Düzce Üniversitesi Bilim ve Teknoloji Dergisi

Araştırma Makalesi

Atık Kayıt Ortamlarının Veri Güvenliği Yaklaşımı ile Değerlendirilmesi

Tuba ÖZTÜRK [a, *]

[a] *Çevre Müh. Bölümü, Çorlu Müh. Fakültesi, Tekirdağ Namık Kemal Üniversitesi, Tekirdağ, TÜRKİYE*
** Sorumlu yazarın e-posta adresi: ozturk_tuba@yahoo.com*
DOI: 10.29130/dubited.799565

ÖZET

Bu çalışmada yapılarında kayıt ortamı bulunduran cihazların, atık konumuna geçtikten sonra veri güvenliği açısından değerlendirilmesi amaçlanmıştır. İçinde bulunduğumuz çağın özelliklerine bağlı olarak günümüz insanları, büyük ölçüde teknoloji odaklı yaşamaktadır. Bilgisayar, akıllı telefon, tablet, internet vs. artık yaşamın ayrılmaz parçaları olarak, hemen hemen tüm faaliyetlerin merkezinde bulunmaktadır. Günümüz teknolojisinin en önemli özelliği çok kısa sürede kendini yenilemesi, geliştirmesi, değiştirmesidir. Bu durum teknoloji temelli cihazların kullanım ömürlerinin, her geçen gün daha da kısalmasına neden olmaktadır. Gerek cihazların depolama kapasiteleri, gerekse aktivitelerin çoğunlukla bu cihazlar üzerinden gerçekleştirilmesi, söz konusu cihazlarda önemli miktarda bilginin toplanması ve depolanması anlamına gelmektedir. Cihazların kullanım süreleri dikkate alındığında bu durum, veri güvenliği açısından ciddi endişelere yol açmaktadır. Verilerin kalıcı şekilde silinmesinin, teknik bilgi gerektiren oldukça karmaşık bir süreç olması bu endişelerin başlıca nedenidir. Çoğu durumda kullanıcıların teknik bilgilerini aşan silme işlemi, veri yönetiminin en az verilerin saklanması kadar önemli bir diğer alanıdır. Bu yaklaşım her durum ve her ortamdaki veri için geçerlidir. Özellikle atık kayıt ortamlarındaki verilerin bu kapsamda değerlendirilmesi gizlilik ve güvenlik açısından son derece önemlidir.

Anahtar Kelimeler: *Atık kayıt ortamı, Kayıt teknolojisi, Veri güvenliği, Veri imha*

Assessment of Waste Recording Media with the Data Security Approach

ABSTRACT

In this study it is aimed to assess devices that contain recording media in their structures after they become waste in terms of data security. Based on the characteristics of the era we are in, today's people are living in a largely technology-focused way. Computers, smartphones, tablets, the internet, etc. are now at the center of almost all activities as indispensable parts of life. The most important characteristic of today's technology is that it renews, improves and changes itself in a very short time. This situation means increasingly shortened usage lifespans of technology-based devices. Not only the storage capacities of the devices but also the fact that activities are carried out mostly over these devices indicate collection and storage of a significant amount of information on the devices in question. Considering the usage times of devices, this situation leads to serious concerns in terms of data security. The fact that permanently deleting data is a highly complicated process that requires technical knowledge is the main reason for these concerns. The operation of data wiping, which mostly exceeds the technical knowledge of users, it another field of data management which is at least as important as data storage. This approach is valid for every situation and data on every medium. Assessment of especially data on waste recording media in this context is highly important in terms of privacy and security.

Keywords: *Waste recording media, Recording technology, Data security, Data destruction*

Geliş: 24/09/2020, Düzeltme: 27/09/2020, Kabul: 29/10/2020

I. GİRİŞ

Yeryüzünde insanlığın başlangıcından itibaren yaşam, insanoğlunun bilgiyi üretme, saklama ve aktarma yeteneğine bağlı olarak şekillenmiştir. Bu noktada elde edilen bilginin korunarak başkalarına, gelecek nesillere aktarılması insanlığın her zaman en temel ve doğal davranış kalıbını oluşturmuştur. Bilginin korunması, aktarılması doğal olarak her geçen gün geliştirilmesini, çoğalmasını ve insanlığın günümüzdeki yaşam koşullarına ulaşmasını sağlamıştır. İnsanlar ilk çağlardan beri edindikleri bilgiyi saklamak ve korumak için çeşitli kayıt ve depolama sistemlerine ihtiyaç duymuşlardır. İnsanoğlunun doğuştan sahip olduğu en temel bilgi depolama ortamı, beyindir. Ancak insan beyini, her durum, amaç ve bilgi türü için tek başına yeterli değildir. Bunun temel nedenlerinden birisi, bilginin geri alınması/çağrılması durumda bilgi güvenliğinin, bireye ve yaşam koşullarına bağlı olarak değişmesidir. Diğeri ise bireyin yaşamının sona ermesinden sonra bilgiye ulaşılamamasıdır. Tüm bu gerçekler insanlığı kayıt ortamı olarak önceleri taş, kâğıt vs. kullanmaya, sonrasında ise daha fonksiyonel bilgi depolama sistemleri geliştirmeye sevk etmiştir.

Genel olarak bilgi depolama sistemlerinden beklenen temel işlevler verileri gerektiğinde geri almak için güvenli şekilde korumak, bilgileri yaymak ve iletmek olarak sıralanmaktadır [1]. Bu kavramlar insanların günlük yaşamlarını dijital teknoloji ile çevrili olarak geçirdikleri günümüz dünyasında, daha da anlam kazanmaktadır. İçinde yaşadığımız bilgisayar çağının gereği olarak insanlar giderek artan şekilde sosyal ve eğitim uygulamalarında, ticari ve resmi işlemlerinde çeşitli dijital platformları kullanmakta, buna bağlı olarak da bilgisayar, akıllı telefon, tablet, internet vs. günlük yaşamın ayrılmaz parçası haline gelmektedir. Bu şekilde günlük aktivitelerin çoğunlukla dijital platformlara kayması, hareketli ve sürekli artan veri hacimlerinin oluşmasına neden olmaktadır [2,3]. Yapılan araştırmalar mobil dijital cihaz kullanımının sürekli ve katlanarak büyüdüğünü, 2014 yılında mobil veri trafiğinde Latin Amerika'nın %133'lük bir artışla ilk sırada, Avrupa'nın ise %98'lik artışla ikinci sırada yer aldığını göstermektedir. Aynı yıl için küresel mobil cihaz aboneliklerinin 7,1 milyara ulaştığı ve 2020 yılında 9,5 milyara ulaşacağı tahmin edilmektedir [4]. Bunun yanı sıra hızla artan akıllı mobil cihaz kullanımı ile 2015 yılında ayda 3,7 eksabayt olan küresel mobil veri trafiğinin, 2020 yılında 30,6 eksabayta çıkması beklenmektedir [5]. Teknolojinin geldiği bu son duruma bağlı olarak araştırmalar, teknolojik ortamda verinin depolanması ve iletimine odaklanmaktadır. Her geçen gün yazılımcılar tarafından verileri izlemek, görselleştirmek, iletmek ve bağlantı kurmak için geliştirilen çok sayıda cihaz piyasaya sürülmektedir [2,3].

Yaşanan bu dijital dönüşüm ve teknolojiye karşı oluşan büyük ilgi, gündelik hayatın içinde yer alan ve yoğun şekilde kullanılan çok sayıda dijital cihaz gerçeğine neden olmaktadır. Mevcut bilgiye ve araştırmalara bağlı olarak bu cihazların en önemli özelliği kullanım ömürlerinin çok kısa olmasıdır. Teknolojik gelişmeler, günün gerekleri ve bilginin somutlaştırılma hızı söz konusu bu cihazların kısa sürede eski, yetersiz ve demode olarak atık konumuna düşmesine sebep olmaktadır. Farklı isimlerle adlandırılan yaşadığımız bu dönem ve onunla özdeşleşen dijitalleşme siber güvenlik, veri güvenliği, veri imha vs. gibi gizlilik ve güvenlikle ilgili çeşitli kavramların ve kaygıların teknolojiyi kullanırken ya da atık olarak elden çıkarmak istediğimizde hayatımıza girmesine sebep olmaktadır.

II. KAYIT ORTAMLARI VE TEKNOLOJİLERİ

Bilgi teknolojisinin küreselleşmesi ile veri depolama, içinde bulunduğumuz dijital çağın en önemli sorunlarından birisi haline gelmiştir [6]. Veri depolama fizik, kimya, malzeme başta olmak üzere temel ve uygulama alanındaki pek çok disiplini ilgilendiren multidisipliner bir konudur. Herhangi bir veri depolama sisteminin belirli bir takım temel kriterleri karşılaması beklenmektedir. Bunlardan ilki verilerin üzerine yazılacağı bir depolama ortamı, diğeri ise verilerin yazılması, okunması ve yorumlanmasıdır [1,6]. Bu amaçla geçmişten günümüze kullanılan ya da kullanılmış olan, mikrofilmler, manyetik bantlar, dijital lineer bantlar, CD (Compact Disc), DVD (Digital Versatile Disc) ve Blu-Ray'ler, taşınabilir bellekler, kartlar, floppy diskler, sabit diskler, manyeto-optik diskler vs. gibi çok

çeşitli mekanizmalar ve kayıt ortamları bulunmaktadır. Sabit diskler üzerine verilerin kaydedildiği manyetik malzeme ile kaplanmış bir veya daha fazla sert plakadan oluşan ve büyük miktarlarda bilginin depolanabildiği manyetik kayıt ortamlarıdır. Sabit disk teknolojisi eski olmasına rağmen, depolama yoğunluğu yılda yaklaşık %30 oranında artmaktadır. Mikrofilmler, küçültülmüş fotoğraf kaydı içeren nispeten ucuz depolama ortamlarıdır. Seçilen film türüne de bağlı olarak, iyi korunan mikrofilmler ile veriler uzun süre saklanabilmektedir. Manyetik bantlar, verilerin kodlanabileceği manyetik kaplamalı plastik şeritlerdir. Bunlar yüksek depolama kapasitesine sahip, uzun süreli depolamalar için uygun olmayan, nispeten ucuz sıralı erişim kayıt ortamlarıdır. Dijital lineer bantlar, veri depolamada kullanılan bant teknolojisi ile geliştirilmiş dayanıklı ve yüksek kapasiteli depolama ortamlarıdır. Manyetik bantlara göre veriye erişim çok daha hızlı gerçekleşmektedir. Floppy diskler, manyetik malzeme ile kaplanarak, koruyucu içine alınmış esnek, plastik disklerdir. Manyeto-optik diskler, yüksek kapasiteli, hızlı veri erişimi sağlayan hem manyetik hem de optik kayıt ortamlarıdır. CD, DVD ve Blu-Ray'ler, lazer ile yazılıp okunan, farklı depolama kapasitelerine sahip, en çok kullanılan optik kayıt ortamlarıdır [1,7,8].

Son yıllarda veri depolama yoğunluğunda yaşanan büyük artışa karşın elektronik cihaz boyutlarının dikkat çekici şekilde küçüldüğü görülmektedir. Bu durum belleklerin fiziksel sınırlarının aşılmasında yüksek yoğunluk, hızlı yanıt, uzun süre saklama ve yeniden yazma yeteneğini birleştiren yeni kayıt ve malzemelere karşı talep oluşmasına neden olmaktadır. Verilerin kaydedilmesinde manyetik, optik ve elektriksel kayıt teknolojileri kullanılmaktadır. Valdemar Poulsen tarafından 1890'lı yıllarda geliştirilen manyetik kayıt, hala veri depolamadaki en önemli teknolojilerden birisi olarak kullanılmaktadır [1,6]. Optik kayıt manyetik depolamadan sonra geliştirilmiş, yüksek depolama kapasitesine ve uyuma sahip kayıt teknolojisidir. Elektriksel kayıt bilginin, uygulanan gerilime yüksek ve düşük iletkenlik tepkisine dayanarak depolandığı bir kayıt tekniğidir. Manyetik depolamanın aksine süperparamanyetik, optik depolamanın aksine dalga boyu sınırının olmaması en önemi avantajları olarak sıralanmaktadır [6].

Tüm bu kayıt teknikleri ve kayıt ortamlarına bağlı olarak kapasite, erişim, hız, dayanıklılık, güvenlik ve kullanım ömrü gibi kavramlar, dijital yaşamla gelişen ihtiyaç ve beklentilerin odağındaki araştırma konularını oluşturmaktadır. Bunun yanında kayıt ortamlarının fiziksel ömürleri, yapılarının stabilize edilerek bu sürelerin iyileştirilmesi ve en uygun depolama ortamlarının seçilmesi giderek önem kazanmaktadır. Tablo 1'de bazı kayıt ortamları için fiziksel kullanım süreleri verilmektedir.

Tablo 1. *Bazı kayıt ortamlarının tahmini kullanım süreleri [7].*

Kayıt Ortamı	**İdeal Kullanım Süresi** *(yıl)*	**Uygun Kullanım Süresi** *(yıl)*
Sabit sürücü	<100	10-20
Sabit disk kartuşu	<100	20-40
Manyetik bant	30-100	5-20
Mikrofilm	500	100-200
Manyeto-optik disk	5-100	2-30
Dijital lineer bant	30-100	5-20
WORM	30-200	5-50
DVD	100	20
DVD-R	20-30	10
CD-R	5-100	2-30
CD-ROM	30-200	5-50

III. ATIK KAYIT ORTAMLARINDA VERİ GÜVENLİĞİ

Bilgi çağında veri, kritik bir değer olarak kabul edilmekte ve uzun süre korunması, depolanması, teknolojinin en temel kaygısı haline gelmektedir. Bu noktada başlıca veri kayıpları kasıtlı veya kasıtsız veri imhası, ortamın bozulması, ortamın, donanımın veya yazılımın eskimesi nedeniyle gerçekleşmektedir. [7]. Bilgilerin yaklaşık %70'inin herhangi bir basılı formata dönüştürülmeden

sadece depolama ortamlarında saklanması, yapılan çalışmaları ve teknolojik gelişmeleri daha çok veri kayıplarının önlenmesi ve verilerin geri alınması üzerine yoğunlaştırmaktadır. Bu durum kayıt ortamlarındaki verilen silinmesini oldukça karmaşık ve zor bir süreç haline getirmektedir. Ancak veri yönetimi açısından verilerin uzun süre korunması, saklanması kadar güvenli bir şekilde silinmesi ve imha edilmesi de büyük önem taşımaktadır [9]. Veri güvenliği ve imhası atık kayıt ortamları yönetiminin en önemli başlığını oluşturmakta, veri yönetimini bu süreci de kapsayacak şekilde genişletmektedir.

Modern dünyada her yıl mevcut depolama kapasitesinin buna bağlı olarak veri hacmi ve hareketliliğinin katlanarak arttığı bilinmektedir. Buna karşın teknolojik bilgi ve cihazların kullanım ömürleri her geçen gün daha da kısalmaktadır. Kısalan kullanım süreleri veri imhasını, yapısında kayıt ortamı bulunduran her türlü cihaz ve araç açısından başlı başına bir güvenlik problemi haline getirmektedir [10]. Yaşantımızı çevreleyerek günlük hayatımızın ayrılmaz bir parçası konumuna gelen teknolojik cihazların çoğu, yüksek depolama kapasitesine sahip kayıt ortamları içermektedir. Atık akışında ciddi miktarlarda bulunan bu cihaz, araç ve parçaları, içerdikleri bilgiler ve bu bilgilerin risk düzeyleri açısından atık yönetiminde ciddi bir sorun haline dönüşmektedir [11]. Literatürde bu konuda yapılan çalışmalar elden çıkarılan kayıt ortamlarındaki bilgilerin hacmi ve türünün endişe verici boyutlarda olduğunu göstermektedir. Bu konuda yapılan bir çalışmada elden çıkarılan bilgisayarların %10'undan daha az bir kısmında verilerin uygun şekilde imha edildiği, %75'inde bilgilerin okunabilecek ve kurtarılabilecek şekilde bulunduğu belirtilmektedir. Ayrıca erişilen bilgilerin kredi kartı numaraları, banka hesap numaraları, işlem tarihleri, hesap bakiyeleri, tıbbi kayıtlar, özel yazışmalar vs. gibi hassasiyet düzeyi yüksek veriler olduğu ifade edilmektedir [7]. Yine yapılan başka bir çalışmada disklerin %52'sinden kurumsal bilgilerin, %51'inden de kişisel bilgilerin geri alınabileceği, bu disklerin sadece %31'inden verilerin kolaylıkla geri alınamayacak standartlarda silindiği ortaya konulmaktadır. Elde taşınan cihazların %23'ünden kurumsal bilgilerin, %19'undan kişisel bilgilerin geri alınabileceği yine bu cihazların %51'inden ise kullanılan yöntem ve araçlarla verilerin geri alınamayacağı belirtilmektedir. Bilgisayarlar, cep telefonları vs. gibi depolama ortamları içeren cihazları, bilgi güvenliği açısından riskli hale getiren en önemli faktörlerden birisi, bu cihazların depolama kapasitelerinin buna paralel olarak kayıtlı bilgi hacminin sürekli artıyor olmasıdır. Ayrıca her türlü veri için yeterince depolama alanının olması, bilgilerin etkin şekilde silinmesi için çaba gösterilmesini engellemektedir [12].

Bilgilerin etkin şekilde silinmesi çoğunlukla standart silme yöntemleri ile sağlanamamaktadır. Sistem, dosyaları kayıt ortamına yazarken başka bir yere de dosyanın konumunu yazmaktadır. Silme komutları ile yalnızca dosyaların konumları hakkındaki bilgiler silinerek, adı üzerinden dosyaya ulaşılması engellenmektedir. Dosya alanının kullanılabilir olarak işaretlendiği standart silme yöntemlerinde, dosyanın kendisi ortamda kalmaktadır [7,13]. Sistemler bilgilerin silinmesinden çok bilgilerin korunması, kurtarılması ve geri alınması odaklı çalışmaktadır. Bu nedenle de silinen ya da çeşitli nedenlerle kaybedilen bilgilerin geri alınmasını sağlayacak, çok sayıda program ve araç geliştirilmiştir. Verilerin geri alınması artık ticari bir hizmet alanı konumundadır ve profesyonel anlamda kayıp verilen %80-90 oranında geri alınabileceği belirtilmektedir [7]. Bu durum teknolojinin ve dijital teknolojiyi kullanan uygulamaların yaygınlaştığı, insanların yaşam biçimini değiştirdiği, sınır ötesi elektronik ticaretinin arttığı günümüzde, güvenlik ve gizlilik kavramları ile birlikte değerlendirilmelidir. Her türlü bilgiyi toplayan, işleyen ve dağıtan sistemlerin giderek daha açık ve bağlantılı hale gelmesi, veri yönetiminde yeni güvenlik teknolojilerine duyulan ihtiyacın boyutlarını ortaya koymaktadır. Dijital içerik dağıtımı, günümüzde ortaya çıkan en hızlı faaliyet alanlarından birisidir. Bunun temel nedeni bilgiye erişimin çok kolay ve hızlı olmasıdır. Bilginin yaygınlaşması, çeşitli avantajlarının yanısıra yetkisiz veri erişimi ile kişisel veya kurumsal bilgilere kolaylıkla ulaşılmasını, kopyalanmasını ve dağıtılmasını sağlamaktadır [10,14]. Bilgi güvenliği gizlilik, bütünlük ve kullanılabilirlik yaklaşımları etrafında değerlendirilmelidir. Veri güvenliği ihlallerini, veri sızıntılarını ve bunların sonucunda ortaya çıkacak çeşitli problemleri önlemek için veri imha güvenliğinin, veri yönetiminin önemli bir parçası haline gelmesi gerekmektedir. Sağlam bir veri yönetimi verileri toplarken, depolarken, alırken, atarken gizli bilgilere yetkisiz erişimin engellenmesi, iyi bir veri imha politikası ve süreci anlamına gelmektedir [13,15]. Bu yaklaşım verilerin yetkisiz erişim, kullanım, imha, değiştirme ve ifşaya karşı korunmasını esas almaktadır. Bunu için de verilerin niteliğine ve risklerine göre uygun araç ve yöntemlerin kullanılması temel ilkedir (10,16). Veri imhasında kullanılan çok sayıda araç ve yöntem bulunmaktadır. Ancak çoğu durumda silinen dosya ve veri bloklarının geri alınabiliyor olması, bu konuda güvenilir,

onaylanmış yöntemlerin kullanılmasını kritik hale getirmektedir [13]. Tüm bu veri güvenliği ve yönetimi ile ilgili temel prensiplerin her durum ve her ortamdaki veriler için geçerli olduğu bilinmektedir. Özellikle atık kayıt ortamlarındaki verilerin bu temel prensipler kapsamında değerlendirilmesi son derece önemlidir.

Pratikte uygulanan veri imha yöntemleri yazılım tabanlı, donanım tabanlı veri silme ve kayıt ortamının fiziksel imhası olarak üç başlık altında toplanmaktadır. Genel bir veri imha süreci farklı kayıt ortamlarının, farklı yöntemler gerektirdiği gerçeği üzerine kurulmalıdır. Yöntemler arasındaki farklılıkların doğru analiz edilebilmesi, veri kayıt teknolojilerinin bilinmesine bağlıdır [10,13,15].

Günümüzde en çok kullanılan veri imha yöntemlerinden birisi, depolanan verilerin anlamsız karakterlerle değiştirilerek imha edildiği üzerine yazma yöntemidir. Bir disk silme yazılımının kullanıldığı yöntem, tüm kayıt ortamının ya da yalnızca belirli bir dosyanın üzerine anlamsız karakterlerin birden çok (7, 35 vs.) yazılmasıyla gerçekleştirilir. Yazılımın verileri temizlemesi GB başına yaklaşık 30-40 dakika sürmektedir. Ortamın manyetikliğinin giderilmesi ile verilerin imha edildiği yöntemde ise genel olarak iki teknik kullanılmaktadır. Bu tekniklerden birisi kalıcı mıknatıs etkisine diğeri elektromanyetik etkiye dayanmaktadır. Verilerin imhasında, üzerine yazma yönteminden çok daha etkili olduğu kabul edilen bu yöntemde, verilerin tamamen silinmesi için ortamın büyük bir manyetik güce maruz bırakılması gerekmektedir. Kayıt ortamının fiziksel olarak tahrip edilmesine dayanan veri imha yönteminde ise bu amaçla kırma, parçalama, öğütme gibi işlemler kullanılmaktadır. Bu yöntem mevcut yöntemeler arasındaki en etkili veri imha yöntemi olarak değerlendirilmektedir. Sürecin başarıya ulaşması için işlemlerin, ortam tamamen tahrip edilinceye kadar devam etmesi önemlidir. Fiziksel imha yönteminde tanımlanmış farklı hasar seviyeleri bulunmaktadır. Bazı hasar seviyelerinin ortamın onarılarak verilerin geri alınmasına olanak sağladığı bilinmektedir. İmha özelliklerinin yanı sıra üzerine yazma işleminin atık kayıt ortamlarının yeniden kullanılmasına imkân tanıdığı, manyetikliğin giderilmesi işleminin ise çoğunlukla ortamın bozulmasına neden olduğu gerçeği, yöntemlerin değerlendirilmesi açısından göz önünde bulundurulmalıdır. [9,15,17,18]. Yapılan çalışmalar her yöntemin farklı seviyelerde olmakla birlikte, bir miktar risk taşıdığını göstermektedir. Bu risklerin mümkün olduğu kadar azaltılması için üzerine yazma ve fiziksel imha veya manyetikliği giderme ve fiziksel imha yöntemlerinin birlikte kullanılması önerilmektedir. Süreçlerin kullanımı kolay, güvenliği kanıtlanmış ekipmanlarla yürütülmesi ve işlem sonuçlarının test edilerek, emin olunması büyük önem taşımaktadır. Veri imha süreci geri dönüşüm tesisi veya geri dönüşüm tesisinin çalıştığı imha firması tarafından mutlaka belgelenmelidir. İmha belgeleri tarih, yöntem, kayıt ortamı ile ilgili teknik bilgi, kayıt tarihleri, imhayı denetleyen ve tanık olanların imzalarını içermeli ve kalıcı olarak saklanmalıdır [9,12,17].

IV. SONUÇ

Teknoloji çağının en kritik kavramlarından birisi haline gelen veri kaydedilmesi, imhası, geri alınması ve güvenliği ile yeni ihtiyaçlar, beklentiler ve endişeler oluşturmaktadır. Günümüzde teknolojik araştırmalar çoğunlukla kayıt tekniklerinin ve kayıt ortamlarının iyileştirilmesi, geliştirilmesi odaklı ilerlemektedir. Bunların sonucu olarak da kayıt ortamlarında depolanan veri miktarı, sürekli ve katlanarak artmaktadır. Kurumsal ya da kişisel her türlü verinin uzun süre depolanması kadar, yetkisiz erişime karşı korunması da teknolojik çalışmalar için önemli bir araştırma konusudur. Bu noktada en önemli güvenlik mekanizmalarından birisi, verilerin kayıt ortamlarından geri alınamayacak şekilde kalıcı olarak silinmeleridir. Ancak mevcut teknoloji aynı zamanda bu konudaki en büyük engeli oluşturmaktadır. Çünkü teknolojik sistemler verilerin silinmesinden çok mümkün olduğunca fazla miktarda verinin, mümkün olduğunca uzun süre depolanması esas alınarak tasarlanmaktadır. Bu yaklaşım verilerin silinmesinden çok geri alınmasının önünü açmakta ve kolaylaştırmaktadır. Gerçekten de günümüzde kayıt ortamlarından verilerin kalıcı şekilde silinmesi, teknik bilgi gerektiren oldukça karmaşık ve zor bir süreçtir. Ancak veri, cihaz sahipleri tarafından çoğunlukla bu süreç ve potansiyel riskleri tam olarak anlaşılamamaktadır. Bu durum atılan, elden çıkarılan cihazlarla birlikte önemli miktarda yüksek hassasiyete sahip veriyi, her türlü erişime açık hale getirmektedir. Özellikle günün

gereği olarak atık akışında yoğun şekilde bulunan teknolojik cihazlar ve yapılarındaki kayıt ortamları, veri güvenliği açısından oldukça kritik atıklardır. Bu nedenle de atık konumundaki bozuk ya da çalışan her türlü kayıt ortamının, sızıntı ve yetkisiz erişime karşı veri güvenliği kapsamında yönetilmesi, her geçen gün daha da önem kazanmaktadır.

V. KAYNAKLAR

[1] S. N. Piramanayagam, "Introduction," *Developments in Data Storage Materials Perspective,* S.N. Piramanayagam and T. C. Chong, Eds. John Wiley& Sons ABD, 2012, ss. 1-9.

[2] E. Ruppert, J. Law and M. Savage, "Reassembling Social Science Methods: The Challenge of Dijital Devices, *Theory, Culture & Society,* c. 30, s. 4, ss. 22-46, 2013.

[3] N. Livari, S. Sharma, L. Venta-Olkkonen, "Digital Transformation of Everyday Life – How COVID-19 Pandemic Transformed the Basic Education of the Young Generation and Why Information Management Research Sould Care?," *International Journal of Information Management,* Article in Press.

[4] A. Viloria, O. B. Pineda Lezama, N. Mercado-Caruzo, "Factors that Describe the Use of Digital Devices in Latin American Universities, *Procedia Computer Science,* c. 175, ss. 127-134, 2020.

[5] J. Ma, L. Song and Y. Li, "Cost Efficiency for Economical Mobile Data Traffic Management from Users' Perspective," *IEEE Transactions on Wireless Communications,* c. 16, s. 1, ss. 362-375, 2017.

[6] H. Wu, L. Zhang and Y. Song, "High Density Magnetic Data Storage," *High Density Data Storage Prenciple, Technology, and Materials,* Y. Song, D. Zhu, Eds. World Scientific, Singapur, 2009, ss. 1-68.

[7] P. T. Davis, "Data Management: Data Destruction and Preservation, Part 1," *EDPACS,* c. 31, s. 3, ss. 1-15, 2003.

[8] A. Thomasian, "Secondary Storage Systems," *Computer Sciences,* A. B. Tucker, Ed. Taylor & Francis, ABD, 2004, ss. 555-588.

[9] M. D. Bergren, "Data Destruction," *The Journal of School Nursing,* c. 21, s. 4, ss. 243-246, 2005.

[10] M. Petkovic, W. Jonker, J. Terstegge, P. Brey, "Introduction," *Security, Privacy, and Trust in Modern Data Management,* M. Petkovic and W. Jonker, Eds. Springer, Almanya, 2007, ss. 1-38.

[11] T. Öztürk, "Elektronik Atık Yönetiminde Veri İmha Güvenliğinin Yeri ve Önemi," 7. *Ulusal Katı Atık Yönetimi Kongresi-UKAY'2015,* 14-16 Ekim, Gaziantep, 2015.

[12] A. Jones, "Lessons not Learned on Data Disposal," *Digital Investigation,* c. 6, ss. 3-7, 2009.

[13] R. Raman and D. Pramod, 2013, "A study on Data Privacy, Protection & Sanitization Practices During Disk Disposal by Indian Educational Institutes," *International Journal of Computer Science Issues,* c. 10, s. 2, ss. 53-58, 2013.

[14] C. Pauletto, "Options toward a Global Standard for the Protection of Individuals with Regard to the Processing of Personal Data," *Computer Law & Security Review,* Article in Press.

[15] R. Winter, “SSD vs HDD-Data Recovery and Destruction,” *Network Security*, c. 2013, s. 3, ss. 12-14, 2013.

[16] C-H. Lin, P-K. Yang, and Y-C. Lin, “Detecting Security Breaches in Personal Data Protection with Machine Learning” *2020 14th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, Tayvan, 2020.

[17] A. Kelleher, “How to Responsibly Destroy Hard Drives” *Health Management Technology*, c. 32, s. 10, 16-18, 2011.

[18] G. Cantrell and J. R. Through, “The Five Levels of Data Destruction a Paradigm for Introducing Data Recovery in a Computer Science Course” *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*, USA, 2019.