgisayar programları ve kütükleri olarak belirtilmiştir. Buna göre;

Bilgisayar, çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin olarak tanımlanmaktadır[532].

Bilgisayar programı, 5846 sayılı FSEK m. 1/B'de "Bir bilgisayar sisteminin özel bir işlem veya görev yapmasını sağlayacak bir şekilde düzene konulmuş bilgisayar emir dizgesini ve bu emir dizgesinin oluşum ve gelişimini sağlayacak hazırlık çalışmaları" şeklinde tanımlanmaktadır. Dünya Fikrî Mülkiyet Teşkilatı Fikrî Haklar Anlaşması'na göre ise bilgisayar programı, "makinenin okuyabileceği bir taşıyıcıya yüklendikten sonra, bilgi işleme yeteneğine ehil böyle bir makinenin belirli bir işlev veya görevi yerine getirmesini ya da belirli bir sonuca ulaşmasını sağlayabilen komutlar dizini" şeklinde tanımlanmıştır[533].

Bilgisayar programları kullanıcıların bilgisayara işlem yaptırabilmelerini sağlamaktadırlar. İşlemlerin yaptırılabilmesi için ise girilen komutların bir arada ve bir dizi şeklinde olması gerekmektedir. Bu komutlar ve diziler belli bir kurala göre yazılmıştır ve bu kurallara "programlama dili" denilmektedir[534].

---

[532] Türk Dil Kurumu, http://www.tdk.gov.tr/tdksozluk/sozbul.ASP?kelime (02 Ekim 2014).

[533] Sevilay Eroğlu, **Rekabet Hukukunda Bilgisayar Programlarının Korunması**, İstanbul: Beta Yayınevi, 2000, s. 2.

[534] Şentürk (Ed.), s. 40.

Bilgisayar programlarının bilgisayarda bulunmaları doğal olduğu için bilgisayarlarda yapılan aramalar bilgisayar programlarını da kapsamaktadır. Bununla birlikte bilgisayar programları, bilgisayar dışındaki veri saklama birimlerinde de bulunabilmektedirler. Bu bakımdan, bilgisayar programlarında arama yapılması söz konusu olduğunda bu tedbirin uygulaması veri saklama birimlerine de yansıyacaktır[535].

Bilgisayar programı olarak kötü niyetli yazılımlar da bir suçun aydınlatılmasında delil olarak kullanılabilmektedir. Bir bilişim sisteminin işleyişinin bozulması veya bilişim sisteminin suçun işlenmesinde aygıt olarak kullanılmasının kötü niyetli bir yazılım vasıtasıyla gerçekleştirildiği durumlarda, söz konusu yazılım suça ait bir delil olarak karşımıza çıkabilmekte ve tedbirin kapsamına girebilmektedir. Benzer şekilde, fikri mülkiyet haklarının ihlal edilmesi suretiyle çoğaltılan yazılımlar da, kendisi suçtan meydana gelen eşya niteliğinin yanı sıra suça ilişkin birer delil olarak ortaya çıkmaktadırlar[536].

Bilgisayar kütükleri'nin ise; sabit disk olarak anlaşılması gerektiği belirtilmektedir. İngilizce "log" kelimesinin karşılığı olan kütükler daha çok internet servis sağlayıcılarının internet erişimi sağladıkları kullanıcılara ait IP numaralarını ve diğer erişim bilgilerini depoladıkları veri tabanlarını ifade etmektedir[537]. Bunun dışında, büyük kapasitedeki verileri saklayan veri tabanları veya arşiv amacıyla saklanan büyük çaptaki veri saklama birimleri de bilgisayar kütüğü olarak nitelendirilebilirler[538].

CMK m. 134/1'de tedbirin kapsamı şüphelinin kullandığı bilgisayar, bilgisayar programları ve kütükleri olarak belirtilmiş olmasına karşın kullanım amaçları çok çeşitli olmakla birlikte içeriğinde bilişim teknolojisi barındıran cep telefonu, cep bilgisayarı, dijital fotoğraf makinesi, dijital kamera vb. gibi taşınabilir cihazlara yönelik herhangi

[535] Ünal, s. 96.

[536] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 332.

[537] Veli Özer Özbek, Ceza Muhakemesi Hukuku, s. 363; Buna karşın öğretide kütük kelimesinin her ne kadar "log" kelimesinin sözlük karşılığı olsa da bilişim terminolojisindeki karşılığı olamayacağı, "log" kelimesinin karşılığının günlük olarak kullanıldığı, bu bağlamda kütükleri, insan müdahalesi ile bilişim sistemi tarafından oluşturulan ve saklanan dosyalar olarak tanımlamak gerekirken "log"ları ise insan müdahalesi olmadan bilişim sistemi tarafından oluşturulan ve saklanan dosyalar olarak tanımlamak gerektiği savunulmuştur. Bkz. Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 52-53.

[538] Ünal, s. 96.

bir hüküm bulunmadığı görülmektedir. Adli bilişimin esas konusunun elektronik delil olması nedeniyle elektronik delilin kaynağını sadece bilgisayar ile sınırlandırmak meseleye çok dar bir pencereden bakmak anlamını taşımaktadır. Teknolojinin gelişimi ile günümüzde hemen herkesin kullanmış olduğu bu cihazlarda adli bilişim uzmanlarınca elde edilebilecek çok önemli delillerin bulunduğu da aşikârdır[539].

Kaldı ki; bünyelerinde dijital bir veri barındırmıyor olsalar bile bir modem, telefon, uzaktan kumanda, kamera vs. gibi çeşitli elektronik cihazlar da elektronik delil niteliği taşıyabilmektedir. Zira bu tip cihazlar bünyelerindeki değişik mantık kapıları ile karar verebilen elektronik devreler sayesinde başka bir elektronik delili tetikleyebilecek bir mekanizmaya sahip olabilirler[540].

Bu bakımdan kullanım amaçları çok çeşitli olsa da içeriğinde bilişim teknolojisi barındıran cihazlar bu kapsamda değerlendirilmelidir. Buna göre; cep telefonu, çağrı cihazı, dijital kamera ve fotoğraf makinesi, özel amaçlı kameralar (ısıya hassas, kızıl ötesi, vb.), fotokopi makinesi, ATM cihazı, elektronik ajanda, faks makinesi, elektronik veri bankası, akıllı kart ve POS makinesinin bu kapsamın içindedirler. Son zamanlarda günlük kullanıma sunulan elektronik veya mekanik ürünlerin pek çoğunda bilişim sistemleri ile bütünleşme sağlanmıştır. Bu nedenle bu kapsama alınabilecek pek çok ürün daha bu listeye eklenebilir.

Uygulamada bu tür cihazlarda bulunması muhtemel delillere ulaşmak için CMK'nın 116 ve 123. maddelerinde düzenlenen arama ve elkoymaya ilişkin genel hükümler kullanılmaktadır. Ancak, bilgisayar ve bilgisayar programları ile bilgisayar kütüklerine yönelik işlemlerin genel arama ve elkoyma hükümlerinden ayrı tutulup özel bir hüküm konumundaki CMK m. 134 uyarınca işleme tabi tutulmaları karşısında, teknik açıdan aynı kapsamda değerlendirilmesi gereken ve yukarıda verilen bilgisayar tanımı içerisinde değerlendirilebilecek cep telefonu, cep bilgisayarı gibi işleme, saklama ve iletme özelliğine sahip olan cihazlar ile bünyesinde elektronik veri depolama özelliğine sahip birçok aygıta yönelik arama, kopyalama ve elkoyma işlemlerinin de ek bir hükme

[539] Aydoğan, s. 19; Mustafa İlker Öztürk, s. 62.

[540] Semih Dokurer, "Adli Bilişim", Levent Bayram (Ed.), **Ses Görüntü ve Data İncelemeleri** içinde (239-249), Ankara: Adalet Yayınevi, 2008, s. 242.

gerek olmaksızın CMK'nın 116 ve 123. maddelerinde belirtilen genel arama ve elkoyma hükümleri yerine CMK'nın 134. maddesi uyarınca gerçekleştirilmesi gerektiği kanaatindeyiz[*].

Gerçekten de, bilişim sisteminin unsuru olan pek çok cihazı CMK m. 134 hükmü kapsamında tek tek saymak bir yasada bulunması gereken "açıklık" ve "belirlilik" ilkesine uygun ise de gelişen teknoloji karşısında yasa hükmünün yetersiz bir konuma düşmesine neden olabileceği de açıktır. Bu bakımdan yasa hükmünün uygulama alanının bilişim sistemleri ve bağlı donanımlarını kapsayacak ve de gelişen teknolojinin gerisinde kalmayacak genel bir çerçevede belirlenmesi hatta bir adım daha ileri gidilerek elektronik delil, bilişim suçları, adli bilişim, bilişim sistemlerinde uygulanacak koruma tedbirleri gibi bilişim hukukuna ilişkin hususların -medeni yargılama hukukuna bakan yönleri de kapsayacak biçimde- ayrı bir kanunda ve tereddütlere mahal vermeyecek biçimde yeniden düzenlenmesi gerektiğini düşünmekteyiz.

Son olarak elektronik posta üzerinden elde edilmesi muhtemel elektronik delillerin tedbir kapsamında olup olmadığı hususunun da belirlenmesi gerekmektedir. Buna göre öğretide bir görüş, elektronik posta üzerinden elektronik delil elde edilmesi söz konusu olduğunda CMK m. 134'te düzenlenen tedbir yerine CMK m. 135'te düzenlenen telekomünikasyon yoluyla iletişimin denetlenmesi tedbirine başvurulması gerektiğini savunmaktadır[541].

Benzer bir görüşe göre ise, elektronik postanın adli soruşturmalar bakımından CMK m. 135 uyarınca teknik takibinin mümkün olmasının yanı sıra idari (önleyici) maksatla Polis Vazife ve Selahiyet Kanunu (PVSK) ek m. 7 ve Jandarma Teşkilatı Kanunu ek m.

[*] Aksi görüşte olan Taşkın'a göre ise; cep telefonundan doğrudan doğruya internete girilerek bir bilişim suçu işlendiğinde bu suçun CMK. m. 134'teki soruşturma yöntemine göre soruşturulması mümkün değildir. Zira CMK. m. 134, bilgisayarların aranmasını düzenlemekte, internete girilmek suretiyle bilişim suçu işlemeye müsait cep telefonu ise bilgisayar olmadığı için bu düzenlemenin kapsamına girmemektedir. Şaban Cankat Taşkın, **Bilişim Suçları,** İstanbul: Beta Yayınevi, 2008, s. 173.

[541] Ünal, s. 98-99; Cumhur Şahin, "Telekomünikasyon Yoluyla İletişimin Denetlenmesi-Yargıtay Kararları Çerçevesinde Bir Değerlendirme", **Bilişim Hukuku Konferansı-YARGITAY**, Ankara, 09-10 Ekim 2008, s. 124.

5 uyarınca ve istihbarat amaçlı olarak Milli İstihbarat Teşkilatı Kanunu m. 6 uyarınca da teknik takibe konu olabilir[542].

Öğretide başka bir görüşe göre ise, elektronik posta hizmetinin çoğu zaman web posta hizmeti olarak sunulduğu, web posta hizmetinde, kişiye ait olan alanda kişinin elektronik postalarının saklandığı, teknik olarak göndericinin sunucusundan, alıcısının sunucusuna elektronik postanın ulaşması durumunda, elektronik postanın akış halinin sona erdiği, bu bakımdan, elektronik postanın sunucular arasında nakli esnasında, paket toplama programları sayesinde toplanarak elde edilmesi durumunda CMK m. 135 hükmünün uygulanabileceği, nitekim bu durumda, iletişimin içeriğinin hedeflenmesi nedeniyle bir iletişimin dinlenmesi tedbirinden bahsedilebileceği, ancak elektronik posta hizmetini sunan kurumun bilişim sistemlerinde yer aldığı sırada okunmamış bile olsa CMK m. 134 uyarınca işlem tesis edilmesi gerektiği savunulmuştur[543].

Bununla birlikte CMK'nın 134. maddesinin gerekçesinde belirtildiği üzere elektronik postanın durağan olma niteliğini haiz bir hizmet olması dikkate alınarak şüphelinin elektronik posta kutusunda ya da servis sağlayıcılarda bulunan ve sunucularda kayıtlı olan elektronik postalar üzerindeki elektronik delil elde etme işleminin, CMK'nın 134. maddesinde düzenlenen tedbir hükümleri uyarınca yerine getirilmesi, akışkan vaziyetteki elektronik postalar üzerindeki elektronik delil elde etme işleminin ise CMK'nın 135. maddesine eklenecek bir yasal düzenleme ile iletişimin tespiti tedbiri kapsamında ele alınması yönünde bir çözümün bu hususta tereddütleri ortadan kaldıracağı kanaatindeyiz.

3.2.4. Tedbirin Uygulanma Koşulları

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirinin uygulanacağı suç tipleri bakımından kanunda herhangi bir sınırlayıcı düzenleme bulunmamaktadır. Tedbirin niteliği gereği daha çok bilişim suçları için uygulanabileceği yönünde bir izlenim bulunmakta ise de pekâlâ diğer suçlar bakımından

[542] Ersan Şen, "E-Posta Takibi", **Terazi Hukuk Dergisi,** Cilt. 9, Sayı. 97, (Eylül 2014), s. 88.

[543] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 332-333.

da uygulanabileceği açıktır[544]. Bununla birlikte tedbirin uygulanması kanunda belirli koşullara bağlanmıştır.

3.2.4.1. Suç Dolayısıyla Başlatılmış Bir Soruşturmanın Bulunması

Tedbirin uygulanabilmesi için öncelikle suç dolayısıyla başlatılmış bir soruşturmanın bulunuyor olması gerekmektedir. CMK m. 134/1'de suçun ağırlık derecesi bakımından herhangi bir sınırlama getirilmemesinin yanı sıra madde metninin ilk halinde şüphenin niteliğinden de bahsedilmemekteydi. Bu bakımdan CMK'nın 134/1 maddesinde 21.02.2014 tarihli ve 6526 sayılı Kanunla yapılan değişiklikten önce herhangi bir suçun işlendiğine dair basit (makul) şüphenin varlığı tedbirin uygulanabilmesi için yeterliydi.

Bu durum öğretide; temel hak ve özgürlüklerin korunması bakımından bu tedbirin uygulanmasının ancak "kuvvetli suç şüphesi"nin varlığında[545] ve belli ağırlıktaki suçlar bakımından uygulanması gerektiği[546], tasarıda yer alan *"iki yıl veya daha fazla hürriyeti bağlayıcı cezayı gerektiren cürümler hakkında yapılan soruşturmalarda"* bu tedbirin uygulanabilmesine ilişkin şartın mevcut yasada yer almamasının ise oranlılık ilkesi bakımından ciddi bir eksiklik olduğu[547] yönünde eleştirilere neden olmaktaydı.

CMK'nın 134/1 maddesine 21.02.2014 tarihli ve 6526 sayılı Kanunun 11. maddesiyle yapılan değişiklik ile yukarıda belirtilen eleştiriler kısmen karşılık bulmuştur. Buna göre tedbirin uygulanması "somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı" şartına bağlanmıştır. Bu değişiklik tedbirin uygulanmasını güçleştirmesine karşın temel hak ve özgürlükler bakımından olumlu bir gelişmedir[548].

---

[544] Veli Özer Özbek, Ceza Muhakemesi Hukuku, s. 364.

[545] Muharrem Özen ve İhsan Baştürk, **Bilişim-İnternet ve Ceza Hukuku,** Ankara: Adalet Yayınevi, 2011, s. 147; Ünal, s. 101-102.

[546] Centel ve Zafer, s. 391; Ceza kanunlarında suç olarak tanımlanan her fiil için söz konusu tedbire başvurmanın oranlılık ilkesinin ihlali olacağı hususunda bkz. Özen ve Baştürk, s. 148.

[547] Güray Dağ, "Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması", (**Yayınlanmamış Doktora Tezi**, Marmara Üniversitesi SBE, 2011), s. 237; Benzer bir görüşe göre de; tedbirin uygulanmasında ceza üst sınırı veya katalog suçların uygulanmaması hatalı olmuştur. Bkz. Yaşar ve Dursun, s. 10.

[548] Yusuf Başlar, "Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri", **Uyuşmazlık Mahkemesi Dergisi**, Cilt. 1, Sayı. 3, (Haziran 2014), s. 87-88.

Belirtmek gerekir ki; 21.02.2014 tarihli ve 6526 sayılı Kanunun 9. maddesiyle genel arama tedbirinin düzenlendiği CMK'nın 116. maddesinde yer alan "makul şüphe" ibaresi, CMK'nın 134/1 maddesindeki değişikliğe benzer şekilde "somut delillere dayalı kuvvetli şüphe" olarak değiştirilmiş, ancak kısa bir süre sonra 02.12.2014 tarihli ve 6572 sayılı Kanunun 40. maddesiyle bu maddede yer alan "somut delillere dayalı kuvvetli şüphe" ibaresi tekrar "makul şüphe" şekline dönüştürülmüştür. Bununla birlikte benzer bir geriye dönüş CMK'nın 134. maddesi bakımından gerçekleştirilmemiş ve madde hükmüne getirilen "somut delillere dayanan kuvvetli şüphe" ibaresi aynen muhafaza edilmiştir.

Kuvvetli şüphenin iki hususa yönelik olarak bulunması gerekmektedir. Öncelikli olarak şüphelinin, soruşturmaya konu olan suçu işlediğine ilişkin kuvvetli şüphenin bulunması gerekmektedir. Bu durum, şüphenin belirli bir yoğunluğa ulaşmadan, kişilerin haklarına müdahale teşkil eden koruma tedbirlerine müracaat edilememesinin de bir sonucudur. İkinci olarak ise, kuvvetli şüphenin, şüphelinin kullandığı bilişim sisteminde suç soruşturmasıyla ilgili bir delilin bulunabileceğine ilişkin olmalıdır. Buna göre, şüpheli hakkında soruşturmaya konu olan suçu işlediğine dair kuvvetli şüphe bulunsa bile, şüphelinin kullandığı bilişim sisteminden soruşturulan suça ilişkin bir delil elde edileceği yönünde beklentinin bulunmadığı durumda, söz konusu tedbire başvurulması rasyonel olmayacaktır[549].

Bununla birlikte kanunda bu tedbire başka türlü delil elde etme imkânının bulunmaması halinde başvurulabileceği hususunun belirtilmiş olması karşısında "somut delillere dayalı kuvvetli şüphe" sebeplerinin varlığı şartının da eklenmesiyle uygulama alanı önemli derecede sınırlanmış bu tedbire başvurulması için "belli ağırlıktaki suçlar bakımından uygulanma" şartının da aranması durumunun tedbiri uygulanamaz hale getirmesi de muhtemeldir. Bu nedenle Kanunda son değişiklikle oluşan mevcut düzenlemeye tedbirin "belli ağırlıktaki suçlar bakımından uygulanma" şartının da eklenmesinin gerekli olmadığı düşüncesindeyiz[*].

[549] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 352-353.

[*] Bununla birlikte, CMK m. 134 uyarınca gerçekleştirilen tedbir sonucunda elde edilen verilerden konusu suç teşkil etmese de kamu otoritesini bozacak ve ilgilinin tabi olduğu iç düzeni sarsıcı nitelikte olanları yürütülmekte olan bir disiplin soruşturmasında kullanılabilecektir. Bkz. Kenan Koçer, "Telekomünikasyon Aracılığıyla Yapılan İletişimin

Tedbirin uygulaması bakımından suç tipiyle ilgili de herhangi bir kısıtlama getirilmemektedir. Tedbir, genellikle bilişim suçları ile birlikte anılmakta ise de "bir suç dolayısıyla yapılan soruşturma" ibaresinden de anlaşılacağı üzere bu tedbir bilişim suçlarına özgü olmayıp bilişim suçları da dâhil olmak üzere tüm suçlardan dolayı yapılan soruşturmalarda, bilişim sistemlerinden elektronik delil elde edilmesine yöneliktir[550]. Buna karşın, tedbirin kabahat veya disiplin eylemleri nedeniyle yürütülen soruşturmalar bakımından uygulanması mümkün değildir.

Tedbirin uygulamasında suç tipiyle ilgili bir kısıtlama olmamakla birlikte aramanın soruşturmaya konu bir suç ile ilgili elektronik veriyi elde etmek amacıyla yapıldığının hâkim kararında belirtilmesi gerekir. Bu bağlamda tedbir herhangi bir suç için elde edilmesi muhtemel herhangi bir delil için uygulanamaz. Uygulanacak tedbirde elde edilmesi umulan delilin bireyselleştirilmesi gerekir ki bu söz konusu tedbirin belirliliği bakımından gereklidir. Aksi halde bilişim sistemlerinde herhangi bir sınırlama getirilmeksizin uygulanacak bu tedbir hâkim kararında gösterilen suç ile ilgisi bulunmayan birçok kişisel verinin kolluk denetimine tabi tutulması sonucunu doğuracaktır.

Bununla birlikte uygulanacak tedbirin belirliliğinden kastedilen belirli bir türde dosya ve delilin bilişim sisteminin belirli bir yerinde olacağı gibi spesifik nitelikte bir belirlilik olmayıp tedbirin uygulanacağı bilişim sistemi ile tedbire konu suç arasında bir ilişkinin kurulması şeklindedir. Buna göre, tedbirin uygulanmasına sebep olan suç ile tedbirin uygulanacağı bilişim sistemi arasında kurulan ilişkinin tedbir kararında belirtilmesi gerekir.

Ayrıca bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbiri soruşturma aşaması sona ermeden önce uygulanması gerekmektedir. Nitekim kanunda sanıktan bahsedilmeyip sadece şüpheliden bahsedilmesinin yanı sıra

---

Denetlenmesi, Gizli Soruşturmacı, Teknik Araçlarla İzleme ya da Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El Koyma Suretiyle Elde Edilen Sesli veya Görüntülü Verilerin Disiplin Soruşturmasındaki Kıymeti", **Ceza Hukuku Dergisi,** Sayı. 10, (Ağustos 2009), s. 20.

[550] Ali Parlar ve Muzaffer Hatipoğlu, **5271 Sayılı Ceza Muhakemesi Kanunu Yorumu ve İlgili Mevzuat**, 1. Cilt, Ankara: Yayın Matbaacılık, 2008, s. 532.

tedbire ancak soruşturma aşamasında başvurulabileceği açıkça belirtilmiştir. Bu bakımdan bu tedbire kovuşturma aşamasında başvurulabilmesi mümkün değildir[551].

Bu tedbire başvurmanın amacı, başka türlü elde edilemeyen delili elde etmektir. Kamu davasının açılarak kovuşturmanın başlaması ise kamu davası için yeterli şüphenin oluşmasını sağlayacak delilin elde edildiğini gösterir. Bu durumda ise söz konusu tedbire başvurmaya gerek bulunmamaktadır [552] . Nitekim aleni bir duruşmada mahkemenin bu tedbire karar vermesi durumunda, tedbirden haberdar olan ilgililerin delilleri yok etmesi söz konusu olacak ve bu tedbire başvurmadaki yarar ortadan kalkacaktır[553].

Bununla birlikte, öğretide, madde hükmünde "soruşturma", "hâkim", ve "şüpheli" kavramlarından söz edilmesine karşın "kovuşturma", "mahkeme" ve "sanık" kavramlarından bahsedilmemesi, bu tedbire sadece soruşturma aşamasında başvurulabileceği izlenimini vermekte ise de yargılama sırasında delil toplanmasını engelleyen bir hüküm bulunmaması ve mahkemenin re'sen araştırma yetkisine sahip bulunması nedenleriyle kovuşturma aşamasında da bu tedbire başvurulabilmesinin mümkün olduğu savunulmuştur[554].

3.2.4.2. Son Çare Prensibi

Tedbirin uygulanabilmesi için başka surette delil elde etme imkânının bulunmaması gerekmektedir. Tedbire karar verecek hâkimin öncelikle tedbiri gerekli kılan şüpheyi değerlendiren ve başka surette delil elde etme imkânının bulunmadığını saptayan bir

[551] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1098.

[552] Haluk Çolak ve Mustafa Taşkın, **Açıklamalı-Karşılaştırmalı-Uygulamalı Ceza Muhakemesi Hukuku**, 2. Basım, Ankara: Seçkin Yayıncılık, 2007, s. 607; Osman Yaşar, **Ceza Muhakemesi Kanunu Yeni İçtihatlarla Uygulamalı ve Yorumlu,** I. Cilt, 5. Basım, Ankara: Seçkin Yayıncılık, s. 1339.

[553] Centel ve Zafer, s. 390.

[554] Şahin, Ceza Muhakemesi Hukuku I, s. 268; Ünal, s. 100; Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 318; Parlar ve Hatipoğlu, s. 532; Yaşar ve Dursun, s. 9, Tanrıkulu, s. 400.

gerekçe yazması gerekir[555]. Bu gerekçe, itiraz ve temyiz aşamalarında, verilen tedbir kararının hukuken incelenmesine dayanak teşkil edecektir[556].

Bu tedbir de her koruma tedbirinde olduğu gibi hükümden önce bazı temel hak ve özgürlüklere müdahale etmektedir. Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma özel hayatla doğrudan bağlantılıdır. Zira kişilerin bilişim sistemlerinde sakladıkları kendilerine ilişkin önemli verileri bu tedbir sonucunda deşifre olmaktadır[557].

Telekomünikasyon yoluyla iletişimin denetlenmesi tedbiri ve diğer gizli koruma tedbirlerinde de yer alan bu şart, bu tedbirin diğer tedbirlere nazaran ikincil nitelikte olduğunu göstermektedir[558]. Bu bakımdan, delilleri elde etme ve koruma amacına yönelik diğer tedbirlerde olduğu gibi bu tedbirin de zarar-fayda dengesi gözetilerek ölçülü bir şekilde uygulanması gerekmektedir.

Oranlılık ilkesinin gereği olarak işlenen bir suçu aydınlatmak amacıyla birden fazla tedbirin uygulanmasının söz konusu olduğu durumlarda öncelikle temel hak ve özgürlüklere en az müdahale teşkil eden tedbire başvurulması gerekmektedir. Bir zorunluluk olmadıkça bu tedbir dışındaki yollara başvurularak delil elde edilmeye çalışılmalıdır. Temel hak ve özgürlüklere ağır bir müdahale sonucunu doğuracak olması, bu tedbire son çare olarak başvurulmasının gerekçesini teşkil etmektedir[559]. Bu bakımdan, başka surette delil elde edilememesi ön koşulu temel hak ve özgürlükler açısından önemli ve yerindedir.

Bununla birlikte, bu ön koşulun bilişim suçları ile ilgili yürütülen soruşturmalarda da katı bir şekilde uygulanması elektronik delillere ulaşmada soruna neden olmaktadır. Zira bilişim suçlarında, işin doğası gereği öncelikle şüphelinin bilişim sistemlerinde

[555] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1098; Benzer görüş için bkz. Özen ve Baştürk, s. 150.

[556] Tanrıkılu, s. 406.

[557] Veli Özer Özbek, Ceza Muhakemesi Hukuku, s. 362.

[558] Bahri Öztürk (Ed.), Nazari ve Uygulamalı Ceza Muhakemesi Hukuku Ders Kitabı, s. 640.

[559] Şahin, Ceza Muhakemesi Hukuku I, s. 288-289.

arama tedbirlerinin uygulanması gerekmektedir. Bu bakımdan, CMK m. 134 uyarınca önce başka delillerin var olup olmadığının araştırılması, sonra başka delil elde etme imkânının olmadığının ortaya konulması ve akabinde şüphelinin bilişim sistemlerinde arama, kopyalama ve elkoyma işlemlerine izin verilmesi, bilişim suçlarının soruşturulmasında sıkıntıya neden olabilir[560].

Ancak son çare prensibinin bilişim suçları bakımından daha geniş yorumlanması, bu bağlamda, başka surette delil elde etme imkânının bulunmaması şartının bilişim suçları bakımından soruşturmanın hemen başında anlaşılabildiği durumlarda, başka bir ifadeyle genel arama ve elkoyma tedbirinin uygulanması halinde de delil elde etme imkânının olmadığının baştan öngörülebildiği hallerde, bu şartın gerçekleştiğinin kabulü ile başkaca delil araştırmasına gidilmeksizin bu tedbire başvurulması durumunun CMK'nın 134. maddesine özel bir düzenleme yapılmasına gerek duyulmaksızın sorunun çözümüne katkı sağlayacağı kanaatindeyiz. Nitekim uygulamada da maddenin yorumlanmasının bu şekilde yapıldığı görülmektedir.

3.2.4.3. Cumhuriyet Savcısı Talebi ve Hâkim Kararı

Tedbir, Cumhuriyet savcısının talebi üzerine hâkim kararı ile uygulanabilmektedir. Tedbir kararını verecek hâkim ise soruşturmanın yürütüldüğü yer sulh ceza hâkimidir. Ancak soruşturma Cumhuriyet savcısı tarafından yürütülmekte ve bu tedbir sadece soruşturma aşamasında uygulanabilir nitelikte olması nedenleriyle hâkimin, savcılık talebi olmaksızın re'sen bu tedbirin uygulanmasına karar vermesi mümkün değildir.

Kanun koyucu eğer farklı bir yaklaşımı benimsemiş olsaydı CMK m. 75 (şüpheli ve sanığın beden muayenesi), CMK m. 76 (diğer kişilerin beden muayenesi), CMK m. 119 (arama), CMK m. 127 (elkoyma), CMK m. 129 (postada elkoyma), CMK m. 135 (iletişimin tespiti), CMK m. 139 (gizli soruşturmacı tayini), CMK m. 140/2 (teknik araçlarla izleme) tedbirlerinde olduğu gibi madde metnine "hâkim kararıyla veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının emriyle" ifadesini madde

[560] Karagülmez, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, s. 391; Henkoğlu, s. 18; Taşkın, s. 171; Tan, http://mbasic.facebook.com/notes/gazi-%C3%BCniversitesi-adli-bili%C5%9Fim-anabilim-dal%C4%B1/adli-bili%C5%9Fim-computer-forensic-aydo%C4%9Fantan/ 502561823148516/?refid=17 (06 Nisan 2014).

metnine koyabilirdi. Oysaki tedbirin uygulanması ancak Cumhuriyet savcısının istemi üzerine hâkim kararı ile uygulanabilecektir[561].

Tedbirin, soruşturma aşamasında ve ancak Cumhuriyet savcısının talebi üzerine hâkim kararı ile uygulanabilmesi ve maddede gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının yazılı kararı ile tedbirin uygulanabileceğine cevaz verilmemesi, söz konusu tedbirin sıkı koşullara bağlı şekilde düzenlendiğini göstermektedir. Düzenleme bu haliyle temel hak ve özgürlükler bakımından güvence sağlamaktadır[562].

Bununla birlikte Taşkın'a göre; CMK m. 163'te belirtilen hallerde bu tedbir, hâkim tarafından Cumhuriyet savcısının talebi olmaksızın re'sen uygulanabilecektir. Buna göre; CMK m. 163 uyarınca suçüstü hali veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısına ulaşılamaması veya olayın genişliği itibariyle Cumhuriyet savcısının iş gücünü aşan durumlarda sulh ceza hâkimi de bütün soruşturma işlemlerini yapabilmektedir. Bu bağlamda yazara göre; küçük bir ilçede tek Cumhuriyet savcısının varlığı durumunda Cumhuriyet savcısının otopsi işlemlerini yapma zorunluluğunun bulunduğu ve aynı anda derhal harekete geçilmemesi halinde bir bilişim suçunun failinin izini kaybettireceği durumda hâkim CMK m. 163 uyarınca söz konusu tedbiri re'sen uygulayabilecektir[563].

Kanaatimizce CMK m. 163 uyarınca soruşturma işlemlerini Cumhuriyet savcısının yerine yürüten sulh ceza hâkiminin tedbirin uygulanmasına re'sen karar vermesi, tedbirin ancak Cumhuriyet savcısının talebi ve hâkimin kararı ile uygulanabileceğini düzenleyen madde metnine uygun değildir. Böyle bir durumda, soruşturma işlemlerini Cumhuriyet savcısının yerine yürüten sulh ceza hâkimi ancak söz konusu tedbirin uygulanmasını talep edebilir. Talebin değerlendirilerek karara bağlanması ise başka bir sulh ceza hâkimi tarafından yerine getirilmelidir.

PVSK m. 9 uyarınca gerçekleştirilen önleme araması kapsamında bilişim sistemlerinde arama yapılıp yapılmayacağı hususu üzerinde de durmak gerekmektedir. Kural olarak

[561] Taşkın, s. 168.

[562] Ünal, s. 105.

[563] Taşkın, s. 168-169.

hâkim kararı ile ve fakat gecikmesinde sakınca bulunan hallerde mahallin en büyük mülki amirinin yazılı emriyle uygulanabilen önleme araması ile bilişim sistemlerinin aranamayacağı kanaatindeyiz. Cumhuriyet savcısının gecikmesinde sakınca bulunan hallerde bile tek başına tedbirin uygulanmasına karar veremediği bir durumda önleme araması ile böyle bir aramanın yapılması tedbirin düzenlenme amacına da ters düşecektir. Kaldı ki, önleme aramalarının adli arama gibi uygulandığı ülkemizde böyle bir uygulamaya cevaz vermek temel hak ve özgürlükler bakımından ayrı bir sorun teşkil edecektir.

Son olarak belirtmek gerekir ki; Kanun, bu tedbirin Cumhuriyet savcısının doğrudan vereceği karar ile uygulanmasına cevaz vermemekte ise de; bilişim teknolojilerindeki hız ve değişkenlik, delillerin derhal ele geçirilmesini gerektirdiğinden delillerin geç elde edilmesinde sakınca bulunduğu hallerde sonradan hâkim onayına sunulmak kaydıyla Cumhuriyet savcısının kararı ile de bu tedbirin uygulanabilmesi yönünde bir kanun değişikliği yapılması yerinde olacaktır.

3.2.4.4. Şüphelinin Kullandığı Bilişim Sistemlerinde Uygulanması

Suç soruşturması başlamış olmasına karşın, henüz şüpheli statüsünde bir kişinin mevcut olmaması durumunda CMK m. 134 uyarınca tedbir uygulanamayacaktır[564]. Bu bakımdan bu tedbir ancak şüphelinin kullandığı bilgisayar, bilgisayar programları ve kütükleri üzerinde uygulanabilecektir. Sanık statüsüne geçmiş kişiler veya üçüncü kişilerin bilgisayar, bilgisayar programları ve kütükleri üzerinde ise bu tedbir uygulanamaz. Nitekim kanun koyucu eğer şüphelinin dışındaki kimseler hakkında bu tedbirin uygulanmasını öngörmüş olsaydı madde hükmünde bunu açıkça belirtirdi. Buna göre, tedbirin uygulama alanını şüphelinin dışındaki kimseler aleyhinde genişletmek kanun koyucunun özel olarak ve temel hak ve özgürlükler lehine dar bir alanda düzenlediği tedbirin yapısına uygun düşmemektedir.

Diğer taraftan maddede şüphelinin "sahip olduğu" ibaresine değil şüphelinin "kullandığı" ibaresine yer verilmiştir. Kişilerin işlemiş oldukları suçlarda kendi adlarına kayıtlı olan veya faturalardan kendileri adına alındığı tespit edilebilecek durumdaki

[564] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 318.

bilgisayar, bilgisayar programları ve kütüklerini kullanmayabilecekleri hususu dikkate alındığında madde metninin yerinde olduğu görünmektedir. Eğer sadece "sahip oldukları" denilmiş olsaydı tedbirin uygulama alanı oldukça daraltılmış olacaktı[565].

Nitekim Yargıtay bir kararında *"...Olay tarihinde sanıkla maktulun internet üzerinde sohbet ettikleri söylenen kafede sanığın 'Kaan' kod adıyla 21 no.lu masada ve maktulün kullandığı belirtilen bilgisayarların ve kullandıkları programın saptanarak bilgisayarlarda ve bilgisayar programının merkezi sisteminde sohbet kaydının mevcut olup olmadığı ve içeriğinde hakaret ve tahrik edici sözler olup olmadığı tespit edilmeden yazılı şekilde hüküm kurulması usule aykırı bulunduğundan hükmün BOZULMASINA, oy birliği ile karar verildi…*[566]" demek suretiyle, başkasına ait olması durumunda da şüpheli tarafından kullanılan bilişim sistemlerinde arama yapılabileceğine karar vermiştir.

Bununla birlikte, şüpheliye ait olmayan ve fakat onun tarafından kullanılan bir bilişim sistemi hakkında söz konusu tedbirin uygulanmasının talep edildiği durumlarda, ilgili talepte şüpheli ile kullandığı belirtilen bilişim sistemi arasındaki bağın kurulması, sulh ceza hâkiminin ise bu hususu denetledikten sonra öyle olduğuna kanaat getirmesi halinde tedbirin uygulanmasına karar vermesi gerekmektedir.

Diğer taraftan uzaktan erişim veya çok kullanıcılı erişim şeklindeki "sanal kullanma" durumlarında tedbirin uygulanabilip uygulanamayacağı hususu üzerinde de durmak gerekmektedir. Öncelikle, şüphelinin bir bilişim sistemini kullanarak uzaktan erişim sayesinde başka bir bilişim sistemine girmesi ve bu bilişim sistemini bazı kötü niyetli yazılımlar ile kendi isteği doğrultusunda kullanması durumunda uzaktan erişilen bilişim sistemi bakımından tedbirin uygulanabilip uygulanamayacağı hususunun belirlenmesi gerekir. Belirtmek gerekir ki, işlendiği iddia olunan suçun delillerine, uzaktan erişilen bilişim sistemlerinde ulaşılabilmesi mümkündür. Ancak, şüpheli tarafından kullanılan ifadesinin bu kadar geniş şekilde anlaşılması durumunda, özellikle internete bağlı bilişim sistemlerinde, ulaşılan her bir bilişim sisteminin, bağlantı kurulan her bir

[565] Çolak ve Taşkın, s. 608.

[566] Yargıtay 1. CD. 14.11.2005. E. 2005/3891, K. 2005/3230, Bkz. Ölmez, s. 50.

sunucunun da bu tedbire tabi tutulacağı sonucuna varılır ki, bu sonucun temel hak ve özgürlüklere ciddi şekilde zarar vereceği açıktır[567].

Sanal kullanımın ikinci şekli ise, çok kullanıcılı işletim sistemlerinde, kişinin hesabına girerek yapmış olduğu kullanımdır. Burada, fiziki olarak tek bilgisayar kullanıldığı halde, bilgisayar sanal olarak birçok parçaya ayrılmıştır. Kullanıcı hesabı, çok kullanıcılı sistemlerde sadece belirlenmiş olan bazı dosyalarla ilişkilidir ve kullanıcı sadece o dosyalar üzerinde işlem yapabilmektedir. Bu bakımdan, çok kullanıcılı işletim sistemlerinde de ancak kişi tarafından kullanılan hesaba ait veriler üzerinde inceleme yapılabilmeli ve söz konusu veriler kullanılabilmelidir. Bunun dışında, sanal olarak bölünmüş bir sistemin tamamı üzerinde tedbirin uygulanması doğru olmayacaktır[568].

Tedbirin mağdur veya şikâyetçinin bilişim sistemlerinde uygulanıp uygulanamayacağı hususu üzerinde de durmak gerekmektedir. Kanun metninde şüphelinin kullandığı bilişim sistemlerinden bahsedilmesine karşın mağdur veya şikâyetçiye ait bilişim sistemlerinden bahsedilmemektedir. Bununla birlikte özellikle bilişim suçlarında mağdur veya şikâyetçinin bilişim sistemlerinden elde edilecek elektronik veriler şüpheliye ulaşmak açısından öncelikle müracaatı gereken deliller niteliğinde olabilmektedirler.

Kanaatimizce bilişim sistemlerinin mağdur veya şikâyetçiye ait olması koşuluyla ve mağdur veya şikâyetçinin açık rıza beyanı doğrultusunda gerekli arama, kopyalama ve muhafaza işlemleri CMK m. 134'te belirtilen koşullar gözetilmeksizin gerçekleştirilebilir. Ancak bu şekilde gerçekleştirilecek işlemler artık CMK m. 134 anlamında bir tedbir uygulaması olarak değil CMK m. 160/2 kapsamında Cumhuriyet savcısının maddi gerçeğin araştırılması ve adil yargılamanın yapılması için emrindeki kolluk marifetiyle gerçekleştirmekle yükümlü bulunduğu delilleri toplama ve muhafaza altına alma yükümlülüğü kapsamında değerlendirilmelidir.

CMK m. 134 uyarınca arama yapılacak bilişim sisteminin şüpheli tarafından kullanılması bir şart olarak belirtilmiş ise de söz konusu bilişim sisteminin kamu tüzel

[567] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 321.

[568] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 321-322.

kişilerine veya özel kişilere ait olması arasında bir fark gözetilmemiştir. Bu durumda, şüphelinin kullanmış olduğu belirlendikten sonra kamu tüzel kişiliğine ait olan ve gizlilik dereceli bilgiler barındıran bilişim sistemlerinde de söz konusu tedbir uygulanabilecektir[569].

Son olarak kamu görevlilerinin çalıştıkları kurum tarafından verilen bilişim sistemleri üzerinde kurum amiri veya teftişle görevli kişi tarafından arama işleminin yapılması için CMK m. 134 uyarınca tedbir kararına ihtiyaç olup olmadığı hususu üzerinde de durmak gerekmektedir. Öğretide bir görüşe göre; kurum tarafından verilen bilişim sisteminin özel değil kurum işlerinde kullanılmak üzere verildiği, bu bilişim sistemlerinin her zaman geri alınabileceği, bu bakımdan cihazın içeriğinin incelenmesi için bu bilişim sisteminin kullanıcısı olan kamu görevlisinin rızasına dahi gerek duyulmaksızın yetkili amir veya onun adına hareket eden kimsenin emri ile inceleme yapılabileceği savunulmuştur[570].

Buna karşın bizim de katıldığımız başka bir görüşe göre ise, devlet kurumlarında görev yapan kamu görevlilerinin, kurum tarafından kendilerine verilen bilişim sistemleri üzerinde de mahremiyet hakları bulunmaktadır. Bununla birlikte bu mahremiyet hakkı, ilgili kurum tarafından ilan edilen ve periyodik olarak uygulanan bilişim sistemleri üzerindeki denetimleri engellemeyecektir. Ancak bu denetim, bilişim sisteminin kurum politikaları uyarınca kullanılıp kullanılmadığına yönelik olmalıdır. Bu bakımdan, kurum amirleri, bir suç ihbarı üzerine kamu görevlisi tarafından kullanılan ve fakat kuruma ait olan bilişim sistemleri üzerinde delil olarak kullanılmak üzere veri araması yapamaz. Bir suçun işlendiği haber alındıktan sonra sistem kurum amirleri tarafından başlatılan delil arama faaliyetleri, kişilerin mahremiyet beklentilerinin bulunduğu alanda yapıldığı takdirde elde edilen deliller hukuka aykırı kabul edilmeli ve değerlendirme dışı bırakılmalıdır[571]. Bu bakımdan böyle bir arama ve elkoyma faaliyeti CMK m. 134 uyarınca soruşturma birimlerince gerçekleştirilmelidir.

---

[569] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 398.

[570] Yavuz Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Cilt. 12, Özel Sayı, (2010), s. 1410.

[571] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 340.

3.2.5. Tedbirin Uygulanması

CMK m. 134/1 hükmü uyarınca yukarıda belirtilen koşulların varlığı halinde öncelikle şüphelinin bilgisayar, bilgisayar programları ve kütüklerinde arama yapılarak suçla ilgili elektronik delilin varlığı araştırılacak, bu delile ulaşıldığı takdirde de kopyalanabilecek ve ayrıca elde edilen ve kopyalanan delil çözülerek metin haline getirilebilecektir.

CMK m. 134/1 kapsamında bilgisayar, bilgisayar programları ve kütüklerinde yapılacak arama adli bilişim kurallarına uyularak gerçekleştirilmeli ve delillerin zarar görmesi engellenmelidir. Delil mahiyetinde elektronik kayıtların tespiti durumunda bu kayıtların birebir kopyası (imajı) çıkartılmalı ve bu kayıtlar çözülerek metin haline dönüştürülmelidir. Bu fıkra hükmü uyarınca metin haline dönüştürülen bilgisayar kayıtları delil niteliğinde olduğu değerlendirilen ve kopyası alınan kayıtlardan ibarettir. Belirtmek gerekir ki, bu fıkra hükmüne göre gerçekleştirilen birebir kopyalama işlemi akabinde sistemin hash (veri bütünlük) değerinin alınması gerekmektedir.

Bununla birlikte, CMK m. 134/2'ye göre, bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilecektir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde ise, elkonulan cihazların gecikme olmaksızın iadesi yapılacaktır. Bu fıkra hükmünde belirtilen kopyalama işlemi de birebir kopyalamadır ve bu işlemin akabinde de sistemin hash değeri alınmalıdır.

Esasen CMK m. 134/2 hükmü olmasaydı da bilgisayar, bilgisayar programları ve bilgisayar kütüklerine genel hükümler uyarınca elkoymak yine de mümkün olurdu. Ancak söz konusu hükümle amaçlanan asıl husus, bilişim sistemlerine elkoymaksızın da verilere ulaşmanın mümkün olduğu hallerde (CK m. 134/5), bilişim sistemlerinin tümüne elkonularak kişilerin bilişim sistemlerine erişiminin engellenmesini önlemektir[572].

Bazı bilişim sistemlerine ait şifrelerin çözülmesi zaman alabildiği için kanun koyucu şifre içeren bilişim sistemlerinin yer aldığı araçlara elkoyma yetkisini vermiştir.

[572] Ünver ve Hakeri, 1. Cilt, s. 579.

Bununla birlikte kanun koyucu, oranlılık ilkesinin bir gereği olarak bilgisayar, bilgisayar programları ve kütüklerine elkoyma tedbirinin uygulanabilmesi için şifrenin çözülememesinden dolayı sisteme girilememesi veya gizlenmiş bilgilere ulaşılamaması koşulunun varlığını aramıştır[573].

Bununla birlikte madde metninde belirtilen bilişim sistemlerine elkoyma şartının bilişim sistemlerindeki şifrenin çözülememesine bağlanması doğru bir yaklaşım tarzı değildir. Bu bağlamda, bir bilgisayardaki verilere erişim için bu bilgisayarı çalışır hale getirmek ve bilgisayardaki işletim sistemini açmak gerekmemektedir. Bu bilgisayardaki sabit diskin fiziken sökülerek içerisinde bulunan verilerin başka bir medyaya kopyalanması mümkündür[574].

Ayrıca değişik işletim sistemleri, kullanıcı şifresi ile sisteme ulaşılamadığı sürece, sabit diske erişimi engelleyebilmektedir. Bu bakımdan, kullanıcı şifresi olmadan sistem belleğine ulaşılamadığı, birebir kopyalamanın yapılamadığı ve şifrenin de ilgili kişi tarafından aramayı yapan görevlilere verilmediği hallerde elkoyma işlemi yapılabilecektir[575].

Şüphelinin bilişim sistemlerindeki suçla ilgili elektronik delili, veri gizlemek için tasarlanmış bazı bilgisayar programlarını kullanmak suretiyle gizlemesi veya silmesi mümkündür. Bu gizlenmiş veya silinmiş bilgilere olay yerinde ulaşılamaması durumunda da elkoyma tedbirine başvurulabilecektir. Her ne kadar madde metninde "silinmiş" bilgilerden bahsedilmemekte ise de, maddede geçen "gizlenmiş" bilgilerin "silinmiş" bilgileri de kapsayacak şekilde geniş yorumlanması gerektiği kanaatindeyiz.

Diğer taraftan elkoyma işleminin bilişim sistemlerine ait şifrelerin çözülememesi veya gizlenmiş bilgilere ulaşılamaması şartına bağlanmış olması uygulamada başka sorunlara da neden olmaktadır. Zira bilgisayar veya çıkarılabilir depolama aygıtları ve bunların içerisindeki verilerin çok fazla olduğu durumlarda kopyalama işleminin çok uzun zaman alabildiği ve bu nedenle de uygulamada kolluğun şifrenin çözülebilir olup olmadığına

[573] Veli Özer Özbek, Ceza Muhakemesi Hukuku, s. 365.

[574] Aydoğan, s. 112.

[575] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 367-368.

bakmaksızın şifrenin çözülemediğine ilişkin tutanak tutmak suretiyle elkoyma işlemini gerçekleştirerek kopyalama işlemini olay mahalli yerine kolluk birimlerine ait laboratuvarlarda gerçekleştirdikleri görülmektedir. Bu bakımdan, uygulamada karşılaşılan bu sorunun çözümü yönünde yasal düzenleme yapılması gerekmektedir.

Elkoyma işleminden sonra şifrenin çözümünün yapılması ve gerekli kopyalama işleminin yerine getirilmesi durumunda elkonulan cihazların gecikme olmaksızın iadesi gerekmektedir. Madde metninde sınırlayıcı bir süreden bahsedilmemekle birlikte bahse konu işlemlerin makul bir sürede tamamlanarak iade işleminin gerçekleştirilmesi gerekmektedir.

Nitekim Avrupa İnsan Hakları Mahkemesi bir kararında (Smirnov vs./Rusya), müştekinin bilgisayarının 6 günden daha uzun bir süre içerisinde alıkonulmasının bir nedeninin olmadığı, bilgisayarın müştekinin mesleğini ifa etmesi için bir araç olduğu ve elkoyma-müsadere işlemlerinin onun mesleki faaliyetlerini bozduğu, bu nedenle Rus adli makamlarının toplumun genel çıkarları ve avukatın hakları arasındaki adil dengeye müdahalede başarısız olduğu ve yapılan işlemin hukuka aykırı olduğuna hükmetmiştir[576].

Diğer taraftan CMK m. 134/2'de belirtilen bilişim sistemlerine "şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması hali"nin bulunmaması durumunda içerisinde suç unsuru bulunan elektronik medyaya CMK m. 134/2 uyarınca elkoyma işleminin yapılamaması, dolayısıyla içerisinde suç unsuru bulunan elektronik medyanın şüphelide kalmaya devam etmesi ya da elkoyma işlemi gerçekleşse de gerekli işlemler tamamlandıktan sonra bu medyanın şüpheliye iade edilmesi konusu da ayrı bir sorun teşkil etmektedir.

Öğretide içerisinde suç unsuru bulunan elektronik medyanın şüpheliye verilmemesi, verme işleminin verilerin kopyasını verme şeklinde yapılması, verilerin kopyasının şüpheliye verileceği durumda da bu kopyanın içerisinde bulunan suça konu verilerin silinerek şüpheliye iade edilmesi gerektiği ileri sürülmüş[577] ise de, silinen verilerin

[576] Ünal, s. 130-131.

[577] Ünal, s. 122; Ahi, "Adli Bilişim Nedir ?", http://www.bilisimhukuk.com/2009/07/adli-bilisim-nedir/ (04 Mayıs 2014).

tekrar getirilebileceği düşünüldüğünde söz konusu görüşün mevcut soruna etkin bir çözüm getirmeyeceği kanaatindeyiz.

Öğretideki başka bir görüşe göre ise, bu gibi durumlarda bilgisayar, bilgisayar programları ve bilgisayar kütüklerine, bir suçun aracı olarak kullanılmaları nedeniyle, ileride müsadere edilebilecek eşya sıfatına haiz olduklarından CMK m. 127 uyarınca elkonulabilmektedir [578] . Benzer bir görüşe göre ise, burada eşya müsaderesinin konusunu oluşturan mal varlığı değeri mevcut olduğu için CMK m. 123 uyarınca elkoyma işlemi yapılması gerekmektedir[579].

Gerçekten de, özellikle suçta kullanılan bir silahın şüpheliye iade edilmesinde olduğu gibi içerisinde (çocuk pornografisi, fikri haklara aykırı şekilde yapılan kopya programlar, kişilerin kredi kartı bilgileri vb.) suç unsurunun bulunduğu bir elektronik medyanın kendisinin veya dijital kopyasının şüpheliye geri verilebileceği anlamını taşıyan mevcut düzenlemenin uygulanabilir olmadığı ve bir an önce değiştirilmesi gerektiği düşüncesindeyiz.

Bununla birlikte bu konudaki sorunu çözecek yasal bir düzenleme yapılıncaya kadar Avrupa Konseyi Siber Suç Sözleşmesinin 19/3-d maddesi yol gösterici olarak benimsenebilir. Buna göre, Sözleşmenin 19/3-d maddesinde suç unsuru veya suç aracı olan verilerin erişilemez ve kullanılamaz hale getirilmesi ve hatta kopyaları alındıktan sonra silinmesi düzenlenmiştir. Bu tip verileri barındıran elektronik medyadaki verilerin kopyaları alındıktan sonra silinmesi sonrasında elektronik medyanın şüpheliye iade edilmesini etkili bir çözüm yolu olarak benimsememekle birlikte verilerin erişilemez veya kullanılamaz hale getirilmesi kapsamında söz konusu verilerin bulunduğu medyaların şüpheliye iade edilmemesi ve şartları varsa yargılama sonrasında müsaderesine karar verilmesi gerektiği kanaatindeyiz.

Sözleşmenin 19/3-d maddesi uyarınca verilerin erişilemez veya kullanılamaz hale getirilmesi kapsamında elektronik verileri barındıran cihazları geri vermeme yolunun

[578] Özcan Özbey, "Adli Bilişim ve Sayısal Deliller (5271 Sayılı CMK'nın 134. Maddesi)", **Yargıtay Dergisi,** Cilt. 36, Sayı. 3, (Temmuz 2010), s. 121; Ünver ve Hakeri, 1. Cilt, s. 580.

[579] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 377; Benzer görüş için bkz. Veli Özer Özbek ve Diğerleri, s. 398.

benimsenmesi, soruşturmada görev alan ve elkonulan cihazların gecikme olmaksızın iade edilmesinde sorumluluğu bulunan görevliler açısından da hukuki güvence sağlayacaktır. Zira Sözleşmenin TBMM tarafından uygun bulunarak 02.05.2014 tarihinde yürürlüğe girmesi, Anayasa'nın 90/5 maddesi uyarınca Sözleşmenin gerek -sonra yürürlüğe giren- kanun hükmünde sayılması gerekse usulüne göre yürürlüğe konulmuş temel hak ve özgürlüklere ilişkin milletlerarası andlaşmalarla kanunların aynı konuda farklı hükümler içermesi nedeniyle çıkabilecek uyuşmazlıklarda milletlerarası andlaşma hükümleri esas alınacağına ilişkin amir hükmün bulunması nedenleriyle bahse konu sorunun çözümünde temel hak ve özgürlüklere ilişkin milletlerarası andlaşma olduğunda şüphe duyulmayan Sözleşme hükümlerinin esas alınması yönündeki çözüm yolunun benimsenmesi yerinde olacaktır.

Belirtmek gerekir ki, söz konusu tedbir, bilişim sistemlerinin toplum yaşantısındaki rolünün giderek artması neticesinde daha fazla müdahale teşkil eden bir tedbir haline dönüşmektedir. Nitekim bir kimsenin kişisel bilişim sistemlerine elkonularak, uzun süre kişinin bu bilişim sistemlerini kullanmaktan mahrum edilmesinin verdiği zarar ile tüm işlemlerin bilişim sistemleri aracılığıyla yürüten bir ticari işletmenin bilişim sistemlerini kullanmaktan mahrum edilmesinin verdiği zarar aynı değildir. Bu nedenle bilişim sistemlerine elkoyma işlemi olabildiğince dikkatli ve olay bazlı değerlendirilmelidir[580].

Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılmalıdır (CMK m. 134/3). Elkoyma işlemi nedeniyle bazı bilgilerin kaybolması ve bu sebeple şüphelinin mağdur olmasının önlenmesi amacıyla yedekleme yapılması zorunludur. Nitekim kanunda elkoyma sırasında yedekleme yapılması, şüpheli talebine veya görevlilerin gerek duymasına bırakılmamış, zorunlu olarak yedekleme yapılması hükme bağlanmıştır. Bu bakımdan, bilgilerin kaybolması veya bir zarar meydana gelmesi söz konusu olmasa bile yedekleme yapılmak zorundadır. Bu önlemin bir amacı da delil uydurmanın önüne geçmektir[581]. Bu hüküm,

[580] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 360.

[581] Çolak ve Taşkın, s. 609.

uygulamada bilgisayar ve ürünlerinin dış müdahaleye uğrama olasılığına karşı son derece önemli bir hükümdür[582].

Diğer taraftan kanun metninde kullanılan "elkoyma işlemi sırasında" ifadesini, incelemeye başlamadan önce şeklinde yorumlamak yerinde olacaktır. Zira elektronik veriler üzerinde inceleme yaparken verilerin zarar görmesi, değişmesi veya yok olması muhtemeldir[583].

CMK m. 134/3'te bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesinin yapılacağından bahsedilmesine karşın bilgisayar programlarına elkonulması durumunda yedekleme işleminden bahsedilmemektedir. Bilgisayar programları genellikle bilgisayarın sabit diskinde bulunduklarından bilgisayardaki tüm verilerin yedeklemesi bilgisayar programını da kapsayacaktır[584].

Bununla birlikte bilgisayar programları, bilgisayar dışındaki veri saklama birimlerinde de bulunabildiğinden uygulamada karşılaşılabilecek sorunların çözümü bakımından bu hususta yasal düzenleme yapılması gerekmektedir. Ayrıca, bilişim sistemlerinin incelenmesi sırasında MSN kaydı veya başka bir iletişime ait bir kayda rastlanması durumunda bu verilerin de yedeklenip yedeklenemeyeceği madde hükmünde açık değildir. Bu konuyla ilgili olarak yeni bir hâkim kararının gerekip gerekmediği hususundaki duraksamayı ortadan kaldıracak bir düzenlemenin yapılması da yerinde olacaktır.

CMK m. 134/3 uyarınca elkoyma işlemi esnasında sistemdeki bütün verilerin yedeklenmesi işlemi sonucunda bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilmeli ve bu husus tutanağa geçirilerek imza altına alınmalıdır (CMK m. 134/4). Madde metninin ilk halinde bu durum şüpheli ya da vekilinin istemi durumunda gerçekleşmekteydi. Şüphesiz bu durum savunma hakkının kısıtlanması anlamını taşımaktaydı. Ancak CMK'nın 134/4 maddesinde 6520 sayılı Kanunun 11. maddesiyle

[582] A. Güçlü Sevimli, "Bilgisayar ve Bilgisayar Kütüklerine El Konulması ve Uygulamadaki Sorunlar", **İstanbul Barosu Dergisi**, Cilt. 81, Sayı. 3, (Mayıs-Haziran 2007), s. 997.

[583] Veli Özer Özbek, Ceza Muhakemesi Hukuku, s. 365.

[584] Ünal, s. 119.

yapılan yerinde bir değişiklik ile herhangi bir talebe gerek duyulmaksızın yedekleme işlemi sonucunda elde edilen yedekten bir kopyanın şüpheli ve vekiline verilmesi zorunludur.

Söz konusu fıkrada belirtilen yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilmesi işleminin tutanağa geçirilerek imza altına alınmasının amacı elde edilen elektronik delile ilişkin hukuka aykırılık iddialarını bertaraf etmektir. Bu bakımdan, kopyanın şüpheliye veya vekiline verilmesi işlemi olay yerinde yerine getirilmeli, bunun yerine getirilememesi durumunda ise adli bilişim inceleme ve analiz işlemlerine başlamadan önce bu işlem tamamlanmalıdır.

Madde metninde geçen "vekil" kavramının "şüpheliyi temsil eden kişi" şeklinde geniş yorumlanması gerekmektedir. Bu bağlamda, bu kavramın içerisine şüpheli müdafiinin yanı sıra -özellikle günümüzde bilişim suçlarının küçük çocuklar tarafından da işlenebildiği dikkate alındığında- suça sürüklenen çocuklar bakımından anne-baba veya evde bulunan diğer yasal temsilcilerin de dâhil edilmesi gerekmektedir[585].

Bununla birlikte, içerisinde suç unsuru bulunan medyanın bir kopyasının da şüpheliye verilip verilmeyeceği[*], şüpheliye hangi formatta ve nasıl bir medya üzerinde verileceği, bu medyayı kimin sağlayacağı, diğer taraftan bu yedeklerin kimin tarafından, nasıl ve ne kadar süreyle muhafaza edilecekleri, veri depolama aygıtlarının kapasitelerinin giderek arttığı dikkate alındığında ilgili birimlerde bu kadar medyayı saklayacak depolama ünitelerinin bulunup bulunmadığı gibi hususlar Kanunda belirtilmemiş olması sebebiyle uygulamada soruna neden olduğundan bu ve benzeri hususların açıklığa kavuşturulması gerekmektedir[586].

Bilgisayar veya bilgisayar kütüklerine elkonulmaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyasının alınması mümkündür. Boş alanların ve silinen

---

[585] Ünal, s. 123.

[*] Yukarıda belirtilen Avrupa Konseyi Siber Suç Sözleşmesi'nin 19. maddesinin öncelikle uygulanarak "içerisinde suç unsuru bulunan elektronik medyanın şüpheliye iade edilmemesi" yönündeki çözümün yolunun aynı nitelikteki medyanın kopyasının verilip verilmeyeceği hususundaki sorun bakımından da uygulanabilir bir çözüm yolu olduğu kanaatindeyiz.

[586] Hakan Hekim ve Oğuzhan Başıbüyük, "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları", **Uluslararası Güvenlik ve Terörizm Dergisi**, Cilt. 4, Sayı. 2, (2013), s. 152.

verilerin de kopyasının alınması gerektiğinden madde metnine göre yapılacak kopyalama işleminden kastedilen birebir kopyalama işlemidir. Bu durumda kopyası alınan verilerin kâğıda yazdırılarak, bu hususun tutanağa bağlanması ve ilgililer tarafından imza altına alınması gerekmektedir (CMK m. 134/5).

Belirtmek gerekir ki; adli bilişim yöntemlerine göre bir bilgisayarın veya bilgisayar kütüğünün yedeği alınırken, sistem sadece kapalıyken değil aynı zamanda sistem açıkken de yedek alınabilmektedir. Sistem açıkken yedek alma işlemi sırasında çok dikkatli olunmalıdır. Sistem açıkken yedek alma işlemi sırasında hem sistemin çalışmasına zarar verilmemesi hem de doğru ve gerekli bölümlerin yedeğinin alınması gerekmektedir[587].

CMK m. 134/5 hükmü sayesinde şüpheli konumundaki kişilerin bilgisayar sistemini, programlarını ve verilerini kullanmaya devam edebilmeleri sağlanmıştır. Tutanak altına alınarak yedeklenen verilerin değiştirilmesi, bu aşamadan sonra bir anlam taşımamaktadır. Uygulamada, kolluk görevlilerinin bu hükmü üç kopya çıkartarak, birini şüpheliye vermek, birini incelemek, diğerini ise daha sonra ortaya çıkabilecek uyuşmazlıkların giderilmesi için ayrı bir birimde koruma altına almak şeklinde yerine getirdikleri görülmektedir[588].

Birebir kopyalama işlemi sırasında alınan hash değerinin de söz konusu tutanağa kaydedilmesi gerekmektedir. Buna ilişkin olarak maddede herhangi bir açıklayıcı hüküm bulunmamasına karşın, delil bütünlüğünün sağlanması, daha sonra delil eklendiği yönünde iddiaların önlenmesi bakımından hash değerinin de ilgili tutanağa kaydedilmesi suretiyle ilgili kişiye verilmesi gerekmektedir[589].

Gerek CMK'nın 134/1 maddesinde belirtilen kopyası alınan bilgisayar kayıtların çözülerek metin haline getirilmesi gerekse CMK'nın 134/5 maddesinde belirtilen sistemdeki verilerin tamamı veya bir kısmının kopyasının alındığı hallerde kopyası alınan verilerin kâğıda yazdırılması hususundaki mecburiyetin getirilmesinin nedeni

[587] Osman Nihat Şen, "Ceza Hukukunda Bilgisayar Araştırmaları", **Ceza Hukuku Dergisi (CHD),** Sayı. 1, (Ekim 2006), s. 392.

[588] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1102.

[589] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 363.

elektronik delilin kaybolma riskini ortadan kaldırmak ise de, elektronik delilin kaybolma riskini ortadan kaldırmaya yönelik birçok yol vardır. Bunlardan biri, birden fazla kopya alınmak suretiyle, kopyaların elektronik delillerin zarar görmeyeceği biçimde usulüne uygun koruma altına alınmasıdır. Nitekim kanun koyucuyu, elektronik delilleri, fiziksel delil niteliğine büründürme çabasına iten neden, ceza yargılamasının süjelerinin elektronik delillere yönelik önyargılı tutumlarıdır[590].

Bununla birlikte, Kanun, arama sırasında kopyalanacak olan verilerin yazdırılması hususunu bir mecburiyet haline getirmekte ise de, büyük hacimli dosyaların yazdırılması pratikte bazı zorlukları beraberinde getirecektir [591] . Gerçekten de, günümüzde çok büyük hacimlere sahip sabit disklerde bulunan ve milyonlarca A4 sayfası tutabilecek elektronik verinin yazdırılması mecburiyetinin uygulanabilirliği bulunmamaktadır. Kaldı ki; bu miktardaki yazdırılmış verinin adli makamlarca da incelenebilmesi imkân dâhilinde değildir[592].

Öğretide metin haline getirilmesi gereken verilerin çok fazla olduğu durumlarda bu verilerin veri depolama cihazlarına kaydedilerek delil olabilecek verilerin özetlerinin metin haline getirilmesi gerektiği[593] hususu çözüm olarak ileri sürülmüşse de gerçek çözüm yolunun uygulama kabiliyeti olmayan mezkûr madde metninin uygun bir tarzda değiştirilmesi olduğu kanaatindeyiz.

Ülkemiz uygulamasında çokça karşılaşılmamakla birlikte kolluğun kimi zaman şüphelilere ait bilişim sistemleri üzerinde bulunan dosyaların hash değerinin tespitini yaparak yasa dışı materyal veri tabanındaki hash değerler ile karşılaştırma yapmak suretiyle suçlulara ulaşma yoluna gittiği görülmektedir. Buna göre bilişim sistemleri üzerinde klasik anlamda arama, kopyalama veya elkoyma niteliğinde olmayan hash değerlerinin tespiti ile sınırlı uygulamalar bakımından CMK m. 134 uyarınca tedbir kararı alınması gerekip gerekmediği hususu üzerinde de durmak gerekmektedir.

---

[590] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 378.

[591] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1100; Aydoğan, s. 22.

[592] Yunus Balı, "CMK 134. Madde Düzeltilmelidir", http://www.dijitaldeliller.com/cmk134.htm (18 Kasım 2013).

[593] Ünal, s. 113.

Kanaatimizce, kolluk tarafından hash değeri tespiti ile sınırlı da olsa, şüphelinin sahibi olduğu veya kullandığı bir bilişim sistemi üzerinde yapılacak herhangi bir müdahale, bilişim sistemi üzerinde arama, kopyalama veya elkoyma işlemlerinin yapılıp yapılmadığı ve böylece şüpheliye ait bilgilerin ifşa edilip edilmediği hususlarına bakılmaksızın CMK m. 134 uygulamasını zorunlu kılacaktır. Zira hash değeri tespiti dosyaların açılarak içerisindeki bilgilerin ifşa edildiği klasik anlamda bir arama işlemi olmasa da yine de kişilerin mahremiyet alanına dolaylı biçimde de olsa müdahale teşkil eden değişik türden bir arama biçimi olarak değerlendirilmelidir.

3.2.6. Genel Hükümlerin Geçerliliği

Arama ve elkoyma tedbirinin özel bir şekli niteliğindeki bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirinin uygulanması sırasında Ceza Muhakemesi Kanunu'ndaki arama ve elkoymaya ilişkin genel hükümler geçerliliğini korumaktadırlar. Bu bağlamda, arama kararında bulunması gereken bilgiler, arama ve elkoymanın tutanağa bağlanması, aramayı yapan kolluk görevlilerinin isimlerinin tutanağa yazılması, arama sırasında bulunulması gereken kişiler, arama sonucunda verilecek belge, elkonulmayacak belgelerle ilgili hükümler bu tedbire aykırı olmadığı sürece geçerli olacaktır[594].

Ayrıca, bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbirinin uygulanmasına karşı hangi kanun yollarına başvurulabileceği hususunda açık bir hüküm bulunmamaktadır. Bu durumda bahse konu meselenin de genel hükümler çerçevesinde çözümlenmesi gerekir. Buna göre, CMK m. 267 uyarınca hâkimin ilgili tedbir kararı üzerine şüpheli veya müdafii itiraz yoluna gidebileceklerdir. Bununla birlikte CMK m. 35/2 uyarınca bu koruma tedbiri hazır bulunmayan ilgililere tebliğ olunmayacağı için şüpheli ve müdafii bu tedbir kararına öğrendikleri tarihten itibaren itiraz edebileceklerdir.

CMK m. 120/1 uyarınca tedbirin uygulanması sırasında arama yapılan bilişim sisteminin sahibi veya zilyedi aramada hazır bulunabilir. Bu kişilerin bulunmaması durumunda temsilcileri veya ayırt etme gücüne sahip hısımlarından biri veya

[594] Çolak ve Taşkın, s. 609.

kendileriyle birlikte oturmakta olan bir kişi veya komşusu hazır bulundurulur. Şüphelinin avukatının aramada hazır bulunmasına da engel olunamaz (CMK m. 120/3).

Yukarıda belirtildiği üzere tedbirin uygulanması sonucunda bilgisayar ve bilgisayar kütüklerine elkonulması veya elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyasının alınması durumlarında bu hususlar tutanağa bağlanacaktır. Bununla birlikte yapılan arama neticesinde herhangi bir veriye ulaşılamaması durumunda ise hakkında tedbir uygulanan kişinin talebi üzerine CMK m. 121/1'de belirtilen genel hükümler uyarınca bu durumu ve aramanın konusunu teşkil eden fiilin niteliğini belirten bir belge tanzim edilerek ilgilisine verilir.

CMK m. 122/1 uyarınca hakkında arama işlemi uygulanan kimsenin belge veya kâğıtlarını inceleme yetkisi, Cumhuriyet savcısına ve hâkime aittir. Bu bakımdan, söz konusu genel hüküm uyarınca CMK m. 134 uyarınca yerine getirilen tedbiri uygulayan kolluğun, bilişim sistemlerinde bulunan verileri kâğıda yazdırmaları durumunda, bu belgeler üzerinde incelemede bulunmaksızın Cumhuriyet savcısına teslim etmeleri gerekmektedir.

Kamu tüzel kişiliklerine ait bilişim sistemlerinde yapılan arama sırasında, devlet sırrı niteliğinde bilgi içeren belgelerle karşılaşılması durumunda, bahse konu belgeler üzerindeki inceleme CMK m. 125/2 uyarınca hâkim veya mahkeme başkanı tarafından yapılmalıdır. Buna göre, devlet sırrı niteliğindeki bilgi içeren belgelerde CMK m. 125/2 uyarınca Cumhuriyet savcısı tarafından inceleme yapılamayacağından dolayı, söz konusu belgelerin delil olarak değerlendirilmesi de Cumhuriyet savcısı tarafından yapılamayacaktır[595].

Diğer taraftan devlet sırrı niteliğindeki belgelerin sadece incelenmesinden bahsedilmesi nedeniyle bu nitelikteki belgeler alınamaz, sureti çıkarılamaz, fotokopisi yapılamaz, filmi çekilemez. Belgelerde yer alan ve sadece yüklenen suçu açıklığa kavuşturacak olan bilgiler hâkim veya mahkeme başkanı tarafından tutanağa kaydedilebilir[596]. Bu bağlamda, elektronik delilin de belge delillerinden olduğu dikkate alındığında devlet

[595] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 398.

[596] Zeki Hafızoğulları ve Muharrem Özen, "Türk Ceza Hukukunda Devlet Sırrına Genel Bir Bakış", **Ankara Barosu Dergisi**, Sayı. 1, (2010), s. 29.

sırrını ihtiva eden bir bilişim sistemi üzerinde yapılacak inceleme sırasında CMK'nın 125. maddesindeki hükümlerin dikkate alınması, incelemenin hâkim tarafından* yapılması ve bu bilişim sistemleri üzerinde kopyalama işleminin yapılamaması gerekmektedir.

CMK m. 126 uyarınca şüpheli ve sanık ile tanıklıktan çekinebilecek kimseler arasındaki mektuplara ve belgelere, bu kimselerin nezdinde bulunduğu sürece elkonulamaz. Bu bağlamda, şüphelinin kullandığı ve fakat soruşturma kapsamında tanıklıktan çekinebilecek bir kimseye ait olan bir bilişim sisteminde arama yapılması durumunda, bilişim sisteminde bulunan şüpheli ve tanıklıktan çekinebilecek kişi arasındaki mektup ve belge niteliğindeki verilere elkonulamayacaktır. Tedbir kapsamında yapılan kopyalama işlemi de bir nevi elkoyma niteliğinde olduğundan bu nitelikteki veriler hakkında kopyalama işlemi de yapılamaz.

Şüphelinin bilgisayarında, bilgisayar programlarında ve kütüklerinde yapılacak aramanın ölçüsüz biçimde yerine getirilmesi durumlarında tazminat hükümlerinin uygulanması da genel hükümlere göre belirlenecektir. Tedbirin özel hayata doğrudan müdahale etme niteliği göz önüne alındığında, tedbirin ölçüsüz bir biçimde uygulanması durumunda şüpheli veya müdafii CMK m. 141/1-i uyarınca tazminat talebinde bulunabilecektir.

Bilgisayarda, bilgisayar programlarında ve bilgisayar kütüklerinde yapılacak arama neticesinde elde edilen verilerin genel hükümler uyarınca müsadereye tabi olup olmayacağı hususu üzerinde de durulması gerekmektedir. Bir malın müsadere edilebilmesi maddi bir varlığa sahip olmasına bağlıdır. Bilişim sistemlerinden elde edilecek verilerin ise gayri maddi mal vasfına haiz oldukları ortadadır.

TCK m. 54'te iyiniyetli üçüncü kişilere ait olmamak koşuluyla, kasıtlı bir suçun işlenmesinde kullanılan veya suçun işlenmesine tahsis edilen eşyanın müsaderesine karar verilebileceği hükme bağlanmıştır. Bu bağlamda madde metninde belirtilen

* CMK'nın 134. maddesindeki tedbir kovuşturma aşamasında uygulanamayacağından CMK'nın 125/2 maddesinde geçen incelemenin mahkeme başkanı tarafından da yapılacağına ilişkin hüküm bu tedbir bakımından uygulanabilir değildir. Bu durumda bilişim sistemlerinde bulunan devlet sırrı niteliğindeki dijital belgelerin incelenmesi işlemi yalnızca soruşturma aşamasında ve hâkim tarafından yapılabilir.

koşulların varlığı halinde bilişim sistemlerinde yer alan verilerin içerisinde bulunduğu aygıtla birlikte müsaderesine karar verilebilecektir.

CMK m. 134 uyarınca yapılacak arama, kopyalama ve elkoyma tedbirinin kişi bakımından uygulanmasına ilişkin istisnai bir düzenleme bulunmamaktadır. Bu nedenle CMK m. 134 hükmünün CMK m. 130 hükmü ile birlikte değerlendirilmesi sonucunda bahse konu tedbirin avukatların bürolarında da uygulanabilmesi mümkündür[597]. Buna göre; söz konusu tedbir avukat bürolarında hâkim kararıyla, Cumhuriyet savcısının denetiminde ve baro başkanı veya onu temsil eden bir avukat huzurunda yapılabilecektir. Nitekim avukat bürolarında bilişim sistemleri üzerinde yapılan bir aramada hazır bulunanın konumuna dikkat çekilen bir Avrupa İnsan Hakları Mahkemesi kararında;

"*İşbu davada can alıcı nokta sözü geçen (ç.n. yazılı belgeye dair) güvencelerin elektronik veriler açısından uygulanmamış oluşudur. Çok sayıda faktör, başvuruculaların bu bağlamdaki haklarını kullanmalarının sınırlandırılmış olduğunu göstermektedir. İlk olarak, her ne kadar baro temsilcisi bilgisayar sistemlerinin aranması sırasında geçici olarak huzurda bulunmuşsa da, temsilci esasen yazılı belgelerin el konulmasını denetlemekle meşguldür ve bu nedenle elektronik veriler açısından denetim rolünü uygun bir şekilde yerine getirememiştir. İkinci olarak, hangi arama kriterlerine başvurulduğu, hangi dosyaların kopyalandığı ve hangilerine el konulduğunu gösteren bir arama, el koyma tutanağı el koyma işleminin sonunda değil aynı gün daha sonra tanzim edilmiştir. Ayrıca, göründüğü kadarıyla görevliler, işlerini bitirdiklerinde aramanın sonucu hakkında birinci başvurucuyu veya Baro temsilcisini bilgilendirmeksizin ayrılmışlardır (paragraf 63).*

Sonuç olarak Mahkeme; ilgili resmi makamlarca herhangi bir şekilde görevin kötüye kullanılmasını veya keyfi davranılmasını önlemeyi ve ayrıca avukatın mesleki sır saklama yükümlülüğünü korumayı amaçlayan usulü güvencelere uygun davranılmamasının, ilk başvurucunun elektronik verilerinin aranması ve el konulması işlemlerinin hedeflenen meşru amaç ile orantısız olmasına neden olduğunu tespit eder"

[597] Veli Özer Özbek, Ceza Muhakemesi Hukuku, s. 364; Ünal, s. 94.

(paragraf 66) (Wieser ve Biocos Beteligungen GmBH/Avusturya, 16.10.2007) [598] hükmüne yer verilmiştir.

3.2.7. Tesadüfen Elde Edilen Deliller

CMK m. 138/1 uyarınca bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama yapılması sırasında, yapılmakta olan soruşturma ve kovuşturmayla ilgisi olmayan, ancak diğer bir suçun işlendiği şüphesini uyandırabilecek bir delilin elde edilmesi durumunda, bu delilin muhafaza altına alınması ve durumun Cumhuriyet savcısına bildirilmesi gerekmektedir.

Bununla birlikte, tesadüfen elde edilen deliller konusunda dikkatli bir yaklaşım tarzının benimsenmesi ve arama sırasında soruşturmaya konu suçun dışına çıkılmaması gerekmektedir. Soruşturmaya konu suç bahane edilerek başka suçlarla ilgili delil araştırması yoluna gitmek, maddede öngörülen "bir suç soruşturmasının varlığı" şartına aykırılık teşkil edebilecektir. Bu bakımdan, soruşturmayla ilgili elde edilen suç delillerinin arasında başka bir suçun işlendiğine ilişkin bir bilginin varlığı halinde sadece bu delil değerlendirilmeli, buna dayanılarak aramayı genişletmeksizin durum derhal Cumhuriyet savcısına haber edilmelidir. Nitekim sınırlı ve ölçülü bir uygulamanın benimsenmemesi halinde, tedbirin, mevcut suç soruşturmasının dışına kayması ve hukuka aykırılıklara neden olunması muhtemeldir[599].

Bu bağlamda, bilişim alanında işlenen suçların aydınlatılması amacıyla yapılan bir arama sırasında çocuk pornografisine ilişkin resimlerin de elde edilmesi durumunda aramanın TCK m. 226/3'de düzenlenen müstehcenlik suçunun delillerini bulmaya yönelik yoğunlaştırılmaması, aramada tesadüfen elde edilen müstehcenlik suçuna ilişkin delillerin muhafaza altına alınması ve bu suçun soruşturulması amacıyla Cumhuriyet savcısına bildirilmesi, tesadüfen elde edilen verilerin müstehcenlik suçunun şüphelisi hakkında kamu davası açmaya yeterli olmadığı kanısına varılması durumunda ise bu defa bahse konu suçun soruşturulmasına esas olmak üzere yeni bir arama kararı ile bu

[598] Serkan Cengiz (çev.), İnsan Hakları Avrupa Mahkemesi Kararları, **Türkiye Barolar Birliği Dergisi**, Sayı. 82, (Mayıs 2009), s. 461-462.

[599] Ünal, s. 125-126.

suçun delillerinin elde edilmesi yolunun benimsenmesinin daha isabetli olacağı kanaatindeyiz.

Bilişim sistemlerinde yapılan arama işlemi sırasında kolluğun veya adli bilişim uzmanının yalnızca soruşturmaya konu elektronik delilleri toplamayı hedef alması gerekir. Zira bu kişilerin görevi delil toplamak ve inceleme/analiz işlemlerini yaparak gerçekleri sunmaktan ibarettir[600]. Bu bakımdan tesadüfen elde edilen delilden söz edilebilmesi için kolluğun veya adli bilişim uzmanının arama kararının sınırları dışına çıkmaması, arama kararında belirtilen fiil veya eşya ile ilgisi olmayan diğer bir eşyayı veya fiile ilişkin delili arama faaliyetine girişmemesi gerekmektedir. Bu sınırın çizilmesi durumunda, tesadüfen elde edilen delil kavramı anlam kazanacaktır. Nitekim bilişim sistemlerinde yapılan arama sırasında elde edilen ve arama kararında yer alan fiil veya eşya ile ilgisi olmayan bir elektronik delilin, tesadüfen elde edilen delil olarak kabul edilmesi yapılan aramayı keşif aramasına dönüştürecek ve kişilerin temel hak ve özgürlüklerine yönelik ciddi bir müdahale teşkil edecektir[601].

3.2.8. Tedbirin Temel Hak ve Özgürlükler Açısından Değerlendirilmesi

Koruma tedbirlerinin uygulanmasının genellikle temel hak ve özgürlüklere müdahale ettiği gerçeği karşısında CMK m. 134 uyarınca bilişim sistemlerinin aranması, kopyalanması ve elkonulması şeklinde uygulanan söz konusu koruma tedbirinin de bazı temel hak ve özgürlüklere müdahalede bulunduğu ortadadır. Bu bakımdan bu koruma tedbirinin özel hayatın gizliliğinin korunması, haberleşmenin gizliliğinin korunması ve düşünceyi açıklama ve yayma özgürlüğünün korunması bakımlarından ayrı ayrı değerlendirilmesi gerekmektedir.

3.2.8.1. Özel Hayatın Gizliliğinin Korunması

Özel hayat, hukuk tarafından korunması gereken bir temel hak olmasının yanı sıra bireylerin özel bilgileri, sosyal ilişkileri, haberleşme hürriyeti gibi birçok kavramı da içinde barındırmaktadır. Özel hayatın gizliliği ve korunması ise bireyin, kişiliğini

[600] Lisa Oseles, "Computer Forensics: The Key to Solving the Crime", 2001, http://faculty.ed.umuc.edu/~meinkej/inss690/oseles_2.pdf. (9 Ocak 2013).

[601] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 450.

geliştirmek, maddi ve manevi değerlerine güvence sağlamak için başkaları tarafından bilinmesini istemediği hususların oluşturduğu ve korunması hukuken gerekli görülen hayat alanı üzerindeki hakkı ifade etmektedir[602].

Hayatın gizli alanı, hayatın sadece kişiyi ilgilendiren ve ondan başkasının bilemeyeceği kısmı olarak tanımlanmakta ve mutlak manada korunmaktadır. Bu nedenle de, hayatın gizli alanı ile ilgili deliller yargılamada delil olarak kullanılamamaktadır. Bu bağlamda; suç teşkil etmemek koşuluyla, kişinin cinsel yaşamı veya dini düşüncesi, yalnızca onu ilgilendirdiği ve onun hayatının gizli alanına ait olduğu için yargılama konusu yapılamamakta, herhangi bir araştırmaya konu edilememekte ve delil olarak değerlendirilememektedir. Buna karşın, özel hayat ise, yalnızca bireyin yakınları tarafından bilinebilen yaşam alanını ifade etmektedir. Hayatın gizli alanından farklı olarak, özel hayatın nispi bir korumaya mazhar olup, özel hayat ile ilgili olarak elde edilen verilerin delil olarak değerlendirilip değerlendirilmeyeceği hususu, Anayasa, yasalar ve uluslararası sözleşmeler çerçevesinde kamu yararı ve oranlılık ilkesi dikkate alınarak belirlenmelidir[603].

Özel hayatın gizliliğinin korunması insan haklarına ilişkin en temel metinlerden biri olan Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesiyle güvence altına alınmıştır. AİHS'ne göre, özel hayatın gizliliği hakkı Sözleşmede belirtilen hallerde ve oranlılık ilkesine uymak kaydıyla ancak kanunla sınırlandırılabilir.

1982 Anayasa'sının 20, 21 ve 22. maddelerinde özel hayatın gizliliği hakkının kişinin aile hayatı, konut dokunulmazlığı ve haberleşme hürriyetiyle birlikte ele alındığı görülmektedir. 2010 Anayasa değişikliği ile Anayasa'nın 20. maddesinde yapılan ek bir düzenlemeyle kişilerin kendileriyle ilgili kişisel verilerin korunmasını isteme hakkı da özel hayatın gizliliği kapsamında koruma altına alınmıştır.

Anayasa'nın 20. maddesinde de herkesin, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı, ayrıca kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına

[602] Ersan Şen ve Yasemin Yurttaş, "Bilgisayar Programları Karşısında Özel Hayatın Korunması", **Terazi Hukuk Dergisi**, Cilt. 5, Sayı. 42, (Şubat 2010), s. 29.

[603] Avcı, s. 36.

sahip olduğu hükme bağlanmıştır. Özel hayatın gizliliğine ne zaman, kimler tarafından ve ne şekilde müdahalede bulunulabileceği ve bu müdahalenin hangi koşullarda hukuka uygun olacağı ise Anayasa'nın 20/2 maddesinde düzenlenmiştir.

Buna göre; özel hayata müdahale niteliğindeki kişilerin üstü, özel kâğıtları ve eşyasının aranması ve bunlara elkonulması; milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması hallerinden biri veya birkaçına bağlı olarak usulüne göre verilmiş hâkim kararı veya gecikmesinde sakınca bulunan hallerde kanunla yetkili kılınmış merciin yazılı emrine bağlıdır. Yetkili merci tarafından verilecek elkoyma kararı yirmi dört saat içerisinde hâkim onayına sunulmalıdır. Hâkim, kararını elkoyma işleminden itibaren kırk sekiz saat içerisinde açıklamalıdır. Aksi halde elkoyma kendiliğinden ortadan kalkacaktır. Anayasa'nın 21. ve 22. maddeleri uyarınca da aynı koşulların varlığı durumunda özel hayat kapsamındaki konut dokunulmazlığı ve haberleşme hürriyetine yönelik müdahalelerin hukuka uygunluğu düzenlenmiştir.

Bu bağlamda, kişilerin özel bilgilerinin yer aldığı bilişim sistemlerine ulaşabilmek ve bu surette delil elde edebilmek, mevcut yasal düzenlemelere ve Anayasa'nın 20/2 maddesindeki hükme aykırı davranmamakla mümkündür [604] . Ayrıca, kişilerin kendilerine ait olan özel hayatları ve kişisel verileri üzerinde karar verme ve belirleme yetkisi bulunduğundan bu Anayasa ve mevcut yasalara göre düzenlenen tedbirin uygulanmasının da sıkı koşullara tabi tutulması önem arz etmektedir.

Bilişim sistemlerinde yer alan bilgiler özel hayata ilişkin olabileceği gibi kişisel veri, ticari sır veya meslek sırrı niteliğinde bilgiler de olabilir. Ancak bu bilgiler, aynı zamanda, maddi gerçeğin ortaya çıkartılabilmesi açısından önemli bir delil niteliğinde de olabilir. Bir taraftan temel hak ve özgürlüklerin korunması, diğer taraftan ise maddi gerçeğin ortaya çıkartılabilmesi şeklindeki kamusal yarar göz önüne alınmak suretiyle bilişim sistemleriyle ilgili arama, kopyalama ve elkoyma CMK'da özel olarak düzenlenmiştir[605].

[604] Şen ve Yurttaş, s. 30.

[605] Şahin, Ceza Muhakemesi Hukuku I, s. 267.

Bu bağlamda, bu şekilde özel bir koruma tedbiri düzenlenmesindeki amaç, maddi gerçeğe ulaşılması esnasında müdahale edilecek hak ve özgürlüklerin, müdahalenin amacı doğrultusunda azami ölçüde korunmasıdır. Nitekim kanun koyucu, madde gerekçesinde; *"Madde, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve geçici elkoyma konularını düzenlemektedir. Bireye ait kişisel bilgiler üzerindeki hak, temel insan hakları olduğundan hakkın kısıtlanabilmesi için yasal düzenleme gerekeceği açıktır."* demek suretiyle, bu tedbire ilişkin düzenlemenin özel niteliğine de işaret etmiştir[606].

Yukarıda da değinildiği üzere CMK m. 134'de düzenlenen bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbiri, her koruma tedbirinde olduğu gibi hükümden önce bazı temel hak ve özgürlüklere müdahale etmektedir. Bu bağlamda söz konusu tedbir de özel hayatın gizliliği ile doğrudan bağlantılıdır.

Diğer taraftan, kişiler, elektronik ortama dâhil olmalarıyla birlikte bazı kişisel verilerini de kullanıma açmış olurlar. Günümüzde veri toplayabilme imkânı olan birçok elektronik sistem, kullanıcı ile etkileşime geçtiği anda, hiçbir bilgi kaydedemese bile kullanıcının benzersiz numarasını ve sisteme bağlandığı zamanı, sistem günlüğüne kaydetmektedir [607] . Özellikle bu bilgilerin kişinin kimliğinin, sosyal, psikolojik, ekonomik ve diğer özelliklerinin tespit edilmesi amacıyla toplanması, işlenmesi ve aktarılması durumlarında kişisel verilerin korunmasına ilişkin hakkın ihlali söz konusu olacaktır[608].

Yazılım uzmanları bu nitelikteki kişisel verileri kaydetmeyi güvenlik gerekçesiyle ortaya çıkan bir ihtiyaç olarak açıklasalar da, bu durumun kişiler hakkında daha fazla bilgi elde etme yönü de bulunmaktadır. Zira hangi türden bir elektronik ortam olursa

[606] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 315.

[607] Habip Oğuz, "Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum", **Uyuşmazlık Mahkemesi Dergisi**, Cilt. 1, Sayı. 3, (Haziran 2014), s. 4.

[608] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 107.

olsun, çoğu zaman ihtiyaç duyulandan daha fazla kişisel veriye erişme eğilimi bulunmaktadır[609].

Kişisel verilerin elektronik işlem yöntemleriyle derleme, sınıflandırma ve saklama faaliyetlerine tabi tutulması ve istendiğinde istenilen biçimde sunulabilmesi olanağının bulunması ise, bu verilerin haksız biçimde kullanılabilmesi olasılığını artırmış, kişilerin rızası alınmadan başkalarına açıklanmasını ve verilerin bulunduğu yerden başka yerlere aktarılmasını kolaylaştırmıştır[610].

Bu itibarla söz konusu tedbir, özel hayatın gizliliği kavramının içinde yer alan ve hatta ayrılmaz bir parçasını teşkil eden kişisel verilerin korunması bakımından da özellik göstermektedir. Zira bilgisayarların nitelikleri gereği kişilerin gerek özel yaşamlarına gerekse iş yaşamlarına ilişkin birçok kişisel veriyi depolamaları nedeniyle bu tedbirin uygulanması sonucunda birçok kişisel veriye ulaşılmakta ve kişilerin kendileriyle ilgili gizledikleri önemli kişisel verileri deşifre olmaktadır[611].

Bu bakımdan, tedbirin uygulanmasının somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı şartına bağlanması, özel hayatın gizliliğinin korunması bakımından önemlidir. Bununla birlikte, söz konusu tedbirin ihlal etmesi muhtemel kişilik hakları dikkate alındığında, hakkında tedbir uygulanan şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilip bu kararın kesinleştiği hallerde tedbir sonucunda elde edilen verilerin soruşturma dosyasından ve tüm kayıtlardan çıkartılarak yok edilmesi konusunda herhangi bir düzenlemenin bulunmaması bir eksikliktir. Bu nedenle ilgili maddeye bu duruma ilişkin bir hükmün eklenmesi yerinde olacaktır.

Bununla birlikte mevcut düzenleme yapılıncaya kadar CMK m. 137'de belirtilen telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbiriyle ilgili verilen kararın uygulanması sırasında şüpheli hakkında kovuşturmaya yer olmadığına ilişkin karar verilmesi durumunda, yapılan tespit veya dinlemeye ilişkin kayıtların Cumhuriyet savcısının denetimi altında en geç on gün içinde yok edilerek durumun tutanakla

[609] Oğuz, s. 4-5.

[610] Sevil Yıldız, s. 227.

[611] Dağ, s. 235, 238.

tespitine ilişkin hükmün, CMK m. 134 uyarınca uygulanan tedbirde, şüphelinin lehine kıyasen uygulanması yerinde olacaktır. Bu durumda şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi halinde, bilişim sistemlerinden elde edilen veriler, Cumhuriyet savcısının denetimi altında ve on gün içinde yok edilerek durum tutanakla tespit edilebilecektir.

Bu bağlamda, CMK m. 134'de ifadesini bulan tedbirle ilgili düzenlemeye bir bütün olarak bakıldığında söz konusu tedbirin gerek Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde gerekse Anayasanın 20/2 maddesinde belirtilen istisna hallerde ve oranlılık ilkesine uygun şekilde uygulanabilir olduğu görülmektedir.

Bununla birlikte her ne kadar yasal düzenleme Avrupa İnsan Hakları Sözleşmesi ve Anayasaya uygunluk göstermekte ise de uygulama sırasında hakkında söz konusu tedbir uygulanan kişinin temel hak ve özgürlüklerinin hukuki sınırlarını aşacak biçimde sınırlandırılmaması gerekmektedir. Özellikle bu tedbirin uygulanmasında, ceza yargılamasının amacına uygun bir şekilde özel hayatın gizliliğinin ve kişisel verilerin korunması, tedbiri uygulayan mercilerin birinci görevi olmalıdır.

3.2.8.2. Haberleşmenin Gizliliğinin Korunması

Haberleşmenin gizliliği hakkı, kişilerin hangi araç ve yolla olursa olsun diğer kişilerle yaptığı ve özel nitelik taşıyan haberleşmelerini kişilerden veya devlet organınca öğrenilme endişesinden uzak bir biçimde yapabilmeleri hakkını ifade etmektedir. Bu bakımdan üçüncü kişilerin veya devletin, kişilerin mektup, elektronik posta, faks, telefon, teleks vb. araçlarla yaptığı yazışma ve konuşmaları, okumaması, dinlememesi ve içeriğine ait bilgilere ulaşamaması gerekmektedir[612].

Haberleşmenin gizliliğinin korunması Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesi ile güvence altına alınmıştır. Sözleşmeye göre, haberleşmenin gizliliği hakkı Sözleşmede belirtilen hallerde, oranlılık ilkesine uymak kaydıyla ancak kanunla sınırlandırılabilir.

[612] Ömer Anayurt, **Avrupa İnsan Hakları Hukukunda Kişisel Başvuru Yolu**, Ankara: Seçkin Yayıncılık, 2004, s. 116-117.

Avrupa İnsan Hakları Mahkemesi, Sözleşmenin resmi Fransızca ve İngilizce metnindeki "correspondance" ve "correspondence" kelimelerinin yalnızca sözlük anlamındaki "yazışmayı" değil, bunun yanı sıra her çeşit yol ve araç vasıtasıyla kişiler arasında gerçekleştirilen özel nitelikteki haberleşmeyi ifade ettiği belirtilmiştir (Mah. K., Klass ve öte./ Almanya, 6.9.1978, A 28, § 10 ve 11; Malone/İngiltere, 2.8.1984, A 82, § 64; A./Fransa, 23.11.1993, A 277, § 36; Schenk/İsviçre, 12.7.1988, A 140, § 43-44)[613].

Anayasa'nın 22. maddesinde herkesin haberleşme hürriyetine sahip olduğu ve haberleşmenin gizliliğinin esas olduğu hükme bağlanmıştır. Haberleşme hürriyetine ve haberleşmenin gizliliğine ne zaman, kimler tarafından ve ne şekilde müdahalede bulunulabileceği ve bu müdahalenin hangi koşullarda hukuka uygun olacağı ise Anayasa'nın 22/2 maddesinde düzenlenmiştir.

Bilişim sistemlerinde elektronik delil niteliğini haiz veriler her zaman durağan halde ve depolanmış vaziyette bulunmamaktadır. Bazı hallerde elektronik posta ile yapılan haberleşmelerde olduğu gibi akış halindeki veriler de delil değerine sahip olabilmektedirler [614] . Elektronik posta ile verilerin iletilmesindeki gizlilik, haberleşmenin gizliliği garantisi ile korunduğundan[615] elektronik postalarda olduğu gibi akış halindeki verilerin elde edilmesi, kişinin haberleşme hürriyetine ve haberleşmenin gizliliğine müdahale teşkil edecektir[616].

Bununla birlikte, haberleşmenin gizliliği hakkı mutlak bir nitelik taşımamaktadır. Bu nedenle meşru sebeplere bağlı olarak, yasal bir temele dayanılarak, bireylere güvenceler sunmak ve oranlılık ilkesine bağlı kalmak kaydıyla haberleşmenin gizliliğine devlet tarafından müdahalede bulunulabilir[617].

---

[613] Gözübüyük ve Gölcüklü, s. 341.

[614] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 99.

[615] Zafer Gören, "Düşünceyi Açıklama Özgürlüğü", **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi**, Sayı. 24, (Güz 2013/2), s. 49.

[616] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 99.

[617] Anayurt, s. 117.

Bu bağlamda, CMK m. 134'de ifadesini bulan tedbirle ilgili düzenlemeye haberleşmenin gizliliği hakkı kapsamında bir bütün olarak bakıldığında söz konusu tedbirin gerek Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde gerekse Anayasanın 22/2 maddesinde belirtilen istisna hallerde ve oranlılık ilkesine uygun şekilde uygulanabilir olduğu görülmektedir.

3.2.8.3. Düşünceyi Açıklama ve Yayma Özgürlüğünün Korunması

Düşünceyi Açıklama ve Yayma Özgürlüğü Avrupa İnsan Hakları Sözleşmesi'nin 10. maddesi ile güvence altına alınmıştır. Sözleşmeye göre, düşünceyi açıklama ve yayma özgürlüğü Sözleşmede belirtilen hallerde, ancak kanunla bazı merasime, koşullara, sınırlamalara veya yaptırımlara bağlanabilir.

Avrupa İnsan Hakları Mahkemesi, düşünceyi açıklama, haber ve bilgi alıp verme hakkına sahip olma özgürlüğünü koruma altına alan 10. maddenin demokratik toplumdaki önemini, bu konuya ilişkin davaların hemen hepsinde açık bir dille ve altını çizerek ifade etmektedir[618].

AİHM pek çok kararında, düşünceyi açıklama özgürlüğünün demokratik toplumun köşe taşlarından, kişilerin ilerlemelerinin ve kişiliklerini geliştirmelerinin esaslı koşullarından biri olduğunu vurgulamıştır. Mahkemeye göre, demokrasi, düşünceyi açıklama özgürlüğü ile beslenir. Çoğulculuğun olmadığı yerde demokrasiden söz edilemez. Demokrasinin temel ilkelerinden birisi de, bir ülkenin sorunları ile ilgili olarak şiddete başvurmaksızın, diyalog yoluyla çözümü konusunda fikir ve düşüncelerin serbestçe ifade edilebilmeleri imkânının tanınıp güvence altına alınmasıdır[619].

AİHM'ye göre Sözleşmenin 10. maddesinde yer verilen düşünceyi açıklama özgürlüğü, sadece itibar gören veya zararsız yahut önemsiz sayılan haberler veya fikirler bakımından değil; aynı zamanda devlet veya halkın bir bölümü için aykırı, kural dışı, şaşırtıcı veya endişe verici cinsten olaylar açısından da geçerlidir. Nitekim demokratik

[618] Gözübüyük ve Gölcüklü, s. 358.

[619] Anayurt, s. 121-122.

toplumun vazgeçemeyeceği çoğulculuk, hoşgörü ve açık fikirliliğin gereği bunu gerektirmektedir[620].

Anayasa m. 25/1'de öncelikle herkesin düşünce ve kanaat hürriyetine sahip olduğu düzenlenmiştir. Anayasa m. 25/2'de ise her ne sebeple ve amaçla olursa olsun kimsenin, düşünce ve kanaatlerini açıklamaya zorlanamayacağı, düşünce ve kanaatleri sebebiyle kınanamayacağı ve suçlanamayacağı düzenlenmiştir. Bu fıkra ile düşünceyi açıklamama ve yaymama (negatif düşünceyi açıklama ve yayma) özgürlüğü korunmaktadır.

Anayasa'nın 26/1 maddesinde ise herkesin, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahip olduğu, bu özgürlüğün resmi makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestîsini kapsadığı belirtilerek (pozitif) düşünceyi açıklama ve yayma özgürlüğü koruma altına alınmıştır. Düşünceyi açıklama ve yayma özgürlüğüne ne zaman ve ne şekilde müdahalede bulunulabileceği Anayasa'nın 26/2 maddesinde düzenlenmiştir.

Anayasa'nın 26/1 maddesinde koruma altına alınan pozitif düşünceyi açıklama ve yayma özgürlüğünde düşüncenin yöneltilen kişiye ulaşması güvence altına alınırken, Anayasa'nın 25/2 maddesinde koruma altına alınan negatif düşünceyi açıklama ve yayma özgürlüğünde ise, düşüncenin, açıklayan ve yayan kişinin ulaşmasını istemediği kişilere ulaşmaması güvence altına alınmıştır[621].

Teknolojinin geldiği nokta dikkate alındığında, internetin herkese kendi basın ve yayın aracına sahip olma imkânını tanıdığı görülmektedir. İnternet üzerinden insanlar düşüncelerini açıklamakta, yaymakta ve diğer kişilerin görüş ve düşüncelerine erişebilmektedir. CMK m. 134 uyarınca bilişim sistemlerinde arama ve elkoyma tedbirinin uygulanması, bilişim sistemleri aracılığıyla düşünce açıklama ve yayma hakkı ile doğrudan bağlantılıdır. Diğer taraftan, kişilerin düşüncelerine açıklayabilmeleri ve yayabilmeleri, iletişim araçlarıyla gerçekleştirilebilecek haklardandır. Akış halindeki

[620] Gözübüyük ve Gölcüklü, s. 358.

[621] Gören, s. 38.

verilerin ele geçirilmesinin de kişilerin düşüncelerini açıklama ve yayma haklarına müdahale teşkil edeceği açıktır[622].

Bu bağlamda, CMK m. 134'de ifadesini bulan tedbirle ilgili düzenlemeye düşünceyi açıklama ve yayma özgürlüğü açısından bakıldığında söz konusu tedbirin gerek Avrupa İnsan Hakları Sözleşmesi'nin 10/2 maddesinde gerekse Anayasa'nın 26/2 maddesinde belirtilen istisna hallerde ve oranlılık ilkesine uygun şekilde uygulanabilir olduğu görülmektedir.

3.2.9. Tedbirin Avrupa Konseyi Siber Suç Sözleşmesi Açısından Değerlendirilmesi

Avrupa Konseyi Siber Suç Sözleşmesi'nin 19. maddesinde "Saklanan bilgisayar verilerinin aranması ve bunlara elkonulması" düzenlenmiştir. Bazı eksikliklerin varlığının kabulüyle birlikte CMK m. 134'ün esas itibariyle bu sözleşme hükmünün iç hukuka uyarlanmış şeklini ifade ettiği söylenebilir. Buna göre;

CMK m. 134/1 ve m. 134/2'de bilgisayar ve bilgisayar kütüklerinde hangi hallerde arama yapılacağı ve bunlara ne şekilde elkonulabileceği hükme bağlanmıştır. Yukarıda da değinildiği üzere maddenin birinci fıkrasına getirilen arama işleminin "somut delillere dayanan kuvvetli suç şüphesinin varlığı" şartının da eklenmesi, tedbirin uygulanmasıyla ilgili temel hak ve özgürlükler bakımından olumlu bir gelişme sağlamıştır. Tüm bunlar göz önüne alındığında mevcut düzenlemelerin Sözleşmeye uygun olduğu belirtilmelidir.

CMK m. 134/3'de düzenlenen bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında sistemdeki bütün verilerin yedeklemesinin yapılmasına ilişkin hüküm verilerin bütünlüğünün korunması ve soruşturma sonuçlanıncaya kadar soruşturma ile ilgili delil niteliği taşıyabilecek verilerin değiştirilmesi, bozulması, erişilemez hale getirilmesi ve silinmesinin engellenmesi bakımından Sözleşmeyle paralellik arz etmektedir. Ancak CMK'da elkoyma gerekçelerinin detaylı bir şekilde açıklanmamış olması eksiklik olarak görülmektedir[623].

[622] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 102.

[623] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1102.

CMK m. 134/4'de sistemdeki bütün verilerin yedeklemesinin yapılması durumunda bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilmesi ve bu hususun tutanağa geçirilerek imza altına alınmasına ilişkin düzenleme ile CMK m. 134/5'te düzenlenen bilgisayar veya bilgisayar kütüklerine elkoymaksızın da sistemdeki verilerin tamamının veya bir kısmının kopyasının alınabileceğine ilişkin hükmü de Sözleşme ile uyumluluk göstermektedir.

Bununla birlikte, verilerin suç oluşturan içerik veya virüs programı ya da çocuk pornografisi gibi başlı başına suç unsuru veya suç aracı olması durumunda erişilemez veya kullanılamaz hale getirilmesi ve hatta kopyaları alındıktan sonra silinmesi gerekmektedir. Sözleşmede bu hususta bir düzenleme bulunmasına rağmen CMK'nın 134. maddesinde düzenlenen tedbirde bu konuda herhangi bir hükmün yer almaması önemli bir eksikliktir[624].

Sözleşme, arama ve elkoyma yetkisinin internet vb. telekomünikasyon ağları ile yasal olarak erişilebilen diğer sistemler ya da bilgisayar sistemine doğrudan bağlı bulunan veya yakınında bulunan veri depolama aygıtları için de genişletilebileceğini öngörmekte ve uygulamayı taraf devletlerin iç hukukuna bırakmakta ise de CMK m. 134'te bu yönde açık bir hükmün bulunmuyor olması da bir diğer eksiklik olarak görülmektedir[625]. Bu eksiklik aşağıda inceleneceği üzere Adli ve Önleme Yönetmeliği m. 17/3 hükmü ile kısmen de olsa giderilmeye çalışılmıştır.

3.3. Adli ve Önleme Aramaları Yönetmeliği'nin 17. Maddesi

Adli ve Önleme Aramaları Yönetmeliği'nin 17. maddesinin 1, 2 ve 4. fıkraları CMK'nın 134. maddesinin 1, 2 ve 4. fıkraları ile birebir aynı niteliktedir. Yönetmeliğinin 17. maddesinin 3 ve 5. fıkralarına ise CMK'nın 134. maddesinin 3 ve 5. fıkralarındaki -uygulamada da sıklıkla eleştirilen- eksiklikleri gidermeye yönelik ek hükümler getirilmiştir.

Yönetmeliğinin 17/3 maddesi CMK'nın 134/3 maddesi ile uyumlu olarak *"Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin*

[624] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1102.

[625] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1102.

yedeklemesi yapılır" hükmü ile başlamış ancak CMK 134/3'de olmayan *"Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır"* hükmüne de yer verilmiştir.

Yönetmeliğe eklenen *"Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır"* ifadesi ile olay mahallindeki bilgisayarların yanı sıra CD, DVD, disket, çıkarılabilir hafıza birimleri (usb memory, SD Card vb.) gibi veri depolama ünitelerinin yedeklenebileceği belirtilmektedir. Ayrıca, bu hüküm ile network'e (LAN, WAN gibi) bağlı bilgisayarlardan uzaktan yedekleme yapılabileceği öngörülmektedir. Yönetmelikte yapılan bu düzenleme, CMK m. 134/3'deki eksiklikleri giderme noktasında önemli bir adımdır[626].

Bununla birlikte Yönetmeliğin 17/3 maddesi her ne kadar aramadan bahsetmeyip yalnızca yedeklemeden bahsetmekte ise de CMK'nın 134. maddesi uyarınca arama işlemine konu olmamış araçlar üzerinde doğrudan yedekleme işleminin uygulanması mümkün değildir. Zira elektronik verilere ulaşılabilmesi her şeyden önce arama yapılmasına bağlıdır. Yedekleme, arama işleminden sonra yapılması gereken bir uygulamadır. Bu bakımdan, Yönetmelik hükmü uyarınca bilgisayar ağları, uzak bilgisayar kütükleri ve çıkarılabilir donanımlar hakkında da arama, kopyalama ve elkoyma işlemleri uygulanabilecektir[627].

Diğer taraftan bilgisayar ve bilgisayar kütüklerine uzaktan erişimle ilgili mevzuatta özel bir düzenleme olmaması nedeniyle Yönetmelik hükmünde bulunan bu ifadeyi arama, kopyalama ve elkoyma tedbiri sonucunda yapılacak yedekleme işlemleri ile sınırlı tutmak ve uzaktan erişimle arama şeklinde geniş yorumlamamak gerekmektedir[628].

Mevzuattaki düzenlemelerin şirketlere bazı kayıtları saklama zorunluluğu yüklemesi, kayıtların elektronik ortamda depolanmasının uygun ve düşük maliyette olması gibi nedenler bilgisayarlarda yapılan arama ve elkoyma işlemlerinin işletmeler bakımından

[626] Aydoğan, s. 23.

[627] Yaşar ve Dursun, s. 16.

[628] Ünal, s. 139.

da yaygın biçimde uygulanmasına sebebiyet vermektedir[629]. Bu bağlamda bir şirkete ait bilgisayarlarda veri araması yapıldığı esnada, gerekli bilgilendirme yapılarak söz konusu Yönetmelik hükmü uyarınca şirket ağına bağlı başka bilgisayarlardaki veriler kontrol edilebilir veya kopyalanabilir. Bu durum teknik açıdan uzaktan erişimle aramayı akla getirmekteyse de hukuksal açıdan uzaktan erişimle arama olarak değerlendirilemez[630].

Bu bakımdan, bilişim sistemlerinin yapısı ve bilgisayar sistemlerinin birbirlerine bağlanabilir olma özellikleri dikkate alındığında, bilgisayar verilerinin ağa bağlı başka bir sistemde saklanabilmesi de her zaman mümkün olduğundan tek cümle ile ifade edilen bu düzenleme yetersiz olup arama ve elkoyma işleminin genişletilmesi hususunda sınırların mümkün olduğunca net çizilmesine imkân sağlayıcı düzenlemelerin yapılması gerekmektedir[631].

Yönetmeliğinin 17/5 maddesi CMK'nın 134/5 maddesi ile uyumlu olarak *"Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir"* hükmü ile başlamış ancak CMK m. 134/5'de yer alan ve uygulamada çokça tartışılan *"Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır"* hükmü yerine *"Kopyası alınan verilerin mahiyeti hakkında tutanak tanzim edilir ve ilgililer tarafından imza altına alınır. Bu tutanağın bir sureti de ilgiliye verilir"* hükmüne yer verilmiştir.

Yönetmelikte yapılan bu düzenlemeyle kopyalanan verilerin ne olduğu içerik olarak değil, liste bazında adlarının neler olduğu ele alınacaktır. Bu şekilde kopyalanan verilerin liste bazında adlarının neler olduğunun raporlanması yedekleme işleminde kullanılan bilgisayar programları ile raporlanabilmektedir. Yönetmelikteki bu hüküm sayesinde CMK'nın 134/5 maddesinde belirtilen yığınlarca doküman çıktısı alma işlemine gerek kalmamaktadır[632].

---

[629] Linda Volonino, "Electronic Evidence and Computer Forensics", **Communications of the Association for Information Systems,** Vol. 12, (October 2003), s. 458.

[630] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 199.

[631] Kunter, Yenisey ve Nuhoğlu, Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku, s. 1102-1103.

[632] Aydoğan, s. 24.

Belirtmek gerekir ki; Yönetmeliğin 17. maddesi, CMK'nın 134. maddesinde düzenlenen arama, kopyalama ve elkoyma tedbirinin uygulama alanını hem kolaylaştırmakta (m. 17/5) hem de genişletmektedir (17/3). Esasen temel hak ve özgürlükleri kısıtlayan ve yasayla düzenlenen bir koruma tedbirinin yönetmelik hükümleriyle uygulama alanının genişletilmesi tartışmaya konu bir husus ise de CMK'nın 134. maddesinde düzenlenen tedbirin uygulama alanının bulunmadığı bir eşya üzerinde doğrudan CMK'nın 116 vd. maddeleri ile 127. maddesinde düzenlenen klasik arama ve elkoyma tedbirlerinin gündeme gelecek olması nedeniyle Yönetmelik hükümleriyle uygulama alanı bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları bakımından genişletilen CMK'nın 134. maddesindeki tedbirin -yeni bir yasal düzenlemeyle mevcut sorun çözülene kadar- evleviyetle uygulanması gerektiği kanaatindeyiz.

3.4. Suç Eşyası Yönetmeliği'nin 9. Maddesi

Elektronik delil, hassas yapısından dolayı, yanlış muhafaza koşulları altında kolaylıkla değişikliğe uğrayabilir, bozulabilir ya da yok olabilir. Bu nedenle, elektronik delilin muhafaza edilmesi için özel önlemlerin alınması gerekir. Aksi halde, elektronik delil kullanılamaz veya yürütülmekte olan soruşturma ve kovuşturmayı sonuca götüremez duruma gelebilir. Bu bakımdan elektronik delilin bu hassas yapısı Suç Eşyası Yönetmeliği'nin 9. maddesinde ortaya konulmuştur.

Diğer taraftan soruşturma ve kovuşturma sırasında ortaya çıkabilecek itirazlar ve şüpheler bakımından, elektronik delilin elde edildiği cihazların, iz ve eserlerin ortaya konulması ve saklanması gerekmektedir. Elde edilen elektronik deliller, kovuşturma kesin hükümle sonuçlanıncaya kadar dijital yapıda muhafaza edilmelidirler. Bu noktada, elektronik delillerin uygun koşullarda ve zarar görmeden saklanma (emanette tutulma) yerleri de sağlanmalıdır[633].

Bu bağlamda Suç Eşyası Yönetmeliğinin "Kıymetli eşya ve evrak ile bozulacak, değerini kaybedecek veya muhafazası zor olan suç eşyası hakkında yapılacak işlemler" başlıklı 9. maddesinin 2. fıkrasında *"Bilgisayar, bilgisayar kütükleri ve bu sisteme*

[633] Ali Karagülmez, "Bilişim Suçlarında Delil Toplamayı Etkileyen Başlıca Konular", **2. Polis Bilişim Sempozyumu**, Ankara, 14-15 Nisan 2005, s. 33.

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" hükmüne yer verilmiştir.

Avrupa Konseyi Siber Suç Sözleşmesi'nin "Saklanan Bilgisayar Verilerinin Hızlı Bir Biçimde Korunması" başlıklı 16. maddesinde elde edilen bilgisayar verilerinin silinmeden, değiştirilmeden, bozulmadan özgün niteliği ile korunması hedeflenmekte ve taraf ülkelere verilerin korunmasına yönelik bir takım yasama işlemlerini yerine getirme mükellefiyeti yüklemektedir. CMK m. 134'te bu konu ile ilgili herhangi bir düzenleme bulunmamaktadır.

Yönetmelikte yapılan bu düzenlemeyle CMK m. 134 hükmünde belirtilmeyen elektronik delilin nasıl muhafaza edileceği sorununa çözüm getirilmiştir. Buna göre; el konulan elektronik delillerin nem, ısı, manyetik alan ve darbelerden korunmalarını sağlayacak, belli sayıda yetkili kişinin erişebildiği ve giriş çıkış kayıtları tutulan uygun ortamlarda muhafaza edilmeleri gerekmektedir. Bu düzenlemeyle CMK m. 134'de öngörülmeyen ve adli bilişim süreci bakımından da bir eksiklik niteliğinde olan "elektronik delil muhafaza etme" hususunun da güvenceye alınması sağlanmıştır[634].

Bununla birlikte bilişim aygıtlarının belli sürelerde güç beslemesinin yapılması, sistemdeki verilerin silinmemesi bakımından bir gerekliliktir. Bu açıdan Yönetmelik hükümlerinin tekrar gözden geçirilerek, aygıttaki verilerin silinmemesi, zarara uğramaması ve aygıttaki verilerin delil niteliğine zarar gelmemesi anlamında sürekli ve periyodik kontrol tedbirlerinin alınması hususunda hükümlerin eklenmesi yerinde olacaktır[635].

Sonuç olarak elektronik delilin hukuken denetlenmesi ve adli bilişim sürecinin ceza usul mevzuatımıza yansıması CMK'nın 134. maddesi ile bu maddeye ek olarak Adli ve Önleme Aramaları Yönetmeliği'nin 17. ve Suç Eşyası Yönetmeliği'nin 9. maddeleri ile sağlanmaya çalışılmıştır. Günümüzde bilişim sistemlerinin baş döndürücü bir hızla ilerlemesi ve buna bağlı olarak adli bilişimin büyüyen ve gelişen bir bilgi yumağına

[634] Aydoğan, s. 25; Aktepe, s. 68.

[635] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 372.

dönüşmesi karşısında mevcut düzenlemelerin uygulanabilirliği oldukça zor görünmektedir. Bu bakımdan yukarıda sıraladığımız eleştiriler doğrultusunda mevcut tedbirin daha geniş kapsamlı olarak yeniden düzenlenmesi gerektiği kanaatindeyiz.

3.5. Türk Hukukunda Düzenlenmeyen Durumlar

3.5.1. Uzaktan Erişimle Arama

Teknolojideki akıl almaz ilerleme sonucunda üretilen çok farklı tür ve ebattaki bilişim sistemleri sayesinde birçok yerde hızlı ve kolay internet iletişimi sağlanabilmektedir. Teknolojideki bu ilerlemenin olumsuz bir sonucu olarak ise internet erişimine sahip söz konusu bilişim sistemlerinin dışarıdan müdahaleye maruz kalmalarının söz konusu olmasıdır. Buna göre, internet bağlantısı durumundaki bir bilişim sistemine, kullanıcının bilgisi haricinde erişim sağlanarak kullanmış olduğu bilişim sistemindeki verilere ulaşmak mümkündür.

Bununla birlikte bilişim sistemlerine uzaktan erişim sağlanarak arama işleminin yapılıp yapılmayacağı hususu mukayeseli hukukta ve iç hukukumuzda tartışma konusu edilmiştir. Nitekim yukarıda mukayeseli hukukta bu konuya ilişkin ülke uygulamalarından bahsedilmiştir.

Avrupa Konseyi Siber Suç Sözleşmesi'nin 32. maddesine göre bilgisayarda depolanmış verilere, söz konusu bilgisayar sistemi üzerinden erişim yetkisine haiz olan kişinin yasal izninin bulunduğu veya bu verilerin herkesin ulaşabileceği şekilde açık olduğu durumlarında sınır ötesinden erişim sağlanabileceği belirtilmektedir.

Türk hukuk sisteminde uzaktan erişimle arama yapılabileceğini savunan Bıçak, CMK'nın 134. maddesinde belirtilen "arama" ibaresinin "elektronik veri takibi" olarak anlaşılması gerektiğini, elektronik veri takibinin ise bilişim sisteminin kolluğun hâkimiyetine alınması suretiyle açık olarak yapılabileceği gibi bilişim sistemine uzaktan erişim sağlanarak yazılım üzerinden ve gizli olarak da yapılabileceğini ileri sürmüştür[636].

[636] Bıçak, s. 671-673.

Karşı görüşte olan Değirmenci'ye göre ise; CMK m. 134 uyarınca bilişim sistemine kötü niyetli bir yazılım yüklemek suretiyle arama yapılmasına, sistemde yer alan verilerin bir yere gönderilmesine, sistem hareketlerinin izlenmesine imkân bulunmamaktadır. CMK m. 134 durağan verilerde yapılan aramayı düzenleyen, arama esnasında ilgili kişinin haberi olması gereken, aramanın kanunda belirtilen usul ve esaslarda yapılmasını gerekli kılan bir koruma tedbiridir. Uzaktan arama yapmak amacıyla ilgili kişinin haberi bulunmaksızın, yüklenen kötü niyetli yazılımlarla bilişim sisteminde arama yapılması mümkün görülmemektedir. Nitekim kötü niyetli yazılımlar kullanılmak suretiyle veri elde edilmesi hususu bir arama işlemi olarak da nitelendirilemez. Zira arama sürekli bir faaliyet olmayıp anlık bir faaliyettir. Bununla birlikte, kötü niyetli yazılımlar kullanılmak suretiyle veri elde etmek sürekli bir faaliyet niteliğindedir. Uzaktan aramanın diğer bir şekli olan sisteme erişmek suretiyle, ilgilinin haberi olmaksızın bilişim sistemleri üzerinde arama yapılması da CMK m. 134 anlamında mümkün görülmemektedir. Nitekim CMK'nın 134. maddesinde ilgili kişinin haberi olmaksızın bilişim sisteminde arama yapılabileceğinden bahsedilmemiştir[637].

Ünal'a göre de, uzaktan erişim sağlanarak bilişim sisteminde arama yapma, CMK m. 134'te öngörülen bir arama biçimi değildir. Nitekim böyle bir arama da temel hak ve özgürlüklere ağır müdahale anlamını taşımaktadır. Bu bakımdan, bu nitelikte bir arama için yeni bir yasal düzenleme yapılması zorunluluğu bulunmaktadır[638].

Gerçekten de; yeni teknolojilerin gelişimi, suç işleme olanaklarını artırmakta, bu nedenle de teknoloji destekli suçlarla mücadelede teknoloji destekli soruşturma yöntemlerine ihtiyaç duyulmaktadır. Bu bakımdan Türk hukukunda da, yeni bir yasal düzenlemeye bağlı olarak, daha az maliyetle suç delilleri elde edilebilmesini sağlayabilen uzaktan arama tedbirinin ceza yargılaması bakımından ağır cezayı gerektiren kimi suçlar için ve hâkim kararı ile uygulanması düşünülebilir. Ancak böyle bir durumda da, uzaktan arama suretiyle elde edilecek verilerin, otomatik sistemler kullanılarak suç ile ilgili olmayanlarının ve özel hayatın çekirdek alanına ait olanlarının

[637] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 364-365.

[638] Ünal, s. 111.

ayıklanması ve söz konusu verilerin hiçbir şekilde insan tesirine maruz bırakılmaması gerekmektedir[639].

3.5.2. Bulut Bilişimde Arama

Bulut bilişimin kullanılması yürütülmekte olan soruşturma sürecinde delil niteliğini haiz elektronik verilerin elde edilmesi bakımından önemlidir. Bununla birlikte üçüncü kişilerin kontrolünde olan verilerin ne şekilde elde edileceği ve bunların delil değerinin ne ölçüde bağlayıcı olacağı mevcut yasal düzenlemeler karşısında tartışma konusu olmaya devam etmektedir[640].

Bulut bilişim hizmetinin özel ve kapsamının dar olduğu bir ağda verildiği hallerde, şüpheli tarafından kullanılan hesap bilgilerinin CMK m. 134 uyarınca alınacak arama kararına istinaden elde edilmesi mümkündür. Bu durumda kullanıcının hesap bilgilerine ait olan verilerin elde edilmesi ve kopyalanması mümkün olacaktır[641].

Bununla birlikte, bulut bilişimde kişi sanal bir kullanım gerçekleştirmektedir. Bu nedenle, kişinin ancak hesabına bağlı veriler üzerinde arama yapılabilmelidir. Aksi takdirde bulut bilişim hizmeti veren kuruluşun sunucu bilgisayarlarının tamamında arama yapılabileceği anlamı çıkar ki, bu durum hem CMK m. 134 düzenlemesine ilişkin olarak kanun koyucunun arzu etmediği bir sonucun ortaya çıkması hem de suç soruşturması ile ilgisi olmayan üçüncü kişilerin mahremiyet haklarının ciddi şekilde zarar görmesi sonucunu doğuracaktır[642].

Diğer taraftan kamusal bulut açısından ise kamusal bulut hizmetinin sunulduğu yerin ülke sınırları içinde veya dışında olup olmadığına göre meselenin çözümü gerekmektedir. Kamusal bulut bilişim hizmetini sunan hizmet sağlayıcının ülke sınırları içinde bulunması durumunda, kamusal nitelikteki bulut bilişimde sunulan ve kullanıcıya

---

[639] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 366.

[640] Serhat Turan, "Bulut Bilişim (Cloud Computing) Teknolojisi ve Güncel Hukuki Problemler", (t.y.) http://www.egeweb.com/bulut-bilisimi-cloud-computing-teknolojisi-ve-guncel-hukuki-problemler-y17.html (23 Kasım 2014).

[641] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 242.

[642] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 322.

ait olan veri, program veya altyapı bilgilerinin elde edilmesinde farklı bir usul izlemek gerekmektedir. Burada kullanıcıya ait veriler bulunmakta ve söz konusu verilerin kişinin bilişim sistemlerinde tutulması ile bulut bilişimde tutulması arasında herhangi bir fark bulunmamaktadır. Bu nedenle CMK m. 134 uyarınca alınacak bir arama kararı ile bulut bilişimde arama yapma imkânı bulunmaktadır. Bulut bilişim hizmetini sunan hizmet sağlayıcısının ülke sınırları dışında bulunması durumunda ise bulut bilişimde arama yapılması ve verilere elkonulması adli yardımlaşma hükümleri çerçevesinde gerçekleştirilecektir[643].

[643] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 242-243.

BÖLÜM 4: ADLİ BİLİŞİM

4.1. Genel Olarak

Kriminalistik uzmanı Prof. Edmond Locard'ın ortaya koyduğu ve günümüzde locard teoremi olarak da bilinen "Değişim Prensibi"ne göre, bir ortamı terk eden bir kimsenin orada bulunduğuna dair iz bırakmaması ya da üstünde o ortamdan bir şeyler alıp götürmemesi mümkün değildir. Olay yeri incelemesi ile elde edilen en önemli şey maddi delillerdir. Bu tür deliller şüphelinin aleyhine dilsiz birer tanık niteliğindedir. Nitekim canlı tanıkların (şahitlerin) varlığı bile onları yok edemez[644].

Değişim prensibindeki birbirine temas eden iki nesne arasındaki değiş tokuş fiziksel ortamda söz konusu olduğu kadar dijital ortamlar için de söz konusudur. Bu bakımdan nasıl ki fiziksel ortamda her temas iz bırakmakta ise bilişim sistemleri üzerinde de iz bırakmadan işlem yapmak neredeyse imkânsızdır. Önemli olan bu izleri doğru bir şekilde tespit edip, sonuca götürücü verilere ulaşmaktır[645]. Bu işlemlerin sağlıklı ve bilimsel olarak yürütülmesi amacıyla da adli bilişim bilimi ortaya çıkmış ve gelişmiştir[646]. Bu doğrultuda da adli bilişim yöntemlerinin ve ceza muhakemesi ilkelerinin denkleme uygun biçimde yerleştirilmesi zorunluluğu ortaya çıkmıştır[647].

Uzun yıllar boyunca adli tıp, adli kimya gibi adli uzmanlık alanları suç soruşturmalarını yürüten makamlara yardımcı olarak birçok adli vak'anın bilimsel yöntemlerle çözülmesinde yardımcı olmuşlardır. Uzmanlar, olay mahallindeki biyolojik ve fiziksel izlerin kendilerine gösterdikleri ipuçları doğrultusunda olay hakkında ayrıntılı bilgi elde etme imkânını bulabilmişlerdir. Bununla birlikte, günümüzde suç ve suçluların elektronik ortamda kendilerini sıkça göstermeleri nedeniyle olayı aydınlatmaya çalışan

---

[644] Şevket Kümüştaş, "Maddi Delillerin Elde Edilmesi ve Hukuka Uygunluğu", **Çağın Polisi Dergisi**, Sayı. 66, (Haziran 2007), s. 36.

[645] Uzunay ve Bıçakçı, http://www.emo.org.tr /ekler/ 4843973f9b66701ek. pdf. (31 Ekim 2014).

[646] Çakır ve Sert, s. 146.

[647] Onur Özbek, "Hukuk Devletinde Bireysel Güvenlik Ekseninde Bilişim Teknolojileri", **1. Hukukun Gençleri Sempozyumu (Hukuk Devletinde Kişisel Güvenlik),** Ankara, 20-21 Mart 2009, http://www.umut.org.tr/tr-TR/hukukun-gencleri-sempozyumlari-dizisi--1-hukuk-devletinde-kisisel-guvenlik/111. aspx (25 Şubat 2015).

uzmanlar artık doğadaki iz ve emarelerin değil bilişim sistemlerindeki manyetik olarak kodlanmış vaziyetteki 1 ve 0'ların peşine düşmüşlerdir[648].

Adli bilişim kavramı tahmin edildiğinin aksine "adli" ve "bilişim" kelimelerinin bir araya getirilmesi sonucunda oluşturulmuş bir kavram değildir. Dilimize, "computer forensic" tanımından çevrilmiş olan ve yeni bir anlam kazandırılan adli bilişim kavramı, geniş bir anlama sahip olan "bilişim" kelimesinin esas alınması sonucunda "computer forensic"in Türkçe karşılığı olan "bilgisayar adli bilimi" kavramının yerine kullanılmaktadır.

Bununla birlikte adli bilişim kavramı önceleri yaygın olarak "computer forensic" kavramının karşılığı olarak kullanılmaya başlanmasına karşın bilişim teknolojisindeki baş döndürücü gelişmeler sonrasında gerçekte elektronik delilin yalnızca bilgisayarlarda bulunmadığının anlaşılması üzerine "computer forensic" kavramının yerine ondan daha genel nitelikte olan "digital forensic" kavramı da kullanılmaya başlanmıştır.

Adli bilişim, yeni bir hukuk dalı olarak ortaya çıkan ve fakat etkinliği günden güne artan bilişim hukuku konularına ilişkin bir yardımcı disiplin olarak doğmuştur. Nitekim adli bilişim yöntemlerine gerek ceza yargılamasında gerekse hukuki ihtilaflarda sıkça başvurulmaktadır. Bu bağlamda adli bilişim, ceza yargılamasında etkin biçimde kullanılmasına karşın özel hukuk alanındaki ihtilafların çözümünde de yargılamaya delil katkısı sağlayabilecek bir bilim dalı olarak kendini göstermektedir[649].

Adli bilişim süreci, bir bakıma olay yeri inceleme esaslarına benzemektedir. Bu süreç sonunda görünmez nitelikte olan elektronik delil, görünür ve anlaşılır hale gelmektedir. Süreç içerisinde bir elektronik delilin sonradan değiştirilip değiştirilmediği veya tahribata uğrayıp uğramadığı da saptanabilmektedir[650].

Adli bilişim, suçun aydınlatılabilmesi için bilimsel yöntemler kullanılarak, çeşitli varyasyonlardaki elektronik medyalar üzerinde bulunan, suçla ilgili elektronik delilin değişmeden ve zarar görmeden anlaşılabilir bir şekilde yargı makamları önüne

[648] Dokurer, Adli Bilişim, 2. Polis Bilişim Sempozyumu, s. 226.

[649] Özbey, s. 65.

[650] Ünal, s. 21.

sunulmaya hazır hale getirilmesini sağlayan ve başlı başına bilimsel teknik prensiplerin uygulandığı bir delil inceleme sürecinin bütünüdür[651].

Başka bir ifadeyle adli bilişim, elektromanyetik, elektro optik ortamlarda korunan ve/veya bu ortamlarca iletilen ses, görüntü, veri bilgileri veya bunun bileşiminden oluşan her türlü bilişim nesnesinin mahkemelerde elektronik delil niteliği taşıyacak biçimde tanımlanması, elde edilmesi, saklanması, incelenmesi ve mahkemeye sunulması sürecidir[652].

Adli bilişimi, bir yargılama sırasında kullanılabilecek potansiyel delillerin belirlenmesi için bilişim sistemlerinin kullanılması şeklinde tanımlamak da mümkündür. Nitekim adli bilişim, bilişim sistemleri kullanılarak ne, kim, nerede, ne zaman ve nasıl sorularına cevap bulmaya çalışmaktadır[653]. Bu bağlamda adli bilişim, elektronik delillerin ihtiva ettiği bilgileri, delil inceleme prosedürlerini, hukuki ve etik sorumlulukları göz önünde bulundurup delil bütünlüğünü koruyarak ve gerçeği açığa çıkartmak amacıyla elektronik delili toplama, inceleme, analiz etme ve raporlama sürecini ifade etmektedir[654].

Adli bilişimin, bilişim sistemlerindeki elektronik delile ilk temas edildiği andan yargı makamlarının önüne getirilmesi anına kadar geçen sürecin bütünü olarak ele alınması, onu, adli bilimler içerisinde değerlendirilecek bir disiplin haline getirmektedir. Nitekim adli bilişimin, ceza ve hukuk yargılamasında bilişim sistemlerinde bulunan delillerin toplanması, incelenmesi, analiz edilmesi ve raporlanması olarak değerlendirilmesi, adli bilimlerin bir alt disiplini olduğunu açık bir şekilde ortaya koymaktadır.

Elektronik delilin korunması, elektronik ve fiziksel koruma şeklinde kendini göstermektedir. Elektronik koruma, delillerin ilk alındığı andan itibaren değişmediğini, bütünlüğünün bozulmadığını ispatlayacak çeşitli mekanizmaları içermektedir. Bu genellikle kriptografik işlemler sayesinde gerçekleştirilmektedir. Fiziksel koruma ise,

---

[651] Ekizer, http://www.ekizer.net/adli-bilisim-computer-forensics (06 Nisan 2014).

[652] Ahmet Hasan Koltuksuz, "Adli Bilişimde Olay Yeri İnceleme Esasları", **Bilişim Hukuku Konferansı-YARGITAY**, Ankara, 09-10 Ekim 2008, s. 12.

[653] Servet Yetim, "Adli Bilişim ve Canlı Bilişim Sistemlerinde Dijital Delil Araştırma Yöntemleri", **Terazi Hukuk Dergisi**, Cilt. 2, Sayı. 11, (Temmuz 2007), s. 124.

[654] Say, Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi, s. 16.

delillerin incelenecek yere bozulmadan taşınması, mahkemeye sunulacağı ana kadar uygun ortamlarda saklanması ve yine mahkemeye götürülüş sırasında herhangi bir bozukluğa uğramamasını ifade etmektedir[655].

Bireylerin ve toplumların hayatında köklü ve evrensel değişimlere perde aralayan bilişim teknolojilerinin neden olduğu yeni felsefe ve düşünce sistematiği, yönetim ve iş yapma yöntemlerine yeni boyutlar kazandırmıştır. Bu bağlamda, elektronik delilin hukuka uygun bir delil olarak kabul edilebilmeleri, farklı bir mücadeleyi de beraberinde getirmektedir. Bu mücadelenin verilebilmesi için elektronik delil kavramının bilinmesi, elektronik delilin adli prosedüre uygun olarak toplanması ve değerlendirilmesi gerekmektedir. Her türlü çalışmanın idari bir takım tedbir ve iş yapma felsefesi ile desteklenmesi, suçla mücadelede etkinliğin artırılması açısından zorunludur[656].

Adli bilişimin temel amacı, elektronik veriler ile olay arasındaki bağlantıyı veya fiil ile işlenen veriler ve kullanıcı arasındaki bağlantıyı ortaya koymaktır. Hem ceza yargılamalarında hem de özel hukuk alanındaki ihtilaflarda adli bilişim yöntemlerine başvurulmaktadır[657].

Adli bilişimin hukuki boyutundan ziyade, teknik boyutu daha ön plana çıkmaktadır. Zira elektronik sistemlerdeki bulguların, bunlardan ayrıştırılarak birer hukuki delile dönüştürülme süreci, oldukça zahmetli, son derece teknik bilgi gerektiren ve uzmanlık isteyen bir iş görünümündedir[658]. Bununla birlikte adli bilişim çalışmalarını sadece delil toplama ve sunma süreci olarak ele almayıp bilgisayar depolama ortamları üzerinden yapılan sistematik bir inceleme süreci olarak da değerlendirmek gerekmektedir[659].

Adli bilişim bilimi müstakil bir bilim olup daha çok adli kolluk birimini ve savcıları ilgilendirmektedir. Adli bilişim işlemlerini yapabilmek için, bilişim sistemlerine ve

---

[655] Gözüşirin, s. 94-95.

[656] Mustafa İlker Öztürk, s. 3.

[657] Henkoğlu, s. 1.

[658] Tan, http://mbasic.facebook.com/notes/gazi-%C3%BCniversitesi-adli-bili%C5%9Fim-anabilim-dal%C4%B1/adli-bili%C5%9Fim-computer-forensic-aydo%C4%9Fan-tan/502561823148516/?refid=17 (06 Nisan 2014).

[659] Hüseyin Çakır ve Mehmet Serkan Kılıç, "Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bir Bakış", **Polis Bilimleri Dergisi**, Cilt. 15, Sayı. 3, (2013), s. 24.

diğer cihazlara usulüne uygun şekilde elkoymak, adli bilişim kurallarına uygun şekilde yedekleme yapmak, alınan yedekleri incelemek, mahkemeye sunulacak şekilde hazırlamak ve uygun şekilde paketlemek, taşımak ve saklamak gerekmektedir[660]. Bu bakımdan, olay yerinde bulunup incelemeye alınan herhangi bir materyal mahkemede kabul edilmediği sürece delil niteliği taşımayacağından adli bilişim süreci ne kadar çok usule uygun gerçekleşirse elde edilen bulguların da mahkemece delil niteliği taşıma olasılığı o derece artacaktır[661]. Nitekim adli bilişim, kimi zaman kovuşturmaya konu olayın çözümünde tek delil niteliğindeki bir elektronik verinin herhangi bir zarara uğramaksızın mahkeme önüne getirilmesi fonksiyonunu üstlenmektedir[662].

Bilişim sistemleri ve diğer elektronik cihazlar üzerindeki adli bilişim işlemleri, gerek bu cihazların kişiler tarafından suç işlemede araç olarak kullanılması gerekse herhangi bir suçun işlenmesinde doğrudan kullanılmayıp kişilerin bu cihazları kendi aralarındaki iletişim için veya işlemlerini kolaylaştırmak ve bilgileri yedeklemek için kullanmaları durumunda gerçekleştirilmektedir[663].

Hayatın her alanında var olan suç olgusu, teknolojiyi de araç olarak kullanmakta, buna bağlı olarak geleneksel suçların yapısı değişmekte, sonuçta da bilişim ortamlarında işlenilmekte olan suç miktarı artmaktadır[664]. Kişilerce işlenen suçların cezalandırılması ve bunun için gerekli adil yargılamanın gerçekleşebilmesi ise usulüne uygun elde edilecek delillerle mümkündür. Bu bakımdan, adli bilişim süreci, elektronik delilin önem arz ettiği suçlar bakımından hayati öneme sahiptir.

Adli bilimler içerisinde yer almakta olan adli bilişim bilimi sayesinde suç ve suçlu ile mücadele edilmekte, işlenen suçların delillendirilmesi sağlanmakta ve suçla ilgisi olmayan masum kişiler korunabilmektedir[665]. Bugün hemen herkes tarafından birçok

---

[660] Aydoğan, s. 9.

[661] Dokurer, Adli Bilişim, 2. Polis Bilişim Sempozyumu, s. 227.

[662] Onur Özbek, http://www.umut.org.tr/tr-TR/hukukun-gencleri-sempozyumlari-dizisi--1-hukuk-devletinde-kisisel-guvenlik/111. aspx (25 Şubat 2015).

[663] Aydoğan, s. 9.

[664] M. Zekeriya Gündüz, "Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti", (**Yayınlanmamış Yüksek Lisans Tezi**, Fırat Üniversitesi FBE, 2012), s. 23.

[665] Çakır ve Kılıç, s. 24.

işin yapılmasında bilgisayarlar veya diğer elektronik cihazların kullanıldığı düşünüldüğünde, sadece bilişim suçlarının araştırılması ve soruşturulmasında değil diğer birçok suç türünün araştırılması ve soruşturulmasında adli bilişim tekniklerinden yararlanıldığı görülmektedir[666].

Bununla birlikte, günümüzün teknik gelişmelerine bağlı olarak hızla gelişimini devam ettiren adi bilişim bilimi, yargı organlarına yardımcı olmanın yanı sıra bugün bazı şirketler ve kişiler tarafından da veri kurtarma, imha etme veya sair amaçlarla ihtiyaç duyulan bir alan haline gelmiştir. Nitekim günümüzde birçok büyük şirket, bünyelerinde bir adli bilişim uzmanı görevlendirme veya bu konuda hizmet veren firmalarla sürekli çalışma yolunu seçmektedir[667].

Adli bilişim sürecinin belirleyici iki unsurundan birisi adli bilişim uzmanı iken; diğeri ise söz konusu incelemenin yapılacağı laboratuvar ortamı ve kullanılacak donanımlar ve yazılım programlarıdır[668]. Bu bakımdan, bu sürecin genellikle olay yerinde kolluk birimleri ve sonrasında da bilirkişiler tarafından (çoğu zaman laboratuvar ortamında) yerine getirildiği görülmektedir[669].

Suçlular adli bilişim biliminin ve adli bilişim uzmanlarının soruşturma becerilerinin farkında olmalarından dolayı işlemiş oldukları suç sırasında bilişim sistemlerini ve ağları daha karmaşık şekilde kullanmaktadırlar. Bazıları ise adli bilişim yöntemlerinin başarılı olamamasını sağlamak amacıyla eylemlerini gizlemek ve elektronik delilleri yok etmek için verileri geri dönülemez şekilde silme, verileri gizleme, verileri bozma, dosya imzalarını bozma ve hash çakışması oluşturma gibi bazı delil karartma (anti forensic) yöntemleri geliştirmekte ve buna yönelik araçlar icat etmek suretiyle çoğu zaman adli bilişim uzmanlarının işlerini zorlaştırmaktadırlar. Bu durum adli bilişim uzmanlarının adli bilişim sürecinde son derece dikkatli olmalarını gerekli kılmaktadır.

---

[666] Yetim, Dijital Kanıt Araştırma Yöntemleri, s. 1209; Tan, http://mbasic.facebook.com/notes/gazi-%C3%BCniversitesi-adli-bili%C5%9Fim-anabilim-dal%C4%B1/adli-bili%C5%9Fim-computer-forensic-aydo %C4%9Fan-tan/502561823148516/?refid=17 06 Nisan 2014.

[667] Gündüz, s. 23.

[668] Leyla Keser Berber, **Adli Bilişim,** Ankara: Yetkin Yayınları, 2004, s. 7.

[669] Henkoğlu, s. 22.

Genel olarak olay yerinde gerçekleşen işlemlere "elektronik delilin toplanması ve muhafazası", laboratuvar ortamında yapılan işlemlere ise "elektronik delilin incelenmesi" ve "elektronik delilin analizi" denilmektedir. Son olarak "elektronik delilin raporlanması ve sunumu" ile de adli bilişim süreci sonuçlandırılmaktadır. Öğretide adli bilişim süreci farklı isimlerle tanımlanmakla birlikte biz çalışmamızda adli bilişim sürecini yukarıda belirtilen tanımlamaya uygun şekilde inceleyeceğiz.

4.2. Elektronik Delilin Toplanması ve Muhafazası

4.2.1. Genel Olarak

Bir suçun varlığından şüphelenilmesi durumunda bahse konu suç veya olayla ilgili potansiyel delillerin toplanması gerekir. Sürecin doğru bir şekilde işlemesi, uygun prosedürün uygulanmasına ve hukuki şartların yerine getirilmesine bağlıdır. Deneyimli soruşturmacılar için bu safhadaki temel amaç, elektronik veya fiziksel tüm delilleri toplama değil, nelerin toplanıp nelerin toplanılmayacağı hususunda mantıklı kararlar vermek, doküman oluşturmak ve sonrasında da gereğini yerine getirmektir[670].

Elektronik delil toplama süreci hukuka uygun bir zeminde başlamalıdır. Bu bağlamda öncelikle, eğer bir adli soruşturma kapsamında elektronik delil toplanacaksa -ülke uygulamasına göre- arama ve elkoyma öncesinde gerekli hukuksal sürecin işletilmesi ve bu hususta yazılı bir savcılık veya mahkeme emrinin bulunması gerekmektedir[671].

Bu aşamada, adli kolluk görevlilerinin yapacakları arama işlemlerinde ciddi bir plan dâhilinde hareket etmeleri gerekir. Bu plan yalnızca arama işlemlerinin gerçekleştirilmesiyle ilgili değildir. Söz konusu plan, en başta arama kararı alınırken büyük öneme sahiptir. Soruşturma evresinde, işin başında yapılacak arama planı, alınacak arama kararının kapsamını da belirleyecektir. Arama kararı talebinin ciddi bir plan dâhilinde yapılmaması durumunda ise alınan arama kararına dayalı olarak yapılan arama işlemleri sırasında, çoğu zaman arama kararının kapsamı yetersiz gelmekte bu durum da yeni bir arama kararının istenmesi, yetkisiz arama işlemi yapılması ve arama

[670] Gündüz, s. 13.

[671] Jasmin Cosic and Zoran Cosic, "Chain of Custody and Life Cycle of Digital Evidence", **Computer Technology and Application**, Vol. 3, No. 2, (February 2012), s. 127.

işlemine son verilerek başarısızlığa neden olunması gibi sorunlara neden olabilmektedir. Belirtmek gerekir ki, bu durumda, yeni bir arama kararı istenilmesi en uygun çözüm gibi görünse de, arada geçecek zaman nedeniyle, bilişim sisteminin kendine özgü yapısı karşısında, başarı elde edilebilmesi zordur[672].

Diğer taraftan elektronik delile ilk kimin temas edeceği hususu da son derece önemlidir. Bu hususta ülkeden ülkeye farklılık arz eden bir uygulama söz konusudur. ABD gibi bazı ülkelerde bu tür delillere nasıl davranılması gerektiği konusunda eğitim almış özel birimler (ilk müdahale ekipleri) bulunurken Türkiye gibi kimi ülkelerde ise bu işi söz konusu hususta herhangi bir eğitim almamış kolluk personeli (polis memuru) yerine getirmektedir[673].

Günümüzde bilişim sistemleri suç işlemek için kullanılabilmekte, suça ilişkin delilleri içerebilmekte ve hatta bizatihi kendileri suçun hedefi olabilmektedirler. Bu bakımdan olaya ilk müdahale eden personelin elektronik delilin tanınmasında, bulunmasında, korunmasında ve taşınmasında temel bilgilere sahip olması hassas bir yapıya sahip olan elektronik delil için oldukça önemlidir[674].

Elektronik delil yapısı gereği, dış dünyaya ancak görsel veya işitsel olarak yansıtılabilir. Ancak, elektronik delilin elde edilmesi kolay değildir. Çoğunlukla, incelenen bilişim cihazlarından başka bilişim materyali kullanılarak delil elde edilmeye çalışılmaktadır. Bu nedenle kullanılacak ürünlerin kapsamı ve yetenekleri ölçüsünde delil elde edilebilmektedir. Bu döngünün sorgulanabilmesi için bilişim cihazlarında suça ait iz ve emarelerin bulunabileceği yerlerin iyi bilinmesi ve tüm ihtimaller üzerinde titizlikle durulması gerekmektedir. Bilişim cihazlarındaki elektronik delilin tespiti için en önemli husus, bu cihazların iyi tanınması ve delil olabilecek verilerin iyi bilinmesidir[675].

Elektronik delilde bilgiler manyetik ortamda yazılarak saklanır. Bu bakımdan suçtaki hedef alanın niteliğine göre elektronik delil elde etme yöntem ve donanımı (programı)

[672] Karagülmez, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, s. 98.

[673] Cosic and Cosic, s. 127.

[674] Ali Osman Özdilek, **Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku**, İstanbul: Vedat Kitapçılık, 2006, s. 202.

[675] Mustafa İlker Öztürk, s. 55-56.

da farklılık gösterebilir. Bu karmaşık yapı içerisinde, delillerin toplanmasında yapılacak yanlış bir müdahale işi başarısız kılabilir[676].

Elektronik delil toplandığında devletin adli makamları tarafından muhafaza altına alınması gerekir. Muhafaza aşaması aynı zamanda koruma zinciri (chain custody) oluşturulması sürecini ihtiva etmektedir. Nitekim koruma zincirinin herhangi bir şekilde bozulması elektronik delilin geçerliliği konusunda şüpheye neden olacaktır. Diğer taraftan, muhafaza aşaması elektronik delile kasıtlı zarar vermek isteyen kötü niyetli kişilerden veya kazara zarar verebilmesi muhtemel tecrübesiz personelden güvenli bir şekilde korunmasını da içermektedir.

Elektronik delilin toplanması ve muhafazası aşamasında, delillerin toplanması, delillerin bütünlüğünün sağlanması ve kontrol edilmesi yapılmaktadır. Aslında bu aşamadan önce veya bu aşamayla birlikte yürütülen bir başka süreç de elektronik delilin belirlenmesi/tespiti sürecidir. Bu süreçte ise nelerin elektronik delil olduğu belirlenerek buna göre delil toplama ve muhafaza işlemi yürütülmektedir[677].

Elektronik delilin tespiti ve toplanarak muhafaza altına alınmasının kendine mahsus özellikler arz etmesine karşın elektronik delilin araştırılma yöntemleri ile fiziksel delillerin araştırılma yöntemleri birçok yönüyle de benzerlik göstermektedir. Bilişim sistemleri, suçlular tarafından suçun işlenmesinde araç olarak kullanılmaları veya herhangi bir suçun işlenmesinde doğrudan olmasa bile suçluların kendi aralarındaki iletişimi veya işlemleri kolaylaştırmak ve bilgileri yedeklemek için kullanmaları durumunda adli bilişime konu olmaktadır. Bilgisayar teknolojileri işlenen suçların araştırılmasında kullanılan aygıtlar olabileceği gibi bu cihazların kullanılması ile de birçok suç işlenebilmektedir. Nitekim kasten öldürme eyleminin silahla gerçekleştirilmesi ile dolandırıcılık eyleminin bilişim sistemleri aracı kılınarak gerçekleştirilmesi arasında fark bulunmamaktadır[678].

---

[676] Karagülmez, Bilişim Suçlarında Delil Toplamayı Etkileyen Başlıca Konular, s. 31.

[677] Osman Nihat Şen, "Polisin Adli Bilişimde Kullanabileceği Programların Bir Değerlendirmesi", **2. Polis Bilişim Sempozyumu**, Ankara, 14-15 Nisan 2005, s. 36.

[678] Yetim, Dijital Kanıt Araştırma Yöntemleri, s. 1209.

Bilgisayar bağlantılı suçların araştırılması sırasında olay yerinde çalışma yapan adli bilişim ekibinin en çok zaman ayırdığı aşama delillerin toplanması ve belgelere kaydedilmesi aşamasıdır. Bu aşamada gösterilen titizlik, elektronik delilin nerelerden elde edilebileceği hakkında önemli ipuçlarının yakalanmasını sağlayabilir[679].

4.2.2. Elektronik Delil Toplanırken Uyulması Gereken Temel İlkeler

Elektronik delilin toplanması ve muhafaza edilmesi aşaması adli bilişim sürecinin başlangıç aşaması olup delil bütünlüğünün sağlanması bakımından çok önemli bir safhasıdır. Zira bu aşamada elektronik delilin zarar görmesi veya yok olması oldukça muhtemeldir. Nitekim bilgisayarın basit bir şekilde hareket ettirilmesi bile kimi zaman dosya, veri, zaman mührü (damgası) gibi elektronik nitelikteki delilin değişmesine neden olabilmektedir. Bu durum ise elektronik delilin toplanması aşamasında bazı kurallara riayet etme zorunluluğunu doğurmaktadır.

Ülkemizde elektronik delilin ne şekilde elde edileceğine ilişkin kapsamlı bir yasal düzenleme bulunmamaktadır. Oysa -ABD gibi- kimi ülkelerde, soruşturma evresinde elektronik delilin elde edilmesine ilişkin çalışmalarda bulunan teknik ekibin nasıl hareket edeceklerini bağlayıcı kılan, yanlış yapılan işlemlerin bir ihlal olarak değerlendirilerek cezai takibatı gerektireceğini düzenleyen yasal hükümler yer almaktadır. Ülkemizdeki, elektronik delilin elde edilmesine ilişkin yasal boşluğun başlıca nedenleri arasında bilişim teknolojilerinin ülkemize alt yapısı olmaksızın ithal edilmiş olması, işlenen bilişim suçlarının boyutlarının yeterince bilinmemesi ve suç mağdurlarının konunun farkında olmaması gösterilebilir[680].

Adli bilişim süreci günümüzde soruşturma ve kovuşturma işlemlerinin ayrılmaz bir parçası haline gelmiştir. Suç ve suç yeri ile ilk temasa geçen kolluk görevlilerinin aranıp gerektiğinde elkonulacak bilişim sistemlerine ve ekipmanlarına nasıl müdahalede bulunmaları, bunları incelemenin yapılacağı yere ne şekilde götürmeleri gerektiğine ilişkin tavsiye kuralları veya örnek uygulamanın bilinmesi ve yerine getirilmesi,

[679] Henkoğlu, s. 5.

[680] Karagülmez, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, s. 403.

toplanan delillerin hukuka aykırılığı iddialarının önüne geçilmesi açısından büyük önem taşımaktadır[681].

Elektronik delil elde etme aşaması elektronik delile yönelik olay yeri çalışması ile başlar ve elektronik delil elde edilmesi muhtemel bilişim cihazlarına usulüne uygun müdahale edilmesi ile devam eder. Bu bakımdan olay yerinde yapılan işlemlerde yapılan hatalar delillerin gerçekliği ve güvenilirliğine gölge düşürebilir ve tüm süreci sekteye uğratabilir[682].

Olay yerini inceleyen ilk müdahale ekibi öncelikle delil elde etmede kullanılacak cihazları hazır etmeli, kendi güvenliğinden emin olmalı, olay yerinin güvenliğini sağlamalı, daha sonra da olay yerindeki elektronik nitelikte olan veya olmayan tüm delillerin sağlamlığını ve bütünlüğünü koruma altına almalıdır[683].

İşlemlere başlamadan önce kullanılacak olan kontrol listeleri, donanım birimleri ve ihtiyaç duyulacak yazılımlar hazırlanmalıdır. Kontrol listeleri, olay yerindeki olumsuz havanın etkisine rağmen, herhangi bir adımı atlamadan, sağlıklı ve eksiksiz bir çalışma yapılmasına yardımcı olacaktır[684].

Elektronik delil elde etme işlemleri mümkün oldukça adli bilişim uzmanları tarafından yapılmalıdır. Gerçekten de, elektronik delilin elde edilmesi aşamasında değişikliğe uğramaması bakımından bu işe liyakatsiz kimselerin karışması, işi baştan sonuçsuz kılabilir. Bu bakımdan elektronik delilin elde edilmesi için işi iyi bilen bir adli bilişim uzmanının delil elde etme işlemini sürdürmesi gerekmektedir. Elektronik delilin fiziksel delillere göre farklı yapısı bu durumu zorunlu kılmaktadır[685]. Zira ancak bir adli bilişim uzmanı, delil kaybına neden olmaksızın -ya da mümkün olan en az kayıpla- elektronik delili toplayabilecektir[686].

---

[681] Keser Berber, Adli Bilişim, s. 7.

[682] Henkoğlu, s. 17; Aydoğan, s. 13.

[683] Yetim, Dijital Kanıt Araştırma Yöntemleri, s. 1209.

[684] Henkoğlu, s. 19.

[685] Karagülmez, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, s. 401; Çakır ve Sert, s. 156.

[686] Özbey, s. 73.

Olay yerinde herhangi bir işleme başlamadan önce ve yapılan işlemler sırasında olay yeri ile bilgisayar sistem ve donanımlarının farklı açılardan ve mümkün olduğunca çok sayıda fotoğrafı çekilmelidir. Ayrıca sistemin tüm bağlantıları, irtibatları, görüntüleri, ekranları üzerindeki yazılar ve seri numaraları detaylı ve incelenebilecek şekilde görüntüye alınmalıdır. Çekilen fotoğraflar ve alınan görüntü kayıtları, gözden kaçan noktaları sonradan tespit edebilmek ya da daha sonra duyulabilecek şüpheleri gidermek amacıyla kullanılabilir[687].

İnceleme sırasında faydalı olacağından olay yerinde bulunan bilişim sisteminin bağlantı şemasının çizilmesi gerekmektedir. Elektronik delillere zarar verecek herhangi bir duruma karşı dikkatli olunmalı, olay yerinde hesap adı, şifre bilgisi olabilecek notlara dikkat edilmelidir[688].

Olay yerinde bulunan ve delil olarak değerlendirilmesi muhtemel tüm malzemelerin üzerinde yeterli açıklayıcı bilgi bulunan delil etiketleri ile etiketlenmesi oldukça önemlidir. Diğer taraftan bir envanter oluşturularak olay yerinde elkonulan tüm nesneler seri numaraları ile birlikte kaydedilmelidir. Her türlü nesne için farklı bir envanter listesi oluşturulmalı ve oluşturulan listeler grup içerisinde bulunan farklı kişiler tarafından da kontrol edilmelidir. Envanterlerin kopyalanması ve her kopyanın imzalatılması ihmal edilmemelidir[689]. Ayrıca elkonulan bilişim sistemlerinin daha sonra tekrar birleştirilebilmesi için tüm kablolar renk kodu ile kodlanmalıdır[690].

Elektronik delilin elde edilmesi ile ilgili tüm işlemler belgelenmeli (tutanağa bağlanmalı) ve yeni bir inceleme için kullanılabilir halde korunmalıdır. Elektronik delilin elde edilmesine ilişkin araştırmalar fiziki ortama dayalı olmadığı için başından sonuna kadar yapılan işlemlerin tek tek tutanağa bağlanması önem taşımaktadır. Zira bu tutanaklar, elektronik delilin, delil niteliğini kuvvetlendirmekte ve onunla bütünleşmektedir. Diğer taraftan elektronik delilin elde edilmesi işlemleriyle ilgili her aşamada tutulan tutanaklar, kovuşturma aşamasında bu delile ceza muhakemesi

[687] Mustafa İlker Öztürk, s. 67; Henkoğlu, s. 19.

[688] Günal, s. 41.

[689] Henkoğlu, s. 19.

[690] Değirmeci, s. 214.

kurallarına göre yöneltilen itirazlar karşısında, tarafsız uzman bilirkişi raporu alınmasında, bu delilin gerçekten söz konusu bilişim sisteminden elde edilip edilmediğinin kontrolü bakımından da kolaylık sağlayacaktır[691].

Olay yerinde bulunan bilişim sistemlerinden kapalı olanlarının açılmaması gerekmektedir. Zira bilişim sistemlerinde elektronik delilin bulunması muhtemel durumlarda sistemin açılması mevcut delillerin zarar görmesine sebep olabilir. Örneğin, bilişim sistemlerinin işletim sistemleri açılırken birçok konfigürasyon dosyasına erişim sağlanmakta ve delil niteliğindeki verilerin zarar görmesine yol açılabilmektedir. Dosyaların erişim tarihlerinin dahi bazı durumlarda delil niteliği taşıyabileceği düşünüldüğünde böyle bir uygulama sakınca doğurabilir. Aynı zamanda, işletim sistemlerinin açılırken oluşturabilecekleri geçici dosyalar ve geçici hafıza disk alanları daha önceden silinmiş verilerin delil niteliğinde kurtarılabilme ihtimalini ortadan kaldırmış olacak ve bu durum da delil bütünlüğünün bozulmasına neden olacaktır[692].

Diğer taraftan, olay yerinde bulunan bilişim sistemlerinden açık durumdaki bilişim sistemlerine ise dokunulmamalı, ekranda açık olan herhangi bir pencere ya da yapılan bir işlem varsa bu durum tutanağa bağlanmalı, sonrasında ise cihazın türüne göre kontrol edilerek gücü kesilmek suretiyle kapatılmalıdır. Ayrıca, bilişim teknolojileri ile ilgili bir olay yeri müdahalesi öncesinde muhtemel olay yerine uzaktan erişim ile delillerin karartılması ihtimaline karşı elektromanyetik koruma sağlayacak donanım ve yazılımlar bulundurulmalıdır[693].

Olay yerinde elektronik delilin dışında fiziksel delillerinin de yer alması kuvvetle muhtemeldir. İnceleme yapılacak bilgisayar ve bağlı donanımlar üzerinde bulunabilecek parmak izleri, olay mahallinde bulunan şüpheliye ait giysiler ve sair eşyalar da delil niteliğinde olabilir. Bu bakımdan konuyla ilgili kriminalistik inceleme de ihmal edilmemelidir. Ancak bu inceleme, hassas yapıya sahip elektronik delile zarar vermeden

[691] Karagülmez, Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, s. 401.

[692] Ekizer, http://www.ekizer.net/adli-bilisim-computer-forensics (06 Nisan 2014).

[693] Mustafa İlker Öztürk, s. 68; Çakır ve Sert, s. 157.

gerçekleştirilmelidir. Bu bakımdan, kriminal veri toplama işlemleri ile adli bilişim verileri toplama işlemleri arasında makul bir denge sağlanmalıdır[694].

İmaj alma işlemi sırasında farklı bilgisayarlar kullanılmalı ve imajların karışmaması için yapılan isimlendirme ve etiketleme işlemlerinde titiz davranılmalıdır. Ayrıca, tüm veri depolama birimlerinin adli bilişim standartlarına uygun şekilde imajları alınmalıdır. Taşıma esnasında orijinal diskler güvenli ortamlarda ve zarar gelmeyecek şekilde saklanmalıdır[695].

4.2.3. Canlı Analiz İşlemi

Elektronik delil toplamak amacıyla olay yerine gelen ekipler, öncelikle üzerinde inceleme yapılacak olan bilgisayarların düzgün bir şekilde kapatılması ve muhafazasından sorumludurlar. Bundan sonra ise söz konusu bilgisayarlar üzerinde bulunan ve diğer veri depolama ünitelerinin imaj alma işlemlerine başlanır. Bununla birlikte üzerinde inceleme yapılacak bilgisayarların kapatılması veya yeniden başlatılması, sistem üzerinde bulunan uçucu verilerin kaybedilmesine neden olmaktadır[696].

Birkaç yıl öncesine kadar adli bilişim sürecinde incelenen bilgisayarın çalışır vaziyetteyken elkonulmasına karar verildiğinde bilgisayarı kapatarak değil geleneksel metot olan doğrudan kablo çekilmek (pull the plug) suretiyle elektriğin birden kesilmesi sonucunda bilgisayar kapatılmakta ve böylece elkoyma işlemi gerçekleştirilmekteydi. Bu yöntemle elektrik kesilmesi sonrasında kapanan bilgisayardaki bilgilerin bilgisayar içerisinde bir yerlere kaydedilmesi ve sonrasında bilgilerin soruşturmada kullanılması hedeflenmekteydi[697].

---

694 Tan, http://mbasic.facebook.com/notes/gazi-%C3%BCniversitesi-adli-bili%C5%9Fim-anabilim-dal%C4%B1/adli-bili%C5%9Fim-computer-forensic-aydo%C4%9Fan-tan/502561823148516/?refid=17 (06 Nisan 2014).

695 Henkoğlu, s. 21.

696 Henkoğlu, s. 26.

697 Bilal Şen, "Elektronik Ekipmanlarda Arama El Koyma ve Elektronik Deliller", **Ankara Barosu Uluslararası Hukuk Kurultayı**, Cilt. 3, Ankara, 11 Ocak-15 Ocak 2010, s. 69.

Bununla birlikte zaman içerisinde gelişen teknolojiyle açık biçimde elkonulan bilgisayarlarda bulunan uçucu verilerin olayların aydınlatılmasındaki önemi anlaşılarak bilgisayar kapatıldığında kaybolacak uçucu verilerin kaybolmaya maruz kalmaksızın elde edilmesine yönelik araçlar üretilmiş ve aynı amaçla canlı analiz yöntemi uygulanmaya başlanmıştır.

Günümüzde çalışır vaziyette bulunan bilgisayar sistemlerindeki uçucu verilerin toplanması amacıyla canlı analiz yapma özelliğine sahip birçok yazılım bulunmaktadır. Bu yazılımların en önemli özelliği sisteme kurulmadan çalışabilmeleridir. Bu sayede incelenen sistemin diski üzerinde herhangi bir ekleme yapılmaksızın ve elektronik delilin orijinalliği bozulmaksızın gerekli işlemler yapılabilmektedir[698].

Canlı analiz yöntemi, sıradan elektronik delil elde etme işleminin ötesinde teknik uzmanlık gerektiren bir yöntemdir. Bazen, suç işlemekte çokça kullanılan bilgisayarlar üzerinde, elektronik delilleri yok edecek veya bir virüsü etkin hale getirebilecek tuzakların bulunduğu görülmektedir. Özellikle, zararlı kodların dağıtımı, siber saldırılar, kredi kartları ve internet aracılığıyla işlenen dolandırıcılık suçlarının işlenmesinde kullanılan bilgisayarlar üzerinde yapılacak incelemelerde söz konusu bilgisayarlar kapatılmadan uçucu verilerin elde edilmesi ve kayda alınması gerekmektedir. Elektronik delillerin toplanması sırasında uçucu verilerin elde edilmesi amacıyla kullanılan bu yöntem, herhangi bir siber saldırıya maruz kalınması halinde, sistem yöneticileri tarafından verileri kurtarmak amacıyla da kullanılmaktadır[699].

Bu bağlamda, olay yerine varıldığında açık olan bir bilgisayarla karşılaşılması ve bilgisayar üzerinde bazı şifreleme programlarının tespit edilmesi durumunda bilgisayar kapatılmadan önce canlı analiz işleminin yapılması gerekmektedir. Canlı analiz işlemini gerekli kılan diğer bir husus ise, olay yerinde açık halde bulunan bilgisayarın üzerinde hâlihazırda şüpheli programların çalışıyor olması ve ekranda delil niteliğine sahip

[698] Henkoğlu, s. 29.

[699] Henkoğlu, s. 27.

dosyaların açık bulunmasıdır. Zira uçuculuğu yüksek olan bu tür verilere de sistemin kapatılması halinde tekrar ulaşılması imkânsızdır[700].

Ağ trafiği bilgilerinin elde edilmesine yönelik işlemler de canlı analiz işlemini gerekli kılan başka bir durumdur. Ağ trafiği bilgileri toplanırken, sistem canlı halde bulundurulduğundan sistemin anlık resminin çekilmesi suretiyle o anda sistemde bulunan veriler ele geçirilerek analize tabi tutulmaktadır[701].

4.2.4. İmaj Alma (Birebir Kopyalama)

Elektronik verinin elde edilmesi sürecine ilişkin olarak soruşturma veya kovuşturmaya konu suçun aydınlatılmasına fayda sağlayacak elektronik verinin orijinalinin elde edilemeyerek sadece normal kopyasının elde edildiği bir durumda, bu kopya üzerinden yeni bir kopya çıkartılarak bilirkişi incelemesi yapılması usule uygun kabul edilmeyecektir. Zira genel hukuk kuralları gereğince belgeler üzerinde yapılacak olan sahtecilik incelemesinin, ancak orijinal metin üzerinden yapılması gerekmekte olup, fotokopi üzerinden sahtecilik incelemesi yapılamayacağından normal kopyası elde edilen bir elektronik verinin de geçerli bir elektronik delil olarak kabul edilmesi olayın ispatı konusunda soru işaretlerine neden olacaktır.

Bununla birlikte adli bilişim sürecinde elektronik verinin imajının (birebir kopyasının) alındığı durumlarda elektronik verilerden hangisinin asıl olduğunun bir önemi bulunmayacağından belge fotokopilerinin, aslı gibi oldukları tevsik edilmediği sürece hukuksal sonuçlar doğurmayacağına ilişkin genel kuralın imajı alınan elektronik delil bakımından geçerli olmadığı söylenebilir[702].

Bilişim sistemlerinde kopyalama işlemi genellikle üç seviyede gerçekleştirilir. Bunlar, dosya seviyesi, bölüm seviyesi ve disk seviyesi kopyalamalarıdır. Dosya seviyesinde ve bölüm seviyesinde yapılan kopyalamalar, herhangi bir dosyayı normal bir kullanıcı olarak kopyalamaktadır. Bu durumda, diskte bulunan silinmiş veya kısmen silinmiş dosyalar kurtarılamayacaktır. Ancak disk seviyesinde yapılan kopyalama ile orijinal

[700] Henkoğlu, s. 27.

[701] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 223.

[702] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 140.

diskin birebir kopyası alınabilmektedir. Adli bilişimde kullanılan kopyalama yöntemi de disk seviyesinde yapılan birebir kopyalamadır. Bu kopyalama türünde orijinal disk ile kopya disk her anlamda birbirine denktir[703].

Adli bilişimde yapılan birebir kopyalama işlemine imaj (forensic image) denilmektedir. Birebir kopyalama, veri depolama birimi üzerindeki tüm verilerin kopyasının alınmasını ihtiva etmektedir. Alınan birebir kopya, mevcut verileri, silinmiş verileri, gizli bölümleri, veri depolama birimindeki diğer verileri de kapsamaktadır[704]. Ancak birebir kopyalama işlemi sırasında uygun adımlar atılmak suretiyle orijinal veride meydana gelebilecek değişikliklerin önüne geçilmelidir. Bu husus elektronik delil toplama aşamasının en önemli unsurlarından birisidir[705].

Bilişim sistemlerinde yer alan verilerin imajının alınmasının amacı verilerin bütünlüğünü ve güvenilirliğini sağlamaktır. Verilerin imajının alınması iki açıdan verilerin bütünlüğünün ve güvenilirliğinin sağlanmasına hizmet etmektedir. Öncelikle şüphelinin kullanmış olduğu bilişim sisteminde elkonulan verilerin daha sonra değiştirilmemiş, verilere herhangi bir ekleme veya çıkarma yapılmamış olduğu güvence altına alınmış olacaktır. Bu sayede savunma tarafından ileri sürülecek "delillerin değiştirildiği veya sonradan eklendiği" yönündeki iddiaların önüne geçilmiş olacaktır. İkinci olarak ise bilişim sistemindeki verilerin toplanması aşamasında verilerin zarar görmesinin önlenmesi sağlanacaktır. Nitekim bilişim sisteminde veri toplanması zor ve riskli bir faaliyet olduğundan bazı durumlarda sistemde yer alan veriler toplama faaliyeti sırasında zarar görebilmektedir[706].

Disk imajının oluşturulması, elektronik delilin adli analiz sürecinin başlangıç noktasıdır. Disk imajının doğru bir şekilde alınması, tüm adli süreci etkileyebilecek kadar önemli bir konudur. Alınan imajın doğruluğunun, elektronik delilin adli analizinin yapılması ve mahkeme süreci esnasında sorgulanması bunun bir göstergesidir. Elektronik delilin

---

[703] Say, Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi, s. 71.

[704] Ahmet Serhat Şirikçi ve Nergis Cantürk, "Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi", **Bilişim Teknolojileri Dergisi**, Cilt. 5, Sayı. 3, (Eylül 2012), s. 30.

[705] Stephen Mason (Ed.), **International Electronic Evidence,** London: BIICL, 2008, s. xlvi.

[706] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 76.

analizinin söz konusu delil üzerinde doğrudan gerçekleştirilmesi, üzerinde suç şüphesi bulunan veri depolama biriminin zarar görmesine veya inceleme yapan kişi tarafından verilerin değişmesine neden olabilmektedir[707].

İnceleme ve analiz işlemleri sırasında yapılacak küçük nitelikteki bir hata bile kimi zaman delil olabilecek bir verinin yok olmasına neden olabilir. Ancak, imaj üzerinde yapılacak çalışmada hata yapılsa bile orijinal veriler yeni bir imajın üretilmesinde kullanılabilir. Bu nedenle elektronik delil üzerinde analiz işleminin yapılması adli inceleme kuralları açısından doğru değildir ve bu açıdan da orijinal diskin imajının (birebir kopya) alınması bir zorunluluktur[708].

İmaj alma işlemi, sistemdeki verilerin özel yazılımlar kullanılmak suretiyle ve alt seviye bit bazında başka bir ortamda bir örneğinin oluşturulması suretiyle yapılır. Alt seviye bit bazında kopyalama yapılmasının önemi, daha sonraki incelemelerde silinmiş, değiştirilmiş, deforme edilmiş verilere de ulaşma olanağını vermesidir[709]. İmaj alma işlemi sonucunda elde edilen birebir kopya, adli kopya (forensic duplicate) olarak da adlandırılmaktadır[710].

Birebir kopyalama işlemi, günlük kullanımda uygulanan normal kopyalamadan farklıdır. Normal kopyalama işlemi, kullanıcı tarafından oluşturulan dosyaların bir kaynaktan başka bir kaynağa aktarılması işlemini ifade etmekte olup sistem dosyaları ve gizli dosyaların kopyalanmasını içermemektedir. Normal kopyalama işleminde dosyaların veri ya da sistem dosyası olduğu ve tarih/zaman bilgileri gibi detaylar

[707] Henkoğlu, s. 47.

[708] Aktepe, s. 69; Say, Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi, s. 86.

[709] Günal, s. 51.

[710] Aydoğan, s. 35.

yanıltıcı olabilmektedir[711]. Ayrıca, normal kopyalama sırasında dosya alanındaki bilgilerin silinmesi veya bozulması da mümkündür[712].

Diğer taraftan işletim sistemlerinde günlük yaşamda yapılan normal kopyalama işleminde kullanıcılar tarafından görülen dosya veya klasörler başka bir bilişim sistemine aktarılması sırasında bazı yeni dosya yapılarında (NTFS) daha detaylı bilgiler tutulabilmekte iken burada bulunan dosya veya klasör eski dosya yapısıyla (FAT) formatlanmış bir veri depolama birimine kopyalandığında bazı üst verilerin kopyalanamadığı görülmektedir. Bu bakımdan adli bilişim uygulamalarında normal kopyalama tercih edilmemekte, birebir kopya elektronik delil üzerindeki verilerin tümünü kapsadığından incelemeler de birebir kopyalar üzerinden yapılmaktadır[713].

Yukarıda da belirtildiği üzere geçerli bir imajın alınabilmesi için sistemdeki tüm verilerin alt seviye bit bazında başka bir ortamda bir örneğinin oluşturulması gerekmektedir. Ancak değişik türden kopyalama yazılımları kullanılarak yapılan kopyalarda sadece sistem üzerinde var olan dosyaların kopyalama işlemine tabi tutulmaları geçerli bir imaj almaya imkân sağlamamaktadır. Zira alt seviye bit bazında kopyalamada sistem üzerinde veri depolama biriminin sektör* bazında yansıması alındığından veri depolama birimi üzerindeki boş veri alanları, silinmiş veri alanları ve disk yapısı olduğu gibi klonlanmaktadır[714].

Partition Imager ve Norton Ghost gibi sistemin yedeğini almaya yarayan imaj alma çözümleri, sistem üzerindeki veri depolama ünitelerini sadece açılış kaydı, bölümleme tablosu, dosya sistemi tablosu ve mevcut dosyalar bazında klonladıklarından dolayı sistem üzerinde bulunan ve fakat dosyaların olmadığı alanları kopyalamamaktadır. Bu

---

[711] Henkoğlu, s. 48.

[712] Güven Şeker, "Bilişim Suçlarının Delillendirilmesinde Amerikan Uygulaması ve Ülkemizdeki Durum", **Uluslararası İnsan Bilimleri Dergisi**, Cilt. 1, Sayı. 1, (2004), s. 7; Osman Nihat Şen, Polisin Adli Bilişimde Kullanabileceği Programların Bir Değerlendirmesi, s. 36.

[713] Murat Özbek, "Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları", **1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu**, Elazığ, 20-21 Mayıs 2013, s. 2.

* Sektör; izlerin dilimlenmesi ile oluşan ve işletim sisteminin veri yazma işlemi yapabildiği en küçük alanı ifade eder. Bkz. Henkoğlu, s. 69.

[714] Ekizer, http://www.ekizer.net/adli-bilisim-computer-forensics (06 Nisan 2014).

durum ise silinmiş verilerin yer alması muhtemel boş disk alanların kaybolmasına yani inceleme aşamasında delil kaybına neden olmaktadır[715].

Bununla birlikte disk imajının adli bilişim standartlarına uygun olarak alınması, elektronik delilin elde edilmesi ve analizi sürecinin doğru bir şekilde başlayıp sonuçlandırılması açısından önemlidir. Bu sürecin doğru işlemesi, mahkemede elektronik delilin niteliklerine gölge düşmeyecek şekilde sunulması ve doğru kararların verilmesinde etkili olacaktır[716].

Birebir kopyalama işlemi aktif ve pasif olmak üzere iki şekilde yapılmaktadır. Aktif kopyalama, canlı sistemlerin kopyalarının alınmasında kullanılır. Bu kopyalamada, canlı sistem, uygulanan kopyalama işleminden etkilenmez. Ancak, işlem sırasında değişen dosyalar kopyalanamaz. Pasif kopyalamada ise bilişim sisteminin gücü kesilir ve sabit disk üzerinde yazmaya karşı korumalı yazılım ve donanımlar aracılığıyla disk üzerine erişim engellenir. Bu işlemden sonra disk tümüyle kopyalanır[717].

Adli bilişim sürecinin en önemli işlemlerinden birisi olan imaj alma işlemini standartlara uygun şekilde gerçekleştirmek üzere çeşitli özel yöntemlerin kullanılması gerekmektedir. Günümüzde kullanılan başlıca yöntemler ise, donanımsal araçlarla imaj alma ve bilgisayar yazılımları ile imaj alma yöntemleridir.

4.2.4.1. Donanımsal Araçlarla İmaj Alma

Donanımsal araçlarla imaj alma işleminde bit-by-bit imaj alma işlemi özel donanımsal araçlarla yapılır. Bu işlem türünde donanımsal imaj alma programları şüpheli diski "temiz" bir diske doğrudan kopyalamaktadırlar. Donanımsal imaj alma programları, yazılımsal imaj alma programlarına göre daha hızlı çalışırlar[718].

Donanımsal imaj alma araçları orijinal delile fiziksel veri bağlantısı kurularak kendi üzerindeki gömülü işletim sistemindeki imaj alma adımları takip edilmek suretiyle

[715] Ekizer, http://www.ekizer.net/adli-bilisim-computer-forensics (06 Nisan 2014).

[716] Henkoğlu, s. 59.

[717] Say, Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi, s. 71.

[718] Osman Nihat Şen, Polisin Adli Bilişimde Kullanabileceği Programların Bir Değerlendirmesi, s. 37.

delilin imajını almaktadırlar. Bu yöntemin avantajı herhangi bir bilgisayara ihtiyaç duymaması ve olay yerinde imaj almaya elverişli olmasıdır. Bu araçlarda basit bir işletim sistemi bulunur ve kullanıcıya imaj alma esnasında yapması gereken adımları seçmesi sağlanır. "Write block*" özellikleri sayesinde imaj alma işlemi sırasında delilin orijinalliğini bozmamak için sadece delilden bit-by-bit kopyalama yaparak kendi depolama biriminde imaj dosyasını oluşturur. Orijinal delile yazma işlemi "write block" özellikleri sayesinde fiziksel olarak engellenmiştir[719].

Donanımsal tabanlı olarak imaj alma işlemi yapan araçlar, olay yerinde imaj alma işlemlerinden dolayı tercih edilmekte ve tüm sabit disk çeşitleri ile (USB, IDE, SATA, SCSI) bağlantı yapılarak kullanılmaktadır. Donanım tabanlı imaj alma işlemleri araçlarının tümü, imajı alınan diske fiziksel olarak erişim yaptığı için, sabit disk üzerindeki dosya sistemlerine bağlı kalmaksızın imaj alabilmekte ve hash değeri hesaplaması yapabilmektedir. Çoğu bağımsız olarak çalışmaktadır ve sistemin bir tarafına imajı alınan disk, diğer tarafına imajın kopyalanacağı disk bağlanarak yapılan işlem bir LCD panelden takip edilir. Genel olarak donanım tabanlı imaj alma araçlarının tek amacı disk imajı almaktır. Ayrıca, çok pahalı olmakla birlikte, üzerinde tümleşik olarak bulunan bilgisayar sayesinde analiz işleminde kullanılan donanım tabanlı imaj alma araçları da bulunmaktadır[720].

Donanım tabanlı imaj alma araçlarının en büyük avantajı daha hızlı ve daha verimli çalışmasıdır. Fakat veri transfer hızı ve ara yüz uyumluluğu gibi özellikler üreticilerin belirlediği marka ve modellere bağlı olarak farklılık göstermektedir. Birçoğunda disk hataları atlayarak işlemi mutlaka sonlandırma özelliği bulunmaktadır[721]. Bu tip imaj almada delil diskinin bağlı olduğu girişin yazma korumalı olması sebebiyle delil

* Block; birçok bölgede aynı objeden bulunduğunda, çalışmayı kolaylaştıran komutu, write block ise; blockları bir ad vererek diske kaydetmeyi ifade etmektedir. Bkz. Deniz Ağaoğlu, "Bilgi Mimarlık Yaz Stajı", 2014, http://bilgimimdeniz agaoglu.blogspot.com.tr/2014/11/teknoloji-staji-2014.html (24 Ocak 2015).

[719] Aydoğan, s. 35-36.

[720] Henkoğlu, s. 61.

[721] Henkoğlu, s. 61.

bütünlüğünün bozulması ihtimali de söz konusu değildir[722]. Donanımsal araçlarla imaj alma yöntemi cep telefonları için de uygulanabilmekte olup bu işlem, kendi içerisinde gömülü yazılım bulunduran GSM forensic cihazları ile yapılabilmektedir[723].

4.2.4.2. Bilgisayar Yazılımları ile İmaj Alma

Bilgisayar ortamında imaj alma yazılımları ile imaj alma işleminde ise orijinal delil bilgisayara fiziksel veri bağlantısı kurularak bağlandıktan sonra imaj alma yazılımındaki adımlar takip edilmek suretiyle delilin imajı alınmaktadır. Bu ürünler harici "write block" cihazlarına ihtiyaç duymazlar. Orijinal delilin bütünlüğünü korumak için "write block" özelliği yazılımlarda yer almaktadır ve kopyalama sırasında delilin değişmediği imaj alma işlemi sonucunda MD5 (Message-Digest 5) ve SHA (Secure Hashing Algorithm) algoritmaları kullanılarak üretilen hash değerlerinden tespit edilebilmektedir[724].

Bilgisayar yazılımları ile imaj alma yöntemi cep telefonları için de uygulanabilmektedir. Bu işlemin yapılabilmesi için öncelikle imajı alınacak telefonun marka ve modeline göre hangi tür bir bağlantı (kablo, bluetooth ve infrared bağlantısı) ile bilgisayara bağlanabileceği tespit edilmekte, sonrasında da hedef telefon bilgisayara uygun bağlantı türü ile bağlanıp bilgisayar yazılımı kullanılmak suretiyle imaj alma işlemi gerçekleştirilmektedir[725].

4.2.5. Hash (Veri Bütünlük) Değeri

Teknolojinin kaydettiği hızlı gelişme ve internetin küresel nitelikte kullanımı, çeşitli teknolojilere açık bir yaklaşım biçimini ve elektronik yoldan aktarılan verilerin tasdikini sağlayacak hizmetlerin sunulmasını gerekli kılmıştır. Bu gereğin bir anlam ifade edebilmesi ise buna bağlanacak hüküm ve sonuçların ispat edilebilirliğinin de

---

[722] Nigel Jones ve Diğerleri (hzl.), **Bilişim Suçları Eğitim Modülü (Türk Ceza Adalet Sisteminin Etkinliğinin Geliştirilmesi Avrupa Birliği & Avrupa Konseyi Ortak Projesi),** Ankara: MATBAM Ajans & Reklam & Tanıtım, 2014, s. 146.

[723] Aydoğan, s. 66.

[724] Aydoğan, s. 36.

[725] Aydoğan, s. 66.

sağlanmasını zorunlu kılmaktadır. Aksi takdirde bilişim teknolojisinden tam anlamıyla yararlanmak mümkün olmayacaktır[726].

Bu bağlamda elektronik delille ilgili üzerinde durulması gereken en önemli hususlardan birisi de elektronik delilin bütünlüğüdür. Zira elektronik delillerin bütünlüğü, elde edilen, üzerinde çalışılan ve çalışma sonrasında hakkında kanaat bildirilen elektronik verinin herhangi bir şekilde değişikliğe uğrayıp uğramadığı hususuyla ilgilidir. Olay yerinden elde edilen bir verinin orijinal hali ile üzerinde çalışılan verinin birebir aynı olması gerekmektedir[727].

Bu bakımdan adli bilişim uygulamasında elektronik delilin bütünlüğünün sağlanması yani ilk olay verisinin orijinal hali ile kullanıldığına ilişkin teknik ispatın yapılabilmesi, elektronik delilin korunması ve kontrolünün yapılması için -aşağıda incelenecek olan zaman damgasının (time stamping) yanı sıra- birebir kopyalama işlemi sırasında hash değerinin tespit edilmesi gerekmektedir[728].

Bir veri veya veri depolama biriminin ilk sektörden başlayarak son sektöre kadar tümünün belirli bir algoritmik fonksiyondan geçmesi sonucunda bir hash değeri oluşmaktadır. Son sektörün de aynı işleme tabi tutulması sonucunda ortaya çıkan değere ise o veriye ait hash değeri denilmektedir. Bu değer benzersiz (unique) nitelikte olduğu için veri depolama birimi üzerideki bir karakterin değişmesi hash değerinin de değişmesine neden olur. Bu bakımdan elektronik delil veya elektronik delilden alınan imaj üzerinde herhangi bir değişiklik yapılıp yapılmadığını kontrol etmek amacıyla hash değeri hesaplatılır ve böylece üzerinde çalışılan verilerin orijinali ile aynı olup olmadığının doğruluğu kontrol edilmiş olur[729].

---

[726] Seyithan Deliduman, "Elektronik Verilerin Delil Değeri", **Bilişim Hukuku**, Mete Tevetoğlu (drl.), İstanbul: Kadir Has Üniversitesi Yayınları, 2006, s. 47.

[727] Henkoğlu, s. 80.

[728] Mustafa İlker Öztürk, s. 78; *"Sanığın kullandığı bilgisayar üzerinde usulünce imaj alma işlemi yapılarak sonucunda çıkan veri bütünlük (hash) değerlerinin tespit edilmemiş bulunması..,"* Yargıtay 8. CD. 24.10.2013, E. 2012/21817, K. 2013/25428 (UYAP).

[729] Akarslan, s. 124; Murat Özbek, s. 2.

Hash algoritmaları imaj alma işlemi sırasında uygulanabileceği gibi imaj alma işlemi sonrasında da her dosya için ayrı ayrı uygulanabilir. Çeşitli hash algoritmaları bulunmakla birlikte, bu algoritmaların hangisi uygulanırsa uygulansın belli boyuttaki bir veri için bulunan hash değeri hep aynı olacaktır[730]. Günümüzde en sık kullanılan hash algoritmaları MD5 ve SHA'dır. Bu algoritmalar sonucu ortaya çıkan değerler imaj ile birlikte aynı dosya içerisinde saklanabilir veya ayrı bir dosya içerisinde toplanabilir[731].

Hash hesaplaması sonucu çıkan hash değeri ile ilk hesaplanan hash değerinin birbirleri ile aynı olmaları durumunda elektronik delilin veya elektronik delilden alınan kopyanın herhangi bir değişikliğe uğramadığı sonucuna varılır. Bu bağlamda, hash değeri, elektronik verinin bir nevi mührü konumundadır[732].

Parmak izinde olduğu gibi ait olduğu diske özel ve tek olan hash fonksiyonu, değişken uzunluğa sahip bir mesajı girdi olarak almakta ve sabit uzunluklu bir mesajı çıktı olarak üretmektedir. Bu çıktı mesajı, belirli bir girdi için tek bir sonuç üretir ve başka bir girdinin aynı sonucu üretmesi mümkün değildir. Girdi bir dosya, mesaj veya komple bir sabit disk olabilir. Girdideki bir mesajın bir biti bile değiştirilmiş olsa hash fonksiyonu sonucu üretilen yeni değer eski değerden farklı olacaktır[733].

Adli bilişim uzmanının bilirkişi raporunda vermiş olduğu hash değeri ile inceleme yapılan şüpheli sabit diskin imajının alındığı sırada oluşturulan ve imajı alınan diskin kullanıcısına verilen kopya üzerindeki hash değerinin aynı olmaması durumunda yapılan analiz sonucunda elde edilen bulgulara itiraz edilebilecek ve söz konusu bulguların geçerli bir delil olarak kabul edilmesi mümkün olmayacaktır. Uygulamada karşılaşılan en büyük ihmallerden biri, hash değerinin takibinin ve kontrolünün yapılmamasıdır. Bazen delillerin elde edilmesi ve imaj alma işlemleri sırasında kolluk birimleri tarafından elde edilen ve rapora işlenen hash değerinin, bilirkişi raporunda yer alan hash değerinden farklı olduğu durumlarla karşılaşılmaktadır. Bu durum, bilirkişinin

[730] Turgay Sarıakçalı, **İnternet Üzerinden Akdedilen Sözleşmeler,** Ankara: Seçkin Yayıncılık, 2008, s. 69.

[731] Say, Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi, s. 78.

[732] Murat Özbek, s. 2.

[733] Günal, s. 52.

incelemiş olduğu imajın gerçeğinden farklı olduğu ve imaj üzerinden elde edilen bulguların adli bilişim açısından delil değeri taşımadığı tartışmalarına yol açacaktır[734].

Bununla birlikte açık olan sistemlerden, RAM'lardan ve cep telefonlarından alınan imajlarla ilgili olarak tekrar imaj alınması ve hash değerlerinin kıyaslanması yoluna gidilmemektedir. Zira açık olan sistemler, RAM'lar ve cep telefonları üzerinde kayıtlı olan verilerin adli kopyaları alınırken sistem çalışmaya devam ettiği için, halen sistem içi zararsız küçük değişiklikler yapılmakta olduğu bilindiğinden ve tekrar adli kopya alındığında aynı hash değeri elde edilemeyeceği düşünüldüğünden böyle bir kıyaslama cihetine gidilmemektedir. Bu sistemlerden alınan ve elde edilen ilk adli kopyalar üzerinden tüm inceleme ve değerlendirmeler yapılmakta, orijinal elektronik deliller üzerinde tekrar hash hesaplaması işlemi yapılmaksızın adli kopya, delil olarak kullanılmaktadır[735].

Hash değeri üzerindeki hassasiyet nedeniyle bilirkişilerin kendilerine verilen disk imajlarını öncelikle üzerinde çalışacakları başka bir diske kopyalamaları ve kendilerine verilen imaj üzerinde çalışma yapmamaları gerekmektedir. Zira herhangi bir nedenle imaj üzerinde meydana gelebilecek değişiklik hash değerinin değişmesine ve o zamana kadar yapılan tüm inceleme işlemlerinin geçersiz kabul edilmesine neden olabilecektir[736].

Bununla birlikte, elektronik delillerin depolandığı cihazların sınırlı bir kullanım ömrü ve karmaşık veri depolama yapıları bulunmaktadır. CD-DVD gibi optik veri depolama aygıtları, sabit diskler gibi manyetik veri depolama aygıtları ve SSD diskler gibi flash yongalar üzerinde veri depolama teknolojisine sahip cihazlar bulunmaktadır. Bu cihazların her birinin kendilerine mahsus teknolojik özellikleri ve maruz kaldıkları etkenlere göre değişen bir kullanım ömürleri bulunmaktadır. Bu durum ise hash problemlerinin gündeme gelmesine neden olmaktadır[737].

---

[734] Henkoğlu, s. 54-55.

[735] Murat Özbek, s. 6.

[736] Henkoğlu, s. 55.

[737] Murat Özbek, s. 2.

Gerçekten de elektronik verinin orijinal olup olmadığı hususunda hash değeri çok önemli olmakla birlikte bu hususun tespitinde tek ölçüt değildir. Hash değeri, bir sürecin sonrasında veride değişiklik olup olmadığının tespitinde kullanılmaktadır. Veriye yapılan işlemler sırasında alınan hash değerinin değişmemiş olması verinin mutlak surette ele geçirildikten sonraki orijinalliğini koruduğunu gösterir, ancak verinin hash değerinin değişmiş olması verinin orijinal olmadığına kesin bir kanıt teşkil etmez. Zira hash değeri, sadece verinin değiştirilmesinden değil, veri depolama aygıtında meydana gelen mekanik bozulmalardan veya bozuk sektörlerden de kaynaklanabilir. Bu bakımdan, verinin güvenli bir delil olup olmadığının tespitinde bu hususların da dikkate alınması gerekmektedir[738].

Diğer taraftan hash değeri, bilişim sistemlerinde bulunan elektronik verinin arama sonucunda elde edildiği hali ile onun üzerinde çalışılan ve mahkemeye sunulan hali veya adli imajı arasındaki güvenilirliği sağlamakta kullanılabilir. Buna karşın, bilişim sisteminde bulunan elektronik veriye ilk temas edildiği arama sırasındaki hash değerinin alınmasından önce bu elektronik verilerde değişiklik yapıldığına ilişkin iddiaların doğruluğunu veya yanlışlığını hash değeri aracılığı ile tespit etmek mümkün değildir. Bu bakımdan hash değerlerinde herhangi bir problemin yaşanmamış olması tek başına elde edilen elektronik delilin güvenilir olduğu sonucunu ortaya koymaz. Bu nedenle elektronik delilin bütünlüğünün tespitinde diğer değişkenlerin de denetlenmesi gerekmektedir.

Son olarak belirtmek gerekir ki; hash değeri uygulaması, genellikle birebir kopyalama sırasında kopyalanan veri ile asıl verinin birbiri ile aynı olduğunu doğrulamak için kullanılmaktadır. Bununla birlikte, hash değeri uygulaması, kopyalanan verinin değiştirilmemiş olduğunu göstermek amacıyla da kullanılabilir[739].

[738] Kızılyar, s. 86.

[739] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 253.

4.2.6. Zaman Damgası (Time Stamping)

Yukarıda da değinildiği üzere elektronik delilin bütünlüğünün korunması için birebir kopyalama işlemi sırasında elektronik verilerin hash değerinin alınmasının yanı sıra bu durumun zaman damgası kullanılarak muhafaza altına alınması büyük önemi haizdir.

Mahkeme sürecinde elektronik delile ne zaman erişildiği, görevli personelin ne kadar süreyle delille temas halinde bulunduğu, elektronik delilin bütünlüğünün ne kadar süreyle sağlanabileceği hususlarına ilişkin soruların cevaplanabilmesi gerekmektedir. Zira elektronik delilin bütünlüğünün ispatlanması ve ayrıca elektronik delile ulaşılma zamanının tam olarak bilinmesi son derece önemlidir. Bu husus ise zaman damgası ile sağlanabilmektedir[740].

Zaman damgasına ilişkin birçok tanım bulunmaktadır. Gerçek hayatta zaman damgası herhangi bir anı temsil edebilmekteyken dijital dünyada zaman damgası dijital formatta belirli (spesifik) bir anı ifade etmektedir. Bu bağlamda zaman damgası adli bilişim açısından çok önemli bir rol oynamaktadır. Zira soruşturma sürecinde belirli anların tam zamanını bilme gerekliliği bulunmaktadır[741].

Zaman damgası, bir elektronik verinin üretildiği, değiştirildiği, gönderildiği, alındığı, kaydedildiği zamanın tespit edilmesini sağlayan elektronik bir veridir[742]. Zaman damgasının bu niteliği sayesinde elde edilen elektronik delilin üretim, erişim veya değiştirilme zamanları üzerinde oynama yapılması veya değiştirilmesi engellenmiş ve delillerin doğruluğu ispatlanmış olmaktadır[743].

Nitekim 30.11.2007 tarihli ve 26719 sayılı Resmi Gazete'de yayınlanan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında

[740] Jasmin Cosic and Miroslov Baca, "(Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp, http://czb.foi.hr/upload/datoteke/10_400.pdf (21 Ekim 2014).

[741] Cosic and Baca, http://czb.foi.hr/upload/datoteke/10_400.pdf (21 Ekim 2014).

[742] Zaman Damgası Nedir ?. (t.y) https://www.turktrust.com.tr/zaman-damgasi.html (24 Ekim 2014).

[743] Aydoğan, s. 37.

Yönetmelik'in yer sağlayıcının* yükümlülüklerini düzenleyen 7/1-c maddesinde yer sağlayıcının trafik bilgisini altı ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle yükümlü oldukları hükme bağlamıştır.

Bununla birlikte, gerçek ve dijital dünya zamanı daima saat ayarına bağlı olduğundan zamanın kaynağının da güvenilir olması gerekir. Bu bakımdan zaman damgasının her hal ve şartta güvenilir bir sonuç doğuracağı söylenemez. Örneğin, başkasına ait ve saat ayarı yanlış olan bir bilgisayar kullanıldığında yanlış bir zaman damgası elde edilecek demektir. Böyle bir durumda zamanın tamamen güvenilir olduğundan bahsedilemez ve bu şartlar altında elde edilen zaman damgası, elektronik delile ilişkin bir soruşturmada olayların değerlendirilmesine dair hayati öneme sahip bir faktör olarak kullanılamaz[744].

Zaman damgasına ilişkin olarak zamansal hatanın en yaygın kaynağı sistem saatindeki kaymalardır. Eğer bir yönlendiricinin saati birkaç saat öndeyse, bu uyumsuzluk diğer sistemlerdeki kayıtlarla olayları ilişkilendirmekte sıkıntıya neden olabilir ve sonraki süreçte yapılacak analizlere zarar verebilir. Ayrıca, elektronik delilin toplandığı sistem saatindeki hatalar analiz ve raporlama aşamalarında oluşması muhtemel tutarsızlıklara sebebiyet verebilir. Örneğin, çoğu sistem günlüğü sunucuları* ağ üzerindeki uzak sistemlerden alınan günlük kayıtları için bir zaman damgası oluşturmaktadır. Bu nedenle, sistem günlüğü mesajını gönderen bilgisayar saati doğru olsa bile sunucudaki saat kayması hataya neden olabilecektir[745].

Ağ günlüklerindeki bir diğer yaygın zamansal hata kaynağı ise saat dilimi farklılıklarıdır. Migrosoft gibi bazı web sunucuları GMT (Greenwich Mean Time) zaman damgasına göre günlük kayıtlarını oluşturmaktadır. Bununla birlikte dünya

* Yer sağlayıcı; hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişileri ifade eder. (5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun m. 1-m).

[744] Cosic and Baca, http://czb.foi.hr/upload/datoteke/10_400.pdf (21 Ekim 2014).

* Sunucu (server); dijital bilgileri kapasiteleri oranında depo ederek diğer bilgisayarlara hizmet sağlayan bilgisayarlar ya da programları ifade etmektedir. Bkz. Tamer Soysal, "İnternet Servis Sağlayıcılarının Hukuki Sorumluluğu", **Türkiye Barolar Birliği Dergisi**, Sayı. 61, (Kasım-Aralık 2005), s. 309.

[745] Eoghan Casey, "Error, Uncertainty, and Loss in Digital Evidence", **International Journal of Digital Evidence**, 2002, Vol. 1, No. 2, dblp veritabanı, (24 Ekim 2014).

genelindeki bilgisayar sistemleri ise genellikle kendi günlük kayıtlarında yerel saat dilimini kullanırlar. Bu bakımdan zaman dilimi farklılıklarını düzeltmede yaşanacak bir başarısızlık karışıklığın daha da büyümesine sebebiyet verebilir. Örneğin bir internet servis sağlayıcısından bilgi istendiğinde, saat dilimi uyumsuzluğu internet servis sağlayıcısının yanlış abone bilgilerini vermesine ve dolayısıyla masum bir kimsenin töhmet altında kalmasına neden olabilir[746].

4.2.7. Koruma Zinciri (Chain of Custody)

Koruma zinciri, bir delilin fiziki veya elektronik olarak toplanması, muhafaza edilmesi, başka bir yere aktarılması ve analiz edilmesini gösteren kronolojik belgelendirme sürecini ifade etmektedir. Koruma zinciri sayesinde delillerin doğrulanması sağlanmaktadır [747] . Bu bakımdan elektronik verilerin ceza yargılamasında kullanılabilecek nitelikte "sağlam delil" olarak kabul edilebilmesi, bu verilerin ele geçirildiği ilk andan itibaren koruma zinciri (chain of custody) kıstaslarına uygun olarak temiz bir şekilde el değmeden korunarak incelemeyi yapacak uzmanın önüne götürülmesinin sağlanmasına bağlıdır[748].

Delillendirme sürecinin en önemli unsurlarından birisi delillerin koruma zinciri ile toplanması ve belgelendirilmesidir. Bu bakımdan soruşturma aşamasında elektronik delili elde eden her kişi, bu delilin ilk elde edildiği hali ile mahkemede ileri sürüldüğü halinin aynı olup olmadığı hususunda ifadeye çağrılabilir. Her ne kadar delillere temas eden (delilleri toplayan) her kişinin her durumda mahkemede hazır edilmesi gerekli olmasa bile, bu durumun asgari seviyede tutularak elektronik delilin ilk toplandığı andan mahkemeye sunulduğu ana kadar değiştirilmediği hususunun açıklığa kavuşturulması yerinde olacaktır[749].

Koruma zinciri adli bilişim süreci bakımından elektronik delilin geçerliliği hususunda çok önemli bir rol oynamaktadır. Zira adli bilişimin her aşamasında elektronik delilin

[746] Casey, Error, Uncertainty, and Loss in Digital Evidence, dblp veritabanı, (24 Ekim 2014).

[747] Gözüşirin, s. 93.

[748] Kunter, Yenisey ve Nuhoğlu, Açıklamalı Ceza Muhakemesi Kanunu, Cilt. I, s. 1320.

[749] Casey, Digital Evidence and Computer Crime, s. 21.

nerede, ne zaman, nasıl keşfedildiği, ne şekilde toplandığı ve incelemeye tabi tutulduğu, yine delile ne zaman ve kim tarafından ilk olarak temas ettiğinin bilinmesi gerekmektedir. Uygun bir koruma zinciri bu gibi tüm soruların cevaplarını belgeleriyle ortaya koyabilmelidir[750].

Bunu sağlamanın en kolay yolu delilin kayıt altına alınmasıdır. Bu kayıt belgesi muhafaza edilerek elektronik delinin elde edildiği andan beri değiştirilmediği ispatlanmış olacaktır. Bu belge, elektronik delinin ne zaman, nereden, nasıl ve kim tarafından alındığı sorularına cevap verecek şekilde düzenlenmelidir[751].

Eğer bu sorulardan yalnızca biri bile cevapsız kalırsa koruma zinciri bozulmuş sayılır. Elektronik delil mahkemeye sunulduğunda, eğer koruma zincirindeki herhangi bir halka eksikse, mahkeme delilin suçla ilişkisini kabul etmeyebilir ve bu nedenle de tüm bir soruşturma sonuçsuz kalabilir[752].

Sağlam bir koruma zincirinin olmaması elektronik delilin usulüne uygun biçimde elde edilmediği, değiştiği, bozulduğu, başka suçlara ait verilerle karıştığı veya sair nedenlerle kirletildiği iddialarına neden olabilir. Koruma zincirinin bozulmasının muhtemel sonuçları arasında delilin yanlış belirlenmesi, delilin kirlenmesi, delilin veya ilgili unsurlarının geçerliliğini kaybedilmesi tehlikesi de bulunmaktadır[753].

Koruma zinciri meselesi dijital veri ile ilişkili olduğu kadar bu dijital verinin içerisinde bulunduğu elektronik cihazla da ilişkili olduğu için koruma zinciri hem elektronik cihazı hem de bu cihazda bulunan dijital veriyi kapsamaktadır. Bu nedenle soruşturma kapsamında ele geçirilen elektronik cihazın da koruma zinciri güvencesiyle korunması gerekir.

Gerek genel gerekse özellikli olarak elektronik delille ilgili koruma zincirine ilişkin -eğer varsa- akreditasyon standartlarının, laboratuvar politikalarının, prosedürlerin ve

[750] Cosic and Baca, http://czb.foi.hr/upload/datoteke/10_400.pdf (21 Ekim 2014).

[751] Adli Bilişim Prensipleri Nelerdir ?, http://www.teknospaper.com/2014/04/adli-bilisim-prensipleri/ (25 Ekim 2014).

[752] Cosic and Baca, http://czb.foi.hr/upload/datoteke/10_400.pdf (21 Ekim 2014).

[753] Casey, Digital Evidence and Computer Crime, s. 22.

diğer kuralların bilinmesi ayrıca bunların takip edilip edilmediği veya bunlardan sapma olup olmadığının belirlenmesi gerekir. Söz konusu standart, politika ve prosedürlerde sapma olması, dava sürecini etkileyeceğinden bu tür sapmaların yaşanması durumunda mahkemeyi ikna edecek açıklamalar yapılmalıdır. Diğer taraftan politikalar, prosedürler ve diğer kurallar da dinamik tutulmalıdır[754].

4.2.8. Elektronik Delilin Paketlenmesi, Taşınması ve Muhafazası

Bilişim sistemlerinden elde edilen elektronik delillerle ilgili en önemli husus bu delillerin güvenilirliğinin korunması noktasında kendini göstermektedir. Nitekim inceleme ve analiz işlemlerinin yerine getirilmesine yönelik birçok teknolojik cihaz üretilmesine karşın adli bilişim sürecinde bilişim sistemlerinden çıkartılan elektronik delilin bütünlüğünün korunması konusu soruşturma makamları ve taraflarını en çok endişelendiren mesele haline gelmiştir[755].

Gerçekten de elektronik delil, hassas yapısından dolayı, yanlış paketleme, taşıma veya yanlış muhafaza edilmesi sonucunda kolaylıkla değişikliğe uğrayabilir, bozulabilir ya da yok olabilir niteliğe sahiptir. Bu nedenle, elektronik delili paketlemek, taşımak ve muhafaza etmek için özel önlemler alınması gerekir. Aksi halde, elektronik delil kullanılamaz veya sonuca götüremez duruma gelebilir.

Nitekim uygulamada CD, DVD vb. elektronik medyalara aşırı basınç uygulayarak yazı yazılması, zımba teli ile üzerlerinde delik açılması, sıcak mührün elektronik medyalar üzerine uygulanması, çeşitli yapışkanlar kullanılması sonucunda medyalar üzerinde kâğıt ve yapışkan madde bakiyelerinin kalması gibi yanlış uygulamalar nedeniyle elektronik medyalara zarar verildiği görülmektedir[756].

Bu bakımdan toplanan elektronik delillin paketlenmesi işlemine başlamadan önce delillerin doğru bir şekilde dokümanının yapılması ve etiketlenmesi gerekir. Gizli ve görülmeyen delillere özel olarak dikkat edilmeli ve bunların muhafazası için gerekli

---

[754] Nilsson (Ed.), s. 21.

[755] Chet Hosmer, "Providing the Integrity of Digital Evidence with Time", **International Journal of Digital Evidence,** Vol. 1, No. 1, (Spring 2002), s. 1.

[756] Levent Bayram, **Adli Bilimlerde Ses ve Konuşma İncelemeleri,** Ankara: Seçkin Yayıncılık, 2008, s. 155.

işlemler yapılmalıdır. Manyetik araçlar, kâğıt veya plastik torbalar gibi anti statik ambalajlara sarılmalı, normal plastik torbalar gibi statik elektrik üreten materyaller kullanılmamalıdır. Disket, CD-ROM veya bantlar gibi bilgisayar araçlarının katlanmaması, bükülmemesi ve çizilmemesi gerekmektedir. Delilleri taşımak amacıyla kullanılan konteynerlerin ise doğru bir şekilde etiketlenmiş olması gerekir[757].

Veri depolama ünitelerine ait alınan imajların MD5 ve SHA hash değerleri alınmalı ve bu değerler tutanak kayıtlarında belirtilmek suretiyle daha sonra meydana gelebilecek itirazların önüne geçilmelidir[758]. Yukarıda da belirtildiği üzere hash değeri, alınan imajların orijinalliğinin bozulmadığını belirler ve yedekleme işlemi sırasında alınan imaj dosyası ile imajı alınan sabit diskin birebir aynı olduğunu gösterir[759].

İmaj alma işlemi mümkünse olay mahallinde bağımsız fiziksel kopyalama cihazları ile gerçekleştirilmeli ve bu imajlar muhafaza edilerek orijinal medyalar adli emanete teslim edilmelidir. Olay yerinde imaj alma mümkün değil ise veri depolama üniteleri mühürlü torbalara konularak şüpheli avukatı huzurunda açılmalı, imaj alınmalı ve akabinde adli emanete teslim edilmelidir[760].

Elektronik delilin taşınması sırasında manyetik alanlardan uzak tutulması gerekir[761]. Radyo vericileri, ısıtmalı koltuklar bu delillere zarar verebilirler. Elektronik delilin araç içerisinde uzun süre bulundurulmaması gerekir. Zira aşırı sıcak, nem veya soğuk elektronik delile zarar verebilir. Diğer taraftan konteynerlere yerleştirilmeyen bilgisayar ve diğer bileşenlerin araç içerisinde şoklardan veya aşırı titreşimlerden etkilenmeyecek şekilde güvenli olarak taşınması gerekir[762].

---

[757] Keser Berber, Adli Bilişim, s. 72.

[758] Henkoğlu, s. 25.

[759] Aydoğan, s. 15.

[760] Çakır ve Sert, s. 159.

[761] Michael B. Mukasey, Jeffrey L. Sedgwich and David W. Hagy, **Electronic Crime Scene Investigation: A Guide for First Responders,** Second Edition, Washington: PhotoDisc, Inc, 2001, s. 21.

[762] Keser Berber, Adli Bilişim, s. 72.

Tüm elektronik delillerde olduğu gibi cep telefonlarında bulunan veriler de adli bilişim sürecinde değişikliğe veya bozulmaya karşı korunmalıdır. Cep telefonlarının diğer cep telefonlarıyla veya hücresel ağlarla bağlantı kurmasına izin verilmesi bu cihazlarda bulunan elektronik verilerin zarar görmesine neden olabilir. Bu yüzden, cep telefonları tüm ağlardan izole edilmelidir. Bunun için ise radyo sinyallerini veya diğer telefonlarla bağlantıyı engelleme özelliği olan faraday poşetleri (faraday bags) kullanılmalıdır[763].

Nitekim cep telefonlarının faraday poşetlerinde taşınması, taşınma sırasında telefona gelebilecek aramalar ve kısa mesajların engellenmesini ve ayrıca telefonun hizmet aldığı son konum bilgisinin değişmemesini sağlamaktadır. Aksi halde telefona gelebilecek arama ve kısa mesajlar sonucunda kişilerin son arama listesi ve mesaj kutusu değişebilir ve hatta silinen mesajlar üzerine veri yazıldığı için tekrar elde edilmeleri engellenebilir. Ayrıca, şüphelinin en son hizmet aldığı konum bilgisi de taşıma esnasında değişerek delillerin orijinalliği bozulabilir[764].

Elektronik delilin muhafazası ile ilgili olarak; üzerinde elektronik delilin yer aldığı bazı elektronik aygıtların (PDA gibi) bataryasının tamamen boşalması halinde bu aygıtlar, bünyelerindeki tüm program ve tarih/zaman bilgilerini unutarak fabrika ayarlarına dönmektedirler. Bu tür batarya ile çalışan aygıtlara ve cep telefonlarına elkonulması halinde, bataryasının tamamen boşalmadan şarj edilmesi, olası delil kaybını önlemek bakımından önemlidir. Diğer taraftan adli emanete ya da incelenmek üzere laboratuvara götürülen her bilişim sisteminin, toz, nem, rutubet, aşırı ısı ve manyetik alanlar gibi zararlı olabilecek etkilerden uzak tutulması sağlanmalıdır[765].

Son olarak belirtmek gerekir ki; elektronik medyanın muhafazasında yeterince özen gösterilmemesi halinde bu elektronik medya bozulabilmekte, kaybolabilmekte veya özelliğini kaybedebilmektedir. Bu bakımdan adli emanete teslim edilecek olan orijinal medya, mühürlü torbada muhafaza edilmelidir[766].

---

[763] Daniel and Daniel, s. 265; Mukasey, Sedgwich and Hagy, s. 21.

[764] Aydoğan, s. 14.

[765] Henkoğlu, s. 26.

[766] Çakır ve Sert, s. 160.

4.3. Elektronik Delilin İncelenmesi

4.3.1. Genel Olarak

Bilişim sistemlerinden toplanan tüm veriler, hemen analiz işlemine tabi tutulmazlar. Bazı verilerin adli bilişim uzmanı tarafından analize tabi tutulabilmesi, bir takım ön işlemlerin yapılmasını gerekli kılabilir[767]. Bu bakımdan toplama aşamasının sona ermesinden sonra öncelikle inceleme aşamasına geçilir. İnceleme aşamasından kastedilen elektronik medya üzerindeki verilerin incelenmesidir. İnceleme aşamasına başlamadan önce elde edilen medyanın imajının alınmış olması delil bütünlüğünün korunması açısından son derece önemlidir. Zira inceleme işleminin imaj üzerinde yapılması, meydana gelmesi olası herhangi bir hata sonucu delil bütünlüğünün kaybolmasını engelleyecektir[768].

İnceleme aşamasında yapılması gerekenler planlanmaktadır. Bu planlamanın başarısı bahse konu olayın iyi anlaşılması ve nelerin arandığının net bir şekilde bilinmesine bağlıdır. Neleri arayacağını bilen uzman kişilerin bundan sonra arayacağı verileri nerede araması gerektiğini tespit etmesi gerekir. Buna göre, bir elektronik posta görüşmesi aranıyorsa bunun bilgisayar diskinin neresinde saklandığının da bilinmesi gerekir[769].

Uygulamada adli mercilerin inceleme işlemini yapacak birimden geniş bir yelpazede taleplerinin olduğu görülmektedir. Bu talep bir organize suç örgütünün tüm bilişim sistemleri üzerinde olabileceği gibi bir cinayet suçunda dahi inceleme ve delillendirme talep edilebilmektedir. Genellikle kredi kartı dolandırıcılığı, msn hırsızlığı, hacking, çocuk pornografisi gibi suçlar için inceleme istenirken; cinayet, dolandırıcılık gibi suçlarla ilgili de inceleme talebinde bulunulabilmektedir. Diğer taraftan hakaret, tehdit, özel hayatın gizliliğinin ihlali, yaralama gibi birçok suçla ilgili elektronik veri üzerinde

[767] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 255.

[768] Günal, 48; John Ashcroft, Deborah J. Daniels and Sarah V. Hart, Forensic Examination of Digital Evidence: A Guide for Law Enforcement, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf (12 Ocak 2015), s. 1.

[769] Akarslan, s. 124.

delil elde etme imkânı olup herhangi bir suç hakkında elektronik veri incelemesi talep edilebilmektedir[770].

İnceleme aşaması delilin gözle görülür hale getirildiği ve orijininin belirlendiği aşamadır. Bu aşamada öncelikle tüm veriler toplanarak işe yarayanlarla yaramayanların birbirlerinden ayrılmaları sağlanır. Bu sayede işe yarayacak delilin ve bu delilin içeriğinin ne olduğu belirlenebilecektir[771].

Bu aşamada pek çok şeyin tamamlanması sağlanır. Öncelikle elektronik delilin kendi bütünlüğü içerisinde içeriğinin ve durumunun belgelenmesi sağlanır. Bu dokümantasyon, tarafların, delilin içerisinde ne olduğunu keşfetmelerine imkân sağlar. Bu süreçte ayrıca gizli veya mahrem bilgiler araştırılmaktadır. Bir kez tüm bilgilerin görülebilirliği sağlandıktan sonra önemli verilerin önemsizlerinden ayıklaması işlemine geçilebilecektir[772].

Diğer taraftan inceleme aşamasında delil bütünlüğünün korunması ve laboratuvar çalışmalarında delil olabilecek verilerin başka verilerle karıştırılmaması ve delillerin değişikliğe uğramaması amaçlanmaktadır[773]. Zira böyle bir durum tüm soruşturma faaliyetine zarar verebilir.

Elektronik delilin incelenmesi aşamasında, deliller üzerinde tam bir analiz işlemine geçmeden önce silinmiş, gizlenmiş, şekli değiştirilmiş veya mevcut işletim sistemi ya da dosya sistemi ile görüntülenemeyen verilerin ortaya çıkartılması gerekmektedir. Bu sayede normal şartlarda görünmeyen bir olgunun fark edilebilmesi sağlanarak yeni elektronik delile ulaşılabilir[774].

İnceleme aşamasında, elektronik delile uygulanan prosedürün kayıt altına alınması gerekir. Eğer uygulanan prosedür kayıt altına alınmazsa delillerin mahkemede maddi

[770] Çakır ve Sert, s. 163.

[771] Özdilek, Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku, s. 202.

[772] Keser Berber, Adli Bilişim, s. 45.

[773] Ünal, s. 23-24.

[774] Gözüşirin, s. 96.

geçerliliğini kaybetmesi ihtimali ortaya çıkabilir. Diğer taraftan tutulan bu kayıtlar, elektronik delilin laboratuvara nasıl ulaştırılması gerektiği konusunda da bilgi verir[775].

Bilgisayarlarda yapılabilecek delil inceleme aşamasında; bilgisayardaki dosyaların erişim, oluşturulma ve son yazma sürelerinin tespiti, internette girilmiş olunan web sitelerinin ve bu sitelere ne zaman girildiğinin tespiti, bilgisayara internet üzerinden indirilen dosyaların tespiti, şifre korumalı dosyaların içeriğinin görüntülenmesi, gizlenen veya uzantısı (dosya tipi) değiştirilen dosyaların görüntülenmesi, silinen verilerin geri getirilmesi, bilgisayardan yazıcıya gönderilen dosyaların görüntülenmesi, bilgisayardaki dosyalar içinde kelime araması yapma, dosya filtreleme gibi işlemler yapılabilir[776].

Cep telefonlarında yapılabilecek delil inceleme aşamasında ise; cep telefonuna kayıtlı adres defterinin tespit edilmesi, SIM karta kayıtlı adres defterinin tespit edilmesi, son arama (arayan ve aranan) listesinin tespit edilmesi, mesaj kutusu (SMS box) içeriğinin görüntülenmesi, silinen mesajların (SMS) elde edilmesi (recovery), cep telefonun son hizmet aldığı lokasyon (Cell ID) bilgisinin tespiti, cep telefonundaki doküman, resim, video vb. dosyaların tespiti gibi işlemler yapılabilir[777]. Aşağıda inceleme aşamasında ön plana çıkan bazı işlemlere değinilecektir.

4.3.2. Anahtar Kelime Arama İşlemi

Adli bilişim uzmanlarının elektronik medyaları inceledikleri sırada kullandıkları program türlerinden birisi de anahtar kelime arama programlarıdır. Anahtar kelime arama programları tek tek veya liste halinde verilen kelimeleri elektronik medyanın bütününde aramakta ve sonuçları liste halinde vermektedir. Anahtar kelime arama programlarının kullanılmasındaki amaç elektronik medyanın şüpheli tarafından suçla ilgili bir konuda kullanıp kullanmadığını belirlemek ve kullanılması durumunda medyanın hangi bölümünde hangi tür verilerin bulunacağını öğrenmektir[778].

[775] Say, Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi, s. 100.

[776] Aydoğan, s. 16; Özbey, s. 74.

[777] Aydoğan, s. 16.

[778] Osman Nihat Şen, Polisin Adli Bilişimde Kullanabileceği Programların Bir Değerlendirmesi, s. 39.

Özellikle elektronik verilerin toplanması aşamasında, toplanan verilerin boyutunun büyük olması, manüel arama yöntemi ile elektronik delile ulaşmayı olanaksız hale getirdiğinden, inceleme sürecinde anahtar kelime arama yönteminin uygulanmasında zorunluluk bulunmaktadır[779]. Anahtar kelime arama işleminin hukuksal bakımdan bir başka faydası ise şüphelinin bütün dokümanlarını incelemeden sadece isnat edilen suça ait konudaki dokümanları inceleme imkânı sunması ve böylece kişisel mahremiyetin ihlal edilmesinin önlenmesidir[780].

Anahtar kelime arama işlemi, adli kopya üzerinde metin arama şeklinde olabileceği gibi hexadecimal[*] değer ile de yapılabilmektedir. Örneğin, "ahmet" kelimesinin el konulan bilgisayara ait adli kopya ile ilgisinin tespit edilebilmesi için yapılacak arama işlemi, ahmet kelimesinin metin olarak aranması veya 616C6978 hexadecimal karşılığının aranması şeklinde olabilir. Bu işlem sonucunda internet geçmişi, konuşma günlükleri, doküman içeriği de dâhil bilgisayara ait adli kopyanın tamamı taranır ve çıkan sonuçlar listelenir[781].

Bazı anahtar kelime arama programlarında konulara özel kelimeler bulunmaktadır. Bu özel kelimeler kullanılarak belirli konulara ait anahtar kelimeler bulunabilmektedir[782]. Bu programlarda bulunan özel kelime arama özelliği, önemli tarih, adres, elektronik posta adresi, telefon numarası, IP numarası, banka hesap numarası, kredi kartı numarası, vatandaşlık numarası, şifre veya örgütsel jargon gibi bilgilerin aranması işlemini oldukça kolay hale getirmektedir. Adli bilişim uzmanları, en çok kullanılan aranan kelimelerin "anahtar kelime değerini" belirleyerek, yeni olaylarla ilgili inceleme işlemi

[779] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 256.

[780] Osman Nihat Şen, Polisin Adli Bilişimde Kullanabileceği Programların Bir Değerlendirmesi, s. 39.

[*] Hexadecimal; "onaltılık" düzenin alabileceği değerleri (0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F) ifade eder. 0'dan F'ye kadar olan karakterlerin toplam adedi 16 olduğundan buna onaltılık düzer denilmektedir. Örneğin, bilgisayar "ahmet" ismini onaltılık düzende "61686d6574" şeklinde algılar. Bkz. http://ahmeti.net/bit-byte-binary-decimal-ve-hexadecimal-nedir/ (21 Nisan 2015).

[781] Çakır ve Kılıç, s. 32.

[782] Osman Nihat Şen, Polisin Adli Bilişimde Kullanabileceği Programların Bir Değerlendirmesi, s. 39.

yapılacağında da bu özel kelimeleri kullanarak arama işleminde zaman kazanabilmektedirler[783].

4.3.3. Disk Yazma Koruma İşlemi

Disk yazma koruma işlemi, asıl olarak delilleri barındıran diskin tek yönlü veri akışına imkân verecek şekilde uyarlanarak diskin içerisindeki verilerin bütünlüğünün muhafaza altına alınması işlemini ifade etmektedir. Disk yazma koruma işlemi iki şekilde sağlanmaktadır. Bunlardan donanımsal yazma koruma işleminde, inceleme konusu disk veya medya ile bilgisayar arasında köprü vazifesi gören cihazlar verilerin okunmasını sağlarken diske veri yazılmasını engellemek üzere tasarlanmıştır. Diğer koruma işlemi olan yazılımsal yazma koruma işleminde ise; çeşitli yazılımlar yoluyla incelemede kullanılacak bilgisayarın incelenecek diske veri yazma komutlarını bloke etmek suretiyle koruma işlemi sağlanmaktadır[784].

4.3.4. Silinen Verilerin Kurtarılması

Koruma altına alınmış bir elektronik delil üzerinde tam bir analiz işlemi yapmaya başlamadan önce silinmiş, gizlenmiş veya mevcut işletim sistemi ya da dosya sistemi ile görüntülenemeyen verilerin ortaya çıkartılması gerekmektedir. Bu işlemin yapılmasındaki amaç normalde görülmeyen ancak bir olayın aydınlatılmasında elektronik delil özelliği gösterebilecek ve soruşturmaya yön teşkil edebilecek önemli verilere ulaşmaktır[785].

Normal dosya silme işlemi ile silindiği düşünülen dosyalar, gerçekte disk üzerinde hiç silinmemiş gibi varlıklarını devam ettirmekte ve adli bilişim teknikleriyle kayıpsız olarak geri getirilebilmektedir. Bu bakımdan, silinen verilerin kurtarılması işlemi, kullanıcı veya işletim sistemi tarafından artık erişilmesi mümkün olmayan ve fakat dosya sistemi üzerinde varlığını devam ettiren dosyaların, tamamının veya bir

[783] Aydoğan, s. 52.

[784] Günal, s. 49-50.

[785] Uzunay, Dijital Delil Araştırma Süreci, s. 45.

bölümünün adli bilişim yazılımları aracılığıyla dosya sistemi üzerinden çıkartılmasını ifade etmektedir[786].

Verilerin silinmesi işlemi, verilerin sabit disk üzerinde bulunan adres bilgisinin silinmesi anlamına geldiğinden esasen veriler tamamen silinmeyip olduğu yerde bulunmakta ancak kullanıcı ve işletim sistemi bunu görememektedir. Bu nedenle uygun yazılımlar ile yapılacak tarama sonucunda elde edilen silinmiş veriler adli bilişim uzmanının dikkatle incelemesi gereken verilerdir[787].

Verilerin silinmesi işlemi her zaman yukarıda belirtildiği şekliyle basit silme şeklinde gerçekleşmemektedir. Veriler kimi zaman kalıcı silme işlemi (wipe) ile disk üzerindeki tüm değerleri ile birlikte "0" olacak şekilde silinir ve üzerine yazma işlemi gerçekleştirilir. Kalıcı silme işlemi (wipe) sonrasında disk üzerindeki her sektör "0" bilgisiyle işaretlenir. Böylece diske daha sonradan yapılan kopyalama işlemlerine eski verilerin dâhil olma ihtimali ortadan kaldırılır[788].

Bilişim sistemlerinde bir dosya silindiği zaman, sabit bellek üzerinde silinen dosya için ayrılan alan yeni bir veri ile doldurulmadığı sürece değişmeyecektir. Bu bakımdan basit programlar ile silindiği düşünülen veriler geri getirilebilecektir. Silinen verilerin üzerine yazıldığı zaman bile artık alan boşluklarında daha önce silinen veriler bulunduğundan, artık alan boşluklarından elde edilen verilerden, silinen dosyaya ilişkin bazı bilgileri kurtarma imkânı vardır. Bilgisayar sabit belleğinde bulunan verinin üzerine veri yazıldığı durumlarda, artık alan boşluklarında bulunan veriler hariç, yazılımsal olarak verinin kurtarılması mümkün değildir. Bununla birlikte, sabit diskin elektron mikroskoplarıyla okunarak veya sabit disk kazıması yapılması suretiyle verilerin yine de kurtarılması mümkündür. Ancak, bu durumda, sabit diskin zarar görme ihtimali bulunmaktadır[789].

[786] Henkoğlu, s. 56, 75-76.

[787] Çakır ve Kılıç, s. 31.

[788] Say, Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi, s. 76.

[789] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 259.

Belirtmek gerekir ki; şüpheli disk üzerinden imaj alma işlemi öncesinde silinen dosyalar, şüphelinin gizlemeye çalıştığı işlemlere ilişkin önemli ipuçlarına ulaşmayı sağlamaktadır. Bu bakımdan, günümüzde kullanılan adli bilişim teknikleriyle, silinen dosyaların tekrar elde edilmesinin zor ve karmaşık işler arasında yer almadığı dikkate alındığında, bir adli inceleme sırasında silinen dosyaların kurtarılma işleminin yapılmaması, incelemenin eksik yapıldığı ve çok önemli delillerin elde edilemediği düşüncesini haklı çıkartacaktır[790].

4.3.5. Yazıcı Dosyalarının (Spool Dosyalar) İncelenmesi

Yazıcı dosyaları (spoll dosyalar) bilgisayara bağlı yazıcılara belge yazdırma işlemi amacıyla oluşturulan dosyalardır. Belge yazdırma işlemi sırasında belgenin içeriği ve belgeye ait kullanıcı bilgileri ile belge adı gibi bilgiler iki farklı dosyaya kaydedilmektedir. Belge yazdırma işlemi sona erdiğinde bu dosyalar bilgisayar sabit diskinden silinirler. Eğer belge yazdırma işlemi sırasında bir sorun meydana gelmişse veya elektrik kesintisi olmuşsa belge yazdırma işlemi tamamlanmadığı için yazıcı dosyaları silinmezler. Bu bakımdan yazıcı dosyalarının incelemesi ile hangi kullanıcının, ne zaman ve hangi belgeyi yazıcıdan çıktı olarak aldığı tespit edilebilmektedir[791].

4.3.6. Üst Veri Bilgilerinin İncelenmesi

Üst veri bilgileri (metadata), sistem üzerinde bulunan dokümanlara ait kullanıcı, kayıt ve zaman bilgilerini ifade etmektedir. Office dosyaları için kullanıcı ve zaman bilgileri önemliyken, resim dosyaları için kayıt makinesi, konum ve zaman bilgileri önem arz etmektedir[792].

Üst veri bilgilerinin incelenmesi, bir elektronik belgenin değiştirilip değiştirilmediği ya da bu belgeye sonradan ekleme yapılıp yapılmadığını ortaya koyması bakımından önemlidir. Bu bakımdan üst veri incelemesi sonucunda bir olayla ilgili yeterli elektronik delil elde etmek mümkündür.

[790] Henkoğlu, s. 74.

[791] Aydoğan, s. 38-39.

[792] Çakır ve Kılıç, s. 36.

4.3.7. İnternet Geçmişinin İncelenmesi

Önceleri yalnızca bilgisayarlar üzerinden elektronik delil elde etmeye yönelik araştırmalar yapılırken, şimdilerde birbirine entegre edilmiş sistemlerden oluşan bilgisayar ağlarının ve bu ağların gelişmesiyle ortaya çıkan internetin bilişime yönelik etkinliklerinin temelini oluşturmasıyla birlikte bilgisayar ağları üzerinden de elektronik delil elde etmeye yönelik çalışmalar yoğunlaşmış ve "Bilgisayar Ağlarına Yönelik Adli Bilişim" kavramı doğmuştur[793].

Bu bağlamda şüphelinin kullanmış olduğu bilişim sistemleri ile erişim sağladığı internet geçmişinin incelenmesi sonucunda ziyaret edilen internet siteleri, ziyaret saatleri, yapılan kelime aramalarının belirlenmesi mümkün olduğundan bu incelemenin yapılması elektronik delil elde edilmesi bakımından önemlidir.

4.3.8. Dosya İmzalarının İncelenmesi

Bilinen tüm dosyaların başlık bölümü içerisine yerleştirilmiş bir imza bulunmaktadır. Dosya imzaları kullanılmak suretiyle dosya isim ve uzantısı değiştirilen dosyaların gerçek kimliklerine (jpg, doc, xls vb.) ulaşmak ve ilgili programı kullanmak suretiyle içeriğini görüntülemek mümkündür[794].

Dosya imzaları, adli bilişim uzmanlarının dosya incelemesi aşamasında şüpheli dosyayı ortaya çıkartmak amacıyla kullandıkları en önemli ipuçlarından birisidir. Varlığı bilinen bir dosyanın, şüpheli bilgisayar üzerinde araştırılarak ortaya çıkartılması, çoğu zaman klasik yöntemlerle mümkün olmamaktadır. Zira kullanıcılar kimi zaman dosya üzerinde değişiklikler yapmak suretiyle de dosyaları gizleyebilmektedirler. Ancak, dosya üzerinde yapılan bu değişiklikler, dosyanın kimliğini/imzasını değiştirmemektedir. Bu bakımdan, dosya imzalarının incelenmesi suretiyle bir dosyanın hangi kimliğe sahip olduğunu ve hangi programı kullanmak suretiyle açılabileceğini tahmin etmek mümkündür[795].

[793] Uzunay, Bilgisayar Ağlarına Yönelik Adli Bilişim, s. 1.

[794] Henkoğlu, s. 81.

[795] Henkoğlu, s. 81.

4.3.9. Gizli Verilerin İncelenmesi

Veri gizleme, şüphelilerin elektronik veriler üzerinde değişiklik yaparak bu verilerin başkaları tarafından erişimini engelleme işlemidir. Bu şekilde gizlenmiş veriler titiz bir çalışma yapılmadığı takdirde adli bilişim uzmanları tarafından tespit edilemeyebilirler. Dosyaların uzantılarının değiştirilmesi veya klasör içeriğinin gizli olarak ayarlanması ilk akla gelen ve basit nitelikte veri gizleme tekniklerindendir[796].

Bununla birlikte, kelime işlemci dosyasının uzantısı olan ".doc" uzantısı, resim dosyası uzantısı olan ".jpg" olacak şekilde yapılacak bir dosya uzantısı değişikliği her ne kadar basit aramalar bakımından gizlenmiş olacaksa da adli bilişim yazılımları, dosya içeriği ile uzantısını kontrol etmek suretiyle söz konusu gizleme yöntemini basit bir şekilde tespit edecektir. Aynı şekilde adli bilişim yazılımları, gizli olarak ayarlanan klasörleri de tespit edebildiğinden, basit bir adli bilişim yazılımı ile bahse konu gizleme yöntemi de aşılabilecektir[797].

Veri gizleme yöntemlerinin en önemlilerinden birisi de steganografidir. Steganografi uygulanmış verilerin incelenmesi hususiyet gerektirmektedir. Buna göre; steganografi, veri/mesaj, dosya veya kötü niyetli kodları bir başka dosya üzerine gizleme yöntemidir. Günümüzde steganografi birçok amaç için kullanılabilmektedir. Bilgisayar üzerindeki ilk verinin işlendiği günden beri veri gizlemeye yönelik olarak kullanılan steganografi, zararlı kodları gizlemeye yönelik olarak da günümüzde yaygın olarak kullanılmaktadır. Diğer bir ifadeyle, zararlı kodların dağıtımında kullanılan en etkili yöntemlerden biri de steganografidir. Zararlı kodu taşıyan bir dosya (örneğin JPEG dosyası), görünüşte zararsız ve tamamen orijinal gibi olsa da, çalıştığı anda sistem üzerinde büyük etkiler doğurabilmektedir. Steganografi yöntemiyle bir veriyi bilgisayar üzerinde bir dosya içerisine gizleyebilmek için yüzlerce program bulunmaktadır. Bu programlardan birçoğu güçlü şifreleme metotlarına da sahip oldukları için, gizlenen dosya veya veri için kırılmayı zorlaştıran fazladan güvenlik sağlamaktadır[798].

---

[796] Aydoğan, s. 37.

[797] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 261.

[798] Henkoğlu, s. 83-84.

Elektronik verilerin incelenmesi esnasında, bilgisayar içerisinde bulunduğu değerlendirilip klasik yöntemlerle elde edilemeyen birçok dosyanın steganografi yöntemi ile gizlendiği görülmektedir. Özellikle terör örgütlerinin kullandıkları iletişim yöntemleri arasında steganografi yöntemi ön plana çıkmakta, film ve resimler üzerine veri yerleştirmek suretiyle haberleştikleri tespit edilmektedir. Elektronik veri inceleme aşamasında steganografi yöntemi ile gizlenen mesaj ve dosyaları açığa çıkartmak için özel yöntemler uygulanmaktadır. Dosya ve mesajları başka bir dosya içerisine gizlemek için kullanılan algoritmalar, gizli dosya ve mesajların tekrar elde edilmesi veya açığa çıkartılması amacıyla da kullanılabilir[799].

Bununla birlikte, adli bilişim incelemeleri sırasında elde edilen dosyalardan hangisinde steganografi ile mesaj saklandığı bilinmediği için tüm dosyaların steganografi incelemesinden geçirilmesi gibi bir durum ortaya çıkmaktadır. Ayrıca mesajlar hangi yöntemle gizlenmiş ise aynı yöntem uygulanarak deşifre edilmesi gerekmektedir. Başka bir ifadeyle hangi dosya ya da dosyalarda steganografi olduğu ve bu dosyalara uygulanan steganografi yönteminin ne olduğu bilinmemektedir. Uygulamada steganografi çözümlerinin çoğunlukla sonuçsuz kalması nedeniyle adli bilişim uzmanlarının zaman kaybının önüne geçmek amacıyla bu uygulamayı göz ardı ettikleri görülmektedir[800].

Steganografi ile ilgili yapılan işlemlerin en başında, incelemeye konu disk üzerinde halen herhangi bir steganografi yazılımının kurulu olup olmadığı veya daha önceden böyle bir yazılımın kurulmuş olup olmadığının tespiti gelmektedir. İncelemeye derinlik katacak ve öncü olacak etkenlerin en önemlisi böyle bir yazılımın varlığının tespit edilmesidir. Zira bu tür yazılımların varlığının tespiti, steganografi ile ilgili verilere rastlama olasılığının yüksek olduğu ve göz ardı edilmesi durumunda incelemenin kesinlikle eksik yapıldığı anlamını taşıyacaktır. Herhangi bir steganografi programının varlığı, programın türüne ve desteklediği steganografi metotlarına göre, inceleme yaparken kullanılabilecek yardımcı inceleme programları hakkında da ipucu verir[801].

[799] Henkoğlu, s. 85.

[800] Aydoğan, s. 38.

[801] Henkoğlu, s. 87.

Orijinal resim dosyası ile üzerinde mesaj veya dosya bulunduğundan şüphelenilen dosyanın gözle dikkatle incelenmesi sonucunda da steganografi yönteminin kullanıldığına ilişkin izlere ulaşmak mümkündür. Ancak bunun için, kullanılan orijinal dosyanın çok yüksek çözünülürlükte veya başka bir ifadeyle büyük boyutta bir dosya olmaması gerekir. Steganografi yöntemi kullanılarak üzerinde mesaj veya dosya gizlenen dosya orijinal dosya ile karşılaştırılarak yakından incelendiğinde, resim üzerindeki bozulmalar ve küçük beyaz noktalar dikkati çekmektedir. Fakat birçok olayda resmin orijinali ile karşılaştırma imkânı bulunmadığı için, üzerinde inceleme yapılan resimdeki bozulmalar pek çok nedene bağlanarak göz ardı edilebilmektedir. Steganografinin temel amacı gizlilik olduğu için, güçlü algoritma kullanılmış ve doğru büyüklükte dosyaların seçilmiş olması halinde, gizliliğin gözle fark edilemeyecek derecede olması beklenmelidir. Bu nedenle, üzerinde gizli veri olduğundan şüphelenilen dosyanın mümkün olması halinde orijinal veri ile karşılaştırılması, istatiksel inceleme yöntemlerinin kullanımı ve çeşitli steganografi yazılımlarının kullandığı algoritmaları tanıyabilen yardımcı yazılımlardan faydalanılması inceleme sonucunda daha fazla bulgu elde etmek için gereklidir[802].

4.3.10. İncelemenin Sonucu

Bilişim sistemleri ve bağlı donanımları üzerinde yapılacak imaj alma işleminden sonra artık adli bilişim uzmanının elinde bir takım bulgular bulunmaktadır. Bunların bir kısmı görünür nitelikte olmasına karşın bir kısmı ise gizli, silinmiş veya şifrelenmiş niteliktedirler[803]. İnceleme aşaması sonucunda her türlü veri ortaya konulmaktadır. Örneğin; fotoğraflar, grafik dosyaları, videolar, çeşitli yazı dokümanları (MS Word), MS Ewcel, OpenOffice v.b), anlık mesajlaşma kayıtları (Facebook chat, MSN, Gtalk, ICQ, v.b), elektronik postalar, ziyaret edilmiş ve sık kullanılan web siteleri, silinmiş, gizlenmiş veya sıkıştırılmış dosya ve klasörler, şifreli dizinler, dosyaların oluşturulma, değiştirilme ve erişim tarih kayıtları ilk akla gelen ve en sık rastlanan bulgulardır[804].

[802] Henkoğlu, s. 88.

[803] Dülger, s. 678.

[804] Günal, s. 56.

4.4. Elektronik Delilin Analizi

4.4.1. Genel Olarak

İşletim sisteminden imajı alınmış verilerin tümünün gözle görülür hale getirilmesinden sonra analiz aşamasına geçilmektedir. Bu aşamada, elde edilen verilerin hangilerinin ve ne ölçüde raporlanacağının tespiti yapılmaktadır. Bu aşamanın bir tür ayıklama safhası olduğu söylenebilir. Soruşturmayla ilgisi olmayan dosyalar analiz aşamasında elenir, işe yarayabileceği değerlendirilen bulgular ise elde ediliş yöntemleri de belirtilerek adli mercilere sunulurlar[805]. Analiz, inceleme aşamasında çıkartılan verilerin mantıklı ve yararlı bir biçime konarak yorumlanması anlamını taşımaktadır[806]. Bu bakımdan analiz aşamasının amacının soruşturma için gerekli olan elektronik delilin tespitini yapmak olduğu söylenebilir[807].

Analiz aşaması, adli bilişim sürecinde elde edilen elektronik delilden olayı aydınlatıcı kısmını bulma ve toplama safhasıdır. Örneğin, bir dolandırıcılık olayında analiz işleminin öncelikli hedefi, mali işlemleri içeren kayıtların silinmesi ihtimalinden ötürü, mali kayıtlardır. Bir çocuk pornografisi suçunda ise analizin hedefi yasak nitelikteki fotoğraf veya video kayıtlarını bulmaktır. Bu bakımdan, analiz aşamasında gerek aranan delil türü gerekse benimsenen yaklaşım biçimi itibariyle büyük ölçüde değişkenlik gösteren her bir soruşturma kendine mahsus koşullar açısından ayrıcalık göstermektedir. Ayrıca, analiz aşaması kişisel beceriler, araç kullanımı ve adli bilişim uzmanlarının eğitimi açısından da büyük etkiye sahip olan bir alandır[808].

Analiz aşamasında toplanan ve gizli veya müphem durumda olup da görünür hale getirilen elektronik delilin yürütülen soruşturma ve açılması muhtemel kamu davası açısından taşıdığı hukuki değer belirlenir. Bu bakımdan analiz, inceleme aşamasında

---

[805] Tan, http://mbasic.facebook.com/notes/gazi-%C3%BCniversitesi-adli-bili%C5%9Fim-anabilim-dal%C4%B1/adli-bili%C5%9Fim-computer-forensic-aydo%C4%9Fan-tan/502561823148516/?refid=17 (06 Nisan 2014); Özbey, s. 75.

[806] Ashcroft, Daniels and Hart, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf (12 Ocak 2015), s. 1.

[807] Brian Carrier, "Open Source Digital Forensics Tools: The Legal Argument", 2002, http://www.digital-evidence.org/papers/opensrc_legal.pdf (18 Nisan 2015), s. 2.

[808] Daniel and Daniel, s. 12-13.

elde edilen verilerin önemi ve ispat değeri açısından yapılan bir işlem olması nedeniyle inceleme işleminden farklıdır. İnceleme, adli bilişim uygulayıcılarının uzmanlık alanlarına giren ve delilleri ortaya çıkarmaya yönelik teknik bir gözden geçirme iken analiz, araştırma ekibi tarafından gerçekleştirilen ve teknik olarak belirlenen delilleri bir hukuki değer verilmesi aşamasıdır[809].

Elektronik delilin incelenmesi aşaması teknik konuları kapsamakla birlikte bu teknik bilgilerin elde edilmesi sırasında soruşturmanın başka aşamalara da kayabilmesi muhtemeldir. Bu bakımdan analiz işlemini yapacak uzmanların bu teknik inceleme sonuçlarını analiz etmesi ve buna göre soruşturmaya yön vermesi gerekmektedir. Bu sayede elektronik delilin bütününün incelenmesi üzerine yapılacak analiz sonucunda anlamlı bir yargıya varma imkânı doğacaktır.

Kapalı bilgisayar ve genellikle sabit disk gibi veri depolama araçları üzerinde yapılan bir inceleme işlemi niteliğindeki elektronik delillerin analizi işlemi genellikle laboratuvar ortamında gerçekleştirilir[810]. Bu bakımdan, bilişim laboratuvarlarının akredite edilmesi, kaliteli raporların hazırlanması ve bunların kamu tarafından kabul görmesi bakımından önemlidir. Bu hususta özellikle uluslararası alanda kabul görmüş yazılımların ve donanımların kullanılması özellikle bilişim suçlarının soruşturulması aşamasında daha uygun görülmektedir[811].

Analiz işlemine başlamadan önce, analizi yapılacak sabit disk üzerinde yüklü bulunan işletim sisteminin sürümünün öğrenilerek uygulanacak işlemler sırasında kullanılması düşünülen yazılımların belirlenmesi zaman kaybının önlenmesi bakımından önemlidir[812].

Analiz işlemi, adli standartlarda alınan imajın adli kopyası üzerinde yapılır ve böylelikle orijinal delil riske atılmadan çalışma tamamlanır. Hash algoritmasının oluşturulmasıyla daha önce alınmış olan imajın orijinali ile kıyaslanması sağlanır. Böylece, analiz

[809] Özdilek, Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku, s. 202; Keser Berber, Adli Bilişim, s. 45; Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 167.

[810] Dülger, s. 672.

[811] Gözüşirin, s. 96.

[812] Henkoğlu, s. 139.

sonrasında elektronik delilin değiştirilip değiştirilmediğine dair şüphe oluşması halinde karşılaştırma yapılarak elektronik delilin güvenilirliği kontrol edilmiş olur[813].

Elektronik delilin imajına ait adli kopya genellikle uluslararası alanda kabul gören adli bilişim programları ile incelenerek analiz edilmektedir. Bunlardan en çok kullanılan EnCase ve FTK programlarıdır. Fiziksel arızalı delillere ise PC3000 adlı cihaz ile müdahale edilebilmektedir. Bununla birlikte uygulanan yöntem analizi yapacak uzmanın tecrübe ve kabiliyetine kalmıştır. Ancak uygulamada belli programların ağırlıklı olarak kullanıldığı görülmektedir. Bu programların ihtiyaca cevap vermediği özel durumlarda ise analizi yapacak uzmana bağlı olarak çeşitli açık kaynak kodlu programlar kullanılmaktadır[814].

Adli merciler, analiz işlemini yapacak birimlerden elektronik verilerin özellikle soruşturma ya da kovuşturma açısından önem arz eden dosyaların kimin hangi elektronik medyasından çıktığı, bu medyaya daha sonradan mı kopyalandığı yoksa medya üzerinde mi oluşturulduğu, kim tarafından hangi tarihte oluşturulduğu yönündeki bilgileri istemektedirler[815]. Bu bilgilerin adli mercilere tam olarak verilmemesi, şüphelinin kendisine ait elektronik medyadan elde edilen elektronik delilin elde edilme tarihinden önce veya sonra başkaları tarafından yüklendiği yönündeki savunmasını bertaraf etme noktasında, adli süreci olumsuz etkileyebilecek sorunlara neden olabilmektedir.

Elektronik delilin analizi aşamasında bazı sorunlarla da karşılaşıldığı görülmektedir. Özellikle üzerinde analiz yapılacak medyaya hangi suç ile ilgili elkonulduğu, o medyada ne tür bilgiler elde edilebileceği gibi bir yol haritası çizilmeden başlatılan analiz işlemlerinden sonuç alınmama riski bulunmaktadır. Ayrıca, ortaya çıkan bir sorunun çözümünde başka kaynaklarda yeterli araştırmanın yapılmadığı veya bu araştırmanın yapılması için verilen sürenin yeterli olmadığı durumlar görülebilmektedir.

[813] Dülger, s. 672-673.

[814] Çakır ve Sert, s. 161.

[815] Çakır ve Sert, s. 162.

Diğer taraftan karşılaşılan en belirgin sorunlardan biri de analiz işleminin detaylı yapılmaması veya değerlerin rapora girişi sırasında hataların olmasıdır[816].

Gelişen teknolojiye ayak uydurularak yapılan analizlerde karşılaşılan hataların genellikle maddi nitelikte oldukları görülmektedir. Bu bağlamda, raporlama sırasında delile ait özelliklerin yanlış girilmesi önemli bir sorun teşkil etmektedir. Bu durum genellikle adli bilişim uzmanlarının raporlama aşamasında kendilerine ait bilgilere verdikleri büyük önemden kaynaklandığı değerlendirilmektedir[817]. Aşağıda analiz aşamasında ön plana çıkan bazı işlemlere değinilecektir.

4.4.2. Dosyalarda Bulunabilecek Zararlı Kodların Analizi

Elektronik delilin elde edilmesi ve analizi aşamasında zararlı kodların varlığının tespit edilmesi, analiz sonucunu etkileyebilmektedir. Bu bakımdan, yapılmakta olan araştırmanın konusu ne olursa olsun meydana gelen sonuca etki eden bir zararlı kodun varlığı adli bilişim uzmanları tarafından değerlendirmeye alınmalıdır[818].

Zararlı kodların sistem dosyaları üzerinde yapmış oldukları değişikliklerin tespiti amacıyla kullanılan en önemli yöntem kıyaslama tekniğidir. İşletim sistemi ve servis paketlerinde bulunan dosyalar, belirli bir dosya bütünlüğüne sahip olup kurulumdan kuruluma farklılık göstermezler. Bu bakımdan, analiz aşamasında üzerinde işlem yapılmamış bir sistemin dosyaları ile şüphe duyulan sistem dosyaları karşılaştırılarak sonuca ulaşılabilir[819].

4.4.3. Birebir Aynı Dosyaların (Duplike Dosyalar) Analizi

Gerçekte birbirlerinin aynen kopyası olup bilgisayarda farklı klasörlerde görünüme sahip olan dosyalara duplike dosyalar denilmektedir[820]. Farklı isimlerle oluşturulan

[816] Çakır ve Sert, s. 163.

[817] Çakır ve Sert, s. 163.

[818] Henkoğlu, s. 82.

[819] Henkoğlu, s. 82-83.

[820] Askville By Amazon (t.y), http://askville.amazon.com/duplicate-files-pc-effect-havng-performance/AnswerViewer.do?requestId=16358454 (05 Şubat 2014).

ancak içerik itibariyle birbirleriyle aynı nitelikte olan duplike dosyaların hash değerleri de aynıdır. Zira hash değerinin hesaplanmasında dosya adının bir önemi bulunmayıp önemli olan dosyaların içeriğidir. Bu bakımdan içeriği aynı olan dosyaların hash değerleri de aynı olacağından yapılan analiz sırasında adları farklı olsa da aynı içeriğe sahip duplike dosyaların tespitinin sağlanması mümkündür.

4.4.4. Takas Dosyaların Analizi

Takas alanı, işletim sisteminin kullanmış olduğu fiziksel belleğin yetersiz kalması durumunda, önceden işletim sistemi ya da kullanıcı tarafından büyüklüğü belirlenen ve fiziksel belleğe ek olarak kullanılabilen sabit disk üzerinde tanımlı sanal bellek alanını ifade etmektedir. Bu alan, işletim sistemi üzerinde gizli bir sistem dosyası olarak bulunmaktadır[821].

Şüpheliler tarafından elektronik delilin yok edilmesi amacıyla uygulanan kalıcı silme yöntemi yaygın şekilde kullanılmasına karşın takas dosyalarının içerisinde bulunması muhtemel önemli delillerin varlığı çoğu zaman gözden kaçırılmaktadır. Takas dosyaların analizi suretiyle, farklı bir yöntemle elde edilemeyecek verilere ulaşılabilmesi mümkündür. Nitekim kredi kartı numaraları ve telefon numaraları gibi bilgiler, takas dosyalarından elde edilen parçalar halindeki veriler içerisinden daha kolay fark edilebilecek nitelikteki verilerdir[822].

4.4.5. Sistem Kayıtlarının Analizi

Sistem kayıtlarının analizi, tüm analiz işlemlerinin sonuçları arasındaki bağlantıyı oluşturması bakımından önemlidir. Kullanıcıların yapmış oldukları işlemler, kurulan programlara ilişkin bilgiler ve işletim sisteminin tutmuş olduğu kayıtlar arasındaki tutarlılık disk/dosya analizinde oluşan sonucu desteklemelidir. Bu bağlamda, disk üzerinden elde edilen delil niteliğindeki belgenin oluşturulma ve değiştirilme tarihi, sistemin açıldığı tarih bilgileri ve kullanıcı profiline ait kayıtlarla bağlantılı olmalıdır. Aksi takdirde belge ile bilgisayar ya da kullanıcı eşleştirilmesinin yapılmaması

[821] Henkoğlu, s. 88.

[822] Henkoğlu, s. 89.

durumunda belgenin hazırlanışı ve kim tarafından kullanıldığı konusunda daha detaylı bir inceleme zorunluluğu doğacaktır[823].

4.4.6. Elektronik Posta Analizi

Elektronik posta (e-posta), internet üzerinde bilgisayarlar ve insanlar arasında bilgi alışverişini sağlayan ve en yaygın kullanılan internet uygulamasıdır. Elektronik posta, istemci/sunucu prensibi doğrultusunda çalışmaktadır. Buna göre, kullanıcılar elektronik posta göndermek veya elektronik posta içeriğine ulaşmak için elektronik postanın geldiği veya gönderildiği bilgisayara, yani sunucuya erişmeleri gerekmektedir[824].

Elektronik posta, internetin en çok kullanılan özelliklerinden birisidir. Elektronik posta, klasik postaya nazaran alıcısına çok daha hızlı biçimde ulaştırılabilmektedir. Bu haberleşme tarzında, elektronik posta göndericisi, alıcı olarak birden fazla kişiyi seçmek suretiyle aynı içerikteki iletiyi aynı anda birden fazla kişiye gönderebilmektedir. Ayrıca, aynı kişinin birden çok elektronik posta adresi sahibi olması ve bu kişinin genel ve kişisel kullanımlarına göre bu elektronik posta adresleriyle iletilerini gönderebilmesi mümkündür[825]. Elektronik postanın bu özellikleri, onu en önemli elektronik delil kaynaklarından biri haline getirmektedir.

Elektronik posta, değişik açılardan ceza yargılamasında elektronik delil olarak kullanılabilir. Öncelikle, elektronik postanın alındı ve gönderildi bilgileri, kişiler arasındaki iletişime işaret ettiğinden dolayı taraflar arasındaki iletişimi belgeler. İkinci olarak, elektronik posta göndericisinin yazmış olduğu metin, elektronik delil olarak kullanılabilir. Üçüncü olarak ise elektronik posta, HTML formatında elektronik belge üzerine yazılabildiği gibi elektronik postaya değişik türdeki dosyalar da eklenebilmektedir. Bu nedenle, elektronik posta metni kadar, eklenen dosyalar da elektronik delil olarak kullanılabilmektedir[826].

---

[823] Henkoğlu, s. 91.

[824] E-Posta Nedir?, http://www.frmtr.com/bilgisayar-guvenligi-hakkinda-sorulariniz-ve-sorunlariniz/65966-e-posta-nedir.html (18 Kasım 2014).

[825] Servet Yetim, "Elektronik Posta (e-posta) Hesabı İçeriği Mirasa Konu Olabilir mi?", **Terazi Hukuk Dergisi**, Cilt. 3, Sayı. 21, (Mayıs 2008), s. 51.

[826] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 153.

Bu bağlamda, elektronik posta, zararlı kodların gönderilmesi, hırsızlık suçları ve internet dolandırıcılığı gibi birçok bilişim suçunda araç olarak kullanılmasının yanı sıra hakaret, kasten öldürme gibi klasik suçlarla ilgili yürütülen soruşturmalarda olayın aydınlatılmasına yarar sağlayacak verilere ulaşılabilen kaynaklar arasındadır. Bu bakımdan adli bilişim incelemeleri sırasında analizi gereken öncelikli alanlardan birini de elektronik posta iletileri oluşturmaktadır[827].

Diğer taraftan, elektronik postalar, alıcı kişinin sunucusuna ulaşıncaya kadar birçok sunucudan geçerler. Bu arada bazı sunucularda, elektronik posta iletişimine ilişkin dijital izler kalabilmektedir. Bu bakımdan, sunucularda kalan ve elektronik postanın varlığına delalet eden dijital izler de elektronik delil olarak kullanılabilir[828].

Elektronik postanın hukuki ve cezai sorumluluğu elektronik postayı hazırlayan ve gönderen kişiye aittir. Bununla birlikte, elektronik posta kısmında yalnızca ad ve soyadın görünmüş olması, elektronik postanın altında kişinin ad ve soyadının yazıyor olması bu ad ve soyada sahip kişinin doğrudan sorumlu tutulması için yeterli değildir. Zira internette herkes adına elektronik posta adresi açma olanağı bulunmakta ve elektronik postayı gönderen kişi olarak herhangi bir kişinin ad ve soyadı kolayca eklenebilmektedir. Bu nedenle suça konu elektronik postayı gönderen gerçek kişinin kuşkuya yer vermeyecek biçimde belirlenmesi gerekmektedir[829].

Bu bakımdan elektronik delil analizi gerçek suçlunun tespiti açısından büyük öneme sahiptir. Elektronik posta analizi, temel olarak, her ileti üzerinde gizli olarak bulunan verilerin incelenerek, suçun kaynağını ve muhtemel hedeflerini tespit etmek amacıyla gerçekleştirilir. Bu işlem çoğu zaman sadece iletiyi alan kullanıcı ile sınırlı kalmamakta, yurt dışı kaynaklı elektronik posta sunucularını da içine almakta ve bu durum ise yürütülmekte olan soruşturmayı zora sokmaktadır. Elektronik posta analizi hususunda yeteneğin artabilmesi için, zararlı kodların dağıtım tekniği, bilgisayar ağları ve veri

[827] Henkoğlu, s. 114.

[828] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 153.

[829] Özgür Eralp, "Elektronik Postaların İspat Hukuku Açısından Delil Olma Değeri", 2011, http://www.ozgureralp.av.tr/detay/makaleler/elektronik-postalarin-ispat-hukuku-acisindan-delil-olma-degeri/6/328/ (24 Ocak 2015).

paketlerinin bilgisayar ağları üzerindeki ilerleyişini doğru algılamak ve buna göre çözüm üretmek gerekmektedir[830].

4.5. Elektronik Delilin Raporlanması ve Sunumu

CMK m. 209/1 hükmüne göre naip veya istinabe yoluyla sorgusu yapılan sanığa ait sorgu tutanakları, naip veya istinabe yoluyla dinlenen tanığın ifade tutanakları ile muayene ve keşif tutanakları gibi delil olarak kullanılacak belgeler ve diğer yazılar, adli sicil özetleri ve sanığın kişisel ve ekonomik durumuna ilişkin bilgilerin yer aldığı belgeler, duruşmada okunur. CMK m. 214/1 hükmüne göre ise, bir açıklamayı ve görüşü içeren resmi belge ve diğer yazılar ve fenni muayene ve doktor raporlarının okunmasından sonra gerekli görülürse belge ve diğer yazılar veya raporda imzası bulunanlar, açıklamada bulunmak üzere duruşmaya çağrılabilirler.

Adli bilişim uzmanı suça konu eylemin seyrinin belirlenebilmesi için davanın kapsamına da riayet ederek elektronik delilleri iyi bir şekilde değerlendirmelidir[831]. Nitekim adli bilişim uzmanı tarafından yapılan inceleme ve analizler, ancak yargılamaya konu olay ile irtibatlandırılması ve mahkemeye uygun şekilde sunulması durumunda anlam ifade etmektedir. CMK'nın 209. ve 214. maddeleri birlikte değerlendirildiğinde, adli bilişim uzmanının raporu, delil olarak kullanılacak belge niteliğinde olacağından duruşmada okunmalıdır. Bu bağlamda, hazırlanacak raporun, ceza yargılamasına katılan kişiler ve özellikle mahkeme tarafından anlaşılır dille yazılması gerekir[832].

Kriminalistik biliminde delil inceleme aşamasında genellikle elle tutulan ve gözle görülen somut deliller bulunmasına karşın adli bilişim bilimi elektronik ortamdaki delillerle ilgilenmektedir. Bu bakımdan, bilişim sistemlerindeki elektronik delil olarak kullanılması muhtemel verilerin tespiti ve delil olarak ortaya konulması, verilerin muhafaza edildikleri manyetik ve dijital ortamdan anlaşılır bir şekilde çıkartılarak yazılı metin haline dönüştürülmesi suretiyle mümkündür. Bazı durumlarda veriler, yazılı

[830] Henkoğlu, s. 114-115.

[831] Ashcroft, Daniels and Hart, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf (12 Ocak 2015), s. 1.

[832] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 269.

metne dönüştürülse bile bilişim sistemleri hakkında bilgi ve birikimi olması beklenmeyen adli makamlar tarafından anlaşılacak nitelikte olmamaları nedeniyle açıklanmaları ve izah edilmeleri gerekmektedir. Zira adli bilişim bilimi çoğunlukla elektronik delil üzerine yoğunlaşmaktadır[833].

Bu bağlamda, adli bilişim sürecinin şeffaf bir görünüm arz etmesi için daha önceki aşamalarda belirtilen tüm metot ve prosedürün önemli detaylarının adli bilişim sürecinin sonundaki rapor ve sunum aşamasında mutlaka belirtilmesi gerekmektedir. Raporun önemli bir kısmı sonuca götürücü analiz ve bunları destekleyen delillerin tanımlanmalarıyla ilgili olacaktır. Destekleyici nitelikteki deliller tam ve doğru bir şekilde tanımlanmadıkça sonuç yazılamayacaktır[834].

Elektronik delilin elde edilmesine ilişkin süreç özel bir uzmanlık gerektirmektedir. Ancak uzmanlık incelemeleri teknik konuları kapsaması nedeniyle sonucun izah edilmesi sırasında hem mahkemenin hem de tarafların anlayacağı ve ikna olacağı şekilde bir yolun izlenmesi gerekmektedir. Bu bakımdan elde edilen elektronik delilin raporlanması ve sunumu adli bilişim sürecinin önemli bir parçasıdır[835]. Nitekim bu aşamada mahkemeye delil olarak sunulabilecek tüm delillerin bilgilendirilmesi yapıldığı için iyi rapor edilmemiş bir adli bilişim çalışmasından gerçek verim elde edilmesi düşünülemez[836].

Raporda, inceleme sürecinin akış aşamaları ve delil inceleme sürecinin adımları gibi önemli aşamaların belirtilmesi gerekir. Böylece raporda sunulan bilgilerin nasıl elde edildiği açıklığa kavuşturulmalı, inceleme sürecinin güvenilirliği ortaya konulmalı ve delil bütünlüğünün korunduğu vurgulanmalıdır. Ayrıca, inceleme sürecinin tekrar edilebilirliği yani aynı cihazlar üzerinde başka bir uzman tarafından inceleme yapılması durumunda da aynı sonuçların alınacak olduğu, başka bir anlatımla raporun bilimsel

[833] Ekizer, http://www.ekizer.net/adli-bilisim-computer-forensics (06 Nisan 2014).

[834] Uzunay, Dijital Delil Araştırma Süreci, s. 46.

[835] Dokurer, Adli Bilişim, 2. Polis Bilişim Sempozyumu, s. 228.

[836] Aydoğan, s. 17.

olduğu açıkça ortaya konulmalıdır. Aksi halde, yargılama sırasında delillerin güvenilirliği konusunda soru işaretleri doğabilecektir[837].

Elektronik delilin olay yerinden toplanıp inceleme ve analiz aşamasından geçtikten sonra raporlanarak adli makamlara sunulmaları hukuki ve teknik bir değerlendirmeyi ifade etmektedir. Bununla birlikte raporlama ve sunum aşamasında elektronik delilin nasıl elde edildiğine ilişkin teknik boyutu ve hangi adli bilişim yönteminin kullanıldığının ayrıntılı ve anlaşılır bir şekilde belirtilmesi gerekmektedir. Raporda ayrıca araştırmanın yapıldığı zaman dilimi, incelenen elektronik deliller ve araştırma sonucunda ele geçen bulgulara ilişkin bilgiler de verilmelidir[838].

Elektronik delilin toplanması, incelenmesi ve analizi işlemlerinin her zaman birbirini takip eden düz bir çizgide ilerlemediği, bazen inceleme veya analiz aşamalarında elde edilen verilerin, gözden kaçan bazı delilleri elde etmek üzere yeniden olay yerine gidilmesini gerektirdiği görülmektedir. Ancak, elektronik delillerin toplanması, incelenmesi ve analizi işlemlerinin yapıldığı sürecin mümkün oldukça birbirlerini düz bir çizgi halinde takip etmesi ve bilirkişi sunum ve raporlama aşamasında da tüm süreç boyunca yapılan işlemlerin kararı verecek makamı şüpheye düşürmeyecek şekilde sıralı olarak açıklanması sağlanmalıdır[839].

Soruşturma sürecinde delillerin iyi bir şekilde organize edilerek raporlandırılması her zaman önemlidir. Delil organize işlemi hem elektronik delil hem de fiziksel deliller için önem arz etmektedir. Elektronik delil organize edilirken çoğu zaman fiziksel delillere de ihtiyaç duyulmaktadır. Bu bakımdan delillerin organize edilişi sırasında bu durum göz önünde bulundurulmalı ve hangi delilin hangi konu ile ilgili olduğu belirlenmelidir. Konunun gelişimi çoğu zaman hem elektronik hem de fiziksel delillerin doğru bir sıraya konulması ile anlaşılabilmektedir. Elektronik delilin yoğunluğu ve iyi organize edilmemiş olması araştırmacıların delil inceleme aşamasında doğruyu bulamamalarına veya geç bulmalarına neden olabilmektedir. Bu bakımdan da adli bilişim sürecinde tüm

[837] Yunus Balı, "Adli Bilişim Rapor Metinlerinin Yargılama Sürecinde Kullanımı ve Anlamlandırılabilirliği", Levent Bayram (Ed.), **Ses Görüntü ve Data İncelemeleri** içinde (231-238), Ankara: Adalet Yayınevi, 2008, s. 234.

[838] Günal, s. 68.

[839] Henkoğlu, s. 23.

aşamalar doğru şekilde geçilmeli, deliller mantık sırasına göre organize edilmeli ve mahkemeye tatmin edici bir rapor sunulmalıdır[840].

Elektronik delilin raporlanması ve sunumu aşamasında karşılaşılan en büyük sorunlardan birisi, adli makamların adli bilişim alanına yeterince hâkim olmamaları ve işlemlerin ne kadar zaman ve dikkat isteyen ayrıntılı bir analizi gerektirdiği hususunu bilmemeleri nedenleriyle istenilen raporun verilen süre içerisinde yerine getirilememesidir. Diğer bir sorun ise çoğu zaman adli makamlara inceleme ve analiz aşamasında kullanılan terimlerin ne anlama geldiğinin anlatılması sırasında yaşanan sıkıntılardır[841].

Raporlama ve sunum aşamasının tamamlanmasıyla adli bilişim süreci de sona ermiş olacaktır. Bundan sonra mahkeme kendisine sunulan rapora dayanarak hüküm verebileceği gibi delillerin serbestçe değerlendirilmesi ilkesi uyarınca sunulan rapora dayanmaksızın da karar verebilecektir.

4.6. Adli Bilişim Sürecinde Karşılaşılan Sorunlar

Adli bilişim süreci sonucunda bilişim sistemlerinden veya veri depolama birimlerinden elde edilen elektronik veriler, çözümlenerek anlaşılır vaziyette elektronik delil haline getirilmektedirler. Elektronik verilerin kaynağının ne olduğu, ne zamandan beri bilgisayarda bulunduğu, bu verilerde değişiklik yapılıp yapılmadığı, yapılmış ise nasıl ve ne zaman yapıldığı gibi soruşturma için hayati öneme sahip bilgiler adli bilişim sürecinde tespit edilmektedir.

Adli bilişim süreci, potansiyel riskleri beraberinde taşıyan bir süreçtir. Bu süreç, adli bilişim uzmanlarını, çalışma sürecinde bazı kritik materyallerin kaybolması veya önem arz eden bir işin devri gibi bazı sorumlulukların altında bırakmaktadır. Ayrıca, ortaya çıkan birçok içsel sorun, elektronik delilin adli bilişim sürecinde kaybolmasına neden olabilmektedir[842].

[840] Yetim, Dijital Kanıt Araştırma Yöntemleri, s. 1217.

[841] Çakır ve Sert, s. 163.

[842] Şeker, s. 7.

Fiziksel niteliğe sahip olmayan elektronik delilin hızlı bir şekilde kaybolması ise mevcut yapı içerisinde ağır işleyen soruşturma işlemlerinin etkin şekilde yürütülmesini engellemektedir. Bu nedenle soruşturma sürecinde mümkün olduğunca hızlı hareket edilmeli ve sadece bu nitelikte soruşturmalarda faaliyet yürütecek birimler kurulmalıdır. Ayrıca, kamu görevlilerinin yasak soruşturma yöntemlerini kullanmaktan kaçınmaları büyük önem arz etmektedir[843].

Bu bakımdan delillerin karartılmaması hususunun önemi tüm kademe personeli tarafından kesinlikle anlaşılmalıdır. Tüm adli süreçte yer alan personel, elektronik delilin kolaylıkla değiştirilebilir olduğunu bilmeli ve delillerin toplanması, incelenmesi ve analizi süreci boyunca alınan prensip ve prosedürlere uymalıdır. Zira delillerin karartılmasına neden olabilecek yanlış uygulamalar mahkemeler tarafından delillerin reddedilmesine yol açacaktır[844].

Bununla birlikte potansiyel sorunların haricinde de adli bilişimin ilke ve standartlarının henüz belirlenmemiş olması, usul uygulamalarında konunun öneminin bilinmemesi, araştırmalara ve bilimsel incelemelere kaynak ayrılmaması, ilgili kurumların ve görevlilerin yeterince eğitilmemesi, asgari standartların sağlandığı laboratuvarların henüz istenen seviyeye getirilmemiş olması gibi adli bilişim sürecini zora sokan sorunlarla karşılaşılmaktadır[845].

Uluslararası alanda kabul edilen adli bilişim ilkelerine ülkemizde de önem veriliyor olmasına karşın elektronik delilin elde ediliş sürecine ilişkin işlemlerin ne şekilde yapılacağı hususu ile uyulması gereken standartlar ve sorumluluklara ilişkin yeterli ve net yasal düzenlemelerin bulunmaması uygulamada birçok elektronik delilin henüz elde ediliş sürecinde geri dönülemeyecek şekilde kaybolmasına zemin hazırlamaktadır[846].

Diğer taraftan uluslararası alanda kabul edilen adli bilişim ilkelerine önem verilmesi ve bunların yasal bir zemine oturtulmasının yanı sıra bu ilkelere uygun teknolojik alt

[843] Uçkan ve Beceni, s. 423.

[844] Say, Bilişim Suçlarında Olay Yeri İncelemesinin Hukuki Boyutu, s. 259.

[845] Ahi, "Adli Bilişim Nedir ?", http://www.bilisimhukuk.com/2009/07/adli-bilisim-nedir/ (04 Mayıs 2014).

[846] İlker Çiçek, "Ülkemizde Adli Bilişim Laboratuarı Kurulumu ve Bilişim Suçlarıyla Mücadeleye Katkıları", (**Yayınlanmamış Yüksek Lisans Tezi**, Haliç Üniversitesi FBE, 2008), s. 14.

yapının kurulmasına da ağırlık verilmelidir. Ayrıca, teknolojik alt yapı kurulsa dahi teknoloji üretilmedikçe delil elde etmede kullanılan programlar, cihazlar ve teçhizatlar zamanla eskiyecek ve yenilerini edinebilmek için ithal edilmek zorunda kalınacaktır. Bu bakımdan adli bilişim süreci ne kadar pahalıya mâl olursa olsun laboratuvarların kurulması ve bilirkişilik bakımından personel eğitimi için gerekli sermayenin sağlanması hayati önem arz etmektedir[847].

Elektronik delil, diğer delil türleri ile benzer veya ortak özelliklere sahip olmanın yanı sıra bir takım farklı özelliklere de sahiptir. Elektronik delilin sahip olduğu farklı özelliklerin, adli bilişim sürecinde görev alan teknik personeller tarafından bilinmesi ve bu doğrultuda araştırmaların yürütülmesi hayati öneme sahiptir[848]. Bu bakımdan adli bilişim uzmanlarının bilişim sistemlerinde çok ileri düzeyde bilgiye sahip olmaları, bu özelliklerini daima sürdürebilecek şekilde güncel teknolojiyi takip etmeleri ve ayrıca temel seviyede kendi alanları için gerekli hukuk bilgisine haiz bulunmaları gerekmektedir[849].

Adli bilişim sürecinde tek bir bilişim sisteminden dahi pek çok anlamlı veri çıkartılabilmekte ve adli bilişim uzmanının bu verilerden somut olayla doğrudan ilgili ve faydalı olanlarını tespit etmesi beklenmektedir. Adli bilişim uzmanının dava konusu olaya yeterince hâkim olamaması ise bu eleme işleminin sağlıklı yapılamaması ve yargılama sürecinin olumsuz etkilenmesi sonucunu doğurmaktadır[850].

Gerçekten de, adli bilişim konusunda özel ve uzman personelin olmayışı neticesinde halen elektronik delil elde etme imkânı olmayan birçok malzemenin toplandığı, veri cihazlarına yedekleme yapılmadan ve elektronik olarak mühürlenmeden el konulduğu, şüpheliye ve avukatına herhangi bir tutanak verilmediği, bilişim sistemlerinin ve diğer veri depolama aygıtlarının manyetik alan etkisinden soyutlanmadan özensizce taşındığı, tamirhaneleri andıran odalarda veri yazmayı önleyen cihazlar (FRED) olmaksızın

[847] Ünal, s. 153.

[848] Say, Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi, s. 99.

[849] Şeref Sağıroğlu ve Mehmet Karaman, "Adli Bilişim", **Teletapi Haberleşme ve Bilişim Teknolojileri Dergisi,** Sayı. 203, (Ağustos 2012), s. 67.

[850] Akarslan, s. 132.

elektronik delil incelemesi yapıldığı görülmektedir. Bu yanlış uygulamalara yapılan itirazlar ise kimi zaman kaynak yetersizliği, insan ve teknik altyapı yetersizliği bahaneleriyle geri çevrilmektedir[851].

Bu bağlamda özel eğitimli teknik personelin bilişim alanındaki baş döndürücü gelişmelere bağlı olarak adli bilişim süreci ile ilgili sürekli olarak eğitimlerinin yenilenmesi büyük önem taşımaktadır. Özellikle, türü ve kapsamı genişleyen bilişim suçlarına ve faillerine ulaşmada, bilinen metotların kısa sürede güncelliğini yitirmesi, teknik personelin eğitimlerinin sürekli olarak yenilenmesini gerekli kılmaktadır[852].

Diğer taraftan bilgisayar ve ağ sistemlerinin incelenmesi hususunda hâkim ve savcıların geniş yetkilere sahip olmalarına karşın teknik anlamda yeterli donanıma sahip olmamaları ve onları bu konuda yönlendirecek standartların bulunmaması nedeniyle kimi zaman ehliyetsiz kişilerin bilirkişi olarak atandıkları görülmektedir[853]. Hatta bilgisayar mühendisi olmasına rağmen ne tür bir inceleme yaptığının farkında olmayan, kendisine sorulan sorular haricinde raporunu ilgisiz konularla ve gereksiz teknik terimlerle dolduran uzman bilirkişilerin de var olduğu görülmektedir[854].

Ülkemizde, diğer pek çok ülke uygulamasına benzer şekilde, bilirkişi olarak atanan kişilerin bilimsel ehliyetlerini ön şart olarak ortaya koyacak ve takip edecek bir mevzuatın bulunmadığı görülmektedir[855]. Bununla birlikte "Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı"'nın 35. maddesinde "adli bilişim uzmanı" düzenlenmişti. Buna göre; bu tasarı kapsamına giren suçlarla ilgili olarak sadece adli bilişim uzmanı yetki belgesine sahip olanlar bilirkişilik yapabilecek, adli bilişim uzmanlığı ve adli bilişim yetki belgesine ilişkin esas ve usuller yönetmelikte belirlenecek ve adli bilişim uzmanları hakkında Ceza Muhakemesi Kanunu'nun

[851] Ahi, "Adli Bilişim Nedir ?", http://www.bilisimhukuk.com/2009/07/adli-bilisim-nedir/ (04 Mayıs 2014); Özbey, s. 107.

[852] Karagülmez, Bilişim Suçlarında Delil Toplamayı Etkileyen Başlıca Konular, s. 33.

[853] Cevat Özel ve M. Gökhan Ahi, "Bilişim Suçlarında Usul ve Sorumluluk Sistemi Üzerine Öneriler", http://www.turkhukuksitesi.com/makale_179.htm (6 Eylül 2014).

[854] Ahi, "Adli Bilişim Nedir ?", http://www.bilisimhukuk.com/2009/07/adli-bilisim-nedir/ (04 Mayıs 2014); Özbey, s. 107.

[855] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 121.

bilirkişiliğe ilişkin hükümleri uygulanacaktı. Ancak bu zamana kadar söz konusu tasarı kanunlaştırılamamış ve uygulama CMK'nın bilirkişiliğe ilişkin ilgili maddeleri uyarınca gelişmiştir.

Öğretide "Adli Tıp Kurumu Kanunu"nda köklü değişikliğe gidilerek Kanun'un adının "Adli Bilirkişilik Kurumu Kanunu" olarak değiştirilmesi, önceleri sadece tıp alanında bilirkişilik ihtiyacını karşılamak için kurulan ve daha sonra morg, fizik, kimya, gözlem, trafik, biyoloji vb. ihtisas daireleri eklenerek sadece tıbbi alanda bilirkişilik yapma fonksiyonundan hızla uzaklaşan kuruma, elektronik delilin sağlıklı bir şekilde toplanması amacıyla adli bilişimi bütün boyutlarıyla içine alacak "Adli Bilişim İhtisas Kurulu"nun kurulması, kurulacak bu birimde çalışacak olan adli bilişim uzmanlarının belli bir sertifikasyon programına tabi tutularak adli bilişim alanında gerekli eğitimlerin verilmesi, ayrıca yazılım, donanım, veri tabanı yönetimi, veri kurtarma ve network yönetimi gibi işlerden anlayan uzman kişiler bulunması gerektiği vurgulanmıştır[856].

Bu bakımdan, eğitimli teknik personelin uygun bir bünyede teşkilatlandırılması, bu konuda Adli Tıp Kurumu ve hatta mümkün olduğu takdirde üniversiteler bünyesinde "Adli Bilişim İhtisas Kurulu" tarzında bilirkişilik kurumlarının kurulması gerekmektedir[857]. Zira bilirkişilik alanında adli bilişim uzmanları ile diğer bilgisayar uzmanları arasında yaklaşım farklılıkları ortaya çıkmaktadır. Adli bilişim uzmanları kendi alanlarıyla ilgili hukuki bilgiye sahip olup dünyaca kabul gören bir takım adli bilişim standartlarına vâkıftırlar. Bu standartlara vâkıf olma bir takım sertifikalarla kanıtlanmaktadır. Bilirkişi seçiminde bu sertifikaların dikkate alınması adli bilişim sürecinin başarılı bir şekilde işletilmesinde yardımcı olacaktır[858].

Günümüzde soruşturma organları ile kolluk güçlerinin karşılaştığı en büyük sorunlardan birisi bilişim sistemlerinin veri saklama kapasitelerinin büyüklüğüdür. Delil olarak kullanılacak elektronik veri, sistemde yer alan verinin yüzde, binde veya onbinde biri seviyesindedir. Bu bakımdan, bilişim sistemlerinde yer alan her türlü bilginin değil

[856] Yetim, Dijital Kanıt Araştırma Yöntemleri, s. 1202.

[857] Gökhan Ahi, "Bilişim Suçlarında Usul ve Sorumluluk", **Bilişim Hukuku**, Mete Tevetoğlu (drl.), İstanbul: Kadir Has Üniversitesi Yayınları, 2006, s. 102; Karagülmez, Bilişim Suçlarında Delil Toplamayı Etkileyen Başlıca Konular, s. 33.

[858] Ünal, s. 141.

ancak yargılamaya konu olayı aydınlatacak, fail veya failleri belirleyecek, bir olayı doğrulayacak veya yanlışlığını ispat edecek verinin, özetle delil değeri olan verinin elde edilmeye çalışılması gerekmektedir ki bu durum çok da kolay bir husus değildir[859].

Bu bakımdan adli bilişim uzmanlarının yer imkânları, olay yerinde bağımsız fiziksel kopyalama cihazları gibi teknik cihaz sayıları ve en önemlisi yetişmiş personel sayısı artırılmalı, uzmanlaşmış yöneticiler eşliğinde çalışmalarını yapmaları sağlanmalıdır. Ayrıca sadece adli bilişim alanına hizmet edebilecek tam donanımlı ve yer sıkıntısı olmayan inceleme laboratuvarları kurulmalıdır [860] . Bu bağlamda adli bilişim uzmanlarının adli olayların çözümünde istifade edecekleri son derece ileri düzey laboratuvarların kurulması gerekmektedir. Elektronik delilin niteliği itibariyle alınan imaj ve yedeklerin uzun süre boyunca saklanması gerekeceğinden bu ihtiyacı giderici mahiyette yedekleme üniteleri bulunmalıdır[861].

Göz ardı edilmemesi gereken bir husus da şudur ki; suçluların elektronik delillerle ilgili kaygıları bulunmakta ve bu kaygılarından kurtulmak için bilişim sistemlerini tahrif etmeye gayret göstermektedirler. Bu nedenle adli bilişim sürecinde görev alan uygulayıcıların adli bilişim süreciyle ilgili o zamana kadar yapılan çalışmalara her soruşturma bakımından kolayca güvenmemeleri, yeni oluşacak koşullara ilişkin çalışmaları ve bunların sonuçlarını da yakından takip etmeleri gerekmektedir.

Adli bilişim alanındaki bu baş döndürücü gelişmeleri takip edebilmek için özellikle üniversitelerde bilişim ve bilgisayar derslerinin yanı sıra hukukçuların da bir araya gelerek ortak çalışmalar düzenlemeleri gerekmektedir. Özellikle adli bilişimle ilgili konferans, panel ve seminerler düzenlenerek hukukçuların ve bilişim uzmanlarının katılımı sağlanmalıdır. Bu tür etkinliklerin düzenlenmesiyle adli bilişim süreci daha iyi kavranacak ve bilişim şuuru geliştirilerek bilişim suçlarıyla mücadelede etkinlik sağlanacaktır[862].

---

[859] Değirmenci, Ceza Yargılamasında Sayısal (Dijital) Delil, s. 62.

[860] Çakır ve Sert, s. 161.

[861] Yetim, Dijital Kanıt Araştırma Yöntemleri, s. 1202-1203.

[862] Ünal, s. 153-154.

Nitekim adli bilişim alanında en ileri ülkelerden biri olan ABD, ceza yargılamasında bilişim sistemlerine yönelik arama ve elkoyma tedbirlerini uygularken adli bilişim sürecini belirli kıstaslara uyarak icra etmektedir. Bununla birlikte ABD'deki adli bilişim birimleri bu kriterleri her zaman gözden geçirerek gelişen teknoloji ve yeni suç tiplerine göre güncellemekte ve bu kriterlerin belirlendiği sempozyum ve konferanslara ev sahipliği yapmaktadır. Bu bağlamda adli bilişim sürecinde, elektronik delilin güvenilirliği ve kabul edilebilirliği konularında yaygın ve etkin olabilecek standartları belirleme yönündeki çalışmalar bu ülkede devam etmektedir[863].

Soruşturma görevlileri için özellikle adli bilişim faaliyetlerini kapsayan soruşturmalarda, yol gösterici olması amacıyla hazırlanan eğitici kaynaklar temin edilmelidir. Gerçekten de, savcılar ve kolluk görevlilerinin soruşturma faaliyetinde hangi hususlara dikkat etmeleri, ne şekilde bir soruşturma yürütmeleri gerektiğini açıklayan ve pratik eğitimlerle de desteklenen kaynaklar hazırlanması son derece faydalı olacaktır[864].

Bu bağlamda Avrupa Birliği ve Avrupa Konseyi ortak projesi olan "Türk Ceza Adalet Sisteminin Etkinliğinin Geliştirilmesi Projesi" kapsamında Türkiye Adalet Akademisinin eğitim müfredatına destek verilmesi ve geliştirilmesi amacıyla yerli ve yabancı uygulayıcı ve akademisyenlerin de katıldığı uzman toplantıları sonucunda oluşturulan "Bilişim Suçları Eğitim Modülü" kitabının uygulayıcıların bilişim suçlarıyla mücadelede gerekli soruşturma teknikleri ve elektronik delil elde etme yöntemlerini öğrenmeleri ve kendilerini bu konularda geliştirmeleri hususunda yararlı bir kaynak olduğu kanaatindeyiz.

[863] Ünal, s. 72.

[864] Uçkan ve Beceni, s. 424-425.

SONUÇ

Ceza yargılamasının amacı maddi gerçeğin ortaya çıkartılması olup bu amaç meydana gelen olay ile söz konusu olayı gerçekleştiren kişi arasındaki bağın ispatıyla sağlanmaktadır. Bu ispat ameliyesi ise soruşturma ve kovuşturma aşamalarında elde edilen ve davaya konu olay hakkında karar verecek olan hâkimin vicdani kanaate ulaşmasına aracılık eden delillerle gerçekleştirilir.

Bununla birlikte olayın ispatını sağlayacak delillerin belli özelliklere sahip olmaları gerekir. Bu anlamda delilin gerçekçi olması, akla ve mantığa uygun olması, erişilebilir olması, geçmişte yaşanmış olayı temsil edici olması, davanın bütün taraflarınca bilinir ve tartışılabilir ölçüde müşterek olması ve en önemlisi de hukuka uygun olması gerekmektedir.

Masumiyet (suçsuzluk) karinesinin işlerliğini sağlama fonksiyonu bulunan deliller üç grupta incelenmektedir. Bunlardan birincisi beyan delilidir. Buna göre soruşturma veya kovuşturmaya konu olay hakkında bilgisi olan kişilerin yazılı ve sözlü olarak ifade vermeleri beyan delilini oluşturmaktadır. İkinci delil türü olan belge delili, insanlar tarafından oluşturulan ve somut bir olayı temsil eden ispat aracını ifade etmektedir. Belge delili yazılı belge, şekil tespit eden belge, ses ve görüntü tespit eden belge ve bilişim verisi şeklinde belge olmak üzere dört biçimde karşımıza çıkmaktadır. Üçüncü delil türü olan belirti delili ise ispata konu olayın dolaylı olarak ispatına yardımcı olan ve olaydan geriye kalan her türlü iz ve esere denir. Bu bağlamda; tezimizin konusunu teşkil eden elektronik delilin bilişim verisi şeklindeki belge delillerinden olduğu sonucuna varılmıştır.

CMK'nın 217/1 maddesine göre hâkim huzuruna gelen delilleri vicdani kanaatine göre serbestçe takdir edecektir. Bu hüküm iç hukukumuzca da kabul edilen delil serbestîsinin bir tezahürüdür. Ancak CMK'nın 217/2 maddesinde delil serbestîsine sınır getirilmiş ve yüklenen suçun ancak hukuka uygun şekilde elde edilmiş her türlü delille ispat edilebileceği hükme bağlanmıştır. Aynı doğrultuda CMK'nın 206/2-a maddesinde kanuna aykırı olarak elde edilen delillerin duruşmada ortaya konamayacağı, Anayasa'nın 38/6 maddesinde de kanuna aykırı elde edilmiş bulguların delil olarak

kabul edilmeyeceği hükme bağlanmıştır. Bu anlamda kural olarak hukuka aykırı delillerin yargılamada ispat aracı olarak kullanılmaması gerekmektedir.

Bununla birlikte hukuka aykırı delillerin yargılamada delil olarak kullanılıp kullanılmayacağına ilişkin üç farklı yaklaşım bulunmaktadır. Birincisi kesin kabul yaklaşımıdır ki; modern hukukta çok da uygulanırlığı bulunmayan bu yaklaşıma göre yargılamaya konu olayın aydınlatılmasına fayda sağlayacak her delilin nasıl elde edildiğine bakılmaksızın kullanılabileceği savunulmaktadır. İkincisi yaklaşım olan kesin ret yaklaşımına göre; hukuka uygun olmayan yöntemlerle elde edilmiş delilin hiçbir şekilde yargılamada kullanılamayacağı savunulmaktadır. Üçüncü yaklaşım olan esnek yaklaşım ise; bu konuda hâkime takdir yetkisi veren, delilin kabul edilebilirliği hususunda sabit bir kural koymak yerine hâkimin her davada birey ve toplumun yarışan menfaatlerini göz önüne alarak delili değerlendirmesi gerektiği görüşünü savunmaktadır.

Türk hukuk sisteminde hukuka aykırı delillerin yargılamada değerlendirilmeye alınıp alınmayacağı hususunda kesin ret yaklaşımının mı yoksa esnek yaklaşımın mı benimsendiği hususunda faklı görüşler ileri sürülmektedir. Bizim bu konuda benimsediğimiz görüş esasen Yargıtay Ceza Genel Kurulu'nun *"ele geçirilen delillerin yalnızca bazı şekli kurallara uyulmadığından bahisle hukuka aykırı olarak elde edilmiş sayılamayacağı ve mahkûmiyet hükmüne dayanak teşkil edilmemelerinin kabul edilemeyeceği"* yönündeki Anayasa Mahkemesi tarafından da benimsenen yaklaşım tarzıdır. Bu yaklaşım tarzını ille de kesin ret veya esnek yaklaşımdan birisi içinde değerlendirmek gerekecekse esnek yaklaşım tarzının benimsenmesi gerektiği kanaatindeyiz.

Türk hukukunda zehirli ağacın meyveleri olarak da tanımlanan hukuka aykırı delillerin uzak etkisi meselesi de geniş kapsamda tartışılmıştır. Delil yasaklarının uzak etkisi konusunda Anayasa'da ve Ceza Muhakemesi Kanunu'nda hâkimin takdir yetkisini ortadan kaldıran sınırlayıcı bir hüküm bulunmaması karşısında bu hususun somut olayın özelliklerine göre hâkim tarafından değerlendirilmesi, bununla birlikte işkence, insanlık dışı veya onur kırıcı davranış sonucu yapılan itiraflar üzerine elde edilen delillerin ise istisna tutularak yargılamada değerlendirmeye alınmaması gerektiği sonucuna varılmıştır. Nitekim Yargıtay Ceza Genel Kurulu da bir kararında hukuka aykırı

aramada elde edilen maddi delillerin değerlendirmeye alınamayacağı ve fakat bunların dışında kalan diğer delillerin, bu bağlamda sanık hakkındaki ihbar ile sanığın mevcut ikrarının somut olayda mahkûmiyet için yeterli delil olarak kabul edilebileceğini hükme bağlayarak hukuka aykırı delillerin uzak etkisini kabul etmemiştir.

Birinci bölümde üzerinde tartıştığımız konulardan birisi de hukuka aykırı delillerin dosyadan çıkartılıp çıkartılmayacağı hususu olmuştur. Öğretide hukuka aykırı delillerin dosyadan çıkartılması gerektiği ya da dosyadan çıkartılmasa da bu tür delillerin hukuka aykırılığının tespiti hususunda "delil yasakları davası" adında bir tali davanın açılarak delilin gerçekten hukuka aykırı olup olmadığının denetlenmesi gerektiği ileri sürülmüş ise de CMK'da hukuka aykırı delillerin dosyadan çıkartılmasına ilişkin herhangi bir hüküm olmadığı gibi yargılama devam ediyorken bir ara kararla delillerin hukuka aykırılığına karar verilmesi de mümkün görünmemektedir. Ayrıca CMK m. 206, 230/1-b, 289 ve 302/3-4 hükümleri de hukuka aykırı şekilde elde edilmiş delillerin dosyada muhafaza edilmesi gerektiğine delalet etmektedir. Bu bakımdan hukuka aykırı şekilde elde edildiği düşünülen delillerin dosyadan çıkartılmasının hukuk sistemimiz bakımından mümkün olmadığı kanaatindeyiz.

Tezimizin birinci bölümde ceza yargılamasında deliller genel olarak ele alınmasından sonra elektronik delil ve kullanıldıkları suç tipleri konusu incelenmiştir. Esasen tarafımızca elektronik delil olarak tanımlanan kavram öğretide dijital delil veya sayısal delil olarak da tanımlanmıştır. Sayısal delil, dijital delil kavramının Türkçe ifade ediliş biçimi olup aralarında anlam farkı bulunmamaktadır. Elektronik delil kavramı ise hem elektronik cihazı hem de bu cihaz içerisinde bulunan dijital (sayısal) verileri kapsaması ve dijital (sayısal) delil ifadesine göre daha üst bir anlamı içermesi nedeni ile tarafımızca benimsenmiş ve kullanılmıştır.

Günümüz teknoloji dünyasında haberleşmeden alış verişe kadar hemen her alanda bilişim sistemleri kullanılmaktadır. Bu durumun doğal yansıması olarak da bilişim sistemleri işlenen suçların kimi zaman aracı kimi zaman ise konusu durumunda bulunmaktadırlar. Bu durum, bilişim suçları gibi daha önce bilinmeyen yeni suç tiplerinin ortaya çıkmasına neden olduğu gibi birçok klasik suç tipinin bilişim sistemleriyle işlenir biçimde güncellenmesine de neden olmuştur. Bu bakımdan elektronik delil, hem bilişim suçlarının hem de bilişim sistemleri aracılığıyla işlenen

dolandırıcılık, hırsızlık, hakaret, tehdit gibi birçok suç tipinin soruşturulması ve suç faillerinin tespiti bakımından büyük öneme sahiptir. Hatta bazen kasten öldürme olayını aydınlatacak delillerin bilişim sistemlerinde saklanması durumunda olduğu gibi tamamen gerçek dünyada meydana gelen bir olayın aydınlatılmasında da hayati fonksiyon icra edebilmektedir.

Elektronik delil kendine mahsus özelliklere sahiptir. Elektronik delilin en belirgin özelliklerinden birisi DNA ve parmak izi gibi gizli yapıya sahip bir delil türü olmasıdır. Elektronik delilin anlaşılabilmesi bazı alet ve cihazlarla nicel bir gözlem yapmayı gerektirmektedir. Diğer bir önemli özelliği ise elektronik delilin hassas bir yapıya sahip olmaları ve bu nedenle kolay bir şekilde değişikliğe ve tahrifata maruz kalabilmeleridir.

Elektronik delilin kendine mahsus yapıları bazı sorunlarla karşılaşılmasına neden olabilmektedir. Bu bağlamda; elektronik delilin dağınık ve kaygan yapıya sahip olması kolay elde edilmesini engellemektedir. Elektronik delilin soyut verilerden oluşması bu verilerden kesin bir sonuç çıkartılmasını kimi zaman zorlaştırmaktadır. Elektronik delilin muhafazasının zor olması bütünlüğünün sağlanması bakımından sorunlar yaşatmaktadır. Elektronik delilin kasten veya kazaen değiştirilebilir olma niteliği onun güvenilir bir delil türü olması hususlarında itirazlara neden olabilmektedir.

Bununla birlikte elektronik delilin bazı özellikleri de yukarıda belirtilen kaygıları hafifletir niteliktedir. Buna göre; elektronik delilin kolay çoğaltılabilmeleri ve birebir kopya üzerinde inceleme yapılması uygulaması orijinal delilin zarar görme olasılığını önlemektedir. Elektronik delilin tamamen yok olması zor ya da imkânsız bir durumdur. Elektronik delilin silinmesi durumunda da çoğu zaman geri getirmek mümkündür. Elektronik delilin değiştirilmesi ve tahrif edilmesi durumunda da orijinal delil ile kıyaslama yapmak suretiyle bu durumun tespiti mümkündür.

Bu bakımdan elektronik delilin geçerliliği hukuken ve teknolojik olarak geçerliliğinin denetlenmesine bağlıdır. Bu anlamda elektronik delil öncelikli olarak fiziksel delillerde de bulunması gereken gerçeklik, akılcılık, erişebilirlik, temsil edicilik, müştereklik ve hukuka uygunluk şartlarını taşıması gerekir. Bundan sonda ise elektronik delilin yapısı gereği teknolojik denetiminin yapılması gerekir. Buna göre; elektronik delilin

bütünlüğü, doğrulanması, inkâr edilememesi, doğruluğu ve daha sonra ele alınabilirliği noktasındaki teknolojik geçerlilik ilkelerine uygun olması gerekir.

Tezimiz kapsamında elektronik delilin hukuken ve teknolojik geçerlilik şartları açıklandıktan sonra ceza yargılamasında kabul edilebilirliği üzerinde durulmuştur. Mukayeseli hukuk bakımından ABD, İngiltere, Almanya ve Fransa örneklerinde olduğu üzere elektronik delilin delil serbestîsi kapsamında ceza yargılamasında delil olarak kullanılabileceği kabul edilmiştir.

Tez kapsamında Türk hukukunda elektronik delilin kabul edilirliği konusu daha detaylı incelenmiştir. Buna göre; Türk hukuk sistemi öğreti ve uygulamasında elektronik delilin ceza yargılamasında delil olarak kullanılabileceğine ilişkin genel bir kabul bulunmaktadır. Bununla birlikte esas tartışma konusu olan nokta elektronik delilin tek başına mahkûmiyet kararı vermek için yeterli olup olmadığı hususudur.

Öğretide elektronik delilin kolay değişebilir ve bozulabilir yapılarından dolayı tek başlarına mahkûmiyet kararı için yeterli bir delil türü olmadıkları, bu nedenle başka delillerle desteklenmesi gerektiği yaygın olarak dile getirilmektedir. Buna karşın bizim vardığımız sonuca göre; elektronik delilin başkaca delil olmadan mahkûmiyet hükmü için yeterli kuvvette olmadığı ve bu nedenle başka delillerle desteklenmesi gerektiğine ilişkin yasal bir zorunluluk bulunmamaktadır. Özellikle bilişim suçlarında fiziksel delillere müracaat etme olanağının bulunmadığı hallerde böyle bir zorunluluk getirme bilişim suçlarının sonuçlandırılması bakımından büyük sorunlara neden olacaktır. Bu bakımdan hukuki ve teknolojik geçerliliği konusunda tereddüt bulunmayan hallerde elektronik delilin tek başına mahkûmiyet hükmü kurmak için yeterli kuvvette bir delil türü olduğu kanaatindeyiz.

Bununla birlikte elektronik delilin tek başına kullanılmasına ilişkin yasal bir zorunluluğun bulunmamasına karşın yapılarından kaynaklanan hassasiyet nedeniyle çoğu zaman savunma tarafından elektronik delilin hukuki ve teknolojik geçerliliğine ilişkin itirazda bulunulduğu, bu itirazların yargılama sürecinde oluşturacağı şüpheyi yenmek adına da sair delillerle bu itirazların karşılanması zorunluluğunun bulunduğu, dolayısıyla da yasal olarak olmasa da elektronik delilin yapıları gereği çoğu zaman

elektronik delilin kullanımının diğer delillerle birlikte gerçekleştiği de fiili bir gerçek olarak ortaya çıkmaktadır.

Elektronik delilin geçerliliğinin kabulü onun hukuken ve teknolojik olarak geçerliliğinin denetlenmesine bağlıdır. Elektronik delilin hukuken geçerliliğinin denetlenmesi ise elektronik delilin hukuka uygun usul işlemleri sonucunda elde edilmiş olmasıyla ilgilidir. Bu bakımdan biz de ikinci ve üçüncü bölümlerde elektronik delil elde etmek amacıyla bilişim sistemlerinde gerçekleştirilen arama ve elkoyma koruma tedbirlerini mukayeseli hukuk ve iç hukukumuz açısından öğretideki görüşler ve mahkeme içtihatları doğrultusunda inceledik.

Tezimizin ikinci bölümünde incelenen mukayeseli hukukta bilişim sistemlerinde yapılan arama ve elkoyma tedbirleri bakımından en önemli düzenleme ülkemiz için de bağlayıcılığı bulunan Avrupa Konseyi Siber Suç Sözleşmesi'dir. Sözleşmenin 14-21. maddeleri arasında usul hükümleri düzenlenmiştir. Arama ve elkoyma ile ilgili düzenleme ise Sözleşmenin 19. maddesinde bulunmaktadır. Bu madde uyarınca taraf ülkelerin, yetkili makamlarını kendi ulusal sınırları içinde, bir bilgisayar sisteminde veya sistemin bir parçasında ya da veri saklama cihazlarında arama yapma veya benzer şekilde erişim yapma konusunda yetkilendirmeleri gerekmektedir.

Tez kapsamında Avrupa Konseyi Siber Suç Sözleşmesine taraf olan ülkelerden ABD, İngiltere, Almanya, Fransa ve İtalya hukuk sistemlerinin bilişim sistemlerinde yapılacak arama ve elkoyma tedbirini ne şekilde yerine getirdikleri hususu üzerinde durulmuştur. Bu kapsamda İngiliz Polis ve Suç Delili Kanunu (PACE) ve Soruşturma Yetkilerinin Düzenlenmesi Kanunu (RIPA) ile Fransız Ceza Muhakemesi Kanunu'nda bulunan düzenlemelerin saklanan bilgisayar verilerinin aranması ve bunlara elkonulmasına ilişkin Avrupa Konseyi Siber Suç Sözleşmesi'nin 19. maddesindeki düzenlemeye uygun iç hukuk düzenlemeleri olduğu görülmüştür.

Bununla birlikte ABD, Almanya ve İtalya gibi ülkeler Avrupa Konseyi Siber Suç Sözleşmesi'ne taraf olmakla birlikte iç hukuklarında elektronik verilerin aranması ve elkonulması hususunda Sözleşmenin 19. maddesi anlamında özel düzenlemeler yapma yoluna gitmeyerek arama ve elkoyma tedbirlerine ilişkin genel hükümler ve mahkeme içtihatları çerçevesinde meselenin çözümünü benimsemişlerdir.

Tezimizin üçüncü bölümünde Türk hukukunda bilişim sistemleri üzerinde arama ve elkoyma konusu işlenmiştir. Bu bağlamda özellikle Ceza Muhakemesi Kanunu'nun 134. maddesinde düzenlenen koruma tedbiri ile bu yasa maddesiyle bağlantılı olan Adli ve Önleme Aramaları Yönetmeliği'nin 9. maddesi ve Suç Eşyası Yönetmeliği'nin 17. maddesi hükümleri incelenmiştir. Son olarak ise uzaktan erişimle arama ve bulut bilişimde arama konularına da kısaca değinilmiştir.

Elektronik delilin elde edilmesine ilişkin koruma tedbirleri, özel bilgi kullanımını gerektiren ve hızlı işleyen bir usul işlemidir. Diğer taraftan bu tedbirlerin kullanılması sonucunda elde edilen verilerin ceza yargılamasında delil olarak kullanılmalarını sağlayacak ve temel hak ve özgürlükleri korumaya yönelik garantilerle donatılmış özel yasal yetkileri de içermesi gerekmektedir. Bu bakımdan bu tedbirlerin uygulanmasına yönelik yasal düzenlemelerde hem elektronik delilin kullanıldığı suçlarla mücadele imkânını sağlayacak hem de bunu yaparken kişilerin temel hak ve özgürlüklerini müdahale niteliği taşıyan bu tedbirlerin uygulamasını oranlılık ilkesine bağlı kalarak gerçekleşmesini sağlayacak yasal düzenlemelere ihtiyaç duyulmaktadır.

Türk hukukunda elektronik delilin elde edilmesine yönelik usul işlemleri Ceza Muhakemesi Kanunu'nda yapılan tek maddelik bir yasa hükmüyle düzenlenmeye çalışılmıştır. Tez çalışmamız kapsamında incelediğimiz ve CMK'nın 134. maddesinde ifadesini bulan bilgisayar, bilgisayar programları ve bilgisayar kütüklerinde arama, kopyalama ve elkoyma koruma tedbirine ilişkin hükmün, en önemli temel hak ve özgürlüklerden olan özel hayatın gizliliği ve haberleşmenin gizliliği ile düşünceyi açıklama ve yayma özgürlüğünün korunması hakları bakımından Avrupa İnsan Hakları Sözleşmesi'nin 8/2 ve 10/2 maddeleri ile Anayasa'nın 20/2, 22/2 ve 26/2 maddelerinde belirtilen istisna hallerde ve oranlılık ilkesine uygun şekilde uygulanabilir olduğu kanaatine varılmıştır. Bununla birlikte tedbirin uygulanması sırasında yasa hükümlerinin doğru yorumlanmaması veya kolluğun yanlış tutumundan kaynaklı ihlallerin gündeme geldiği de bir gerçektir.

Özellikle bilgisayarın tüm niteliklerine sahip olması nedeniyle bilgisayar tanımı içerisinde kabul edilmesi gereken ve fakat uygulamada bilgisayar olarak tanımlanmayan cep telefonu, cep bilgisayarı ve elektronik veri barındıran birçok cihazın CMK m. 134

hükmü yerine CMK m. 116 ve 123 hükümlerine göre arama ve elkoyma işlemlerine tabi tutulması temel hak ve özgürlükler bakımından ihlallere neden olabilmektedir.

Bu bakımdan yasa hükmünün uygulama alanının bilişim sistemleri ve bağlı donanımlarını kapsayacak ve de gelişen teknolojinin gerisinde kalmayacak genel bir çerçevede belirlenmesi hatta bir adım daha ileri gidilerek elektronik delil, bilişim suçları, adli bilişim, bilişim sistemlerinde uygulanacak koruma tedbirleri gibi bilişim hukukuna ilişkin hususların -medeni yargılama hukukuna bakan yönleri de kapsayacak biçimde- ayrı bir kanunda ve tereddütlere mahal vermeyecek biçimde yeniden düzenlenmesi, bu düzenlemeler yapılıncaya kadar ise madde metnindeki kavramların bilişim sistemlerinin genelini kapsayacak biçimde yorumlanarak uygulamanın buna göre tesis edilmesi gerektiği sonucuna varılmıştır.

Diğer taraftan CMK'nın 134. maddesinde düzenlenen koruma tedbirinin büyük ölçüde Avrupa Konseyi Siber Suç Sözleşmesi'nin 19. maddesindeki düzenlemeye uygunluk gösterdiği belirtilmelidir. Bununla birlikte Sözleşmede yer alan suç unsuru veya suç aracı olan verilerin erişilemez veya kullanılamaz hale getirilmesi ve hatta kopyaları alındıktan sonra silinmesine ilişkin hükmün CMK'nın 134. maddesinde yer verilmeyerek maddede sanki bu tür verilerin de şüpheliye iade edilebileceği anlamını taşıyan ifadelere yer verilmesi, söz konusu yasal düzenleme için getirebilecek en önemli eleştirilerden birini teşkil etmektedir. Bu nedenle mevcut eksikliğin yasal bir düzenlemeyle bir an önce giderilmesi gerekmektedir.

Bununla birlikte bu konudaki sorunu çözecek yasal bir düzenleme yapılıncaya kadar Avrupa Konseyi Siber Suç Sözleşmesi'nin 19/3-d maddesi yol gösterici olarak benimsenmelidir. Buna göre, Sözleşmede belirtilen bu tip verileri barındıran elektronik medyadaki verilerin kopyaları alındıktan sonra silinmesi sonrasında elektronik medyanın şüpheliye iade edilmesi hususunu etkin bir çözüm yolu olarak benimsememekle birlikte verilerin erişilemez veya kullanılamaz hale getirilmesi kapsamında söz konusu verilerin bulunduğu medyaların şüpheliye iade edilmemesi ve şartları varsa yargılama sonrasında müsaderesine karar verilmesi gerektiği kanaatindeyiz.

Diğer taraftan hakkında tedbir uygulanan şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilip bu kararın kesinleştiği hallerde tedbir sonucunda elde edilen verilerin soruşturma dosyasından ve tüm kayıtlardan çıkartılarak yok edilmesi konusunda herhangi bir düzenlemenin bulunmaması da dikkat çeken bir eksiklik olup bu eksikliğin yasal düzenleme ile çözülmesi gerektiği, bu yönde düzenleme yapılıncaya kadar ise telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbiriyle ilgili CMK'nın 137. maddesinde belirtilen hükmün CMK'nın 134. maddesi uyarınca uygulanan tedbir bakımından kıyasen uygulanması gerektiği kanaatindeyiz. Buna göre; şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi halinde, bilişim sistemlerinden elde edilen veriler, Cumhuriyet savcısının denetimi altında yok edilebilecektir.

CMK'nın 134. maddesinde eksik düzenlenen veya hiç düzenlenmeyen bazı hususlar Adli ve Önleme Arama Yönetmeliğinin 17. ve Suç Eşyası Yönetmeliğinin 9. maddelerinde giderilmeye çalışılmış ise de bu eksikliklerin tam manasıyla giderilebildiğini söylemek çok da mümkün olmamıştır. Kaldı ki; özellikle bilişim suçlarının etkin şekilde soruşturulmasında birinci derece önemli olan ve temel hak ve özgürlükleri doğrudan ilgilendiren bir yasa hükmündeki eksikliklerin yönetmelikle giderilmeye çalışılması da doğru değildir. Bu bakımdan mevcut eksikliklerin de kapsamlı bir yasal değişiklikle giderilmesi yerinde olacaktır.

Ayrıca CMK'nın 134. maddesinde düzenlenen koruma tedbirinin uzaktan erişimle arama için uygulanamayacağı düşüncesindeyiz. Bu tedbirin bulut bilişim üzerinde uygulanıp uygulanamayacağı hususu ile ilgili olarak ise; özel ve dar kapsamlı özel bulut bilişim ile servis sağlayıcısı yurt içinde bulunan kamusal bulut bilişim hakkında söz konusu koruma tedbirinin uygulanabileceği, servis sağlayıcısı yurt dışında bulunan kamusal bulut bilişim hakkında ise adli yardımlaşma ilkeleri çerçevesinde hareket edilmesi gerektiği sonucuna varılmıştır.

Son olarak tezimizin dördüncü bölümünde ise adli bilişim konusu incelenmiştir. Yukarıda da değinildiği üzere elektronik delilin geçerliliğinin kabulü onun hukuken ve teknolojik olarak geçerliliğinin denetlenmesine bağlıdır. Elektronik delilin hukuken geçerliliğinin denetlenmesi elektronik delilin hukuka uygun usul işlemleri ile elde

edilmiş olmasıyla ilgiliyken teknolojik olarak geçerliliğinin denetlenmesi ise büyük ölçüde adli bilişim sürecinin işlerliği ile ilgilidir.

Gerçekten de, elektronik medyalar üzerinde bulunan suça ilişkin elektronik delilin bozulmadan ve zarar görmeden anlaşılabilir bir şekilde yargı makamları önüne sunulmasını sağlayan ve bilimsel teknik prensiplerin uygulandığı bir delil inceleme sürecinin bütünü olarak da tanımlanan adli bilişim, esasen elektronik delilin teknolojik olarak geçerliliğini sağlamaya yönelik bir süreç olarak da dikkat çekmektedir. Bu sürecin en belirgin iki unsuru adli bilişim uzmanı ile laboratuvar ortamıdır.

Öğretide farklı ayrım ve tanımlamalar olmakla birlikte biz adli bilişimi "elektronik delilin toplanması ve muhafazası", "elektronik delilin incelenmesi", "elektronik delilin analizi" ve "elektronik delilin raporlanması ve sunumu" olmak üzere dört aşamada inceledik.

Elektronik delilin toplanması ve muhafazası aşaması adli bilişimin başlangıç aşaması olup delil bütünlüğünün sağlanması bakımından çok önemli bir safhadır. Bu bakımdan elektronik delile ilk müdahale edecek kişinin yeterliliği, müdahale sırasında uyulması gereken kurallara bağlılık, toplanan delillerin paketlenmesi, nakli ve muhafazasında gösterilmesi gereken hassasiyet düzeyi elektronik delilin bütün halde incelenmesi, analizi ve raporlanarak yargı makamlarının huzuruna getirilmesinde belirleyici olmaktadır. Bu bakımdan tez kapsamında bu kural ve kaideler üzerinde ayrıntılı biçimde durulmuştur.

Bununla birlikte bu ilk aşamada elektronik delil üzerinde uygulanması gereken bazı teknik işlemler bulunmaktadır ki bu işlemlerin elektronik delilin bütünlüğüne yönelik savunma tarafından ortaya atılması muhtemel iddiaların bertaraf edilmesi bakımından muhakkak yerine getirilmesi gerekmektedir.

Bunlardan birisi birebir kopyalama (imaj alma) işlemidir. Birebir kopyalama işlemi, elektronik medyada bulunan tüm verilerin mevcut, silinmiş ve gizlenmiş halleriyle bir bütün olarak kopyalanması işlemini ifade etmektedir. Bu bağlamda birebir kopyası alınmış bir verinin aslıyla farkı bulunmamakta, bu durumda elektronik veri üzerinde

yapılması gereken inceleme ve analiz işlemlerinin bu birebir kopya üzerinde yapılması ve orijinal verinin bu işlemler sırasında zarar görmemesi sağlanmaktadır.

Bir diğer işlem ise orijinal veya birebir kopyası alınmış verinin hash (veri bütünlük) değerinin hesaplanmasıdır. Hash değeri elektronik veri üzerinde yapılan matematiksel algoritma ile oluşturulan tek taraflı bir değerdir. Elektronik verinin elde edilmesinden sonra alınan ilk hash değeri ile mahkeme huzuruna sunulan ve bilirkişi raporunda belirtilen hash değerinin aynı olması bu verinin elde edilmesinden sonra herhangi bir değişikliğe uğramadığı ve bütünlüğünün korunduğu sonucunu çıkartır. Bununla birlikte elektronik veriye ilk temas edildiği arama sırasındaki hash değerinin alınmasından önce bu elektronik veride değişiklik yapıldığına ilişkin iddiaların doğruluğu veya yanlışlığı hash değeri aracılığı ile tespit edilemez.

Bu aşamada yapılması gereken bir diğer önemli işlem elektronik verinin üretildiği, değiştirildiği, gönderildiği, alındığı ve kaydedildiği zamanın tespitinin sağlanması amacıyla verinin zaman damgasının tespitini yapmaktır. Bu sayede elektronik verinin üretim, erişim veya değiştirilme zamanları üzerinde değişiklik yapma imkânı engellenmiş olacaktır.

Elektronik delilin toplanması ve muhafazası aşamasında üzerinde durulan bir başka husus da koruma zincirinin (chain of custody) sağlanması gerekliliğidir. Elektronik (veya fiziksel) delilin, toplanması, muhafaza edilmesi, başka bir yere aktarılması ve analiz edilmesini gösteren kronolojik belgelendirme sürecini ifade eden koruma zinciri, elektronik delilin doğrulanması ve geçerliliğinin sağlanması bakımından büyük öneme sahiptir.

Tez kapsamında adli bilişimin ikinci aşaması olarak ele alınan elektronik delilin incelenmesi aşaması, elektronik verilerin gözle görülür hale getirilerek bunlardan delil niteliğine sahip olabileceklerin tespiti ve ortaya çıkartılması safhasını ifade etmektedir. Bu aşamada daha önce toplanan verilerden işe yarayanlarla yaramayanların birbirlerinden ayrılmaları sağlanır. İnceleme işlemi genellikle anahtar kelime arama işlemi ile yerine getirilir. Silinen verilerin kurtarılması, internet geçmişinin incelenmesi, gizlenmiş verilerin ortaya çıkartılması hep bu aşamada gerçekleştirilir.

Adli bilişimin üçüncü aşaması olan elektronik delilin analizi aşamasında ise inceleme aşamasından geçerek delil olma vasfı taşıdığı değerlendirilen verilerden hangilerinin ve ne ölçüde söz konusu suça temas ettiği hususu ortaya konularak bunlardan adli makamların önüne sunulmak üzere raporlanacak olanların belirlenmesi sağlanır. Bu anlamda inceleme aşaması delilleri ortaya çıkartmaya yönelik teknik bir işlem olmasına karşın analiz aşaması teknik olarak ortaya konan elektronik delilin önemi ve ispat değerini ortaya koyan hukuki değer verme işlemidir.

Adli bilişimin son aşaması olarak ele aldığımız raporlama ve sunum aşaması toplama, muhafaza altına alma, inceleme ve analiz aşamalarından geçen elektronik delilin yargılamanın tüm taraflarınca anlaşılır biçimde ortaya konulması işlemidir. Bu bakımdan diğer aşamalar adli bilişim esaslarına uygun yerine getirilmiş olsa da iyi bir raporlama işlemi ile mahkemeye sunulmadığı sürece adli bilişim sürecinin verimliliğinden söz edilemez. Bu nedenle raporlama ve sunum aşamasında adli bilişim sürecindeki elektronik delilin bütünlüğünü sağlamaya yönelik teknik bilgiler de dâhil tüm hususların tarafların anlayacağı ve tatmin olacağı biçimde ortaya konulması gerekir.

Tezimizin dördüncü bölümünün sonunda adli bilişime ilişkin sorunlar ve buna ilişkin çözüm önerilerinden bahsedilmiştir. Buna göre; adli bilişim süreci elde edilen elektronik delilin zarar görmesi olasılığını taşıması nedeniyle bu süreçte görev alan tüm personelin elektronik delile ilişkin yapılan tüm işlemlerle ilgili prensip ve prosedürlere karşı bilgilendirilmeleri ve uyarılmaları gerektiği vurgulanmıştır. Ayrıca tez kapsamında bu potansiyel sorunların haricindeki adli bilişimin ilke ve standartlarının belirlenmemesi, uyulması gereken usule ilişkin işlemlerin öneminin bilinmemesi, yeterince kaynak ayrılmaması, adli bilişimde görevli kişilerin yeterince eğitilmemesi, adli bilişimin en önemli unsurlarından olan adli bilişim uzmanı ve laboratuvarların yeterli seviyeye getirilmemiş olması gibi adli bilişimi zora sokan sorunların tespiti yapılmış ve bu sorunlara ilişkin çözüm önerilerimiz sıralanmıştır.

Yukarıda yapılan değerlendirmeler ışığında elektronik delilin elde edilmesi sürecinde ortaya çıkan sorunlara çözüm sağlamak amacıyla yapılacak yasal düzenlemelerde dikkat edilmesi gereken hususları maddeler halinde yeniden belirtmek gerekirse;

- Elektronik delil elde etmek amacıyla yapılacak arama, kopyalama ve elkoyma koruma tedbirinin kapsamı bilişim sistemleri ve bağlı donanımları şeklinde belirlenmelidir.

- Tedbirin uygulanması sırasında suç unsuru veya suç aracı olarak ele geçirilen elektronik veriler ve de bunlara ait adli kopyaların iadesi engellenmelidir.

- Hakkında tedbir uygulan şüpheli hakkında kovuşturmaya yer olmadığına dair karar verilmesi durumunda bu verilerin makul süre içerisinde imhası sağlanmalıdır.

- Gecikmesinde sakınca bulunan hallerde ve hâkim onayına sunulmak kaydıyla Cumhuriyet savcısının kararı ile de tedbirin uygulanmasına imkân sağlanmalıdır.

- Bilişim sistemlerine elkoymaksızın sistemdeki verilerin tamamının veya bir kısmının kopyasının alınması şeklinde uygulanacak tedbirde kopyası alınacak verilerin kâğıda yazdırılması zorunluluğundan vazgeçilmelidir.

- Tedbirin uygulanmasında "*başka surette delil elde etme imkânı bulunmaması"* şeklinde ifade edilen son çare prensibi bilişim suçları bakımından istisna tutulmalıdır.

- Bilişim sistemlerinde arama, kopyalama ve elkoyma tedbiri durağan haldeki veriler üzerinde uygulanma imkânına sahip olduğu için akış haldeki verilerin elde edilmesi hususunda iletişimin tespiti, dinlenmesi ve kayda alınması tedbirinin düzenlendiği CMK'nın 135. maddesinde ek bir düzenleme yapılmalıdır.

- Elektronik delilin teknolojik anlamda geçerliliğinin sağlanması bakımından hayati öneme sahip adli bilişim konusunda yapılacak yasal düzenlemede ise; adli bilişim uzmanının tanımı yapılmalı, görev sınırları belirlenmeli ve adli bilişim standartları açıkça ortaya konulmalıdır.

KAYNAKÇA

Kitaplar

Ahi, Gökhan. "Bilişim Suçlarında Usul ve Sorumluluk", **Bilişim Hukuku.** Mete Tevetoğlu (drl.). İstanbul: Kadir Has Üniversitesi Yayınları, 2006, ss. 100-107.

Akarslan, Hüseyin. **Bilişim Suçları.** Ankara: Seçkin Yayıncılık, 2012.

Altaylı, Behçet. **Bilgisayarlar ve Basic ile Programlama.** İstanbul: Filiz Kitabevi, 1985.

Amato, Astolfo Di. **Criminal Law in Italy.** The Netherlands: Kluwer Law International, 2011.

Anayurt, Ömer. **Avrupa İnsan Hakları Hukukunda Kişisel Başvuru Yolu.** Ankara: Seçkin Yayıncılık, 2004.

Atalay, Oğuz. "Elektronik Belgelerin Delil Değeri", **Bilişim Hukuku.** Mete Tevetoğlu (drl.). İstanbul: Kadir Has Üniversitesi Yayınları, 2006, ss. 139-146.

Balı, Yunus. "Adli Bilişim Rapor Metinlerinin Yargılama Sürecinde Kullanımı ve Anlamlandırılabilirliği", Levent Bayram (Ed.). **Ses Görüntü ve Data İncelemeleri** içinde. Ankara: Adalet Yayınevi, 2008, ss. (231-238).

Bayram, Levent. **Adli Bilimlerde Ses ve Konuşma İncelemeleri.** Ankara: Seçkin Yayıncılık, 2008.

Beceni Yasin. "Avrupa Siber Suçlar Sözleşmesi", **Bilişim Hukuku.** Mete Tevetoğlu (drl.). İstanbul: Kadir Has Üniversitesi Yayınları, 2006, ss. 96-99.

Bıçak, Vahit. **Suç Muhakemesi Hukuku.** 2. Basım. Ankara: Seçkin Yayıncılık, 2013.

Biyan, Özgür. **Türk Vergi Hukukunda İspat – Delil.** Ankara: Adalet Yayınevi, 2012.

Casey, Eoghan, **Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet**. Third Edition, California: Academic Press, 2011.

Centel, Nur ve Hamide Zafer. **Ceza Muhakemesi Hukuku.** 9. Basım. İstanbul: Beta Yayınevi, 2012.

Çolak, Haluk ve Mustafa Taşkın. **Açıklamalı-Karşılaştırmalı-Uygulamalı Ceza Muhakemesi Hukuku.** 2. Basım. Ankara: Seçkin Yayıncılık, 2007.

Daniel, Larry and Lars Daniel. **Digital Forensics For Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom.** Waltham: Syngress Publishing, 2012.

Değirmenci, Olgun. **Ceza Muhakemesinde Sayısal (Dijital) Delil**. Ankara: Seçkin Yayıncılık, 2014.

Deliduman, Seyithan. "Elektronik Verilerin Delil Değeri", **Bilişim Hukuku.** Mete Tevetoğlu (drl.). İstanbul: Kadir Has Üniversitesi Yayınları, 2006, ss. 44-56.

Demirbaş, Timur. **Sanığın Hazırlık Soruşturmasında İfadesinin Alınması.** İzmir: Dokuz Eylül Üniversitesi Döner Sermaye İşletmesi Yayınları, 1996.

Dokurer, Semih. "Adli Bilişim", Levent Bayram (Ed.). **Ses Görüntü ve Data İncelemeleri** içinde. Ankara: Adalet Yayınevi, 2008, ss. (239-249).

Donay, Süheyl. **Ceza Yargılama Hukuku.** İstanbul: Beta Yayınevi, 2010.

Dülger, Murat Volkan. **Bilişim Suçları ve İnternet İletişim Hukuku.** 2. Basım. Ankara: Seçkin Yayıncılık, 2012.

Erdoğan, Yavuz. **Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa Konseyi Siber Suçlar Sözleşmesi ve Yargıtay Kararları İle).** İstanbul: Legal Yayıncılık, 2012.

Erdurak, Yılmaz Güngör. **En Son Değişiklikleriyle Notlu-İçtihatlı Ceza Muhakemeleri Usulü Kanunu.** Ankara: Sevinç Matbaası, 1985.

Ergün, İsmail. **Siber Suçların Cezalandırılması ve Türkiye'de Durum.** Ankara: Adalet Yayınevi, 2008.

Eroğlu, Sevilay. **Rekabet Hukukunda Bilgisayar Programlarının Korunması.** İstanbul: Beta Yayınevi, 2000.

Erturgut, Mine. **Medeni Usul Hukukunda Elektronik İmzalı Belgelerin Delil Olarak Değerlendirilmesi.** Ankara: Yetkin Yayınları, 2004.

Eryılmaz, Mesut Bedri. **Ceza Muhakemesi Hukuku Dersleri.** Ankara: Seçkin Yayıncılık, 2012.

Feyzioğlu, Metin. **Ceza Muhakemesi Hukukunda Tanıklık.** Ankara: Ankara Üniversitesi Hukuk Fakültesi Yayınları, 1996.

Feyzioğlu Metin, **Ceza Muhakemesinde Vicdani Kanaat.** Ankara: Yetkin Yayınları, 2002.

Geyer, Florian. "Zehirli Ağacın Meyvesi", Burcu Başak Uluçay ve Barış Hocaoğlu (Çev.). Yener Ünver (Ed.). **Ceza Muhakemesi Hukukunda Delil ve İspat** içinde. Ankara: Seçkin Yayıncılık, 2014, ss. 457-485.

Gless, Sabine. "Delil Yasakları ve Uzak Etki", Kerem Öz (Çev.). Yener Ünver (Ed.). **Ceza Muhakemesi Hukukunda Delil ve İspat** içinde. Ankara: Seçkin Yayıncılık, 2014, ss. 345-359.

Göksu, Mustafa. **Hukuk Yargılamasında Elektronik Delil.** Ankara: Adalet Yayınevi, 2011.

Gözübüyük A. Şeref ve Feyyaz Gölcüklü. **Avrupa İnsan Hakları Sözleşmesi ve Uygulaması Avrupa İnsan Hakları Mahkemesi İnceleme ve Yargılama Yöntemi.** 9. Basım. Ankara: Turhan Kitabevi, 2011.

Helvacıoğlu, Aslı Deniz. "Avrupa Konseyi Siber Suç Sözleşmesi Temel Hükümlerinin İncelenmesi", **İnternet ve Hukuk.** Yeşim Atamer (drl.). İstanbul: Bilgi Üniversitesi Yayınları, 2004, ss. 277-299.

Henkoğlu, Türkay. **Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi.** İstanbul: Pusula Yayıncılık, 2011.

Hock Lai Ho. "Ceza Davasında Hukuka Aykırı Elde Edilen Delilin Yasaklanması Kuralı", Doruk Özgündüz (Çev.). Yener Ünver (Ed.). **Ceza Muhakemesi Hukukunda Delil ve İspat** içinde. Ankara: Seçkin Yayıncılık, 2014, ss. 85-111.

Jones Nigel, Esther George, Kasım Karagöz, Murat Volkan Dülger ve Gözde Modoğlu (hzl.), **Bilişim Suçları Eğitim Modülü (Türk Ceza Adalet Sisteminin Etkinliğinin Geliştirilmesi Avrupa Birliği & Avrupa Konseyi Ortak Projesi),** Ankara: MATBAM Ajans & Reklam & Tanıtım, 2014.

Karagülmez, Ali. **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri.** 2. Basım. Ankara: Seçkin Yayıncılık, 2011.

Kaygısız, Mustafa. **Kriminalistik Olay Yeri İnceleme Suç Yeri ve Olay Güvenliği.** Ankara: Adalet Yayınevi, 2007.

Kaymaz, Seydi. **Uygulama ve Teoride Ceza Muhakemesinde Hukuka Aykırı (Yasak) Deliller.** Ankara: Seçkin Yayıncılık, 1997.

Keser Berber, Leyla. **Adli Bilişim.** Ankara: Yetkin Yayınları, 2004.

Ketizmen, Muammer. **Türk Ceza Hukukunda Bilişim Suçları.** Ankara: Adalet Yayınevi, 2008.

Kunter, Nurullah ve Feridun Yenisey. **Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku.** 11. Basım. İstanbul: Beta Yayınevi, 2000.

Kunter, Nurullah, Feridun Yenisey ve Ayşe Nuhoğlu. **Muhakeme Hukuku Dalı Olarak Ceza Muhakemesi Hukuku.** 18. Basım. İstanbul: Beta Yayınevi, 2010.

Kunter, Nurullah, Feridun Yenisey ve Ayşe Nuhoğlu, **Açıklamalı Ceza Muhakemesi Kanunu**. Cilt I. İstanbul: Beta Yayınevi, 2013.

Kurt, Levent. **Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Yeri.** Ankara: Seçkin Yayıncılık, 2005.

Mason, Stephen (Ed.). **International Electronic Evidence.** London: BIICL, 2008.

Mukasey, Michael B., Jeffrey L. Sedgwich and David W. Hagy. **Electronic Crime Scene Investigation: A Guide for First Responders.** Second Edition. Washington: PhotoDisc, Inc, 2001.

Nilsson, John. D. (Ed.), **Digital Evidence in the Courtroom.** New York: Nova Science Publishers, Inc., 2010.

Okan, Neval, Ozan Ercan Taşkın, Nazmiye Özenbaş Boydağ, Hakan Karakehya (Ed.). **Ceza Muhakemesi Hukuku.** Eskişehir: Anadolu Üniversitesi Yayınları, 2005.

Özbek, Veli Özer. **Ceza Muhakemesi Hukukunda Koruma Tedbiri Olarak Arama.** Ankara: Seçkin Yayıncılık, 1999.

Özbek, Veli Özer. **Ceza Muhakemesi Hukuku.** Ankara: Seçkin Yayıncılık, 2006.

Özbek, Veli Özer, Mehmet Nihat Kanbur, Koray Doğan, Pınar Bacaksız ve İlker Tepe. **Ceza Muhakemesi Hukuku.** 5. Basım. Ankara: Seçkin Yayıncılık, 2013.

Özboyacı, Alper. **Ceza Muhakemesi Hukukunda Delil Yasakları (Yargıtay İçtihatları İle).** İstanbul: Kazancı Hukuk Yayınevi, 2008.

Özdilek, Ali Osman**. İnternet ve Hukuk.** İstanbul: Papatya Yayıncılık, 2002.

Özdilek, Ali Osman. **Uygulamadan Örnek Olaylarla Bilişim Suçları ve Hukuku.** İstanbul: Vedat Kitapçılık, 2006.

Özen Muharrem ve İhsan Baştürk. **Bilişim-İnternet ve Ceza Hukuku.** Ankara: Adalet Yayınevi, 2011.

Özkan, Halid. "Ceza Muhakemesinde Ekran Görüntüsü Çıktılarının Delil Niteliği", Yener Ünver (Ed.). **Ceza Muhakemesi Hukukunda Delil ve İspat** içinde. Ankara: Seçkin Yayıncılık, 2014, ss. 265-287.

Öztürk, Bahri. **Yeni Yargıtay Kararları Işığında Delil Yasakları (Hukuka Aykırı Olarak Elde Edilen Deliller, Yasak Kanıtlar).** Ankara: Ankara Üniversitesi Siyasal Bilimler Fakültesi İnsan Hakları Merkezi Yayınları, 1995.

Öztürk, Bahri (Ed.). **Nazari ve Uygulamalı Ceza Muhakemesi Hukuku Ders Kitabı.** Ankara: Seçkin Yayıncılık, 2009.

Öztürk, Bahri (Ed.). **Nazari ve Uygulamalı Ceza Muhakemesi Hukuku Ders Kitabı.** 7. Basım, Ankara: Seçkin Yayıncılık, 2014.

Öztürk, Bahri, Mustafa Ruhan Erdem ve Veli Özer Özbek. **Uygulamalı Ceza Muhakemesi Hukuku.** 7. Basım. Ankara: Seçkin Yayıncılık, 2002.

Öztürk, Cemal. **Ceza Muhakemesinde İz Bilimi Kriminalistik Gerçeği,** Ankara: Seçkin Yayıncılık, 2006.

Parlar, Ali ve Muzaffer Hatipoğlu. **5271 Sayılı Ceza Muhakemesi Kanunu Yorumu ve İlgili Mevzuat.** 1. Cilt. Ankara: Yayın Matbaacılık, 2008.

Parlar, Ali, Muzaffer Hatipoğlu ve Erol Güngör Yüksel. **Açıklamalı-İçtihatlı Ceza Muhakemesi Hukukunda Deliller Çapraz Sorgu ve İspat.** Ankara: Yayın Matbaacılık, 2008.

Picotti, Lorenzo and Ivan Salvadori (hzl.). **National Legislation Implementing the Convention on Cybercrime-Comparative Analysis and Good Practices.** Strasbourg: Discussion Paper, 2008.

Sarıakçalı, Turgay. **İnternet Üzerinden Akdedilen Sözleşmeler.** Ankara: Seçkin Yayıncılık, 2008.

Say, Kubilay. "Bilişim Suçlarında Olay Yeri İncelemesinin Hukuki Boyutu", Levent Bayram (Ed.), **Ses Görüntü ve Data İncelemeleri** içinde. Ankara: Adalet Yayınevi, 2008, ss. 251-260.

Say, Kubilay. "Data İncelemeleri", Oğuz Karakuş (Ed.). **Kriminalistik** içinde. Ankara: Adalet Yayınevi: 2009, ss. 510-531.

Sınar, Hasan. **İnternet ve Ceza Hukuku.** İstanbul: Beta Yayınevi, 2001.

Soyaslan, Doğan. **Ceza Muhakemesi Hukuku.** 4. Basım. Ankara: Yetkin Yayınları, 2010.

Şafak, Ali ve Vahit Bıçak. **Ceza Muhakemesi Hukuku ve Polis.** 6. Basım. Ankara: Roma Yayınları, 2005.

Şahin, Cumhur. **Ceza Muhakemesi Hukuku I.** 4. Basım. Ankara: Seçkin Yayıncılık, 2013.

Şahin, Cumhur ve Neslihan Göktürk. **Ceza Muhakemesi Hukuku II.** 2. Basım. Ankara: Seçkin Yayıncılık, 2013.

Şen, Ersan. **Türk Hukuku'nda Telefon Dinleme-Gizli Soruşturmacı-X Muhbir.** 6. Basım. Ankara: Seçkin Yayıncılık, 2013.

Şentürk, Aysan (Ed.). **Bilgisayar Kullanımı ve İnternet.** Ankara: Ekin Yayınevi, 2007.

Tanrıkulu, Cengiz. **Ceza Muhakemesi Hukukunda Bilişim Sistemlerinde Arama ve Elkoyma.** Ankara: Adalet Yayınevi, 2014.

Thaman, Stephen C. "Karşılaştırmalı Hukukta Yasak Ağacın Meyveleri", Ahmet Emrah Geçer (Çev.). Yener Ünver (Ed.). **Ceza Muhakemesi Hukukunda Delil ve İspat** içinde. Ankara: Seçkin Yayıncılık, 2014, ss. 361-407.

Taşkın, Şaban Cankat. **Bilişim Suçları.** İstanbul: Beta Yayınevi, 2008.

Toroslu, Nevzat ve Metin Feyzioğlu. **Ceza Muhakemesi Hukuku.** 7. Basım. Ankara: Savaş Yayınları, 2009.

Turhan, Faruk. **Ceza Muhakemesi Hukuku.** Ankara: Asil Yayınları, 2006.

Uçkan, Özgür ve Yasin Beceni. "Bilişim-İletişim Teknolojileri ve Ceza Hukuku", **İnternet ve Hukuk.** Yeşim Atamer (drl.). İstanbul: Bilgi Üniversitesi Yayınları, 2004, ss. 363-430.

Ünver Yener ve Hakan Hakeri. **Ceza Muhakemesi Hukuku.** 1. Cilt. 8. Basım. Ankara: Adalet Yayınevi, 2013.

Ünver Yener ve Hakan Hakeri. **Ceza Muhakemesi Hukuku.** 2. Cilt. 7. Basım. Ankara: Adalet Yayınevi, 2013.

Yaşar, Osman. **Ceza Muhakemesi Kanunu Yeni İçtihatlarla Uygulamalı ve Yorumlu.** I. Cilt, 5. Basım, Ankara: Seçkin Yayıncılık, 2011.

Yaşar, Osman. **Ceza Muhakemesi Kanunu Yeni İçtihatlarla Uygulamalı ve Yorumlu.** II. Cilt, 5. Basım, Ankara: Seçkin Yayıncılık, 2011.

Yenidünya, A. Caner ve Olgun Değirmenci. **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları.** İstanbul: Legal Yayıncılık, 2003.

Süreli Yayınlar

Abel, Wiebke. "Agents, Trojans and Tags: The Next Generation of Investigation". **International Review of Law, Computers & Technology.** Vol. 23, No. 1&2, March-July 2009, ss. 99-108.

Abel, Wiebke and Burkhard Schafer, "The German Constitutional Court on the Right in Confidential and Integrity of Information Technology Systems - A Case Report on BVerfG, NJW 2008, 822", **Scripted.** Vol. 6, Issue. 1, April 2009, ss. 106-123.

Aksoy İpekçioğlu, Pervin. "Gözaltında Alınan İfadenin Önemi ve Delil Değeri". **Ankara Üniversitesi Hukuk Fakültesi Dergisi.** Cilt. 57, Sayı. 3, 2008, ss. 51-82.

Akyürek Güçlü. "Ceza Yargılamasında Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu". **Türkiye Barolar Birliği Dergisi.** Sayı. 101, Temmuz-Ağustos 2012, ss. 61-82.

Başlar, Yusuf. "Koruyucu Hakları Etkisiz Kılmaya Yönelik Hazırlık Hareketleri Suçu". **Uyuşmazlık Mahkemesi Dergisi.** Cilt. 1, Sayı. 1, Mayıs 2013, ss. 243-259.

Başlar, Yusuf. "Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri". **Uyuşmazlık Mahkemesi Dergisi.** Cilt. 1, Sayı. 3, Haziran 2014, ss. 82-105.

Bayram, Levent. "Ses ve Görüntü Kayıtlarının Türk Hukukundaki Yeri". **Polis Bilimleri Dergisi.** Cilt. 6, Sayı. 3-4, 2004, ss. 1-12.

Bayraktar, Bülent. "Muhakemelerde Delillerin Önemi". **Kırgızistan-Türkiye Manas Üniversitesi Sosyal Bilimler Enstitüsü Dergisi.** Sayı. 25, 2011, ss. 9-19.

Cengiz, Serkan (çev.). "İnsan Hakları Avrupa Mahkemesi Kararları". **Türkiye Barolar Birliği Dergisi.** Sayı. 82, Mayıs 2009, ss. 447-466.

Cosic, Jasmin and Zoran Cosic. "Chain of Custody and Life Cycle of Digital Evidence". **Computer Technology and Application.** Vol. 3, No. 2, February 2012, ss. 126-129.

Çakır, Hüseyin ve Mehmet Serkan Kılıç. "Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bir Bakış". **Polis Bilimleri Dergisi.** Cilt. 15, Sayı. 3, 2013, ss. 23-44.

Çeken, Hüseyin. "Amerika Birleşik Devletlerinde İnternet Yolu İle İşlenen Suçlara İlişkin Düzenlemeler". **Askeri Adalet Dergisi.** Sayı. 114, Mayıs 2002, ss. 73-95.

Çınar, Ali Rıza. "Hukuka Aykırı Kanıtlar". **Türkiye Barolar Birliği Dergisi.** Sayı. 55, Kasım-Aralık 2004, ss. 31-64.

DeGaine, Jacqueline J. "Digital Evidence". **The Army Lawyer.** May 2013, ss. 7-34.

Değirmenci, Olgun. "Bilgi Toplumunun Delil Türü: Sayısal Deliller ve Bilimselliği". **Terazi Hukuk Dergisi,** Cilt. 9, Sayı. 97, Eylül 2014, ss. 14-28.

Ercan, Tuncay ve Doğukan Nacak. "Kablosuz Ağlardaki Paket Trafiğine Adli Bilişim Yaklaşımı". **Journal of Yaşar University.** Cilt. 4, Sayı. 13, 2009, ss. 1909-1921.

Erdağ, Ali İhsan. "İletişimin Denetlenmesi Kapsamında İki Önemli Sorun Olarak: Mağdurun İletişimin Tespiti ve İletişimin Mağdur Tarafından Kaydedilmesi". **Türkiye Barolar Birliği Dergisi.** Sayı. 92, Mart-Nisan 2011, ss. 31-61.

Erdoğan, Yavuz. "Bilişim Sistemine Girme ve Kalma Suçu". **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi.** Cilt. 12, Özel Sayı, 2010, ss. 1363-1433.

Feyzioğlu, Metin. "Belirtilerin Şüphenin Yenilmesindeki İşlevi ve Benzer İsnadlara Ait Delil Araçlarının Somut Olayın Çözümünde Birlikte Değerlendirilmesi". **Ankara Barosu Dergisi.** Sayı. 1, 2000, ss. 19-46.

Gökcan, Hasan Tahsin. "Gizli Kamera Kaydı Delil Olarak Kabul Edilebilir mi?", **Terazi Hukuk Dergisi.** Cilt. 5, Sayı. 42, Şubat 2010, ss. 73-86.

Gökcan, Hasan Tahsin. "Cumhuriyet Savcısının Delilleri Değerlendirme Yetkisi ve Yargıtay Uygulaması". **Ankara Barosu Dergisi.** Sayı. 1, 2012, ss. 193-206.

Gören, Zafer. "Düşünceyi Açıklama Özgürlüğü". **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi.** Sayı. 24, Güz 2013/2, ss. 31-60.

Gross, Emanuel. "The Struggle of a Democracy Against the Terror of Suicide Bombers: Ideological and Legal Aspects". **Wisconsin International Law Journal.** Vol. 22, No. 3, Fall 2004, ss. 597-710.

Hafızoğulları, Zeki ve Muharrem Özen. "Türk Ceza Hukukunda Devlet Sırrına Genel Bir Bakış". **Ankara Barosu Dergisi.** Sayı. 1, 2010, ss. 21-30.

Hancı, Hamit, Ayşim Tuğ ve Yeşim Doğan, "Kriminalistik Kriminoloji Değildir". **Türkiye Barolar Birliği Dergisi.** Sayı. 48, 2003, ss. 261-266.

Hekim, Hakan ve Oğuzhan Başıbüyük. "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları". **Uluslararası Güvenlik ve Terörizm Dergisi.** Cilt. 4, Sayı. 2, 2013, ss. 135-158.

Henkoğlu, Türkay ve Özgür Külcü. "Bilgi Erişim Platformu Olarak Bulut Bilişim: Riskler ve Hukuksal Koşullar Üzerine Bir İnceleme". **Bilgi Dünyası Dergisi.** Cilt.14, Sayı.1, Nisan 2013, ss. 62-86.

Hosmer, Chet. "Providing the Integrity of Digital Evidence with Time". **International Journal of Digital Evidence.** Vol. 1, No. 1, Spring 2002, ss. 1-7.

Insa, Fredesvinda. "The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime-Results of a European Study". **Journal of Digital Forensic Practice.** Vol. 1, No. 4, 2006, ss. 285-289.

İçel, Kayıhan. "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri". **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası.** Cilt. 59, Sayı. 1-2, 2001, ss. 3-10.

Kaşıkara, M. Serhat. "Ceza Muhakemesi Hukukunda Delil Elde Etme Yasakları". **Ceza Hukuku Dergisi (CHD).** Sayı. 10, Ağustos 2009, ss. 177-208.

Kerr, Orin S. "Digital Evidence and the New Criminal Procedure". **Columbia Law Review.** Vol. 105, January 2005, ss. 279-318.

Kerr, Orin S. "Searches and Seizures in a Digital World". **Harvard Law Review.** Vol. 119, 2005, ss. 531-585.

Keskin, İbrahim. "Bilişim Suçları". **Adalet Dergisi.** Sayı. 29, Eylül 2007, ss. 101-119.

Keskin, Serap. "Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi". **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası.** Cilt. 59, Sayı. 1-2, 2001, ss. 155-180.

Kızılyar, Murat. "Ceza Yargılamasında Dijital Verilerin Delil Değeri". **Adalet Dergisi.** Sayı. 50, Eylül 2014, ss. 72-89.

Koca, Mahmut. "Ceza Muhakemesinde Hukuka Aykırı Delilleri Değerlendirme Yasağı". **Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi (AÜEHFD).** Cilt. IV, Sayı. 1-2, 2000, ss. 105-146.

Koca, Mahmut. "Ceza Muhakemesi Hukukunda Deliller". **Ceza Hukuku Dergisi (CHD).** Sayı. 2, Aralık 2006, ss. 207-225.

Kenan Koçer. "Telekomünikasyon Aracılığıyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı, Teknik Araçlarla İzleme ya da Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El Koyma Suretiyle Elde Edilen Sesli veya Görüntülü Verilerin Disiplin Soruşturmasındaki Kıymeti", **Ceza Hukuku Dergisi.** Sayı. 10, Ağustos 2009, ss. 5-40.

Kümüştaş, Şevket. "Maddi Delillerin Elde Edilmesi ve Hukuka Uygunluğu". **Çağın Polisi Dergisi.** Sayı. 66, Haziran 2007, ss. 36-41.

Leroux, Olivier. "Legal Admissibility of Electronic Evidence". **International Review of Law, Computers & Technology.** Vol. 18, No. 2, July 2004, ss. 193-220.

Mahmutoğlu, Fatih Selami. "Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu". **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası.** Cilt. 59, Sayı. 1-2, 2001, ss. 39-49.

Moore, Robert. "To View or Not to View: Examining the Plain View Doctrine and Digital Evidence". **American Journal of Criminal Justice.** Vol. 29, No. 1, 2004, ss. 57-74.

Moshirnia, Andrew Vahid. "Separating Hard Fact From Hard Drive: A Solution for Plain View Doctrine in the Digital Domain". **Harvard Journal of Law & Technology.** Vol. 23, No. 2, Spring 2010, ss. 609-634.

Odman, M. Tevfik. "Askeri Yargıtay'ın Hukuka Aykırı Deliller Konusunda Verdiği Kararlar". **Askeri Adalet Dergisi.** Sayı. 95, Ocak 1996, ss. 9-32.

Oğuz, Habip. "Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum". **Uyuşmazlık Mahkemesi Dergisi.** Cilt. 1, Sayı. 3, Haziran 2014, ss. 1-38.

O'Leary, Kaitlyn R. "What the Founders Did See Coming: The Fourtyh Amendment, Digital Evidence, and the Plain View Doctrine". **Suffolk University Law Review.** Vol. 46, 2013, ss. 211-241.

Ölmez, Aslan, "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Kopyalama ve Bunlara El Koyma". **Terazi Hukuk Dergisi.** Cilt. 4, Sayı. 30, Şubat 2009, ss. 45-52.

Özbek, Veli Özer. "Elektronik Ortamda Saklı Bulunan Verilerin Ceza Muhakemesinde Delil Niteliği ve Değerlendirilmesi". **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası.** Cilt. 59, Sayı. 1-2, 2001, ss. 181-202.

Özbek, Veli Özer. "İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları". **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi.** Cilt. 4, Sayı. 1, 2002, ss. 101-158.

Özbey, Özcan. "Adli Bilişim ve Sayısal Deliller (5271 Sayılı CMK'nın 134. Maddesi)". **Yargıtay Dergisi.** Cilt. 36, Sayı. 3, Temmuz 2010, ss. 61-126.

Pallı, Hayati. "Türk Ceza Kanununda Yer Alan Başlıca Bilişim Suçları". **Adalet Dergisi.** Sayı. 33, Ocak 2009, ss. 114-133.

Robinton, Lily R. "Courting Chaos: Confilicting Guidance from Courts Highlights The Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence". **Yale Journal of Law and Technology.** Vol. 12, 2010, ss. 310-347.

Sağıroğlu, Şeref ve Mehmet Karaman, "Adli Bilişim". **Teletapi Haberleşme ve Bilişim Teknolojileri Dergisi.** Sayı. 203, (Ağustos 2012), ss. 62-67.

Soyaslan, Doğan. "Hukuka Aykırı Deliller". **Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi (AÜEHFD).** Cilt. 7, Sayı. 3-4, Aralık 2003, ss. 9-26.

Soysal, Tamer. "İnternet Servis Sağlayıcılarının Hukuki Sorumluluğu". **Türkiye Barolar Birliği Dergisi.** Sayı. 61, Kasım-Aralık 2005, ss. 304-339.

Sevimli, A. Güçlü. "Bilgisayar ve Bilgisayar Kütüklerine El Konulması ve Uygulamadaki Sorunlar". **İstanbul Barosu Dergisi.** Cilt. 81, Sayı. 3, Mayıs-Haziran 2007, ss. 993-1000.

Şahbaz, İbrahim. "Karşılaştırmalı Hukukta ve Avrupa İnsan Hakları Mahkemesi Kararlarında Hukuka Aykırı Deliller". **Ankara Barosu Dergisi.** Sayı. 1, 2006, ss. 101-128.

Şeker, Güven. "Bilişim Suçlarının Delillendirilmesinde Amerikan Uygulaması ve Ülkemizdeki Durum". **Uluslararası İnsan Bilimleri Dergisi.** Cilt. 1, Sayı. 1, 2004, ss. 1-13.

Şen, Ersan. "Ceza Yargılaması Süreci". **Türkiye Barolar Birliği Dergisi.** Sayı. 97, Kasım-Aralık 2011, ss. 269-300.

Şen, Ersan. "E-Posta Takibi". **Terazi Hukuk Dergisi.** Cilt. 9, Sayı. 97, Eylül 2014, ss. 88-89.

Şen, Ersan ve Yasemin Yurttaş. "Bilgisayar Programları Karşısında Özel Hayatın Korunması". **Terazi Hukuk Dergisi.** Cilt. 5, Sayı. 42, Şubat 2010, ss. 29-44.

Şen, Hikmet. "Bilimsel Yöntemlerle Elde Edilen Delillerin Hukuka Aykırılığı Sorunu ve Bağlayıcılığının Değerlendirilmesi". **Adalet Dergisi.** Sayı. 34, Mayıs 2009, ss. 110-118.

Şen, Osman Nihat. "Ceza Hukukunda Bilgisayar Araştırmaları". **Ceza Hukuku Dergisi (CHD).** Sayı. 1, Ekim 2006, ss. 375-395.

Şirikçi. Ahmet Serhat ve Nergis Cantürk. "Adli Bilişim İncelemelerinde Birebir Kopya Alınmasının (İmaj Almak) Önemi". **Bilişim Teknolojileri Dergisi.** Cilt. 5, Sayı. 3, Eylül 2012, ss. 29-34.

Ünver Yener. "Ceza Muhakemesinde İspat, CMK ve Uygulamamız". **Ceza Hukuku Dergisi (CHD).** Sayı. 2, Aralık 2006, ss. 103-205.

Vaciago, Giuseppe. "Remote Forensics and Cloud Computing: An Italian and European Legal Overview", **Digital Evidence and Electronic Signature Law Review.** Vol. 8, 2011, ss. 124-129.

Volonino, Linda. "Electronic Evidence and Computer Forensics", **Communications of the Association for Information Systems.** Vol. 12, October 2003, ss. 457-468.

Yaşar, Yusuf. "Bir Suçun İspatı Amacıyla İletişimin Kayda Alınmasının Hukuki Niteliği". **Türkiye Adalet Akademisi Dergisi (TAAD).** Sayı. 14, Temmuz 2013, ss. 353-396.

Yaşar, Yusuf ve İsmail Dursun. "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi (MAR-HAD).** Cilt. 19, Sayı. 3, 2013, ss. 3-34.

Yavuz, Mehmet, "Ceza Muhakemesinde İspat Sorunu". **Türkiye Adalet Akademisi Dergisi (TAAD).** Sayı. 9, Nisan 2012, ss. 151-176.

Yetim, Servet. "Adli Bilişim ve Canlı Bilişim Sistemlerinde Dijital Delil Araştırma Yöntemleri". **Terazi Hukuk Dergisi.** Cilt. 2, Sayı. 11, Temmuz 2007, ss. 123-129.

Yetim, Servet. "Dijital Kanıt Araştırma Yöntemleri". **İstanbul Barosu Dergisi.** Cilt. 82, Sayı. 3, Mayıs-Haziran 2008, ss. 1201-1222.

Yetim, Servet. "Elektronik Posta (e-posta) Hesabı İçeriği Mirasa Konu Olabilir mi?". **Terazi Hukuk Dergisi.** Cilt. 3, Sayı. 21, Mayıs 2008, ss. 49-65.

Yıldız, Ali Kemal. "Ses ve/veya Görüntü Kayıtlarının İspat Fonksiyonu". **Ceza Hukuku Dergisi (CHD).** Sayı. 2, Aralık 2006, ss. 253-264.

Yıldız, Özcan Rıza. "Bilişim Dünyasının Yeni Modeli: Bulut Bilişim (Cloud Computing) ve Denetim". **Sayıştay Dergisi.** Sayı. 74-75, Temmuz-Aralık 2009, ss. 5-23.

Yılmaz, Sacit. "5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar". **Türkiye Barolar Birliği Dergisi.** Sayı. 92, Mart-Nisan 2011, ss. 62-100.

Diğer Yayınlar

Abel, Scritto da Wiebke and Burkhard Schafer. "The German 'Federal Trojan' – Challenges Between Law and Technology", 2009, http://www.teutas.it/societa-informazione/prova-elettronica/634--the-german-federal-trojan-challenges-between-law-and-technology-wiebke-abel-llm-university-of-edinburgh-script-wabelsmsedacuk-burkhard-schafer-university-of-edinburgh-joseph-bell-centre-1-introduction-the-council-of-the-european-uni.html (21 Kasım 2014).

Adli Bilişim Prensipleri Nelerdir ?. 2014, http://www.teknospaper.com/2014/04/adli-bilisim-prensipleri/ (25 Ekim 2014).

Ağaoğlu, Deniz. "Bilgi Mimarlık Yaz Stajı", 2014, http://bilgimimdenizagaoglu.blogspot.com.tr/2014/11/teknoloji-staji-2014.html (24 Ocak 2015).

Ahi, M. Gökhan. "Adli Bilişim Nedir ?". http://www.bilisimhukuk.com/2009/07/adli-bilisim-nedir/ (04 Mayıs 2014).

Aktepe, Basri. "Emniyet Personelinin Bilgisayar ve Bilgisayarla İlintili Suçlarla Mücadelede Dikkat Etmesi Gereken Hususlar (Adli Tıp Esaslarına Uygun Olarak Delillendirme)", **1. Polis Bilişim Sempozyumu.** Ankara, 21-22 Ekim 2003, ss. 66-69.

Alaca, Bahaddin. "Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutu İle)", **Yayınlanmamış Yüksek Lisans Tezi.** Ankara Üniversitesi SBE, 2008.

Altunkaş, Aysun. "Hukuka Aykırı Delil Teorisi Işığında İfade Alma ve Sorgu", **Yayınlanmamış Yüksek Lisans Tezi.** İstanbul Bilgi Üniversitesi SBE, 2006.

Anayasa Mahkemesi. 22.06.2001. E. 1999/2, K. 2001/2 (**Anayasa Mahkemesi Kararlar Dergisi,** Cilt. 2, Sayı. 37, 2002), ss. 922-1552.

Anayasa Mahkemesi (Yüce Divan). 19.12.2012. E. 2011/1, K. 2012/1, http://www.anayasa.gov.tr/files/yuce_ divan_2011.doc (08 Aralık 2014).

Anayasa Mahkemesi. 18.06.2014. BN. 2013/7800, http://www.kararlaryeni.anayasa.gov.tr/BireyselKarar/Content/de3fd0d1-cced-4a35-8377-750ed661dd6b?wordsOnly=False (15 Ekim 2014).

Arslan, Hasan Tahsin. "Anlaşma Çerçevesinde Bilişim Suçlarının İzlenmesi", **1. Polis Bilişim Sempozyumu.** Ankara, 21-22 Ekim 2003, ss. 205-210.

Ashcroft, John (Ed). "Electronic Crime Scene Investigation: A Guide for First Responders", Washington: PhotoDisc, Inc, 2001. https://www.ncjrs.gov/pdffiles1/nij/187736.pdf (09 Eylül 2014).

Ashcroft, John, Deborah J. Daniels and Sarah V. Hart. Forensic Examination of Digital Evidence: A Guide for Law Enforcement, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf (12 Ocak 2015).

Askville By Amazon, (t.y) http://askville.amazon.com/duplicate-files-pc-effect-havng-performance/AnswerViewer.do?requestId=16358454 (05 Şubat 2014).

Avcı, Feyzullah. "Ceza Yargılamasında Özel Hayatın Gizliliği Hak ve Hürriyetinin Hukuka Aykırı Olarak Elde Edilen Deliller Nedeniyle İhlali", **Yayınlanmamış Yüksek Lisans Tezi.** Selçuk Üniversitesi SBE, 2006.

Aydoğan, Hakan. "Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri", **Yayınlanmamış Yüksek Lisans Tezi.** Polis Akademisi GBE, 2009.

Balı, Yunus. "CMK 134. Madde Düzeltilmelidir", http://www.dijitaldeliller.com/cmk134.htm (18 Kasım 2013).

Bilişim Ajandası. "Nihayet Türkiye de 'Sanal Suçlar Sözleşmesi'ni İmzaladı", **Bilişim Kültür Dergisi.** 2010, ss. 10-12, http://www.bilisimdergisi.org/s127 (04 Mart 2014).

Birtek, Fatih. "İstihbarat Amacıyla İletişim Özgürlüğüne Müdahale Edilmesi ve Müdahaleden Elde Edilen Materyallerin Delil Olarak Kabul Edilebilirliği", (t.y.), http://www.turkhukuksitesi.com/makale_1284.htm (05 Ocak 2015).

Carrier, Brian. "Open Source Digital Forensics Tools: The Legal Argument", 2002, http://www.digital-evidence.org/papers/opensrc_legal.pdf (18 Nisan 2015).

Carrier, Brian. D. "A Hypothesis-Based Approach to Digital Forensic Investigations", **PhD Thesis.** Purdue Üniversity, 2006.

Casey, Eoghan, "Error, Uncertainty, and Loss in Digital Evidence", International Journal of Digital Evidence, 2002, Vol. 1, No. 2, dblp veritabanı, (24 Ekim 2014).

Cosic, Jasmin and Miroslov Baca, "(Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp", http://czb.foi.hr/upload/datoteke/10_400.pdf (21 Ekim 2014).

Cryptography Defined/Brief History, http://www.laits.utexas.edu/~anorman/BUS.FOR/course.mat/SSim/history.html (18 Ocak 2015).

Çakır, Hüseyin ve Ercan Sert. "Bilişim Suçları ve Delillendirme Süreci", Örgütlü Suçlar ve Yeni Trendler, **Uluslararası Terörizm ve Sınıraşan Suçlar Sempozyumu (UTSAS 2010) Seçilmiş Bildirileri.** Oğuzhan Ömer Demir ve Murat Sever (dr.), Ankara, 2011, ss. 143-170.

Çekiç, Burak. "İnternet Aracılığı İle İşlenen Suçlar", **Yayınlanmamış Yüksek Lisans Tezi.** Marmara Üniversitesi SBE, 2006.

Çiçek, İlker. "Ülkemizde Adli Bilişim Laboratuarı Kurulumu ve Bilişim Suçlarıyla Mücadeleye Katkıları", **Yayınlanmamış Yüksek Lisans Tezi.** Haliç Üniversitesi FBE, 2008.

Dağ, Güray. "Kişisel Verilerin Ceza Muhakemesi Hukukunda Delil Olarak Kullanılması", **Yayınlanmamış Doktora Tezi.** Marmara Üniversitesi SBE, 2011.

Darende, M. İhsan, "Hukuka Aykırı Delil", http://www.turkhukuksitesi.com/makale_622.htm (28 Ocak 2014).

Dilek, Halil İbrahim. "Bilişim Suçları ve Türk Hukuk Sistemindeki Yeri", **Yayınlanmamış Yüksek Lisans Tezi.** Diyarbakır Üniversitesi SBE, 2007.

Dinler, Veysel. "Ceza Muhakemesinde Delillerin Toplanması", **Yayınlanmamış Yüksek Lisans Tezi.** Polis Akademisi GBE, 2009.

Dokurer, Semih. "Adli Bilişim", **2. Polis Bilişim Sempozyumu.** Ankara, 14-15 Nisan 2005, ss. 226-229.

Ekizer, A. Hakan. "Adli Bilişim (Computer Forensics)", http://www.ekizer.net/adli-bilisim-computer-forensics, (10 Nisan 2014).

Erdoğan, Burcu. "Bir Kişiyi Suçlamak İçin IP Adresi Yeterli midir?", (t.y.), http://www.bilisimhukuk.com/2010/02/bir-kisiyi-suclamak-icin-ip-adresi-yeterli-midir/ (10 Ocak 2015).

E-Posta Nedir?. (t.y) http://www.frmtr.com/bilgisayar-guvenligi-hakkinda-sorulariniz-ve-sorunlariniz/65966-e-posta-nedir.html (18 Kasım 2014).

Eralp, Özgür. "Elektronik Postaların İspat Hukuku Açısından Delil Olma Değeri", 2011, http://www.ozgureralp.av.tr/detay/makaleler/elektronik-postalarin-ispat-hukuku-acisindan-delil-olma-degeri/6/328/ (24 Ocak 2015).

Erol, Mehmet. "Ceza Muhakemesi Hukukunda Delil Olarak Telefon Dinleme", **Yayınlanmamış Yüksek Lisans Tezi.** Kocaeli Üniversitesi SBE, 2010.

Eryılmaz, Ali. "Ceza ve Disiplin Muhakemesinde Hukuka Aykırı Delillerin Değerlendirilmesi Sorunu", **Yayınlanmamış Yüksek Lisans Tezi.** Polis Akademisi GBE, 2011.

Galves, Fred and Christine Galves. "Ensuring the Admissibility of Electronic Forensic Evidence and Enhancing Its Probative Value at Trial", Criminal Justice Magazine. Vol. 19, No. 1, Spring 2004, http://www.americanbar.org/publications/criminal_justice_magazine_home/crimjust_cjmag_19_1_electronic.html (16 Aralık 2014).

Gözüşirin, Mesih. "5237 Sayılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları ile Mücadeleye İlişkin Model Önerisi", **Yayınlanmamış Yüksek Lisans Tezi.** Kara Harp Okulu SBE, 2011.

Günal, Cem. "Adli Bilişim ve Delillerin Toplanması", **Özyeğin Üniversitesi Hukuk Fakültesi Bilişim Hukuku Sertifika Programı Sunumu.** İstanbul, 18 Şubat-11 Mart 2012, ss. 1-69.

Gündüz, M. Zekeriya. "Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti", **Yayınlanmamış Yüksek Lisans Tezi.** Fırat Üniversitesi FBE, 2012.

Hargreaves, Christropher James. "Assessing The Reliability Of Digital Evidence From Live Investigations Involving Encryption", **PhD Thesis.** Cranfield University, 2009.

http://ahmeti.net/bit-byte-binary-decimal-ve-hexadecimal-nedir/ (21 Nisan 2015).

http://analog.nedir.com/ (21 Nisan 2015).

http://www.legislation.gov.uk/ukpga/1984/60/section/1 (03 Ocak 2015).

http://www.legislation.gov.uk/ukpga/1984/60/section/4 (03 Ocak 2015).

http://www.legislation.gov.uk/ukpga/1984/60/section/8 (03 Ocak 2015).

http://www.legislation.gov.uk/ukpga/1984/60/section/19 (03 Ocak 2015).

http://www.legislation.gov.uk/uksi/2008/2503/article/2/made (03 Ocak 2015).

Jarrett, H. Marshall and Michael W. Bailie. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations", http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf (21 Aralık 2014).

Kamışlık, Özgür. "Bilişim Hukukunda Delillerin Toplanması", **Ankara Barosu Uluslararası Hukuk Kurultayı.** Cilt. 2, Ankara, 08-11 Ocak 2008, ss. 158-189.

Karagülmez, Ali. "Bilişim Suçlarında Delil Toplamayı Etkileyen Başlıca Konular", **2. Polis Bilişim Sempozyumu.** Ankara, 14-15 Nisan 2005, ss. 30-34.

Keser Berber, Leyla. "Adli Bilişimle İlgili Olarak AB ve ABD'deki Yasal Düzenlemeler ve Kişisel Verilerin Korunması", **Bilişim Hukuku Konferansı-YARGITAY.** Ankara, 09-10 Ekim 2008, ss. 19-53.

Keser Berber, Leyla. "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El Koyma", **Ankara Barosu Avukatlık Akademisi Bilişim Hukuku Sertifika Programı 13. ve 14. Gruplar Sertifika Töreni.** Ankara, 9 Temmuz 2008, ss. 4-10.

Kessler, Gary Craig. "Judges' Awareness, Understanding, and Application of Digital Evidence", **PhD Thesis.** Nova Southeastern University, 2010.

Koç Serhat ve Selva Kaynak. "Bilişim Suçları Bağlamında Yeni Medya Olarak İnternet ve Kişisel Güvenlik", **Akademik Bilişim'10-XII. Akademik Bilişim Konferansı Bildirileri.** Cilt.1, Muğla, 10-12 Şubat 2010, ss. 71-78.

Koltuksuz, Ahmet Hasan. "Adli Bilişimde Olay Yeri İnceleme Esasları", **Bilişim Hukuku Konferansı-YARGITAY.** Ankara, 09-10 Ekim 2008, ss. 9-18.

Kozushko, Harvey. "Electronic Evidence", 2003. http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/DigitalEvidencePaper.pdf (12 Kasım 2013).

Listrom, Linda L., Eric R. Harlan, Elizabeth H. Ferguson and Robert M. Redis, "The Next Frontier: Admissibility of Electronic Evidence", ABA Annual Meeting, Summer 2007, http://www.mccarthyfingar.com/files/20110129123145-A%20B%20A%20(00276545).PDF (19 Ocak 2015).

Mason, Stephen. "Bilişim Hukukunda Delillerin Toplanması", **Ankara Barosu Uluslararası Hukuk Kurultayı.** Cilt. 2, Ankara, 08-11 Ocak 2008, ss. 158-189.

Member States of the Council of Europe, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (01 Ocak 2015).

Orta, Mesut, "Bilişim Suçlarında İspat", **1. Polis Bilişim Sempozyumu.** Ankara, 21-22 Ekim 2003, ss. 288-292.

Oseles, Lisa. "Computer Forensics: The Key to Solving the Crime", 2001, http://faculty.ed.umuc.edu/~meinkej/inss690/oseles_2.pdf. (9 Ocak 2013).

Önal, Huzeyfe. "Bilişim Suçlarında IP Adresi Analizi-Adli Bilişim Açısından IP Adresleri", 2010, http://www.bga.com.tr/calismalar/ip_forensic.pdf (18 Ocak 2015).

Özbek, Murat. "Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları", **1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu.** Elazığ, 20-21 Mayıs 2013, ss. 1-7.

Özbek, Onur. "Hukuk Devletinde Bireysel Güvenlik Ekseninde Bilişim Teknolojileri", **1. Hukukun Gençleri Sempozyumu (Hukuk Devletinde Kişisel Güvenlik).** Ankara, 20-21 Mart 2009, http://www.umut.org.tr/tr-TR/hukukun-gencleri-sempozyumlari-dizisi--1-hukuk-devletinde-kisisel-guvenlik/111. aspx (25 Şubat 2015).

Özdemir, Mehmet. "Bilişim Suçları ve Mücadelede Taşra Teşkilatında Karşılaşılan Problemler ve Çözüm Önerileri", **1. Polis Bilişim Sempozyumu.** Ankara, 21-22 Ekim 2003, ss. 284-287.

Özel Cevat ve M. Gökhan Ahi. "Bilişim Suçlarında Usul ve Sorumluluk Sistemi Üzerine Öneriler", http://www.turkhukuksitesi.com/makale_179.htm (6 Eylül 2014).

Özgen, Eralp. "Askeri Yargıtay Kararlarına Göre Delil Değerlendirmesi ve Savunma Hakkı", **Askeri Yargıtay'ın 80'inci Kuruluş Yıl Dönümü Sempozyumu.** Ankara, 6-7 Nisan 1994, ss.75-101.

Özocak, Gürkan. "Ceza Muhakemesinde Elektronik Delillerin Tespiti ve Toplanması". **İzmir 2. Uluslararası Bilişim Hukuku Kurultayı.** İzmir, 17-19 Kasım 2011, ss. 110-125.

Öztunç, Özgün. "Ceza Muhakemesinde Hukuka Aykırı Deliller", **Yayınlanmamış Doktora Tezi.** Marmara Üniversitesi SBE, 2010.

Öztürk, Mustafa İlker. "Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri", **Yayınlanmamış Yüksek Lisans Tezi.** Ankara Üniversitesi SBE, 2007.

Rand Europe & Lawfort. "Update to the Handbook of Legal Procedures of Computer and Network Misuse In Eu Countires For Assiting CSIRT, D: 15 Final Report", 2005. ftp://ftp.cordis.europa.eu/pub/ist/docs/directorate_d/trust-security/ec-csirt-d15.pdf (01 Ocak 2015).

Say, Kubilay. "Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi", **Yayınlanmamış Yüksek Lisans Tezi.** Ankara Üniversitesi SBE, 2006.

Şahin, Cumhur. "Telekomünikasyon Yoluyla İletişimin Denetlenmesi-Yargıtay Kararları Çerçevesinde Bir Değerlendirme", **Bilişim Hukuku Konferansı-YARGITAY.** Ankara, 09-10 Ekim 2008, ss. 123-135.

Şen, Bilal. "Elektronik Ekipmanlarda Arama El Koyma ve Elektronik Deliller", **Ankara Barosu Uluslararası Hukuk Kurultayı.** Cilt. 3, Ankara, 11 Ocak-15 Ocak 2010, ss. 69-70.

Şen, Osman Nihat. "Polisin Adli Bilişimde Kullanabileceği Programların Bir Değerlendirmesi", **2. Polis Bilişim Sempozyumu.** Ankara, 14-15 Nisan 2005, ss. 35-41.

Tan, Aydoğan. Adli Bilişim (Computer Forensic), 2009, http://mbasic.facebook.com/notes/gazi-%C3%BCniversitesi-adli-bili%C5%9Fim-anabilim-dal%C4%B1/adli-bili%C5%9Fim-computer-forensic-aydo%C4%9Fan-tan/ 502561823148516/?refid=17 (06 Nisan 2014).

Tulum, İsmail. "Bilişim Suçları ile Mücadele", **Yayınlanmamış Yüksek Lisans Tezi.** Süleyman Demirel Üniversitesi SBE, 2006.

Turan, Serhat. "Bulut Bilişim (Cloud Computing) Teknolojisi ve Güncel Hukuki Problemler", (t.y.) http://www.egeweb.com/bulut-bilisimi-cloud-computing-teknolojisi-ve-guncel-hukuki-problemler-y17.html (23 Kasım 2014).

Turhan, Oğuz. "Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar)", **Yayınlanmamış Planlama Uzmanlığı Tezi.** Başbakanlık Devlet Planlama Müsteşarlığı Hukuk Müşavirliği, Ankara, 2006.

Türk Dil Kurumu. http://www.tdk.gov.tr/tdksozluk/sozbul.ASP?kelime (02 Ekim 2014).

Uzunay, Yusuf. "Dijital Delil Araştırma Süreci", **2. Polis Bilişim Sempozyumu.** Ankara, 14-15 Nisan 2005, ss. 42-47.

Uzunay, Yusuf. "Bilgisayar Ağlarına Yönelik Adli Bilişim", **İzmir Yüksek Teknoloji Enstitüsü Adli Bilişim Çalıştayı.** İzmir, 19-20 Mayıs 2005, ss. 1-9.

Uzunay, Yusuf ve Kemal Bıçakçı. "A3D3M: Açık Anahtar Altyapısı Destekli Dijital Delilleri Doğrulama Modeli", **Ağ ve Bilgi Güvenliği Ulusal Sempozyumu.** İstanbul, 9-11 Haziran 2005, http://www.emo.org.tr /ekler/ 4843973f9b66701ek. pdf. (31 Ekim 2014).

Uzunay, Yusuf ve Mustafa Koçak, "Bilişim Suçları Kapsamında Dijital Deliller", **AB'05 Akademik Bilişim Konferansı.** Gaziantep, 31 Ocak - 4 Şubat 2005, http://ab.org.tr/ab05/tammetin/134.pdf. (30 Ekim 2014).

Ünal, Osman Gazi, "Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma", **Yayınlanmamış Yüksek Lisans Tezi.** Gazi Üniversitesi SBE, 2011.

Yargıtay C.G.K. 19.04.1993. E. 1993/6-79, K. 1993/108, (**Yargıtay Kararları Dergisi,** Cilt. 19, Sayı. 10, Ekim 1993), ss. 1564-1565.

Yargıtay C.G.K. 29.11.2005. E. 2005/7-144, K. 2005/150 (**Yargıtay Kararları Dergisi,** Cilt. 32, Sayı. 3, Mart 2006), ss.460-486.

Yaycı, Esra. "Bilişim Suçları", **Yayınlanmamış Yüksek Lisans Tezi.** Gazi Üniversitesi SBE, 2007.

Yıldız, Ali Kemal. "Ceza Muhakemesinde İspat ve Delillerin Değerlendirilmesi", **Yayınlanmamış Doktora Tezi.** İstanbul Üniversitesi SBE, 2002.

Yıldız, Sevil. "Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi", **Yayınlanmamış Doktora Tezi.** Selçuk Üniversitesi SBE, 2006.

Zaman Damgası Nedir ?. (t.y) https://www.turktrust.com.tr/zaman-damgasi.html (24 Ekim 2014).

ÖZGEÇMİŞ

Yusuf Başlar 1981 yılında İstanbul ili Kadıköy ilçesinde doğmuştur. İlk ve orta öğrenimini Konya'da tamamlamıştır. 1998-2002 yılları arasında Marmara Üniversitesi Hukuk Fakültesinde lisans eğitimini tamamlamıştır. Adalet Bakanlığının 2004 yılında açmış olduğu Hâkimlik ve Savcılık sınavını kazanarak 2004-2006 yılları arasında Ankara Adliyesinde savcılık stajını tamamlamış ve akabinde 2006 yılında Cumhuriyet Savcılığı görevine başlamış olup halen Mersin ili Silifke ilçesinde Cumhuriyet Savcısı olarak görev yapmaktadır. 2005-2008 yılları arasında Kırıkkale Üniversitesi Sosyal Bilimler Enstitüsü Özel Hukuk Bölümünde yüksek lisans, 2010-2015 yılları arasında Sakarya Üniversitesi Sosyal Bilimler Enstitüsü Siyaset Bilimi ve Kamu Yönetimi Bölümünde doktora eğitimini tamamlayan yazar evli ve iki çocuk babasıdır.