323K449 nolu Geçmişten Geleceğe: Elektronik Belgelerin Güvenilirliği TÜBİTAK Projesi 1. Çalıştay Raporu

Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) tarafından desteklenen 323K449 nolu "Geçmişten Geleceğe: Elektronik Belgelerin Güvenilirliği" adlı Proje sonucunda bir hak, yetki veya yükümlülük içererek delil değerine sahip olan, Türkiye'nin geçmişine dair önemli bilgiler içererek Türk milletinin devamlılığını sağlayan elektronik belgelerin geleceğe sağlıklı bir şekilde taşınması için gerekli olan koşullara ilişkin bir yol haritasının sunulması hedeflenmektedir. Proje'de kamu kurum ve kuruluşlarının fonksiyonları neticesinde oluşan ve arşivlik değere sahip olan sosyal medya kayıtları, elektronik postalar (e-postalar), web siteleri, veri tabanları ve video ve fotoğraf gibi görsel-işitsel malzemelerin güvenilirliğinin korunması için hangi kriterlerin benimsenebileceği analiz edilecektir. Bununla birlikte, bu belgelerin güvenilirliğinin korunmasında düzenleyici ve yönlendirici kurumların rolleri incelenecektir. Aynı zamanda, Proje kapsamında kamu kurum ve kuruluşlarında çeşitli saha araştırmaları yapılacaktır.

Proje'nin ilerlemesi için çeşitli çalıştayların yapılması planlanmıştır. Bu plan doğrultusunda Proje'nin ilk çalıştayı 23 Aralık 2024 tarihinde Cumhurbaşkanlığı Millet Kütüphanesinde düzenlenmiştir. Desteklerinden dolayı Cumhurbaşkanlığı Genel Sekreterliğine teşekkür ederiz.

Proje kapsamında incelenen belge türleri olan sosyal medya kayıtları, elektronik postalar (e-posta), web siteleri, veri tabanları ve görsel-işitsel malzemeler için oluşturulan beş (5) çalışma grubunda Proje ekibi ve akademisyenler ile kamu ve özel sektörde çalışan konu uzmanları bir araya getirilmiştir. Çalıştay katılımcıları, incelenen belge türlerinin güvenilirliğinin nasıl korunabileceğine yönelik tartışmalar yapmıştır. Öne çıkan sonuçlar, belge türleri özelinde şöyle belirtilebilir:

Sosyal medya kayıtları:

- Sosyal medya kayıtlarının arşivlenmesine yönelik yeteri kadar uygulamanın mevcut olmadığı anlaşılmıştır. Bu durumun temel nedeni kamu kurumlarında konuyla ilgili bir düzenleme bulunmamasıdır.
- Sosyal medya kayıtları, e-imzalı belgeler gibi senet hükmünde olmadığından delil başlangıcı olarak kabul edilmektedir. Kurumlarda yapılacak arşivsel değerlendirme sonrası, zaman damgası ve kurumsal mühür gibi araçlarla bu belgelerin delil değeri kuvvetlendirilebilir. Bu tür belgeler, resmî belge statüsünde işlem görmelidir.
- Sosyal medya kayıtlarının arşivsel değerlendirme ilkelerinin belirlenmesine ihtiyaç duyulmaktadır. Tüm arşivleme sürecini yönlendirecek politika ve merkezi bir otorite gereklidir.
- Sosyal medya kayıtlarının yönetiminde uluslararası standartlar kullanılmalıdır.
- Elektronik Yazışma Paketi (EYP), sosyal medya kayıtlarının arşivlenmesi için geliştirilmediğinden elektronik arşivleme paketi (EAP) oluşturulmalıdır. EAP'ta kullanılacak asgari üstveriler belirlenmelidir.

- Sosyal medya kayıtları, kurumsal faaliyet ve fonksiyonlarla ilişkilendirilerek arşivlenmelidir.
- Unutulma hakkının kamu görevi yapan kişiler için söz konusu olamayacağından hareketle Kişisel Verileri Koruma Kurumu, sürece dâhil edilmelidir.
- Sosyal medya kayıtlarının arşivlenmesi için etik kurallar oluşturulmalıdır.
- Üst düzey kamu görevlilerinin sadece paylaşımları değil, gelen yorumlar ve etkileşimler de kayıt altına alınmalıdır.
- Belirli aralıklarla teknolojik göç testleri yapılmalıdır.
- Arşivlenen sosyal medya kayıtlarının korunmasında çift faktörlü doğrulama, dakikada yapılan sorgu sınırı getirilmesi gibi yöntemler benimsenebilir.
- Extendend Markup Language (XML) formatında saklanan veriler, birlikte çalışabilirlik açısından daha başarılı sonuçlar vermektedir.
- Sosyal medyayla ilgili log kayıtları, en az arşivsel değerlendirme yapılana kadar saklanmalıdır. Bunun yanı sıra, log kayıtlarında yer alacak hususlar kararlaştırılmalıdır.

E-postalar:

- E-postalar, e-imzalı belgeler gibi senet hükmünde olmadığından delil başlangıcı olarak değerlendirilmektedir. Durum böyle olunca, bazı kurumlar e-postaları çok da saklama gereği duymamaktadır. Ancak kurumsal iş ve işlemlerin gerçekleştirilmesinde e-postaların önemli bir yeri olduğundan bu belgelerin arşivlenmesi neticesinde delil değerleriyle ilgili tartışmalar oldukça azalacaktır.

- E-postaların standart protokollerle gönderilip alınması yönetilebilir bir sistem için gerekli unsurlardandır. Kullanılan mevcut protokoller daha çok e-postanın alıcıya gönderilmesine yönelikken, belgenin hem gönderim hem de saklama ve arşivleme sürecinde değişip değişmediğine yönelik bir protokol ve standardın duyurulmasına ihtiyaç vardır.

- Kurumlarda e-postaların değerlendirilmesine ilişkin bir yaklaşımın pek bulunmadığı anlaşılmıştır. Bunun neticesinde hangi e-postaların arşivlik belge olarak muamele göreceği kararlaştırılamamaktadır. Bu soruna bir çözüm olarak e-postalar, kurumsal fonksiyon ve faaliyetlerle ilişkilendirilmeli; bir tasnif planı oluşturularak saklama planları hazırlanmalıdır.
- Saklama süreleri, e-postalar oluşturulmadan önce tayin edilmelidir. E-postalar, Standart Dosya Planı'na entegre edilerek bir tasnif koduyla oluşturulabilir.
- Arşivlenecek e-postalara birim belge yöneticileri karar verebilir.
- Düzenleyici ve yönlendirici kurumların yukarıdaki hususları içerecek şekilde e-postalarla ilgili çıkaracağı politika gibi bir metin oldukça gereklidir.
- E-postaların iletimine yönelik Simple Mail Transfer Protocol (Basit Posta Aktarım Protokolü [SMTP]) ve Internet Engineering Task Force (İnternet Mühendisliği Görev Gücü [IETF]) gibi standartlar mevcutken zaman içerisinde değişmemesine yönelik protokollerin eksikliği dikkat çekmektedir. Düzenleyici ve yönlendirici kurumların bu konuda girişimler başlatmasına ihtiyaç duyulmaktadır.

- E-postalar için log kayıtlarının oluşturulduğu bilinmektedir. Bu kayıtlar, e-postalar için belirlenen ya da belirlenecek olan saklama süreleri boyunca saklanmalıdır. Log kayıtlarının saklama süresi, e-postaların saklama süresinden daha kısa olmamalıdır. Log kayıtlarına zaman damgası eklenmelidir.
- E-postaların tüm öğeleriyle birlikte saklanmasına ilişkin çeşitli zorluklarla karşılaşılmaktadır. Ekler ve gövdedeki bağlantıların da e-postayla birlikte arşivlenmsi gerekir. Bunun için konu ile gövdenin özet değeri ayrı ayrı saklanabilir.
- E-postaların saklanması için manyetik diskler kullanılabilir.
- Birbirinden farklı konumlarda ve teknolojilerde birden çok yedek tutulmalıdır. Bu yedekler, aynı dosya formatı ve saklama biçimine sahip olmamalıdır.
- Felaket senaryoları belirlenerek iş sürekliliği merkezi kurulmalıdır. Kritik iş süreçleri tayin edilerek bu süreçlerle ilgili olan e-postaların arşivlenmesine öncelik verilebilir.
- E-postaların yönetiminde International Organization for Standardization (Uluslararası Standartlar Teşkilatı [ISO]) tarafından çıkarılan Açık Arşivlik Bilgi Sistemi Standardı (Open Archival Information System [OAIS], ISO 14721) kullanılabilir. Burada katmanlı bir yapı benimsenebilir. E-postaların sistemde oluşan, erişime sunulan ve arşivlenen paketlerinde bulunması gereken bilgiler ve üstverilerin belirlenmesine ihtiyaç duyulmaktadır. Bu bağlamda e-postaların arşivlenmesini de mümkün kılacak bir EAP oluşturulmalıdır.
- E-posta arşivlerine erişimde kimlik doğrulama yöntemlerinden yararlanılabilir.

Web siteleri:

- Web sitelerinin arşivlenmesine yönelik bir rehber/kılavuz bulunmamaktadır.
- Web siteleri, arşivsel değerlendirme yapılarak kurumsal faaliyet ve fonksiyonlarla ilişkilendirilmelidir. Web sitelerinin saklama süreleri, ilişkilendirildikleri faaliyetle bağlantılı olmalıdır.
- Web siteleri, ISO standartları ışığında hıfz edilmelidir (capture).
- Web sitelerinin arşivlenmesinde resmi kurumlar tarafından çıkarılan karşılıklı çalışabilirliği esas alan ve kayıtları Web Archive (WARC) formatında saklayabilen uygulamalar kullanılmalıdır.
- Kamu İnternet Siteleri Rehberi güncellenmelidir.
- 5651 sayılı Kanun gereği log kayıtları en fazla iki yıl tutulmaktadır. Ancak web sitelerine ilişkin log kayıtları, en az web sitesine tanımlanan saklama süresi kadar muhafaza edilmelidir.
- Web sitelerinin imhası için gerekli teknik standartlar tanımlanmalıdır.
- Yedeklemeler için kamu bulut altyapısının oluşturulmasına ihtiyaç duyulmaktadır.
- Arşivlenen web sitelerine erişilirken çok faktörlü kimlik doğrulama yapılabilir.
- Saklamalar için Redundant Array of Independent Disks (Bağımsız Disklerin Artıklık Dizisi [RAID] tabanlı diskler kullanılabilir.

Veri Tabanları:

- Veri tabanlarının arşivlenmesine yönelik olarak herhangi bir yasal düzenleme ya da kural bulunmamaktadır. Dolayısıyla bir uygulama birliği geliştirilmemiş ya da düşünülmemiştir. Bunun neticesinde veri tabanlarında neyin arşivleneceği kararlaştırılmamıştır. Hâliyle kamuda veri tabanlarının arşivlenmesine yönelik yeteri kadar uygulama mevcut değildir.
- Veri tabanlarının yönetiminde ISO standartlarının benimsenmesi yönünde çalışmalar yapılmalıdır.
- Verilerin dağınık yapılarda farklı sistemlerde tutulması entegrasyon ve uyum sorunlarına neden olmaktadır. Kamusal bulut altyapısının eksikliği, kamu kurumlarında veri işlem süreçlerini yavaşlatan bir etmen olarak kabul görmektedir.
- Veri tabanlarının sahipliği konusunda tereddütler yaşanmaktadır. Bazı kurumlarda bağlı kuruluşlarının veri tabanı yönetim işlemleri bütüncül bir bakış açısıyla gerçekleştirilmemektedir. Veri tabanlarının yönetiminde bir dokümantasyona ihtiyaç duyulmaktadır.
- Verilerin değerlendirmesinin yapılmaması, uzun vadeli arşivleme planlarını zorlaştırmaktadır. Veriler; operasyonel, yasal ve tarihsel önem gibi kategorilere ayrılmalıdır. Hangi verilerin ne kadar süreyle saklanacağı daha veriler üretilmeden önce kararlaştırılmalıdır. Bunun için Dijitalleştirme Komisyonu gibi müstakil bir Değerlendirme Komisyonu kurulabilir.
- Kamu için veri tabanlarının arşivlenmesi konusunda politika gibi rehberler hazırlanmalıdır. Bu rehberde arşivlik değere sahip olmayan veriler için imha işlemleri ve ilgili süreç açıklanmalıdır.
- Saklamada Write Once Read Many (Bir kez yazılabilir çok kez okunabilir [WORM]) disklerin kullanılması önerilmektedir.
- Veri tabanı logları, en az veri tabanında tutulan faaliyetlere tanımlanan saklama süresi kadar muhafaza edilmelidir.
- Veri tabanı sistemlerinde kullanım ve saklama kopyaları arasında pek bir ayrım yapılmamaktadır. Bununla birlikte kullanılan formatlarda bir ayrım bulunmamaktadır. Veri tabanlarını da kapsayacak şekilde kamu için OAIS yapısı geliştirilmelidir.
- Veri tabanı sözlük ve kataloglarının hazırlanarak, veri tabanındaki tablolarda ihtiyaç duyulan üstverilerin belirlenmesine ihtiyaç duyulmaktadır.
- Veri tabanlarının yönetiminde şifreleme uygulamaları pek yaygın değildir. Bu durum bir güvenlik açığı doğurabilir. BTK tebliğlerine uygun şekilde güçlü şifreleme yöntemleri benimsenmelidir.
- Veri tabanlarının teknolojik göçü söz konusu olduğunda bu iş için hasredilmiş özel veri göç aracıları kullanılmalıdır. Teknolojik göç süreçleri, ISO standartlarına uygun olarak yapılmalıdır.
- Kamu kurumları için felaket kurtarma merkezlerine ve depolama alanı olarak bulut altyapılarının kullanılmasına yönelik bütüncül bir yaklaşım geliştirilmelidir.

Görsel-İşitsel Malzemeler:

- Görsel işitsel malzemelerin yönetimi için düzenleyici ve yönlendirici kuruluşlar tarafından kriterler geliştirilmelidir.
- Bu tür malzemelerin arşivlenmesi için bir EAP oluşturulmalıdır.

- Belgelerin yönetiminde sunum, işlem ve depolama olmak üzere üç katmanlı bir mimari benimsenmelidir.
- Arşivsel değerlendirme kriterleri, fotoğraf, sesli kayıtlar ve videolar için ayrı ayrı hazırlanmalıdır. Format seçimi, arşivlik değere göre yapılmalıdır.
- Güvenlik kontrolleri, kullanıcı rollerine göre oluşturulmalıdır.
- Log kayıtlarının saklama süresi, belgenin saklama süresinden kısa olmamalıdır. Belgelere saklama süresi tayin edilmediği durumlarda log kayıtları silinmemelidir.
- Ortak bir bulut altyapısına ihtiyaç duyulmaktadır.
- Belgeleri saklamada WORM diskler ya da Linear Tape-Open (Doğrusal açık bant [LTO]) gibi manyetik teypler kullanılabilir.
- Üstveriler, XML formatında oluşturulmalı ve saklanmalıdır.
- Belgeler, kurumsal faaliyet ve fonksiyonlarla ilişkilendirilmelidir.
- Görsel-işitsel malzemelerde bulunan kişisel veriler, Kişisel Verileri Koruma Kanunu kapsamında değil kamusal profil bağlamında değerlendirilmelidir.
- Yapay zekâ gibi uygulamalar için nitelikli veri setleri oluşturulmalıdır.
- Belgelerin kalite kontrolü için kullanılabilecek Digital Record Object Identification (Dijital Belge Nesnesi Kimliklendirme [DROID]) gibi uygulamalar geliştirilmelidir.

TÜBİTAK 323K449 nolu Geçmişten Geleceğe: Elektronik Belgelerin Güvenilirliği Projesi adına Proje ekibi

- Prof. Dr. Fahrettin Özdemirci, Ankara Üniversitesi (Danışman)
- Dr. Özhan Sağlık, Bursa Uludağ Üniversitesi (Yürütücü)
- Doç. Dr. Bahattin Yalçınkaya, Marmara Üniversitesi (Araştırmacı, Sosyal medya kayıtları)
- Dr. Öğretim Üyesi Levent Kutlutürk, İzmir Kâtip Çelebi Üniversitesi (Araştırmacı, Web siteleri)
- Dr. Öğretim Üyesi Muhammet Emin Gedikli, Marmara Üniversitesi (Araştırmacı, E-postalar)
- Prof. Dr. Nevzat Özel, Ankara Üniversitesi (Araştırmacı, Veri tabanları)
- Dr. Öğretim Üyesi Varol Saydam, Marmara Üniversitesi (Araştırmacı, Görsel-işitsel malzemeler)

Bursiyerler:

- Burcu Yılmaz, Ankara Üniversitesi (Bursiyer, Veri tabanları)
- Deniz Ermişoğlu, Marmara Üniversitesi (Bursiyer, Web siteleri)
- Ekrem Akçay, Marmara Üniversitesi (Bursiyer, E-postalar)
- Serhat Uran, İstanbul Üniversitesi (Bursiyer, Görsel-işitsel malzemeler)
- Tuğba Sarıkaya, Marmara Üniversitesi (Bursiyer, Sosyal medya kayıtları)