ISSN: 2149-6021 INTERNATIONAL JOURNAL OF LEGAL PROGRESS www.intjolep.com

Volume: 1 Year: 2015 Number: 2

MAKALE

SAYISAL DELİLİN ORTAYA ÇIKARILMASI KAPSAMINDA KORUMA TEDBİRLERİ

(Revealing of Digital Evidence and Search as a Protective Measure)

Engin ŞAHİN[**]

Doi number: http://dx.doi.org/10.20978/ijlp.80518

[*] Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Bilişim Hukuku Yüksek Lisans Öğrencisi
[*] skorzny@hotmail.com

ISSN: 2149-6021 INTERNATIONAL JOURNAL OF LEGAL PROGRESS www.intjolep.com

Volume: 1 Year: 2015 Number: 2

ÖZET

Ceza muhakemesi hukukunda delil serbestisi ilkesi geçerlidir. Buna göre, hukuka uygun şekilde elde edilen her türlü delil, ispat aracı olarak kullanılabilecektir. Delillerin bulunması, analiz edilmesi, elde edilen delillerin özellikleri adli tıp, adli bilişim ve adli psikoloji gibi alt bilim dallarının oluşmasına neden olmuştur. Adli olayların sayısal sistemler üzerinde incelenmesi ve delillendirilmesini sağlayan adli bilişim kavramı; disket, sabit disk ve çıkartılabilir disklerden delil elde etme amacıyla veri kurtarma, kopyalama, belirleme, çözümleme, yorumlama ve belgeleme süreçlerine karşılık gelmektedir. Sayısal delil ve buna ilişkin koruma tedbirleri ise; "adli bilişim" başlığı altında inceleme yapılan bir çalışmadır.

Bu çalışmada, sayısal delil kavramı, sayısal delilin ortaya çıkarılması ve bu ortaya çıkarılma sürecinde bir koruma tedbiri olarak arama ve türleri incelenecektir.

Anahtar kelimeler: sayısal delil, adli bilişim, adli tıp, adli bilişim, adli psikoloji.

ABSTRACT

Principle of freedom of evidence is applicable in law of criminal procedure. According to this principle, any evidence which was obtained lawfully can be used as a means of proof. Subdivisions such as forensic medicine, forensic information and forensic psychology have developed as a result of finding, analyzing and Characteristics of evidence. The Concept of forensic informatics which enables forensic cases to be evidenced on digital systems correspondes the processes of rescuing, copying, determination, analyzing, interpreting the data with a View to obtaining the evidence from disk, hard disk and removable disks. Digital evidence and related protective measures is studied under the title of forensic informatics.

The Concept of digital evidence, revealing of digital evidence and search as a protective measure will be analyzed in this study.

Keywords: digital evidence, forensic informatics, forensic medicine, forensic information, forensic psychology.

GİRİŞ

Ceza yargılamasında, adli makamlar karşılaştığı olaylarda öncelikle somut olayın maddi yönünü tespit etmekte, daha sonra bunun hukuki nitelendirmesini yapmaktadır. Bu nedenle ceza mahkemeleri sırasıyla fiilin işlenip işlenmediğini, işlenmişse kanunda suç olarak tanımlanıp tanımlanmadığını, tanımlanmışsa fiilin sanık tarafından gerçekleştirilip gerçekleştirilmediğini tespit edecektir.[1] Kanunlarda suç olarak tanımlanan fiili işlediği sabit görülen sanık mahkûm edilecek, sabit görülmeyen ise beraat edecektir. Hâkimin belirtilen sonuçlara ulaşmasını sağlayacak ispat araçlarına delil denmektedir. Ceza muhakemesi hukukunda delil serbestisi ilkesi geçerlidir. Buna göre, hukuka uygun şekilde elde edilen her türlü delil, ispat aracı olarak kullanılabilecektir.

Ceza Muhakemesi hukukunda delillerin bulunması, analiz edilmesi, elde edilen delillerin özellikleri adli tıp, adli bilişim ve adli psikoloji gibi alt bilim dallarının oluşmasına neden olmuştur.[2]

Adli olayların sayısal sistemler üzerinde incelenmesi ve delillendirilmesini sağlayan adli bilişim[3] kavramı; disket, sabit disk ve çıkartılabilir disklerden delil elde etme amacıyla veri kurtarma, kopyalama, belirleme, çözümleme, yorumlama ve belgeleme süreçlerine karşılık gelmektedir. Bununla birlikte, adli bilişimi, "bilgi güvenliği" ana başlığının altında hukuk ve bilgisayar güvenliği birimlerinin toplamı olan bir alt bilim dalı olarak tanımlayabilmek mümkündür.[4] Adli bilişim alanının içerisine dâhil uygulamadaki örneklere bakıldığında; intihar etme gibi bir eylemden, uyuşturucu tacirleri arasındaki iletişimlerinin ortaya çıkarılmasına, sosyal medya ortamında hakaretten, bir bankanın veri tabanındaki bilgilerin saldırganlarca ele geçirilmesine ve hatta siber saldırı yöntemleri kullanılarak bir ülkenin diğer bir ülkenin bilgisayar sistemlerini çökertmesine kadar oldukça geniş örneklere

1 Bkz. ÖZEN, M. / ÖZOCAK, G..: "Ali Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)", *Ankara Barosu Dergisi,* Y. 2015, S. 1, s. 56.
2 ÖZEN / ÖZOCAK, s. 44.
3 ŞENGÜL G.. / ATSAN F. K. / BOSTAN, A.: "Adli Bilişim Alanındaki Mevcut Problemler, Çözüm Önerileri ve Gelecek Öngörüleri", *7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı,* 17-18 Ekim 2014, Bildiriler Kitabı, s. 95.
4 Bkz. ÖZEN / ÖZOCAK, s. 45.

rastlamak mümkündür.[5] Sayısal delil ve buna ilişkin koruma tedbirleri ise "adli bilişim" başlığı altında inceleme yapılan bir çalışmadır.

Bu bağlamda çalışmada, sayısal delil kavramı, sayısal delilin ortaya çıkarılması ve bu ortaya çıkarılma sürecinde bir koruma tedbiri olarak arama ve türleri incelenecektir.

SAYISAL DELİL KAVRAMI

"Sayısal delil[6]*, bir davadaki konularla ilgili olarak, örneğin bilgisayar hard diskine, CD'ye, USB'ye ve benzeri unsurlara elektronik şekilde (formda) depolanmış bilgidir. Bir başka tanıma göre sayısal delil, yasal bir davada kullanılabilen herhangi bir bilgisayar aygıtındaki elektronik olarak depolanmış bilgidir. 2001 yılında Fransa'nın Lyon şehrinde yapılan 13. Interpol Adli Bilişim Sempozyumunda 'sayısal delil, elektronik delil, elektronik yapıdaki bir iletimi veya depolanmış değeri kanıtlayan bilgidir' şeklinde tanımlanmıştır."*[7]

Elde edildikleri kaynaklara ve kullanım amaçlarına göre değişkenlik gösteren sayısal veriler, genellikle bilişim sistemlerinden ve belli bir hafızaya sahip elektronik aygıtlardan elde edilir. Bu veriler, kişiler tarafından kaydedilen, biriktirilen veya transfer edilen bilgilerden ya da kullanıcıların bu sistem ve aygıtları kullanarak bıraktığı dijital izlerden oluşabilir. Belirtmek gerekir ki, sayısal veriler bilişim suçlarının yanı sıra her çeşit suçun aydınlatılmasında kullanılabilmektedir. Bu bağlamda sayısal bir veriden yola çıkılarak hırsızlık, dolandırıcılık, adam öldürme, cinsel suçlar, uyuşturucu ticareti gibi birçok suç çözülebilir.[8]

CMK'da sayısal delillerden veya sayısal delilin kaynağı olan verilerden bahsedilmemekte ancak CMK'nın delil elde etme konusundaki sistematiğinden anılan delillere ilişkin çıkarımda bulunabilmemiz mümkündür. Bilişim sistemlerinde yer alan veriler olan sayısal deliller;

- Üçüncü kişilerde,

5 EMEKCİ, A. / KUĞU, E.: "Adli Bilişim ve Etmen Tabanlı Sistemler", *7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı,* 17-18 Ekim 2014, Bildiriler Kitabı, s. 66.

6 Bu kaynağın ve diğer kaynakların orijinal halinde geçen "elektronik delil" ibareleri çalışmanın kavramsal bütünlüğün sağlanabilmesi açısından "sayısal delil" olarak kullanılmıştır.

7 Bkz. KARAGÜLMEZ, A.: *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, Seçkin, Ankara, 2009, s. 288-289.

8 Bkz. KIZILYAR, M.: "Ceza Yargılamasında Dijital Verilerin Delil Değeri", *Adalet Dergisi*, Y. 2014, S. 50, s.79.

- Akış halinde veya
- Durağan halde bulunabilmektedir.

Bu bağlamda sayısal veriler şüphelinin kullandığı bilişim sitemlerinde durağan halde bulunabilmektedir. Bu şekilde durağan halde bulunan delillere ulaşma CMK'nın 134. maddesi kapsamında uygulanabilecektir. Sayısal veriler şüphelinin kullandığı bilişim sistemi ile diğer başka bilişim sitemlerinin iletişimi esnasında akış halinde de bulunabilmektedir ve bu durumda CMK'nın 135. maddesi kapsamındaki tedbir uygulamaya sokulacaktır. Bu maddelerin kapsamına girmeyen sayısal deliller ise, Cumhuriyet savcısının genel delil toplama yetkisi kapsamında değerlendirmeye tabi tutulacaktır. Bu bağlamda; bazı verilerin niteliğinden kaynaklanan farklı bir durum gündeme gelebilmekte; elektronik postalar gibi bazı veriler iki sunumcu arasında akış halinde iken alıcının hesabına ulaştıktan sonra durağan hale gelebilmektedirler.[9]

Fiziksel delillerin kural olarak sabit bir yapıya sahip olmaları dolayısıyla yapısal olarak değiştirilmeleri zorken, sayısal delillerin bilgisayara ve uzun iletişim hatları içerisinde her an yapılarının değiştirilmeleri mümkün gözükmektedir. Fiziksel delillerde mümkün olan bir değişiklik yapıldığında söz konusu değişikliğin fark edilmesi kolayken, elektronik delillerin yapılarında hiçbir iz bırakmaksızın kolaylıkla değişiklik yapılabilmektedir. Yine fiziksel delillere nazaran, sayısal deliller özellikle elde edilme aşamasında kolaylıkla değişikliğe uğrayabilmekte olup, bu sebeple sayısal delillerin elde edilmesi sırasında çok dikkatli davranılmalıdır. Elektronik deliller elde edildiklerinde insanlar tarafından hemen okunması mümkün olmamakta ve içeriği hakkında bilgi sahibi olunamamaktadır. Sayısal delillerin genellikle bilgisayar çıktısı alındıktan sonra belli şekillerde ilk bilgileri görülebilmektedir. Ancak bazen söz konusu çıktılar alınsa dahi kolluk görevlileri tarafından bir rapor düzenlememişse delillerin anlaşılırlık düzeyi düşük olabilmektedir.[10] Söz konusu kolluk görevlileri, bilişim alanında özel eğitim ve uzmanlığa sahip görevliler olup, uygulamada anılan delillerin elde edilme aşamasında bu konuda eğitilmemiş kolluk görevlilerince işlemlerin yapılması var olan verilerin değiştirilmesine veya yok olmasına neden olabilmektedir.

Sayısal deliller üzerinde yapılacak incelemeler, elektronik delilin adli bir kopyasından yapılmaktadır. Bu sebeple, orijinal delil üzerinde bulunan verilerin değişmemesi için orijinal

9 DEĞİRMENCİ, O.: *Ceza Muhakemesinde Sayısal (Dijital) Delil,* Seçkin, 2014, s. 309-310.
10 Bkz. KARAGÜLMEZ, s. 289-290.

delil üzerinde inceleme yapılmamaktadır. Ancak konuya ilişkin ilgili istisnai durumlar bulunmaktadır.[11] Anılan durum sayesinde depolanmış durumda bulunan sayısal delillerin değişmemesi veya yok olmaması sağlanır. Tabiidir ki, delillerin hukuki sürecin ilerleyen safhalarında da ihtiyaç duyulması halinde (yargılamanın yenilenmesi, temyiz, ikinci bir bilirkişi incelemesine ihtiyaç duyulması vb.) ispat aracı olarak kullanılabilmesi için kullanılabilir bir durumda muhafaza edilmeleri gereklidir.

Bunun yanı sıra, adli bilişim kapsamında sayısal sistemler üzerinde inceleme yapıp, delil araştırmak karmaşık sayılabilecek nitelikte teknik bilgiye ve bazı özel cihaz, sistem ve yazılımlara da sahip olmayı beraberinde gerektirmektedir. Bunun yanında, sayısal sistemlerdeki veri ve kayıtların boyutların da büyük olmasından dolayı değinilen safhalar esasında oldukça zahmetli ve zaman alıcı olabilmektedir.[12]

SAYISAL DELİLİN ORTAYA ÇIKARILMASI

Sayısal delillere ulaşılacak kaynaklar çeşitli olup bunların başlıcaları; bilgisayar (diz üstü dahil), monitör, PDA (taşınabilir küçük bilgisayar), bilgisayar bağlantılı makineler, yazıcı, akıllı kart, modem, telesekreter, hard drive keyboard, disk gibi bilgisayarlarda depolanan alanlar, faks tarayıcısı, fotokopi makinası, otomatik bilgi giriş terminalleri ve bilgisayar günlükleri, kontrol erişim listeleri, intranet bağlantıları, çağrı cihazları, kablosuz cihazlar, bilgi yüklenebilen dijital saatler ve sürekli eklenen yeni teknoloji ürünleri vb.[13]

Sayısal delilin elde edilmesi, yeni bir konu olması nedeni ile hem tartışmalı hem de az bilinen bir konudur. Ülkemizde bilişim teknolojilerinin gerekli alt yapı olmadan ithal edilmesi, bu alanda işlenen suçların kapsamlarının yeterince bilinmemesi gibi nedenlerle sayısal delilin nasıl ortaya çıkarılacağına ilişkin kapsamlı bir yasal düzenleme bulunmamaktadır.[14]

Yukarıda da değinildiği üzere adli bilişimin kapsamı oldukça geniş olup; bilgisayar ve bilişim teknolojileri kullanılarak işlenen fiillerin ilk işlendiği andan başlayarak analiz edilerek verilerin toplanması, toplanan verilerin incelenmesi, sonucunda fiillerin suç teşkil etmesi halinde ilgili suçla ilişkilendirmeler yapılarak varılan sonuçların rapor halinde soruşturma

11 Bkz. ÖZBEK, M.: "Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları", 1st International Symposium on Digital Forensics and Security (ISDFS'13), 20-21 May 2013, s. 2.
12 ŞENGÜL / ATSAN / BOSTAN, s. 95.
13 Bkz. KARAGÜLMEZ, s. 292.
14 KARAGÜLMEZ, s. 299.

veya kovuşturma makamlarına sunulması hususlarının yanı sıra bilişim teknolojilerine ilişkin güvenliğin sağlanmasına kadar yapılan birçok işlem bu kapsama dâhildir.[15] Anılan işlemler yerine getirilirken Aşağıda yer alan süreçlere uyulması önem arz etmektedir:

- *Delillerin bulunduğu ortamın boşaltılması ve kamera ile sürecin takip edilmeye başlanması gerekmektedir.*
- *Delillerin toplanması bağlamında, plastik eldivenler vasıtası ile gerekli bilgisayarın açılması, açılış sürecinin analizi, açılmışsa o anki durumunun tayini, var olan kablosuz bağlantıların hemen tespit edilip kapatılıp kapatılmayacağına karar verilmesi, gerekli delil toplama işlemlerinin üstün yetenekli programlar vasıtası ile yapılması ve bilgisayarın kapatılması süreçlerinin tamamı, adli birimler tarafından belirlenmiş sistematiğe göre yapılıp raporlanmalıdır.*
- *Elde edilen deliller, programlar vasıtası ile incelenmeli ve gerekiyorsa şifre çözme yöntemleri kullanılmalıdır.*
- *Analiz sonucu ortaya konulan rapor, adli birimlere, anlaşılır bir biçimde ve teknik terimlerden gerektiğince kaçılarak sunulmalıdır.*[16]

Tüm bu süreçlerden sonra gelinen safhada sayısal delilin ortaya çıkarılması sürecinde arama ve elkoyma gibi koruma tedbirleri gündeme gelmektedir.

Ancak değinmek gerekir ki; elektronik ortamda bulunan delillerin kısa süre içerisinde karartılabilir olma özellikleri itibariyle bu olasılığı en alt seviyeye düşürebilecek koruma tedbirlerinin bulunması ve bu hassasiyete uygun bir şekilde uygulanması gereklidir.[17] Yine sayısal delilin elde edilmesine ilişkin koruma tedbirlerinin gerek özel bilgi gerektirmesi ve hızlı işleyen usulü niteliğe sahip olmaları gerekse de elde edilen verilerin ceza yargılamasında delil olarak kullanılmaları sebebiyle bu tedbirlerin kullanılmasını içeren düzenlemelerde hem sayısal delillerin kullanıldığı suçlarla mücadeleye imkan verecek hem de bunu yaparken kişi temel hak ve özgürlüklerine müdahale niteliğindeki bu işlemlerin ölçülülük ilkesine bağlı kalarak uygulanmasını sağlayan yasal düzenlemelere ihtiyaç duyulmaktadır.[18]

15 Bkz. YAŞAR, Y. / DURSUN, İ.: "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri", *MÜHF*, C. 19, S. 3, s. 7.
16 Bkz. ÖZEN / ÖZOCAK, s. 51-52.
17 BAŞLAR, Y.: "Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri", *Uyuşmazlık Mahkemesi Dergisi*, Y. 2013, s. 82.
18 BAŞLAR, s. 101-102.

SAYISAL DELİLİN ORTAYA ÇIKARILMASI KAPSAMINDA KORUMA TEDBİRLERİ

a. Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma

Arama koruma tedbiri, genel bir düzenleme olarak, 5271 sayılı Ceza Muhakemesi Kanunu'nun 116. maddesiyle 122. maddesi arasında yer almaktadır. 134. maddede ise; "bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma" ayrı bir koruma tedbiri olarak düzenleme altına alınmıştır.

CMK'nın 134. maddesinde düzenlenen koruma tedbiri, aslında 116 ve 123. maddelerinde düzenlenen arama ve elkoyma koruma tedbirlerinin özel bir şeklini oluşturmaktadır.[19] Zira bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbiri özel koşullara bağlı, son çare olarak başvurulabilecek bir koruma tedbiri niteliğine sahip olup, CMK'nın 116 ve 134. maddeleri arasında düzenlenen arama ve elkoyma tedbirlerinde yer alan genel hükümler, niteliğine uygun düştüğü ve bu hükümlerin aksine bir düzenleme bulunmadığı ölçüde özel nitelikteki bilgisayarlarda ve bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma koruma tedbiri açısından da uygulanabilmektedir.[20] Bu bağlamda elinizdeki bu çalışmada CMK'da düzenlenen genel arama ve türleri değil, söz konusu mecralarda işlenen suçların niteliğinden kaynaklanan ve bu suçlara özgü düzenlenen bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma tedbiri incelenmektedir.

Anılan maddede somut delillere dayanan kuvvetli şüphe sebeplerinin soruşturma esnasında varlığı ve başka surette delil elde etme imkânının bulunmaması koşullarının birlikte bulunması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılacağı, bilgisayar kayıtlarından kopya çıkarılacağı ve hâkim kararı ile anılan kayıtların çözümlenerek metin haline getirileceği düzenlenmiştir. Bu bağlamda değinilen düzenlemenin kişinin temel hak ve özgürlüklerini koruma altına almak amaçlı getirildiği aşikârdır. "*Yalnızca soruşturma evresinde başvurulabilen bu tedbir ile başka türlü elde edilemeyen delil elde edilmiş olacaktır. Bu tedbire yalnızca soruşturma evresinde başvurulabileceği üzere, hakim veya mahkeme*

19 YAŞAR / DURSUN, s. 3.
20 YAŞAR / DURSUN, s. 3.

tarafından re'sen tedbirin uygulama alanı bulması mümkün olmayıp, Cumhuriyet savcısının istemi gerekmektedir."[21]

Maddede geçen somut delil ibaresi, 21/02/2014 tarihli değişiklikle maddeye eklenmiştir. Metne yapılan ekleme ile değinilen koruma tedbirinin uygulanması zorlaştırılmak istenmiş olup, anılan tedbire başvurulup, karar verilirken çok dikkatli ve titiz olunması gerekir. Aksi takdirde deliller hukuka aykırı olarak elde edilmiş delil niteliğine bürünecek ve bu haliyle de kullanılmaları mümkün olmayacaktır.[22]

Kişilerin sahibi olduğu şahsi bilgisayarları incelendiğinde, bilgisayarı kullanan kişinin özel verilerine ulaşmak kuvvetle muhtemel görülmektedir. Dolayısıyla şahsi bilgisayar, özel hayatın önemli bir unsuru niteliğine haiz olup; sahibinin günlüğü, düşünceleri, fotoğrafları ve özel niteliğe sahip birçok verisinin depolandığı bir bilgisayar olma özelliğine sahiptir. Ancak bilgisayarlar programları ve kütüklerinde yapılan bir arama, işlenen bir suç ile ilgili önemli ve gizli nitelikteki önemli delillerin ortaya çıkarılmasına hizmet de etmektedir. Söz konusu tedbir, kişinin temel hak ve özgürlüklerine doğrudan müdahalede niteliğine de sahiptir ve anılan tedbir 1982 Anayasası'nın 20. maddesiyle yakından ilgilidir.[23] Anılan maddede herkesin özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu ve özel hayatın ve aile hayatının gizliliğine, bazı istisnalar haricinde, dokunulamayacağı düzenlemiştir. Maddenin ikinci fıkrasında yer verilen istisnalar; "*Milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kağıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hakimin onayına sunulur. Hakim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar."* şeklinde genel bir hüküm niteliğine sahip olarak belirtilmiştir.

---

21 YAVUZCAN, E.: "Bilgisayarlarda, Bilgisayar Programlarında Ve Kütüklerinde Arama, Kopyalama Ve Elkoyma (CMK 134)", s. 2. Ayrıntılı Bilgi İçin Bkz. http://www.hukuki.net/hukuk/index.php?act=file&id=4&article=3242 , (Erişim Tarihi: 02/11/2015).

22 DÜLGER, M. V.: "Bilişim Sistemleri Üzerinde Arama, Kopyalama ve El Koyma Tedbiri", s. 6. Ayrıntılı Bilgi İçin Bkz. https://www.academia.edu/9449240/B%C4%B0L%C4%B0%C5%9E%C4%B0M_S%C4%B0STEMLER%C4%B0_%C3%9CZER%C4%B0NDE_ARAMA_KOPYALAMA_VE_EL_KOYMA_TEDB%C4%B0R%C4%B0 (Erişim Tarihi: 06/11/2015)

23 YAVUZCAN, s. 2.

Yine maddede açık bir şekilde düzenlendiği üzere anılan tedbirin uygulanmasına hâkim karar verecek olup, bu tedbirin diğer koruma tedbirlerinden ayrılan temel özelliklerinden birisi bu tedbirin uygulanabilmesine karar verme yetkisinin sadece hâkimde olması durumudur. CMK'da düzenlenen arama ve elkoyma hükümlerinden farklı olarak; gecikmesinde sakınca bulunan hallerde dahi savcının anılan tedbire karar verme yetkisi bulunmamaktadır. Yine hâkim tarafından verilen CMK'nın 119. maddesi kapsamındaki bir arama kararıyla şüpheliye ait bilgisayar, bilgisayar programları ve kütüklerinde arama, kopyalama ve elkoyma işlemlerinin yapılması mümkün değildir. Söz konusu karar mutlaka 134. madde kapsamında alınacak bir karar olmalıdır.[24]

Maddenin devamında bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, anılan araç ve gereçlere elkonulabileceği ve şifrenin çözümünün yapılarak, gerekli kopyaların alınması durumunda elkonulan cihazların gecikme olmaksızın iade edileceği düzenleme altına alınmıştır. Yine söz konusu elkoyma işlemi sırasında sistemde bulunan tüm verilerin yedeklemesinin yapılacağı ve bilgisayar veya bilgisayar kütüklerine elkoymaksızın da sistemdeki verilerin tamamının veya bir kısmının kopyasının alınabileceği düzenlenmiştir. Ancak buradaki elkoyma işlemi, şifre çözümü yapıldıktan ve gerekli olan kopyalar alındıktan sonra gecikme olmaksızın elkoyulan araç ve gereçlerin ilgilisine iade edilmesi kaydıyla mümkün olan bir elkoyma işlemidir. Özetle; "*şifrenin çözülememesi ve nihayetinde gizli olan verilerin incelenememesi durumunda fiziksel olarak bilgisayarın kendisine, harici belleklere veyahut sair araç ve gereçlere elkonulabileceği belirtilmiştir. Elkoyma işlemi geçici nitelikte olup, şifrelemenin çözümlenmesi ve kopyalamanın yapılmasının ardından bu tedbire son verilir. Kanun koyucu elkoyma işlemi bakımından süre limiti koymamış olup, gerekli işlemlerin yapılmasının ardından "gecikme olmaksızın" şeklindeki ibare ile durumu açıklığa kavuşturmuştur. Tüm bu işlemlerin de makul sürede yapılması gereği tartışmasızdır."*[25]

Maddenin eski halinde yer alan, bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesinin yapılacağı ve istemesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline (bu husus tutanağa geçirilerek ve imza altına alınarak) verileceği düzenlenmiştir. Bu durumda elkoyma işlemini gerçekleştiren kolluk

24 YÜCETÜRK, B.: "Soruşturmalarda Bilgisayara Elkoyma", *Bilişim Dergisi,* S. Nisan, Y. 2014, s. 104.
25 YAVUZCAN, s. 2.

görevlilerinin alınan yedekten bir kopya vermek gibi bir zorunluluğu bulunmamakta olduğu açık iken; 21/02/2014 yılında yapılan değişiklikle üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verileceği ve bu hususun tutanağa geçirilerek imza altına alınacağı düzenlenmiştir. Yapılan değişiklikle kopya verilmesi bir zorunluluk haline getirilmiş olup, getirilen düzenleme eski haline nazaran oldukça olumlu gözükmektedir.

Maddenin son fıkrasında; bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyasının alınabileceği, kopyası alınan verilerin kâğıda yazdırılarak, bu hususun tutanağa kaydedileceği ve ilgililer tarafından imza altına alınacağı düzenlenmiştir.

Burada bahsedilen son çare olarak bu koruma tedbirine başvurulması konusu, diğer koruma tedbirleri uygulanarak delil elde etme imkânı söz konusuysa kişisel bilgileri de içermesi çok yüksek olan bu tedbire başvurulmaması ancak diğer tedbirlerle veya yöntemlerle delil elde edilebilmenin mümkün olmaması halinde bu tedbire başvurma anlamına gelmektedir. Söz konusu vurgu maddede "*başka surette delil elde etme imkânının bulunmaması*" ifadesi ile verilmiştir.

Yukarıdaki maddede değinilen kuvvetli şüphe, şüpheli tarafından soruşturmaya konu suçun işlendiği ve üzerinde arama yapılacak bilgisayarda o suça dair delillerin bulunacağı yönde kuvvetli şüphe olarak algılanmalıdır.[26]

Anılan madde bilgisayarlarda önce yerinde inceleme/arama yapılmasını, bu şekilde delil elde edilmesi mümkün olmazsa yani bilgisayar, bilgisayar programları ve bilgisayar kütüklerinde bulunan şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması durumları söz konusuysa bilgisayarlara elkonulmasını öngörmektedir. Bilgisayarda yerinde inceleme yapılması çoğu kez mümkün olmadığından, delilleri korumak ve şüphelinin mağduriyetini önlemek amacıyla tüm önlemlerin alınarak bilgisayara elkonulması ve teknik uzmanlar tarafından laboratuvar ortamında incelenmesinin daha uygun olacağı ileri sürülerek, bahsi geçen hükmün aslında teknik anlamda içerisinde hata barındırdığı bazı yazarlar tarafından ileri sürülmektedir.[27]

Başka bazı yazarlar tarafından, anılan fıkranın açık bir şekilde istisna düzenlemesine rağmen, bilişim sistemlerinde yapılan aramalarda değinilen istisnanın kural haline

26 Bkz. ÖZEN / ÖZOCAK, s. 62.
27 Ayrıntılı bilgi için Bkz. ÖZEN / ÖZOCAK, s. 63.

getirildiğini, kolluk güçlerinin CMK'nın 134. maddesi bağlamında yaptıkları aramaların tamamında ikinci fıkradaki istisna hükmünü işletmekte ve arama yapacakları bilişim sisteminde şifre olduğuna ilişkin işleme katılan diğer kolluk güçleriyle birlikte tutanak tutarak yasayı dolandıkları ancak bu şekilde elde edilen delillerin hukuka aykırı nitelikte delil olduğu ileri sürülmektedir. Bunun gerekçesi olarak ise; tutulan tutanaklarda şifrenin veya gizli verinin türünün, bunların neden işin uzmanı niteliğindeki bilişim polisi tarafından etkisiz kılınamadığına dair herhangi bir kayıt yer almadığı ve tutulan tutanakların gerçekçi ve denetlenebilir bir tarafı olmadığını, yapılan işlemin hukuka aykırı bir delil elde etme yöntemi olduğu ve bu yolla elde edilen delillerin de yargılamanın hiçbir aşamasında kullanılmamaları gereken yasak nitelikte delil olduğu ileri sürülmektedir.[28]

Anılan tedbirin aynı zamanda Adlî ve Önleme Aramaları Yönetmeliği'nin 17. maddesinde de düzenleme altına alındığı görülmektedir. "*Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma*" başlığını taşıyan maddenin, 134. maddeden farklı düzenleme getiren kısmı üçüncü fıkradır. Üçüncü fıkra; *"Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır."* şeklindeki düzenlemeyi içermektedir. Böylelikle, "*Yönetmelikte el koyma işlemi sadece bilgisayarlarla münhasır kılınmamış aynı zamanda bilgisayar ağları, uzak bilgisayarlar ve çıkarılabilir donanımlar için de geçerli"*[29] olacak şekilde düzenleme altına alınmıştır.

Burada önemli bir noktaya değinmek gerekirse; CMK'nın 134. maddesi şüpheli tarafından kullanılan bilişim sisteminde durağan halde bulunan verilerin toplanmasına ilişkin ve sayısal delillerin toplanması konusunda sıklıkla başvurulan koruma tedbiridir.[30]

Son olarak anılan tedbir AİHM'in içtihatlarına da konu olmuş olup bu içtihatlarda Mahkemenin, anılan tedbirin kişinin özel hayatına ve kişisel verilerine müdahale oluşturduğuna değindikten sonra, bu tedbirin uygulanabilmesinde müdahalenin demokratik toplumda zorunlu ölçülerde yapılması ve tedbire dair kararların sınırlı olması ile aranacak,

28 DÜLGER, s. 7.
29 KESER BERBER, L.: "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El Koyma", *Ankara Barosu Bilişim Kurulu,* 09 Temmuz 2008 tarihli Panel, s. 7; Ayrıntılı bilgi için Bkz. https://www.google.com.tr/search?q=Bilgisayarlarda,+Bilgisayar+Programlar%C4%B1nda+ve+K%C3%BCt%C3%BCklerinde+Arama,+Kopyalama+ve+El+Koyma&ie=utf-8&oe=utf-8&gws_rd=cr&ei=9NZBVtqIDsWysQH5y4OACQ, (Erişim Tarihi: 07/11/2015)
30 Bkz. DEĞİRMENCİ, s. 309.

kopyalanacak ve el konulacak araçların verilen kararda açıkça belirtilmesi gerektiğine işaret ettiği görülmektedir.[31]

b. Akış Halindeki Sayısal Verinin Elde Edilmesi

CMK'nın 135. maddesinde "*iletişimin tespiti, dinlenmesi ve kayda alınması*" tedbiri düzenlenmiş olup, bu tedbirin şüphelinin kullandığı bilişim sistemi ile diğer bilişim sistemlerinin iletişimi anında ve akış halinde bulunan veriler üzerinde kullanılacağına yukarıda değinilmişti.

"İnternet haberleşmesinde internet servis sağlayıcılar ve iletişim şirketler aracılığıyla bilişim araçlarının diğer bilişim araçlarıyla kurduğu iletişime ilişkin arama, aranma, yer bilgisi ve kimlik bilgilerinin tespit edilmesi işlemi de ceza muhakemesinde kullanılacak nitelikte bir delil olarak karşımıza çıkmaktadır. Söz konusu deliller, internet servis sağlayıcıları ile iletişim şirketlerinin bilişim sistemlerinde veri olarak kaydedilmekte ve depolanmaktadır."[32]

CMK'nın 135. maddesi anılan tedbire, bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç işlendiğine dair somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda başvurulabileceği belirtilmiştir. Burada dikkat edilmesi gereken nokta her iki koşulun da aynı anda gerçekleşmesinin gerektiğidir. Yine Kanun "*başka suretle delil elde edilmesi imkânının bulunmaması*" ifadeleriyle söz konusu tedbire son çare olarak başvurulabileceğini vurgulamıştır.

Maddenin devamında; şüpheli veya sanığın telekomünikasyon yoluyla iletişiminin dinlenebilmesine, kayda alınabilmesine ve sinyal bilgilerinin değerlendirilebilmesine ağır ceza mahkemesi tarafından oy birliğiyle veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının kararıyla karar verilebileceği belirtilmiştir. Cumhuriyet savcısının kararının derhâl mahkemenin onayına sunulacağı ve mahkemenin de kararını en geç yirmidört saat içinde vereceği düzenlenmiştir.

Taşınabilir bir telefonun kayıtlandığı baz istasyonu ile mobil telefonun yerinin tespiti işlemi yapılarak bu madde kapsamında yer bilgisi tespit edilebilir. Ancak bazı durumlarda yer bilgisi tespiti sinyal bilgilerinin tespitini de gerektirebilir.

31 YAŞAR / DURSUN, s. 34.
32 Bkz. DEĞİRMENCİ, s. 383.

Bilişim sistemlerindeki iletişimin denetlenebilmesi için, öncelikle iki bilişim sistemi aygıtı arasında gerçekleşen bir iletişimin bulunması tabî olarak gereklidir.[33]

Madde tedbire hükmeden kararda; yüklenen suçun türünün, hakkında tedbir uygulanacak kişinin kimliğinin, iletişim aracının türünün, telefon numarasının veya iletişim bağlantısını tespite imkân veren kodun, tedbirin türünün, kapsamının ve süresinin belirtileceğini düzenlenmiştir. Bu sayede tedbire hükmedilmesinde keyfiliğin önlenmesi amaçlanmış ve tedbir bazı sıkı şartlara bağlanmıştır. Yine tedbir kararının en fazla iki ay için verilebileceği ve gerektiğinde sürenin bir ay daha uzatılabileceği düzenlenmiştir. Sürelerle ilgili olarak, örgüt faaliyeti çerçevesinde işlenen suçlarla ilgili gerekli görülmesi halinde, mahkemenin üç aya ek olarak her defasında bir aydan fazla olmamak ve toplam üç ayı geçmemek üzere tedbir süresinin uzatılmasına karar verebileceği düzenlenmiştir. "*135. maddenin ifadesinde sürenin ne zaman başlayacağı konusunda bir açıklık yoktur. Kanımızca süre, kararın verildiği andan itibaren başlatılmalıdır. Aksi yöndeki düşünce tedbirin uygulama aşamasında kötüye kullanılabileceği ihtimalini gündeme getirebilir."*[34]

Madde kapsamında yapılacak dinleme, kayda alma ve sinyal bilgilerinin değerlendirilmesine ilişkin hükümlere ancak maddede katalog halinde sayma suretiyle belirtilen suçlarla ilgili başvurulabileceği düzenlenmiştir. TCK'da yer alan bu suçlar arasında; göçmen kaçakçılığı ve insan ticareti, kasten öldürme, işkence, cinsel saldırı (birinci fıkra hariç, m. 102), çocukların cinsel istismarı, nitelikli hırsızlık ve yağma, uyuşturucu veya uyarıcı madde imal ve ticareti (m. 188), anayasal düzene ve bu düzenin işleyişine karşı suçlar, devlet sırlarına karşı suçlar ve casusluk gibi bazı suçlar sayılmıştır.

Madde de şüpheli veya sanığın tanıklıktan çekinebilecek kişilerle arasındaki iletişiminin kayda alınamayacağı ve eğer kayda alma gerçekleşmiş ise bu durumun anlaşılması halinde, alınan kayıtların derhal yok edileceği düzenlenmiştir. *"Dikkat edilirse, maddede yalnızca iletişimin "kayda alınamayacağı"ndan söz edilmiş, "tespit edilmesi" ve "dinlenmesi"nden bahsedilmemiştir. Oysa tanıklıktan çekinme hakkına sahip olanlar lehine bir istisna getiren bu hüküm, her üç durumu da içine alacak bir şekilde düzenlenmiş olmalıydı."*[35]

33 Bkz. DEĞİRMENCİ, s. 385.
34 Bkz. YAVUZ, H. A.: "Ceza Yargılamasında Bir Koruma Tedbiri Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi" *TBB Dergisi*, S. 60, Y. 2005, s. 253.

35 Bkz. YAVUZ, s. 249.

Madde, şüpheli veya sanığın yakalanabilmesi için mobil telefonun yerinin, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla tespit edilebileceğini düzenlemiştir. Bu konuda verilen kararda, mobil telefon numarasının ve tespit işleminin süresinin belirtileceği ve tespit işleminin en çok iki ay için yapılabileceği, yine bu sürenin bir ay daha uzatılabileceği belirtilmiştir.

Taşınabilir telefonun kayıtlandığı baz istasyonu esas alınarak yer bilgisi tespiti yapılması işlemi, mobil telefonun yerinin tespit işlemidir. Ancak bazı durumlarda yer bilgisi tespiti, sinyal bilgilerinin değerlendirilmesini gerektirmektedir. Bu durumda da bu madde kapsamında tedbir kararı alınması gerekmektedir. Ancak burada şu ayrıma değinmek yerinde olacaktır; taşınabilir telefonlar eğer kendi navigasyon sistemlerini kullanarak yer bilgisini kendi belleklerine kaydediyorlarsa bu durumda taşınabilir telefonun bilgisayar olarak kabul edilmesi şartı gerçekleşirse CMK'nın 140. maddesi uygulama alanı bulacaktır.[36]

Madde de; şüpheli ve sanığın telekomünikasyon yoluyla iletişiminin tespitinin soruşturma aşamasında hâkim kararıyla, kovuşturma aşamasında ise mahkeme kararıyla yapılacağı belirtilmiştir. Konuyla ilgili verilen kararda, yüklenen suçun türü, hakkında tedbir uygulanacak kişinin kimliği, iletişim aracının türünün, telefon numarasının veya iletişim bağlantısını tespite imkân veren kodunun ve tedbirin süresinin belirtileceği düzenlenmiştir. Maddenin en sonunda madde hükümlerine göre alınan kararların ve yapılan işlemlerin tedbir süresince gizli tutulacağı düzenlenmiştir.

İşlenen veya saklanan veri bilişim sistemleri aracılığıyla bu sistemler arasında transfer edilmekte ve bu transfer sırasında elde edilen deliller, sayısal delil niteliğine sahip olmaktadırlar. CMK'nın 135. maddesi gerekçesinde; bilgisayar işlemekteyken içeri girilmesinden bahsedilmektedir. Ancak, anılan madde kişilerin bilgisayarına girerek de akış halindeki verilerin elde edilmesine imkân vermemektedir. Kişilerin bilgisayarına girilerek yani bilgisayara erişilerek içeriğinde uzaktan arama yapılmasına hukukumuz imkân vermemektedir.[37]

Belirtilmelidir ki; anılan tedbirlere başvurulması bazen keyfi uygulamalara yol açabilecek niteliğe bürünebilmekte bu da kişilerin sahip olduğu özel hayatın gizliliği ve haberleşme hürriyetini ihlal edebilecektir. Bu durumu engelleyebilmek adına uygulayıcılar tarafından

36 DEĞİRMENCİ, s. 312.

37 DEĞİRMENCİ, s.382-385.

anılan tedbir kesin çizgilerle belirlenerek, açık ve net kurallar çerçevesinde yapılmalıdır. Bu sayede özel hayatın gizliliği ve haberleşme hürriyetine ancak çok istisnai nitelikteki durumlarda ve demokratik toplumun gereklerine uygun bir biçimde müdahale edilmelidir.[38]

38 YAVUZ, s. 240.

SONUÇ

Genellikle bilişim sistemlerinden veya elektronik aygıtlardan elde edildiği görülen sayısal deliller sayesinde, çok geniş bir yelpazede toplanabilen birçok suç açığa çıkartılarak çözümlenebilmektedir. Bu delil türleri sayesinde şüpheli veya sanığın kullandığı bilişim sistemlerinde bulunan, suça ilişkin bazı delillere ulaşılabilmesi mümkün bulunmaktadır. Ancak söz konusu delillerin herhangi bir iz bırakılmaksızın kolaylıkla değiştirilebilmeleri hatta yok edilmeleri gibi ihtimallerin söz konusu olmasının yanı sıra, bu delillere dair işlemlerin adli bilişim alanında özel eğitime tabi tutulan kolluk görevlileri tarafından yapılması ve yine sayısal delilin ortaya çıkarılmasında belirli aşamalara dikkat edilmesi gereklidir. Aksi durumda, delillerin tahrip olması, değiştirilmesi hatta yok olması gündeme gelebilecektir. Bu bağlamda, bilişim sistemlerinde bulunan sayısal deliller; üçüncü kişilerde, şüphelinin kullandığı bilişim sistemi ile diğer başka bilişim sitemlerinin iletişimi esnasında akış halinde veya şüphelinin kullandığı bilişim sitemlerinde durağan halde bulunabilmektedir.

Bu delillerin ortaya çıkarılması sürecinde başvurulan koruma tedbirlerine bakıldığında; arama ve elkoyma koruma tedbirinin, 5271 sayılı Ceza Muhakemesi Kanunu'nun 116. maddesiyle 122. maddeleri arasında genel olarak düzenlendiği görülmektedir. Aynı Kanun'un 134. maddesinde ise; "*bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma"* ayrı ve özel bir koruma tedbiri olarak düzenleme altına alınmış olup, arama ve elkoyma tedbirlerine dair genel hükümler, niteliğine uygun düştüğü ve aksine bir düzenleme bulunmadığı ölçüde özel nitelikteki 134. madde açısında da uygulama alanı bulabilecektir. Yine CMK'nın 135. maddesinde "*iletişimin tespiti, dinlenmesi ve kayda alınması*" tedbiri düzenlenmiş olup, bu tedbir şüphelinin kullandığı bilişim sistemi ile diğer bilişim sistemlerinin iletişimi anında ve akış halinde bulunan veriler üzerinde uygulama alanı bulmaktadır.

Belirtilen tedbirler sayesinde, birçok suç açığa çıkartılarak çözümlenebilmektedir. Bununla birlikte şartları oluşmaksızın veya gereğinden fazla başvurulması halinde bu tedbirler, kişilerin özel hayatının gizliliği ve haberleşme hürriyetini ihlal edebilecek keyfi uygulamalara da yol açabilecek niteliktedir. Bu nedenle söz konusu tedbirler, demokratik toplumun ve hukuk devleti olmanın gereklerine uygun bir biçimde sadece kanunda belirtilen şartların varlığı halinde ve yine kanunda belirtilen sınırları içerisinde uygulanmalıdır.

KAYNAKÇA

Kitap ve Makaleler

BAŞLAR, Y.: "Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri", *Uyuşmazlık Mahkemesi Dergisi*, Y. 2013.

DEĞİRMENCİ, O.: *Ceza Muhakemesinde Sayısal (Dijital) Delil,* Seçkin, 2014.

EMEKCİ, A. / KUĞU, E.: "Adli Bilişim ve Etmen Tabanlı Sistemler", *7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı,* 17-18 Ekim 2014, Bildiriler Kitabı.

KARAGÜLMEZ, A.: *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, Seçkin, Ankara, 2009.

KIZILYAR, M.: "Ceza Yargılamasında Dijital Verilerin Delil Değeri", *Adalet Dergisi*, Y. 2014, S. 50.

ÖZBEK, M.: "Adli Bilişim Uygulamalarında Orijinal Delil Üzerindeki Hash Sorunları", 1st International Symposium on Digital Forensics and Security (ISDFS'13), 20-21 May 2013.

ÖZEN, M. / ÖZOCAK, G..: "Ali Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)", *Ankara Barosu Dergisi,* Y. 2015, S. 1.

ŞENGÜL G. / ATSAN F. K. / BOSTAN, A.: "Adli Bilişim Alanındaki Mevcut Problemler, Çözüm Önerileri ve Gelecek Öngörüleri", *7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı,* 17-18 Ekim 2014, Bildiriler Kitabı.

YAŞAR, Y. / DURSUN, İ.: "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma Koruma Tedbiri", *MÜHF*, C. 19, S. 3.

YAVUZ, H. A.: "Ceza Yargılamasında Bir Koruma Tedbiri Olarak Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi" *TBB Dergisi*, S. 60, Y. 2005.

YÜCETÜRK, B.: "Soruşturmalarda Bilgisayara Elkoyma", *Bilişim Dergisi,* S. Nisan, Y. 2014.

Elektronik Kaynaklar

http://www.hukuki.net/hukuk/index.php?act=file&id=4&article=3242

https://www.academia.edu/9449240/B%C4%B0L%C4%B0%C5%9E%C4%B0M_S%C4%B0STEMLER%C4%B0_%C3%9CZER%C4%B0NDE_ARAMA_KOPYALAMA_VE_EL_KOYMA_TEDB%C4%B0R%C4%B0

https://www.google.com.tr/search?q=Bilgisayarlarda,+Bilgisayar+Programlar%C4%B1nda+ve+K%C3%BCt%C3%BCklerinde+Arama,+Kopyalama+ve+El+Koyma&ie=utf-8&oe=utf-8&gws_rd=cr&ei=9NZBVtqIDsWysQH5y4OACQ