Elektronik Belgelerin Arşivlenmesinde Gerçekliğin ve Bütünlüğün Korunması*

Preservation of Integrity and Authenticity in the Archiving of Electronic Records

*Cengiz AYDIN** ve Fahrettin ÖZDEMİRCİ****

Öz

Belgeler, bilgi teknolojilerinin kurumsal yapılarda yoğun bir şekilde kullanılmasıyla birlikte elektronik ortamda yönetilmeye başlanmıştır. Elektronik belgelerin kurumsal yapı içinde yoğun bir şekilde kullanılmaya başlanması sağlıklı bir arşivlemeyi ve buna bağlı olarak elektronik belgelerin gerçekliğini ve bütünlüğünü korumayı zorunlu hale getirmiştir. Buna yönelik sağlıklı çözümler geliştirmek elektronik belge yönetim sisteminin başarısı açısından büyük önem taşımaktadır. Bu makalede, elektronik belgelerin, bilgi teknolojileri bağlamında gerçekliğinden ve bütünlüğünden taviz vermeden uzun dönem arşivlenmesi için gereken hususlar ortaya konulmuştur.

Anahtar sözcükler: *Elektronik belge yönetimi, e-Arşivleme, e-Belge bütünlüğü, e-Belge gerçekliği, Dijital koruma, Dijital imza*

Abstract

Records have become to be managed in electronic media ever since information technologies were used in institutional structures intensively. The use of electronic records in institutional structures makes it compulsory to make a good archiving, and hence to realize the protection of the authenticity and integrity of electronic records. It is significantly important to find sustainable solutions to this for the success of management systems of electronic records. In this article, the necessary issues in order to provide the sustainable archiving of electronic records and protecting the authenticity and integrity of them are explained.

Keywords*: Electronic records management, e-Archiving, Integrity of e-records, Authenticity of e-records, Digital preservation, Digital signature*

* Bu calışma Cengiz Aydın'ın "Elektronik Belgelerin Arşivlenmesi ve Erişim" (2010) başlıklı doktora tezine dayanmaktadır.

** Kültür ve Tanıtma Ataşesi; Türkiye Cumhuriyeti Saraybosna Büyükelçiliği, Bosna-Hersek. (aydincen@hotmail.com)

*** Doç.Dr.; Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Bilgi ve Belge Yönetimi Bölümü, Ankara. (ozdemirci@ankara.edu.tr)

Giriş

Elektronik belgeler, genel olarak bilgisayar teknolojilerine dayalı bir yapı içerisinde iş süreçleri sonucunda üretilen, işlenen ve arşivlenen belgelerdir. Bu çerçevede üretilen belgelerin etkin arşivlenmesi ve güvenli erişim yapısı içinde kullanılması gerekmektedir. Zira arşivleme sistemindeki zafiyet ya da erişim sistemindeki güvenliğe yönelik açıklar elektronik belgelerin gerçekliğini ve bütünlüğünü tehlikeye sokacaktır. Bu açıdan elektronik belgelerin gerçekliğini ve bütünlüğünü koruyan bir yapı içinde arşivlenmesi kaçınılmaz bir zorunluluktur. Bu yasal ve idari açıdan karşılaşılabilecek muhtemel sorunları önleyecek ve elektronik belgelerin delil vasfının korunmasını sağlayacaktır. Bu bağlamda, elektronik imzanın geçerliliğinin zamana bağlı olup, sürekliliğinin sağlanamaması gibi gerçekliği ve bütünlüğü tehdit edecek elektronik imza sorunları ve bilgi teknolojilerinin kullanılmasından kaynaklanan olumsuzlukları çözüme kavuşturmak ya da asgari düzeye indirmek için gerekli çalışmaların yapılması bir zorunluluk olarak ortaya çıkmaktadır.

Etkin arşivleme sistemi, beraberinde iyi işleyen elektronik belge yönetim sistemini gerektirir. Arşivlemeye ve güvenli erişime ilişkin teknolojik altyapının ve e-belge yönetim modellemesinin yetersiz olduğu kurumlarda e-belge üretmek ve e-arşiv oluşturmak kurumun kendi bilgi birikimine erişimini sekteye uğratacaktır. Bununla birlikte elektronik belge yönetimi sistemi içinde, belgelerin gerçekliği ve bütünlüğü önemli risklerle karşı karşıya kalacak ve teknolojik sürdürülebilirlik imkânsız hale gelecektir.

Elektronik Belge ve Yönetimi

Belge deyince kurumsal yapı içindeki iş süreçleri sonucunda her türlü ortamda üretilen belge anlaşılmaktadır. Bu açıdan bilgi teknolojilerindeki gelişmelere paralel olarak belge kavramı, elektronik anlayış içinde değerlendirilmeli, tanımlanmalı ve bu çerçevede yönetilmelidir. Bu kapsamda elektronik belge; bilgisayar ya da diğer elektronik cihazlar aracılığıyla elektronik ortamda iş süreçleri sonucunda üretilen, arşivlenen, erişilen, iletilen ve imha edilen her türlü belgeyi ifade eder. Bununla birlikte dijitalleştirilmiş kâğıt belgelerin, elektronik belge sayılabilmesi ve yasal açıdan gerçekliğinin olabilmesi için dijitalleşme sırasında değişime uğramadığına dair değiştirilemez bir zaman damgasının vurulması gerekmektedir. Bu işlem dijitalleştirme faaliyeti esnasında olabileceği gibi, dijitalleştirilen belgeye ayrı bir zaman damgası işlemi yapılmak suretiyle de gerçekleştirilebilir (Aydın, 2010, s. 44). Böylece dijital belgenin gerçekliği ve bütünlüğü korunmuş olur. Ancak yasal açıdan dijital ortama aktarılmış kâğıt belgelerin geçerliliğini kabul eden kanuni hükümler henüz bulunmadığı için delil niteliği taşımamaktadır. Bununla birlikte dijitalleştirilen belgelere vurulan zaman damgası elektronik belgelerle ilgili kanunlar bağlamında değerlendirilerek yasal açıdan kabul edilebilir.

Elektronik dokümanlar, uygulama yazılımları ve bilgisayar kullanımıyla dijital ortamda üretilen ve depolanan bilgi ya da veri dosyalarıdır. Değişik manyetik ve optik depolama ortamlarında bilgisayar yazılım ürünleri vasıtasıyla oluşturulurlar. Bir başka

ifade ile elektronik doküman, elektronik ortamda belgenin üretimi, düzenlemesi, gönderilmesi, alınması ya da depolanması olarak tanımlanabilir (California Records and Information Management [CalRIM], 2002, s.3).

Elektronik belge ile elektronik doküman aynı değildir. Elektronik doküman, elektronik belge hüviyetini ancak kurumsal işlemlerde kullanıldığında ve bu işlemlerin delili olarak saklandığında kazanır. Örneğin, kelime işlemci programı kullanılarak yazılan resmi bir yazı, bütün onay süreçleri tamamlanana kadar elektronik doküman niteliğindedir. Onay süreçleri tamamlandığında, yani kurumsal yapı içinde nihai onay makamı imzaladığında ise elektronik belge hüviyetini kazanır. Elektronik doküman sistem içinde saklanabilir ve bir sonraki resmi yazıya temel oluşturmak için kullanılabilir. Ancak elektronik belge resmi bir nitelik kazandığı için değiştirilemez özelliktedir. Bu belgeyi dokümandan ayıran temel özelliktir.

Belgelerin elektronik ortamda bulundurulması etkin bir e-belge yönetimi için yeterli değildir. Bu bağlamda entelektüel kontrol sağlamak ve etkin yönetimi gerçekleştirmek için elektronik belgeler üretilmeden önce e-belge yönetim sistemine sahip olmak gerekir. Sistem tasarımında belge yönetim sürecinin aşamaları göz önünde bulundurulmalı ve sistem yaklaşımı benimsenmelidir. Sistem tasarlama aşamasında, her bir belgenin üretimi ve tanımlamasıyla ilgili sistematik bir şekilde saklama sürelerinin ve imha tarihlerinin belirlenmesi, güvenli erişim ve koruma, belli belgelere erişimin kısıtlanması ve kimin yetkili olduğunun belirlenmesi gibi konularda kararlar alınmak durumundadır (Shepherd, 1994, s. 42). Bu nitelemelerin birçoğu rutin belge yönetim aktiviteleridir. Elektronik belgelerde belge üretilmeden önce, işin başında yönetim sistemi oluşturulmalı, belge yönetim gereksinimleri, operasyonel iş süreçleri dahil olmak üzere, belgelerin üretilmesi, imhası, saklanması gibi yasal ve arşivsel gereklilikler sistem tasarımında belirlenmeli ve tanımlanmalıdır. Bu bağlamda Elektronik Belge Yönetim Sistemi (EBYS), belgenin yaşam döngüsü çerçevesinde oluşturulmalıdır. Kâğıt belgenin yaşam döngüsü üretilmesinden itibaren başlarken, elektronik belgelerin yaşam döngüsü bilgisayara dayalı bilgi sisteminin tasarım aşamasında başlamalıdır (Kandur, 1999a, s. 40) Bu açıdan, e-belgenin üretimi, saklama süresi, imhası, sınıflandırılması ve sistem içinde akışıyla ilgili kararlar bu aşamada alınmalı ve bu çerçevede sistem oluşturulmalıdır.

E-Belgelerin Arşivlenmesinde Temel Gereklilikler

Elektronik belge yönetiminde arşivleme, büyük oranda paylaşılmış bilginin düzenlenmesi, organize edilmesi ve ulaşılabilirliğinin sağlanmasına dayanmaktadır. Arşivleme sistemi, elektronik belgeleri saklama süreleri boyunca yönetilebilmelidir. Arşivleme sistemi e-belge yönetimi uygulamalarıyla bütünleşik bir yapıda çalışmalıdır. Rhodes (1991, s.16), elektronik belgelerin arşivlenmesinde öncelikle dikkate alınması gereken hususları şöyle sıralamaktadır:

- ◊ *Depolanan materyal:* Ne tür materyalin arşivleneceğinin, yani materyalin hangi formatta olacağının belirlenmesi (veri, grafik, video gibi formatlardan hangilerini içereceği),
- ◊ *Ne kadar süreyle saklanacağı ve ne kadar süreyle kullanım ihtiyacı olacağı*: Elektronik belgenin ne kadar süreyle saklanacağının ve kullanım ihtiyacının ne kadar süreceğinin belirlenmesi (buna göre arşivleme ortamlarının belirlenmesi),
- ◊ *Ne tür kullanımın olacağı:* Kullanıcıların belgeye ne şekilde ulaşacağının tespiti (çevrimiçi ya da tam metin erişim ve iletim gibi),
- ◊ *Belge, yaşam döngüsünün hangi aşamasında dijital olacak:* Elektronik ortamda üretilmeyen belgenin yaşam döngüsünün hangi aşamasında dijital olacağının tespiti,
- ◊ *Uzun dönem saklama kriterleri nelerdir*: Hız, fiyat, kapasite, kolay taşınabilirlik ve süreklilik gibi uzun dönem saklama kriterlerinin belirlenip, buna dönük gerekliliklerin yerine getirilmesi.

Uzun dönem arşivleme açısından, uygun standartların göz önünde bulundurulması, özel olmayan veri formatlarının kullanılması, zorunlu standartlarla uyumlu olarak gerekli dokümantasyon ve üst verinin sağlanması büyük önem taşımaktadır (Hollier, 2001)**.** Uzun dönem arşivleme açısından benimsenmiş tek bir çözüm bulunmamaktadır. Teknolojide yaşanan hızlı değişim buna etken olmakla birlikte bazı ortak yaklaşımlarda bulunmaktadır. Bilgi teknolojilerindeki hızlı değişim, temel olarak arşivlenecek belge formatını ve gelecekte etkin kullanım sağlayacak teknolojik bileşenleri kapsamaktadır (Sproull ve Eisenberg, 2005, s. 21). Teknolojik değişime yönelik planlamanın önemli unsurunu yazılım ve donanım oluşturmaktadır. Yani, arşivleme işlemlerinin de gerçekleştirildiği elektronik belge yönetim sisteminin temelini oluşturan yazılım ve donanım unsurlarının, değişen teknolojiyle uyumunu sağlamak için belli periyotlarla gözden geçirilmesi ve gereken değişikliklerin yapılması sağlanmalıdır.

Arşivlemede, ülkelerin milli arşivleri gibi yetkinliği ve yeterliliği olan belirli bir merkez tarafından belirlenen teknik standartların ve bilgi teknolojileri mimarisinin kullanılması ve benimsenmesi kurumlararası belge paylaşımı açısından önemlidir. Ulusal ve uluslararası standartların ortaya koyduğu teknik özelliklere uygun sistemler, benzer sistemler arasında belgelerin paylaşım ve erişimini sağlayan, birbirleriyle konuşabilen bir yapı oluşturmayı sağlayacaktır.

Kamuya açık olmayan kişisel bilgiler içeren gizlilik derecesi yüksek belgeler, verilen zaman diliminde şifreli formda arşivlenmelidir. Elektronik belgeler, üstlendiği fonksiyon gereği ve ağ üzerinden iletilmesi sırasında güvenlik amacıyla bazen şifrelenirler. E-belgelerin, güvenlikle ilgili yasal ve idari düzenlemelerin öngördüğü çerçevede şifrelenmiş formda muhafaza edilmesi gereklidir. Ancak, şifre çözme anahtarının kaybolması ya da tahrip olması, şifrelenmiş belgelere erişmede bazı kayıplara sebep olabilir. Güvenlikle ilgili böyle bir tespitin yapılması, kurumların elektronik belgeleri

şifrelenmiş formda arşivlemeyi tercih etmemelerine yol açabilir. Bu açıdan şifre çözme anahtarlarının etkin muhafazasının önemi konusunda kurum gereken tedbiri almalıdır.

Elektronik belge saklama gerekliliklerini karşılayan saklama çözümleri, elektronik belgelerin orijinal işlevselliğini gereken düzeyde muhafaza etmelidir. Birçok e-belge, eğer orijinal ortamında sahip olduğu işlevini yerine getiremiyorsa ya da kullanılamıyorsa anlamını ve yararlılığını kaybetmiş demektir (A National Electronic Commerce Coordinating Council E-Sign Policy Workgroup [NECC E-Sign Policy Workgroup] 2001, s. 9). Bu açıdan, e-belgenin güncel teknolojiyle işlenebileceği ya da kullanılabileceği formatta muhafaza edilmesi önemli bir gerekliliktir. Bu gerekliliğin, elektronik belgelerin bileşenleri arasındaki bağlantıları ve bağlamı korunmalıdır. Böylece elektronik belgelerin anlamını açıklamak için, bütün gerekli dosya yapıları ve belge bileşenleri arasındaki ilişkiler belgenin saklama periyodunda muhafaza edilebilecektir. Örneğin, elektronik olarak imzalanmış belgeyi doğrulamak için kullanılan açık anahtarın belgenin saklama periyodunda muhafaza edilmesini gerektirir.

Resmi belgelerin değiştirilemeyeceği anlamına gelen tamlık, bütünlük ve gerçekliğinin sağlanması önemli bir zorunluluktur. Kurumda saklama sürelerinin sona ermesinden sonra devlet arşivlerine gönderilecek, elektronik dosyaların ve dosyaların içerdiği belgelerin bütün bağlamsal bilgileri içermesi ve bu bağlamsal bilginin, belgenin bir parçası ya da sürümü ya da eki olarak arşivlenmesi gereklidir.

Elektronik belgelerin uzun dönem arşivlenmesi açısından zaman içindeki güvenirliliğini ve kullanılabilirliğini sağlamak için taşıma, koruma, üst veri ve XML (Extensible Markup Language - Genişletilebilir İşaretleme Dili) gibi araçlar, yalnızca belgelerin korunmasına yardımcı olmaz; aynı zamanda gerçek değerlerinin fark edilmesinde desteleyici rol oynar. Teknolojik gelişim, yazılım ve donanımın hızla değişmesine neden olmakta ve kurumları zor seçimlerle karşı karşıya getirebilmektedir. Buradaki esas hedef, bilginin güvenirliliğinin ve yararlılığının, verimli ve etkin maliyetle korunmasıdır. Kurum elektronik belgelerle ilgili bir koruma planına sahip olmalı ve bu plan, yazılım ve donanımdaki değişiklikleri, depolama ortamlarındaki kısıtlamaları ve bilginin potansiyel kullanım değeri gibi hususları içermelidir (Minnesota Historical Society, 2004, s. 2).

Elektronik belgelerin yaşam süresi, depolama ortam türüne bağlı olarak değişebilmektedir (Minnesota Historical Society, 2004, s. 4). Belgeler, çeşitli yazılım uygulamaları kullanılarak farklı dosya formatlarında üretilir ve depolanırlar. Zaman içinde, yazılım uygulamalarının yeni sürümleri çıkacak ya da kullanımdan kalkacaktır. Sürümü yükseltilmiş yazılım uygulamaları, daha önceki sürümde üretilmiş belgeleri aynı özellikleriyle okuyamayacak ve saklayamayacaktır. Bu durumda yazılımın koruması bir seçenek olabilir, ancak maliyetle ilgili soruların ötesinde, yazılımın zaman içinde çalışamaz duruma gelmesi ve belgelere erişememe riskiyle karşı karşıya kalınması daha önemli bir sorun olarak değerlendirilmelidir. Arşivlemenin devamlılığı açısından ortak bir çözüm; yazılım ortamının sürekli değişmesiyle birlikte, dosyaların bir sürümden diğer bir sürüme ve bir formattan diğer bir formata dönüştürülmesi olacaktır.

Arşivlemede önemli hususlardan biri de hata sezme ve düzeltme işlemidir. Veri bir uçtan diğer uca aktarılırken bazı bitler bozulabilir, bunun alıcı tarafından sezilmesi büyük önem taşımaktadır (Çölkesen ve Örencik, 2008, s. 45). Öyle ki, veri paketinin içerisinde taşınan veri yükü bitleri bozulabileceği gibi paketin başlık kısmındaki alıcı veya gönderici adres de bozulabilir. Bu durumların sezilmesi ve mümkünse belgenin bütünlüğüne zarar vermeyecek şekilde düzeltilmesi gereklidir. Uzun dönem saklanması gereken belgelerin veri yapılarının bozulma olasılığı bulunmasından dolayı, arşivleme sisteminde hata sezme ve düzeltme teknikleri kullanılmalıdır. Hata sezmek için kullanılan tekniklerden bazıları yalnızca hata olup olmadığını sezerken, bazıları da belirli oranda hata düzeltmesi yapar. Hata sezme ve düzeltmede kullanılan teknikler; boyuna fazlalık sınaması, çevrimli fazlalık sınaması ve doğrusal hata düzelten hamming kodlamasıdır (Çölkesen, 2008, s. 55).

Arşivlenen ya da arşivlenecek veri veya e-belge üzerinde bazı işlemlerin yapılma olasılığı vardır. Bunlar yeni veri ya da e-belge kaydetme, mevcut veriyi güncelleme, mevcut veri ya da e-belgeyi silme ve bu yapı içinde bilgi arama gibi işlemlerdir (Kurnaz, 2008, s. 239). E-belge özelliğini kazanmış bir yapı üzerinde ise yukarıda bahsedilen işlemlerden güncellemenin yapılması söz konusu olmamalıdır. Zira yapılacak değişiklik ya da güncelleme, elektronik belgenin bütünlüğünü ve gerçekliğini ortadan kaldıracaktır. E-belgeyi silme gibi diğer işlemler de elektronik belge yönetim sistemi içinde belirli bir plan, program ve yetki çerçevesinde yapılmalıdır.

Kayıp olmaları ya da zarar görmeleri durumunda kurumun varlığının tehlikeye girmesi ve kişilerin haklarının kaybolması gibi olumsuz sonuçlar doğmasına sebep olan hayati belgelerin korunması elektronik belge yönetiminin belge muhafaza aşamasında önemli bir rol oynamalıdır (Menkus, 1996, s. 4). Zira hayati belgeler, felaket ve acil durumlarda korunması zorunludur. Hayati belgelerin ne olduğu kurumun yapısı ve işlevine göre değişebilmektedir. Mesela; doğum, ölüm ve evlilik belgeleri hayati belgeler kategorisine girmektedir. Bu bağlamda hayati belgelerin korunması, devamlılığı sağlayacak bir planlama çerçevesinde geliştirilmelidir. Hayati belgelerin bir nüshası, kurum dışında kontrol altında güvenli bir ortamda arşivlenebilir (Aydın, 2003, s. 41). Bu anlamda elektronik belge saklama birimleri çevresel şartlara, elektrik ve manyetik alanlara karşı duyarlı olması sebebiyle bilginin güvenli kopyasının harici saklama birimlerine aktarılması gerekmektedir (Kandur, 1999b, s.16). Bu yüzden elektronik belge arşivleme ortamları sürekli kontrol altında olmalı ve okunabilirliğini sağlayıcı önlemler alınmalıdır. Bununla birlikte teknolojik değişimlere paralel olarak yeni ortamlara transferini gerçekleştirmek gerekmektedir.

Arşivleme Mekân Özellikleri

Elektronik belgelerin gerçekliğinin ve bütünlüğünün korunması ve arşivlemenin sağlıklı yürütülebilmesi açısından fiziksel depolama alanlarının oluşturulmasında ya da seçilmesinde bazı hususların göz önünde bulundurulması gereklidir. E-ortamda bulunan belgelerin etkin koruması için öncelikle elektronik belgelerin bulunduğu

donanımların depolamasını sağlayacak uygun fiziksel ortamların belirlenmesi ve düzenlenmesi gerekmektedir. Arşivleme işlemleriyle ilgili politikaların kurum belge yönetim stratejileriyle ilişkisinin açık bir biçimde belirlenmiş olmalıdır.

Elektronik belgelerin arşivlendiği donanım unsurlarının bulunduğu mekânların doğru seçimi etkin arşivleme açısından önemli bir husustur. Bu hususlara paralel olarak elektronik arşivlemenin sağlıklı yapılabilmesi için State of North Dakota'nın ERM (Electronic Records Management) Kılavuzu (1998)'nda çevresel ve ortama ilişkin şu hususlara dikkat çekilmektedir:

- ◊ Depolama araçlarından her türlü yiyecek ve içeceğin uzak tutulması, bu alanlara yiyecek ve içecekle girilmemesi,
- ◊ Depolama disklerinin ve bantlarının dikey pozisyonda ve tozdan uzak bir ortama muhafaza edilmesi,
- ◊ Depolama disklerinin ve bantlarının uygun ısı ve nemde muhafazasının sağlanması (ısı ve nemde ani dalgalanmalar ya da değişimler, bantların bozulmasını hızlandırabilir),
- ◊ Elektronik belgelerin düzenli bir şekilde yedeklerinin alınması (böylece makine ya da insan hatasından oluşabilecek bilgi kayıplarının önlenmesi sağlanacaktır),
- ◊ İkincil kopyaların, orijinal depolama ortamlarından farklı bir ortamda muhafazasının sağlanması,
- ◊ Belli aralıklarla depolama disklerinde ya da bantlarında herhangi bir veri kaybının olup olmadığının test edilmesi, varsa düzeltilmesi ve buna ilişkin kayıpların nereden kaynaklandığının bulunması,
- ◊ Uzun dönem arşivlenen ya da sürekli arşivlenmesi gereken elektronik belgelerin bulunduğu ortamların belirli aralıklarla test edilmesi ve yeni depolama ortamlarına sağlıklı bir şekilde aktarımının sağlanması,
- ◊ Depolama disklerinin ve bantlarının temiz ortamlarda muhafaza edilmesinin sağlanması,
- ◊ Depolama disklerinin ve bantlarının telefon da dâhil olmak üzere güçlü elektrik ve manyetik akımlardan uzak tutulması,
- ◊ Yetkisiz kişilerin elektronik belgelerin bulunduğu bilgisayarlara, bantlara, disklere ya da dokümanlara erişiminin engellenmesi sağlanmalıdır.

Bu bağlamda arşiv mekânlarının düzenlenmesiyle ilgili ulusal ve uluslar arası standartlar da mutlaka göz önünde bulundurulmalıdır. Türkiye'de arşiv mekânlarının özellikleri ile ilgili yayınlanmış olan "TSE 13212: Arşiv Mekânlarının Düzenlenmesi" standardı arşiv mekânlarının düzenlenmesinde dikkate alınmalıdır. Ancak, arşiv mekânında elektronik belgelerin depolandığı fiziksel araçlar bulunacağı için standartta belirtilen bütün hususların uygulanması söz konusu olmayacaktır. Özellikle yapı ve iç donanım özellikleri bölümünde arşiv malzemelerinin korunması ile ilgili kuralların

belirtildiği kısım değerlendirmeye alınmalıdır. Elektronik belgelerin depolandığı fiziksel araçlar, sistem odası diye tabir edilen mekânlarda da muhafaza edilebilmektedir. Bu elektronik belge yoğunluğuna ve bunun için gerekli donanıma göre değişebilmektedir. Yani, ayrı bir elektronik arşiv mekânı da duruma göre oluşturulabilmektedir. Ancak her iki durumda da temel yaklaşım, çevresel tehlikelere, kazalara ve bilinçli saldırılara karşı dayanıklı elektronik arşiv mekânlarının oluşturulmasıdır. Bunun için de, çevresel tehlikeler olarak nitelenebilecek yangın, duman, toz, deprem, patlama, aşırı sıcaklıklar, yıldırım, titreşim, nem ve suya karşı uygun önlemlerin alınması gereklidir. Ayrıca arşiv mekânına yönelik bilinçli olabilecek saldırılara karşı kapı denetimi ve alarm sistemi mutlaka oluşturulmalıdır. Bununla birlikte elektronik belgelerin arşivleneceği fiziksel mekânın ağ yapısının büyük miktarlardaki bilginin, ses, veri ve görüntü şeklinde iletim ve paylaşımını sağlayan; internet, intranet, video konferans, IP telefonu vb. uygulamaları destekleyen yapısal kablolamaya sahip olması gereklidir. Bu elektronik belge yönetim sisteminin hızlı, sağlıklı ve problemsiz çalışması için dikkate alınması gereken hususlardır.

Arşivlemede Teknolojik Unsurlar

Elektronik belgelerin sisteme bağımlı çalışmalarından dolayı üretildiği yazılım ve donanımın korunması ya da gelişen bilgi teknolojileri bağlamında yenilenmesi gerekmektedir. Elektronik belgelerin arşivlenmesinde birinci önemli husus bağlı olduğu donanımdır. Bu yüzden elektronik ortamdaki veriler belli bir zaman sonra kullanılmaz duruma gelebilir. Optik diskler kimyasal bileşimine göre sürekliliği değişebilmektedir (Shepherd, 1994, s. 43). Optik diskler için 10-15 yıllık bir ömür ifade edilse de, çok daha kısa bir sürede bozulmalar olmaktadır. Diğer yandan sabit diskler verileri iletemez duruma gelebilir. Teknolojik bağlamda makinelerin çok hızlı bir şekilde değiştiği düşünülürse, geleceğin arşivlerinde e-belgelerin erişilebilirliğini sağlamak için bir makine müzesi oluşturulmasına ihtiyaç duyulacaktır. Bunun mümkün olamayacağı düşünülürse, gelişen bilgi teknolojilerine paralel olarak oluşturulan elektronik belge yönetim sisteminin donanımının sürekli güncellenmesi gerekmektedir. İkinci önemli husus yazılımdır. Elektronik verilerin işlenmesi, erişilmesi ve okunması gibi fonksiyonların yazılıma göre değişiklik göstermesi nedeniyle yazılımlardaki değişimler takip edilerek gelişmelere paralel olarak eski elektronik belgelerin yeni yazılımlarla uyumlu bir şekilde çalışması sağlanmalıdır.

Yukarda ifade edildiği gibi yazılım ve donanımla ilgili teknolojik bileşenler, elektronik ortamda üretilen ve depolanan bilginin okunması ve işlenmesi için gerekli teknolojik unsurlardır. E-belge, ayrıntılı bir bilgi sisteminin ve/veya kodlarının ne ifade ettiğini çözmek için bilgi teknolojilerine ihtiyaç duymaktadır. Teknolojik ürünler anlamında tek bir markaya bağımlılığı önlemek için, farklı markalarda teknolojik bileşenler alınmalı ve sistemin farklı marka ürünleri üzerinde de sağlıklı çalışması için gerekli çalışmalar yapılmalıdır (Sproull ve Eisenberg, 2005, s. 23). Bu bağlamda bilgi teknolojileri; sistemin tasarımı ve analizi, verinin dönüşümü, bilgisayar programlama, e-belge depolama ve iletim, ses, video ve veri iletişimleri, sistem kontrolleri, simülasyon,

insan ve makine arasındaki etkileşimin tamamı dahil olmak üzere bütün bilgisayara uyarlanmış ve otomasyonu yapılmış işlenmiş bilginin teknolojik unsurlarının tamamı anlamına gelmektedir (CalRIM, 2002, s. 7). Bilgi teknolojilerinin yönetimi, planlama, bütçeleme, organize etme, yönetme, eğitim, değerlendirme ve bilgi teknolojileri uygulamalarıyla ilişkili diğer kontrol aktivitelerini yürütmektir. Dolayısıyla bu yönetim süreci bilgiyi toplamak, kaydetmek, işlemek, depolamak, erişmek, göstermek ve iletmek için tasarlanmış, oluşturulmuş yönetimsel prosedürler, donanım ve yazılımları içerir. Bu süreç, aynı zamanda ilgili personel, danışman ve uygulayıcıları da içine alır. Bilgi teknolojileri bağlamında değerlendirildiğinde, e-belgelerin arşivlenmesinde, fiziksel depolama ortamları ve buna bağlı yazılım ve donanım ömürleri nedeniyle bazı sorunlarla karşı karşıya kalınmaktadır (Aydın, 2010, s. 68). Aslında, bilgi hangi ortamda bulunursa bulunsun, hepsinin belirli ve sınırlı bir yaşam süresi bulunmaktadır. Bir bilginin değeri, uzun bir depolama süresinden sonra okunabilmesine ve erişilebilir olabilmesine bağlıdır (Stamatiadis, 2005, s. 56). Elektronik arşivleme, karmaşık ve çok yönlü teknolojik unsurları içermesi nedeniyle, arşivleme açısından diğer ortamlar için söylenebilecek zaman sınırının dışında tutulmalıdır.

Donanım teknolojisindeki gelişmeler yazılımların daha çok işlevinin olmasını gerektirirken, yazılım sektöründeki gelişmeler ise daha iyi bir donanımı gerektirir. Kısaca hem donanım hem de yazılım sektörü sürekli birbirlerinin sınırlarını zorlamaktadır. Yazılımlar, elektronik belge yönetimi açısından en önemli faktördür. Mevcut sistemler, genellikle ilgili firmaya özgüdür ve birçok firma kendilerince kapsamlı çözümler sunmaya çalışmaktadır. Her bir ürünün, kullanıcı ara yüzü, veri yapıları, işlem akışı, kuruma özgü bir ürün olarak kapalı bir şekilde muhafaza edilmektedir (Oatway, 2004, s. 4). Bu faktörler, kurumsal yapıya özgü yazılım çözümlerinin geliştirilmesi ve devamlılığının sağlanmasını zorunlu kılmakta, diğer taraftan sistemin sürdürülebilirliği için uluslar arası standartların dikkate alınmasını kaçınılmaz kılmaktadır.

Genel nitelikli paket yazılımlar gerek mali açıdan ve gerekse güvenlik açısından elektronik belgelerin yönetilmesinde önemli riskler taşımaktadır. Firmaya bağımlı bir çözümün kullanılması, uzun vadede ciddi sorunlara sebep olabilmektedir. Alınan paket yazılımların uygulanmasında ve güncellenmesinde ek maliyetlerin oluşması kaçınılmazdır. Kurumsal olarak ortaya konulacak yazılım çözümleri tercih edilmeli, ancak burada önemli sorun sürdürülebilirlik olacaktır. Bu açıdan en önemli nokta, kurumlarda yeterli uzman personelin bulunamaması nedeniyle teknolojik değişimlere paralel olarak yazılımlarda gerekli güncelleme işlemlerinin yapılamamasıdır. Günümüz dinamik teknolojik ortamında kurumların bunu başarmaları oldukça zor gözükmektedir. Ayrıca birlikte işlerlik açısından kurumsal yazılım eğilimleriyle ilgili bir değerlendirmenin de yapılması gereklidir. Çözüm ise kurum yapısına ve uluslararası standartlara uygun çözümler geliştirmek için sisteme ihtiyaç duyan kurum ile bu konuda çözüm sunan firmaların birlikte çalışarak uluslar arası standartlara uygun kurumun ihtiyaçlarını karşılayacak sistemlerin geliştirilerek kullanılmasıdır.

Uygun Arşivleme Ortamı Çözümlerinin Seçimi

Günümüzde e-belge depolanması için var olan birçok ürün; daha hızlı geri iletim gerektiren aktif dosyaların ve geri iletimi daha yavaş olan arşivsel dosyaların her ikisinin de karakteristiğini kapsamaktadır (Shamir, 1996, s. 12). Elektronik belgelerin depolama ortamlarını seçerken ya da bir depolama ortamından başka bir depolama ortamına aktarırken göz önünde bulundurulması gereken faktörlerle ilgili olarak State of North Dakota'nın ERM Kılavuzu (1998)'nda şu hususlara dikkat çekilmektedir:

- ◊ Saklama planlarında belirlenmiş, saklanması onaylanmış belgelerin hacmi ve türü,
- ◊ Elektronik belgeleri elde bulundurmak için gerekli bakım hususları,
- ◊ Elektronik belgelere erişim ve depolama maliyeti,
- ◊ Elektronik belgelerin geri iletimi için erişim zamanı,
- ◊ Elektronik belge yönetim sistemine bağlı olarak zaman içinde elektronik belgelere erişebilirlik,
- ◊ Depolama ortamının taşınabilirliği (seçilen depolama ortamının birden fazla firma tarafından önerilecek araçlarla yürütülmesi ya da aynı ürünler arasında taşınabilirliği),
- ◊ Depolama ortamlarının, mevcut standartlara uygunluğudur.

Uzun dönem arşivleme açısından manyetik bant türü en uygun depolama seçeneğini sunmaktadır. Ömürleri teoride belirtilen diğer depolama seçeneklerine göre daha fazladır. Ancak erişim açısından çok yavaş oldukları önemli bir gerçektir. Uygun nem ve sıcaklık ortamında saklanılırsa 10 yıllık bir ömür biçilmektedir. Bu açıdan pasif aşamada bulunan bir elektronik belge için en uygun depolama ortamıdır. Genel bir yaklaşımla, aktif elektronik belgeler için sabit disk, yarı pasif elektronik belgeler için ise harici depolama çözümler önerilebilmektedir. VTL (Virtual Tape Library) teknolojisi etkin bir arşivleme yapılması açısından önemli bir çözüm sunmaktadır. Zira bu teknoloji, verinin nerede, ne kadar süre kalacağını ve erişileceğini noktasında depolama seçenekleri arasında etkileşimli bir yapı sunar ve sabit diskte saklanan ve belli bir süre sonra arşive aktarılması gereken belgelerin sağlıklı bir şekilde manyetik bantlara aktarılmasını sağlar. Tabi ki buna ilişkin tanımlamaların ve göndermelerin sistem içinde yapılması gerekmektedir (Aydın, 2010, s. 75).

Elektronik belgelerin uzun dönem arşivlemesi açısından depolama ortamları kritik bir öneme sahiptir. Bu açıdan seçim yaparken elektronik belge yönetim sistemimin teknoloji bağlamında bütün unsurları dikkate alınmalı ve bu çerçevede bir planlama yapılmalıdır. Bu çerçevede Dollar (1999, s.40) tarafından ortaya konulan; "depolama ortamları seçerken göz önünde bulundurulması gereken kriterler" mutlaka dikkate alınmalıdır. Bu kriterler aşağıda değerlendirilmiştir:

- *Büyük Çapta Depolama Kapasitesi:* Büyük çapta depolama araçları fiziksel olarak küçülme eğilimindedir. Bir başka deyişle daha küçük çapta bir fiziksel depolama aracı daha büyük çapta elektronik belgeleri saklayabilmektedir. Fiziksel olarak fazla yer kaplamayan depolama araçlarının kullanılması bu kapsamda önemlidir. Uzun dönem arşivleme açısından, elektronik belge üretim yoğunluğu da göz önünde bulundurularak yüksek depolama kapasitesine sahip araçlar seçilmelidir.
- *Yüksek Veri Transfer Hızı:* Bir depolama aracının veri transfer hızı; bir megabaytlık bir verinin transferi için gerekli zaman süreci olarak tanımlanmaktadır. Yüksek hızda bir veri transferi yapmak, okumak için ve verinin bir depolama aracından diğer bir depolama aracına taşınmasında daha az zaman kullanılması demektedir. Genellikle yüksek maliyetli bir disk, yüksek hızda bir veri transferi demektedir. Bu açıdan seçim yaparken yüksek hızda bir depolama aracı seçilmeli, aksi takdirde uzun vadede ciddi mali ve yasal kayıplar oluşabilir.
- *Depolama Aracının Ömrü:* Dijital depolama aracının ömrünün disk yüzeyinde okumadaki ortalama ömrün üzerinde olduğu göz önünde bulundurulmalıdır. Ayrıca, disk yüzeyinde okumadaki ortalama ömür, elektronik belgeyi işlemek ve iletmek için kullanılan yazılım uygulamasının ortalama ömründen daha uzundur. Bu açıdan elektronik belgenin kullanılabilirliğini uzatmanın tek yolu, yeni disk ve yazılımlarla desteklenmiş yeni depolama ortamlarına periyodik olarak transferinin yapılmasıdır.
- *Uygunluk:* Bu kriter, depolama teknolojisinin esas amacı ile uzun dönem erişim gereklilikleri arasındaki uygunluğu ifade etmektedir. Bütün dijital depolama araçları uzun dönem erişim açısından sağlıklı çalışmaz. Bu açıdan uzun dönem erişim açısından sunulan özel çözümler tercih edilmelidir.

Büyük çapta depolama açısından sunucu bilgisayarlar ve buna bağlı sunucu diskler büyük önem taşımaktadır. Bilişim teknolojilerinde sunucu, belirli bir servisi sunmak için üretilmiş yazılım ya da donanımı ifade eder. Sunucu bilgisayarlar, aynı anda birçok kullanıcıya hizmet vermek zorunda oldukları için donanımsal olarak kullanıcı bilgisayarlarından çok daha güçlü bir yapıdadır. Sunucu sistemler, aynı anda birçok bilgisayara hizmet etmek zorunda oldukları için kullanıcı isteklerine yeterli hızlarda cevap vermek zor olabilir. Özellikle elektronik belge yönetim sisteminin çalıştığı sunucular kullanıcı isteklerini cevaplarken disklerini yoğun olarak kullanmak zorundadırlar. Disklerdeki veriyi çok hızlı okuyup, yazılacak veriyi çok hızlı yazmak zorundadırlar. Bu yüzden sunucu sistemlerde yüksek performanslı hızlı diskler kullanılır. Bunu sağlamak için, yani veri erişim hızını artırmak için RAID (Redundant Array of Independent Disk) çözümleri de kullanılmaktadır. RAID, birden fazla diski tek bir diskmiş gibi kullanarak, hızı ve hata toleransını arttırmak için kullanılan teknolojidir (İmamoğlu, 2008, s. 34). RAID çözümler, sunucu bilgisayarlara takılan disklerin tek disk gibi hareket etmesiyle hız artışı sağlar ve olası disk bozulmaları durumunda veri kayıplarını önler.

Depolama ortamının seçimiyle birlikte, depolama bağlamında kullanılan sistem yaklaşımının seçimi de önem taşımaktadır. Temel olarak üç değişik sistem seçeneği bulunmaktadır. Bunlar; DAS (Direct Attached Storage), NAS (Network Attached Storage) ve SAN (Storage Area Network)'dır (Saraçoğlu, 2006, s. 1). *DAS*, temel olarak bir veya daha fazla disk sürücüsü doğrudan bir sunucu bilgisayara bağlı olarak tanımlanabilir. *NAS* bu sistem dosya-tabanlı olup kaynaklar doğrudan yerel ağa bağlı çalışır. *SAN sistemi* ise doğrudan sunuculara bağlanarak ağ trafiğini etkilemeden veri depolama kapasitesi sunmaktadır. Kurumların depolama mimarisinde yapacakları seçimler sistemin bütününü etkileyebilir. Eğer yeterli yönetimsel araçlar mevcut değilse, yüksek performans gerektiren uygulamalarda bazı sunuculara çok yüklenirken diğerleri boş kalabilmektedir. Yukarıda tanımlanan depolama sistemleri arasında SAN; yüklü sunucular arasında dengeleme görevini yerine getirerek maliyetin düşmesine de katkıda bulunur. Ayrıca sistem gereksiz dosya kopyalarını veya veri bütünlüğünü bozacak uygulamaları ortadan kaldırır. Ancak yüksek maliyet gerektirmesi sistemi en önemli dezavantajıdır (Saraçoğlu, 2006, s. 1). Bu tür sistemler seçilirken kurumların esneklik, kolaylık ve toplam sahip olma maliyetini düşünmeleri gerekmektedir. Depolama sistemleri donanımın giderek daha da önem kazanan bir parçasıdır. Bu bağlamda yüksek güvenirlilik, ölçeklenebilirlik, performans ve çoklu platform desteği için tasarlanan depolama çözümleri tercih edilmelidir.

Arşivlemede Uygun Dijital Koruma Tekniklerinin Kullanılması

Elektronik ortamda depolamada her gün yeni teknolojinin ortaya çıkmasına rağmen, elektronik ortamda depolanmış önemli miktarda bilgi bozulmakta ve kaybolmaktadır. Dijitalleştirme çalışmalarındaki sorunların ve başarısızlıkların farkına varılırken, analog bilgiden farklı olarak dijital bilgilerin sonsuza dek kalacağını düşünme eğilimi bulunabilmektedir (Aydın, 2010, s. 82). Buna rağmen çok büyük miktardaki dijital bilgi, içinde yer aldıkları diskin bozulmasından dolayı da kaybolabilmektedir. Günümüzde 20 yıl önce popüler olan 8 inch'lik bilgisayar diskinden bir şey okumak, hemen hemen imkânsızdır. Dolayısıyla uzun bir zaman önce arşivlenmiş büyük miktardaki bilgiler kaybolma ve kullanılamama riskiyle karşı karşıya kalabilmektedir (Sitts, 2000, s. 164). Daha fazla kaybı önlemek için dijital bilginin yaşam süresiyle ilgili konunun ciddi bir şekilde ele alınıp çözülmesi gerekmektedir.

Yazılım ve donanımdaki bu hızlı değişim uzun dönem arşivleme açısından ciddi bir soruna sebep olmaktadır. Bu durum dosya formatları, depolama ortamları, yazılım ve donanım sistemleriyle ilgili problemleri içermektedir (Sitts, 2000, s. 166). Bugünün kelime işlemcisi daha eski bir sürümle üretilmiş dosyaları okuyamamaktadır Dolayısıyla oluşturulan elektronik belgelerin yıllar sonra okunabilir ve kullanılabilir olmasında ciddi sorunların olacağı önemli bir gerçektir. Bu durum, bir formattan diğer bir formata dönüştürmenin çalışmalarını nasıl etkileyebileceğini anlamaları için de önemli bir göstergedir. Bununla birlikte, dijital koruma tekniklerinden taşıma ve yazılım eskimesi konuları henüz tam anlamıyla çözülmemiş sorunlardır.

Elektronik belgelerin zaman içinde kullanılabilir kalmasını sağlamak için uygulanabilir dijital koruma tekniklerini, bütüncül bir yaklaşımla değerlendirmek gerekmektedir. Dijital koruma yaklaşımlarından bir tanesi, belgeleri destelemek için gerekli bütün dokümantasyon, yazılım ve donanımın muhafaza edilmesidir. Gerçekçi olmayan bu bakış açısı, bilgisayar müzesi yaklaşımı olarak da bilinmektedir. Elektronik belgelerin korunmasına yönelik en yaygın yaklaşım, taşıma ve dönüştürme tekniklerinin birleştirilmesiyle ortaya çıkan tekniktir (Minnesota Historical Society, 2004, s. 5). Taşıma, dosyaların değerlerini korumak amacıyla, dosyaların yeni ortama ya da bilgisayar platformuna nakledilmesidir. Dönüştürme, dosyaların bir formattan diğer bir formata değiştirilmesini gerektirir ve Microsoft Word gibi özel bir formattan düz metin ya da XML gibi özel olmayan formata taşınması şeklinde de olabilir. Süreçte veri kaybından korunmak için, ne tür değişiklikler olacağını ve bu değişikliklerin kabul edilebilir olup olmadığını belirlemeye yönelik başlangıç testleri ve analizleri mutlaka yapılmalıdır. Taşıma ve/veya dönüştürme gibi işlemlerde üst veriye erişilebilirliğin korunmasına özel dikkat gösterilmesi gereklidir. Uygun bir şekilde planlandığı ve yürütüldüğü zaman, taşıma ve dönüştürme yaklaşımı muhtemelen günümüzde geçerli olan en kolay ve maliyet etkin koruma metodunu ifade etmektedir.

Diğeri, elektronik belgelerin korunmasında öykünüm (benzemeye çalışma) yaklaşımı elektronik belgelerin muhafazasını tam olarak karşılamamaktadır. Ayrıca bir strateji olarak da işlerliği bulunmamaktadır. Eskimiş yazılım ve donanım yapılarından uygun ortamlara aktarılmamış elektronik belgelerin onlarla birlikte yok olması muhtemeldir. Sonuç olarak, öykünüm çözümü çalıştırılsa bile elektronik belgelerin delilsel niteliği korunamayacaktır. Elektronik belgelerin delil olarak korunmasının gerekli olduğu durumlar için ciddi sorunlar yaşanabilir. Dijital bilginin gelecekte okunabilir olmasını sağlamak için uzun dönem stratejiler üzerinde dikkatle durulmalıdır (Bearman, 1999, s. 2). Maalesef gelecekte okunabilir olmak tek başına elektronik belgelerin korunması için yeterli değildir. Elektronik belgenin delil vasfını zaman içinde kaybetmesi uzun vadede ciddi sorunlar yaratacaktır.

Kurumlar, e-ortamlarda uzun dönem saklamak için depolanan belgeleri korumada kullanılacak taşıma stratejilerini geliştirmelidir. Belgenin ve taşıma yönteminin doğruluğu sağlanmak zorundadır (Public Records Office of Victoria, 2000, s. 4). Taşıma, belge ya da belirli dosya türleri için bir depo olarak kullanılan araçların eskimesinden dolayı, korunmaya yönelik stratejilerdir. Ortam türü eskiyebilir ve geçerli yazılım bununla çalışmayabilir. Dosyaların geçerli biçime aktarımını ve içeriğinin korunmasını temin edecek taşıma programının uygulamaya konmasına ihtiyaç vardır (CalRIM, 2002, s. 28). Her dönüştürmede hata ya da özelliklerin kaybolması riski bulunur. Bu durum, elektronik belgenin bütünlüğünü önemli ölçüde tehlikeye sokar. Değiş-tokuşun (dengelemenin) dikkatli bir şekilde değerlendirilmesi gerekmektedir.

Dijital arkeoloji ve teknolojik koruma yöntemlerinin uzun dönem arşivleme açısından kullanabilirliği söz konusu değildir. Zira dijital arkeoloji yönteminin uzun dönem arşivlenmiş ortamlarda başarı oranı oldukça düşüktür. Bu yöntem, daha çok

güncel uygulamalarda ve donanım çevrelerinde başarılı olmaktadır. Teknolojik koruma ise, gerek felaketten kurtarma stratejilerine uygun bir yöntem olmaması, gerekse bozulan donanım ve yazılım unsurunun yerine uzun vadede aynısını koyma imkânı olmaması dolayısıyla hiçbir şekilde kullanılabilir değildir. Ayrıca bakım ve eski donanım bulma maliyeti oldukça yüksektir. Bu açıdan uzun dönem arşivleme açısından bu yöntemlerin kullanılabilirliği oldukça düşüktür.

Arşivlemede Elektronik Belgelerin Gerçekliğinin ve Bütünlüğünün Korunması

Kurumsal yapı içinde elektronik belgenin gerçekliği, bütünlüğü, güvenliği ve erişilebilirliğinin sağlanması gereklidir. Elektronik belgeler idari, yasal ve arşivsel gereksinimler için kullanılabilir, geri iletilebilir, ulaşılabilir olmak zorundadır.

Elektronik belgeler doğaları gereği kolayca üretilebilir, düzeltilebilir ve imha edilebilirler (Dickman, 2002, s. 54). Bununla birlikte eğer kurumlar elektronik belgeleri yasal süreçte ya da denetim aşamasında delil olarak kullanacaksa, elektronik belgenin bütünlüğünün korunması bağlamında gerekli olan iki unsuru sağlamalıdır. Bunlar; güvenirlilik ve gerçekliktir. Yani elektronik belgelerin, kurumsal ve yasal ihtiyaçlar çerçevesinde kullanılabilmesi için güvenilir ve gerçek olmaları gerekmektedir. Bu iki unsur bölünmez bir bütünün iki parçasıdır. Güvenirlilik belgenin kapsadığı ya da sahip olduğu gerçekliği devam ettirmesidir. Yani bir elektronik belgenin üretiminden itibaren aynı içeriği ve değeri muhafaza etmesidir. Güvenirlilik iki faktöre bağlıdır (Duranti, 2001, s. 43): Bunlardan birincisi, belge formunun tamam olma derecesi, yani belgenin bir bütün olarak belge şeklini taşımasıdır. Örneğin bir imza ya da terim eksikliği önemlidir. İkincisi ise; belge üretim aşamasında gösterilen kontrolün derecesidir. Bu iki faktörün yerine getirilme durumu belgenin güvenirlilik derecesini belirler. Gerçeklik ise belge yapısının aynı şekilde korunması ve tahrip edilmemesidir. Yani belgenin oluşturulduğu andaki içeriğinin korunmasıdır.

Belgelerinin bütünlüğü ve aslına uygunluğu elektronik belge yönetiminin ilgilendiği önemli konulardan birisidir. Gerçek belge, usulüne uygun olarak yetkili kişi ya da kuruluş tarafından oluşturulmuş belgedir. Bir belgenin bütünlüğü, o belge üzerinde herhangi bir değişiklik yapılmaksızın korunması demektir. Kâğıt belgelerin aslına uygunluğunu ve bütünlüğünü sağlamak için, belgeyi üreten ve iletenden belge kullanıcısına kadar saklama zinciri oluşturulmasını sağlayan teknikler kullanılmaktadır (Sproull ve Eisenberg, 2005, s. 59). Aynı teknikler elektronik belgelerde de uygulansa bile, elektronik belgelerin yapısı aslına uygunluğu ve bütünlüğü sağlamak için ek tekniklerin kullanılmasını zorunlu hale getirmektedir. Dijital teknikler kâğıt belgeler için mevcut tekniklerden daha güçlü teminat vermeye elverişlidir. Ayrıca, elektronik belgeler tahrifata ve onaysız değişikliklere karşı daha hassastırlar. Elektronik belgelere yetkisiz erişimin gerçekleşmesi durumunda; bütünüyle kopyalanabilir, silebilir, değiştirebilir ya da belgeler üzerinde denetim ile belirlenebilmesi zor değişiklikler yapılabilir. Ancak bilgi

teknolojilerinde artan deneyim, elektronik belgelerde yapılan değişiklikleri belirleme konusunda farkındalık oluşturmaktadır.

Elektronik belgeyi göndereni doğrulamak ve belgenin değiştirilmediğine emin olmak gereklidir. Her bir belgenin bütünlüğünü belirlemek ve göndericiyi doğrulamak için bir takım politikalar ve prosedürler belirlenmesi bir zorunluluktur. Bu politikalar ve prosedürler, kurumlar tarafından alınan farklı türdeki elektronik belgelerin bütünlüğünü ve gerçekliğini tespit etmede önemlidir. Bu politikalar, belgelerin uygun olmayan bir şekilde açıklanması ve değiştirilmesinden ortaya çıkacak maliyet ve potansiyel riskleri de içine alacak şekilde hazırlanmalıdır. Kurumlar genel devlet alt yapısına uygun internet ve e-posta politikaları geliştirmeli ve uygulamalıdır (Aydın, 2010, s.101).

Arşivlemede Gerçeklik ve Bütünlüğe Yönelik Tehditler

Elektronik belgelerin bütünlüğünü tehlikeye sokacak hatalar, kayıtlar doğrulandıktan sonra ya da iletildikten sonra da arşive sızabilir. Bu donanımın aksamaya uğramasından, işlemsel hatalardan, yazılım arızasından, kasıtlı saldırılardan ya da bunlara benzer başka nedenlerden kaynaklanabilir. Hatalar arşivdeki her bir dosyanın başka bir kopyası ile kıyaslanması, dosyanın okunması, mevcut sağlamasının (hash) hesaplanması ve bu sağlamanın o dosya için korunan kopyası ile karşılaştırılması sonucu tespit edilebilir. Bu kıyaslamaları yapacak sürekli bir sürecin olması gereklidir. Böylece hataların fark edilmesi sağlanmış olur (Sproull ve Eisenberg, 2005, s. 65). Bütünlük kontrolü başarısızlığa uğradığında, hem onarım hem de araştırma gerekli olur. İlk olarak, geçersiz veri, arşivde tasarlanan 'artık' mekanizması tarafından sağlanan yansımalardan ya da yedek kopyalarından geri alınır. İkinci olarak, hatanın nedeninin araştırılması gerekmektedir. Hatalı bütünlüğün bütün durumlarını kesin bir şekilde araştırmadaki başarısızlık, arşivi koruma konusunda da başarısızlığa neden olacaktır (Sproull ve Eisenberg, 2005, s.66).

Belge yeni bir ortama ya da formata aktarıldığında, yapılan işlem belgenin bütünlüğünde bir kısım değişimlere sebep olabilir. Analog ortamdan dijital ortama aktarımda yaşanan sorunların, tamamıyla dijital ortamda yapılan benzer işlemlerde yaşanmayacağı yanılgısına düşmemek gereklidir. Dijital ortamda yapılacak işlemlerde dosya formatı ve boyutu aynı gözükse de belgenin bütünlüğünü etkileyecek bir takım sorunların olması muhtemeldir (Sitts, 2000, s.171). Uygulamada, belgelerini aynı kelime işlemcinin bir önceki sürümü kullanılarak başarılı bir şekilde kopyalama yapılabilmektedir. Ancak bu işlemde, sayfa ortalama, alt çizgi, font değişiklikleri gibi formatlar ve çift tırnak gibi özelliklerini kaybı söz konusu olmaktadır. Bu emulasyon uygulamaları için doğru olabilir. Çünkü bu çalışmaların yaratıcıları uygulamanın hangi kısmını dönüştüreceğinin seçilmesini zorunlu kılmakta ve tek tek her parçayı benzetmeyi ya da dönüştürmeyi öngörmemektedir. Bu husus belgenin bütünlüğünü tehlikeye sokar. Bu çerçevede, yazılım ve donanım güvenirliliği dahil olmak üzere sistem performansının test edilmesi gereklidir. Yazılım ve donanımın güvenirliliği, elektronik

belgelerin gerçekliğini ve bütünlüğünü etkiler. Cihazların bozulması, elektronik belgelerin içeriğini değiştirebilir. Eğer elektronik belge üretmek ve depolamak için kullanılan veri işleme araçları ve yazılımları güvenilir değilse, belgelerin bütünlüğü sağlanamayabilir (Aydın, 2010, s. 102).

Elektronik belgenin gerçekliği ve güvenirliliği açısından fiziksel ve çevresel güvenlik kontrollerinin sürdürülmesi gereklidir. Fiziksel ve çevresel tehditlerin, özellikle kırılgan çevrimdışı ortamlarda depolanan elektronik belgeler üzerinde etkileri vardır. Kurumsal güvenlik programı, büro mekânı, veri merkezi ya da donanım içeren odalar, sistem elektrik tesisatı, destek hizmetleri, yedekleme ortamları ve diğer sistem unsurlarında fiziksel erişim ve uygun çevresel şartları göstermelidir. Güvenlik programının aynı zamanda, yangın, kullanım hatası, yapısal göçme ve tesisatla ilgili bozulmalar gibi tehditleri de göstermesi gereklidir.

Yazılım uygulamalarının değişik fonksiyonları, bilgisayarda üretilen belgelerin bütünlüğünü ve durumunu etkileyebilir. Elektronik belgelerin uygun araçlarda kaydedilmesi gerekmektedir, aksi halde bilgisayar kapatıldığında ya da uygulamadan çıkıldığında belgeyi kaybetme riskiyle karşı karşıya kalınabilir (CalRIM, 2002, s. 18). Elektronik belgenin kopyalanması sürecinin, bütünlüğünün bozulmasında doğrudan etkisi olabilmektedir. Bu etki, kopyalama süreci tesadüfen yanlış yönde oluşursa ortaya çıkabilir. Eğer kullanıcı, taşınabilir diskte yedek kopya oluşturursa ve yedek kopyayı daha sonra sabit diske aktarırsa, dosyanın önceki sürümü mevcut dosyayla yer değiştirebilir. Bu tip durumlar da belgenin bütünlüğünü tehlikeye sokar.

Gerçeklik ve Bütünlüğü Korumaya Yönelik Tedbirler

Dijital denetim araçları elektronik belgelerin bütünlüğünün kontrolü ve sağlanması açısından önemlidir. Belgelerin dijital denetimi temel olarak, bütünlük kontrolünü sağlayan ve belgelerin arşive gönderilmesini ve arşivden iletilmesini güvence altına alan kriptografik tekniklerin kullanılmasına dayanmaktadır (Sproull ve Eisenberg, 2005, s.60). Kriptografik teknikler, aslına uygunluk ve bütünlük için temel araçlar sağlar. Bunlar kriptografik algoritmalara dayanır ve bu algoritmalar sahteciliği sayısal olarak imkânsız hale getirir. Ayrıca bütünlüğü kontrole yönelikte teknikler kullanılmaktadır. Sağlama (hash) özümlemesini hesaplama tekniği bu çerçevede kullanılan bir yöntemdir. Bu teknikle, güvenli sağlama algoritması kaydı oluşturan dijital bitlerden kompakt sağlama özümlemesi hesaplanır (Sproull ve Eisenberg, 2005, s. 60). Yaygın olarak kullanımda olan birçok algoritma vardır. Standart güvenli sağlama algoritması bunlardan biridir. Belge iletimi sırasında, herhangi bir değişiklik olursa, bu farklık bir mesaj özümsemesiyle sonuçlanacaktır. Belge, yönetim sistemine ilk girdiği zaman hesaplanan sağlama özümsemesi, iletimden sonra oluşan değerle kıyaslanarak belgenin bütünlüğü doğrulanır. Belgenin oluşturulduğunda hesaplanan sağlama özümsemesi değişikliğin olup olmadığını tespitte kanıt niteliğindedir. Ayrıca, bu tekniğe benzer olarak, gönderilen ve alınan belgenin aynı olduğundan emin olmak için kullanılan

çeşitli kriptografik teknikler vardır. Bir elektronik belge, belgeyi kullanan herhangi bir kişi tarafından doğrulanan dijital imza oluşturarak aslına uygun hale getirilebilir. Belge herhangi bir şekilde değiştirilirse, imza kontrolü başarısız olacaktır. Elektronik belgenin orijinalliğini doğrulamak için kullanıcı girdiyi aslına uygun hale getirme etiketini ve doğrulanmış aslını ortak anahtar kabul ederek, ikinci tuşlamalı kriptografik iletim içeren algoritma gerçekleştirir (Sproull ve Eisenberg, 2005, s. 61). Çıktı iki terimli bir değerdir, orijinalliği doğrulanmıştır ya da orijinalliği doğrulanmamıştır. Orijinalliği doğrulanmıştır terimi objenin özel anahtara sahip olan biri tarafından oluşturulduğu anlamına gelir. Kişinin, özel anahtarın varsayılan sahibinin o anahtarı koruduğuna güvenmesi gerekir. Böylece, o kişinin aslına uygunluk etiketini oluşturan kişi olduğundan emin olunur.

Belgelerin bütünlüğü açısından değerlendirildiğinde; belgelerin, üretimi, ortamı ve yönetimi belli yasal emirlere, iş ihtiyaçlarına ve geçmişteki deneyimlere bağlıdır. E-belgenin bütünlüğünün korunması değerlendirildiğinde risk yönetimi kavramı faydalı olabilmektedir. Risk yönetimi, risk analizine bağlı olarak potansiyel faydaya bağlı riskleri, bu riskleri belirlemek için seçenekli ölçümleri düşünmeyi ve bu analize bağlı olarak riskleri en iyi belirleyen ölçümleri uygulamayı gerektirir. Elektronik belgelerin bütünlüğünü tehlikeye sokacak risklerin tespit edilmesi ve buna ilişkin tedbirlerin alınması büyük önem taşımaktadır (Aydın, 2010, s.104).

Elektronik belgelerin üretilmesinde, alınmasında ve muhafaza edilmesinde kullanılan süreçlerin ve usullerin doğruluğu ve güvenirliliği, e-belgelerin gerçekliğini, bütünlüğünü ve güvenliğini göstermede kritik faktörlerdir. Bu faktörler, e-belgelerin üretilmesi ve muhafaza edilmesi için kullanılan belirli teknolojilerden, formatı ya da ortamından çok daha önemlidir. Kurumlar, yasal ya da diğer işlemlerde elektronik belgelerinin kabul edilmesini bekliyorlarsa, bu süreçleri ve usulleri tespit etmeli, belirtmeli ve belgelendirmelidir (NECCC E-sign Policy Workgroup, 2001, s. 5). Bu bağlamda eğitim de kritik bir öneme sahiptir. Eğitim, özellikle belgelerin üretimi ve muhafazasında kullanılan sistemin personel tarafından yeterli düzeyde devamlılığının sağlanması açısından önemlidir. Ayrıca, e-belgelere erişim ve kullanım için ihtiyaç duyulan teknolojik platform ve depolanması için kullanılan ortamın kırılganlığına bağlı olarak ortaya çıkan belli yönetim konularından kurumsal yetkililerin haberdar olmasının sağlanması da önemlidir. Kurumsal yetkililerin, elektronik belgelerin yönetimi konusundaki sorumluluklarının farkında da olmaları gerekir. Ayrıca e-belgelerin yasal saklama sürelerinde erişilebilir ve yasal işlemlerde kabul edilebilir olmalarını sağlamları konusundaki bu sorumluluklar özenle yerine getirilmelidir (Aydın, 2010, s.105).

E-belgeler erişilebilirliklerini desteklemek için uygun şekilde muhafaza edildiğinden emin olunması gerekmektedir. Elektronik belgelerin alınmasında ve iletilmesinde, belgelerin yetkisiz kişiler tarafından bozulmasını ve tahrif edilmesini önlemeye yönelik tedbirler alınması büyük önem taşımaktadır. Bunları yapmada başarısız olma durumu, belgelerin gerçekliğini ve bütünlüğünü tehlikeye sokabilir. Elektronik belgelerin alınması, üretilmesi ve dosyalanmasına ilişkin net süreç ve usullerin geliştirilmesi ve

belgelendirilmesi gereklidir (Aydın, 2010, s. 105). Politikalar ve prosedürler, hangi işlemle işin tamamlandığını belirtmekle birlikte, kabul edilebilir belge formatlarını ve belge üzerinde herhangi bir değişiklik yapılmamasını sağlayacak şekilde güvenli bir depolamayı içermelidir.

Elektronik belgelerin bütünlüğü açısından, belgenin düzenlendiği zamanın şüpheye yer bırakmayacak şekilde bilinmesi gerekmektedir. Zaman kaşesi fonksiyonu bu açıdan önemli role sahiptir. Bilgisayar işletim sistemlerindeki tarih ve saat ayarı çok kolay değiştirilebilmektedir. Bu nedenle onay makamları talep üzerine dijital tarihleri, bir zaman kaşesi ile birlikte bildirmeye mecburdurlar. Bu çerçevede e-belgenin alındı zamanı ve tarihini belgelendirme açısından muhafaza edilmesi gereklidir. Birçok resmi işlemlerde bu bilgilerin belgelendirilmesi önemlidir. Yüksek riskli uygulamalar konusunda, güvenli ya da güvenilir zaman-tarih damgası, elektronik zaman ve tarih damgası uygulayan güvenir ve tarafsız üçüncü parti uygulamalarda kullanılabilir. Güvenilir zaman yetkilisi, bunun gibi elektronik zaman damgaları uygular. Güvenilir zaman damgası, açık şifreleme düzeni içinde sağlanabilen diğer bir hizmettir (NECCC E-sign Policy Workgroup, 2001, s. 6).

Bazı iş süreçleri ya da yasal gereklilikler, alınan e-belgelerin doğrulamasını gerektirir. Doğrulama, uygulamanın türüne bağlı olarak farklı formlarda yapılabilir. Yüksek güvenlikli ortamlarda, farklı bir yolla ayrı bir doğrulama tavsiye edilir. Yasal, denetim ve diğer amaçlara yönelik elektronik belgelerin kabulü, elektronik belgeleri üretmek için kullanılan sistemin sağlamlığının gösterilerek gerçekliğini ve güvenirliliğini tespiti şartına bağlıdır (NECCC E-sign Policy Workgroup, 2001, s. 12). Belge üreten sistemlerin, doğru ve uygun şekilde iş süreçlerinin gerçekleştirildiğini göstermeleri zorunludur. Bu amaca yönelik başarılı bir şekilde kullanılan, elektronik belgelerin güvenirlilik ve gerçekliğini korumaya yönelik çabalarda belge yöneticisine yardımcı olacak bazı öneriler geliştirilmelidir. Belge yöneticisinin, sistemin, normal iş süreçlerini uygun, doğru ve güvenilir biçimde yerine getirdiğinden emin olunmalıdır (Aydın, 2010, s. 106). Bunun için, sistem yönetim politika ve prosedürlerinin belgelendirilmesi ve tanımlanması gereklidir. Bu tip tanımlamalar belge bütünlüğünü destekleyecek unsurlardır.

Elektronik belgelerin bütünlüğü aşağıdaki hususlar çerçevesinde korunabilir (NECCC E-sign Policy Workgroup, 2001, s. 13):

- ◊ Bilgi teknolojisi üreticilerinin tavsiyelerine uygun olarak, bakım yapmaya ek olarak rutin bir şekilde yazılım ve donanımın test edilmesi,
- ◊ Yazılım ve donanımın tedariki, yüklenmesi ve bakımıyla ilgili dokümantasyonların muhafaza edilmesi,
- ◊ Sistem faaliyetlerinin ve performansının güvenirliliğini belgelendirmek amacıyla işlem kayıtları ve çalıştırma planlarının muhafaza edilmesi.

Kurumlar, yüksek riskli sistemler için harici teknik değerlendirme ya da denetimi düşünmelidirler. Benzer sistemlerin bağımsız kontrolü ve denetimi, sistemin ve

ürettikleri elektronik belgelerin güvenirliliğini belgelendirilmesini sağlayabilir. Sistem ya da uygulama işlemleri ve kullanıcı aktivitelerinden oluşan işlem geçmiş raporunun muhafaza edilmesi gereklidir. Uygun araçlar ve prosedürler ile birlikte, işlem geçmiş raporu; kişisel sorumluk, yetkisiz giriş belirleme ve problem tespitleri de dâhil olmak üzere güvenlikle ilgili bazı konularda başarıya ulaşılmasında yardımcı olabilir. İşlem geçmiş raporunun, hangi olayların olduğunu ve kimin sebep olduğuyla ilgili yeterli bilgiyi içermesi gereklidir. Bunlar, sistemde depolanan elektronik belgelerin bütünlüğüne ek olarak, sistemin güvenirliliğini ve sağlamlığını belgelendirmekte kullanılabilir. Eğer mümkünse işlem geçmiş raporu, belgelerin alınması, işlenmesi ve muhafaza edilmesi sırasında otomatik olarak yerine getirilmelidir. Bu kapsamda erişimle ilgili benzer uygulamalar gerçekleştirilmelidir. E-belgelerin belli metotlarla erişilebilir olabileceği göz önünde bulundurulmalıdır. Bu erişim metotlarının erişenle ilgili tanımlayıcı bilgileri ve belgede yapılan değişikliklerin içeriğini kaydettiğini ve bu erişim kayıtlarındaki bilgilerin değiştirilemeyeceğini ve silinemeyeceğini onaylayan bir rapor yazılımının geliştirilmesi ya da temin edilmesi gerekmektedir. Bu rapor, yönetim ve idari fonksiyonları kullanan sistem yöneticilerini de kapsayacak şekilde, bütün kullanıcıların erişimlerini içermelidir (Aydın, 2010, s. 106).

Dijital varlıkların uzun süre korunması, arşiv depolama sistemlerinde bulunan büyük miktardaki veri yığınlarının gerçekliğini yönetecek bir mekanizma gerektirir. Arşivleme ortamları, gerçeklikle ilgili kısıtları düzenler ve alt yapıdan bağımsız çözümler oluşturarak depolama sistem teknolojilerindeki dönüşümü yönetir. Büyük arşivlerde gerçeklikle ilgili ihtiyaçlar data grid teknolojisini kullanılarak çözüme ulaştırılır. Data gridler, depolama ortamlarından çıkarma işlemini sağlar, firma bağımlı ürünler arasında veri taşıma işlemini mümkün kılar ve aynı zamanda arşivsel verinin gerçekliğini de temin eder (Moore, 2004, s.101). Data gridler, firma bağımlı depolama arşivleri ile koruma ortamları arasında ara birim özelliğinde yazılım alt yapısı sağlar.

E-belge bütünlüğünü sağlamak için, belge sayısallaştırma sisteminin; belgeyi üreteni, ne zaman üretildiğini ve üretiminden itibaren değiştirilmediği bilgisini içermesi ve bunu belgelemesi gerekmektedir. Belge sayısallaştırma sisteminde, delilsel bütünlük, belge bütünlüğünü sağlayan bilgi elde edilerek arşivlenir. Bu sistem içinde, bütün bir yaşam evresinde belge bütünlüğünü sağlamak, arşiv sisteminin sorumluluğundadır (Public Records Office of Victoria, 2000, s. 2). Bu açıdan, belgenin bir faaliyet sonucunda üretilmesi ve geçirdiği evrelerin kayıt altına alınması belgenin provenansı açısından göz ardı edilmemesi gereken bir kuraldır (Özdemirci ve Yalçınkaya, 2009, s.8). Bu çerçevede elektronik belgelerin, hem kullanıcı ve hem de sistem yöneticisi tarafından değişikliklere karşı korunması gereklidir.

Belge içeriğinin cihaz düzgün çalışmadığında değişebilir olması, bir kurumdan belgenin üretildiği bilgisayarın güvenli bir şekilde çalıştığını gösteren delillerin istenmesini gerektirebilir. Bilgisayar çalışmasıyla ilgili herhangi bir arızanın bulunduğunu gösteren kayıt defteri genelde yeterlidir. Elektronik belgedeki bir yanlış, bilgisayar programındaki bir hatadan da kaynaklanabilir. Bir kurumdan programın testi ve

geliştirilmesiyle ilgili delilleri göstermesi istenebilir (Aydın, 2010, s. 108). Bu konuyla ilgili bilirkişi, doğruluğu ve güvenirliliği belirlemek için genelde programları gözden geçirir. Bir kurumdan, delil amaçlı olarak elektronik belgelerin yönetimi ve verinin işlenmesinde kullanılan belirli bilgisayar program sürümlerini göstermesi istenebilir (CalRIM, 2002, s. 36). Bir programın farklı sürümlerinden eğer sadece biri kullanılır durumda ise sorun yaşanmayabilmektedir. Ancak doğru sürümünün bulunmaması, elektronik belgelerin güvenilirliği ve bütünlüğü konusunda ciddi soru işaretleri meydana getirebilmektedir.

Bütün belirtilen hususlar çerçevesinde, yasal süreçlerde elektronik belgelerin delil olarak kabul edilebilmeleri için, gerçeklik, bütünlük ve orijinal formunda bulunma gibi özelliklerin yukarıda belirtilen hususlar çerçevesinde sağlanması gerekmektedir.

Gerçeklik ve Bütünlüğü Korumada Sayısal İmza

EBYS, elektronik belge ile ilgili dijital imzayı doğrulayabilmelidir. Sistem, aynı zamanda rastgele bir belge örneğinin dijital imzasının doğruluğunu denetleyebilme özelliğine de sahip olmak zorundadır (Public Records Office of Victoria, 2000, s.5). Dijital imzayı doğrulamadaki hatanın belgenin değiştirildiğinin ya da sahtesinin yapıldığının göstergesi olabilmesi dolayısıyla, dijital imzayı doğrulamadaki herhangi bir hata kaydedilmek ve anında yöneticinin dikkatine sunulmak zorundadır. Elektronik belge, doğrulama hatalarında yöneticinin kabulünü de gerektirir. Eğer belge, erişim performansını artırmak için arşiv dışında bir yerde kaydediliyorsa, hızlı bellekteki belgenin değiştirilmediğini, arşivdeki kopyasıyla aynı olduğunu otomatik olarak doğrulamaya imkân vermesi gereklidir (Aydın, 2010, s. 109).

Dijital imzaların koruma zinciri ya da veri bütünlüğü için uzun vadeli saklamalarda sınırlı değere sahip olduğunun farkında olunması önemlidir. İmzanın değeri, geçerlilik ile sınırlıdır. Geçerlilik zamanı, gizli anahtarın gizliliğinin ihlal edilmesi zamanı, imza algoritmasının gizliliğinin ihlal edilmesi zamanı ve açık anahtar alt yapısının eskime zamanına bağlı olarak sona erebilmektedir (Sproull ve Eisenberg, 2005, s. 62). Örneğin, belgeler için dijital imza oluşturmak amacı ile kullanılan özel anahtar belirli bir zamanda gizliliği ihlal edilmiş hale gelirse, o tarihten sonra özel anahtarla doğrulanmış belgeler şüpheli olacaktır. Bir anahtarın gizliliğinin ihlal edilmesinin fark edilmesi aslında bu olayın gerçekleştiği zamandan çok sonra olabilir. Gizlilik ihlali kriptonalitik bir saldırı sonucunda da olabilir (Sproull ve Eisenberg, 2005, s. 62). Bu nedenle dijital imzalar yeni iletilmiş verileri doğrulamak için en mükemmel yöntemdir.

Dijital imzalar, güvenli iletişim kanalı oluşturmak için diğer birçok kriptografik araçlar ile birlikte kullanılabilir. SSL (Secure Socket Layer: Güvenli Soket Katman) Protokolü, ilk olarak Netscape tarayıcısında uygulanmış; daha sonra IETF (Internet Engineering Task Force-İnternet Mühendislik Görev Ekibi) tarafından standartlaştırılmıştır. Bugün ise bütün web tarayıcılarında kullanılmaktadır. Bu da güvenli kanala bir örnektir. TCP (Transmission Control Protocol- İletim Kontrol Protokolü) tarafından sağlanan güvensiz kanalın üstünde güvenli bir kanal kurar. Bunu da delillerin değiş tokuşu dijital imzaları kullanarak paylaşılan gizli anahtarların görüşmesi ve mesajların aslına

uygunluğunu kanıtlayan MAC kodlarının değiş tokuşu ile yapar (Sproull ve Eisenberg, 2005, s. 62). MAC'lar gerekli bir ortak ve gizli anahtar imzası mekanizmasıdır. SSL'lerin uygulanmasında gözden kaçan bir önemli adım protokol raporlarıdır. Bunlar güvenlik bağlantılarının diğer ucundadırlar. Aslına uygunluğun tamamlanması için, alıcının tanımladığı durumun beklenen durum olduğunu görmek için raporu kontrol etmesi gerekmektedir. Birçok mevcut web tarayıcı bu adımı atlamak ya da önemini azaltmak için SSL kullanmaktadır, bunun sonucunda da güvenlik kanalının aslında hiç güvenli olmadığı sonucuna varılabilir. Dolayısıyla belgenin bütünlüğü tehlikeye atılmış olur (Aydın, 2010, s. 109).

Uzun dönem saklamada dijital imza teknolojisi kullanılarak, belge üretiminden sonra yapılan herhangi bir değişikliğin tespit edilebilmesi sağlanır (Public Records Office of Victoria, 2000, s. 2). Dijital teknolojinin olduğu yerde, diğer sistem kullanıcılar tarafından, kişisel anahtarların bulunmamasını sağlamak için korumaya yönelik ciddi tedbirler alınmalıdır. Buna ek olarak, sistemden üst veri sağlamaya ya da zaman ve tarih damgası gibi uygulamalara dikkat edilmelidir. Bilgisayar sistem saatini değiştirerek, sahte belge üretmek mümkün olmamalıdır.

Sonuç

Elektronik belgelerin arşivlenmesinde en önemli konu, belgenin gerçekliğini ve bütünlüğünü tehlikeye sokmayacak bir sistemin oluşturulması ve devamlılığının sağlanmasıdır. Teknolojide yaşanan hızlı değişim elektronik belgelerin gerçekliğini ve bütünlüğünü korumaya yönelik çözümler sunmakla birlikte, tehditlere de sebep olmaktadır. Bu açıdan sistem güvenliğinin süreklilik içinde sağlanması ve buna yönelik çözümlerin takip edilmesi gerekmektedir. Ayrıca arşiv mekânının seçiminde elektronik belgenin bütünlük ve gerçekliğini korumayı sağlayacak güvenlik unsurlarının ve uygun nem ve sıcaklıkla ilgili konular göz önünde bulundurulmalıdır. Elektronik belgelerin veri yapılarının bozulma olasılığı bulunmasından dolayı, arşivleme sisteminde hata sezme ve düzeltme teknikleri kullanılmalı, böylece elektronik belgelerin bütünlüğü korunmalıdır. Elektronik belgenin yaşam süresini ve gerçeklik ve bütünlüğünü etkileyen en uygun depolama ortamı seçimi, performans, depolama kapasitesi ve güvenirlilik kriterleri çerçevesinde yapılmalı, uzun dönem arşivleme açısından manyetik bantlar tercih edilmeli ve zaman içinde gerekli taşıma işlemleri gerçekleştirilmelidir. Elektronik belgelerin uzun dönem erişilebilir olmalarını sağlamak için dijital koruma tekniklerine mutlaka ihtiyaç duyulmaktadır. Bu çerçevede en yaygın yaklaşım olan taşıma ve dönüştürme tekniklerinin birleştirilmesiyle ortaya çıkan tekniğin kullanılması gereklidir. Bu noktada en önemli husus elektronik belgelerin gerçekliğinin ve bütünlüğünün korunmasıdır. Ancak uygun dijital koruma teknikleri kullanıldığında da belgenin bütünlüğünün tehlikeye girmesi muhtemeldir. Bu noktada taşıma ya da dönüştürme işleminden sonra elektronik belgenin yeniden imzalanmasına ya da taşıma işleminin başarıyla gerçekleştirildiğine dair bağımsız belgelendirmelerin yapılması bir çözüm önerisi olarak sunulmaktadır. Tabi ki gerçeklik ve bütünlük açısından en önemli husus dijital imzadır. Bu açıdan sayısal imzanın orijinal veri akışının ve doğrulama zincirinin

korunması önemli bir zorunluluktur. Doğrulama zinciri, uzun dönem arşivlemede imzanın geçerliliğini sağlayan unsurları kapsamaktadır. Dijital arşivin içinde bir sertifika arşivi de kurulması gereklidir. Bu sertifika arşivi çok iyi korunmalıdır. Böylece sertifikalar değiştirilemeyecek ya da sertifikaya herhangi bir ekleme yapılamayacaktır. Sertifikanın geçerlilik tarihi sona ermesi ya da iptal edilmesi durumunda, sertifikanın durumuyla ilgili bilginin de saklanması önemlidir. Zaman damgasının arşivlenmesi, belgelerin dijital sertifika geçerlilik süresi bitmeden ya da iptal edilmeden önce özel bir anahtarla imzalandığının gösterilmesi açısından önemlidir.

Sonuç olarak oluşturulan elektronik belge yönetim sisteminin arşivleme fonksiyonunun sürdürebilirlik bakış açısıyla yönetilmesi gerekmektedir. Arşivleme sistemine yönelik yapılacak bütün çalışmaların elektronik belgelerin gerçekliğini ve bütünlüğünü korumayı amaçlaması önemli bir zorunluluktur.

Kaynakça

Aydın, C. (2003). *Bilgi teknolojilerindeki gelişmeler ışığında arşivcinin değişen rolü.* Yayımlanmamış yüksek lisans tezi, Marmara Üniversitesi, İstanbul.

Aydın, C. (2010). *Elektronik belgelerin arşivlenmesi ve erişim.* Yayımlanmamış doktora tezi, Ankara Üniversitesi, Ankara.

Bearman, D. (1999). Reality and chimeras in the preservation of electronic records. *D-Lib Magazine, 5*(4). 25 Ocak 2010 tarihinde http://www.dlib.org/dlib/april99/bearman/04bearman.html adresinden erişildi.

California Records and Information Management. (2002). *Electronic records management handbook: State of California Records Management Program*. 20 Ağustos 2010 tarihinde http://www.documents.dgs.ca.gov/osp/recs/ERMHbkall.pdf adresinden erişildi.

Çölkesen, R. ve Örencik, B. (2008). *Bilgisayar haberleşmesi ve ağ teknolojileri.* İstanbul: Papatya Yayıncılık.

Dickman, J. C. (2002). Information preservation: Changing role. *Information Management Journal, 36*(5), 54-59.

Dollar, C. M. (1999). Selecting storage media for long-term access to digital records. *Information Management Journal*, *33*(3), 36-43.

Duranti, L. (2001). The impact of digital technology on archival science. *Archival Science, 1*(1), 39-55.

Hollier, A. (2001). The archivist in the electronic age. *HEP Libraries Webzine.* 23 Ağustos 2010 tarihinde http://eprints.rclis.org/bitstream/10760/4251/1/archivist_in_the_electronic_age.pdf adresinden erişildi.

İmamoğlu, F. (2008). *Sistem ve ağ temelleri.* İstanbul: Bilge Adam Yayınları

Kandur, H. (1999a). Management of electronic records: Educating archivist and records managers. *Arşiv Araştırmaları Dergisi, 1*(1), 35-45.

Kandur, H. (1999b). Elektronik arşivler ve arşivcilik mesleğinin geleceği. M. Akbulut ve F. Subaşıoğlu (Hazl.). *Bilgi Çağı, Bilgi Merkezler ve Bilgi Teknolojileri" Sempozyumu 7-8 Mayıs 1997: Bildiriler* içinde (ss.15-21). Ankara: Ankara Üniversitesi.

Kurnaz, S. (2008). *Veri yapıları ve algoritma temelleri*. İstanbul: Papatya Yayıncılık.

Menkus, B. (1996). Defining electronic records. *Records Management Quarterly*, *30*, 1-6.

Minnesota Historical Society. (2004). *Electronic records management guidelines*. 15 Temmuz 2010 tarihinde http://www.mnhs.org/preserve/records/electronicrecords/erguidelinestoc.html adresinden erişildi.

Moore, R. (2004). Preservation enviroments. NASA Goddard Conference, April. 17 Ocak 2011 tarihinde http://www.sdsc.edu/NARA/Publications/Interop-archive.ppt adresinden erişildi.

A National Electronic Commerce Coordinating Council E-Sign Policy Workgroup. (2001). Electronic records management guidelines for State Government: Ensuring the security, authenticity, ıntegrity, and accessibility of electronic records. 15 Ocak 2010 tarihinde http://www.dir.state.tx.us/standards/NEC3-Records_Mgmt_ED.pdf adresinden erişildi.

North Dakota Information Technology Department (2011). Electronic records management guidelines. 11 Mart 2011 tarihinde http://www.nd.gov/itd/standards/records-management/electronic-records-management-guidelines adresinden erişildi.

Oatway, D. (2004). Electronic records in long-term care. *Nursing Homes, 53(9), 84-89.*

Özdemirci, F. ve Yalçınkaya, B. (2009, Ekim). Belge yönetiminde değişim süreci: e-belgelere çok yönlü yaklaşım. 8. Ulusal Büro Yönetimi ve Sekreterlik Kongresinde sunulan bildiri. 10 Ocak 2011 tarihinde http://beyas.ankara.edu.tr/dosyalar/Yararli_dokumanlar/8_buro_yon_sem.pdf adresinden erişildi.

Public Records Office of Victoria. (2000). *System requirement for archiving electronic records*. 14 Ekim 2008 tarihinde http://www.prov.vic.gov.au/vers/standard/ver1/99-7-1.pdf adresinden erişildi.

Rhodes, S. B. (1991). Archival and records management automation. *Records Management Quarterly*, *25*(1), 12-43.

Saraçoğlu, T. (2006). Veri depolama ağları ve yeni gelişen teknolojiler. *İntransa,* 16 Mayıs 2010 tarihinde http://www.if.com.tr/pages/tr/yayinlar.htm adresinden erişildi.

Shamir, H. A. (1996). New technologies for records management. *Records Management Quarterly, 30(3), 9-14.*

Shepherd, E. (1994). Managing electronic records. *Records Management Journal*, *4*(1), 39-49.

Sitts, M. K. Yay. Haz.). (2000). *Handbook for digital projects: A management tool for preservation and access*. Northeast: Northeast Document Conservation Center.

Sproull, R. F. ve Eisenberg, J. Yay. Haz.). (2005). *Building an electronic records archive at the national archives and records administration: Recomendation for a long-term strategy.* Washington DC: National Academies Press.

Stamatiadis, D. (2005). Digital archiving in the pharmaceutical industry. *Information Management Journal, 39(4), 54-59.*

State of North Dakota. (1998). *Electronic records management guidelines*. 23 Eylül 2008 tarihinde http://www.nd.gov/itd/records/erguide.pdf adresinden erişildi.