ADLİ BİLİŞİM SÜRECİNDE KARŞILAŞILAN SORUNLAR VE ÇÖZÜM ÖNERİLERİ*

PROBLEMS ENCOUNTERED IN THE COURSE OF COMPUTER FORENSICS AND SOLUTION PROPOSALS

Yusuf BAŞLAR**

Özet: Adli bilişim, bir soruşturma kapsamında bilişim sistemlerinde bulunan elektronik delile ilk temas edildiği andan yargı makamlarının önüne getirilmesi anına kadar geçen sürecin bütününü ifade etmektedir. Kişilerce işlenen suçların cezalandırılması ve bunun için gerekli adil yargılamanın gerçekleşebilmesi, usulüne uygun elde edilecek delillerle mümkündür. Bu bakımdan, adli bilişim süreci, elektronik delilin önem arz ettiği suçlar bakımından oldukça ehemmiyetlidir. Adli bilişim süreci sonucunda bilişim sistemlerinden veya veri depolama birimlerinden elde edilen elektronik veriler, çözümlenerek anlaşılır vaziyette elektronik delil haline getirilmektedir. Elektronik verilerin kaynağının ne olduğu, ne zamandan beri bilişim cihazlarında bulunduğu, bu verilerde değişiklik yapılıp yapılmadığı, yapılmış ise nasıl ve ne zaman yapıldığı gibi soruşturma için hayati öneme sahip bilgiler adli bilişim sürecinde tespit edilmektedir. Bununla birlikte bu süreçte ortaya çıkan birçok sorun, elektronik delilin kaybolmasına ve/veya kullanılamaz hale gelmesine neden olabilmektedir. Biz de bu çalışmamızda adli bilişim sürecini ve bu süreçte karşılaşılan sorunlar ile çözüm önerilerimizi ortaya koymaya çalıştık.

Anahtar Kelimeler: Adli Bilişim, Elektronik Delil, Elektronik Veri, Bilişim Sistemleri

Abstract: Computer forensics is a term which defines the entire process starting from the first contact with the evidence found in information systems within a scope of an investigation up until the moment of bringing it before the judicial authorities. To punish the crimes committed by individuals and to serve the true justice in this regard is possible only by the way of the duly obtained evidences. Therefore, computer forensics process is rather important particularly in terms of the crimes electronic evidences count. At the end of the computer forensics process, electronic data obtained from information systems or data storage units turned into the collectible

---

* Bu çalışma, "Ceza Yargılamasında Elektronik Delil" isimli doktora tezinden üretilmiştir.

** Dr., Starts Editörlük ve Danışmanlık Hizmetleri, yusufbaslar@hotmail.com, ORCID: 0000-0003-3575-6345, Makalenin Gönderim Tarihi: 13.07.2019, Kabul Tarihi: 13.07.2019

from through data processing. The vital information for investigation such as; what is the source of the electronic data? Since when they are in the information devices? Whether they have been modified or not? If they were modified, when and how? were obtained in the computer forensics process. Besides, various problems emerge in this process could cause the electronic evidence be lost and/or distorted to become useless. So in this study we tried to propound the computer forensics process, the problems emerging in its course and our proposals to solve such problems.

Keywords: Computer Forensics, Electronic Evidence, Electronic Data, Information Systems

Giriş

Kriminalistik uzmanı Prof. Edmond Locard'ın ortaya koyduğu ve günümüzde Locard teoremi olarak da bilinen "Değişim Prensibi"ne göre, bir ortamı terk eden bir kimsenin orada bulunduğuna dair iz bırakmaması ya da üstünde o ortamdan bir şeyler alıp götürmemesi mümkün değildir. Olay yeri incelemesi ile elde edilen en önemli şey maddi delillerdir. Bu tür deliller şüphelinin aleyhine dilsiz birer tanık niteliğindedir. Nitekim canlı tanıkların (şahitlerin) varlığı bile onları yok edemez.[1]

Değişim prensibindeki birbirine temas eden iki nesne arasındaki değiş tokuş fiziksel ortamda söz konusu olduğu kadar dijital ortamlar için de söz konusudur. Bu bakımdan nasıl ki fiziksel ortamda her temas iz bırakmakta ise bilişim sistemleri üzerinde de iz bırakmadan işlem yapmak neredeyse imkânsızdır. Önemli olan bu izleri doğru bir şekilde tespit edip sonuca götürücü verilere ulaşmaktır.[2] Bu işlemlerin sağlıklı ve bilimsel olarak yürütülmesi amacıyla da adli bilişim bilimi ortaya çıkmış ve gelişmiştir.[3] Bu doğrultuda da adli bilişim yöntemlerinin ve ceza muhakemesi ilkelerinin denkleme uygun biçimde yerleştirilmesi zorunluluğu ortaya çıkmıştır.[4]

---

1 Şevket Kümüştaş, "Maddi Delillerin Elde Edilmesi ve Hukuka Uygunluğu", *Çağın Polisi Dergisi*, 2007, S. 66, s. 36.

2 Yusuf Uzunay/Kemal Bıçakçı, "A3D3M: Açık Anahtar Altyapısı Destekli Dijital Delilleri Doğrulama Modeli", Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, İstanbul, 2005, https://docplayer.biz.tr/14459365-A3d3m-acik-anahtar-altyapisi-destekld-ddjdtal-deldllerd-dogrulama-modeld.html Erişim Tarihi: 19.02.2019.

3 Hüseyin Çakır/Ercan Sert, "Bilişim Suçları ve Delillendirme Süreci", Örgütlü Suçlar ve Yeni Trendler, Uluslararası Terörizm ve Sınıraşan Suçlar Sempozyumu (UTSAS 2010), Oğuzhan Ömer Demir/Murat Sever (drl.), Ankara, 2011, s. 146.

4 Onur Özbek, "Hukuk Devletinde Bireysel Güvenlik Ekseninde Bilişim Teknolo-

I. Adli Bilişim Kavramı

Uzun yıllar boyunca adli tıp, adli kimya gibi adli uzmanlık alanları suç soruşturmalarını yürüten makamlara yardımcı olarak birçok adli vakanın bilimsel yöntemlerle çözülmesinde yardımcı olmuştur. Uzmanlar, olay mahallindeki biyolojik ve fiziksel izlerin kendilerine gösterdikleri ipuçları doğrultusunda olay hakkında ayrıntılı bilgi elde etme imkânını bulabilmişlerdir. Bununla birlikte, günümüzde suç ve suçluların elektronik ortamda kendilerini sıkça göstermeleri nedeniyle olayı aydınlatmaya çalışan uzmanlar artık doğadaki iz ve emarelerin değil bilişim sistemlerindeki manyetik olarak kodlanmış vaziyetteki 1 ve 0'ların peşine düşmüşlerdir.[5]

Adli bilişim kavramı tahmin edildiğinin aksine "adli" ve "bilişim" kelimelerinin bir araya getirilmesi sonucunda oluşturulmuş bir kavram değildir. Dilimize, "computer forensics" tanımından çevrilmiş olan ve yeni bir anlam kazandırılan adli bilişim kavramı, geniş bir anlama sahip olan "bilişim" kelimesinin esas alınması sonucunda "computer forensics"in Türkçe karşılığı olan "bilgisayar adli bilimi" kavramının yerine kullanılmaktadır.

Bununla birlikte adli bilişim kavramı yaygın olarak "computer forensics" kavramının karşılığı olarak kullanılmakta ise de bilişim teknolojisindeki baş döndürücü gelişmeler sonrasında gerçekte elektronik delilin yalnızca bilgisayarlarda bulunmadığının anlaşılması üzerine "computer forensics" kavramının yerine ondan daha genel nitelikte olan "digital forensics" kavramı da kullanılmaya başlanmıştır.

Adli bilişim, yeni bir hukuk dalı olarak ortaya çıkan ancak etkinliği günden güne artan bilişim hukuku konularına ilişkin bir yardımcı disiplin olarak doğmuştur. Nitekim adli bilişim yöntemlerine gerek ceza yargılamasında gerekse hukuki ihtilaflarda sıkça başvurulmaktadır. Bu bağlamda adli bilişim, ceza yargılamasında etkin biçimde kullanılmasına karşın özel hukuk alanındaki ihtilafların çözümünde de

jileri", 1. Hukukun Gençleri Sempozyumu (Hukuk Devletinde Kişisel Güvenlik), Ankara, 20-21 Mart 2009, http://www.umut.org.tr/tr-TR/hukukun-genclerisempozyumlari-dizisi--1-hukuk-devletinde-kisisel-guvenlik/111. aspx (25 Şubat 2015).

5 Semih Dokurer, "Adli Bilişim", 2. Polis Bilişim Sempozyumu, Ankara, 14-15 Nisan 2005, s. 226.

yargılamaya delil katkısı sağlayabilecek bir bilim dalı olarak kendini göstermektedir.[6]

Adli bilişim süreci, bir bakıma olay yeri inceleme esaslarına benzemektedir. Bu süreç sonunda görünmez nitelikte olan elektronik delil, görünür ve anlaşılır hale gelmektedir. Süreç içerisinde bir elektronik delilin sonradan değiştirilip değiştirilmediği veya tahribata uğrayıp uğramadığı da saptanabilmektedir.[7]

Adli bilişim, suçun aydınlatılabilmesi için bilimsel yöntemler kullanılarak, çeşitli varyasyonlardaki elektronik medyalar üzerinde bulunan, suçla ilgili elektronik delilin değişmeden ve zarar görmeden anlaşılabilir bir şekilde yargı makamları önüne sunulmaya hazır hale getirilmesini sağlayan ve başlı başına bilimsel teknik prensiplerin uygulandığı bir delil inceleme sürecinin bütünüdür.[8]

Başka bir ifadeyle adli bilişim, elektromanyetik, elektro optik ortamlarda korunan ve/veya bu ortamlarca iletilen ses, görüntü, veri bilgileri veya bunun bileşiminden oluşan her türlü bilişim nesnesinin mahkemelerde elektronik delil niteliği taşıyacak biçimde tanımlanması, elde edilmesi, saklanması, incelenmesi ve mahkemeye sunulması sürecidir.[9]

Adli bilişimi, bir yargılama sırasında kullanılabilecek potansiyel delillerin belirlenmesi için bilişim sistemlerinin kullanılması şeklinde tanımlamak da mümkündür. Nitekim adli bilişim, bilişim sistemleri kullanılarak ne, kim, nerede, ne zaman ve nasıl sorularına cevap bulmaya çalışmaktadır.[10] Bu bağlamda adli bilişim, elektronik delillerin ihtiva ettiği bilgileri, delil inceleme prosedürlerini, hukuki ve etik sorumlulukları göz önünde bulundurup delil bütünlüğünü koruyarak ve gerçeği açığa çıkartmak amacıyla elektronik delili toplama, inceleme, analiz etme ve raporlama sürecinin bütününü ifade etmektedir.[11]

---

6 Özcan Özbey, "Adli Bilişim ve Sayısal Deliller (5271 sayılı CMK'nın 134. Maddesi)", *Yargıtay Dergisi*, 2010, C. 36, S. 3, s. 65.

7 Osman Gazi Ünal, Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma, Yayınlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, 2011, s. 21.

8 A. Hakan Ekizer, Adli Bilişim (Computer Forensics), 2014, http://www.ekizer.net/adli-bilisim-computer-forensics Erişim Tarihi: 12 Şubat 2020.

9 Ahmet Hasan Koltuksuz, "Adli Bilişimde Olay Yeri İnceleme Esasları", Bilişim Hukuku Konferansı-Yargıtay, Ankara, 09-10 Ekim 2008, s. 12.

10 Servet Yetim, "Adli Bilişim ve Canlı Bilişim Sistemlerinde Dijital Delil Araştırma Yöntemleri", *Terazi Hukuk Dergisi*, 2007, C. 2, S. 11, s. 124.

11 Kubilay Say, Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması

II. Adli Bilişimin Önemi

Adli bilişimin, bilişim sistemlerindeki elektronik delile ilk temas edildiği andan yargı makamlarının önüne getirilmesi anına kadar geçen sürecin bütünü olarak ele alınması, onu, adli bilimler içerisinde değerlendirilecek bir disiplin haline getirmektedir. Nitekim adli bilişimin, ceza ve hukuk yargılamalarında bilişim sistemlerinde bulunan delillerin toplanması, incelenmesi, analiz edilmesi ve raporlanması olarak değerlendirilmesi, adli bilimlerin bir alt disiplini olduğunu açık bir şekilde ortaya koymaktadır.

Elektronik delilin korunması, elektronik ve fiziksel koruma şeklinde kendini göstermektedir. Elektronik koruma, delillerin ilk alındığı andan itibaren değişmediğini, bütünlüğünün bozulmadığını ispatlayacak çeşitli mekanizmaları içermektedir. Bu genellikle kriptografik işlemler sayesinde gerçekleştirilmektedir. Fiziksel koruma ise, delillerin incelenecek yere bozulmadan taşınması, mahkemeye sunulacağı ana kadar uygun ortamlarda saklanması ve yine mahkemeye götürülüş sırasında herhangi bir bozukluğa uğramamasını ifade etmektedir.[12]

Bireylerin ve toplumların hayatında köklü ve evrensel değişimlere perde aralayan bilişim teknolojilerinin neden olduğu yeni felsefe ve düşünce sistematiği, yönetim ve iş yapma yöntemlerine yeni boyutlar kazandırmıştır. Bu bağlamda, elektronik delilin hukuka uygun bir delil olarak kabul edilebilmesi, farklı bir mücadeleyi de beraberinde getirmektedir. Bu mücadelenin verilebilmesi için elektronik delil kavramının bilinmesi, elektronik delilin adli prosedüre uygun olarak toplanması ve değerlendirilmesi gerekmektedir. Her türlü çalışmanın idari bir takım tedbir ve iş yapma felsefesi ile desteklenmesi, suçla mücadelede etkinliğinin artırılması açısından zorunludur.[13]

---

ve Laboratuvarda İncelenmesi, Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2006, s. 16; Mehmet Serkan Kılıç, "Elektronik Deliller ve Yapısal Özellikleri", Hüseyin Çakır/Mehmet Serkan Kılıç (ed.), Adli Bilişim ve Elektronik Deliller içinde (137-158), Seçkin Yayıncılık, Ankara, 2014, s. 139.

12 Mesih Gözüşirin, 5237 sayılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları ile Mücadeleye İlişkin Model Önerisi, Yayınlanmamış Yüksek Lisans Tezi, Kara Harp Okulu Savunma Bilimleri Enstitüsü, 2011, s. 94-95.

13 Mustafa İlker Öztürk, Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri, Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2007, s. 3.

Adli bilişimin temel amacı, elektronik veriler ile olay arasındaki bağlantıyı veya fiil ile işlenen veriler ve kullanıcı arasındaki bağlantıyı ortaya koymaktır. Hem ceza yargılamalarında hem de özel hukuk alanındaki ihtilaflarda adli bilişim yöntemlerine başvurulmaktadır.[14]

Adli bilişimin hukuki boyutundan ziyade teknik boyutu daha ön plandadır. Zira elektronik sistemlerdeki bulguların, bunlardan ayrıştırılarak birer hukuki delile dönüştürülme süreci, oldukça zahmetli, son derece teknik bilgi gerektiren ve uzmanlık isteyen bir iş görünümündedir.[15] Bununla birlikte adli bilişim çalışmalarını sadece delil toplama ve sunma süreci olarak ele almayıp bilgisayar depolama ortamları üzerinden yapılan sistematik bir inceleme süreci olarak da değerlendirmek gerekmektedir.[16]

Adli bilişim bilimi müstakil bir bilim olup daha çok adli kolluk birimini ve savcıları ilgilendirmektedir. Adli bilişim işlemlerini yapabilmek için, bilişim sistemlerine ve diğer cihazlara usulüne uygun şekilde elkoymak, adli bilişim kurallarına uygun şekilde yedekleme yapmak, alınan yedekleri incelemek, mahkemeye sunulacak şekilde hazırlamak ve uygun şekilde paketlemek, taşımak ve saklamak gerekmektedir.[17] Bu bakımdan, olay yerinde bulunup incelemeye alınan herhangi bir materyal mahkemede kabul edilmediği sürece delil niteliği taşımayacağından adli bilişim süreci ne kadar çok usule uygun gerçekleşirse elde edilen bulguların da mahkemece delil niteliği taşıma olasılığı o derece artacaktır.[18] Nitekim adli bilişim, kimi zaman kovuşturmaya konu olayın çözümünde tek delil niteliğindeki bir elektronik verinin herhangi bir zarara uğramaksızın mahkeme önüne getirilmesi fonksiyonunu üstlenmektedir.[19]

---

14 Türkay Henkoğlu, Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi, Pusula Yayıncılık, İstanbul, 2011, s. 1.

15 Aydoğan Tan, Adli Bilişim (Computer Forensic), 2009, https://hukuksokagi.com/kaynak/adli-bilisim-computer-forensic/Erişim Tarihi: 19 Şubat 2019.

16 Hüseyin Çakır/Mehmet Serkan Kılıç, "Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bir Bakış", *Polis Bilimleri Dergisi*, 2013, C. 15, S. 3, s. 24.

17 Hakan Aydoğan, Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri, Yayınlanmamış Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü, 2009, s. 9.

18 Dokurer, s. 227.

19 Özbek, http://www.umut.org.tr/tr-TR/hukukun-gencleri-sempozyumlari-dizisi-- 1-hukuk-devletinde-kisisel-guvenlik/111. aspx Erişim Tarihi: 25 Şubat 2015.

Bilişim sistemleri ve diğer elektronik cihazlar üzerindeki adli bilişim işlemleri, gerek bu cihazların kişiler tarafından suç işlemede araç olarak kullanılması gerekse herhangi bir suçun işlenmesinde doğrudan kullanılmayıp kişilerin bu cihazları kendi aralarındaki iletişim için veya işlemlerini kolaylaştırmak ve bilgileri yedeklemek için kullanmaları durumunda gerçekleştirilmektedir.[20]

Hayatın her alanında var olan suç olgusu, teknolojiyi de araç olarak kullanmakta, buna bağlı olarak geleneksel suçların yapısı değişmekte, sonuçta da bilişim ortamlarında işlenmekte olan suç miktarı artmaktadır.[21] Kişilerce işlenen suçların cezalandırılması ve bunun için gerekli adil yargılamanın gerçekleşebilmesi ise usulüne uygun elde edilecek delillerle mümkündür. Bu bakımdan, adli bilişim süreci, elektronik delilin önem arz ettiği suçlar bakımından hayati öneme sahiptir.

Gerçekten de günümüzde bilişim sistemleri ve internetin hayatımızın her alanında yoğun biçimde kullanılması bilişim suçlarının belirgin bir şekilde artmasına neden olmuştur.[22] Bununla birlikte elektronik veri depolama birimlerinin yaygınlaşması nedeniyle elektronik delil, sadece bilgisayar sistemlerinin veri depolama birimlerinde yer almamakta, çok değişik elektronik veri depolama cihazlarında da bulunabilmektedir. Bu durum, elektronik delilin bilişim suçlarının yanı sıra klasik suçlar[23] açısından da önemli bir konuma sahip olmasına neden olmaktadır.[24] Bu bakımdan gerek bilişim suçlarının gerekse veri

---

20 Aydoğan, s. 9.

21 M. Zekeriya Gündüz, Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti, Yayınlanmamış Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, 2012, s. 23.

22 TCK'nın bilişim alanında suçlar bölümünde; hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma (m. 243), bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi (m. 244/1-2), bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama (m. 244/4) ve banka veya kredi kartlarının kötüye kullanılması (m. 245) suçları düzenlenmiştir. Ceza mevzuatımızda bilişim suçlarına ilişkin daha birçok düzenleme bulunmaktadır.

23 TCK'nın malvarlığına karşı suçlar bölümünde; bilişim sisteminin kullanılması yoluyla işlenen hırsızlık (m. 142/2-e) ve bilişim sistemlerinin kullanılması yoluyla dolandırıcılık (m. 158/1-f) suçları düzenlenmiştir. Görüldüğü üzere günlük yaşamda çokça karşılaşılan ve klasik suçlardan olan hırsızlık ve dolandırıcılık suçlarının bilişim sistemleri kullanılarak işlenmesi bu suçları nitelikli hale sokmaktadır. Diğer taraftan kasten öldürme (m. 81), özel hayatın gizliliğini ihlal (m. 134), müstehcenlik (m. 226), silahlı örgüt (m. 314) vb. pek çok klasik suçun ispatına yönelik elektronik delilin de veri depolama aygıtlarında bulunması mümkündür.

24 Ekizer, http://www.ekizer.net/adli-bilisim-computer-forensics Erişim Tarihi: 12 Şubat 2020.

depolama aygıtlarının delil saklama aracı olarak kullanıldığı klasik suçların soruşturmasında hayati öneme sahip olan bir elektronik delilin usule aykırı biçimde elde edilmesi önemli bir ispat aracının yok olmasına yol açabilecektir.

Adli bilimler içerisinde yer almakta olan adli bilişim bilimi sayesinde suç ve suçlu ile mücadele edilmekte, işlenen suçların delillendirilmesi sağlanmakta ve suçla ilgisi olmayan masum kişiler korunabilmektedir.[25] Bugün hemen herkes tarafından birçok işin yapılmasında bilgisayarlar veya diğer elektronik cihazların kullanıldığı düşünüldüğünde, sadece bilişim suçlarının araştırılması ve soruşturulmasında değil diğer birçok suç türünün araştırılması ve soruşturulmasında adli bilişim tekniklerinden yararlanıldığı görülmektedir.[26]

Bununla birlikte, günümüzün teknik gelişmelerine bağlı olarak hızla gelişimini devam ettiren adli bilişim bilimi, yargı organlarına yardımcı olmanın yanı sıra bugün bazı şirketler ve kişiler tarafından da veri kurtarma, imha etme veya sair amaçlarla ihtiyaç duyulan bir alan haline gelmiştir. Nitekim günümüzde birçok büyük şirket, bünyelerinde bir adli bilişim uzmanı görevlendirme veya bu konuda hizmet veren firmalarla sürekli çalışma yolunu seçmektedir.[27]

Adli bilişim sürecinin belirleyici iki unsurundan birisi adli bilişim uzmanı iken; diğeri ise söz konusu incelemenin yapılacağı laboratuvar ortamı ve kullanılacak donanımlar ve yazılım programlarıdır.[28] Bu bakımdan, bu sürecin genellikle olay yerinde kolluk birimleri ve sonrasında da bilirkişiler tarafından (çoğu zaman laboratuvar ortamında) yerine getirildiği görülmektedir.[29]

Suçlular adli bilişim biliminin ve adli bilişim uzmanlarının soruşturma becerilerinin farkında olmalarından dolayı işlemiş oldukları suç sırasında bilişim sistemlerini ve ağları daha karmaşık şekilde kullanmaktadırlar. Bazıları ise adli bilişim yöntemlerinin başarılı olamamasını sağlamak amacıyla eylemlerini gizlemek ve elektronik delilleri yok

---

25 Çakır ve Kılıç, s. 24.

26 Servet Yetim, "Dijital Kanıt Araştırma Yöntemleri", *İstanbul Barosu Dergisi*, 2008, C. 82, S. 3, s. 1209; Tan, https://hukuksokagi.com/kaynak/adli-bilisim-computer-forensic/ Erişim Tarihi: 19 Şubat 2019.

27 Gündüz, s. 23.

28 Leyla Keser Berber, Adli Bilişim, Yetkin Yayınları, Ankara, 2004, s. 7.

29 Henkoğlu, s. 22.

etmek için verileri geri dönülemez şekilde silme, verileri gizleme, verileri bozma, dosya imzalarını bozma ve hash çakışması[30] oluşturma gibi bazı delil karartma (anti forensics) yöntemleri geliştirmekte ve buna yönelik araçlar icat etmek suretiyle çoğu zaman adli bilişim uzmanlarının işlerini zorlaştırmaktadırlar. Bu durum adli bilişim uzmanlarının adli bilişim sürecinde son derece dikkatli olmalarını gerekli kılmaktadır.

III. Karşılaşılan Sorunlar ve Çözüm Önerileri

Adli bilişim süreci sonucunda bilişim sistemlerinden veya veri depolama birimlerinden elde edilen elektronik veriler, çözümlenerek anlaşılır vaziyette elektronik delil haline getirilmektedir. Bu süreçte farklı nedenlerle ortaya çıkması muhtemel sorunlar elde edilen elektronik delilin geçerliliği üzerinde kuşku uyandıracağı için en kısa sürede köklü çözüme kavuşturulmalıdır. Adli bilişim sürecinde ortaya çıkabilecek sorunlar ve buna ilişkin çözüm önerilerimiz aşağıda açıklanmıştır.

A. Adli Bilişim Sürecine İlişkin Potansiyel Riskler

Adli bilişim süreci, potansiyel riskleri de beraberinde taşıyan bir süreçtir. Bu süreç, adli bilişim uzmanlarını, çalışma sürecinde bazı kritik materyallerin kaybolması veya önem arz eden bir işin devri gibi bazı sorumlulukların altında bırakmaktadır. Ayrıca, ortaya çıkan birçok içsel sorun, elektronik delilin adli bilişim sürecinde kaybolmasına neden olabilmektedir.[31]

Fiziksel niteliğe sahip olmayan elektronik delilin hızlı bir şekilde kaybolması ise mevcut yapı içerisinde ağır işleyen soruşturma işlemlerinin etkin şekilde yürütülmesini engellemektedir. Bu nedenle soruşturma sürecinde mümkün olduğunca hızlı hareket edilmeli ve sadece bu nitelikte soruşturmalarda faaliyet yürütecek birimler kurulmalıdır.

---

30 Bir hash algoritmasının farklı mesajlar için aynı hash değeri üretmesine denir. Bkz. Kevser Kırkıl, Kaotik İkeda Haritası ile Güçlü Kriptografik Özetleme Fonksiyonu Elde Edilmesi, Yayınlanmamış Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, 2012, s. 1.

31 Güven Şeker, "Bilişim Suçlarının Delillendirilmesinde Amerikan Uygulaması ve Ülkemizdeki Durum", *Uluslararası İnsan Bilimleri Dergisi*, 2004, C. 1, S. 1, s. 7; Osman Nihat Şen, "Polisin Adli Bilişimde Kullanabileceği Programların Bir Değerlendirmesi", 2. Polis Bilişim Sempozyumu, Ankara, 14-15 Nisan 2005, s. 7.

Ayrıca, kamu görevlilerinin yasak soruşturma yöntemlerini kullanmaktan kaçınmaları büyük önem arz etmektedir.[32]

Bu bakımdan delillerin karartılmaması hususunun önemi tüm kademe personeli tarafından kesinlikle anlaşılmalıdır. Tüm adli süreçte yer alan personel, elektronik delilin kolaylıkla değiştirilebilir olduğunu bilmeli ve delillerin toplanması, incelenmesi ve analizi süreci boyunca alınan prensip ve prosedürlere uymalıdır. Zira delillerin karartılmasına neden olabilecek yanlış uygulamalar mahkemeler tarafından delillerin reddedilmesine yol açacaktır.[33]

Bununla birlikte bu sürece ilişkin potansiyel risklerden birisi de adli bilişim sürecine hiç başlanamaması ve bu nedenle de atılı suça ilişkin delillerin toplanamamasıdır. Gerçekten de günümüzde sosyal paylaşım ağları pek çok suçun kaynağı haline gelmiş olmasına rağmen sosyal paylaşım ağlarını yöneten şirket merkezlerinin ve bu ağlara ait sunucuların (server) yurt dışında bulunması nedeniyle bu platformda gerçekleşen suçlarda elde edilecek deliller ilgili şirketlerden gelecek verilerle sınırlıdır. Bu şirketler de soruşturma makamlarınca istenen verileri çoğu zaman "özel hayatın gizliliği", "kişisel verilerin korunması" vb. ilkeleri gerekçe göstererek göndermemektedir.

Yargıtay 15. Ceza Dairesi konuya ilişkin vermiş olduğu 18.06.2019 tarihli ve 2019/4623 E., 2019/6805 K. sayılı kararında;[34] "*Sosyal medya platformlarında ismi ve fotoğrafları kullanılarak müşteki adına sahte hesaplar açılıp 3. kişilerin bu hesaplar kanalıyla dolandırıldığının iddia edildiği anlaşılmış ise de; sosyal paylaşım ağlarını yöneten şirket merkezinin Amerika Birleşik Devletlerinde bulunması nedeniyle adı geçen ülke adli makamları ile yazışma yapılması gerektiği, ancak benzer soruşturmalar için yapılan yazışmalarda ABD'deki yasal düzenlemelerin şüphelinin tespitine yönelik işlemlerin yapılmasına uygun olmadığı, bu hususta taleplerin olumsuz karşılandığı bilgisine yer verildiği, e-iletilerin gönderilmesinde kullanılan ve yurt dışında*

---

32 Özgür Uçkan/Yasin Beceni, Bilişim-İletişim Teknolojileri ve Ceza Hukuku, İnternet ve Hukuk, Yeşim Atamer (drl.), Bilgi Üniversitesi Yayınları, İstanbul, 2004, s. 423.

33 Kubilay Say, "Bilişim Suçlarında Olay Yeri İncelemesinin Hukuki Boyutu", Levent Bayram (ed.), Ses Görüntü ve Data İncelemeleri içinde (251-260), Adalet Yayınevi, Ankara, 2008, s. 259.

34 https://kararara ma.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ Erişim Tarihi: 12 Şubat 2020.

bulunan serverlerden söz konusu ülkelerdeki *'Kişisel Verilerin Korunması Yasaları' nedeniyle gönderen kişilerin kimliklerinin belirlenmesine yarayacak bilgiler almanın mümkün bulunmadığı, soruşturmanın devamı halinde yeni delillere ulaşmanın teknik ve hukuki açıdan mümkün bulunmadığı, yeni delil elde edilmesi durumda soruşturmanın yeniden ele alınmasının her zaman olanaklı bulunduğu nazara alındığında itirazın reddi yönündeki kararda bir isabetsizlik görülmediğinden, İstanbul Anadolu 6. Sulh Ceza Hâkimliği'nin 07/02/2019 tarihli ve 2019/994 değişik iş sayılı kararına yönelik yapılan kanun yararına bozma isteminin reddine,"* hükmetmiştir.

B. Ağ Trafiği Analizinde Delilin Doğruluğunun ve Gerçekliğinin Sağlanması

Ağ trafiği analizi, adli bilişim sürecinde olayların aydınlatılmasında ve kanıtların elde edilmesinde büyük öneme sahiptir. Bu anlamda ağ trafiği analizinin önemi, olaya ilişkin delil değeri olan veriyi elde etmek amacıyla ağ olaylarının yakalanması, kaydedilmesi ve analizi olarak kendini göstermektedir.[35] Bununla birlikte ağ trafiğinin elde edilmesi sırasında hash değeri üretilmesi mümkün iken bunun karşılaştırılacağı sabit bir veri durumunun söz konusu olmaması ağ trafiği analizinde elde edilen elektronik delilin doğruluğunun ve gerçekliğinin nasıl sağlanacağı konusunda soru işaretlerine neden olmaktadır. Bu noktada ağ trafiğinin zaman damgasının alınmış olması delilin doğrulanması ve gerçekliğinin sağlanması bakımından hayati önem arz etmektedir.

Zaman damgası, bir elektronik verinin üretildiği, değiştirildiği, gönderildiği, alındığı, kaydedildiği zamanın tespit edilmesini sağlayan elektronik bir veriyi ifade eder.[36] Zaman damgasının bu niteliği sayesinde elde edilen elektronik delilin üretim, erişim veya değiştirilme zamanları üzerinde oynama yapılması veya değiştirilmesi engellenmiş ve delillerin doğruluğu ve gerçekliği ispatlanmış olmaktadır.[37]

---

35 Nur Sena Atalay/Şengül Doğan/Erhan Akbal/Türker Tuncer, "Adli Bilişim Alanında Ağ Analizi", *BEÜ Fen Bilimleri Dergisi,* 2019, C. 8, S. 2, s. 594.

36 TÜRKTRUST, Zaman Damgası Nedir ?, https://www.turktrust.com.tr/tr/urunler/zaman-damgasi/ Erişim Tarihi: 3 Mart 2020.

37 Aydoğan, s. 37.

Nitekim 30.11.2007 tarihli ve 26719 sayılı Resmi Gazete'de yayımlanan İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik'in yer sağlayıcının yükümlülüklerini düzenleyen 7/1-c maddesinde yer sağlayıcının trafik bilgisini altı ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşan verilerin dosya bütünlük (hash) değerlerini zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle yükümlü oldukları hükme bağlamıştır. Aynı Yönetmelik'in erişim sağlayıcının yükümlülüklerini düzenleyen 8/1-b maddesinde ise bu yükümlülük 1 yıl süre ile erişim sağlayıcılara da yüklenmiştir.

C. Mobil Cihazlara İlişkin Adli Bilişim İşlemlerinde Yaşanan Sorunlar

Mobil cihazlarda uygulanan adli bilişim işlemi bazı zorlukları içermektedir. Bu bağlamda mobil cihazlarda şifreleme ve cihaz anahtarının olması dijital veriye normal yöntemlerle ulaşılamama sorununu gündeme getirmektedir. Mobil cihazlarda bulunan dijital verinin normal yöntemlerle elde edilememesi fiziksel müdahaleyi de gerekli kılan JTAG, Chip-off, rooting ve jailbreak gibi ileri düzey ek tekniklerin uygulanmasını gerektirmektedir[38]

Mobil cihaz üzerinde fiziksel müdahaleyi gerektiren temelde iki veri çıkarma yöntemi olup bunlar JTAG ve chip-off teknikleridir. Bu teknikler genellikle uygulanması zor ve soruşturma boyunca gerçek cihazlarda denemek için büyük hassasiyet ve deneyim gerektirir. JTAG, cihaz üzerindeki belirli bağlantı noktalarına bağlanıp verileri aktararak gerçekleştirilen gelişmiş veri toplama yöntemidir. Ancak bir yanlışlık durumunda cihaz hasar görebileceğinden JTAG'yi denemeden önce uygun eğitim ve tecrübeye sahip olunmalıdır. Chip-off da verileri ayıklamak için flaş çiplerin cihazdan çıkartılabildiği fiziksel veri çıkarma türüdür. Bu yöntem NAND flaş çiplerinin cihazdan çıkartıldığı ve veri elde etmek için incelendiği bir yöntemdir. Bu nedenle, bu yöntem, cihaz şifre korumalı olduğunda ve USB hata ayıklama etkin olmadığında bile çalışır. İşlem sonrasında cihazın normal çalış-

[38] Hamza Aytaç Doğanay, Mobil Adli Bilişiminin Önemi Bağlamında Hukuki Süreç ve Delil Zinciri Kavramı ile Yeni Nesil Mobil Cihazların İncelenmesinde Karşılaşılan Güncel Zorlukların Değerlendirilmesi, Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sağlık Bilimler Enstitüsü, 2019, s. 63.

tığı JTAG tekniğinin aksine, chip-off tekniği genellikle cihazın tahrip edilmesine neden olur. [39]

Mobil cihazlar üzerinde şifrelenmiş verilere ulaşılması ya da silinmiş verilerin geri getirilmesi hususunda daha başarılı sonuçlar elde edilebilmesi nedeniyle fiziksel imaj alma işlemi de uygulanmaktadır. Mobil cihazlarda uygulanan fiziksel imaj alma işlemi rooting ve jailbreak yöntemleri ile gerçekleştirilmektedir. Bununla birlikte hem Android hem de iOS cihazlar üzerinde yapılan rooting ve jailbreak işlemlerinin ardından yapılan analiz sonucunda bulunan verilerin özellikleri ve sayıları açısından ciddi farklılıklar oluşabildiği görülmektedir.[40]

Mobil cihazlarda bulunan verilere normal bağlantı yolları veya yöntemlerle ulaşılamadığı durumlarda başvurulan JTAG, Chip-off, rooting ve jailbreak gibi daha fazla uzmanlık gerektiren ileri düzey teknik yöntemler belli ölçüde veri kaybı ya da verinin gerçekliğine şüphe düşürme riskini taşıyan yöntemlerdir. Bu bakımdan bu yöntemlerin uygulanması için belirtilen riskin suç verisine ulaşmak için göze alınabilecek bir risk olması ve diğer bütün yolların denenmiş olması gerekir. Riskin göze alınabilme durumu ise elde edilmesi istenen dijital veriye hali hazırda zaten erişilemiyor olmasıdır. Bu bakımdan zaruret olmadıkça bu yöntemlere başvurulmaması önerilmektedir.[41]

D. Adli Bilişimin İlke ve Standartlarının Belirlenmemesi

Adli bilişim ilke ve standartlarının belirlenememiş olması da adli bilişim sürecini zora sokan sebepler arasındadır. Uluslararası alanda kabul edilen adli bilişim ilkelerine ülkemizde de önem veriliyor olmasına karşın elektronik delilin elde ediliş sürecine ilişkin işlemlerin ne şekilde yapılacağı, uyulması gereken standartlar ve sorumluluklar ile bilirkişi görevlendirmesine ilişkin yeterli ve net yasal düzenlemelerin bulunmaması uygulamada birçok elektronik delilin henüz elde ediliş sürecinde geri dönülemeyecek şekilde kaybolmasına ve/veya kullanılamaz hale gelmesine zemin hazırlamaktadır.[42]

---

39 Fatma Güneş Eriş, Mobil Cihazlarda Sosyal Medya Uygulamalarının Adli Bilişim Açısından Analizi, Yayınlanmamış Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimler Enstitüsü, 2018, s. 20.

40 Mesut Ukşal, Mobil Cihazlarda Adli Bilişim, Yayınlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, 2015, s. 73, 119.

41 Doğanay, s. 87.

42 İlker Çiçek, Ülkemizde Adli Bilişim Laboratuarı Kurulumu ve Bilişim Suçlarıyla

Bu bağlamda ülkemizde, diğer pek çok ülke uygulamasına benzer şekilde, bilirkişi olarak atanan kişilerin bilimsel ehliyetlerini ön şart olarak ortaya koyacak ve takip edecek bir mevzuatın bulunmadığı görülmektedir.[43] Bununla birlikte "Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı"nın 35. maddesinde "adli bilişim uzmanı" düzenlenmişti. Buna göre; bu tasarı kapsamına giren suçlarla ilgili olarak sadece adli bilişim uzmanı yetki belgesine sahip olanlar bilirkişilik yapabilecek, adli bilişim uzmanlığı ve adli bilişim yetki belgesine ilişkin esas ve usuller yönetmelikte belirlenecek ve adli bilişim uzmanları hakkında Ceza Muhakemesi Kanunu'nun bilirkişiliğe ilişkin hükümleri uygulanacaktı. Ancak bu zamana kadar söz konusu tasarı kanunlaştırılamamış ve uygulama CMK'nın bilirkişiliğe ilişkin ilgili maddeleri uyarınca gelişmiştir.

Belirtmek gerekir ki adli bilişim bilim dalı uluslararası standartlarla şekillenmiştir. Nitekim ISO tarafından 2012 yılında yayımlanan ve 2018 yılında gözden geçirilen ISO/IEC 27037:2012 bu alandaki en temel belgedir. Bu standart, delil niteliği olabilecek dijital verilerin tanımlama, toplama ve muhafazası için yol göstermektedir. Bu alanda bir standardizasyona gidilmesiyle uluslararası benzer uygulamaların gelişeceği, farklı ülkelerde farklı kişi veya kurumlarda bu tür soruşturmalar yürütüldüğü durumlarda kıyas yapmanın, karşılaştırmanın ve birleştirmenin kolaylaşacağı değerlendirilmektedir.[44]

Bununla birlikte yukarıda da değinildiği üzere ülkemizde elektronik delil elde etme sürecinin ISO/IEC 27037 standardına uygun gerçekleştirilmemesi elektronik delilin henüz elde ediliş sürecinde zarar görmesine yol açabilmektedir. Bu itibarla gerek elektronik delil elde etme sürecinde çalışacak bilirkişilerin görevlendirilmesi gerekse adli bilişim ilke ve standartlarına ilişkin yukarıda değinilen diğer konular bakımdan uluslararası alanda kabul edilen adli bilişim standartlarına önem verilmesi ve bunların yasal bir zemine oturtulması gerekmektedir.

Mücadeleye Katkıları, Yayınlanmamış Yüksek Lisans Tezi, Haliç Üniversitesi Fen Bilimleri Enstitüsü, 2008, s. 14.

43 Olgun Değirmenci, Ceza Muhakemesinde Sayısal (Dijital) Delil, Seçkin Yayıncılık, Ankara, 2014, s. 121.

44 Mehmet Bedii Kaya, "Hukuki Açıdan Bilişim Suçları, Siber Güvenlik ve Adli Bilişim", Şeref Sağıroğlu/Mustafa Şenol (ed.), Siber Güvenlik ve Savunma Problemler ve Çözümler içinde (213-279), BGD Siber Güvenlik ve Savunma Kitap Serisi 2, Grafiker Yayınları, Ankara, 2019, s. 258-259.

E. Laboratuvarların Yeterli Seviyeye Gelmemiş Olması

Uluslararası alanda kabul edilen adli bilişim ilkelerine önem verilmesi ve bunların yasal bir zemine oturtulmasının yanı sıra bu ilkelere uygun teknolojik alt yapının kurulmasına da ağırlık verilmelidir. Ayrıca, teknolojik alt yapı kurulsa dahi teknoloji üretilmedikçe delil elde etmede kullanılan programlar, cihazlar ve teçhizatlar zamanla eskiyecek ve yenilerini edinebilmek için ithal edilmek zorunda kalınacaktır. Bu bakımdan adli bilişim süreci ne kadar pahalıya mâl olursa olsun laboratuvarların kurulması ve bilirkişilik bakımından personel eğitimi için gerekli sermayenin sağlanması hayati önem arz etmektedir.[45]

Öğretide "Adli Tıp Kurumu Kanunu"nda köklü değişikliğe gidilerek Kanun'un adının "Adli Bilirkişilik Kurumu Kanunu" olarak değiştirilmesi önerilmiştir. Diğer taraftan önceleri sadece tıp alanında bilirkişilik ihtiyacını karşılamak için kurulan ve daha sonra morg, fizik, kimya, gözlem, trafik, biyoloji vb. ihtisas daireleri eklenerek sadece tıbbi alanda bilirkişilik yapma fonksiyonundan hızla uzaklaşan kuruma, adli bilişimi bütün boyutlarıyla içine alacak "Adli Bilişim İhtisas Kurulu"nun kurulması gerekliliği savunulmuştur. Ayrıca kurulacak bu birimde çalışacak olan adli bilişim uzmanlarının belli bir sertifikasyon programına tabi tutularak adli bilişim alanında gerekli eğitimlerin verilmesi, bunun yanı sıra yazılım, donanım, veri tabanı yönetimi, veri kurtarma ve network yönetimi gibi işlerden anlayan uzman kişiler bulunması gerekliliği de vurgulanmıştır.[46]

Gerçekten de eğitimli teknik personelin uygun bir bünyede teşkilatlandırılması, bu konuda Adli Tıp Kurumu ve hatta mümkün olduğu takdirde üniversiteler bünyesinde "Adli Bilişim İhtisas Kurulu" tarzında bilirkişilik kurumlarının kurulması büyük önem arz etmektedir.[47] Zira bilirkişilik alanında adli bilişim uzmanları ile diğer bilgisayar uzmanları arasında yaklaşım farklılıkları ortaya çıkmaktadır. Adli bilişim uzmanları kendi alanlarıyla ilgili hukuki bilgiye sahip olup dünyaca kabul gören bir takım adli bilişim standartlarına vâkıftırlar.

---

45 Ünal, s. 153.

46 Yetim, Dijital Kanıt Araştırma Yöntemleri, s. 1202.

47 Gökhan Ahi, Bilişim Suçlarında Usul ve Sorumluluk, Mete Tevetoğlu (drl.), Bilişim Hukuku (ss. 100-107), Kadir Has Üniversitesi Yayınları, İstanbul, 2006, s. 102; Ali Karagülmez, "Bilişim Suçlarında Delil Toplamayı Etkileyen Başlıca Konular", 2. Polis Bilişim Sempozyumu, Ankara, 14-15 Nisan 2005, s. 33.

Bu standartlara vâkıf olma bir takım sertifikalarla kanıtlanmaktadır. Bilirkişi seçiminde bu sertifikaların dikkate alınması adli bilişim sürecinin başarılı bir şekilde işletilmesinde yardımcı olacaktır.[48]

Bu bağlamda 15.08.2016 tarihli ve 674 sayılı OHAL KHK'sı ile 14.04.1982 tarihli ve 2659 sayılı Adlî Tıp Kurumu Kanunu'nun 8/1 maddesine eklenen hüküm uyarınca Adli Bilişim İhtisas Dairesinin kurulması önemli bir adım olmuştur. Nitekim aynı Kanuna eklenen 22/A maddesi ile de Adlî Bilişim İhtisas Dairesinin görevleri "Mahkemeler ile hâkimlikler ve savcılıklar tarafından talep edilen bilişim ile ilgili konularda gerekli incelemeleri yapmak; veri toplama, işleme, depolama veya aktarma işlevi gören bilişim sistemleri ile her türlü sayısal ve elektronik materyal üzerinde inceleme, araştırma ve analizleri yapmak, sonuçlarını bir raporla tespit etmek" şeklinde belirlenmiştir.

Olağan yasa yapma tekniği ile yasal düzenleme sonucu yerine getirilmesi gereken mezkûr işlemin bir OHAL KHK'sı ile hükme bağlanması eleştiriye açık bir husus olmakla birlikte düzenlemenin içeriği itibariyle yerinde olduğu düşüncesindeyiz. Bununla birlikte 02.07.2018 tarihli ve 703 sayılı OHAL KHK'sı ile Adlî Tıp Kurumu Kanunu'nun pek çok maddesi ile birlikte 8/1 ve 22/A maddeleri de mülga olmuştur. Sonraki süreçte ise Adlî Bilişim İhtisas Dairesi'nin kuruluş ve görevlerine ilişkin hükümler aynı şekilde 15.07.2018 tarihli ve 30479 sayılı "Bakanlıklara Bağlı, İlgili, İlişkili Kurum ve Kuruluşlar ile Diğer Kurum ve Kuruluşların Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi"nin 9/1 ve 24/1 maddelerinde düzenlenmiştir.

Belirtmek gerekir ki; elektronik delil elde etme süreci için son derece önemli olan Adlî Bilişim İhtisas Dairesinin kuruluş ve görevlerine ilişkin düzenlemenin yasal prosedür çerçevesinde yeniden ele alınması, yapılacak yasal düzenlemenin öğretide belirtilen görüşler de dikkate alınarak ve hatta üniversiteleri de kapsayacak biçimde geniş bir perspektifle değerlendirilmesi daha yerinde olacaktır.

Günümüzde soruşturma organları ile kolluk güçlerinin karşılaştığı en büyük sorunlardan birisi bilişim sistemlerinin veri saklama kapasitelerinin büyüklüğüdür. Delil olarak kullanılacak elektronik veri, sistemde yer alan verinin yüzde, binde veya on binde biri seviyesindedir.

---

48 Ünal, s. 141.

Bu bakımdan, bilişim sistemlerinde yer alan her türlü bilginin değil ancak yargılamaya konu olayı aydınlatacak, fail veya failleri belirleyecek, bir olayı doğrulayacak veya yanlışlığını ispat edecek verinin, özetle delil değeri olan verinin elde edilmeye çalışılması gerekmektedir ki bu durum çok da kolay bir husus değildir.[49]

Bu bakımdan adli bilişim uzmanlarının yer imkânları, olay yerinde bağımsız fiziksel kopyalama cihazları gibi teknik cihaz sayıları ve en önemlisi yetişmiş personel sayısı artırılmalı, uzmanlaşmış yöneticiler eşliğinde çalışmalarını yapmaları sağlanmalıdır. Ayrıca sadece adli bilişim alanına hizmet edebilecek tam donanımlı ve yer sıkıntısı olmayan inceleme laboratuvarları kurulmalıdır.[50] Bu bağlamda adli bilişim uzmanlarının adli olayların çözümünde istifade edecekleri son derece ileri düzey laboratuvarların kurulması gerekmektedir. Elektronik delilin niteliği itibariyle alınan imaj ve yedeklerin uzun süre boyunca saklanması gerekeceğinden bu ihtiyacı giderici mahiyette yedekleme üniteleri bulunmalıdır.[51]

F. Uygulayıcıların Yeterince Eğitilmemesi

Suçluların elektronik delillerle ilgili kaygıları bulunmakta ve bu kaygılarından kurtulmak için bilişim sistemlerini tahrif etmeye gayret göstermektedirler. Bu nedenle adli bilişim sürecinde görev alan uygulayıcıların adli bilişim süreciyle ilgili o zamana kadar yapılan çalışmalara her soruşturma bakımından kolayca güvenmemeleri, yeni oluşacak koşullara ilişkin çalışmaları ve bunların sonuçlarını da yakından takip etmeleri gerekmektedir.

Elektronik delil, diğer delil türleri ile benzer veya ortak özelliklere sahip olmanın yanı sıra bir takım farklı özelliklere de sahiptir. Elektronik delilin sahip olduğu farklı özelliklerin, adli bilişim sürecinde görev alan teknik personeller tarafından bilinmesi ve bu doğrultuda araştırmaların yürütülmesi hayati öneme sahiptir.[52] Bu bakımdan adli bilişim uzmanlarının bilişim sistemlerinde çok ileri düzeyde bilgiye

---

49 Değirmenci, s. 62

50 Çakır / Sert, s. 161.

51 Yetim, Dijital Kanıt Araştırma Yöntemleri, s. 1202-1203.

52 Say, Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi, s. 99.

sahip olmaları, bu özelliklerini daima sürdürebilecek şekilde güncel teknolojiyi takip etmeleri ve ayrıca temel seviyede kendi alanları için gerekli hukuk bilgisini haiz bulunmaları gerekmektedir.[53]

Adli bilişim sürecinde tek bir bilişim sisteminden dahi pek çok anlamlı veri çıkartılabilmekte ve adli bilişim uzmanının bu verilerden somut olayla doğrudan ilgili ve faydalı olanlarını tespit etmesi beklenmektedir. Adli bilişim uzmanının dava konusu olaya yeterince hâkim olamaması ise bu eleme işleminin sağlıklı yapılamaması ve yargılama sürecinin olumsuz etkilenmesi sonucunu doğurmaktadır.[54]

Gerçekten de adli bilişim konusunda özel ve uzman personelin olmayışı neticesinde halen elektronik delil elde etme imkânı olmayan birçok malzemenin toplandığı, veri cihazlarına yedekleme yapılmadan ve elektronik olarak mühürlenmeden el konulduğu, şüpheliye ve avukatına herhangi bir tutanak verilmediği, bilişim sistemlerinin ve diğer veri depolama aygıtlarının manyetik alan etkisinden soyutlanmadan özensizce taşındığı, tamirhaneleri andıran odalarda veri yazmayı önleyen cihazlar (FRED) olmaksızın elektronik delil incelemesi yapıldığı görülmektedir. Bu tür yanlış uygulamalara yapılan itirazlar ise kimi zaman kaynak, personel ve teknik altyapı yetersizliği gerekçeleriyle geri çevrilmektedir.[55]

Özel eğitimli teknik personelin bilişim alanındaki baş döndürücü gelişmelere bağlı olarak adli bilişim süreci ile ilgili sürekli olarak eğitimlerinin yenilenmesi büyük önem taşımaktadır. Özellikle, türü ve kapsamı genişleyen bilişim suçlarına ve faillerine ulaşmada, bilinen metotların kısa sürede güncelliğini yitirmesi, teknik personelin eğitimlerinin sürekli olarak yenilenmesini gerekli kılmaktadır.[56] Bu bağlamda adli bilişim ve siber güvenlik uzmanlarının yetiştirilmesi açısından ülkemizde de özellikle lisans programları ve sertifika programlarını her geçen yıl artmakta ve bu durum olumlu bir gelişme olarak karşımıza çıkmaktadır. Eğitimin daha yaygın, köklü ve uygulamalı olarak verilmesinin alan bilgi birikimi ve uzmanı açısından ülke gereksinimlerini doğrudan karşılayacağı değerlendirilmektedir.[57]

---

53 Şeref Sağıroğlu/Mehmet Karaman, "Adli Bilişim", *Teletapi Haberleşme ve Bilişim Teknolojileri Dergisi*, 2012, S. 203, s. 67.

54 Hüseyin Akarslan, Bilişim Suçları, Seçkin Yayıncılık, Ankara, 2012, s. 132.

55 Ahi, Adli Bilişim Nedir ?, http://www.bilisimhukuk.com/2009/07/adli-bilisim-nedir/ Erişim Tarihi: 19 Şubat 2019; Özbey, s. 107.

56 Karagülmez, s. 33.

57 Merve Orakcı/İbrahim Kök/Hüseyin Çakır, "Adli Bilişim Eğitiminin Gereksini-

Diğer taraftan bilgisayar ve ağ sistemlerinin incelenmesi hususunda hâkim ve savcıların geniş yetkilere sahip olmalarına karşın teknik anlamda yeterli donanıma sahip olmamaları ve onları bu konuda yönlendirecek standartların bulunmaması nedeniyle kimi zaman ehliyetsiz kişilerin bilirkişi olarak atandıkları görülmektedir.[58] Hatta bilgisayar mühendisi olmasına rağmen ne tür bir inceleme yaptığının farkında olmayan, kendisine sorulan sorular haricinde raporunu ilgisiz konularla ve gereksiz teknik terimlerle dolduran uzman bilirkişilerin de var olduğu görülmektedir.[59]

Bu bakımdan adli bilişim alanındaki baş döndürücü gelişmeleri takip edebilmek için özellikle üniversitelerde bilişim ve bilgisayar derslerinin yanı sıra hukukçuların da bir araya gelerek ortak çalışmalar düzenlemeleri gerekmektedir. Özellikle adli bilişimle ilgili konferans, panel ve seminerler düzenlenerek hukukçuların ve bilişim uzmanlarının katılımı sağlanmalıdır. Bu tür etkinliklerin düzenlenmesiyle adli bilişim süreci daha iyi kavranacak ve bilişim şuuru geliştirilerek bilişim suçlarıyla mücadelede etkinlik sağlanacaktır.[60]

Nitekim adli bilişim alanında en ileri ülkelerden biri olan ABD, ceza yargılamasında bilişim sistemlerine yönelik arama ve elkoyma tedbirlerini uygularken adli bilişim sürecini belirli kıstaslara uyarak icra etmektedir. Bununla birlikte ABD'deki adli bilişim birimleri bu kriterleri her zaman gözden geçirerek gelişen teknoloji ve yeni suç tiplerine göre güncellemekte ve bu kriterlerin belirlendiği sempozyum ve konferanslara ev sahipliği yapmaktadır. Bu bağlamda adli bilişim sürecinde, elektronik delilin güvenilirliği ve kabul edilebilirliği konularında yaygın ve etkin olabilecek standartları belirleme yönündeki çalışmalar bu ülkede devam etmektedir.[61]

Soruşturma görevlileri için özellikle adli bilişim faaliyetlerini kapsayan soruşturmalarda, yol gösterici olması amacıyla hazırlanan eği-

---

mi ve Genel Olarak Değerlendirilmesi", *Bilişim Teknolojileri Dergisi*, 2016, C. 9, S. 2, s. 144.

58 Cevat Özel/M. Gökhan Ahi, Bilişim Suçlarında Usul ve Sorumluluk Sistemi Üzerine Öneriler, http://www.turkhukuksitesi.com/makale_179.htm Erişim Tarihi: 19 Şubat 2019.

59 Ahi, Adli Bilişim Nedir?, http://www.bilisimhukuk.com/2009/07/adli-bilisim-nedir/ Erişim Tarihi: 19 Şubat 2019; Özbey, s. 107.

60 Ünal, s. 153-154.

61 Ünal, s. 72.

tici kaynaklar temin edilmelidir. Gerçekten de, savcılar ve kolluk görevlilerinin soruşturma faaliyetinde hangi hususlara dikkat etmeleri, ne şekilde bir soruşturma yürütmeleri gerektiğini açıklayan ve pratik eğitimlerle de desteklenen kaynaklar hazırlanması son derece faydalı olacaktır.[62]

Bu bağlamda Avrupa Birliği ve Avrupa Konseyi ortak projesi olan "Türk Ceza Adalet Sisteminin Etkinliğinin Geliştirilmesi Projesi" kapsamında Türkiye Adalet Akademisinin eğitim müfredatına destek verilmesi ve geliştirilmesi amacıyla yerli ve yabancı uygulayıcı ve akademisyenlerin de katıldığı uzman toplantıları sonucunda oluşturulan kitabın[63] uygulayıcıların bilişim suçlarıyla mücadelede gerekli soruşturma teknikleri ve elektronik delil elde etme yöntemlerini öğrenmeleri ve kendilerini bu konularda geliştirmeleri hususunda yararlı bir kaynak olduğu kanaatindeyiz.

G. Adli Bilişim Sürecinde Yaşanan Hukuka Aykırılık Halleri

Türk hukukunda elektronik delilin ceza yargılamasında hükme esas alınması her şeyden önce hukuki ve teknolojik geçerliliği konusunda tereddüt bulunmadığının ispatına bağlıdır. Elektronik delilin teknolojik geçerliliği düzgün bir adli bilişim süreci sonrasında adli makamlara sunulmuş olmasına bağlı iken hukuki geçerliliği ise başta CMK'nın 134. maddesine uygun bir tedbir kararı uyarınca hukuka uygun şekilde elde edilip ceza muhakemesi hukukunda bir delil için öngörülen özellikleri taşımasına bağlıdır. Bu bakımdan elektronik delilin elde edilmesi sürecinde teknolojik geçerliliği ifade eden adli bilişim kurallarına uygun hareket edilmiş olsa bile bu delilin hukuka aykırı bir şekilde elde edilmesi ceza yargılamasında geçerliliğini mutlak biçimde etkileyecektir.

Adli bilişim sürecinin başlangıcında CMK'nın 134. maddesinde düzenlenen bir arama, kopyalama ve elkoyma tedbirinin alınmaması ya da bu yönde bir karar alınmış olsa bile delil elde etme işlemlerinin

---

62 Uçkan/Beceni, s. 424-425.

63 Nigel Jones/Esther George/Kasım Karagöz/Murat Volkan Dülger/Gözde Modoğlu (hzl.), Bilişim Suçları Eğitim Modülü (Türk Ceza Adalet Sisteminin Etkinliğinin Geliştirilmesi Avrupa Birliği & Avrupa Konseyi Ortak Projesi), MATBAM Ajans & Reklam & Tanıtım, Ankara, 2014.

bu tedbir kararına uygun gerçekleşmemesi elde edilecek delilin hukuka aykırılığı sorununu gündeme getirecektir. Daha önceleri sadece hâkim kararı ile uygulanabilen tedbir CMK'nın 134. maddesinin 1. fıkrasında 25.07.2018 tarihli ve 7145 sayılı Kanunla yapılan değişiklikle birlikte "gecikmesinde sakınca bulunan hâllerde" Cumhuriyet savcısı kararıyla da uygulanabilecektir.[64] Bu durumda Cumhuriyet savcısı tarafından verilen karar yirmi dört saat içinde hâkim onayına sunulmak zorundadır. Kolluğun savcılık makamına daha kolay ulaşması bakımından bu değişiklik tedbir kararı alınmaksızın gerçekleşen usulsüz uygulamalara yönelik yakınmaları azaltacak niteliktedir.

Bununla birlikte tedbirin ön şartı olan "somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması" kuralının somut olayda ne ölçüde gerçekleştiği ya da savcı tarafından verilecek kararda "gecikmesinde sakınca bulunan hâl"in olup olmadığı yönündeki sorunlar halen devam etmekte olup uygulamada da buna yönelik üst yargı denetimleri etkin şekilde gerçekleşmemektedir.

CMK'nın 134. maddesinin 2. fıkrasında 7145 sayılı Kanun'la yapılan değişiklikle "bilgilere ulaşılamaması" ibaresinden sonra gelmek üzere "işlemin uzun sürecek olması" durumu da bilişim sistemlerine elkoyma nedeni olarak eklenmiştir. Bu değişiklik öncesinde CMK'nın 134. maddesi uyarınca gerçekleşen tedbirlerde "şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması" şartının var olup olmadığına bakılmaksızın bilişim cihazlarına elkonuluyor ve gerekli işlemler ilgili laboratuvarlarda gerçekleştiriliyordu.[65] Bu bakımdan yasaya eklenen söz konusu hüküm bu yöndeki usule aykırılıklara engel olacak mahiyettedir. Bununla birlikte CMK'nın 134/3-4 hükümleri uyarınca elkoyma işlemi sırasında sistemdeki bütün verilerin yedeklemesinin yapılması ve bu yedekten bir kopyanın şüpheli ya da vekiline verilmesi kuralları halen geçerliliği korumaktadır. Uygula-

---

64 CMK'nın 134. maddesinde düzenlenen tedbirin gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı kararıyla da uygulanabileceği ilk olarak "bazı suçlar bakımından ve olağanüstü halin devamı süresince" 27.07.2016 tarihli ve 668 sayılı OHAL KHK'sının 3/1-j maddesinde düzenlenmiştir.

65 Yusuf Başlar, "Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri", *Uyuşmazlık Mahkemesi Dergisi,* 2014, S. 3, s. 91-92.

mada elkoyma işlemi sırasında yerine getirilmesi gereken bu kurallara halen riayet edilmemekte ve bu da itirazlara neden olmaktadır.

Tedbirin uygulanması sırasında CMK m. 134 hükmünün doğru yorumlanmamasından kaynaklı ihlallerin de gündeme geldiği görülmektedir. Özellikle bilgisayarın tüm niteliklerine sahip olması nedeniyle bilgisayar tanımı[66] içerisinde kabul edilmesi gereken ancak uygulamada kimi zaman bilgisayar olarak tanımlanmayan cep telefonu, cep bilgisayarı ve elektronik veri barındıran birçok cihazın CMK m. 134 hükmü yerine CMK m. 116 ve 123 hükümlerine göre arama ve elkoyma işlemlerine tabi tutulması temel hak ve özgürlükler bakımından ihlallere ve elde edilen delillerin hukuka aykırı olmasına neden olabilmektedir.[67]

Bu bakımdan yasa hükmünün uygulama alanının bilişim sistemleri ve bağlı donanımlarını kapsayacak ve de gelişen teknolojinin gerisinde kalmayacak genel bir çerçevede belirlenmesi hatta bir adım daha ileri gidilerek elektronik delil, bilişim suçları, adli bilişim, bilişim sistemlerinde uygulanacak koruma tedbirleri gibi bilişim hukukuna ilişkin hususların ayrı bir kanunda ve tereddütlere mahal bırakmayacak biçimde yeniden düzenlenmesi, bu düzenlemeler yapılıncaya kadar ise madde metnindeki kavramların bilişim sistemlerinin genelini kapsayacak biçimde yorumlanarak uygulamanın buna göre tesis ettirilmesi gerekmektedir.

---

66 Türk Dil Kurumu, bilgisayarı; "Çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin" şeklinde tanımlanmaktadır. Bkz. Türk Dil Kurumu, https://sozluk.gov.tr/ Erişim Tarihi: 20 Şubat 2020.

67 CMK m. 134 uyarınca tedbir kararı alınmaksızın cep telefonu üzerinde yapılan aramanın hukuka aykırı olduğu hususunda bkz. Yargıtay 17. Ceza Dairesi'nin 15.02.2017 tarihli ve 2015/27517 E., 2017/1716 K. sayılı kararı; "Cumhuriyet Savcısının talimatıyla yapıldığı belirtilen, telefon inceleme tutanağının 20.04.2014 saat 14.10'da düzenlendiği, bu saatten daha önceki bir saatte saat 12.57'de düzenlenen 'fotoğraf teşhis tutanağına' göre şüphe üzerine durdurulan sanığın cep telefonunun Cumhuriyet Savcısının emri ya da mahkeme kararı olmadan kolluk görevlileri tarafından incelendiği ve telefonda, müştekiye ait çalıntı motosikletin fotoğrafının telefonda K ismiyle kayıtlı bir kişiye gönderildiğinin tespiti üzerine sanık hakkında mahkumiyet kararı verilmiş ise de; işlevi itibarıyla bilgisayar niteliğinde olan cep telefonu üzerinde inceleme yapılabilmesi için CMK'nın 134. maddesi uyarınca hakim kararı alınması gerektiği bu kararın alınmaması nedeniyle arama ve incelemenin yasaya aykırı olduğu ve bu delilin mahkumiyete esas alınmayacağı…" https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ Erişim Tarihi: 20 Şubat 2020.

Belirtmek gerekir ki CMK'nın 134. maddesinde düzenlenen tedbirinin uygulanmasına ilişkin yukarıda belirtilen yasa ihlallerinin tamamı elektronik delilin hukuki geçerliliğine ilişkin itirazları beraberinde getirmekte ve zaten yapısı gereği suistimale açık olan elektronik delilin[68] ceza yargılamasında kullanılabilir bir delil olup olmadığı konusundaki kuşkuları da artırmaktadır. Kanaatimizce bireylerin bilişim sistemlerinde muhafaza altına almış oldukları kişisel verilerinin CMK'nın 134. maddesine aykırı biçimde elde edilmesi durumunda bu elektronik verilerin yasak delil kapsamında değerlendirilmesi ve ceza yargılamasında kullanılamaması gerekir. Bu durum hâkim ya da savcı kararı olmaksızın yapılacak işlemler için geçerli olduğu kadar -bilişim sistemlerinde yapılacak aramanın temel hak ve özgürlüklere önemli ölçüde müdahale ettiği düşünüldüğünde- ilgili makamdan alınmış kararların uygulaması sırasında ortaya çıkacak usulsüz işlemler açısından da geçerlidir.

Yargıtay Ceza Genel Kurulu öğretideki görüşlere de atıflarda bulunduğu 22.10.2019 tarihli ve 2017/961 E., 2019/622 K. sayılı kararında[69] CMK'nın 134. maddesinde düzenlenen tedbirle ilgili uyulması gereken hususlara vurgu yapmıştır. Yargıtay Ceza Genel Kurulu mezkûr kararında; CMK'nın 134. maddesinde düzenlenen tedbirin elektronik delilin suistimale açık yapısı nedeniyle "son çare" olarak başvurulabilecek "özel koşullara bağlı" bir koruma tedbiri olduğundan, bu tedbire başvurabilmek için (1) bir suç şüphesinin mevcudiyetinin bulunması, (2) bir suç şüphesi nedeniyle adli bir soruşturmanın başlatılmış olması, (3) başka surette delil elde etme imkânının bulunmaması ön koşullarının gerçekleşmesi gerektiğinden, elkoyma işlemi sırasında sistemdeki bütün verilerin yedeklenmesi (imaj alma işlemi), yedeklenen kayıtların bir kopyasının şüpheliye veya vekiline verilmesi, bu hususun tutanağa geçirilerek imza altına alınması gerekliliğinden ayrıntısıyla bahsetmiş ve sonuç olarak;

"… yapılan denetim sırasında sanık tarafından rıza ile teslim edilen ve iş yerinde görünür vaziyette bulunan 85 adet film ve oyun CD/DVD'sinin mu-

---

68 Yargıtay 16. Ceza Dairesi'nin 21.04.2016 tarihli ve 2015/4672 E., 2016/2330 K. sayılı kararı https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ Erişim Tarihi: 11 Şubat 2020.

69 https://karararama.yargitay.gov.tr/YargitayBilgiBankasiIstemciWeb/ Erişim Tarihi: 11 Şubat 2020.

hafaza altına alınması sebebiyle bu materyallerin hukuka uygun yöntemlerle elde edilen delillerden olduğu ancak sanığın iş yerinde bulunan bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılması, bilgisayar kayıtlarından kopya çıkarılması, bu kayıtların çözülerek metin hâline getirilmesi için sanık tarafından gösterilen rızanın yeterli olmayacağı ve mutlaka 'Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma' başlıklı CMK'nın 134. maddesine göre hâkim kararı alınması gerektiği, hâkim kararı olmaksızın bilgisayar ve hard disklerde yapılan arama sonucunda elde edilen delillerin hukuka aykırı yöntemlerle elde edilen delil niteliğinde olduğunun anlaşılması karşısında…… bilgisayar ve hard disklerden elde edilen delillerin hukuka aykırı yöntemlerle elde edilmesi sebebiyle hükme esas alınamayacağı,…… Bu itibarla, Yerel Mahkemece verilen direnme kararına konu hükmün bozulmasına karar verilmelidir" hükmüne yer vermiştir.

Yargıtay Ceza Genel Kurulu'nun 22.10.2019 tarihli ve 2017/961 E., 2019/622 K. sayılı kararında ortaya koymuş olduğu ölçütler çerçevesinde usulüne uygun hakim kararı ya da gecikmesinde sakınca bulunan hallerde savcı kararı olmaksızın bilgisayarlarda, bilgisayar programlarında ve kütüklerinde yapılan arama, kopyalama ve elkoyma işlemi -şüphelinin rızası olsa bile- hukuka aykırı olduğu gibi bu işlemlerin ilgili merci kararı ile yapılması halinde dahi yasada belirtilen ön koşullar gerçekleşmeksizin tedbir kararının verilmesi ya da tedbirin uygulanması sırasında yasada ayrıntısıyla belirtilen usul işlemlerinin yerine getirilmemesi durumunda da elde edilen delil hukuka aykırı yöntemlerle elde edilmiş sayılacak ve hükme esas alınmayacak, böylece adli bilişim sürecinde gerçekleştirilen diğer işlemleri de geçersiz kılacaktır.

Bununla birlikte her ne kadar söz konusu kararda; şüpheli tarafından rıza ile teslim edilen 85 adet film ve oyun CD/DVD'sinin muhafaza altına alınması sebebiyle bu materyallerin hukuka uygun yöntemlerle elde edildiği kabul edilmiş ise de kararın bu kısmına katılmamaktayız. Adli ve Önleme Aramaları Yönetmeliği'nin 17/3 hükmü uyarınca[70] CD/DVD, harici bellek, usb memory, SD Card vb. çıkarılabilir veri de-

[70] Adlî ve Önleme Aramaları Yönetmeliği'nin 17/3 maddesinde; "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" hükmüne yer verilmiştir.

polama cihazları üzerindeki arama, kopyalama ve elkoyma işlemlerinin de CMK'nın 134. maddesine göre yapılması gerekmektedir. Bu nedenle rıza sonucunda muhafaza altına alınmış olsa da usulüne uygun tedbir kararı olmadan bu cihazlardan elde edilecek elektronik delilin hukuka uygun olmayacağı kanaatindeyiz.

Şifreli verilerde, şifre çözme anahtarlarının cihaz sahibinden ya da üçüncü kişilerden istenip istenemeyeceği hususu üzerinde de durmak gerekir. Anayasamızda, *nemo tenetur* ilkesi yalnızca beyanla sınırlı olarak düzenlenmiş olmayıp kişinin delil göstermeye zorlanması da yasaklanmıştır. Kişinin bilişim sistemlerinde yer alan verileri korumak amacıyla kullanmış olduğu şifre anahtarını rızaen vermemesi üzerine bunu teslime zorlanması ve bu sayede elde edilecek dijital verilerin kişi aleyhinde delil olarak kullanılması, kişinin kendi aleyhinde delil göstermeye zorlanması olarak kabul edilecektir.[71] Bu durumda da söz konusu delilin hukuka aykırılığı sorunu gündeme gelecektir.

Şifreli verilerde şifre çözme anahtarının üçüncü kişilerden istenip istenemeyeceği hususuna gelince; hukuka uygun bir arama, kopyalama ve elkoyma tedbiri sonucunda bilişim cihazlarından elde edilmiş şifreli verilere şifre kırma işlemleri ile ulaşılmasının hukuka uygunluğunda sorun olmaması karşısında elektronik verilere zarar gelmemesi amacıyla bu yöntemleri uygulamadan önce ya da bu yöntemlerin uygulanmasına rağmen verilere ulaşılamadığı durumlarda şifre çözme anahtarlarını bilen üçüncü kişilerden bu anahtarların rıza dâhilinde istenmesinde bir hukuksuzluk olmadığı kanaatindeyiz. Ancak şifre çözme anahtarlarını rızaen vermeyen üçüncü kişilerin bunları vermeye zorlanamayacağı da açıktır.

Son olarak bilişim cihazlarında uzaktan erişim yoluyla yapılan aramanın hukuka uygun olup olmadığı sorununa da değinmek yerinde olacaktır. Teknolojideki akıl almaz ilerleme sonucunda internet bağlantısı olan bir bilişim sistemine, kullanıcının bilgisi haricinde erişim sağlanarak elektronik verire ulaşmak mümkün hale gelmiştir. Bu durum bilişim sistemlerine uzaktan erişim yoluyla arama işleminin yapılıp yapılmayacağı hususunu gündeme getirmiştir. Avrupa Konseyi Siber Suç Sözleşmesi'nin 32. maddesinde bilgisayarda depolanmış

71 Değirmenci, s. 266.

verilere, söz konusu bilgisayar sistemi üzerinden erişim yetkisini haiz olan bir kişinin yasal izninin bulunduğu veya bu verilerin herkesin ulaşabileceği şekilde açık olduğu durumlarda sınır ötesinden erişim sağlanabileceği belirtilmektedir. Ancak bu tür bir aramanın CMK'nın 134. maddesine uygun bir arama işlemi olup olmadığı tartışma konusudur.

Türk hukuk sisteminde uzaktan erişim yoluyla arama yapılabileceğini savunan bir görüşe göre; CMK'nın 134. maddesinde belirtilen "arama" ibaresinin "elektronik veri takibi" olarak anlaşılması gerekmekte olup elektronik veri takibi ise bilişim sisteminin kolluğun hâkimiyetine alınması suretiyle açık olarak yapılabileceği gibi bilişim sistemine uzaktan erişim sağlanarak yazılım üzerinden ve gizli olarak da gerçekleşebilir.[72]

Bizim de katıldığımız diğer bir görüşe göre ise CMK'nın 134. maddesi uyarınca bilişim sistemine bir yazılım yüklemek ya da gizli biçimde sisteme erişmek suretiyle ilgilinin haberi olmaksızın bilişim sistemleri üzerinde uzaktan erişimle arama yapılması hukuken mümkün değildir.[73] Bu bakımdan uzaktan erişim sağlanarak bilişim sisteminde arama yapma, CMK'nın 134. maddesinde öngörülen bir arama biçimi olamaz. Kaldı ki böyle bir arama da temel hak ve özgürlüklere ağır müdahale anlamını taşımaktadır. Bu bakımdan, bu nitelikte bir arama için yeni bir yasal düzenleme yapılması zorunluluğu bulunmaktadır.[74]

Sonuç

Adli bilişim, bir soruşturma kapsamında bilişim sistemlerinde bulunan elektronik delile ilk temas edildiği andan bu delilin toplanma, incelenme, analiz edilme ve raporlanma işlemleri tamamlanarak yargı makamlarının önüne sunulduğu ana kadar devam eden sürecin bütününü ifade etmektedir. Bu bakımdan adli bilişim, bir suçun ispatında elektronik delilin kullanılması zorunluluğunun bulunduğu hallerde büyük bir fonksiyona sahiptir.

---

72 Vahit Bıçak, Suç Muhakemesi Hukuku, 2. Basım, Seçkin Yayıncılık, Ankara, 2013, s. 671-673.

73 Değirmenci, , s. 364-365.

74 Ünal, s. 111.

Günümüz ceza yargılamalarında artık baskın bir delil türü haline gelen elektronik delil, hassas, kolayca değiştirilebilir ve silinebilir yapıda olup toplanması ve korunması aşamasında dahi bozulabilir olma özelliğine sahiptir.[75] Bu durum elektronik delilin kullanılmasında en önemli unsurlarından biri olan delil bütünlüğü ilkesinin sağlanması bakımından ayrı bir hususiyet arz etmekte ve adli bilişimin önemini bir kat daha artırmaktadır.

Bununla birlikte uygulamada adli bilişim sürecinde gerek donanım ve yetişmiş personel eksikliğine gerekse yeterli yasal alt yapının olmamasına bağlı olarak birçok sorunla karşılaşıldığı ve bu sorunların çözülememesi nedeniyle ceza soruşturma ve kovuşturması süreçlerinde toplanan pek çok delilin kaybolması ya da kullanılamaz duruma gelmesi sonucuna sebep olunduğu görülmektedir. Bu bakımdan soruşturmanın başladığı andan itibaren savcı ve kolluk personeli ile başlayan ve yargılama safhasında da devam eden delil toplama sürecinde harcanan emek, mesai ve maddi kaynakların israf olmaması için adli bilişime gerekli önemin verilmesi ve bu süreçte karşılaşılan sorunların en kısa sürede çözüme kavuşturulması gerekmektedir.

Kaynakça

Ahi Gökhan, Bilişim Suçlarında Usul ve Sorumluluk, Mete Tevetoğlu (drl.), Bilişim Hukuku içinde (ss. 100-107), Kadir Has Üniversitesi Yayınları, İstanbul, 2006.

Ahi M. Gökhan, Adli Bilişim Nedir?, 2009, http://www.bilisimhukuk.com/2009/07/adli-bilisim-nedir/ Erişim Tarihi: 19 Şubat 2019.

Akarslan Hüseyin, Bilişim Suçları, Seçkin Yayıncılık, Ankara, 2012.

Atalay Nur Sena/Şengül Doğan/Erhan Akbal/Türker Tuncer, "Adli Bilişim Alanında Ağ Analizi", *BEÜ Fen Bilimleri Dergisi*, 2019, C. 8, S. 2, ss. 582-594.

Aydoğan Hakan, Adli Bilişim'de Yeni Elektronik Delil Elde Etme Yöntemleri, Yayınlanmamış Yüksek Lisans Tezi, Polis Akademisi Güvenlik Bilimleri Enstitüsü, 2009.

Başlar Yusuf, "Ceza Yargılamasında Elektronik Delillerin Elde Edilmesine ve Korunmasına İlişkin Usul Hükümleri", *Uyuşmazlık Mahkemesi Dergisi*, 2014, S. 3, ss. 82-105.

Başlar Yusuf, "Elektronik Delil ve Ceza Yargılamasında Kabul Edilebilirliğine İlişkin Bir İnceleme", *Legal Hukuk Dergisi*, 2018, C. 16, S. 184, ss. 1655-1687.

[75] Yusuf Başlar, "Elektronik Delil ve Ceza Yargılamasında Kabul Edilebilirliğine İlişkin Bir İnceleme", *Legal Hukuk Dergisi,* 2018, C. 16, S. 184, s. 1656-1657.

Bıçak Vahit, Suç Muhakemesi Hukuku, 2. Basım, Seçkin Yayıncılık, Ankara, 2013.

Çakır Hüseyin/Ercan Sert, "Bilişim Suçları ve Delillendirme Süreci", Örgütlü Suçlar ve Yeni Trendler, Uluslararası Terörizm ve Sınıraşan Suçlar Sempozyumu (UTSAS 2010), Oğuzhan Ömer Demir/Murat Sever (drl.), Ankara, 2011.

Çakır Hüseyin/Kılıç Mehmet Serkan, "Bilişim Suçlarına İlişkin Delil Elde Etme Yöntemlerine Genel Bir Bakış", *Polis Bilimleri Dergisi*, 2013, C. 15, S. 3, ss. 23-44.

Çiçek İlker, Ülkemizde Adli Bilişim Laboratuarı Kurulumu ve Bilişim Suçlarıyla Mücadeleye Katkıları, Yayınlanmamış Yüksek Lisans Tezi, Haliç Üniversitesi Fen Bilimleri Enstitüsü, 2008.

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

Doğanay Hamza Aytaç, Mobil Adli Bilişiminin Önemi Bağlamında Hukuki Süreç ve Delil Zinciri Kavramı ile Yeni Nesil Mobil Cihazların İncelenmesinde Karşılaşılan Güncel Zorlukların Değerlendirilmesi, Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sağlık Bilimler Enstitüsü, 2019.

Dokurer Semih, "Adli Bilişim", 2. Polis Bilişim Sempozyumu, Ankara, 14-15 Nisan 2005, ss. 226-229.

Ekizer A. Hakan, Adli Bilişim (Computer Forensics), 2014, http://www.ekizer.net/adli-bilisim-computer-forensics Erişim Tarihi: 12 Şubat 2020.

Gözüşirin Mesih, 5237 asyılı Türk Ceza Kanununda Bilişim Suçları ve Bilişim Suçları ile Mücadeleye İlişkin Model Önerisi, Yayınlanmamış Yüksek Lisans Tezi, Kara Harp Okulu Savunma Bilimleri Enstitüsü, 2011.

Gündüz M. Zekeriya, Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti, Yayınlanmamış Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, 2012.

Güneş Eriş Fatma, Mobil Cihazlarda Sosyal Medya Uygulamalarının Adli Bilişim Açısından Analizi, Yayınlanmamış Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimler Enstitüsü, 2018.

Henkoğlu Türkay, Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi, Pusula Yayıncılık, İstanbul, 2011.

Jones Nigel/George Esther/Karagöz Kasım/Dülger Murat Volkan/Modoğlu Gözde (hzl.), Bilişim Suçları Eğitim Modülü (Türk Ceza Adalet Sisteminin Etkinliğinin Geliştirilmesi Avrupa Birliği & Avrupa Konseyi Ortak Projesi), MATBAM Ajans & Reklam & Tanıtım, Ankara, 2014.

Karagülmez Ali, "Bilişim Suçlarında Delil Toplamayı Etkileyen Başlıca Konular", 2. Polis Bilişim Sempozyumu, Ankara, 14-15 Nisan 2005, ss. 30-34.

Kaya Mehmet Bedii, "Hukuki Açıdan Bilişim Suçları, Siber Güvenlik ve Adli Bilişim", Şeref Sağıroğlu/Mustafa Şenol (ed.), Siber Güvenlik ve Savunma Problemler ve Çözümler içinde (213-279), BGD Siber Güvenlik ve Savunma Kitap Serisi 2, Grafiker Yayınları, Ankara, 2019.

Keser Berber Leyla, Adli Bilişim, Yetkin Yayınları, Ankara, 2004.

Kılıç Mehmet Serkan, "Elektronik Deliller ve Yapısal Özellikleri", Hüseyin Çakır/Mehmet Serkan Kılıç (ed.), Adli Bilişim ve Elektronik Deliller içinde (137-158), Seçkin Yayıncılık, Ankara, 2014.

Kırkıl Kevser, Kaotik İkeda Haritası ile Güçlü Kriptografik Özetleme Fonksiyonu Elde Edilmesi, Yayınlanmamış Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, 2008.

Koltuksuz Ahmet Hasan, "Adli Bilişimde Olay Yeri İnceleme Esasları", Bilişim Hukuku Konferansı-Yargıtay, Ankara, 09-10 Ekim 2008, ss. 9-18,

Kümüştaş Şevket, "Maddi Delillerin Elde Edilmesi ve Hukuka Uygunluğu", *Çağın Polisi Dergisi*, 2007, S. 66, ss. 36-41.

Orakcı Merve/Kök İbrahim/Çakır Hüseyin, "Adli Bilişim Eğitiminin Gereksinimi ve Genel Olarak Değerlendirilmesi", *Bilişim Teknolojileri Dergisi*, 2016, C. 9, S. 2, ss. 137-145.

Özbek Onur, "Hukuk Devletinde Bireysel Güvenlik Ekseninde Bilişim Teknolojileri", 1. Hukukun Gençleri Sempozyumu (Hukuk Devletinde Kişisel Güvenlik), Ankara, 20-21 Mart 2009, http://www.umut.org.tr/tr-TR/hukukun-gencleri-sempozyumlari-dizisi--1-hukuk-devletinde-kisisel-guvenlik/111. aspx Erişim Tarihi: 25 Şubat 2015.

Özbey Özcan, "Adli Bilişim ve Sayısal Deliller (5271 sayılı CMK'nın 134. maddesi)", *Yargıtay Dergisi*, 2010, C. 36, S. 3, ss. 61-126.

Özel Cevat/Ahi M. Gökhan, "Bilişim Suçlarında Usul ve Sorumluluk Sistemi Üzerine Öneriler", http://www.turkhukuksitesi.com/makale_179.htm Erişim Tarihi: 19 Şubat 2019.

Öztürk Mustafa İlker, Bilişim Cihazlarındaki Sayısal Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri, Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2007.

Sağıroğlu, Şeref/Mehmet Karaman, "Adli Bilişim", *Teletapi Haberleşme ve Bilişim Teknolojileri Dergisi*, 2012, S. 203, ss. 62-67.

Say Kubilay, Bilişim Suçlarında Elde Edilen Delillerin Olay Yerinden Toplanması ve Laboratuvarda İncelenmesi, Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, 2006.

Say Kubilay, "Bilişim Suçlarında Olay Yeri İncelemesinin Hukuki Boyutu", Levent Bayram (ed.), Ses Görüntü ve Data İncelemeleri içinde (251-260), Adalet Yayınevi, Ankara, 2008.

Şeker Güven, "Bilişim Suçlarının Delillendirilmesinde Amerikan Uygulaması ve Ülkemizdeki Durum", *Uluslararası İnsan Bilimleri Dergisi*, 2014, C. 1, S. 1, ss. 1-13.

Şen Osman Nihat, "Polisin Adli Bilişimde Kullanabileceği Programların Bir Değerlendirmesi", 2. Polis Bilişim Sempozyumu, Ankara, 14-15 Nisan 2005, ss. 35-41.

Tan Aydoğan, Adli Bilişim (computer forensic), 2009, https://hukuksokagi.com/kaynak/adli-bilisim-computer-forensic/ Erişim Tarihi: 19 Şubat 2019.

Türk Dil Kurumu, https://sozluk.gov.tr/ Erişim Tarihi: 20 Şubat 2020.

TÜRKTRUST, Zaman Damgası Nedir?, https://www.turktrust.com.tr/tr/urunler/zaman-damgasi/Erişim Tarihi: 3 Mart 2020.

Uçkan Özgür/Beceni Yasin, Bilişim-İletişim Teknolojileri ve Ceza Hukuku, İnternet ve Hukuk, Yeşim Atamer (drl.), Bilgi Üniversitesi Yayınları, İstanbul, 2004.

Ukşal Mesut, Mobil Cihazlarda Adli Bilişim, Yayınlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, 2015.

Uzunay Yusuf/Bıçakçı Kemal, "A3D3M: Açık Anahtar Altyapısı Destekli Dijital Delilleri Doğrulama Modeli", Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, İstanbul, 2005, https://docplayer.biz.tr/14459365-A3d3m-acik-anahtar-altyapisi-destekld-ddjdtal-deldllerd-dogrulama-modeld.html Erişim Tarihi: 19.02.2019.

Ünal Osman Gazi, Bilgisayarlarda Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama ve Elkoyma, Yayınlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, 2011.

Yetim Servet, "Adli Bilişim ve Canlı Bilişim Sistemlerinde Dijital Delil Araştırma Yöntemleri", *Terazi Hukuk Dergisi*, 2007, C. 2, S. 11, ss. 123-129.

Yetim Servet, "Dijital Kanıt Araştırma Yöntemleri", *İstanbul Barosu Dergisi*, 2008, C. 82, S. 3, ss. 1201-1222.