International Journal of Human Sciences
ISSN:1303-5134

Volume: 12 Issue: 2 Year: 2015

Collection and protection of digital evidences in audit processes

Denetim süreçlerinde dijital delillerin elde edilmesi ve korunması

İlker Koç[1]
Hüseyin Çakır[2]

Abstract

Wide usage of information technologies in banking, finance, health and other commercial sectors requires performing of audit of these sectors through information systems. Collecting and protecting electronic evidence is critically important for both judicial process and results of audit activities. Gathering electronic evidences from an information system is a subject for computer forensics and requires special expertise and equipment. Conversely, in Turkey, most of the institutions responsible for supervision of financial and other relevant sectors have not enough knowledge and experience about forensic audit. Due to the absence of technical knowledge and tools, there would be deficiencies in collecting electronic evidence in accurate manner. In order to prevent these deficiencies, some alternative solutions are offered in this study. These solutions are adapting the computer forensic techniques to audit processes, providing appropriate training to auditors, establishing a legal environment, sharing of information system audit resource and outsourcing of forensic audit activities.

Keywords: Audit, Digital Evidence, Computer Forensic, Information System, Electronic Evidence, Judicial Process

Özet

Bankacılık, finans, sağlık ve diğer ticari sektörlerde bilgi teknolojilerinin kullanımının artması, denetim faaliyetlerinin de bilgi sistemleri üzerinden gerçekleştirilmesi gereksinimini doğurmaktadır. Elektronik ortamlardan dijital delil elde edilmesi ve korunması hem denetim faaliyetinin sonuçları hem de adli süreç açısından önem taşımaktadır. Dijital delillerin elde edilmesi ve korunması adli bilişim faaliyeti kapsamına girmektedir. Adli bilişim faaliyeti uzmanlık ve özel donanımların kullanımını gerektirmektedir. Ancak, Türkiye'de dış denetimle görevli kurumların faaliyetlerinde, adli bilişim yöntemlerine ilişkin yeterli teknik bilgi ve donanım bulunmamaktadır. Bu durum nedeniyle kamu denetim faaliyetlerinde dijital ortamlardan delil elde edilmesi ve korunmasında çeşitli eksiklikler söz konusudur. Bahse konu eksiklikler, denetim sonuçlarının adli sürece taşınması durumunda, çeşitli problemlere yol açabilecek niteliktedir. Bu çalışmada, adli bilişim teknik ve donanımlarına ilişkin eksikliklerin neden olabileceği olası problemlerin önlenebilmesi için çeşitli çözüm önerileri sunulmaktadır. Çözüm önerileri, adli bilişim sürecinin denetim faaliyetlerine uyarlanması, denetçilere eğitim verilmesi, uygun bir yasal altyapı oluşturulması, bilgi sistemi denetim uzman ve araçlarının ortak kullanımı ve dış

[1] Ph.D., Senior Banking Sprecialist, CISA, Banking Regulaton and Supervision Agency, ilker.koc@yandex.com
[2] Assist. Prof., Ph.D., Gazi Üniversity, hcakir2000@yandex.com

Koç, İ., & Çakır, H. (2015). Denetim süreçlerinde dijital delillerin elde edilmesi ve korunması. *International Journal of Human Sciences*, *12*(2), 1092-1110. doi: 10.14687/ijhs.v12i2.3333

(Extended English abstract is at the end of this document)

kaynak sağlanmasıdır.

Anahtar Kelimeler: Denetim, Dijital Delil, Adli Bilişim, Bilgi Teknolojileri, Elektronik Delil, Adli Süreç

Giriş

Bir ülkedeki insanların birlikte yaşamasını sağlayan aygıt olan devlet yapısının en önemli görevlerinden birisi, ekonomik, sağlık, siyasi ve idari anlamda toplum yaşantısını ilgilendiren alanlarda belirlenen sınırlara uyulup uyulmadığının denetlenmesidir. Devlet tarafından gerçekleştirilen denetim faaliyeti, yargısal, siyasi veya idari şekilde gerçekleşebilmektedir. Yargısal denetim yargı organları olan mahkemeler tarafından gerçekleştirilirken, siyasi denetim yasama organlarınca yapılmaktadır. Diğer tüm yönetsel kurumların, yönetsel araçlar ve yöntemler kullanarak gerçekleştirdiği denetimler ise yönetsel veya idari denetim olarak adlandırılmaktadır (Okur, 2007:11). İdari denetim faaliyetlerinin kapsamı çevre kirliliğinden halk sağlığına, finansal sektörün etkin çalışmasından vergi mevzuatına uyum sağlanmasına kadar oldukça geniş bir alana yayılmaktadır (Köse, 2000:7).

Denetimler fiziki ortamların gözlenmesi, ilgili kişilerle görüşme yapılması veya yasal defterler ve diğer kayıtların incelenmesi şeklinde yapılabilmektedir (Kütük, 2008;107). Özellikle finans sektörü, vergi, bankacılık, kara para ile mücadele gibi ticari faaliyetlerle ilgili denetim süreçleri fiziki ortamlardan ziyade şirketlerin tuttuğu ticari defterler, faturalar, kayıtlar gibi bilgi ve belgeler üzerinden gerçekleştirilmektedir. Günümüz bilgi iletişim teknolojilerinin ulaşmış olduğu seviye ticari faaliyetlere ilişkin kayıtların yoğun olarak bilgisayar ortamlarında tutulması sonucunu doğurmaktadır. Bilgi iletişim teknolojilerini sağlayan donanım ve yazılımların maliyetlerindeki düşüşler, çok küçük boyutlardaki ticari faaliyetlerin bile elektronik ortamda kaydedilmesine imkân sağlamaktadır. Diğer taraftan, işlem, sayı ve tutarlarının çok yüksek miktarlara ulaştığı bankacılık veya sigortacılık gibi faaliyetler için bilgi sistemlerinin kullanımı bir zorunluluk haline gelmiştir (Ömürbek, 2003:145). Günümüz ticaret koşulları, çeşitli yasal uygulamalar ve müşteri istekleri de firmaları bilgi iletişim teknolojilerini kullanmaya zorlamaktadır. Bilişim teknolojilerinin böylesine yoğun kullanıldığı bir ortamda ticari faaliyetlere ilişkin denetim faaliyetlerinin elektronik ortamlar veya dijital medyalar gibi bilgi sistemi unsurları üzerinden yapılmasını kaçınılmaz hale gelmektedir. Bilgi sistemleri üzerinden gerçekleştirilen denetim süreci ise elektronik ortamda bulgu elde etme ve bu bulguların gerektiği durumlarda adli makamlar önünde delil niteliklerinin korunabilmesi sorununu gündeme getirmektedir.

Ülkemizde idari denetim faaliyetlerinin konusunu çoğunlukla, doğrudan Türk Ceza Kanunu (TCK) kapsamında suç unsuru oluşturan konular oluşturmamaktadır. İdari denetimlerde, kara para

Koç, İ., & Çakır, H. (2015). Denetim süreçlerinde dijital delillerin elde edilmesi ve korunması. *International Journal of Human Sciences*, *12*(2), 1092-1110. doi: 10.14687/ijhs.v12i2.3333

aklanması ile mücadele gibi bazı özel denetim türleri hariç olmak üzere, ağırlıklı olarak mevzuat hükümlerine aykırılığı suç oluşturmayan, ancak idari yaptırıma konu olan faaliyetler incelenmektedir. Ancak, denetimlerde doğrudan suç unsuru aranmadığı halde, suç oluşturan durumlarla karşılaşılabilmektedir. Diğer taraftan, TCK kapsamına girmemekle birlikte sonucunda çeşitli şekillerde idari yaptırım uygulanmış bir denetim faaliyeti, idari yaptırımın muhatabı tarafından yargıya taşınabilmektedir. Her iki durumda da idari denetim faaliyeti, adli sürece dâhil olmaktadır. Adli süreçte ise elde edilen denetim bulgularının delil niteliklerinin korunması önem taşımaktadır. Delil niteliğini kaybetmiş bir bulgunun ispat gücü zayıflayabilecektir veya hiç olmayacaktır. Özellikle, elektronik ortamlardan elde edilmiş bulunan dijital delillerin elde edilme ve korunması özel uzmanlık isteyen bir alandır (Göksu, 2010:89). Ülkemizde denetim faaliyeti ile görevlendirilmiş kurumların ise dijital delillerin elde edilmesine ve korunmasına ilişkin olarak yeterli düzeyde teknik uzmanlık, deneyim ve donanımının bulunup bulunmadığı tartışma konusudur. Ayrıca, denetim faaliyetlerinin çok büyük bir kısmında doğrudan TCK'nın konusunu oluşturan bir suç unsurunun tespitinin hedeflenmemesi ve elde edilen bulgulara da bu açıdan yaklaşılmaması nedeniyle dijital delillerin korunması konusunda yeterli özen gösterilmeyebilmektedir.

Bu çalışmada, dijital delil kavramı, dijital delillerin elde edilmesi ve korunmasına ilişkin süreçlerin açıklanması ve denetim faaliyetlerine ve tekniklerine ilişkin verilecek genel bilgiler ışığında idari denetim süreçlerinde dijital bulguların delil niteliklerinin korunmasına ilişkin çeşitli önerilerin sunulması amaçlanmaktadır. Çalışmada, konuya ilişkin teknik bilgi sunan daha önceki akademik çalışmaların derlenmesi yöntemi uygulanmıştır. Bu kapsamda, adli merciler ve kolluk güçleri tarafından kullanılan dijital delil elde etme metotlarına ilişkin yapılmış araştırmalar incelenerek, idari denetim faaliyetlerine uygulanabilecek genel bir yaklaşım geliştirilmeye çalışılmıştır.

1. Denetim Faaliyetleri

Günümüzün sosyal ve ekonomik hayatı, gerçek veya tüzel kişiler arasında veya bu kişiler ile kamu arası kurulmuş hukuki ilişkilere dayanmaktadır. Medeni ilişkiler, ticaret, sosyal hizmetler veya vatandaşlık görevleri gibi faaliyetler söz konusu hukuki ilişkiler aracılığı ile yürütülmektedir. Diğer taraftan, bahse konu ilişkilerin sağlıklı bir şekilde işlemesi için yasal düzenlemelere ihtiyaç bulunmaktadır. Özellikle, istikrarlı, güvenilir ve etkin bir ekonomik ortam sağlanabilmesi için, ticari ve ekonomik alanlardaki ilişkilerin detaylı şekilde düzenlenmesi gerekmektedir. Bu kapsamda, hem ülkemizde hem de dünyada bankacılık, sermaye piyasaları, rekabet hukuku, vergi, kamuyu aydınlatma, sağlık uygulamaları ve iş ve işçi güvenliği gibi alanlarda çok ayrıntılı düzenlemeler bulunmaktadır. Ancak, yalnızca düzenlemelerin olması değil, aynı zamanda bunlara uyulması da bu faaliyetlerin toplum yararına uygun şekilde gerçekleşmesi için önem arz etmektedir. Bu çerçevede,

Koç, İ., & Çakır, H. (2015). Denetim süreçlerinde dijital delillerin elde edilmesi ve korunması. *International Journal of Human Sciences*, *12*(2), 1092-1110. doi: 10.14687/ijhs.v12i2.3333

ekonomik ve sosyal faaliyetlerin mevcut kural ve düzenlemelere dolayısıyla toplum yararına uygun şekilde yürütülmesinin kontrolü, denetim faaliyetleri ile gerçekleştirilmektedir.

1.1. Denetimin Tanımı

Denetim faaliyeti değişik açılardan farklı şekillerde tanımlanabilir. Denetime ilişkin tanımlardan bazıları şöyledir; "Denetim, iktisadi faaliyet ve olaylarla ilgili iddiaların önceden saptanmış ölçütlere uygunluk derecesini araştırmak ve sonuçları ilgi duyanlara bildirmek amacıyla, tarafsızca kanıt toplayan ve bu kanıtları değerleyen bir süreçtir" (Güredin, 2000:5). Denetim, kişilerin, kuruluşların, kurumların, sistemlerin veya işlemlerin değişik yönlerden yapısını, içeriğini, işleyişini inceleyip, herhangi bir tutarsızlık, eksiklik, hata veya çelişki barındırıp barındırmadığının mevzuat hükümleri, genel kurallar ve mantık çerçevesinde değerlendirilmesi çabalarıdır (Aksoy, 2006:47). Amerikan Muhasebeciler Birliğinin tanımına göre ise denetim, "ekonomik faaliyetler ve olaylarla ile ilgili delillerin tarafsızca sağlanması ve belirlenmiş kriterler çerçevesinde değerlendirilerek, sonuçların ilgili kişilere iletilmesine ilişkin sistematik bir süreçtir" (American Accounting Association, 1973). Bu tanımlardan hareketle denetimin temel özelliklerini şu şekilde sıralayabiliriz:

a) Denetim sistematik bir süreçtir: Denetim belirli bir amacın gerçekleştirilebilmesi için aşamaları ve görev başlıkları önceden planlanmış bir faaliyettir. Denetimin amacı yapılacak denetim faaliyetinin türüne göre farklılık göstermekte ve denetim faaliyetinin kapsamını etkilemektedir.

b) Denetim, delil toplanması ve değerlendirilmesine dayanır: Denetim denetçinin kişisel görüşünü yansıtmaktadır. Ancak, bu görüş tarafsız ve kabul edilebilir delillere dayandırılmalıdır. Denetçi görüşlerini destekleyecek deliller aramamalı, deliller denetçinin görüşünü oluşturmasında yol gösterici olmalıdır. Delillerin elde edilmesinde, denetim amacı ve denetimin olası sonuçları göz önünde bulundurulmalıdır.

c) Denetim sonuçları ilgililere iletilir: Bütün denetimlerin ortak amacı, denetlenen hususa ilişkin bir sonuç ortaya çıkmasıdır. Genel olarak, denetim faaliyetleri üçüncü taraflara, resmi makamlara veya bizatihi denetlenene bilgi verilmesi, denetlenen hakkında idari bir uygulama yapılması veya yapılmaması, denetlenen hakkında adli makamlara başvurulması gibi sonuçlar ortaya çıkarır (Hesap Uzmanları Derneği, 2004:7). Denetim faaliyetleri sırasında delil elde edilirken bu olası sonuçların göz önünde bulundurulması, özellikle adli süreçte yer alacak delillerin geçerliliği konusuna dikkat edilmesi önemlidir.

1.2. Denetim Türleri

Denetim faaliyetlerini hukuki sonuçlar, denetimi gerçekleştiren taraf, denetimin amaçları, denetimde gönüllülük, denetimin konusu gibi açılardan farklı türlere ayırmak mümkündür. Bu çalışmada,

Koç, İ., & Çakır, H. (2015). Denetim süreçlerinde dijital delillerin elde edilmesi ve korunması. *International Journal of Human Sciences*, *12*(2), 1092-1110. doi: 10.14687/ijhs.v12i2.3333

çalışmanın alanını belirleyebilmek amacıyla yalnızca denetimi gerçekleştiren taraf ve hukuki sonuçlar açısından denetim türlerine değinilmektedir. Öncelikle, faaliyeti gerçekleştiren taraf açısından denetim, özel denetim ve kamu denetimi olarak ikiye ayrılmaktadır. Özel denetim, bağımsız denetim kuruluşları tarafından zorunlu veya isteğe bağlı olarak kurum veya kuruluşların Mali tablolarının, sistemlerinin veya çeşitli uygulamalarının yasal düzenlemelere veya ulusal ve uluslararası standartlara uygunluğunun denetlenmesidir. Burada denetleyenin özelliği kamu gücüne sahip olmamasıdır. Ancak, özellikle kamuya açıklanacak Mali tabloların bağımsız denetimi gibi çeşitli denetimlerde bu özel kuruluşların faaliyetleri ve bilgi isteme gibi çeşitli yetkileri kanun tarafından belirlenmiştir (Okur, 2007:25). Diğer denetim türü ise kamu denetimi diğer bir değişle idari denetimdir. İdari denetim, "görev ve yetkilerini yasalardan alan ve kamu adına, Kamunun ihtiyaçlarına cevap vermek üzere denetim yapan kişilerce gerçekleştirilen mali tablo, uygunluk ve faaliyet denetimlerini ifade eder" (Hesap Uzmanları Derneği, 2004:12).

Bu çalışma esas olarak idari denetim faaliyetlerine yönelmiştir. Ancak, idari denetim için öngörülen yaklaşımlar, ticari kuruluşların kamuya açıkladıkları Mali tabloların doğruluğuna ilişkin denetim yapan bağımsız denetim faaliyetleri için de uygun niteliktedir.

İdari denetimin temel özelliği denetçilerde kamu bakış açısının bulunmasıdır. Örneğin, incelenecek bir alanın tespitinde, elde edilen bir bulgunun geçerliliğinin belirlenmesinde veya bir hususun önemliliğine karar verirken kamu denetçisi mesleki yargı ve değerlendirmelerinin yanı sıra o konuya ilişkin yasa veya yönetmelikleri de dikkate almalıdır (Aksoy, 2006:348).

İdari denetimin önemi finans, vergi, rekabet gibi ekonomik ve sosyal hayatı etkileyecek ve incelenmesi özel uzmanlık isteyen alanlarda, doğrudan kanun ve mevzuata uygunluk açısından denetim yapılmasıdır. Bu denetimler ayrıca, sistematik olarak ve geniş bir çerçevede yapılmaları nedeniyle, bu alanlarda suç oluşturan faaliyetlerin tespitine en uygun inceleme süreçleridir. Ancak, suç konusu olayların engellenmesi ve suçluların cezalandırılması için denetim sırasında suç unsurunun tespit edilmesi yeterli olmamakta, bu tespitin adli süreçte geçerli olacak delillerle desteklenmesi gerekmektedir.

1.3. Denetim Teknikleri ve Delil Elde Etme

Denetim genel anlamda bir delil toplama ve bu delilleri değerlendirme faaliyetidir. Ancak denetim delilleri adli süreçteki delillerden farklılık arz eder. Bir bilginin delil olup olmaması, denetçinin öznel yargısıyla belirlenir. Hâlbuki, yasal delillerin niteliği önceden konulmuş kanunlarca belirlenmektedir (Güredin, 2000:129).

Bir delilin güvenilirliği, delilin konuyla ilgisine, geçerliliğine, tarihsel olarak uygun olmasına ve objektifliğine bağlıdır. Bir delilin niteliği, niceliği ve yeterliliği, denetçinin mesleki değerlendirmesi sonucunda belirlenir. Delil elde etme çalışmalarında incelenen konunun önem derecesi, niteliği ve

Koç, İ., & Çakır, H. (2015). Denetim süreçlerinde dijital delillerin elde edilmesi ve korunması. *International Journal of Human Sciences*, *12*(2), 1092-1110. doi: 10.14687/ijhs.v12i2.3333

delil toplamanın maliyeti gibi hususlar göz önünde bulundurulur. Delil elde etmek için denetim süreçlerinde uygulanan temel teknikler;

- Fiziki inceleme ve sayım,
- Gözlem,
- Doğrulama,
- Yeniden Hesaplama,
- Göz atma,
- Soruşturma,
- Belge İncelemesi,
- Kayıt Sisteminin İncelenmesi,
- Olağandışı İşlemlerin Derinlemesine Araştırılması,
- İlgili Hesaplar Arasında İlişki Kurma ve Karşılaştırma,
- Revizyon ve
- Analitik İnceleme

olarak sayılabilir. Bunlardan "Olağandışı İşlemlerin Derinlemesine Araştırılması" tekniği özellikle finansal kayıtlardaki hile, yolsuzluk dolandırıcılık gibi suç oluşturacak konuların tespitine yönelik bir tekniktir (Aksoy, 2006:376). Bu teknikler sonucu elde edilen deliller;

- Fiziki deliller,
- Doğrulamalar,
- Belgelenmiş deliller,
- Yazılı deliller,
- Matematiksel deliller,
- Sözlü deliller ve
- Analitik deliller

olmak üzere sınıflara ayrılabilir (Aksoy, 2006:351). Fiziki deliller, denetçinin fiilen görebildiği maddi varlıkların ve faaliyetlerin gözlenmesi sonucu elde edilen delillerdir. Fiziki delillerin tespit edildikleri anda kayıt altına alınmaları gerekir. Her ne kadar doğrudan bir bilgi olmaları nedeniyle güvenilirlikleri yüksek olsa da bu delillerin kayıt altına alınmasında zorluklar yaşanabilir. Doğrulamalar, denetlenen dışındaki üçüncü taraflardan alınan sözlü veya yazılı cevaplardır. Bunlar genellikle, üçüncü tarafın denetlenenle arasındaki ilişkinin teyit edilmesi şeklindedir. Belgelenmiş deliller, denetlenene ilişkin olarak bağımsız üçüncü tarafların hazırlamış olduğu yazılı belgelerin incelenmesi suretiyle elde edilmektedir. Yazılı deliller, denetlenenin veya denetlenen kuruluşun yetkilisinin denetçinin bir faaliyetiyle ilgili olarak denetçiye verdiği yazılı ifadelerdir. Matematiksel ve

Koç, İ., & Çakır, H. (2015). Denetim süreçlerinde dijital delillerin elde edilmesi ve korunması. *International Journal of Human Sciences*, *12*(2), 1092-1110. doi: 10.14687/ijhs.v12i2.3333

analitik deliller denetlenenin finansal ve finansal olmayan verilerinin aritmetik olarak veya karşılaştırma yoluyla incelenmesi sonucu elde edilmiş verilerdir. Sözlü deliller ise görüşme ve soruşturma gibi sözel denetim teknikleri vasıtasıyla ilgili kişilerden alınan bilgilerdir (Kütük, 2008:99). "Olağandışı İşlemlerin Derinlemesine Araştırılması" tekniği sonucu elde edilen delillerin aksine sözlü delillerin geçerliliği yapılan görüşmenin tutanak haline getirilmesi yani yazılı bir belgeye dönüştürülmesine bağlıdır. Yazılı bir belgeye dönüşmemiş görüşmelerde görüşme yapılan kişiler daha sonra verdikleri beyanatları kabul etmeme veya değiştirme olasılığı bulunmaktadır. Görüşmenin sesli kayıt altına alınması da bir diğer alternatif olabilmektedir. Ancak bu durumda da yine kayıttaki sesin ilgili kişi olduğunun kanıtlanması gerekebilecektir.

Bu noktada, bilişim sistemleri üzerinden yapılan denetimler açısından Bilgisayar Destekli Denetim Tekniklerinden (computer assisted audit techniques) bahsetmekte fayda bulunmaktadır. Bilgi sistemleri üzerinden yapılan denetimlerde "bilgisayar çevresinden denetim" ve "bilgisayar üzerinden denetim" olmak üzere iki yaklaşım bulunmaktadır. Bilgisayar çevresinden denetimde yalnızca fatura, irsaliye gibi belgelere ilişkin bilgi sistemine yapılan kayıtlar ve çeşitli kayıtlara ilişkin bilgisayardan alınan çıktılar araştırılmaktadır. Bu yaklaşımda, bilgisayar sisteminin bizatihi içinde hangi işlemin yapıldığı veya sistemde bulunan veriler üzerinde ne gibi değişiklikler yapıldığı incelenmemektedir. Bilgisayar üzerinden denetim yaklaşımında ise bilişim sistemi yazılımlar ve içindeki verilerle birlikte bir bütün olarak incelenmektedir (Selvi, Türel, Şenyiğit, 2005:4). Bu yaklaşımda denetçinin bilgisayar destekli denetim tekniklerini (BDDT) kullanması gerekmektedir.

BDDT, denetçilerin bilgisayar vasıtasıyla denetim yaptıkları kurum veya kuruluşun bilgi sistemine erişerek denetim delilleri elde etmesi olarak tanımlanabilir. BDDT, genelleştirilmiş denetim yazılımı, yardımcı programlar, test verileri, haritalama (mapping) ve uzman denetim sistemleri gibi pek çok tipte araç ve tekniği içermektedir. BDDT vasıtasıyla denetlenenin bilgi sisteminin yazılımları takip edilebilmekte, bilgi sisteminden çekilen veriler üzerinde analiz ve simülasyonlar yapılabilmekte ve hayali veriler üretilerek testler gerçekleştirilebilmektedir (Yurtsever ve Çatıkkaş, 2009:5).

BDDT aracılığıyla denetlenenin bilgi sisteminden alınan veriler üzerinden analiz yaparak birçok bulguya ulaşılabilir. Ancak, bunların kayıt altına alınması ve doğruluğuna ilişkin denetlenenden teyit alınması önemlidir. Bilişim sisteminden tespit edilen denetim bulguları açısından en uygun delillendirme yöntemlerinin başında, tespit edilen hususa ilişkin denetlenenin teyidini içeren yazılı ve imzalı belge alınması gelmektedir. Fakat denetlenen, konusunu suç oluşturan bir olaya ilişkin böyle bir belgeyi vermekten kaçınabilir. Üstelik belge talebinden sonra bilgi sisteminde var olan delili değiştirebilir veya yok edebilir. Çoğu zaman bilgi ve belgeyi ibraz etmemenin yaptırımı, belgenin doğuracağı hukuki sonuçlardan daha hafif olabilmektedir. Örneğin, TCK'nın "Suçtan kaynaklanan malvarlığı değerlerini aklama" başlıklı 282 nci maddesinde "suçtan kaynaklanan malvarlığı

Koç, İ., & Çakır, H. (2015). Denetim süreçlerinde dijital delillerin elde edilmesi ve korunması. *International Journal of Human Sciences*, *12*(2), 1092-1110. doi: 10.14687/ijhs.v12i2.3333

değerlerini, yurt dışına çıkaran veya bunların gayrimeşru kaynağını gizlemek veya meşru bir yolla elde edildiği konusunda kanaat uyandırmak maksadıyla çeşitli işlemlere tâbi tutan kişinin üç yıldan yedi yıla kadar hapis ve yirmibin güne kadar adlî para cezası" ile cezalandırılması öngörülmüş iken (Mevzuat, 2015a), suçtan elde edilmiş mal varlığının aklanmasına ilişkin delilleri gizlemek isteyen kişi, buna ilişkin defter, kayıt ve belgeleri tahrif etmesi veya söz konusu belgeleri gizlemesi halinde Vergi Usul Kanununun (VUK) 359 uncu maddesine göre onsekiz aydan üç yıla kadar hapis cezası ile cezalandırılabilecektir. Bunun da ötesinde, suç unsuru içeren bilgi veya belgeyi denetçiye hiç vermeyen kişi, VUK 355 nci madde uyarınca, özel usulsüzlük cezası ile cezalandırılacak ve yalnızca para cezası ile karşı karşıya kalacaktır (Mevzuat, 2015b).

Diğer taraftan, denetlenen yazılı belge vermekten kaçınmasa bile, teyidi istenen konu binlerce sayfaya basılması gereken, karmaşık analizler sonrasında ortaya çıkarılabilen veya diğer nedenlerden dolayı yazılı belge niteliğine uygun olmayan bir unsuru içerebilir. Bu bakımdan, bilişim sisteminden bulunan bir bulgunun, yazılı belgeye dönüştürmeden de, dijital delil olarak doğrudan elde edilmesi ve korunması gerekliliği söz konusu olabilmektedir.

2. Dijital Delil

Bilişim teknolojilerinin hayatın her alanında yoğun bir şekilde kullanılması bazı hukuki, ekonomik, sosyal ve siyasi kavramların yeniden tanımlanmasına veya mevcut tanımların genişlemesine neden olmuştur. Dijital delil kavramı da bu şekilde, delil kavramının genişlemesi ile oluşmuştur. Dijital delil "bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen soruşturma açısından değeri olan bilgi ve verilerdir" (Keser, 1994: 46). Bu açıdan, her türlü elektronik ortamdaki bilgi delil olabilmektedir. Dijital deliller değişik formlarda olabilir. Bu formlar aşağıdaki gibi sıralanabilir (Koçak ve Uzunay, 2005:3):

- Veri dosyaları,
- Kurtarılmış silinmiş dosyalar,
- Kayıp alanlardan kurtarılmış veriler,
- Dijital fotoğraf ve videolar,
- Sunucu kayıt dosyaları,
- E-posta,
- Yazılı Konuşma (Chat) Kayıtları,
- İnternet Geçmişi,
- Web Sayfaları,
- Kayıt Logları,

Koç, İ., & Çakır, H. (2015). Denetim süreçlerinde dijital delillerin elde edilmesi ve korunması. *International Journal of Human Sciences*, *12*(2), 1092-1110. doi: 10.14687/ijhs.v12i2.3333

- Abone Kayıtları

Dijital delillerin diğer delillerden en önemli farkı, dayanıklılığının fazla olmamasıdır. Fiziki deliller çoğunlukla uzun süre dayanabilmektedir. Hatta kan veya doku gibi organik kanıtlar bile belirli bir süre dayanabilmelerine rağmen dijital deliller çok çabuk bozulabilmekte, değiştirilebilmekte, kaybolabilmekte ve hatta yok edilebilmektedir (Tan, 2010).

Elektronik bir verinin geçerliliği bazı şartlara bağlıdır. Bu şartlar dijital delillerin bütünlüğü, doğrulanması, inkâr edilememesi, doğruluğu ve sonradan dikkate alınabilirliğidir. Bütünlük, kolayca üzerinde değişiklik yapılabilen elektronik ortamdaki veri üzerinde değişiklik yapılmadığının garanti altına alınmasıdır. Doğrulanma, elde edilen verinin belirli bir kişiye ait olduğunun kesin olarak belirlenebilmesi ve kanıtlanmasıdır. İnkâr edilememe, elde edilmiş dijital delilin içeriğinin ilgili kişi tarafından reddedilemeyecek şekilde ortaya konulabilmesidir. Doğruluk, elde edilen verinin doğruları yansıtıp yansıtmadığını tespit edilmesidir. Örneğin, internette yer alan bir bilginin doğruluğu için diğer geçerli kaynaklardan teyit edilmesi gerekmektedir. Sonradan dikkate alınabilme ise elde edilmiş bir verinin üçüncü şahıslar açısından da anlam ifade edebilmesidir (Koçak ve Uzunay, 2005:3).

Bütün bunların yanı sıra bir dijital delilin geçerliliği yani ispat gücü hukuka uygunluğuna bağlıdır. Bu açıdan denetçilerin dijital delillerin hukuk karşısındaki durumlarını bilmeleri ayrıca önem taşımaktadır. Aşağıdaki bölümde dijital deliller hukuki nitelikleri açısından tartışılmaktadır.

2.1. Dijital Delillerin Hukuki Nitelikleri

Dijital delillerin hukuki niteliklerini incelemeden önce hukukta ispat ve delil kavramlarının anlaşılması faydalı olacaktır. İspat, "dava konusu hakkın ve buna karşı yapılan savunmanın dayandığı vakıaların var olup olmadıkları hakkında mahkemeye kanaat verilmesi işlemi" olarak tanımlanmaktadır (Kuru, Arslan, Yılmaz, 2000:423). Aynı şekilde, delil kavramı ispat faaliyetinde kullanılan ve hâkimde dava öncesi, mahkeme dışında gerçekleşmiş olan olayların temsilen yargılama sürecine aktarılmasına yarayan ve olayı temsile elverişli olan bütün inandırma araçlarını içermektedir (Atalay, 1999:7). Delillerin değerlendirilmesi konusundaki düzenlemeler, kesin delile dayalı delil sistemi ve hâkimin takdirine (serbest değerlendirmesine) dayalı delil sistemi olmak üzere iki başlıkta toplanmaktadır. Serbest değerlendirme sisteminde hâkim kendi takdir hakkını kullanarak delilleri serbestçe belirleyebilmektedir. Buna karşılık, kesin delil sisteminde hâkim delil ile bağlıdır ve kanunda bir hususun "kesin delil" ile ispat edilmesi öngörülmüş ise hâkimin başka türlü bir değerlendirmede bulunması mümkün bulunmamaktadır (Nart, 2007:208).

Dijital delillerin yargı süreçlerinde ne şekilde dikkate alınacağı ve ispat güçleri, hukuk türüne göre değişmektedir. Kişiler arasındaki uyuşmazlıklardan kaynaklanan özel hukuk davalarının nasıl

Koç, İ., & Çakır, H. (2015). Denetim süreçlerinde dijital delillerin elde edilmesi ve korunması. *International Journal of Human Sciences*, *12*(2), 1092-1110. doi: 10.14687/ijhs.v12i2.3333

görüleceği Hukuk Muhakemeleri Kanununda (HMK) düzenlenmiştir. HMK'ya göre en önemli kesin delil unsuru "senettir". HMK'da senedin iptal gücü ve ispat alanı oldukça geniş tutulmuştur. Doktrindeki genel tanıma göre senet, belirli bir işlem hakkında tam bir bilgi içeren, bir kişi tarafından kendi aleyhine olacak bir olayın, ilerideki delilini oluşturmak için yazıp veya yazdırıp imzaladığı ve karşı tarafa verdiği belgedir. Bu anlamda güvenli elektronik imzalı elektronik belgeler, HMK'nın 202 maddesinin 2 inci fıkrasına göre, senet hükmündedir (Tuğ, 1994:54). Güvenli elektronik imza ile oluşturulmamış elektronik ortamdaki veriler ise HMK'nın 202 inci maddesine göre delil başlangıcı sayılabilmektedir. Bu veriler, hâkimin takdirine bağlı olarak, senetle ispatı kanunen zorunlu olmayan davalarda delil başlangıcı olarak dikkate alınabilmektedir. İspatı senetle yapılması zorunlu olan konularda ise güvenli elektronik imza ile oluşturulmamış elektronik verilerin varlığı halinde tanık dinlenmesi söz konusu olabilmektedir (Mevzuat, 2015c).

Konusunu suç oluşturan davaların görüldüğü ve davacının mutlaka devlet otoritesi olduğu ceza davalarına ilişkin yargılama usulü Ceza Muhakemesi Kanununda (CMK) düzenlenmektedir. CMK'da hukuk yargılamasının aksine, "kendiliğinden araştırma" ilkesi ve "delil serbestîsi" ilkeleri geçerlidir. Savcı, sanığın aleyhine veya lehine delilleri mahkemeye sunduğu gibi mahkeme heyeti de resen araştırma yapabilmektedir. CMK'da dikkate alınacak deliller konusunda hâkime geniş yetki tanınmıştır. Bu bakımdan her türlü elektronik verinin delil olarak kullanılması mümkündür. Ancak, dijital delillerin elde edilmesi hususunda çeşitli kısıtlamalar bulunmaktadır. CMK'nın "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma" başlıklı 134'üncü maddesine göre bir suç dolayısıyla yapılan soruşturmada, bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine ancak başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine hâkim tarafından karar verilebilmektedir. Yine aynı maddeye göre bilgisayar, bilgisayar programları ve bilgisayar kütüklerine, şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilmektedir. Fakat el konulan cihazlar, şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, gecikme olmaksızın iade edilmek durumundadır. Bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılmalı ve istenmesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilmelidir. Uygun olması halinde, bilgisayar veya bilgisayar kütüklerine el koymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilmektedir. CMK 206 ncı maddesine göre bir delilin geçerli sayılabilmesi için kanuna uygun şekilde elde edilmiş olması gerekmektedir. Bu bakımdan, veriyi usulüne uygun şekilde elde etmek delil olabilmesinin ön şartıdır (Mevzuat, 2015d).

Koç, İ., & Çakır, H. (2015). Denetim süreçlerinde dijital delillerin elde edilmesi ve korunması. *International Journal of Human Sciences*, *12*(2), 1092-1110. doi: 10.14687/ijhs.v12i2.3333

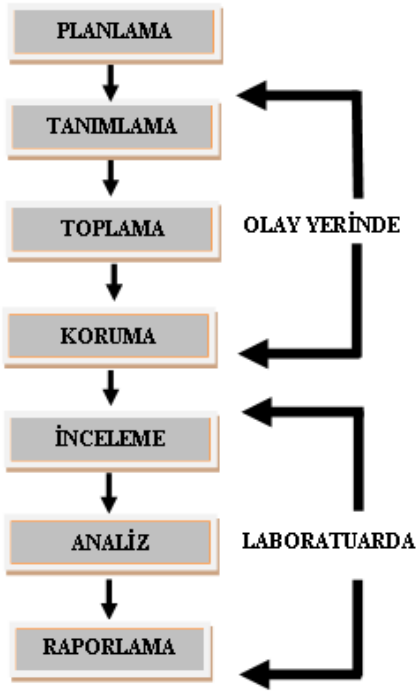
Devlet birimlerinin karar ve uygulamalarının dava edildiği idari davalarda, davacı taraf olan gerçek veya tüzel kişinin idare karşısında güçsüz olması ve dava konusu idari işlem ile ilgili delillerin idarenin elinde olması nedeniyle, haklılığını ispat ve delil sunması gereken taraf çoğunlukla devlettir. İdari yargılama usulü 20.01.1982 tarih ve 2577 sayılı İdari Yargılama Usulü Kanununda (İYUK) düzenlenmiş olup, dijital deliller konusunda hem ceza hukukuna hem de özel hukuka benzer düzenlemeler barındırmaktadır. Ceza hukukunda olduğu gibi idare hukukunda da "kendiliğinden araştırma", "delil serbestîsi" ve "delillerin serbestçe değerlendirilmesi" ilkeleri çerçevesinde sabit disk, hafıza kartı, cep telefonu gibi elektronik ortamdaki veriler idari yargılamalarda delil olarak kullanılabilmektedir (Parlak, 2006:61). İYUK'un 31 nci maddesinde ise delillerin tespitine ilişkin İYUK'da hüküm bulunmayan konularda HMK'nın uygulanacağı belirtilerek, HMK'da yer alan güvenli elektronik imzalı belgelerin delil niteliğine ilişkin hükümlerin idari yargılamalarda da geçerli olması sağlanmaktadır (Mevzuat, 2015e).

Mevzuat hükümleri incelendiğinde, ceza ve idari yargılamalarda delillerin hâkim tarafından serbestçe belirlenebilmesi nedeniyle dijital delillerin ispat gücü ve uygulanma alanı özel hukuk yargılamalarına göre daha yüksek olduğu görülmektedir. Özel hukukta ise güvenli elektronik imza ile imzalanmış belgeler kesin delil niteliğinde olup, bu belgeler en yüksek ispat gücüne sahiptir. Ancak, güvenli elektronik imza ile oluşturulmamış diğer dijital deliller yalnızca delil başlangıcı olarak dikkate alınmaktadır. Ceza ve idari yargılamalarda hâkim delilleri serbestçe belirleyip, değerlendirebilmesine rağmen bir dijital delilin dava sürecindeki geçerliliği, verinin bütünlüğüne, doğruluğu ve doğrulanabilmesine, inkâr edilememesine ve sonradan dikkate alınabilirliğine yani dijital delilin niteliklerinin korunmasına bağlıdır. Dijital bir verinin delil niteliği ise delilin doğru şekilde elde edilmesi ve korunması ise sağlanabilecektir.

2.2. Dijital Delil Elde Etme ve Koruma Yöntemleri

Dijital delillerin elde edilmesi adli bilişim faaliyetinin alanına girmektedir. "Adli bilişim, elektronik ortamlardan elde edilen bulguların, çeşitli teknik donanım ve yazılımlar kullanılarak hukuki delillere dönüştürülme süreci olarak tanımlanabilir" (Tan, 2010). Adli bilişim sürecine ilişkin çeşitli modeller geliştirilmiştir. Adli bilişim sürecini belirli aşamalar halinde gösteren bu modeller, dijital delillendirme sürecine ilişkin bir çerçeve sunmaktadır. Şekil 1'de yer alan geleneksel adli bilişim süreç modeli, 7 basamakta açıklanmaktadır (Debrota, Goldman, Mislan, Rogers, 2006:28).

Koç, İ., & Çakır, H. (2015). Denetim süreçlerinde dijital delillerin elde edilmesi ve korunması. *International Journal of Human Sciences*, *12*(2), 1092-1110. doi: 10.14687/ijhs.v12i2.3333



Şekil 1: Geleneksel Adli Bilişim Süreç Modeli (Debrota, Goldman, Mislan, Rogers, 2006:28)

Şekil 1'deki modelde de görüldüğü gibi, adli bilişim süreç modeli, genel olarak delillerin tanımlanması, toplanması, korunması, incelenmesi, analiz edilmesi ve raporlanması aşamalarından oluşmaktadır.

Delil toplama aşaması, adli bilişim uygulamaları açısından son derece önemlidir. Çünkü zamanında ve doğru şekilde toplanmamış dijital delillerin değiştirilmesi veya yok edilmesi ve dolayısıyla bir daha tespit edilememesi söz konusudur. Dijital bulguları doğru şekilde toplama ve koruma delillendirme sürecinin temelini oluşturmaktadır. Adli bilişimde delil toplama süreci olay yeri inceleme ve ilk müdahale kuralları çerçevesinde gerçekleştirilmektedir.

Olay yerine ilk müdahale mutlaka adli bilişim uzmanı tarafından yapılmalı, öncelikle çevre güvenliği sağlanarak olay yerine giriş ve çıkışlar kontrol altına alınmalıdır. Olay yerine ilgisiz üçüncü şahıslar kadar, konu ile ilgili olmayan kolluk güçleri ve diğer görevlilerin girişine de izin verilmemelidir. Ayrıca, üçüncü şahıslar olay yerinden uzaklaştırılırken delil olabilecek herhangi bir unsuru yanlarında götürmediklerinden emin olunmalıdır (Duman, 2012:12). Daha sonra dijital delil barındırabilecek bilgisayar, harici bellek, akıllı telefonlar gibi tüm medyalar ve bu medyalara erişim şifrelerini barındırabilecek tüm kâğıt ve not gibi dijital olmayan belgeler tespit edilmelidir. Tespit edilen tüm unsurlar tek tek fotoğraflanmalı ve etiketlenmelidir (Aydoğan, 2009:12). Dijital medyalara ilk müdahale yöntemi bilgisayar sisteminin açık veya kapalı olmasına göre farklılaşmaktadır. Eğer bilgisayar sistemi açıksa, herhangi bir müdahale sonucu depolama aygıtlarındaki "uçucu verilerin" kaybedilme olasılığı vardır. Uçucu veriler, bilgisayar kapandığında ortadan kalkan verilerdir (Çakır ve

Koç, İ., & Çakır, H. (2015). Denetim süreçlerinde dijital delillerin elde edilmesi ve korunması. *International Journal of Human Sciences*, *12*(2), 1092-1110. doi: 10.14687/ijhs.v12i2.3333

Sert, 2010:149). Ayrıca, açık bir bilgisayar sistemi saldırı altında olabilir. O yüzden açık bir bilgisayar sistemi ile karşılaşılınca öncelikle saldırının durdurulması, uçucu verilerin kaydedilmesi ve sistemin, "dijital bubi tuzaklarının" çalışmasını engellemek amacıyla, elektrik bağlantısının kesilerek kapatılması gerekmektedir (Duman, 2012:18).

Açık bilgisayar sistemi kapatıldıktan sonra veya kapalı bir bilgisayar sistemi ile karşılaşıldığında delil niteliği taşıyan tüm cihaz ve araçlar etiketlenerek korunmak üzere paketlenmelidir. Tespit edilen ve etiketlenen medyalar birbirlerine zarar vermeyecek ve manyetik ortamların zararlarından korunacak şekilde anti-manyetik ve anti-statik malzemelerle paketlenerek taşınmalıdır (Tulum, 2006:88). Adli bilişim sürecinde dijital medyalardaki veriler orijinal medyalar üzerinden değil, orijinal medyanın dokunulmazlığını bozmayacak şekilde alınmış kopyalar üzerinden incelenir. Bu şekilde delilin bütünlüğü korunmaya çalışılır. İmaj almak için kullanılan çeşitli özel yazılımlar mevcuttur. Adli bilişim alanında en çok kullanılan yazılımlar "EnCase®" ve "FTK®"dır. EnCase yazılımı imaj almanın yanı sıra, verilerin analizinde de kullanılabilmektedir. Fiziksel olarak zarar görmüş medyalardaki verilerin kurtarılmasında ise "PC3000®" adlı cihaz kullanılmaktadır (Çakır ve Sert, 2010:161).

İnceleme aşamasında kopyalanmış medyalar üzerindeki veriler ile silinmiş veya format atılmış veriler analiz edilmek üzere kaydedilir. Bu aşamada dosyaların oluşturulma, değiştirilme veya erişim zamanları, dosyayı oluşturanların kimliği, dosyaların kopyalanıp kopyalanmadığı gibi hususlar incelenir. Dijital delillerin analizi, bir medya üzerinden, işletim sistemi üzerinden veya bilgisayar ağları üzerinden analiz şeklinde üç farklı elektronik ortam türünde olabilmektedir. Elektronik oramda suç unsuru analizi yapabilmek için araştırılacak suçun hukuki özellikleri konusunda da yeterli seviyede bilgi sahibi olmak gereklidir. Çünkü suçun tür ve özelliklerine göre delilin farklı bilişim sistemi unsurlarında aranması gerekebilecektir. Örneğin, dosya üzerinden incelemelerde dosya oluşturma veya dosyaya erişim bilgileri delil olabilmekte, işletim sistemi üzerinden yapılan analizlerde ise sistemin açılıp kapanma tarih ve saatleri, internet erişim kayıtları ve işletim sistemi üzerindeki mesajlar delil kaynağı olarak kullanılabilmektedir (Duman, 2012:32).

Raporlama aşaması, dijital medyalar üzerindeki veriler üzerinden yapılan analiz ve inceleme sonuçlarının mahkeme ve diğer ilgili makamlara sunulma işlemidir. Bu işlem genellikle yazılı rapor şeklinde yapılmaktadır. Raporlamada dikkat edilmesi gereken husus, delillerin tarafların anlayacağı şekilde açıklanıyor olmasıdır (Tan, 2010). Adalet mekanizması içerisinde yer alan hakim, savcı veya avukatların adli bilişim uygulama ve terimlerine ilişkin tüm teknik ayrıntıları bilmeleri beklenmemektedir. Fakat bu kişiler adli bilişim raporları doğrultusunda savunma yapacak, iddia öne sürecek veya karar vereceklerdir. Bu nedenle adli bilişim uzmanı, hazırlayacağı rapordaki teknik

Koç, İ., & Çakır, H. (2015). Denetim süreçlerinde dijital delillerin elde edilmesi ve korunması. *International Journal of Human Sciences*, *12*(2), 1092-1110. doi: 10.14687/ijhs.v12i2.3333

konuları uzman olmayan kişilerin de anlayabileceği şekilde basitleştirmeli, ancak rapora ilişkin bir inceleme yapılmak istendiğinde yeterli bilgiyi sunacak şekilde ayrıntı içermelidir.

Sonuç ve Öneriler

Adli bilişim sürecinin aşamaları ve denetim faaliyetlerinde öngörülen delil toplama teknikleri birlikte ele alındığında denetim faaliyetlerinin adli süreçte yer alacak dijital delillerin sağlıklı bir şekilde elde edilmesi ve bütünlüğünün korunmasına tam olarak uygun olmadığı sonucuna ulaşılmaktadır. Adli bilişim süreci ile denetim faaliyetlerinin farklılıklarına ilişkin bilgiler özet olarak aşağıda sunulmaktadır

Adli bilişim sürecinin özellikleri incelendiğinde;

- Adli bilişim faaliyetinin esas itibarıyla suç odaklı olduğu,
- Delillerin mahkeme sürecinde kullanılmak üzere ilgili mevzuata göre toplandığı,
- Dijital delillerin elde edilmesine ve toplanmasına ilişkin standart prosedürlerin olduğu,
- Kolluk güçlerinin, dijital delillerin elde edilmesine yönelik, uzman birimlerinin bulunduğu,
- Adli bilişim süresinde genellikle elektronik medyaların imajları üzerinden inceleme yapıldığı

görülmektedir. Buna karşın, denetim sürecinin dijital delil elde etmeye yönelik özellikleri değerlendirildiğinde;

- Denetim faaliyetlerinin çoğunlukla suç odaklı olmadığı,
- Delillerin denetçinin yargısına göre toplandığı,
- Dijital delillerin elde edilmesine ve korunmasına yönelik özel bir prosedür bulunmadığı,
- Denetim birimlerinde, dijital delillerin elde edilmesine ilişkin yeterli uzmanlığı olan personelin olmadığı veya çok az sayıda olduğu,
- Denetim faaliyetlerinde incelemelerin genellikle çalışan sistemler üzerinden yapıldığı

sonuçlarına ulaşılmaktadır.

Yukarıda sayılanlar haricinde, denetim süreçlerinde elde edilen dijital delillere yönelik uygulama ve yasal altyapı anlamında da çok ciddi eksiklikler bulunmaktadır. Denetim ile ilgili mevzuatlarda bilgi sistemleri üzerindeki delillerin nasıl elde edileceği hüküm altına alınmamıştır. Dijital deliller, belirli bir standart olmadan denetçinin mesleki yargısı çerçevesinde elde edilmektedir.

Bu durum, denetimlerde idari veya hukuki dava konusu olabilecek veya ceza konusu olan dijital delillerin niteliklerinin kaybedilmesi riskini taşımaktadır. Bilgi sistemlerinin sosyal ve ekonomik

Koç, İ., & Çakır, H. (2015). Denetim süreçlerinde dijital delillerin elde edilmesi ve korunması. *International Journal of Human Sciences*, *12*(2), 1092-1110. doi: 10.14687/ijhs.v12i2.3333

hayatımızdaki kullanımının artışı ve taşıdığı önem dikkate alındığında, dijital delillendirmeye yönelik bu eksikliğin ileride önemli bir sorun olarak karşımıza çıkma ihtimali bulunmaktadır. Ancak, denetim süreçlerinde dijital delillerin elde edilmesi ve korunmasına ilişkin çeşitli yöntemler geliştirilebilir. En uygun çözüm hâlihazırda dijital delillendirmeye yönelik olarak prosedürler geliştirmiş ve uzmanlık kazanmış olan adli birimlerin ve kolluk güçlerinin uygulamış olduğu yöntem ve tekniklerin denetim birimleri faaliyetlerine uyarlanması olacaktır. Bu çerçevede, idari denetim faaliyetlerinde dijital delillendirme süreçlerinin sağlıklı bir şekilde uygulanabilmesi için çeşitli öneriler aşağıda yer almaktadır.

1- Tüm denetçilere adli bilişim uygulamaları dijital delillendirme süreçleri hakkında eğitim verilmelidir. Verilecek eğitim sayesinde denetçilerin istemeden delilleri bozmasının önüne geçilebilecek ve özel uzmanlık istemeyen dijital delillerin denetçiler tarafından elde edebilmesine imkân sağlanabilecektir. Ancak, karmaşık bilgi sistemleri üzerinden yapılan denetimlerde, dijital delillendirme için verilecek eğitimler yeterli olmayabilecek ve başka bir kaynağa ihtiyaç duyulabilecektir.

2- Bilgi Teknolojileri ve İletişim Kurumu ve Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) başta olmak üzere, bilgi ve iletişim teknolojilerinde uzmanlaşmış kurum ve kuruluşların işbirliği ile denetim süreçlerinde delil elde edilmesi ve bu delillerin korunması hakkında yol gösterici standartlar ve yasal altyapı oluşturulmalıdır.

3- Denetim yapmakla görevli tüm kurumlarda, dijital delillendirme konusunda uzman istihdam edilmelidir. Bu şekilde, denetçilerin gerekli durumlarda bu uzmanları denetim ekibine dâhil etmesi veya denetim süreci sırasında destek alması yoluyla dijital delillendirme sürecinin doğru şekilde gerçekleştirilmesi sağlanabilir. Ancak, sürekli personel istihdamının ve adli bilişim faaliyetlerinde kullanılan cihazların maliyetleri düşünüldüğünde sürekli istihdamın kaynak israfına yol açabileceği de göz önünde bulundurulmalıdır.

4- Kurumlar arası işbirliği arttırılarak dijital delillendirmeye yönelik personel veya cihaz gibi kaynakların ortak kullanımına yönelik çalışmalar yapılabilir. Kurumlar arası yapılacak protokollerle veya yasal bir düzenlenme ile ortak kaynak kullanımı sağlanabilir. Örneğin, bu konularda uzmanlığı bulunan Bilgi Teknolojileri ve İletişim Kurumu, dijital delillendirme için gerekli cihazlara sahip, uzman bir ekip istihdam edebilir ve Maliye Bakanlığı, Sermaye Piyasası Kurumu veya Bankacılık Düzenleme Denetleme Kurumu gibi idari denetim yapan kurumlar gerekli durumlarda Bilgi Teknolojileri ve İletişim Kurumundan yardım talep edebilirler. Fakat böyle bir durumda uzman ekibin iş yükünün aşırı olması, yığılma nedeniyle uzman ekibin müdahalesinin gecikmesi ve bu

Koç, İ., & Çakır, H. (2015). Denetim süreçlerinde dijital delillerin elde edilmesi ve korunması. *International Journal of Human Sciences*, *12*(2), 1092-1110. doi: 10.14687/ijhs.v12i2.3333

yüzden dijital delillerin kaybedilmesi, gerekli olmadığı halde uzman ekip kullanımına gidilmesi gibi sorunlar ortaya çıkabileceği dikkate alınmalıdır.

5- Kurumların, dijital delillendirmeye yönelik ihtiyaçlarını dış hizmet alımı (outsourcing) yolu ile karşılaması bir alternatif olarak düşünülebilir. Gerekli durumlarda hizmet sunucu firma, personeli ve gerekli ekipmanı ile denetim ekibine yardımcı olmak üzere denetim sürecine dâhil olabilir. Kurum da aldığı hizmet karşılığı firmaya bir ücret ödeyerek hizmeti satın alabilir. Bir ücret karşılığı hizmet alındığından dolayı gereksiz hizmet alımı yoluna gidilmemesi söz konusu olacaktır. Ancak, dış hizmet alımında hizmet alınacak firmanın yeterliliği, her ihtiyaç duyulduğunda gecikmeden cevap verebilecek kapasiteye sahip olması ve elde edilecek bilgilerin gizliliğinin sağlanması konularına dikkat edilmesi gerekmektedir.

Kaynakça

Aksoy, T. (2006). *Tüm Yönleriyle Denetim*. 2. Baskı, Ankara, Yetkin Yayınları.

American Accounting Association, Committee on Basic Auditing Concepts. (1973). *A statement on Basic Audit Concepts*. Sarasota, USA.

Atalay, O. (1999). *Emare İspatı*. Manisa Barosu Dergisi, 18 (70), 7-8.

Aydoğan, H. (2009). *Adli Bilişimde Yeni Elektronik Delil Elde Etme Yöntemleri*. Polis Akademisi, Güvenlik Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara.

Çakır, H., Sert, E. (2010). *Bilişim Suçları ve Delillendirme Süreci*. 2. Uluslararası Terörizm ve Sınıraşan Suçlar Sempozyumu Bildirisi, 143-170, 7-9.12.2010, Ankara.

Debrota, S., Goldman, J., Mislan, R. & Rogers, K. M. (2006). *Computer Forensics Field Triage Process Model*. ADFSL 2006 Conference on Digital Forensics, USA.

Duman, Emrah. (2012). *Bilgisayarlarda ve Bilgisayar Ağlarında Delil Toplama ve Türkiye'deki Uygulama Sorunları*. Yayınlanmamış Yüksek Lisans Proje Ödevi. Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Güredin, E. (2000). *Denetim* , 7. Baskı, İstanbul: Beta Yayınları.

Göksu, M. (2010). *Hukuk Yargılamasında Elektronik Delil*. Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Yayımlanmamış Doktora Tezi, Ankara.

Hesap Uzmanları Derneği, (2004). *Denetim İlke ve Esasları*. 4. Baskı, Ankara: Maliye Hesap Uzmanları Derneği Yayınları.

Keser, B. L. (1994). *Adli Bilişim (Computer Forensic)*. 1. Basım, Ankara: Yetkin Yayınevi.

Koçak, M., Uzunay, Y. (2005). *Bilişim Suçları Kapsamında Dijital Deliller*. Akademik Bilişim Konferansı Bildirisi, 2-4 Şubat 2005, Gaziantep Üniversitesi. Gaziantep.

Köse, H. Ö. (2000). *Dünyada ve Türkiye'de Yüksek Denetim*. Ankara: Sayıştay Yayınları.

Kuru, B., Arslan, R., Yılmaz, E. (2000). *Medeni Usul Hukuku*. Ankara: Yetkin Yayınları.

Kütük, İ. (2008). *Kamu ve Bağımsız Muhasebe Denetiminde Kanıt Toplama Teknikleri*. Yayınlanmamış Yüksek Lisans Tezi. Trakya Üniversitesi, Sosyal Bilimler Enstitüsü, Edirne.

Koç, İ., & Çakır, H. (2015). Denetim süreçlerinde dijital delillerin elde edilmesi ve korunması. *International Journal of Human Sciences*, *12*(2), 1092-1110. doi: 10.14687/ijhs.v12i2.3333

Mevzuatı Geliştirme ve Yayın Genel Müdürlüğü. (2015a). *Türk Ceza Kanunu.* http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf, (erişim tarihi: 08.10.2015).

Mevzuatı Geliştirme ve Yayın Genel Müdürlüğü. (2015b). *Vergi Usul Kanunu.* http://www.mevzuat.gov.tr/MevzuatMetin/1.4.213.pdf, (erişim tarihi: 08.10.2015).

Mevzuatı Geliştirme ve Yayın Genel Müdürlüğü. (2015c). *Hukuk Muhakemeleri Kanunu.* http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6100.pdf, (erişim tarihi: 08.10.2015).

Mevzuatı Geliştirme ve Yayın Genel Müdürlüğü. (2015d). *Ceza Muhakemesi Kanunu.* http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5271.pdf, (erişim tarihi: 08.10.2015).

Mevzuatı Geliştirme ve Yayın Genel Müdürlüğü. (2015e). *İdari Yargılama Usulü Kanunu.* http://www.mevzuat.gov.tr/MevzuatMetin/1.5.2577.pdf, (erişim tarihi: 08.10.2015).

Nart, S. (2007). *Alman ve Türk Hukukunda Senetle İspat.* Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, 9(1), 207-232.

Okur, Y. (2007). *Türkiye'de Kamu Denetimi; Değişim Süreci ve Performans Denetimi.* Ankara: Nobel Yayınları.

Ömürbek, V. (2003). *Kurumsal Kaynak Planlamasında Muhasebe Bilgi Sisteminin Rolü :Gıda Sektöründe Uygulama.* Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Doktora Tezi, Isparta.

Parlak, B. (2006). *İdari Yargıda İspat ve İspata Yarayan Araçlar.* Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Selvi, Y., Türel, A., Şenyiğit, B. (2005). *Elektronik Bilgi Ortamlarında Muhasebe Denetimi.* 7. Muhasebe Denetimi Sempozyumu Bildirisi, İstanbul.

Tan, A. (2010). *Adli Bilişim (Computer Forensic).* http://edirnebarosu.org.tr/incelemeler/adli-bilisim-computer-forensic/ (erişim tarihi: 20.11.2012).

Tuğ, A. (1994). *Türk Özel Hukukunda Şekil.* 1. Baskı, Konya: Mimoza Yayınları.

Tulum, İ. (2006). *Bilişim Suçları ile Mücadele.* Yayınlanmamış Yüksek Lisans Tezi. Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Isparta.

Yurtsever, G., Çatıkkaş, Ö. (2009). *Bankacılık Sektöründe Bilgisayar Destekli Denetim.* Vergi Sorunları Dergisi, 2009, p251.

Extended English Abstract

This study will discuss deficiencies in obtaining digital evidences in legally admissible way in audit activities in Turkey. Besides, it is aimed to develop a solution proposal to correct deficiencies in question by comparing audit and computer forensic techniques.

Audit has a key role in today's economic and social world. Independent audit activities or supervision of legal authorities provide assurance about different subjects such as effective use of public resources, accountability or stability of financial sector. Audit activities in banking, finance or other commercial sectors have become one of the most important business line in the last few decades. Wide usage of information technologies in financial and other sectors effect audit processes. Auditors must use information system tools, understand IT environment and have knowledge about different IT components for an effective audit. Furthermore, auditors must have knowledge about legal and technical aspects of digital evidences. Obtaining digital evidences

Koç, İ., & Çakır, H. (2015). Denetim süreçlerinde dijital delillerin elde edilmesi ve korunması. *International Journal of Human Sciences*, *12*(2), 1092-1110. doi: 10.14687/ijhs.v12i2.3333

from electronic environments and protecting chain of custody and integrity of digital evidences are important for both audit process and judicial process.

In this study, former studies about computer forensic and audit are compiled and differences between two techniques will be compared.

Scope of audit activities may vary from public health to financial statements. Some basic audit techniques are inspection of tangible assets, observation, confirmation and examination of authoritative documents and other records. Nowadays almost all commercial and noncommercial institutions use information systems to keep financial and other records. Therefore, audit of financial statements have to be performed via information system. Furthermore, computer aided audit techniques (CATT) are used for obtaining and analyzing data from IS in audit process. CATT and other similar audit techniques are basically used for obtaining audit evidence from information systems. In addition, validity of the audit evidence depends on judgment of the auditor; in this respect audit evidence differs from legal evidence, which is circumscribed by rigid rules. However audit evidences are frequently used in legal process. Hence, auditors should be aware of obtaining evidences from information systems in an appropriate manner.

Gathering evidences from an information system falls within area of computer forensics discipline. Computer forensics can be defined as the discipline that combines elements of law and computer science to collect and analyze data from information systems such as computers, networks, wireless communications, and storage devices in a way that is admissible as evidence in a legal process. Computer forensic activities require expertise and special equipment.

Computer forensic examination process can be divided into eight phases. These phases are planning, defining, collecting, preserving, examining, analyzing and reporting. Generally first four phases are related with obtaining evidence and performed in investigation scene. Examining and analyzing phases are performed in laboratory environment.

Computer forensics is primarily concerned with proper acquisition and preservation of digital evidence. Obtaining evidence is maybe the most important activity of computer forensic process. Digital evidences differ from physical evidences in changeability. Digital evidences can be changed, destroyed or converted easily. Therefore, when collecting digital data as evidence, certain rules of computer forensics' crime scene investigation should be followed.

In examination and analysis phases, tasks such as evidence tracing, evidence validation, recovery of hidden/encrypted data, data mining are performed. The last phase of computer forensics process is reporting phase. Tasks related to this phase are documentation and presentation of evidences.

Computer forensic process focuses on crime and evidences are collected in a predetermined, systematic manner to ensure admissibility in court. There are standard procedures to follow to collect, preserve and analysis to digital data. Mostly computer forensic specialists made image copies of digital storages and media. Examinations and analysis are made on these copies in order to prevent from altering the original image.

On the one hand, in Turkey, regulatory authorities and other institutions which are responsible for supervising and auditing different sectors do not have sufficient technical knowledge and equipment for computer forensic investigation. Consequently, there may be problems about admissibility of evidences which are obtained from audit activities in court.

Koç, İ., & Çakır, H. (2015). Denetim süreçlerinde dijital delillerin elde edilmesi ve korunması. *International Journal of Human Sciences*, *12*(2), 1092-1110. doi: 10.14687/ijhs.v12i2.3333

These problems are mainly caused by investigation methodology and shortage of experienced personnel and specialized equipment. Audit activities generally don't focus on crime, and there isn't any specific procedure to collect and preserve digital evidence. Beside, unlike the computer forensic process, audits and examinations are usually performed on living systems, not copied images.

This study aims to develop some proposals to solve these problems that might negatively affect admissibility of digital evidence. These proposals are adoption of computer forensic technics to audit methodologies, provide proper training to auditors and examiners, establish convenient legal infrastructure, common use of computer forensic resources by different institutions and outsourcing.