HAKEMLİ

Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)*

Prof. Dr. Muharrem ÖZEN**
Gürkan ÖZOCAK***

* **Bu makale hakem incelemesinden geçmiştir ve TÜBİTAK–ULAKBİM Veri Tabanında indekslenmektedir.**

** Ankara Üniversitesi Hukuk Fakültesi Ceza ve Ceza Usul Hukuku Ana Bilim Dalı Başkanı, ozen@law.ankara.edu.tr.

*** Ankara Üniversitesi Hukuk Fakültesi Ceza ve Ceza Usul Hukuku Doktora öğrencisi, Avukat, İstanbul Barosu, gurkanozocak@gmail.com.

Prof. Dr. Muharrem ÖZEN
Gürkan ÖZOCAK

ÖZ

Günümüzdeki teknolojik gelişmeler ışığında, ceza muhakemesinde kağıt sisteminin yerini, bir ispat vasıtası olarak bilgisayarlardan ve bilişim sistemlerinden elde edilen elektronik deliller almıştır. Bu bağlamda, elektronik deliller, özellikle bilişim suçlarının ispatlanmasında çok önemli hale gelmiştir. Ne var ki, bu delillerin toplanmasında, delil bütünlüğünü korumak amacıyla dikkat edilmesi gereken teknik hususların yanı sıra, ceza muhakemesi hukuku bakımından korunan kurallara uygun hareket edilmesi de büyük önem arzetmektedir. Aksi halde, 5271 sayılı Ceza Muhakemesi Kanunu'na aykırı bir biçimde elde edilen elektronik delillerin, ceza muhakemesi süreçlerinde delil niteliği kazanması imkansız hale gelmektedir.

Anahtar Kelimeler: *Ceza Muhakemesi, Elektronik Delil, Adli Bilişim, Bilişim Hukuku, Bilişim Suçları, Delillerin Tespiti, Bilgisayarlarda Arama ve El Koyma.*

◆◆◆

COMPUTER FORENSICS, DIGITAL EVIDENCE AND LEGAL REGIME OF SEARCH AND SEIZURE OF COMPUTERS

ABSTRACT

In the light of current technological progress, digital evidences, as probative force, that are gathered from computers and information systems supersede paper evidences. Thanks to this, digital evidences have increased in importance about proving of especially cyber crimes. Even so, it is vital that not only technical issues to preserve the integrity of evidence, but also toeing the rules of criminal procedure law. Otherwise, digital evidences, which are gathered contrary with Turkish Code of Criminal Procedure (CMK) No. 5271, cannot be used as evidence in the process of criminal justice.

Keywords: *Criminal Procedure, Digital Evidence, Computer Forensics, IT Law, Cybercrimes, Detection of Evidence, Search and Seizure of Computer.*

A. GİRİŞ

Tarihte, suç ve suçlu kavramları, neredeyse insan topluluklarının meydana gelmesiyle eşdeğer zamanlarda ortaya çıkmıştır. Suç ve suçlu kavramları ile birlikte ise, delil araştırması ile ceza muhakemesi hukuku kuralları belirginleşmeye başlamıştır. Suç ve suçlunun tespiti için maddi araştırma yapılmaya başlanmış, ceza muhakemesi kuralları da bu ihtiyaçtan doğmuştur. Bugün, suçluların ortaya çıkarılabilmesi için, delillerin toplanması, analizi ve sonuçlandırılarak maddi vakıalara özgülenmesi çok önemlidir.

İşte delillerin bulunması, analiz edilmesi, incelenmesi ve gerekli biçimlerde adli makamlara sunulması, ceza muhakemesi hukuku üst başlığında çeşitli alt bilim dallarının oluşmasına neden olmuştur. Bu bilim dallarına adli bilişim, adli tıp, adli psikoloji gibi disiplinler örnek olarak gösterilebilir.

Önceki dönemlerde delil araştırmasında kağıt dokümanlar talep edilmekte, muhakeme sürecinde soruşturma ve kovuşturma görevi yapan hakim ve savcılar da, aşina oldukları bu "kağıt sistemi"ni uygulamaktaydılar. Ancak, teknolojik gelişmeler ve suç işlenmesinde bilişim sistemlerinin de yoğun bir biçimde kullanılmaya başlanmasıyla birlikte, kağıdın dışında, bilişim sistemlerinde ve bunların parçalarında yapılacak incelemeler gündeme gelmiştir. İşte, suç delillerinin bir kısmının bilgisayar ve diğer elektronik cihazlar üzerinde bulunması ve bunların keşfedilme ihtiyacı neticesinde, en yaygın delil bulma yöntemlerinden biri olarak adli bilişim (*computer forensic*) ortaya çıkmıştır.

Bu itibarla, çalışmamızda adli bilişim kavramını ve türlerini değerlendirdikten sonra, bilgisayardan elde edilen delillerin teknik yapısını ve nihayet bu delillerin elde edilmesinin hukuki rejimini düzenleyen Ceza Muhakemesi Kanunu'nun 134. maddesini inceleyeceğiz.

B. ADLİ BİLİŞİM KAVRAMI VE TÜRLERİ

1. Adli Bilişim Kavramı

a. Genel Olarak

Disketlerden, sabit disklerden ve çıkartılabilir disklerden delil elde etme amacıyla veri kurtarma işlemi olan ve elektronik delillerin muhteva ettiği bilgileri, delil inceleme süreçlerini, hukuki ve etik sorumlulukları göz önünde bulundurarak, delilin bütünlüğünü koruyarak ve maddi gerçeği açığa çıkarmak amacıyla; kopyalama, belirleme, çözümleme, yorumlama ve belgeleme

süreçlerinin bütününe adli bilişim adı verilmektedir[1]. Bu veriler, bilgi saklamak amacıyla kullanılan medyaların aktif alanlarında, silinmiş alanlarında veya artık alanlarında bulunmaktadır[2].

Adli bilişimi, '*Bilgi Güvenliği*' ana başlığının altında, hukuk ve bilgisayar güvenliği bilimlerinden oluşan bir alt bilim dalı olarak tasnif etmek mümkündür. Aynı şekilde, bu disiplin, bilişim suçlarına, bilgi güvenliği açıklarına, ulusal güvenlik tedbirlerine ve bilgisayar suiistimallerine karşı, adli analizler ve çalışmalar içeren bir yaklaşım olarak da kabul edilebilir[3].

b. Adli Bilişimin Amacı

Adli bilişimin temel amacı; potansiyel olarak görülen yasal ve elektronik delillerin sırasıyla keşfedilmesi, toplanması, analiz edilmesi ve sunulması olarak tanımlanabilir[4]. Bir başka deyişle, adli bilişim, tüm adli delillendirme sürecinde, suçlunun tespit edilmesi için ihtiyaç duyulan sayısal delillerin elde edilmesini sağlamaktadır. Bununla beraber, adli bilişimin temel varlık sebebinin herhangi bir kişiyi suçlu ya da masum göstermek değil, adli birimlere sayısal delilleri eksiksiz ve tarafsız bir biçimde sunulmasını sağlamak olduğunu vurgulamak gerekmektedir. Bu açıdan bakıldığında, adli bilişim bir yorum faaliyeti içermeyen, tamamen teknik bir inceleme yöntemidir[5]. Zira, delillerin yorumlanması ve bir kişinin suçlu olup olmadığının belirlenmesi faaliyeti, bu delillerin adli bilişim süreçlerinden geçerek adli birimlere aktarılması sonucu, yargı makamları tarafından gerçekleştirilmektedir.

2. Adli Bilişim Türleri

Adli bilişim, genel olarak üç alt dala ayrılmakta olup, bunlar; bilgisayar adli bilişimi, ağ ve İnternet adli bilişimi ve gömülü cihazlara ait adli bilişimdir. Ancak son dönemlerde dördüncü bir alt dal olarak sosyal ağ adli bilişimi de

[1] Barry, Sean; "Smoking Microchips Tells It All : Computer Forensic Experts Mine Hard Drives For Data That Too-Clever Users Thought Long Deleted", http://www.dataforensics.com/articles/ smoking_microchip_tells_it_all.pdf, (15.04.2014); Keser Berber, Leyla; Adli Bilişim, Ankara, 2004, s. 39.

[2] Say, Kubilay; Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi, Ankara, 2006, s. 16 (Yayımlanmamış yüksek lisans tezi).

[3] Sağıroğlu, Şeref / Karaman, Mehmet; "Adli Bilişim", Telepati Dergisi, S. 203, Ağustos 2012, s. 62.

[4] Kim, Y., Kim, K.J.,"A Forensic Model on Deleted-File Verification for Securing Digital Evidence", 978—1-4244-5493-8710 IEEE, 2010; Wang, Y., Cannady, J., Rosenbluth, J., "Foundation of computer forensics: A technology fort he fight against computer crime", Computer Law & Security Report, s. 21/119-127, 2005; Wolfe, H.B., "Computer Forensics", 0167-4048/03 Elsevier Science, 2003; Sağıroğlu/Karaman, s. 62.

[5] Sağıroğlu / Karaman, s. 62-63.

kabul edilmekte olup, çalışmamızın bu bölümünde bu dört ana dalın genel çerçevesini inceleyeceğiz.

a. Bilgisayar adli bilişimi

Bilgisayarlar için yapılan çalışmalar günümüzde adli makamlarda en çok kullanılan adli bilişim yöntemi olarak bilinmektedir. Adli bilişimin bu dalında, suç işlendikten sonra, suç mahallinde bulunan ya da suçlu tarafından kullanılan masa üstü, dizüstü ve netbook tarzı bilgisayarların, adli birimlerce, teknik prosedürlere ve usul kurallarına uygun bir biçimde ön güvenliğinin sağlanması da dâhil olarak, adli bilişim laboratuvarlarına taşınması, bilgisayarlar içindeki bilgi barındıracak tüm birimlerin incelenmesi, gerekli ilişkilendirmelerin yapılması, raporlanması ve adli makamlara sunulması süreçleri yer almaktadır[6].

b. Ağ ve İnternet adli bilişimi

Ağ ve internet adli bilişim dalı; suçluların bir kurum ya da firmaya ait bir sisteme sızmaları, bu sistemlere maddi çıkar veya kişisel eğlence için zarar vermeleri sonucu kurum ya da firmanın saygınlığının zedelenmesi sebebiyle, tüm sisteme ait logların bilgisayar sunucularının ve ağ üzerinden giden paketlerin incelenmesi, gerekli ilişkilendirmelerin yapılması, raporlanması ve adli makamlara sunulması süreçlerini kapsamaktadır[7].

c. Gömülü cihazlara ait adli bilişim

Gömülü cihazlara ait adli bilişim; *iPhone, Blackberry* ve *iPad* gibi cihazları kullanarak işlenen suçlarda, suçluya ait bu tür cihazların elde edilmesi, gerekli yazılımlar vasıtası ile bu tür cihazların içerisindeki suç unsuru olabilecek bilgilerin çıkarılması, ilişkilendirmelerin yapılması, raporlanması ve adli makamlara sunulması süreçlerini kapsamaktadır.

d. Sosyal ağ adli bilişimi

Sosyal Ağ Adli Bilişimi ise, özellikle son yıllarda bir adli bilişim türü olarak kabul edilmekte olup, Web 2.0 akımıyla birlikte İnternette doğan yeni medya ve paylaşım ekosistemi üzerinden adli bilişim süreçlerinin ve incelemeleri destekleyici çalışmaların yürütülmesi olarak ifade edilebilir.

---

[6] Peisert, S., Bishop, M., Keith, M., "Computer Forensics in Forensic", Third International Workshop on Systematic Approaches to Digital Forensic Engineering, 2008; Bednar, P.M., Katos, V., Hennell, C., "Cyber-Crime Investigations: Complex Collaborative Desicion Making", Third International Annual Workshop on Digital Forensics and Incident Analysis, 2008 Aktaran Sağıroğlu/Karaman, s. 63.

[7] Sağıroğlu / Karaman, s. 63.

Bu adli bilişim türünde, sosyal ağlar ve paylaşım ortamları üzerinden, kayıp kişilerin takibi, kötü amaçlı yazılım yayma, insan kaçakçılığı, dolandırıcılık gibi eylemlerin tespitinin yanı sıra, mevcut elektronik delillerin değerlendirilmesine yardımcı olunması sağlanabilmektedir.

C. ADLİ BİLİŞİM YÖNTEMLERİ

Son birkaç yıldaki adli bilişim uygulamaları incelendiği zaman, ceza muhakemesi hukukunda delil niteliği taşıyabilecek verilerin, sadece kişisel bilgisayarlardan değil, aynı zamanda cep telefonlarından, Xbox vb. oyun konsollarındaki görüşme kayıtlarından, USB belleklerden, dijital ses ve video kayıt cihazları gibi birçok elektronik cihazdan elde edilebildiği görülmektedir.

Adli bilişimde delillerin büyük çoğunluğu kişisel bilgisayarlardan elde edilmektedir, çünkü kişisel bilgisayarlarda internet gezinti bilgileri, silinmiş dosyalar, sistem logları, kullanıcı hesapları ve büyük miktarda şifrelenmiş veri bulunmaktadır. Ancak kişisel bilgisayarlardan elde edilen verinin boyutu ne kadar büyük olursa olsun, en ufak bir delilin tespiti bile soruşturma aşamasında çok büyük öneme sahiptir. Kişisel bilgisayarlar kadar olmasa da gelişmiş cep telefonları (*smart phone*) vb. birçok dijital medya da bireyler tarafından aktif olarak kullanılmakta ve üzerlerinde ceza muhakemesinin konusu olabilecek nitelikte elektronik veri tutulmaktadır.

Bütün bu delillerin incelenmesi ile, soruşturma aşamasında suçluya ait izlerin ortaya çıkması ve ipuçlarına ulaşılması mümkün olmaktadır. Bu elektronik ortamlardan elde edilen en küçük bir veri dahi, ceza muhakemesinde büyük bir vakıayı çözmekte kullanılacak çok önemli bir delil haline gelebilmektedir. Çalışmamızın bu bölümünde, bahsi geçen delillerin elde edilmesine ilişkin olarak, adli bilişimin alt disiplinleri hakkında temel teknik bilgiler değerlendirilecektir[8].

1. Bilgisayar Adli Bilişimi *(Computer Forensic)*

Adli bilişimin bilinen ve en çok kullanılan alt disiplini, *bilgisayar adli bilişimi*dir. Adli işlemlerin hemen hepsinde, yapılan inceleme çoğu kez şüphelinin bilgisayarında yapılmakta ve istatistiksel olarak bakıldığında, bu incelemelerin hatırı sayılır bir kısmı suç fiiline ilişkin delillerin tespitiyle sonuçlanmaktadır. Bu nedenle, bilgisayar adli bilişimi, en sık kullanılan adli bilişim yöntemi olup, çalışmamızın ilerleyen kısmında inceleyeceğimiz Ceza Muhakemesi Kanunu'nun 134. maddesinde düzenlenen koruma tedbiri de bilgisayar adli bilişiminin sınırlarını çizmektedir.

[8] Daniel, L., "Digital Forensic: The Subdisciplines", Digital Forensic for Legal Professions, 2011, s. 17-23.

Bilgisayarlar büyük miktarda veri barındıran, kendine has logları oluşturan, e-posta işlemlerinin yapıldığı, dahili sabit diskinin bulunduğu, kullanıcı hesaplarının yönetilebildiği ve en yaygın kullanılan elektronik cihazlar olması nedeni ile adli makamlar için çok önemli bir veri kaynağı konumundadır. Bu disiplin, adli bilişim alt dalları arasında ilk olarak ortaya çıkmış olan disiplindir ve esas olarak veri kurtarma projesine dayanmaktadır[9].

2. Ağ Adli Bilişimi *(Network Forensic)*

Ağ adli bilişimi, belirli bir sistem içerisinde kurulu olan *Local*, *Wan* ya da İnternet ağ trafiklerinin izlenmesi, analiz edilmesi ve analiz neticeleri doğrultusunda adli makamlara gerekli bilgilerin verilmesi şeklinde tanımlanabilir. Bu disiplin sayesinde elde edilen veriler gerekli görüldüğü durumlarda erken uyarı sistemleri içinde kullanılmaktadır. Ağ seviyesinde yapılan teknik incelemeler, genel olarak paket seviyesinde anlık olarak ya da depolanarak, belirli zaman aralıkları ile yapılmaktadır[10].

3. Mobil Adli Bilişim *(Cellphone Forensic)*

Mobil adli bilişim, cep telefonlarının gelişmesine ve kullanımının yaygınlaşmasına paralel olarak, cep telefonları içerisinde tutulan servis sağlayıcılara ait fatura bilgileri ya da CDR (*call detailed record*) adı verilen arama detay bilgilerinin elde edilmesini sağlayan adli bilişim disiplinidir. CDR bilgilerinin çözümlenmesi sonucunda, kişinin hangi zamanlarda kimleri aramış olduğu, bu kimselerle ne kadar süre iletişimde olduğu gibi, suçun tespiti bakımından çok önemli ve delil niteliği taşıyabilecek bilgiler elde edilebilmektedir.

Günümüzde cep telefonlarının sabit disklerinin büyük olması, e-posta iletişiminin yapılması, text mesajlaşmanın yapılabilmesi, resim ve video çekme, ses kaydı alabilme vb. birçok gelişmiş özelliklere sahip olması, bu cihazları ceza muhakemesinde bir delil elde etme aracı olmaları açısından oldukça önemli kılmaktadır. Az önce sayılan verilerin çoğu cep telefonuna ait sabit diske kaydedilmekte ve silinebilmektedir. Bu sabit disklerden veri kurtarmanın mümkün olması ve bu verilerin bazı durumlarda ceza muhakemesi süreçleri için geçerli olması mobil adli bilişim disiplinini ortaya çıkarmıştır.

Ne var ki, akıllı telefonlar, bugün en az kişisel bilgisayarlar kadar yaygın ve önemli bir delil elde etme aracı olsa da, piyasada binlerce cep telefonu modeli

[9] Sağıroğlu / Karaman, s. 63.

[10] Kretowicz, Joanna; "Network Forensics and Security", https://eforensicsmag.com/wireless-forensic-preorder/, (05.05.2014); Sağıroğlu / Karaman, s. 63.

bulunması ve yapılacak incelemelerin bazı durumlarda model bağımlı olması, mobil adli bilişimin en zayıf olduğu noktadır[11].

Bununla beraber, akıllı telefonların yaygınlaşması ile birlikte, taşınabilir cihazların çağrı ve sms iletişiminin dışında sanal pazarlardan indirilip kullanılabilen ücretsiz haberleşme yazılımları da (*skype, WhatsApp, tango, viber vb.*) ortaya çıkmış, böylelikle telefon uygulamaları ve ilgili verileri de adli bilişimin bir parçası haline gelmişlerdir.

4. GPS Adli Bilişim *(GPS Forensic)*

GPS sistemleri, teknolojinin bu denli geliştiği günümüz dünyasında, yoğun bir biçimde kullanılmakta olup, buna paralel olarak, GSM birimlerine ilişkin teknolojik ilerlemelerde de ciddi ölçüde yol alınmıştır. Kiralanan araçlarda, toplu taşımalarda veya taşımacılık, nakliye vb. birçok sistemde, kişilerin bilgisi dahilinde veya haricinde, birçok GPS birimi, ilgili araçlara entegre durumdadır.

Bu bağlamda, GPS adli bilişim de, bu gelişmiş GPS birimlerinin analizini içeren bir alt disiplindir. Gelişmiş GPS birimleri araçların ziyaret ettikleri yerleri, favori yerleri ve araması yapılan yerleri zaman bilgisi ile beraber tutması nedeni ile ölümcül kazalar gibi önemli adli durumlarda, ilgili aracın o anda o lokasyonda olup olmadığı ile ilgili kararlarda yahut hareketli bir cismin takibinde önemli bir delil tespit aracı olarak kullanılabilir[12].

5. Medya Araçları Adli Bilişimi *(Media Device Forensic)*

PDA, USB Bellekler, dijital müzik oynatıcıları, ses kayıt cihazları ve taşınabilir harici diskler, günlük hayatta, kişiler tarafından aktif ve yaygın olarak kullanılan elektronik cihazlardır. Bir çok şifreli verinin yanı sıra; krokiler yahut çocuk pornosu ihtiva eden videolar da bu cihazlar vasıtası ile taşınabilmekte ve izlenebilmektedir. Yine bu cihazlar vasıtasıyla, ses kayıt cihazları ile uygunsuz olarak ses kaydı yapılabilmektedir.

Bütün bu kayıtlar ve verilere ait içerik ve zaman damgaları, cihazlardaki sabit disklerde bulunmaktadır ve suçlular gerektiği durumlarda bu içerikleri silebilmektedir. İşte medya araçları adli bilişimi, bu verilerin kurtarılması ve delil niteliği taşımak üzere adli makamlara sunulması ile ilgilenen bir alt disiplin olarak karşımıza çıkmaktadır[13].

---

[11] Sağıroğlu / Karaman, s. 63.
[12] Last, David; "Computer Analysts and Experts – Making the Most of GPS Evidence", http://articles. forensicfocus.com/2012/08/27/computer-analysts-and-experts-making-the-most-of-gps-evidence/, (15.05.2014).
[13] Sağıroğlu / Karaman, s. 64.

6. Sosyal Ağ Adli Bilişimi *(Social Network Forensic)*

Son yılların adeta 'moda' tabiri haline gelen sosyal medyayı, bireylerin İnternet üzerinden birbiriyle yapmış olduğu diyalog ve paylaşımların bütünü olarak tanımlamak mümkündür. Sosyal ağlar, bloglar, mikro bloglar, sohbet siteleri, forumlar ve İnternet sözlükleri gibi kişilerin birbirleriyle iletişim kurmasını ve bilgi paylaşmasını sağlayan İnternet siteleri ve uygulamalar sosyal medya kapsamında sayılmaktadır. Bunlar bazen iki kişinin birbiriyle yapmış olduğu sohbetler gibi mikro ölçekte paylaşımlardan oluşsa da, İnternet ortamının sınırsız zenginliğinden kaynaklı olarak, paylaşılan bir bilgi veya içeriğin saniyeler içerisinde binlerce, hatta milyonlarca insana ulaşması mümkün hale gelebilmektedir[14]. En çok kullanılan sosyal ağlara örnek olarak *Facebook, Twitter, Myspace, Linkedin, Ekşi Sözlük* gibi İnternet siteleri verilebilir.

Kişiler üyesi oldukları bu sosyal ağların her birinde farklı farklı özellikler sergileyebilmektedirler. Kimisinde aile ve arkadaş çevresi ile iletişim kurarken, kimisinde belli başlı olaylar hakkında yorumlar yazabilmekte, kimisinde ise iş çevresi ile iletişim kurabilmektedirler. Kişilerin sosyal ağlarda iletişim hallerindeki değişiklikler, haberleşmeler, hakaret ve tehditler, katılmış oldukları gruplar, grup hareketleri vb. birçok iletişim faaliyeti, tanımlamış oldukları mail kutularına ya da kullanmış oldukları uygulamalar vasıtasıyla sistemlerine düşmektedir. Sosyal ağ adli bilişim disiplini, sosyal ağlar üzerindeki bu verilerin incelenmesi, analiz edilmesi ve delil teşkil etmek üzere adli makamlara sunulması ile ilgilenmektedir.

7. Uzaktan Arama Yöntemleri *(Remote Search veya Remote Viewer)*

Yukarıda adı geçen adli bilişim yöntemlerinin dışında, uzaktan arama yöntemleri ile suç delilinin var olduğu şüphesi bulunan bilişim sistemlerine uzaktan erişme de bir delil arama ve elde etme yöntemi olarak kabul edilmektedir. Uzaktan arama, kolluk kuvvetlerine ağa bağlı bir bilgisayarın sabit diskinde yahut çalışan diğer belleklerinde arama olanağı sağladığı gibi, elektronik posta trafiğinin denetlenmesi ve ağ tarayıcısının faaliyetlerini izlemesi olanağı da tanımaktadır[15].

Bu hususla ilgili teknik tartışmaların dışında kalarak şunu söylememiz gerekir ki, uzaktan arama yönteminde şüphelinin kendine ait bilişim sistemlerinde arama yapıldığı ve delil toplandığından bilgisi olmamaktadır. Bu nedenle, söz konusu deliller üzerinde kişinin gözetleme, haklarının korunmasını isteme hakkı ortadan kaldırılmakta, dahası bu delillere kolluk veya üçüncü kişiler tarafından yapılacak hukuka aykırı müdahalelerin de önü açılmaktadır.

---

[14] Özocak, Gürkan, "Sosyal Medyada İşlenen Suç Tipleri ve Suçluların Tespiti", Yenimedya Çalışmaları II. Ulusal Kongresi – Kongre Kitabı, Kocaeli, 2013, s. 465.

[15] Değirmenci, Olgun; Ceza Muhakemesinde Sayısal (Dijital) Delil, Ankara, 2014, s. 225.

Nitekim, Almanya'da yakın zamanda, İç İşleri Bakanlığınca '*Uzaktan Adli Yazılım*' (*Remote Forensic Software*) adlı bir *Trojan* virüsü tasarlanarak, suç faili olduğu düşünülen kişilerin bilgisayarlarında uzaktan arama yoluna gidilmiş ve bu yöntem büyük tartışmalara neden olmuştur. Bu örneğe, çalışmamızın son bölümünde değineceğiz.

Bunun dışında, uzaktan arama yapılırken en sık kullanılan mobil yazılım olan RFS ile elde edilen deliller bakımından *hash değerinin alınması* uygulamasının söz konusu olamayacağı, bu durumda da üzerinde inceleme yapılacak olan kopyanın el konulan orijinal delil ile bütünlüğünün denetlenemeyeceği ve delilin güvenilirliğinin ortadan kalkacağı söylenmiştir[16]. Bütün bu eleştirilere tarafımızca da hak verilmekte olup, uzaktan aramanın en azından bugün için ceza muhakemesinde bir delil elde etme aracı olarak kullanılmasının gerek delillere müdahale, gerekse de temel hak ve özgürlükler bakımından ciddi sorunlara yol açacağı kanaatindeyiz.

D. ADLİ BİLİŞİM SÜREÇLERİ

1. Genel Olarak

Bilgisayarlardan veya diğer bilişim sistemlerinden toplanan verilerin ceza muhakemesinde delil değeri taşıyabilmesi için, bu verilerin teknik gerekliliklere uygun olarak toplanması hayati derecede önem arzetmektedir. Bu bağlamda, bilgisayar ortamında delil toplamak, yalnızca şüphelinin bilgisayarının tamamen kopyalanması ve buradaki içeriğinin adli makamlara sunulmak üzere çıktısının alınması değildir. Bu delil toplama işlemi, teknik gerekliliklerin çok sayıda olduğu, hassas bir süreçler bütünü olarak kabul edilmelidir.

Bu süreç işletilirken, el konulacak bilgisayarlardan veri alınmasından, bilgisayarın dondurulması, verilerin kopyalanması, klonlanması, bilgisayarın kapatılması ve laboratuvara götürülmesine kadar bütün süreçler çok titiz bir biçimde yerine getirilmeli ve eldeki delillerden hiçbirinin kaybolmaması veya zarar görmemesi sağlanmalıdır[17].

Bunlarla beraber, yapılan tüm işlemler adımı, ayrıntılı bir biçimde dokümante edilmelidir. Bu temel süreçlerin bütünü aşağıdaki gibi sıralanabilir:

- *Delillerin bulunduğu ortamın boşaltılması ve kamera ile sürecin takip edilmeye başlanması gerekmektedir.*

[16] Değirmenci, s. 236.
[17] Garfinkel, S.L., "Digital forensics research: The next 10 years", Digital Investigation 7, 2010, s. 64–s. 73 Aktaran Sağıroğlu/Karaman, s. 64.

- *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*[18].

Adli bilişimde olay yerinin incelenmesinden, elde edilen delillerin adli makamlara sunulmasına kadar birçok aşama bulunmaktadır. Ancak, adli bilişim aşamaları, genel olarak *ön inceleme ve olay yeri tespiti, delil toplama, analiz* ve *raporlama* olmak üzere dört ana başlıkta değerlendirilmektedir. Elektronik delillerin toplanmasının hukuki rejimine geçmeden önce, bu aşamalara kısaca değineceğiz.

2. Ön İnceleme ve Olay Yeri Tespiti

- Tüm açılardan bilgisayarın fotoğrafları ve bilgisayarın bağlı olduğu ağa ait bağlantıların ve ortamın fotoğrafları çekilmedir.
- Bilgisayar, eğer bir ağa bağlı ise, bu ağdan ayrılmalı ve güvenli bir bölgeye götürülerek muhafaza altına alınmalıdır.
- Tüm taşıma ve muhafaza işlemlerinin, kanunlara uygun olarak ve kimler tarafından, nasıl yapıldığı tutanak altına alınmalıdır.
- Bu aşamadaki en önemli noktalardan biri, şüphelinin bilgisayarının tekrardan başlatılması ve herhangi bir uygulamanın çalıştırılması sürecidir. Sistemin düzgün olarak yeniden başlatılamaması, BIOS ve tarih/saat gibi önemli bilgilerin değişmesi tehlikesini ortaya çıkarabilir, böyle bir durum da, bazı önemli dosyaların yeniden oluşmasına veya kapatılmamış bir dosyanın kaydedilmeden ortadan kalkmasına ya da Windows'a ait *swap* dosyalarının yok olmasına neden olabilir. Bir başka deyişle, sistem düzgün olarak yeniden başlatılmazsa, ceza muhakemesinde delil olarak kullanılacak verilerin yok olması söz konusu olabilir.

[18] Keser Berber, s. 66 vd; Karaman, Mehmet, Adli Bilişim, Ankara, 2014 (Yayımlanmamış Rapor), s. 7.

- Bilgisayarın inceleme için laboratuvara götürülürken nasıl kapatılacağı hususu, delillerin sıhhatinin korunması açısından elzemdir. Bu kapatılma işlemi, cihazın fişinin çekilmesi şeklinde yahut uygun teknik usuller işletilerek yapılabilir. Bilgisayar kapatılmadan önce, uçucu delil vasfı taşıyan ağ trafiği, ekran görüntüsü, bellek dökümü gibi yararlı bilgilerin yedeklenmesi de delillerin korunması bakımından önemlidir. Zira bu kapatma işlemin doğru yapılmaması durumunda da, yine bir çok delilin yok olması tehlikesi ortaya çıkacaktır.
- Deliller, yazıcı, bilgisayar çıktısı gibi fiziksel sunular olabileceği gibi; cd, flash, zip dosyası gibi herhangi bir sayısal veri olarak da sunulabilir.
- Şüphelinin bilgisayarındaki tüm deliller, teknik gereklere uygun bir şekilde kopyalanmalı ve yeterli bir diskte yedeklenmelidir. Bu nedenle, kopyalama aşamasından herhangi bir eksik veri kaydedilmemesi ya da veri kaybı olmaması için yedeklenecek diskin şüpheli bilgisayar diskinden büyük olması gerekmektedir.
- Araştırmacı haricinde hiç kimse şüphelinin bilgisayarına erişememelidir.
- Veriler düzgün bir şekilde kopyalanmalıdır. Bu kopyalama işlemi için birçok program bulunmaktadır.
- Kopyalanan verilerin de *hash değerleri*[19] alınmalıdır[20].

3. Delil Toplama

Delil toplama aşaması, olay yeri incelemesi sonrası tespit edilen delillerin toplanması ve yeni delillerin elde edilmesini ifade eder. Burada dikkat edilmesi gereken hususlar şunlardır:

- Öncelikli olarak kopyalanmış veri, bu verilere erişim yetkileri ve veri bütünlüğü kontrol edilmelidir.
- Bu aşama, silinmiş verilerin yeniden kurtarılması ve şifrelenmiş verilerin şifre çözme safhalarını içermektedir.
- Tüm analiz ve incelemeler, orijinal kaynağın doğruluğunun korunması için, klon edilmiş veriler üzerinden yapılmalıdır.
- Analizci doğru delilleri bulabilmek için, sistemdeki tüm dosyaları analiz etmelidir. Bunlar;

[19] Hash değeri: Dosyaların parmak izi de denilen ve dosya üzerinde en küçük bir değişiklik yapıldığında baştan sona değişen, dolayısıyla yedeklenen verilerin bütünlüğünü teminat almaya yarayan sayısal değerler.

[20] Sağıroğlu/Karaman, s. 64-65.

- *Normal dosyalar*
- *Silinmiş dosyalar*
- *Gizli dosyalar*
- *Şifreli dosyalar*
- *Şifre korumalı dosyalar*
- *Geçici, swap ya da uygulama ve uygulamaların kullandığı dosyalar*
- *İşletim sistemi dosyaları*

- Eğer şüpheli dosyalar biliniyorsa, bunların içinde de arama yapılmalıdır. Örneğin, txt dosyaları içinde aramalar yapmak gerekir, bu aramalar için birçok program mevcuttur (*Powergrep vb.*). Pornografi vb. suçlara ilişkin deliller aranıyorsa, görüntü ya da video dosyaları aranmalıdır. Bu işlem, sürenin de kısalmasını sağlayacaktır.
- Bunun yanında, *steganografi* yöntemi ile bazı imaj dosyaları içerisinde veri gizlenmesi mümkündür. İsnat edilen suçun niteliği ve kullanıcının bilgisayar üzerindeki becerisi de dikkate alınarak, bu tür kontrolleri yapan araçların kullanılması, imaj içerisinde gizlenmiş delillerin ortaya çıkmasına yardımcı olabilmektedir[21].

4. Delillerin Analizi

Delillerin analiz aşaması, adli bilişim sürecindeki dördüncü aşama olan, toplanan deliller üzerinde gerekli teknik analizlerin yapıldığı aşamadır. Analiz için dikkat edilmesi gereken temel noktalar şunlardır:

- Tüm analizler, delil elde edilmek için kullanılan bilgisayardan farklı bir bilgisayarda yapılmalıdır.
- Analiz işleminde, yalnızca klonlanmış deliller kullanılmalıdır. Bir başka deyişle, orijinal deliller üzerinde, delillerin bütünlüğünü koruyabilmek için, teknik inceleme ve analiz çalışması yapılmamalıdır.
- Orijinal veri ile elde edilen deliller arasında bütünlük ve içerik doğrulama sağlanmalıdır.
- Analiz sürecinde kullanılan her yazılım, donanım ve araç, uygun bir şekilde ve ne amaçla kullandıkları dâhil olmak üzere tutanak altına alınmalıdır.

[21] Altschaffel, R., Kiltz, S., Dittmann, J., "From the Computer Incident Taxonomy to a Computer Forensic Examination Taxonomy", 2009 Fifth International Conference on IT Security Incident Management and IT Forensics, 2009.

- Şüphelinin bilgisayarından elde edilen her türlü dosya, program, uygulama, tarih ve saat bilgisi de yazılarak kayıt altına alınmalıdır.
- En çok aranan nesneler için bir liste oluşturulmalıdır. Tüm hard disk ve diskler için yapılacak delil arama sürecinde, bu anahtar sözcüklerle yeniden arama yapılmalıdır[22].
- Dikkat edilmesi gereken bir diğer önemli nokta da, *unallocated*, *slack space*, *file slack* ya da *swap space* gibi alanlarda bilgisayarın geçmişine ait veriler ve detayların bulunabileceğidir. Bu alanlar, gerekiyorsa tekrar kontrol edilmelidir[23].

5. Raporlama

Adli bilişim sürecindeki son aşama, CMK'nda ve ilgili yönetmeliklerde öngörülen usul kurallarına uygun olarak toplanmış delillerin, yapılan inceleme sonrasında değerlendirilerek, savcılık makamına sunulmasını içeren raporlama aşamasıdır. Bu aşamada dikkat edilmesi gereken teknik hususlar şunlardır:

- Öncelikle, delillerin, kanuna uygun ve ceza muhakemesine esas alınabilecek nitelikte delil olarak kabul edilmesi için, bulunan deliller kanun ve yönetmelikte düzenlenen kurallara uygun olmalı, bir başka deyişle bir sonraki bölümde açıklayacağımız şekilde, CMK'nda öngörülen usullerin tamamına uyularak toplanmış ve incelenmiş olmalıdır.
- Bir delilin, muhakeme makamları olan savcılık ve mahkemece kabul edilmesi için en büyük önceliği, bütünlük ve doğruluğunun sağlanmasıdır[24].
- Analizci, tüm delillerin şüphelinin bilgisayarından alındığını ve bu işlem sırasında kanunda öngörülen tüm sürece ve usul kurallarına uygun hareket edildiğini, raporlar halinde adli makamlara sunmalıdır.
- Tüm deliller, net ve açık olmalı, aşağıda değineceğimiz delillerin gerçek olayı temsil edici özelliğini yansıtmalıdır.
- Tüm araştırma sonucunda verilecek raporda, en başındaki süreç de dahil olmak üzere, bütün süreçler raporlanmalıdır[25]. Zira, analizci muhakeme

[22] Ayers, D., "A second generation computer forensic analysis system", Digital Investigation 6, s. 34-S42, 2009 Aktaran Karaman, Rapor.
[23] Sağıroğlu/Karaman, s. 65.
[24] Abboud, G. / Marean, J. / Yampolskiy, R.V., "Steganography and Visual Cryptography in Computer Forensics", 2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering, 2010.
[25] Rogers, M.K., Seigfried, K., "The future of computer forensics: a needs analysis survey", Elsevier Computers & Security, 23/12-16, 2004; Ekizer, Ahmet Hakan; "Adli Bilişim", http://www.ekizer.net/content/view/16/1/ (01.05.2014).

sürecinde, savcılık yahut mahkeme önünde bu delillerle ilgili ifade verebileceğinden ve muhakemenin ilerleyen safhalarında buna ilişkin detayların unutulması ihtimali bulunduğundan, inceleme ve raporlama aşamalarında bütün detaylar yazılmalı ve yeterli belgelendirme yapılmalıdır.

Adli bilişimin yukarıda açıklanan aşamalarına ilişkin bahsi geçen yasal düzenlemeler, buna göre toplanan delillerin yasaya uygunluğu ve hangi durumlarda "kanuna aykırı delil" sayılarak ceza muhakemesine esas teşkil edemeyeceği hususları, çalışmamızın bundan sonraki bölümünde açıklanacaktır.

E. ELEKTRONİK DELİLLER

1. Ceza Muhakemesinde Delillerin Özellikleri

a. Ceza Muhakemesinde Delil

Ceza muhakemesinde, muhakeme makamları öncelikle önlerine gelen somut olayın maddi yönünü çözmekte, maddi gerçeğin ne olduğunu tespit ettikten sonra bunun hukuki yönünü değerlendirmektedir. Bu nedenle, öncelikli görevi maddi gerçeğe ulaşmak olan ceza mahkemeleri, işlendiği iddia olunan fiilin işlenip işlenmediğini, işlenmişse bu fiilin kanunlar nezdinde bir suç teşkil edip etmediğini ve suç teşkil ediyorsa bunun sanık tarafından işlenip işlenmediğini belirlemek durumundadır[26]. Bu değerlendirme sonucunda hüküm verecek olan hakim, eğer fiilin işlendiğine, suç olduğuna ve sanık tarafından işlendiğine kanaat getirirse, hükmü "*sabit görme*"; ancak bu kriterlerden birinin mevcut bulunmaması durumunda "*sabit görmeme*" biçiminde tezahür edecektir. O halde, birinci durumda maddi gerçek ispatlandığından suçu sabit görülen sanık cezalandırılacak, ikinci durumda ise suç sübut bulmadığından cezalandırılmayacaktır[27]. İşte, hakimin ceza yargılaması esnasında yapacağı maddi olayı çözmek ve bunun için olayın sabit görülüp görülmemesine karar verilmesi olduğundan, yapılacak olan muhakemenin temelinde bu yargıyı oluşturacak delillerin değerlendirilmesi yer almaktadır.

Ceza muhakemesinde, ispat edilecek somut olay geçmişe ilişkin olduğundan ve bu olayların ortaya çıktığı zamanın ve şartların önceden bilinmesi mümkün olmadığından, bu sebeple de hukuk muhakemesinde olduğu gibi delillerin önceden hazırlanamaması sebebiyle, "*delil serbestisi ilkesi*" benimsenmiştir[28].

[26] Toroslu, Nevzat / Feyzioğlu, Metin; Ceza Muhakemesi Hukuku, Ankara, 2006, s. 165-166.
[27] Feyzioğlu, Metin; Ceza Muhakemesinde Vicdani Kanaat, Ankara, 2002, s. 139; Kunter, Nurullah; Ceza Muhakemesi Hukuku, İstanbul, 1989, s. 584; Tosun, Öztekin; Türk Suç Muhakemesi Dersleri, C. I, İstanbul, 1981, s. 585.
[28] Toroslu/Feyzioğlu, s. 168.

Bu nedenle ceza yargılamasında hakim, tarafların ileri sürdüğü delillerle bağlı değildir. Bunun yanında yargılama esnasında süre sınırına bağlı olmaksızın her şey delil olabilir ve her husus her türlü delille ispatlanabilir[29]. Hakim, ortaya konulan bu delilleri değerlendirecek ve bir hususun sabit olduğu hakkındaki hükmünü tam bir inanışla ve kanaatle verecektir (CMK m. 217).

Ne var ki, hakimin delilleri serbestçe değerlendirmesi ve vicdani kanaatle karar vermesi, keyfi hareket edeceği anlamı taşımamaktadır. Hakimin yapacağı değerlendirme akla ve mantığa uygun bir değerlendirme olmak durumunda olduğundan, hakim toplanan hangi delillere neden inanıp inanmadığını ve hangi delilleri hükme neden esas alıp almadığını açıklamak zorundadır. Ancak, bu gerekçeleri açıklamak şartıyla, hakim hem delillerin toplanmasında hem de bu toplanan delillerin değerlendirilmesinde serbestiye sahip olup, bu sisteme "*vicdani delil sistemi*" adı verilmektedir[30].

b. Ceza Muhakemesinde Delillerin Özellikleri

Ceza muhakemesinde delil serbestisi ilkesi ve deliller üzerinde hakimin takdir yetkisi bulunmakta ise de, bu serbesti sınırsız olmayıp, delil sayılabilecek hususların kimi özelliklere sahip olunması aranmaktadır.[31] Buna göre;

i. Deliller **gerçekçi** olmalıdır.

ii. Deliller geçmişte vuku bulan somut olayı **temsil edici** nitelikte olmalıdır. Bir başka deyişle, ceza muhakemesinde deliller geçmişte gerçekleşen olaylarla ilgili olduğundan, ortaya konulan deliller bu olayın tamamını veya bir kısmını yansıtmalı, bu hususta sağlam ve güvenilir emareler taşımalıdır.

iii. Deliller **akılcı** olmalıdır. Bu bağlamda delillerin, maddi gerçeği akla uygun, gerçekçi ve objektif niteliklere dayanan verilerle ispat eder özellikte olması gerekmektedir.

iv. Delillerin **elde edilebilir** olması gerekli olup, somut olarak elde edilerek mahkemenin takdirine sunulması imkan dahilinde olmalıdır.

---

[29] Bu delil serbestisinin bazı istisnaları mevcuttur. Bu istisnaların en önemlisi Yargıtay'ın 24.03.1989 tarihli ve 1988/1 E., 1989/2 K. Sayılı İçtihadı Birleştirme Kararı olup, buna göre imzalı boş kağıdın anlaşma dışı doldurulduğu iddiasıyla açılan ceza davasında, bu fiil Hukuk Usulü Muhakemeleri Kanunu'nun cevaz verdiği istisnai haller dışında tanık beyanıyla ispat edilemeyecektir. Ne var ki, Yargıtay'ın söz konusu İçtihadı Birleştirme Kararı sert eleştirilere uğramış olup, gerçekten de ceza muhakemesinin en temel ilkelerinden birini ihlal eden ve fiilin ortaya çıkışı ve şartlarının yazılı delile bağlanamayacağı bir durum için yalnızca yazılı delille ispat zorunluluğu getiren bu İçtihadı Birleştirme Kararı hukuka açıkça aykırıdır.

[30] Feyzioğlu, s. 49; Kunter, s. 586.

[31] Toroslu/Feyzioğlu, s. 170 vd.; Tosun, C. I, s. 586-587.

v. Deliller **kanuna uygun** olmalıdır. Bu kanuna uygunluk iki biçimde ortaya çıkmaktadır. Buna göre deliller hem kanuna uygun nitelikte delillerden, hem de kanuna uygun yollardan elde edilen delillerden olmalıdır. Bazı deliller, kanuna uygun yollardan elde edilmelerine rağmen, mahkeme makamına sunulduklarında içerikleri sebebiyle delil olarak kullanılamazlar. Örneğin, hekimler, hekim sıfatları sebebiyle hastaları ve bunların yakınları hakkında öğrenmiş oldukları bilgileri, hukuki yollardan elde etmiş olsalar bile, bu kişilerin izinleri olmadan delil olarak mahkemeye sunamazlar. Bazı delillerin ise, elde edilme yöntemleri hukuka aykırı olduğundan dolayı delil olarak kullanılmaları yasaklanmıştır. Örneğin, 5271 sy. Ceza Muhakemesi Kanunu (CMK) md. 148'de yer aldığı üzere, kişinin özgür iradesine dayanmasını engelleyici nitelikte kötü davranma, işkence, ilaç verme, yorma, aldatma, cebir uygulama veya tehditte bulunma, bazı araçlar uygulama gibi kişinin iradesini bozan bedeni yahut ruhi müdahalelerle ya da kanuna aykırı bir menfaat vaadinde bulunarak elde edilen deliller, mahkemede delil olarak kullanılamaz[32].

vi. Deliller **müşterek** olmalıdır. Buna göre, delilin içeriğini yalnız mahkeme makamının bilmesi yetmemekte, bu delilleri muhakemenin taraflarının da bilmesinin sağlanması gerekmektedir. Ceza muhakemesinde buna "*delillerin müşterekliği ilkesi*" denilmekte olup, bu ilke uyarınca sunulan deliller bütün muhakeme taraflarınca tartışılmalı, hakim kişisel bilgisine dayanarak hüküm tesis etmemelidir. Nitekim, dava konusu olay hakkında davanın seyrine etki edecek nitelikte kişisel bilgisi olan hakim, hakim görevinden çekilerek, mahkemede tanıklık yapmalıdır[33].

2. İspatın Konusu

Ceza muhakemesinde, tarafların ihtilaflı olduğu konular dışında uyuştukları konular da ispat konusu olmasına karşın, genel olarak dava konusu fiili ilgilendiren şüpheli olaylar ispat konusu olarak değerlendirilmelidir.[34]

Ceza muhakemesinde, "*delillerin doğrudan doğruyalığı ilkesi*" kabul edilmiştir.[35] Şekli ve maddi anlamda iki boyutu olan delillerin doğrudan doğruyalığı ilkesi şekli olarak, hakim ile deliller ve muhakemeye katılanlar arasında daima bir "ilişkinin" varlığının gerekli olduğu anlamına gelmekte iken, maddi anlamda delillerin doğrudan doğruyalığı ilkesi uyarınca, hakim kanaatini oluştururken

[32] Toroslu/Feyzioğlu, s. 171.
[33] Feyzioğlu, Metin; Ceza Muhakemesi Hukukunda Tanıklık, Ankara, 1996, s. 64.
[34] Leone, Giovanni; Diritto e Procedura Penale, Napoli, 1988, s. 439-440; Kunter, s. 597; Toroslu/Feyzioğlu, s. 172; Yurtcan, Erdener; Ceza Yargılaması Hukuku, İstanbul, 1994, s. 249 vd.
[35] Şahin, Cumhur; Ceza Muhakemesinde İspat, Ankara, 2001, s. 25 vd.

olabildiğince "olaya yakın" delilleri kullanacak, mümkün olduğunca doğrudan, olayı birinci elden ispat eden delillere dayanarak hükmünü tesis edecektir.[36]

Bu bağlamda, söz konusu ilkeler ışığında delilleri değerlendirecek olan hakim, sanığı mahkum edebilmek için gerekli şartların tamamının bulunduğu kanaatine varmak zorundadır. Zira, sanığın beraat etmesi için suçsuzluğunun sabit olması gerekmez, suçlu olduğunun sabit olmaması yeterlidir.[37] Bu itibarla, toplanan delillerin sanığın suçlu olduğunun kabulünü gerektirmesi halinde hakim sanığı cezalandıracak; aksi durumda, sanığın suçlu olduğuna dair yeterli delil bulunmaması durumunda sanık beraat edecektir.

3. Elektronik Delillerin Niteliği

Elektronik deliller (e-delil), "*bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen soruşturma açısından değeri olan bilgi ve verilerdir.*"[38] Elektronik delillerin *latent*, yani gizil yapıda olması, onların incelenmesinin uygun cihazlar ve ölçüm aletleri yardımıyla yapılmasını gerektirir. Çünkü içerdiği bilgiler yalnızca insanın duyu organları ile algılanamaz. Örneğin olay yerinde bulunan bir bıçağın, gerçekten bir bıçak olup olmadığını anlamak amacıyla nitel gözlem yapmak yeterlidir. Ancak yasa kapsamına girip girmediğini anlamak için bıçağın boyu ölçülmelidir. Yani nicel gözlem yapılmalıdır. Buna karşın elektronik delillerin içerisindeki dijital verileri anlayabilmek için ise mutlaka bir uzman tarafından, alet ve cihazlar ile nicel gözlemler yapılmalıdır. Çünkü genellikle makine dili ile kodlanmış olan bilgiler yine bir makine tarafından yorumlanmalıdır[39].

Ceza muhakemesinde kullanılan klasik deliller gözle görülebilir nitelikte, üzerinde el koyma ve muhafaza altına alma kararları verilerek kolayca elde edilebilir deliller iken, bilişim suçlarında söz konusu olan elektronik deliller, klasik delillerden farklı olarak soyut bir yapıya sahiptirler. Şüphesiz ki, elektronik delillerin içerisinde yer aldığı somut bir donanım aygıtı bulunmakta ise de, ceza yargılaması bakımından esas delil teşkil edenler bu donanım aygıtının kendisi değil, içerisinde yer alan dijital nitelikteki delillerdir.

Bu anlamda, çalışmamızın ilk bölümündeki teknik açıklamalardan da hareketle, dijital aygıtlardan elde edilebilecek ve delil oluşturabilecek nitelikteki elektronik deliller şunlar olabilir:

---

[36] Erem, Faruk; Diyalektik Açıdan Ceza Yargılaması Hukuku, Ankara, 1986, s. 290 vd.; Kantar, Baha; Ceza Muhakemeleri Usulü, Birinci Kitap, Ankara, 1957, s. 220; Şahin, s. 257-259; Yurtcan, s. 46.
[37] Leone, s. 440; Toroslu/Feyzioğlu, s. 172.
[38] Keser Berber, Adli Bilişim, s. 46.
[39] Say, s. 29.

- Video görüntüleri,
- Fotoğraflar,
- Yazı dosyaları (Word, Excell, Open Office vb. dosyaları),
- Çeşitli bilgisayar programları,
- İletişim kayıtları (SMS, MSN Messenger, GTalk vb. kayıtları),
- Gizli ve şifreli dosyalar veya klasörler,
- Dosyaların oluşturulma, değiştirilme ve erişim tarih kayıtları,
- Son girilen ve sık kullanılan İnternet siteleri,
- İnternet ortamından indirilen (*download*) dosyalar,
- Ve bu türden olup, silinmiş dosya veya klasörler[40].

F. BİLGİSAYARLARDA ARAMA VE EL KOYMANIN HUKUKİ REJİMİ (CMK M. 134)

1. Ceza Muhakemesinde Arama ve El Koyma

Ceza muhakemesi hukukunda, delillerin toplanmaya başlanabilmesi için öncelikle kanunun öngördüğü yasal durumun oluşması gerekmektedir. Söz konusu yasal durum Ceza Muhakemesi Kanunu'nun 116. maddesinde "*Yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe varsa; şüphelinin veya sanığın üstü, eşyası, konutu, işyeri veya ona ait diğer yerler aranabilir.*" şeklinde düzenlenmiştir. Eğer söz konusu yasal şart somut olayda mevcutsa bu durumda CMK m. 119'a göre arama kararı verilmesi gerekmektedir. Arama kararı verilebilmesinin şartları CMK m. 119'da şu şekilde düzenlenmiştir:

"(1) Hâkim kararı üzerine veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının yazılı emri ile kolluk görevlileri arama yapabilirler.
(2) Arama karar veya emrinde;
a) Aramanın nedenini oluşturan fiil,
b) Aranılacak kişi, aramanın yapılacağı konut veya diğer yerin adresi ya da eşya,
c) Karar veya emrin geçerli olacağı zaman süresi,
Açıkça gösterilir.

[40] Özocak, Gürkan; "Ceza Muhakemesinde Elektronik Delillerin Tespiti ve Toplanması", 2. Uluslararası Bilişim Hukuku Kurultayı Bildiriler Kitabı, İzmir, Kasım 2011, s. 114.

(3) Arama tutanağına işlemi yapanların açık kimlikleri yazılır. Arama sonucunda bazı eşyaya elkoyma söz konusu olduğunda 127 nci maddenin birinci fıkrası hükmü uygulanır.
(4) Cumhuriyet savcısı hazır olmaksızın konut, işyeri veya diğer kapalı yerlerde arama yapabilmek için o yer ihtiyar heyetinden veya komşulardan iki kişi bulundurulur.
(5) Askerî mahallerde yapılacak arama, hâkim veya Cumhuriyet savcısının istem ve katılımıyla askerî makamlar tarafından yerine getirilir."

Dolayısıyla, özellik arzetmeyen eşya ve delil kaynakları bakımından, buralardan delil elde etmek amacıyla arama yapılacağı zaman, CMK m. 119 vd. hükümlerine göre işlem yapılmak durumundadır[41].

2. Bilgisayarlarda Arama ve El Koyma

a. Genel Olarak

Yukarıdaki CMK hükümleri, klasik suçlara ilişkin genel bir arama rejimi ihtiva etmektedir. Oysa bilişim sistemlerinin kullanılması suretiyle işlenen suçlarda yahut klasik suçlara ilişkin delillerin bilgisayar sistemlerinde bulunma ihtimalinin söz konusu olduğu durumlarda, bilgisayarlarda yapılacak arama CMK m. 134'te özel olarak düzenlenmiş olup, bu hallerde arama kararının yalnızca hakim tarafından verilebileceği öngörülmüştür. CMK m. 134 uyarınca;

(1) Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.
(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.
(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.
(4) Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

[41] Aldemir, Hüsnü; Adli – Önleme Arama ve El Koyma, Ankara, 2012, s. 20.

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

b. Tedbirin Amacı

Bilgisayarda Arama ve El Koyma tedbirinin amacı, bilişim sistemleri üzerinde bulunan delillerin elde edilmesidir. Ancak, bilgisayardaki verilerin ilk bölümlerde de açıkladığımız hassas yapısı ve bunların elde edilmesindeki zorluk, verilerin kolayca değiştirilip yok edilebilme ihtimali gibi hususlar nedeniyle, bu tedbir genel arama ve el koyma rejiminden ayrılarak, ayrı bir hüküm ile düzenlenmiştir[42].

c. Tedbirin Şartları

CMK m. 134 uyarınca, bilgisayarlarda ve bilişim sistemlerinde arama ve el koyma işleminin yapılabilmesi için, öncelikle bir suç soruşturmasının varlığı gerekmektedir. Ancak, bu şartı dar anlamda yorumlamamak gerekir. Zira, kovuşturma aşamasında eksik deliller söz konusu ise, elbette bu aşamada da CMK m. 134 uyarınca koruma tedbiri kararı verilebilir[43]. Ayrıca hükme 21.02.2014 tarihinde 6526 sy. Kanun ile bir ibare eklenerek, "*somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı*" şartı da öngörülmüştür. Bu düzenlemeyle, kanun koyucunun CMK m. 134'ün uygulanmasını isabetli bir biçimde zorlaştırdığı ve ancak kuvvetli şüphe doğuracak nitelikte somut emarelerin varlığı halinde bu tedbirin uygulanması yönünde kesin bir irade ortaya koyduğu anlaşılmaktadır. Bu şüphe, uluslararası hukukta "*beyond the reasonable doubt*" da denen, makul şüphenin ötesine geçen, bir suçun işlendiği yönünde çok güçlü işaretler taşıyan bulgulara yönelir. Kuvvetli şüpheyi, hem şüphelinin soruşturma konusu suçu işlediği yönünde, hem de üzerinde arama yapılacak bilgisayarda suç delillerinin bulunacağı yönünde kuvvetli şüphe olarak algılamak gerekmektedir[44].

Bunun yanı sıra, soruşturmada her türlü delil elde etme yönteminin uygulanması, ancak artık başka surette delil elde etme imkanının bulunmaması gerekmektedir. Bir başka deyişle, bilgisayarlarda arama ve el koyma işleminin yapılması delil elde etme açısından son çare olmalıdır. Ne var ki, uygulamada

[42] Özbek, Veli Özer / Kanbur, M. Nihat / Doğan, Koray / Bacaksız, Pınar / Tepe, İlker; Ceza Muhakemesi Hukuku, Ankara, 2012, s. 381.
[43] Baştürk, İhsan; "Bilgisayar Sistemleri ile Verilerinde Arama, Kopyalama ve El Koyma", Fasikül, S. 9, Ağustos 2010, s. 25.
[44] Değirmenci, s. 353.

tedbirin uygulanması için gereken bu önşarta dikkat edildiğini söylemek mümkün değildir.

CMK m. 134, bilgisayarda önce yerince inceleme (arama) yapılmasını, bu şekilde delil elde edilmesi mümkün olmazsa (*bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde*) bilgisayarlara el konulmasını öngörmektedir. Ancak, bu hüküm teknik olarak hatalıdır. Zira, bilgisayarda yerinde inceleme yapılması çoğu kez mümkün olmayıp, tedbirin doğru uygulanışı delilleri koruyucu ve şüphelinin mağduriyetini önleyici tüm önlemlerin alınarak, bilgisayara el konulması ve teknik uzmanlar tarafından laboratuvar ortamında incelenmesidir.

Hükme göre, inceleme kopya üzerine yapılmaktadır. El konulan bilgisayarın (veya daha doğru bir ifadeyle *harddisk*in) kopyası alınıp, orijinali derhal sahibine iade edilmelidir. 21.2.2014 tarihinde yürürlüğe giren ve hükümde değişiklik yapan 6526 sy. Kanun'dan önce, diskin bir kopyasının alınıp şüpheli veya müdafiine verilmesi, şüphelinin isteğine bağlıydı. Ancak uygulamada bu imkanı şüpheliler bir yana, çoğu avukatın dahi bilmemesi karşısında, 6526 sy. Kanun'la yedekleme yapılarak bu yedeğin tutanak ile birlikte şüpheli veya vekiline verilmesi zorunlu hale getirilmiştir. Kanaatimizce, gerek şüphelinin haklarını güvence altına alması, hem de delillerin sıhhatini koruyarak ceza soruşturmasının sağlıklı bir biçimde yürümesini sağlaması bakımından, yapılan değişiklik olumludur.

Nihayet, CMK m. 134'ün uygulanabilmesi için Cumhuriyet savcısının istemi ile tedbire hakimin karar vermesi gerekmektedir. Burada karar verecek olan sulh ceza hakimidir. Diğer koruma tedbirlerinin aksine, suç üstü veya gecikmesinde sakınca bulunan hallerde dahi Cumhuriyet Savcısı bu kararı veremez[45]. Burada dikkat edilmesi gereken husus, kararı veren sulh ceza hakiminin soruşturma bakımından "hakimlik" görevi yapıp yapmadığıdır. Zira, ceza soruşturması esasen Cumhuriyet Savcısı tarafından yürütülmekte ise de, suçüstü ve gecikmesinde sakınca bulunan hallerde soruşturma işlemlerini sulh ceza hakiminin yapması mümkündür. Bu durumda, sulh ceza hakimi "savcılık" sıfatıyla soruşturma görevini yaptığından dolayı CMK m. 134 bağlamında tedbir kararı veremeyecek, bu durumda tedbir kararı aynı yargı çevresinden bir başka sulh ceza hakimi tarafından verilebilecektir[46].

Sonuç olarak şu unutulmamalıdır ki, delil araştırmasının bu aşamasında CMK tarafından öngörülen usule eksiksiz bir biçimde uyulması delillerin hukuki olması ve ceza yargılamasında verilecek hükme esas teşkil edebilmesi

[45] Özen/Baştürk, s. 150.

[46] Kunter, Nurullah / Yenisey, Feridun / Nuhoğlu, Ayşe; Muhakeme Dalı Olarak Ceza Muhakemesi Hukuku, İstanbul, 2007, s. 546.

açısından son derece önemlidir. Zira, ceza muhakemesinde, ancak hukuka uygun yollarla elde edilmiş deliller soruşturma ve yargılamaya konu edilebilir, aksi halde, kanunda öngörülen usullerden birine dahi uyulmaması durumunda, elde edilen delil "kanuna aykırı delil" olacak ve herhangi bir hukuki anlam içermeyecektir. CMK, birçok hükmünde, ceza yargılamasında isnadın ancak kanuna uygun elde edilmiş deliller ile ispatlanabileceği, aksi halde, kanuna aykırı bir delile dayanılarak verilmiş bir hükmün mutlak bir biçimde bozulacağını düzenlemiştir (CMK m. 206, 217, 289/j)[47].

d. Tedbirin Uygulanması (Elektronik Delillerin Toplanması)

Elektronik delillerin toplanmasında, klasik delillerde olduğu gibi olay yeri öne çıkmaktadır. Zira delillerin sağlıklı bir şekilde toplanabilmesi, olay yerine yapılan ilk müdahalenin sağlıklı olup olmamasıyla paralellik göstermektedir. Buna ilişkin açıklamalar, adli bilişime ilişkin teknik açıklamaların yapıldığı bölümde yer almaktadır. Olay yeri tespitiyle ilgili yasal düzenlemelere bakıldığında, karşımıza Adli Önleme ve Aramaları Yönetmeliği çıkmaktadır. Bu yönetmeliğe dayanarak olay yeri incelemesini; suçun aydınlatılması amacıyla olay yerlerinde her türlü iz, eser, emare ve delil niteliği taşıyabilecek bulguların uzmanlaşmış personelce, çeşitli bilimsel, teknik yöntem ve metot kullanarak araştırılması, elde edilen bulguların tespit edilmesi ve kayıt altına alınması (belgelenmesi), toplanması, muhafazası ve incelenmek üzere ilgili yerlere gönderilmesini sağlayan özel amaçlı bir araştırma işlemi olarak tanımlamak mümkündür[48]. Bu gibi durumlarda, klasik suçlarda söz konusu olduğu gibi, olay yerinin güvenliğinin sağlanması ve delillerin toplanması ile ilgisi bulunmayan kişilerin olay mahallinden uzaklaştırılması önem taşımaktadır. Bu şekilde, delil

---

[47] Ne var ki, özellikle Yargıtay'ın son dönem kararlarında yalnızca usul kurallarına uymamanın başlı başına hak ihlali oluşturmayacağı, eğer bu yolla delil elde edilmişse, sadece şekli aykırılığa dayanarak delilin geçersiz sayılamayacağı söylenmektedir. Yargıtay'ın, ceza muhakemesi hukukunun en temel ilkelerine dahi aykırı olan bu görüşüne katılmak imkansızdır:
"Her şekle aykırılığın aynı zamanda bir hak ihlaline de yol açacağı şeklinde bir kabulün doğru olmadığını, bu anlamda, söz konusu olayda olduğu gibi 'Cumhuriyet savcısı, iki ihtiyar heyeti üyesi veya iki komşu' bulunmadan yapılan bir aramada, CYY'nın 119. Maddesine şekli bir aykırılık söz konusu ise de; herhangi bir hakkın ihlal edildiğini söylemenin son derece güç olduğu,
Usulüne göre alınmış arama kararına istinaden, herhangi bir hak ihlaline neden olunmadan yapılan arama sonucunda ele geçen delillerin, sırf arama sırasında bulunması gereken kişilerin orada bulundurulmaması suretiyle şekle aykırı hareket edildiğinden bahisle 'hukuka aykırı elde edilmiş delil' kabul edilemeyeceği..." Yargıtay CGK, 13.3.2012, 2011/8-278 E. ve 2012/96 K. Bkz. Eryılmaz, Mesut Bedri; Ceza Muhakemesi Hukuku Dersleri, Ankara, 2012, s. 140.

[48] Say, s. 22.

elde edilecek elektronik donanımların korunabilmeleri ve elde edilmesi amaçlanan delillerin zarar görmemesi sağlanabilmektedir. Bu aşamada yapılacak en doğru şey, delil toplaması için olay yerine bir adli bilişim uzmanının getirilmesi olacaktır. Bu gibi durumlarda adli bilişim uzmanı delil kaybı ihtimalini asgariye indirerek elektronik delilleri toplayabilecektir[49].

Ancak olay yerinde elektronik delillerden farklı olarak klasik suç delillerinin yer alması da kuvvetle muhtemeldir. Özellikle söz konusu bir bilgisayar olunca, klavye ve fare *(mouse)* üzerinde bulunabilecek parmak izleri, mahalde bulunan şüpheliye ait giysiler, eşyalar vb. unsurlar da birer delildir. Bu nedenle, bu aşamada delil toplanırken kriminalistik inceleme de ihmal edilmemelidir. Ancak bu, toplanması ve incelenmesi azami hassasiyet gerektiren potansiyel dijital delillere zarar vermeden yapılmalıdır[50]. Örneğin, bir CD üzerinde yapılacak parmak izi araştırması, kullanılan kimyasallar CD'nin içerisindeki bilgilerin kaybını doğurabileceğinden, klasik suçlara ilişkin kriminal veri toplama ile adli bilişim verileri toplama arasında makul bir denge tutturulmalı, birine ilişkin inceleme yapılırken diğeri ile ilgili potansiyel delillere zarar verilmemeli ve mümkünse klasik delil toplanırken kullanılacak olan kimyasal maddelerin kullanımı, elektronik delilin kurtarılması işlemi tamamlanıncaya kadar ertelenmelidir[51].

Eğer yapılan olay yeri incelemesi sonrasında potansiyel delillerin bulunduğu bilgisayar muhafaza altına alınacaksa, söz konusu aygıtların hassas yapıları gereği paketlenmesi, taşınması gibi hususlara özen gösterilmeli; söz konusu araçlar sarsıntı, elektrik akımı, elektromanyetik ortamlar, aşırı sıcak, sıvı maddelerle temas gibi işlevlerini olumsuz yönde etkileyecek ve delil niteliğini ortadan kaldıracak zararlı etkilerden korunmalıdır[52].

Önceki bölümlerde de vurguladığımız üzere, elektronik deliller üzerinde yapılacak incelemeler, donanımlar üzerinde değil, bunlardan alınan kopyalar üzerinde yapılmalıdır. Bu metot, söz konusu elektronik donanımlar içerisinde oluşması muhtemel veri kayıplarını önlemeye yönelik delil toplama sürecine katkı sağlayacaktır[53]. Bilgisayarlardan inceleme yapılmak üzere kopya alınacağı durumlarda uyulacak olan rejim, CMK'nun 134. maddesinin 2., 3., 4. ve 5. fıkralarında düzenlenmiştir. Bu tedbirin uygulanma koşulları yukarıda açıklanmış olup, bu koşullardan herhangi birine uyulmaması durumunda,

[49] Adli bilişim uzmanı ve nitelikleri hakkında ayrıntılı bilgi için bkz. Keser Berber, Leyla; "Adli Bilişim Uzmanı Kimdir?", http://turk.internet.com/haber/yaziyaz.php3?yaziid=16728. (31.01.2014)

[50] Karakuş, Oğuz; Kriminalistik, Ankara, 2009, s. 512-513.

[51] Karakuş, s. 513; Özdilek, Ali Osman; Bilişim Suçları ve Hukuku, İstanbul, 2006, s. 221, Özocak, s. 119.

[52] El konulan bilgisayar donanımının el konma ve taşınma işlemleri esnasında dikkat edilmesi gereken hususlar hakkında bilgi için bkz. Say, s. 39-41.

[53] Ekizer, a.g.e (01.05.2014).

bilgisayarlardan veya bilişim sistemlerinden elde edilen delil hukuka aykırı olacak ve ceza muhakemesi süreçlerinde delil olarak kullanılamayacaktır.

Adli bilişimde, elektronik donanımların içerisinden yapılan birebir kopyalama işlemine imaj (*forensic image*) adı verilmektedir. Bu kopyalama işlemi, sistemdeki tüm verilerin özel yazılımlar kullanılmak suretiyle ve düşük seviye bit bazında başka bir ortamda bir örneğinin (*imajının yahut görüntüsünün*) oluşturulması ile yapılmaktadır. Burada düşük seviye bit bazında kopyalama yapılmasının nedeni, daha sonra yapılacak incelemelerde silinmiş, değiştirilmiş veya bozulmuş verilere de ulaşma olanağının bulunuyor olmasıdır. Söz konusu imaj alma işlemi yapılırken, manyetik yahut optik medyaların *bit-to-bit* (*sector-by-sector*) imajı alınmakta, orijinal medya üzerinde herhangi bir değişiklik yapılmamakta ve alınan imajların bütünlüğünün sağlanması *hash* değerleri hesaplanarak yapılmaktadır[54].

Delil çıkartma aşamasında, silinen dosya, klasör ve bölümler (*partition*) kurtarılmakta, medya üzerindeki swap alanından, *slack* alanlardan, *unallocated* bölümlerden, geçici dosyalardan delil olabilecek veriler çıkartılmaktadır. Ayrıca, *hash* fonksiyonları kullanılarak bilinen dosyalar (*known files*) elimine edilerek, incelenecek dosya sayısı azaltılmaktadır. Delil çıkartma aşamasında, medyadan delil olabilecek dosyalar çıkartılmış olmaktadır. Delil çıkartma işlemleri ve safhaları da, yine teknik açıklamaların yapıldığı bölümde ayrıntısıyla anlatılmıştır.

e. Tedbirin Temel Hak ve Özgürlükler Açısından Değerlendirilmesi

CMK m. 134'de öngörülen düzenleme, her koruma tedbiri gibi, kişilerin temel hak ve özgürlüklerine müdahale niteliği taşımaktadır. Bilgisayarlarda ve bilgisayar kütüklerinde arama yapılması ve bunlara el konulması da, kişilerin özel hayatlarının gizliliğine ve mülkiyet haklarına müdahale edilmesini beraberinde getirmektedir.

Devlet tarafından kişilerin temel hak ve özgürlüklerinin kullanımı veya sınırlandırılması bakımından herhangi bir ayrım yapılamaz. Temel hak ve özgürlükler, insanların yalnızca insan olmaları sebebiyle sahip oldukları temel değerlerdir. Devlet tarafından bu hakların uygulanmasında veya sınırlandırılmasında usulsüz bir şekilde ayrım yapılması veya bu haklara haksız bir müdahalede bulunulması durumunda da, Avrupa İnsan Hakları Sözleşmesi'nin (AİHS) ihlali söz konusu olacaktır[55].

---

[54] Şen, Osman Nihat; "Adli Bilişim Bilimi ve Diğer Bilimlerle Olan İlişkisi" http://www.bilgisayarpolisi.com/index.php?sayfa=makaleoku&kategori=11&id=121 (18.05.2014).

[55] Şen, Ersan / Özdemir, Bilgehan; Tutuklama – Uygulamada Şüpheli ve Sanık Haklarının Korunması, Ankara, 2011, s. 50; Değirmenci, s. 97.

Bu nedenle, söz konusu tedbirin AİHS'ne ve Anayasa'ya uygun olmasının sağlanması için, CMK m. 134'teki hükümler düzenlenmiştir. Zira, CMK m. 134'ün öncelikli olarak ilgilendirdiği temel hak olan Özel Hayatın Korunması, AİHS'nin 8. Maddesinde güvence altına alınmıştır. Buna göre, söz konusu hak bir insan hakkı olup, bu hakkın ancak istisnai hallerde ve kanun ile sınırlandırılabilmesi mümkündür.

Bu bağlamda, CMK m. 134 de genel arama ve el koyma hükmünden ayrılarak, özel hayatın gizliliğine kanuni müdahalenin şartlarını düzenlemiş, bunu hakim kararı şartına bağlamış, temin edici kimi usuller öngörmüş ve istisnai bir durum olarak yalnızca suç şüphesi olması durumunda ve başka surette delil elde edilemediğinde bu tedbire başvurulacağını ifade etmiştir[56].

Bunun dışında, bilgisayarlara yapılacak müdahaleye ilişkin olarak bu tedbir, haberleşme özgürlüğü, düşünceyi açıklama ve yayma özgürlüğü, kişisel verilerin korunması hakkı ile de yakından ilgilidir. Dolayısıyla, bu temel haklara yapılacak haksız bir müdahalenin hukuka aykırılık oluşturacağı düşünüldüğünde, yukarıdaki usul kurallarına harfiyen uymanın önemi bir kez daha ortaya çıkmaktadır[57].

f. Elektronik Delillerin Toplanması (CMK m. 134) ile ilgili Sorunlar ve Çözüm Önerileri

Elektronik delillerin toplanması ile ilgili olarak, CMK m. 134'ün gerek kaleme alınışı ile ilgili, gerekse uygulanmasına ilişkin olarak birçok sorun ortaya çıkmaktadır.

Bu sorunların başında, elektronik delil elde etme amacıyla, hakim kararıyla bilgisayarlara el koyan kolluk kuvvetlerinin CMK m. 134'te yer alan hususlara uygun işlem yapmaması gelmektedir. Zira bu hüküm uyarınca bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir. Ancak şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, el konulan cihazlar gecikme olmaksızın iade edilir. Bununla beraber bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. İstenmesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır. Bilgisayar veya bilgisayar kütüklerine el koymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır (CMK m. 134/2, 3, 4, 5).

[56] Özbek/Kanbur/Doğan/Bacaksız/Tepe, s. 380.
[57] Değirmenci, s. 98 vd.

Bu koşullardan, özellikle, bilgisayarlara el konulması esnasında sistemdeki bütün verilerin yedeklemesinin yapılması ve bu yedekten bir kopyanın şüpheliye veya vekiline verilmesi çok önemlidir. Önceki dönemde bu talep hakkından çoğu avukatın dahi haberdar olmaması nedeniyle atıl olan bir hüküm, madde metninde yapılan değişiklikle zorunlu hale getirilmiştir. Ancak, inceleme yapılacak olan harddiskten yedek alınması yeterli değildir. Delillerin alındığı aşamadaki sıhhatinin korunması amacıyla, işlemi yapan kolluk tarafından, bilgisayarın harddiski alındığı anda öncelikle *hash değeri* alınarak tutanak tutulmalı ve bütün bu imaj alma, yedekleme vb. işlemler şüpheli veya vekilinin yanında gerçekleştirilmelidir. Zira, söz konusu yedekleme işlemi yapılmaz ve kişinin bilgisayarına öylece el konulursa, sistemde değiştirilmesi son derece basit olan verilerin, bilgisayarına el konulan kişi aleyhine değiştirilmesi durumunda kişinin hiçbir güvencesi kalmayacak ve bu durum neticesinde kişi en temel hak ve özgürlüklerine halel gelecek biçimde mağdur olabilecektir. Nitekim, CMK'nda yer alan koruma tedbirleri kişilerin temel hak ve özgürlüklerini kısıtlayıcı tedbirler olduğundan, bu tedbirler uygulanırken muhakeme yönünden doğabilecek zararın ağırlığı ve bunun gerçekleşmesi ihtimalinin yoğunluğu ile orantılı olması gerekliliğinin yanı sıra[58], tedbir uygulanırken aleyhine uygulanan kişinin temel hak ve özgürlüklerinin hukuki sınırları aşar biçimde sınırlandırılmamasına ve kişisel verilerinin zarar görmemesine dikkat edilmesi gerekmektedir. Zira, özellikle CMK m. 134'teki koruma tedbirinin uygulanmasında, ceza muhakemesinin amacına uygun bir şekilde kişisel verilerin korunması, tedbiri uygulayan makamların birincil görevi olmalıdır[59].

Bunun yanı sıra, bu yedekleme işleminin el koymadan sonra değil, bizatihi el koyma işlemi esnasında yapılması elzemdir. Zira, el koyma işlemi gerçekleştirildikten sonra çıkartılacak bir yedeğin güvenilirliğinin şüpheli olduğu ve soruşturma evresi yönünden potansiyel ispat sorunları doğurabileceği tartışmasızdır[60].

5271 sy. CMK'nun yanında, 5070 sy. Elektronik İmza Kanunu, Polis Vazife ve Salahiyet Kanunu, Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik ve Telekomünikasyon Sektöründe Tüketici Hakları Yönetmeliği gibi birçok hukuki düzenlemede ve OECD, Avrupa Konseyi, Birleşmiş Milletler ve Avrupa Birliği'nin de birçok düzenlemesinde kişisel verilerin korunması titizlikle hüküm altına alınmıştır[61]. Buna karşın, uygulamada CMK hükmündeki hususlara, özellikle de yedek-

[58] Toroslu/Feyzioğlu, s. 211.
[59] Küzeci, Elif; Kişisel Verilerin Korunması, Ankara, 2010, s. 291 vd.
[60] Özen, Muharrem / Baştürk, İhsan; Bilişim – İnternet ve Ceza Hukuku, Ankara, 2011, s. 158-159.
[61] Keser Berber, Leyla / Lostar, Murat; Bilişimde Biyometrik Yöntemler, Ankara, 2006, s. 82 vd.

leme zorunluluğuna dikkat edilmemesi ve buna paralel olarak kişisel verilere zarar verilmesi, elektronik delillerin toplanması ile ilgili sorunların başında gelmektedir.

Bir başka ve önemli sorun ise, cep telefonlarına el konulması biçiminde tezahür eden koruma tedbirinin uygulanmasında ortaya çıkmaktadır. CMK m. 134, yalnızca bilgisayar ve bilgisayar kütüklerinde yapılacak arama, kopyalama ve el koyma işlemlerinden bahsetmektedir. Bu nedenle, bilgisayar dışındaki eşyalar üzerinde yapılacak arama ve el koyma işlemleri, CMK m. 116 – 129 hükümleri uyarınca yapılmaktadır. Buna göre, yakalanabileceği veya suç delillerinin elde edilebileceği hususunda makul şüphe varsa; şüphelinin veya sanığın üstü, eşyası, konutu, işyeri veya ona ait diğer yerler, hâkim kararı üzerine veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının, Cumhuriyet savcısına ulaşılamadığı hallerde ise kolluk amirinin yazılı emri ile aranabilir. Bununla beraber, hâkim kararı üzerine veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının, Cumhuriyet savcısına ulaşılamadığı hallerde ise kolluk amirinin yazılı emri ile kolluk görevlileri, el koyma işlemini gerçekleştirebilir (CMK m. 127). Buna göre, CMK m. 134'ten farklı olmak üzere, bilgisayar dışındaki eşyalara el konulması hakim dışında Cumhuriyet savcısı ve ona ulaşılamaması durumunda kolluk amirinin vereceği yazılı emir ile mümkün olabilmektedir[62].

Ancak günümüzde, gelişen teknoloji ile birlikte, elektronik donanımı düşünüldüğünde birçok cep telefonu bilgisayardan farksız olup, bir bilgisayarla yapılabilecek her şey (*İnternet bağlantısı, e-posta haberleşmesi, kelime işlemci programlarının kullanımı, veri saklanması vb.*) yeni teknoloji cep telefonlarıyla da yapılabilmektedir. Ne var ki, bir suç şüphesinin var olduğu durumlarda, bilgisayarlardan farklı olmak üzere, cep telefonlarına kolluk amirinin yazılı emriyle el konulabilmekte ve bu el koyma işlemi esnasında hiçbir şekilde yedekleme vb. önlemlere başvurulmamaktadır. Hiç şüphe yok ki, uygulamadaki bu sorun, yukarıda bahsettiğimiz temel hak ve özgürlüklere doğrudan zarar verici nitelikte olup, kişilerin kişisel verilerinin ve özel hayatlarının gizliliğine de evrensel hukuka aykırı bir biçimde müdahale anlamına gelmektedir[63]. Cep telefonlarına el konulması ile ilgili olarak, şöyle bir ayrım yapılması doğru olacaktır:

i. Eğer cep telefonunda yapılan arama – el koyma işlemi, cihazın telefon özelliği ile ilgiliyse; örneğin, konuşma veya mesaj kayıtları incelenecekse, bu durumda genel arama hükmü olan **CMK m. 119**;

[62] Özocak, s. 120-121.
[63] Küzeci, s. 296 vd.; Uçkan, Özgür / Beceni, Yasin; "Bilişim-İletişim Teknolojileri ve Ceza Hukuku", İnternet ve Hukuk, İstanbul, 2004, s. 372.

ii. Yapılan arama – el koyma işlemi, cihazın bilgisayar özelliği ile ilgiliyse; örneğin, arama motoru, trafik kaydı, e-posta kayıtları vb. incelenecekse, bu durumda özel arama hükmü olan **CMK m. 134** uygulanmalıdır.

CMK m. 134'ün uygulanmasında yaşanan bir diğer sorun, hükmün 2. fıkrasındaki, gerekli kopyaların alınması sonrası, el konulan cihazların gecikmeksizin iade edileceğine dair kuraldır. Bu husus, hiç şüphe yok ki, şüphelinin haklarını teminat altına almak amacıyla düzenlenmiştir. Ne var ki, özellikle suçun konusu olan verilerin cihazın içinde yer aldığı örneklerde, bu hüküm ciddi sorunlar doğurmaktadır. Örneğin; TCK m. 226'da düzenlenen Müstehcenlik suçunda çocuk pornografisi içeren görüntülerin yahut TCK m. 245 uyarınca yapılan bir aramada ele geçirilen mağdurun kredi kart bilgilerinin el konulan hard diskin içinde bulunduğu durumlarda, bu cihazların kopyalama sonrası şüpheliye iade edilmesi, suçun işlenmesine devam edilmesine kanun tarafından cevaz verilmesi anlamına gelecektir. Bu gibi durumlarda TCK m. 55 uyarınca eşya müsaderesi gündeme gelebilecekse de, CMK m. 134'ün bu ayrıksı durumlara ilişkin bir düzenleme öngörmemiş olması kanımızca önemli bir eksikliktir.

Elektronik deliller, kişilerin kişisel verilerini barındıran ve tamamen özel hayatına ilişkin eşyalarında (bilgisayar, cep telefonu vb.) yer aldığından, bunlara yapılacak ulusal ve evrensel hukukun sınırlarını aşar bir müdahale, iç hukukta ve bilhassa uluslararası hukukta koruma altına alınan "*özel hayatın gizliliği hakkı*"nı da ihlal etmektedir. Elbette, özel hayatın gizliliği hakkı çeşitli hukuki temellere dayandırılabilmektedir. Ancak konumuzla ilgili olarak, özel hayatın gizliliği hakkı, teknolojik gelişmeler karşısında kişinin güvenliğinin güvence altına alınması anlamında tanımlanabilir[64]. Ne var ki, uygulamadaki bu sorunlar, kişilerin özel hayatlarının gizliliğini de ihlal edici nitelik taşımakta olup, yapılacak yasal düzenlemeler ve bunların yetkili makamlarca takibi ile bu sorunlar asgari düzeye indirilebilir.

Bu bağlamda, ilk etapta yapılması gerekenler;

- CMK m. 134'teki düzenlemenin yeniden kaleme alınması gerekmektedir. Hükmün 5. Fıkrasındaki "*kopyalanan verilerin kağıda dökülmesi*" gibi uygulanması hem gereksiz, hem de bazen maddi olarak imkansız (*tele baytlarca verinin kağıda dökülmesi gibi*) kuralların yapılacak yeni düzenlemede yer almaması gerekmektedir.
- Buna göre, elektronik delillerin nasıl toplanacağı daha detaylı bir biçimde düzenlenmeli, *hash* değeri alınması gibi teknik zorunluluklar yasada da öngörülmeli ve kopyalanan verilerin yedeğinin şüpheli veya vekiline verilmesi zorunlu tutulmalıdır.

[64] Er, Cüneyd; Biyometrik Yöntemler ve Özel Hayatın Gizliliği Hakkı, Ankara, 2007, s. 79.

- Günümüzde en az bilgisayarlar kadar arama ve el koyma tedbirine tabi tutulan akıllı telefonlar da düzenlemeye dahil edilmeli ve yukarıda yaptığımız ayrım bağlamında, bilgisayar özellikleri nedeniyle arama işlemi yapılan cep telefonlarına ilişkin tedbirler de bilgisayarlarla aynı düzenlemeye tabi kılınmalıdır.
- Uygulamada kolluktan kaynaklanan sorunların çözümü için bir ilk adım olarak, elektronik delil temininde CMK ve ilgili yönetmeliklerdeki usul kurallarına uygun hareket etmeyen kamu görevlileri bakımından caydırıcı yaptırımlar öngörülmelidir[65].
- CMK m. 134 belirli bir ağırlık ölçüsü aranmaksızın tüm suçlar için başvurulabilecek bir koruma tedbiri olarak öngörülmüştür. Temel hak ve özgürlüklere bu denli müdahale içeren bir tedbire, ancak belirli bir ağırlığın üzerindeki suçlar için başvurmak yerinde olacağından, kanun metninde bu ağır suçların tahdidi olarak sayılacağı yeni bir düzenleme yoluna gidilmelidir[66].

G. ULUSLARARASI HUKUKTA ELEKTRONİK DELİLLERİN TOPLANMASINDA UYULACAK İLKELERE İLİŞKİN DÜZENLEMELER VE GÜNCEL SORUNLAR[67]

Avrupa Birliği'nin 24 Ekim 1995 tarihli ve 95/46/EC sayılı yönergesi uyarınca, verilerin yalnız açıkça ve hukuka uygun olarak belirlenmiş bir amaç için toplanması ve işlenmesi mümkündür. Dolayısıyla bu amacın yazılı olarak belirlenmesi ve kesin bir biçimde ortaya konulması gerekmektedir. Ayrıca illiyet ilkesi uyarınca, toplanan verilerin ancak söz konusu amaç için gerekli olmaları halinde işleme konulmaları mümkündür. Yine elde edilen verilerin saklanma süresi de, bu amaç doğrultusunda belirlenmeli, belirlenen makul süre içerisinde güncel ve doğru kalmaları güvence altına alınmalıdır[68].

Bununla beraber, elektronik delillerin toplanmasında dikkat edilecek en önemli hususlar olan kişisel verilerin korunması ilkesi ve özel hayatın gizliliği hakkı da, uluslararası hukuk metinlerinde düzenlenmiş ve güvence altına alınmıştır. Birleşmiş Milletler (BM) İnsan Hakları Evrensel Beyannamesi'nin 12. maddesi başta olmak üzere, BM Medeni ve Siyasi Haklara Dair Uluslar arası Misak'ın 17. maddesi, BM'nin çeşitli tarihlerde çıkarttığı Kişisel Verilerin

[65] Özocak, s. 121.
[66] Özen/Baştürk, s. 164.
[67] Makalenin bu kısmı, 2. Uluslararası Bilişim Hukuku Kurultayı Bildiriler Kitabı'nda yer alan tebliğimizdeki aynı başlıklı bölümün güncellenmiş halidir. Bkz. Özocak, s. 122-123.
[68] Er, s. 87.

Korunmasına Dair İlke Kararları'nda, OECD'nin çeşitli tarihlerde çıkartmış olduğu ilke kararlarında[69], Avrupa Birliği Yönergelerinde, Avrupa İnsan Hakları Sözleşmesi'nin 8. maddesinde, Avrupa Konseyince çıkartılan Kişisel Verilerin Korunmasına Dair Avrupa Konseyi Sözleşmesi'nde ve daha birçok Uluslar arası metinde özel hayatın gizliliği ve kişisel verilerin korunması güvence altına alınmış olup, elektronik deliller toplanırken uygulanacak olan tedbirler ve yapılacak olan işlemlerin bütün aşamalarında, ulusal ve uluslararası mevzuatta yapılan düzenlemelere ve konulan kurallara riayet edilmesi gerekmektedir[70].

Avrupa ülkelerindeki teknolojik gelişmelerin ülkemize göre daha ileri düzeyde olduğu gerçeğine paralel olarak, siber suçlar ve bilişim sistemlerine yapılan saldırıların sayısı da gün geçtikçe artmaktadır. Örneğin, Alman Federal Hükümetinin birkaç yıl önce açıkladığı resmi verilere göre, yalnızca Almanya'da bir günde yaklaşık 43 bin sanal saldırı meydana gelmekte[71] olup, bu saldırıların sayısı her geçen gün artmaktadır. Bu bağlamda, 23.11.2001'de Budapeşte'de imzalanan Avrupa Konseyi Siber Suçlar Sözlşemesi'nin 25. maddesine göre, sözleşmenin imzacısı olan ülkeler, siber suçların faillerinin ortaya çıkarılabilmesi için elektronik delillerin toplanması konusunda birbirlerine her türlü yardımı göstermek durumundadırlar. Bunun yanında, Kasım 2009'da da Avrupa Komisyonu bir devletten diğer devlete delil toplanması ile ilgili bir "*Green Paper*"[72] yayınlamış, bu bağlamda devletler arası delil toplanması konusundaki yardımlaşmanın artması amacıyla bir ortak kabul (*mutual recognition*) mekanizması oluşturulmuştur.[73] Ne var ki bu konuyla ilgili Avrupa Konseyi'nde ve akademik alanda tartışmalar devam etmekte olup, konunun bir ortak kabulden ziyade ortak yardımlaşma (*mutual legal assistance*) ağı oluşturularak çözümlenmesi gerektiği, ülkelerin hukuk sistemlerini birbirleriyle ortaklaştırmalarındansa birbirlerinden yarım isteyerek her ülkenin kendi hukuk düzenine uygun bir biçimde diğer ülkenin istediği elektronik delilleri toplayarak diğerine vermesi gerektiği söylenmektedir.[74]

---

[69] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD, http://www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html. (22.04.2014)

[70] Er, s. 79-103; Keser Berber / Lostar, s. 94-98. Ayrıca söz konusu uluslararası düzenlemelere ilişkin detaylı bilgi için Bkz. Küzeci, s. 116 vd.

[71] http://www.veteknoloji.com/almanya-siber-guvenlik-kararghi-kuruyor-39333—0.html. (24.04.2014).

[72] Avrupa Birliği politkaları hakkında hazırlanan ve içerisinde işlemin konusuna ilişkin kimi teklifleri barındıran düzenleyici işlemler.

[73] Spencer, John R.; "The Green Paper on obtaining evidence from one Member State to another and securing its admissibility: the Reaction of one British Lawyer", http://www.zis-online.com/dat/artikel/2010_9_492.pdf, s. 602. (24.04.2014)

[74] Spencer, s. 604-606.

Bununla birlikte, özellikle Almanya siber suçlarla mücadele ve buna ilişkin elektronik delillerin toplanması konusunda çalışmaların yapıldığı ve yoğun tartışmaların yaşandığı ülkelerin başında gelmektedir. Bu ülkede, açıklanan resmi rakamlara göre bir günde onbinlerce sanal saldırı olmakta, siber suçlulukla mücadelede devletin yetersiz kaldığı eleştirileri yapılmaktadır. Yakın zamanda Alman İç İşleri Bakanlığı bu saldırılarla mücadele etmek amacıyla "*Uzaktan Adli Yazılım*" (*Remote Forensic Software*) adı verilen bir *Trojan* virüsü tasarlayarak, siber suç faili olduğundan şüphelenilen kişilerin bilgisayarlarına girme konusunda çalışmalar yapmaya başlamıştır[75]. Ancak Alman Federal Hükümetinin bu çalışmaları, oluşturulan yazılımla yalnızca "şüpheli hareketler" tespit edileceğinden, bu yolla yanlış delillere de gidilebileceği ve birçok kimsenin bu nedenle iletişim özgürlüğünün ve daha birçok temel hak ve özgürlüğünün kısıtlanacağı yönünde eleştirilere neden olmuş; buna rağmen, Alman hükümeti birkaç yıl önce çıkardığı yasayla siber suçlulukla mücadele adına elektronik delillere ulaşılabilmesi amacıyla üzerinde suç şüphesi olduğu düşünülen kişilerin bilgisayarlarına, telefonlarına, e-posta adreslerine girmesini kolaylaştırmış ve bu bağlamda, federal polisin gözaltı ve soruşturma yetkilerini arttırmıştır. Yasa çıktıktan sonra da Alman Meclisinde ve basında sıkça tartışılmış, muhalefet söz konusu yasaya kişilerin Anayasa tarafından garanti altına alınan en temel haklarının ihlal edildiği ve Doğu Almanya istihbarat birimi olan *Stasi*'ye benzer bir denetim mekanizmasının yaratıldığı gerekçesiyle karşı çıkmış, nitekim düzenleme Alman Anayasa Mahkemesi tarafından iptal edilmiştir[76].

Ancak bütün bu düzenlemelere ve tartışmalara rağmen alınan tedbirler ve çıkarılan yasalar Almanya'da siber suçlulukla mücadele ve delillere ulaşma konusunda yeterli olmamış, bu nedenle henüz birkaç yıl önce Federal hükümet tarafından bir "siber güvenlik stratejisi" hazırlanarak Köln'de, emniyet mensupları, istihbarat uzmanları, bilişim uzmanları ve özel sektörden gelen uzmanlardan teşekkül eden bir "Siber Savunma Merkezi" kurulmuştur[77].

[75] http://www.spiegel.de/international/germany/0,1518,502955,00.html. (24.04.2014).
[76] http://www.spiegel.de/international/germany/0,1518,590198,00.html. (24.04.2014).
[77] http://www.dw.de/almanyadan-siber-savunma-hamlesi/a-14739247 (23.10.2014).

H. SONUÇ

Günümüz suç dünyasında artık insan öldürme dahil olmak üzere her suçun bilişim araçlarıyla işlenebilmesi söz konusu olduğundan, ceza muhakemesi hukukunda da kağıt delillerin yerini, başta bilgisayarlar olmak üzere bilişim sistemlerinin içinde yer alan dijital deliller almıştır. Ne var ki, tespiti ve toplanması son derece hassas olan ve teknik uzmanlık gerektiren elektronik deliller, gerek iç hukukta, gerekse uluslararası hukuk metinlerinde düzenlenen insan hakları ilkeleriyle çatışma yaratabilecek uygulamalar ortaya çıkarabilmektedir. 5271 sayılı CMK'nun bilgisayarlarda yapılacak aramalara ilişkin kurallarına uyulmaması, özel hayatın gizliliği ve kişisel verilerin korunması gibi evrensel insan hakları metinleriyle güvence altına alınmış ilkelerin ihlali sonucunu ortaya çıkarabilmektedir.

Bu sorunların çözümünün iki ayağı vardır. Bunların ilki, kanun koyucunun yetki ve sorumluluğundadır. Kanun koyucu, konuyla ilgili çalışmalar yapan hukukçular ve bilişim uzmanlarıyla bir araya gelerek, başta Ceza Muhakemesi Kanunu olmak üzere, konuyla ilgili tüm kanun metinlerinde hem gelişen teknolojinin ihtiyaçlarına cevap verebilecek, hem de bireylerin özel hayatlarının gizliliğini teminat altına alacak yeni düzenlemeleri acilen yapmalıdır. Bilgisayarlarda arama ve el koyma tedbirini öngören CMK m. 134 ivedilikle yeniden düzenlenmeli, hüküm teknolojik ilerlemeye uygun hale getirilmeli ve özellikle *hash değeri* alınması gibi şüphelinin haklarını ve ceza soruşturmasının selametini garanti altına alacak teknik hususlar hükmin kapsamına alınmalıdır.

İkinci ve daha önemli görev ve sorumluluk ise uygulayıcıda, yani kolluktadır. Kolluk, en azından teorik olarak, bir ülkede kanunların uygulanmasının teminatıdır. Bu itibarla, somut olayda şüpheli veya müdafinin kendisine hatırlatmasını beklemeden, kanun hükmünde öngörülen usul kurallarını harfiyen yerine getirmeli, normu titizlikle uygulamalı, kanundan doğan yetkilerini kötüye kullanmadan ve insanlığın evrensel kazanımlarına zarar vermeden, gerektiğinde şüpheliden evvel şüphelinin hakkını koruyarak söz konusu tedbiri tatbik etmelidir. Aksi halde, Dünyanın en çağdaş ve teknolojik gereklere en uygun kanun metni dahi hazırlansa, kötü bir uygulayıcının elinde, bunların kağıda yazılı boş sözlerden öte gitmeyeceği açıktır.

KAYNAKÇA

Abboud, G., Marean, J., Yampolskiy, R.V., "Steganography and Visual Cryptography in Computer Forensics", 2010 Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering, 2010.

Aldemir, Hüsnü; Adli – Önleme Arama ve El Koyma, Ankara, 2012.

Altschaffel, R., Kiltz, S., Dittmann, J., "From the Computer Incident Taxonomy to a Computer Forensic Examination Taxonomy", 2009 Fifth International Conference on IT Security Incident Management and IT Forensics, 2009.

Ayers, D., "A second generation computer forensic analysis system", Digital Investigation 6, 2009.

Barry, Sean; "Smoking Microchips Tells It All : Computer Forensic Experts Mine Hard Drives For Data That Too-Clever Users Thought Long Deleted", http://www.dataforensics.com/articles/smoking_microchip_tells_it_all.pdf, (15.04.2014).

Bednar, P.M., Katos, V., Hennell, C., "Cyber-Crime Investigations: Complex Collaborative Desicion Making", Third International Annual Workshop on Digital Forensics and Incident Analysis, 2008.

Daniel L., "Digital Forensic : The Subdisciplines", Digital Forensic for Legal Professions, 2011.

Değirmenci, Olgun; Ceza Muhakemesinde Sayısal (Dijital) Delil, Ankara, 2014.

Ekizer, Ahmet Hakan; "Adli Bilişim", http://www.ekizer.net/content/view/16/1/ (01.05.2014).

Er, Cüneyd; Biyometrik Yöntemler ve Özel Hayatın Gizliliği Hakkı, Ankara, 2007.

Erem, Faruk; Diyalektik Açıdan Ceza Yargılaması Hukuku, Ankara, 1986.

Eryılmaz, Mesut Bedri; Ceza Muhakemesi Hukuku Dersleri, Ankara, 2012.

Feyzioğlu, Metin; Ceza Muhakemesi Hukukunda Tanıklık, Ankara, 1996.

Feyzioğlu, Metin; Ceza Muhakemesinde Vicdani Kanaat, Ankara, 2002.

Garfinkel, S.L., "Digital forensics research: The next 10 years", Digital Investigation 7, 2010.

Kantar, Baha; Ceza Muhakemeleri Usulü, Birinci Kitap, Ankara, 1957.

Karakuş, Oğuz; Kriminalistik, Ankara, 2009.

Karaman, Mehmet; Adli Bilişim, Ankara, 2013 (Yayımlanmamış Rapor).

Keser Berber, Leyla; Adli Bilişim, Ankara, 2004.

Keser Berber, Leyla; "Adli Bilişim Uzmanı Kimdir?", http://turk.internet.com/ haber/yaziyaz.php3?yaziid=16728. (31.04.2014).

Keser Berber, Leyla / Lostar, Murat; Bilişimde Biyometrik Yöntemler, Ankara, 2006.

Kim, Y., Kim, K.J.,"A Forensic Model on Deleted-File Verification for Securing Digital Evidence", 978—1-4244-5493-8710 IEEE, 2010.

Kretowicz, Joanna; "Network Forensics and Security", https://eforensicsmag.com/wireless-forensic-preorder/, (05.05.2014).

Kunter, Nurullah; Ceza Muhakemesi Hukuku, İstanbul, 1989.

Kunter, Nurullah / Yenisey, Feridun / Nuhoğlu, Ayşe; Muhakeme Dalı Olarak Ceza Muhakemesi Hukuku, İstanbul, 2007.

Küzeci, Elif; Kişisel Verilerin Korunması, Ankara, 2010.

Last, David; "Computer Analysts and Experts – Making the Most of GPS Evidence", http://articles.forensicfocus.com/2012/08/27/computer-analysts-and-experts-making-the-most-of-gps-evidence/ (15.05.2014).

Leone, Giovanni; Diritto e Procedura Penale, Napoli, 1988.

Özbek, Veli Özer / Kanbur, M. Nihat / Doğan, Koray / Bacaksız, Pınar / Tepe, İlker; Ceza Muhakemesi Hukuku, Ankara, 2012.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD, http://www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html. (22.04.2014).

Özdilek, Ali Osman; Bilişim Suçları ve Hukuku, İstanbul, 2006.

Özen, Muharrem / Baştürk, İhsan; Bilişim – İnternet ve Ceza Hukuku, Ankara, 2011

Özocak, Gürkan; "Ceza Muhakemesinde Elektronik Delillerin Tespiti ve Toplanması", 2. Uluslararası Bilişim Hukuku Kurultayı Bildiriler Kitabı, İzmir, Kasım 2011.

Özocak, Gürkan, "Sosyal Medyada İşlenen Suç Tipleri ve Suçluların Tespiti", Yenimedya Çalışmaları II. Ulusal Kongresi – Kongre Kitabı, Kocaeli, 2013.

Peisert, S., Bishop, M., Keith, M., "Computer Forensics in Forensic", Third International Workshop on Systematic Approaches to Digital Forensic Engineering, 2008.

Rogers, M.K., Seigfried, K., "The future of computer forensics: a needs analysis survey", Elsevier Computers & Security, 23/12-16, 2004.

Sağıroğlu, Şeref / Karaman, Mehmet; "Adli Bilişim", Telepati Dergisi, S. 203, Ağustos 2012.

Say, Kubilay; Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi, Ankara, 2006, s. 16 (Yayımlanmamış yüksek lisans tezi).

Spencer, John R.; "The Green Paper on obtaining evidence from one Member State to another and securing its admissibility: the Reaction of one British Lawyer", http://www.zis-online.com/dat/artikel/2010_9_492.pdf, s. 602. (24.04.2014).

Şahin, Cumhur; Ceza Muhakemesinde İspat, Ankara, 2001.

Şen, Ersan / Özdemir, Bilgehan; Tutuklama – Uygulamada Şüpheli ve Sanık Haklarının Korunması, Ankara, 2011.

Şen, Osman Nihat; "Adli Bilişim Bilimi ve Diğer Bilimlerle Olan İlişkisi" http://www.bilgisayarpolisi.com/index.php?sayfa=makaleoku&kategori=11&id=121 (18.05.2014).

Toroslu, Nevzat / Feyzioğlu, Metin; Ceza Muhakemesi Hukuku, Ankara, 2006.

Tosun, Öztekin; Türk Suç Muhakemesi Dersleri, C. I, İstanbul, 1981.

Uçkan, Özgür / Beceni, Yasin; "Bilişim-İletişim Teknolojileri ve Ceza Hukuku", İnternet ve Hukuk, İstanbul, 2004.

Wang, Y., Cannady, J., Rosenbluth, J., "Foundation of computer forensics: A technology fort he fight against computer crime", Computer Law & Security Report, s. 21/119-127, 2005.

Wolfe, H.B., "Computer Forensics", 0167-4048/03 Elsevier Science, 2003.

Yurtcan, Erdener; Ceza Yargılaması Hukuku, İstanbul, 1994.

http://www.spiegel.de/international/germany/0,1518,502955,00.html. (24.04.2014).

http://www.spiegel.de/international/germany/0,1518,590198,00.html. (24.04.2014).

http://www.dw.de/almanyadan-siber-savunma-hamlesi/a-14739247 (23.10.2014).