Hakemli Makaleler

ARŞİV DÜNYASI

Cilt: 6 - Sayı: 2

BİLGİ SAKLAMA SÜREÇLERİNDE YAPAY ZEKÂ SİSTEMLERİNİN KULLANIMINA YÖNELİK RİSK DEĞERLENDİRMESİ

RISK ASSESSMENT FOR THE USE OF ARTIFICIAL INTELLIGENCE SYSTEMS IN INFORMATION RETENTION PROCESSES

Dr. Öğr. Üyesi Türkay HENKOĞLU
Aydın Adnan Menderes Üniversitesi
Yönetim Bilişim Sistemleri Bölümü
turkay.henkoglu@adu.edu.tr

Öz

Artan bilgi miktarına bağlı olarak kalıcı bilgi depolama ortamlarının kapasiteleri de her geçen yıl artmaktadır. İşlenen ve saklanan bilgi miktarındaki artışın meydana getirdiği zorluklar, bu işlemlerin otomatikleştirilmesine yönelik arayışları da hızlandırmaktadır. Bu kapsamda bilgi seçimine ve saklama süreçlerine ilişkin olarak son yıllarda yapay zekâ sistemlerinin kullanımına yönelik ilginin artmakta olduğu görülmektedir. Yapay zekâ sistemleri, otomatikleştirmeye yönelik diğer bilgi işlem süreçlerinden farklı olarak, karar verme aşamasında da etkili olmaktadır. Yapay zekâ, kararların çok daha hızlı alınmasını sağlamakta ve hizmetleri kişiselleştirilmiş bir seviyeye yükseltmektedir. Doğru bir şekilde eğitildiği ve doğru veri kaynakları kullanıldığı sürece, yapay zekâ ile daha az önyargılı ve daha etik kararların alınması mümkün olabilmektedir. Ancak bununla beraber yapay zekâ sistemleri ile otomatikleştirilen karar verme ve saklama süreçlerinin, telafisi mümkün olmayan sonuçlarına hazırlıklı olunmalıdır. Sanallaştırılan bilgi depolama ortamlarında, bilgi kaynaklarının birinci el olma özelliğinin en önemli kanıtı niteliğindeki bilgi bütünlüğünün sağlanmasına yönelik teknik sorunlar, yapay zekâ sistemlerinin kullanımında da geçerliliğini korumaktadır. Bununla beraber, yapay zekâ sistemlerinin bilgi saklama süreçlerine olumsuz etkileri, hukuksal zeminde henüz açıklanabilir durumda değildir. Bu çerçevede çalışmada yapay zekâ sistemlerinin bilgi saklama süreçleri ve kalıcı bilgi depolama ortamlarındaki bilgilerin bütünlüğüne yönelik etkileri değerlendirilmektedir. Bağımsız olarak karar veren ve uygulayan yapay zekâ sistemlerinin hukuksal sorumluluğuna da dikkat çekilerek, çalışma içinde sınırlandırılmış, denetlenebilir ve kontrol edilebilir yapay zekâ sistemlerinin kullanımına yönelik öneriler sunulmaktadır.

Anahtar Kelimeler: *Bilginin Saklanması, Bilginin Bütünlüğü, Yapay Zeka Sistemleri, Karar Süreçleri*

Abstract

The capacities of permanent information storage environments have been increasing year by year due to the increasing amount of information. The difficulties posed by the increase in the amount of information processed and stored accelerate the search for the automation of these processes. In this context, it is observed that interest in the use of artificial intelligence systems related to information selection and retention processes has been increased in recent years. Artificial intelligence systems, unlike other information processing for

automation, are also effective in decision-making processes. Artificial intelligence makes it possible to take decisions much faster and move services to a personalized level. It is possible to make less biased and more ethical decisions through artificial intelligence as long as they are trained properly and right data sources are used. However, it is necessary to be prepared for the irreversible results of decision-making and retention processes automated by artificial intelligence. In virtualized information storage environments, technical problems related to the ensuring the integrity of information, which is the most important proof of the firsthand information, are also valid in use of artificial intelligence. In addition, adverse effects of artificial intelligence systems on information retention processes are not yet explicable on legal basis. In this context, in this study the effects of artificial intelligence systems on information retention processes and the information integrity in permanent storage environments are examined. By drawing attention to the legal responsibility of artificial intelligence systems that independently decide and implement, suggestions for the use of artificial intelligence systems that are able to be limited, checked and controlled are presented within the study.

Keywords: *Information Retention, Integrity of Information, Artificial Intelligence Systems, Decision Making*

Giriş

Kültürel mirasın geleceğe aktarılmasını sağlayan bilgi kaynakları, içeriğin ve araştırma değerinin göz önüne alındığı bir karar süzgecinden geçirilerek saklanmakta ve yönetilmektedir. Geleneksel olarak, uzun süreli koruma için bilgilerin nispeten küçük bir kısmı seçilmektedir. Değerlendirme, seçim ve duyarlılık incelemesi, büyük ölçüde uzman kararına dayanarak elle yapılmaktadır. Kayıtlar, amaca yönelik depolarda saklanmakta ve bir okuma odasında erişime sunulmaktadır. Dijital kayıtlar ise belgelerin yanı sıra, video, web siteleri, yapılandırılmış veri kümeleri ve farklı türde içerikleri barındıran çok fazla çeşitliliğe sahiptir. Çeşitliliğin fazla olması veri bilimi ve arşivler için büyük bir zorluk oluşturmaktadır. Dijital korumanın zorluklarına uzun vadeli tek bir çözüm yöntemi bulunmamaktadır. Bu nedenle nesiller boyunca kayıtların hazır bulunmaya devam etmesi için gereken teknolojik değişime yatırım yapılmalıdır.

1950'li yıllardan itibaren kültürel miras olarak bilginin gelecek kuşaklara aktarımında manyetik ve elektronik ortamlar kullanılmaktadır. Ancak bazı teknolojik gelişmelerin etkilerine bağlı olarak, bilgi saklama süreçleri ve sonuçlarının daha fazla tartışıldığı dönemler bulunmaktadır. 1990'lı yıllardan itibaren her bilgisayar üzerinde sabit disklerin bulunmaya başlaması ile birlikte yerel veri depolama kapasitelerinin ve bilgi erişim hızının artması, bilginin saklanması açısından önemli bir dönüm noktası olarak görülmektedir. 2000'li yıllardan itibaren veri iletişim teknolojilerindeki gelişmelere bağlı olarak bulut bilişim servis ve hizmetlerinin gelişimi, merkezi veri depolama ortamlarının kullanım sürecini başlatmıştır. 2000'li yılların ortalarından itibaren sosyal medya ile birlikte bulut bilişim teknolojisinin kullanımı daha yaygın hale gelmiş ve merkezi veri depolama ortamlarının güvenlik ve hukuksal boyutlarının daha fazla tartışılmasına neden olmuştur. Son yıllarda ise yazılım dünyası ve sistem yöneticilerinin çalışmalarını tamamen otomatikleştirilmiş sistemler üzerine yoğunlaştırdıkları görülmektedir. Bunun için makine öğrenmesine dayalı, insanı taklit eden yapay zekâ sistemlerinin veri saklama süreçlerinde kullanılabilirliğine odaklanmaktadırlar.

Arşivler, kayıtları tutarak ve bunlara erişim sağlayarak topluma değer sağlamaktadırlar. Temelde dijital arşivler de aynı şekilde değer sağlamaktadır. İngiltere Ulusal Arşivi'nin

(2017) yayınladığı dijital strateji raporunda yer alan verilere göre, dijital arşivin kullanıcılarına sunduğu değer için dört kategori bulunmaktadır. Buna göre dijital arşivlerin, araştırma için erişilebilir, kullanılabilir ve anlaşılır olmanın yanı sıra, bütünlüğü bozulmadan saklanması önem taşımaktadır. Bununla beraber, saklama gereksinimi duyulan bilgilere ilişkin bazı beklentiler bulunmaktadır. Bu beklentilerden başlıcaları;

- Korunabilecek dijital kayıt türlerinin genişletilmesi,
- Dijital kayıtların değiştirilmeden orijinal formatlarında korunması,
- Dijital korumanın zorluklarına karşı koyabilmek amacıyla risk yönetiminin uygulanması ve
- Orta vadeli arşivleme çözümlerinin, orta vadeli dijital koruma risklerini yönetebilmesinin sağlanmasıdır.

Bu beklentiler karşılanırken, dijital arşivlerin kullanıcılarına sunmak zorunda olduğu değerlerin göz önünde bulundurulması gerekmektedir. Korunması amacıyla odaklanılan başlıca kayıt türleri arasında; belge biçimleri (örneğin, Word veya Excel), e-postalar, videolar ve karma medyalar (web siteleri dahil) bulunmaktadır. Bu dijital kayıt türlerinin genişletilmesine yönelik çalışmalar, bilgiyi saklama ve güvenliğini sağlama sorumluluğu bulunan bilgi profesyonellerinin iş yükünü arttırmaktadır. Bu nedenle bilgi teknolojilerine dayalı otomatikleştirme işlemlerinden daha fazla yararlanma ihtiyacı oluşmaktadır. Bilginin gelecek kuşaklara aktarılması ve delil niteliğinin korunabilmesi için, bütünlüğünün korunması temel bir zorunluluk haline gelmiştir. Dijital kayıtların çok uzun süreli saklanabilmesi için, gelişen bilgi ve iletişim teknolojilerine uyum sağlaması ve dönüşümlerin bilginin orijinalliğinin bozulmadan yapılması önem taşımaktadır. Bu nedenle bilgi ve iletişim teknolojilerine yapılan yatırımların kesintisiz olarak devam etmesi gerekmektedir. Bilgi saklama süreçleri içinde risk yönetimi yaparken bu durum dikkate alınarak, orta vadeli dijital koruma risklerine yönelik çözümlerin geliştirilmesi öncelikli olarak hedeflenmektedir (UK National Archives, 2017).

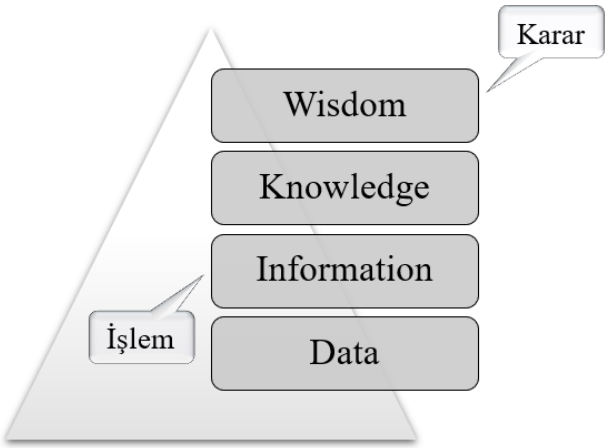
Bu çalışmada yapay zekâ kullanımının bilgi saklama süreçlerindeki karar anına ve bilgilerin bütünlüğüne yönelik etkileri ile teknik ve hukuksal koşullara dikkat çekilmesi amaçlanmaktadır. Çalışmada örneklerle desteklenen riskler dikkate alınarak, sınırlandırılmış, denetlenebilir ve kontrol edilebilir yapay zekâ sistemlerinin kullanımına yönelik öneriler sunulmuştur.

Yapay Zekâ Sistemlerinin Karar Verme Öncesi ve Karar Anına Yönelik Etkileri

Yapay zekâ destekli otomasyon örnekleri hayatın her alanında görülmekte ve kullanılmaktadır. Görüntü işleme ve yüz tanıma sistemleri, ses tanıma özellikli ev yardımcılarının kullanımı, tıbbi teşhis ve tedavi geliştirme süreçleri, bir sonraki satın alımın tahmin ve kontrolü, otonom araçların ve medikal robotların kullanımı, bilgi-eğlence ve reklam ağlarının filtrelenmesi, e-posta görüşmelerine dayanarak önerilen takvim girişleri ve dil çevirileri uygulamalarında, yapay zekânın başarılı olarak kullanıldığı görülmektedir. Bilgi saklama süreçlerinde özellikle arşiv veri tabanlarının kataloglamasında da yapay zekâ sistemlerinden faydalanılmaktadır. Bunun yanı sıra yapay zekâ sistemlerinin, karar verme süreci ve veri bütünlüğünün korunmasına yönelik olarak da etkileri bulunmaktadır. Saklanan bilgilerin bütünlüğü, yapay zekâ çözümleri için kritik başarı faktörüdür. Makine öğrenmesi ve yapay zekânın uygulanması amaçlanan kayıtlar için bilgi bütünlüğüne yönelik standartlar

dikkate alınmalıdır. Bilgi bütünlüğünü sağlamak için basitçe bilgisayar sistem doğrulamasını gerçekleştirmek yeterli değildir (Wolf, 2019).

Geleneksel olarak arşivlerin nispeten küçük bir kısmı uzun süreli koruma için seçilmektedir. Değerlendirme, seçim ve duyarlılık incelemesi, büyük ölçüde uzman kararına dayanarak elle yapılmaktadır. Arşivler, koleksiyonlara fiziksel ve entelektüel erişimi sağlamayı ve araştırmacıların araştırma yapabilmeleri için açıklayıcı bilgi ile koleksiyon düzeyinde entelektüel kontrolü sağlamayı amaçlamaktadır (Conway, 2015). Kayıtlar, amaca yönelik depolarda saklanmakta ve bir okuma odasında halka sunulmaktadır. Dijital kayıtlar ise belgelerin yanı sıra, web siteleri, web tabanlı araçlar, video, yapılandırılmış veri kümeleri ve farklı türde içerikler olabilmektedir. Dijital kayıtların saklama süreç ve koşullarının daha fazla dikkate alınması önem taşımaktadır. Örneğin, dijital kayıtlar için uzun vadeli veri depolama ortamları bulunmaması nedeniyle, birbirinin aynısı olan kopyaların oluşturulması gerekmektedir (UK National Archives, 2017). İçeriğin çeşitliliği ve miktarının artışı ile orantılı olarak personel sayısının artışı mümkün olmadığı için, bilgi saklama süreçlerinde bilişim teknolojilerinden faydalanmaya ve bu süreçlerin otomatikleştirilmesine yönelik ihtiyaç artmaktadır. Ancak robotik teknolojilerin kullanımında ve optik karakter tanıma kullanarak basılı kopya belgelerinin yapılandırılmış bir veritabanına aktarılması örneklerinde görüldüğü gibi, işlemlerin %80'i otomatikleştirilse dahi, kalan %20'sinin daha karmaşık faaliyetler içermesi nedeniyle insan girdisine ihtiyacı olması muhtemeldir (Tomek, 2019; Wolf, 2019).



Şekil 1: DIKW Modeli
(Kaynak: Hey, 2004**)**

Yapay zekâ sistemlerinin bilgi saklama işlemlerinde karar verme sürecine yönelik etkisi, Şekil 1'de görülen Data-Information-Knowledge-Wisdom Modeli[1] (DIKW) üzerinden açıklanabilmektedir. Bilişim sistemlerinin temel unsurları olan giriş, işlem ve çıkış birimlerinin yanı sıra, kültürel mirasın geleceğe aktarılmasını sağlayan bilgi saklama/depolama ortamları da bilgi yönetimi açısından sistemin ana unsuru olarak görülmektedir. Bu temel unsurlar üzerinde bilgi işleme süreçlerine konu olan girdi, DIKW modelinin en alt basamağında yer alan, nesnelerin, olayların ve çevrelerinin özelliklerini

[1] DIKW modeli, Türkçe literatürde yaygın olarak "bilgi piramidi" ya da "bilgi hiyerarşisi" isimleriyle de kullanılmaktadır. Yabancı literatürde ise DIKW için "Knowledge Hierarchy", "Knowledge Pyramid", "Information Hierarchy" ve "Information Pyramid" şeklinde dört farklı kullanım bulunmaktadır.

temsil eden rakamlar ve semboller olarak tanımlanan veridir (Davenport ve Prusak, 2000). Bilgi sistemleri ile verinin üretimi, alınması ve işlenmesi sonrasında veriden bilgi (information)[2] çıkarılır. Bilgi içeriğine ilişkin açıklamada, kimin, neyin, ne zaman ve kaç gibi sorulara cevap bulunabilmektedir. Bilgi (information), metalaştırılmış, nesnel, aktarılabilir, dönüştürülebilir, şeffaf ve ölçülebilirdir. Biçimlendirilmiş, işlenmiş, erişilebilir, üretilmiş, iletilmiş, saklanmış, gönderilmiş, dağıtılmış, aranmış, kullanılmış, sıkıştırılmış ve kopyalanmış olabilir (Hey, 2004). Temel sistem ve bilgi saklama süreçlerinde nesnesi olan, depolanabilen, paylaşılabilen, "information" kullanılmaktadır. Ancak bilgi saklama süreçlerinde hangi bilgilerin saklanacağı ya da nasıl erişim sağlanacağına konusunda karar vermeye yönelik olarak, daha üst seviyeli gerçekleri içeren ve veriden elde edilen bilginin talimata dönüşmesini sağlayan bilgiye (knowledge) ihtiyaç duyulmaktadır. Bilginin (knowledge) elde edilmesi, ona sahip olanın aktarımı, talimat ya da deneyim ile mümkün olabilmektedir. Bu dönüşüm sonrasında bilgi, karar verme sürecine hazır hale gelmektedir. Bilginin değeri, analiz, karar verme, problem çözme ve öğretimde bilginin kullanımından kaynaklanmaktadır (McDermott, 1999). DIKW Modelinde, elde edilen veriler toplanmakta, düzenlenmekte, anlamlı hale getirilmekte, özetlenerek analiz edilmekte ve sentezlenerek bilgi haline gelmektedir. Bilgiye dayalı kararın alınabilmesi için, doğru bilginin, doğru zamanda uygun yere ya da yetkili kişiye iletilmesi sağlanmalıdır (Rowley, 2007). Bilgi saklama ya da bilgi işlem süreçlerinde daha hızlı ve doğru kararların alınabilmesi için, Peter G. Keen tarafından 1972 yılında yeni bir kavram olarak gündeme getirilen karar destek sistemleri kullanılmaktadır. Keen, karar destek kavramını, son kararı verirken yöneticiye destek sağlayan, ancak hiçbir zaman yöneticinin yerini almayan ya da yöneticiyi devre dışı bırakmayan bilgi sistemi olarak tanımlamıştır. Karar destek sistemi, karmaşık problemleri çözümlemek için, insan zekâsı, bilgi teknolojisi ve yazılımın etkileşim içinde olacak şekilde bütünleştirildiği bir sistemdir. Yapay zekâ sistemleri ise karar destek sistemlerinin etkinliğini arttırmaya ve karar vermeye yardımcı olmaya yönelik olarak kullanılabileceği gibi, tamamen insanın yerini alan sistemler olarak tasarlanabilmektedir.

Bilgi saklama süreçlerinde kararın insan ya da makine tarafından alınmış olması, elde edilen sonucun kullanıldığı alana bağlı olarak farklı etki yaratabilmektedir. Yapay zekâ, çok büyük ve karmaşık veri setlerinin analiz edilmesi, adli bilişim gibi alanlarda karmaşık sorunların çoğuyla başa çıkılması ve gerekçelendirme sürecinin açıklanması için ideal bir yaklaşımdır. Yapay zekâ algoritmaları, istatistiksel kanıtlarla tartışmayı destekleyebilir (Chinnikatti, 2018). Örneğin, ceza davasına ait bilgilerle eğitilen bir yapay zekâ uygulamasının risk değerlendirmesinde hâkimlerden daha etkili olması (IRIS, 2017) ya da yüzlerce vakayı inceleyerek, her beş vakanın dördünde (%79) Avrupa İnsan Hakları Mahkemesi kararları ile aynı sonuca ulaşan bir yapay zekâ uygulamasının kesin sonuçlara yol açan davalarda sürece hız kazandıracağı değerlendirilebilir (Aletras, Tsarapatsanis, Preoţiuc-Pietro ve Lampos, 2016). Ancak arşivlerde yer alacak kayıtlardaki %20 ya da daha düşük bir hata ya da yanılma oranı kabul edilebilir değildir. Bu tür saklama ortamlarında temel girdi üzerinden ulaşılacak sonucun otomatikleştirilerek hızlandırılma zorunluluğu bulunmakla birlikte, makine öğrenmesine bağlı olarak değişken sonuçların oluşması istenilmemektedir. Örneğin saklama süreçlerinde bilgi bütünlüğünün kontrolü için önemli bir referans olarak kabul edilen hash

[2] Bu çalışmada "information" karşılığı olarak kullanılan "bilgi" yerine, Türkçe literatürde "enformasyon" terimi da sıklıkla kullanılmaktadır.

değerinin[3] insan iradesinden bağımsız olarak değişmesi, belgeyi hazırlayan kişi ile meydana gelen sonuç arasındaki bağın kurulamamasına neden olabilmektedir. Bu nedenle en son karar verme ve uygulama noktasında yapay zekâ sistemlerinin kullanımının benimsenmesine bağlı riskler oluşabilmektedir (European Commission, 2019a). Yapay zekâ sistemlerinin sağladığı kolaylıklardan en fazla yararlanan teknoloji devlerinden biri olan Google da uygun bir şekilde kullanılması halinde yapay zekânın ekonomiler ve toplum için büyük faydalar sağlayabileceğini ve daha adil, daha güvenli ve daha kapsayıcı olan karar vermeyi destekleyebileceğini belirtmektedir. Ancak Google bununla beraber, yapay zekânın geliştirilmesinin ve kullanımının nasıl yönetileceği, ne ölçüde, ne zaman ve hangi yasal ve etik gözetimin sağlanacağını dikkate almayı da içeren özen ve çaba olmadan yapay zekâ sistemlerinin karar vermeyi desteklemesinin mümkün olamayacağının altını çizmektedir (Google, 2019). Benzer şekilde bir teknoloji devi olan Samsung Hukuk Müşaviri Tom Marshall da yapay zekâ sistemlerinde kontrol kaybı olduğunda zarar verme potansiyelinin bulunduğuna dikkat çekmektedir (Gringras, Stevens, Tench ve Free, 2019). Bilgi saklama süreçlerinde karar verici olarak yapay zekânın kullanılması halinde kontrol kaybının hangi noktada başlayacağı ve bunun nasıl tespit edilebileceği konusunda belirsizlikler bulunmaktadır. Dijital çağda kayıtları yönetmenin zorlukları yapay zekâ sistemleriyle karşılanacaksa, bunları kullanmak için gereken bilgi, beceri ve özene sahip olunması önem taşımaktadır (Rolan ve diğerleri, 2019).

Güvenilir Yapay Zekâ Sistemlerinin Temel Gereklilikleri ve Sınırlılıklar

Genel olarak bilişim alanında etik sorunları arttıran teknolojik eğilimler, yapay zekâ sistemleri için de geçerliliğini korumaktadır. Bilgi sistemleri kullanan organizasyonlarda yaklaşık 18 ayda ikiye katlanan hesaplama gücü, veri saklama tekniklerinde hızlı gelişme ve saklama ünitelerinin maliyetlerinin düşmesi, ağ ve internet teknolojilerindeki gelişmelere bağlı olarak çok büyük bilgilere erişim ve bilginin bir noktadan başka bir noktaya iletilme maliyetinin düşmesi, büyük veri yığınları içinden veri analiz tekniklerinin gelişmesi ve bilginin kolaylıkla izlenebilmesi ya da kaydedilmesi, etik sorunların oluşmasında etkili olan başlıca unsurlardır (Laudon ve Laudon, 2014). Güvenilir yapay zekâ sistemlerinin yürürlükteki tüm yasa ve yönetmeliklere uygunluğu sağlamalı, etik ilke ve değerlere uyumlu olmalı ve hem teknik hem de sosyal açıdan sağlam olmalıdır. Yapay zekâ sistemleri istemeden dahi zararlı olmamalıdır (European Commission, 2019b).

Yapay zekâ sistemlerinin geliştirilme amaç ve kapsamı dışındaki eylemleri gerçekleştirme yeteneğinin küçümsenmesinin, hukuksal sorunların ortaya çıkmasının başlıca nedeni olduğu düşünülmektedir (Karliuk, 2018). Bilgi yöneticilerinin ve saklanan bilgilerin bulunduğu depolama ortamlarından sorumlu sistem yöneticilerinin bilgi güvenliğinin sağlanmasına yönelik hukuksal sorumlulukları bulunmaktadır. Örneğin 5651 Sayılı Kanun'un 5. Maddesinde (2007) olduğu gibi, bilgi güvenliğini sağlama yükümlülüğünü içeren hukuksal düzenlemelerde, bilginin doğruluğunun, bütünlüğünün ve gizliliğinin sağlanması hedeflenmektedir. Bir bilgi sistemi ve üzerindeki bilgilerin güvenliğinin sağlanması, hukuka aykırı olarak sisteme girişlerin engellenmesi ve/veya sistem üzerindeki bilgilerin hukuka aykırı olarak değiştirilmesi, silinmesi ya da yok edilmesine karşı önlemlerin alınması ile

[3] Hash değeri, hash'i hesaplanan veriye özel, benzersiz, tek yönlü bir algoritmik fonksiyondur. Verinin değişikliğe uğrayıp uğramadığını kontrol amacıyla kullanılır. Bununla beraber, hash değerinden verinin kendisine ulaşılamaz.

mümkün olabilmektedir. Bununla beraber, Türk Ceza Kanunu'nun (TCK) 243. ve 244. Maddelerinde (2004) suç olarak tanımlanmış olan hukuka aykırı olarak sisteme girme ve bilgi bütünlüğünün bozulmasına yönelik hareketlerin tespit edilerek hukuksal gerekliliğin yerine getirilmesi de bu sürecin bir parçasıdır. Bu kapsamda TCK'nın 278., 279. ve 281. Maddelerinde düzenlenmiş olan "suçu bildirmeme" ve "suç delillerini yok etme, gizleme veya değiştirme" suçlarının oluşmasına neden olabilecek işlemlerden kaçınılması da önem taşımaktadır. Hukuksal çözüme katkı sunulabilmesi için sistem erişimleri ve veri bütünlüğü kontrol edilerek, meydana gelen hukuka aykırı fiil fark edildiği anda ilgili makamlara bildirilmelidir. Bilgi saklama süreçleri ve yapay zekâ sistemlerinin kullanımına bağlı riskler açısından, saklanan/korunan bilgilere yönelik yetkisiz erişimler ve bu bilgilerin bütünlüğüne yönelik tehditlerin etkileri göz ardı edilmemelidir. Zira normal koşullarda dahi bilişim suçlarında fail ile meydana gelen sonuç arasındaki nedensellik bağının kurulmasında zorluklar bulunurken, bilgi saklama süreçlerinde karar verici olarak yapay zekâ sistemlerinin kullanılması halinde bu bağın kurulmasına engel olan unsurların artacağı aşikârdır. Örneğin 2014 / 29566 esas ve 2015 / 13421 sayılı Yargıtay Kararı'nda (2015) görüldüğü gibi, en küçük bir olasılık dahi fail ile meydana gelen sonuç arasındaki bağın ortadan kalkmasına neden olabilmektedir.

Bilgi saklama süreçlerinde yapay zekâya dayalı otomatikleştirme işlemlerinin kişi aleyhine hukuksal sonuçları ve buna bağlı olarak itiraz hakları oluşabilmektedir. Örneğin 6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK)'nun 11. Maddesinin "g" fıkrasında (2016), "işlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme" hakkı düzenlenmektedir. Bu ve benzer içerikteki düzenlemelere bağlı olarak, yapay zekâ sistemleri karar verici olduğunda, herhangi bir sorun ile karşılaşmadan önce iki temel hususa yönelik hazırlıklı olunmalıdır. Öncelikle makine öğrenmesine bağlı olarak gerçekleştirilen işlemlere itiraz edildiğinde sorumluluğun üstlenilmesi ve gerekli işlemlerin yapılması konusunda bir politikanın yapılmış olması önem taşımaktadır. Bununla beraber, herhangi bir bilgi saklanmaksızın yeni veriler üzerinden öğrenmeyi gerçekleştiren yapay zekâ modellerinin oluşturulup oluşturulmayacağı da ilgili kurum ve kuruluşlar tarafından önceden belirlenmiş olmalıdır. Yapay zekâ sistemlerinin tasarımına yönelik teknoloji ve hukuksal düzenlemelere uyumlu olarak hazırlanan standartların bulunmaması nedeniyle, bilgi saklama süreçlerine yönelik olarak hazırlanan politika ve prosedürler içinde bu tür risklere karşı alınacak önlemler ve sorumlulukların paylaşımına yer verilmelidir.

Yapay zekâ sistemlerine dayalı olarak saklanan bilgilerin saklama ortamı üzerinde bulunduğu alan ve kalıcı silme işlemlerinin gerçekleştirilmesi açısından da hukuksal belirsizlikler içermektedir. Günümüzde özellikle sanallaştırılmış merkezi veri depolama ortamlarında saklanan kayıtların dosya sistemi ve veritabanları üzerinde dağıtık yapıda bulunması analiz işlemlerini zorlaştırmaktadır. Bu durum, delil niteliğinin geçerliliği açısından olduğu kadar kayıtların kalıcı olarak silinmesi açısından da önemlidir. Örneğin KVKK'nın 7. ve 11. Maddelerinde düzenlenen verinin silinmesi, yok edilmesi ve anonimleştirilmesine ilişkin haklarının yapay zekâ uygulamaları ile saklanan veriler üzerinde nasıl ve kim tarafından sağlanacağının önceden belirlenmiş olması gerekmektedir. Bununla beraber, bu tür dağıtık sanal yapılar üzerinde veri tabanına zarar vermeksizin

verilerin kalıcı olarak silinmesi çoğu zaman mümkün olamamaktadır (Villaronga, Kieseberg ve Li, 2018).

Bir yapay zekâ işleminin nasıl çalıştığı yalnızca yapay zekâ sistemlerini tasarlayanlar tarafından tam olarak anlaşılabilmektedir. Bu nedenle sadece açıklama yapılarak yapay zekaya yönelik güvenin kazanılması mümkün olamamaktadır. Bununla beraber, yapay zekâ sistemleri tarafından gerçekleştirilen işlemlerin belgelenmesi de genellikle çok zor olduğu için bu tür uygulamaların güven kazanması uzun zaman alabilmektedir. Daha fazla şeffaflık, yapay zekâ teknolojilerine daha fazla inanç ve güven kazandırabilmektedir. İnsan düşüncesi ile birlikte gelen şeffaflığa ilişkin eksiklik, makineler kullanılarak ortadan kaldırılmaktadır. Ancak şeffaflık, etkileyici bir yapay zekâ sisteminin sırlarının korunması açısından çoğunlukla istenmeyen bir durumdur. Yapay zekâ sistemlerine güven duyulmasına katkı sağlayan unsurlardan biri de hukuksal düzenlemelerin yapılmasıdır. Yapılan hukuksal düzenlemelerle gerekli parametre ve standartların belirlenmesi, bu teknolojilere duyulan güveni arttırmakla birlikte, geliştiricilerini avantajlı duruma getirebilmektedir. Yapay zekâ sistemleri beslendikleri verilerden etkilenebilmekte ve veri kümelerinden yanlış sonuçlar çıkartabilmektedir. Yapay zekâ sistemlerinin belirlenen standartlar kapsamında kontrolünün bir insan tarafından sağlandığının bilinmesi de bu sistemlerin kullanımına yönelik güvenin artmasına neden olmaktadır. Yapay zekâ sistemlerine yönelik bu güven algısı, bir uçakta bulunan yolcuların, uçuşun büyük bölümü otomatikleştirilmiş olsa dahi uçağın sağladığı veri ve kontrollerin pilot tarafından gözlemlenmesini beklemeleriyle benzerlik göstermektedir (Gringras ve diğerleri, 2019). Bilgi saklama süreçlerinde kullanılan yapay zekâ sistemlerinin açıklanabilir olması, gelecek kuşaklara aktarılan kültürel mirasın orijinalliğinin korunmasına yönelik güven sağlaması açısından da önem taşımaktadır.

Yapay zekâ sistemleri araştırmalardan ve insan incelemesinden elde edilen geri bildirimlerden yararlanarak devam eden, kapalı döngü bir geri bildirim süreci ile öğrenmektedirler (EY, 2018). Bilgi saklama süreçlerinde yapay zekâ sistemlerinin insan önyargısından etkilenmemesi önem taşımaktadır. Yapay zekâ destekli bir sistem tarafından oluşturulan tahminlerin ve yanıtların tarafsız olacağı varsayılabilir. Ancak yapay zekâ modellerinin dayandığı iş uygulamalarına yığınlanmış veriler katkı sağlıyorsa, insan önyargısı yapay zekâ sistemlerine dönüştürülebilir. Bu durumun kötü amaçla kullanılması halinde, objektif olmayan sonuçların üretilmesi için işleyişin kontrol edilebilmesi mümkün olabilmektedir (Ganesan, 2019). Yapay zekânın daha iyi veri setlerine erişimine izin verecek bir yol aranırken, bunun zararlı faaliyetler amacıyla da kullanılabileceğinin dikkate alınması gerekmektedir (Gringras ve diğerleri, 2019). Bu nedenle, güçlü bir başlangıç veri seti ile çalışmak, yapay zekâ sistemlerinden güvenilir sonuçlar almak için hayati önem taşımaktadır.

Yapay Zekâ Sistemlerinin Kullanımına Bağlı Sonuçlara İlişkin Yükümlülükler

Yapay zekâ sistemlerinin muazzam potansiyelinin başarılı bir şekilde kullanılması, önemli miktarda veriyi güvenle toplayabilen ve saklayabilen sistemleri gerektirmektedir (Ganesan, 2019). Karar verici ve uygulayıcı sistemler olarak yapay zekâ sistemlerinin bilgilerin saklanma süreçlerinde kullanımı, hukuksal olarak tanımlanmayı bekleyen bazı belirsizliklerin soruna dönüşmesine neden olabilecektir. Yapay zekâ sistemlerinin kişiliği ve bu sistemlerin kullanımına bağlı olarak gelişen olumsuz sonuçların sorumluluğuyla ilgili konular hakkında henüz üzerinde uzlaşılabilen bir çözüm sunulamamaktadır. Bağımsız

karar verebilen makine öğrenimine bağlı sistemlere dayanan bu tür teknolojiler günümüzde nesne olarak tanımlanmamaktadır. Ayrıca sınırlı sayı ilkesi gereğince, kanun tarafından öngörülmedikçe yapay zekâ sistemlerinin bağımsız hak süjesi olması ve buna bağlı "tipe bağlılık ilkesi" gereğince de kanunun öngördüğünden farklı bir faaliyet alanında işlev görmesini sağlayacak karma bir tüzel kişiliğin oluşturulması mümkün değildir (Dursun, 2008). Gerekli düzenleme yapılarak yapay zekâ sistemlerine tüzel kişilik kazandırılması halinde ise manipülasyon olma olasılığı ve birçok zararlı kodun aynı yöntemler üzerinden geliştirilme ve kullanılma riskleri bulunmaktadır. Bu koşulda herhangi bir manipülasyon olmaması için hesap verilebilirliğin sağlanması gerekmektedir. Yapay zekâ sisteminin kişiliği, Türkiye'de ve uluslararası hukukta bir hukuk konusu olarak tanınmamaktadır. Bu konuda çalışmalar devam etmekle birlikte, yol gösterici nitelikte Uluslararası Mukavelelerde Elektronik Haberleşmenin Kullanılmasına İlişkin Sözleşmenin 12. Maddesinde bilgisayarı programlayan gerçek veya tüzel kişinin, makine tarafından üretilen tüm mesajlardan sorumlu olması gerektiği belirtilmektedir (UNCITRAL, 2007, s. 7). Ancak yapay zekâ sistemlerini tasarlayanların yanı sıra, onun satıcısı ve kullanıcısı ile yapılan sözleşmelerin de dikkate alınması gerekmektedir. Bununla beraber, yapay zekâ sisteminin üretmiş olduğu sonucun onu tasarlayanların hedeflerinden uzaklaşıp uzaklaşmadığının tespit edilmesi de oldukça zordur. Yapay zekâ modelleri yalnızca onlara güç veren veriler kadar iyidir. Yapay zekâ sistemlerinin doğru veya yanlış veri kaynağından öğrenip öğrenmediklerini tespit etme yetenekleri bulunmamaktadır. Elde edilen verinin büyük ölçüde değişmesi veri modellerinin ilgisiz kalmasına neden olacaktır (Ganesan, 2019). Bu nedenle öğrenme ve karar verme yeteneğinin veri bütünlüğüne yönelik risk oluşturmadan kullanılabilmesi için öğrenme modellerinin sıklıkla güncellenmesi ve kontrol edilmesi gerekmektedir.

Yapay zekâ sistemlerinin bilgi saklama süreçlerinde kullanımına bağlı olarak gelişen sorunların yapay zekâ kişiliği üzerinden çözümlenmesi ya da değerlendirilmesi hukuksal yöntemlerle yapılamamaktadır. Bu nedenle bilgi saklama işlemleri esnasında istenmeyen sonuçların oluşmasına yönelik olarak, bilgi güvenliği açısından hesap verilebilirliğin sağlanması gerekmektedir. Bu kapsamda, bilginin kaydedilmesi aşamasında ve sonrasında bütünlüğünün ve delil niteliğinin korunmasına yönelik etkileri bulunan e-imza, bilgi kriptolama işlemleri vb. unsurlar öncelikli olarak dikkate alınmalıdır. Bir belgenin elektronik ortamda elde edilmesi ya da oluşturulmasından imhasına kadar olan süreçte bütünlüğünün ve delil niteliğinin korunmasına yönelik olarak kullanılan en önemli araçlardan biri güvenli elektronik imzadır (e-imza). Bu konuda geniş bir e-imza mevzuatı (Bilgi Teknolojileri ve İletişim Kurumu [BTK], 2017) oluşmuş durumdadır. 5070 Sayılı Elektronik İmza Kanunu'nun (2004) 5. Maddesinde, güvenli e-imzanın elle atılan imza ile aynı hukukî sonucu doğurduğu ifade edilmektedir. Bununla beraber, hukuksal düzenlemelerde (6100 Sayılı Kanun, 2011) açık olarak belirtildiği gibi, güvenli e-imza ile oluşturulan belgenin delil niteliğine yönelik tereddüt bulunmamaktadır[4]. E-imza, bir belgenin aidiyetinin saptanması açısından önemli bir gösterge olmakla birlikte, bilgi bütünlüğünün sağlanmasına da katkı sağlamaktadır. Ancak saklanan bilgilerin bütünlüğüne ilişkin olarak sadece dosya içeriğinin değil, delil niteliğinin korunması için belge işlem süreç kayıtlarının da bütünlüğünün sağlanması önem taşımaktadır. Başka bir ifadeyle, e-imza ile imzalanmış olan belgelerin

[4] Türk Hukuk Mevzuatında bu görüşü destekleyen hukuksal düzenlemeler bulunmaktadır. Örneğin, 6100 Sayılı Hukuk Muhakemeleri Kanunu'nun 205. Maddesinde (2011), usulüne göre güvenli elektronik imza ile oluşturulan verilerin senet hükmünde olduğu ve bu senetlerin kesin delil olduğu ifade edilmektedir.

tarih/zaman bilgilerinde herhangi bir nedene bağlı olarak değişiklik yapılmamalıdır. Bu konudaki teknik hususlara ilişkin hukuksal düzenlemenin Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 34.Maddesinde yapıldığı ve gereken teknik kriterlerin tebliğ ile belirleneceği ifade edilmektedir (BTK, 2005b). Elektronik İmza İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğin 10. Maddesinde ise bu işlemlerin "ETSI TS 102 023" standardına uygun olarak yapılacağı belirtilmektedir (BTK, 2005a). ETSI TS 102 023 standardında (2002) ilgili personelin konu uzmanı olması gerekliliği, hangi şartlarda belge süreç kayıtlarına müdahale edebileceği ve sistemin buna hangi ölçüde izin vereceği hususları açık olarak yer almaktadır. Ancak elektronik belge yönetim sistemi (EBYS) üzerindeki bilgilere yönelik denetim ve kontrollerin hukuksal düzenlemelere bağlı olarak yapılamaması, uygulamada bütünlüğün ve belge delil niteliğinin bozulmasına neden olabilmektedir. Kurumlardaki EBYS erişim ve kontrol yetkileriyle, e-imza işlemleri için uygulanması zorunlu olan standartlar arasında uyumsuzluk olabilmektedir. Mevcut durumda EBYS üzerinde belge akış süreçlerine ilişkin işlem kayıtlarının güvenliği konusunda riskler bulunmaktadır. Bu çerçevede yapay zekâ sistemleri ile bu işlemlerin otomatikleştirilmesinin durumu daha karmaşık hale getireceği aşikardır. Yapay zekâ sistemlerinin kullanılması halinde, işlem takibine yönelik kayıtların zarar görmemesi ve belgenin delil niteliğinin bozulmaması için, işlem adımları izlenerek gerekli aşamalarda belge üzerinde işlem yapan ilgililere iletilerin gönderilmesi sağlanmalıdır.

Belgelerin delil niteliğinin ve bütünlüğünün korunması için bilgi saklama ortamları üzerinde uygulanan ilk ve en önemli yöntemlerden biri bilginin kriptolanmasıdır. Yapay zekâ ile belge içeriğine bağlı işlemlerin otomatikleştirilmesi için, belgenin kriptolanmadan saklanması ya da kriptolama işleminde kullanılan algoritmanın yapay zekâ uygulaması içinde tanımlanmış olması gerekmektedir. Her iki yöntemin de taşıdığı riskler nedeniyle tercih edilmesi mümkün değildir. Kayıtların kriptolanmadan saklanması halinde tüm işlemler sadece saklama ortamlarının sorumlularının kontrolü altında gerçekleştirilmektedir. Saklanan verilerin kişisel veriler olması halinde ise veri sahipleri yapılan tüm işlemlere ilişkin olarak saklama ortamlarının sorumlularına güvenmek zorunda kalmaktadır (Ganesan, 2019). Bilgi kriptolamanın yapay zekâ sistemlerini engelleyebildiği kurum ve kuruluşlarda, yapay zekâ sistemlerinin yararları ve bilgi güvenliği arasında denge kurulması gerekir. Bunun için, kripto çözülmeden kriptolu bilgiler üzerinde hesaplamalar yapma yöntemi olan homomorfik kriptolama gibi teknolojiler önerilmektedir. Bilginin işlenmesi sırasında homomorfik kriptolama kullanılarak, kripto çözümüne ihtiyaç duymadan işlemler yapılabilmekte ve işlemlerin kriptolanmamış sonucunu sadece kullanıcı görebilmektedir (Bhuvaneswari, Vasuki ve Kumar, 2017; Ganesan, 2019). Homomorfik şifreleme, sürekli izleme ve diğer stratejileri kullanan çoklu güvenlik katmanları uygulanarak desteklenebilir.

Sonuç ve Öneriler

Bilgi ve iletişim teknolojilerindeki gelişmelere bağlı olarak dijital korumanın artan zorlukları ile mücadele edilebilmesi için, teknolojik değişime yatırım yapılması zorunludur. Bu kapsamda bilgi saklama süreçlerinde makine öğrenmesi ve yapay zekâ sistemlerinden faydalanılarak işlemlerin otomatikleştirilmesine yönelik çözüm arayışları bulunmaktadır. Yapay zekâ sistemlerinin karar destek sistemleri ile birlikte ve insanı tamamlayıcı nitelikte olmasının bilgi saklama süreçlerine önemli katkılarının olabileceği düşünülmektedir. Yapay zekâ sistemlerinin karar vermeyi destekleyebilmesi için, geliştirilme ve kullanılma

süreçlerinde yasal ve etik gözetimin sağlanmasına yönelik özen ve çabanın gösterilmesi önem taşımaktadır. Bu sistemlerin insan iradesinden ve denetiminden bağımsız olarak sınırlandırılmaksızın karar alması ve bunu uygulamaya dönüştürmesi, saklanan bilgilerin bütünlüğü ve delil niteliğine yönelik riskler oluşturmaktadır.

Yapay zekâ sistemlerinin EBYS ve arşivlere yönelik saklama süreçlerinde kullanımına yönelim, bilgi ve iletişim teknolojilerindeki gelişime bağlı doğal bir zorunluluğun başlangıç noktasıdır. Ancak yapay zekâ sistemlerinin öğrenme süreci sonunda sahip olduğu bilgiyi doğrudan karar ve harekete dönüştürmesi istenmeyen sonuçlara neden olabilmektedir. Saklanan verilerin bütünlüğünü kaybetmeden normalleştirilmesi ile verilerin dönüştürülmesi gerekmektedir. Kayıtların tehlikeye atılmamasını sağlamak, başarılı bir yapay zekâ teknolojisi uygulaması için hayati öneme sahiptir. Bilgi saklama süreçlerinin karar aşamasına katkı sunan karar destek sistemlerinin içinde bu sistemlerin tamamlayıcı olarak kullanılması, olası risklerin önüne geçilmesine katkı sağlayacaktır. Bunun yanı sıra, yapay zekâ sistemlerinin kendini geliştirmesine yönelik kontrollerin ve gerekli durumlarda müdahalenin kimler tarafından yapılacağı belirlenmelidir.

Kurum ve kuruluşların saklanan verilere yönelik olarak veri bütünlüğünü sağlayabilmeleri için açıklanabilir yapay zekâ sistemlerine yatırım yapmaları gerekmektedir. Böylece yapay zekâ sisteminin tahminlerine yönelik bir nedenin öne sürülmesi ve gerçekleştirilmesi gereken eylemlere ilişkin açıklamaların sunulması sağlanabilecektir. Bunun sonucunda, elde edilen veri ile veri modelinin ilgisiz kalması gibi risklere karşı koyma fırsatının da oluşması sağlanabilecektir. Bilgi saklama süreçlerinde yapılan otomatikleştirme işlemlerinin açıklanabilirliğinin, tercih edilen sistemlerin bilgi güvenliği politikaları ve hukuksal koşullara uyumluluğuyla da ilişkisi bulunmaktadır. Bu nedenle yapay zekâ algoritmasının nasıl korunacağı, üretilen hatalı sonuçların kim tarafından ve nasıl kontrol edileceği, hatalı sonuçların üretildiği fark edildiğinde hangi alternatif yöntemlerin kullanılacağına yönelik planlamaların bilgi güvenliği politikaları çerçevesinde yapılması önem taşımaktadır.

Yapay zekâ uygulamasının sahip olacağı yeteneklerin etik kurallar ve hukuksal düzenlemelerle uyumluluğu önem taşımaktadır. Bu kapsamda öncelikle veritabanlarında bulunan bilginin bütünlüğünün ve delil niteliğinin kim tarafından ve nasıl korunacağının belirlenmesi gerekmektedir. Elektronik ortamda bulunan bir belgenin hukuksal olarak delil niteliğinin korunması ve doğrulanabilir olması için hash değerinin korunması gerekmektedir. Bu tür doğrulama araçları, yapay zekâ uygulamasının, tasarlayanın amaçlarına hangi ölçüde uyum sağlayabildiğinin anlaşılmasını da kolaylaştırmaktadır. Mevcut hukuksal koşullarda yapay zekâ sistemlerinin kendi kişiliği üzerinden kusurlu bulunması mümkün olmadığı için, uygulama hatasına bağlı hukuka aykırı işlem ve sonuçlara ilişkin sorumluluklar tüm bilgi yönetim süreçlerinde olduğu gibi önceden belirlenmiş olmalıdır. Yapay zekâ sistemlerini tasarlayanların, sistemin ürettiği sonuç ve zararlar kapsamında sorumlulukları bulunmaktadır. Ancak bununla beraber, sistemin kullanıcılarıyla yapılan sözleşmelerin varlığı ve bu sistemlerin denetimini sağlamakla yükümlü kişilerin de sorumluluklarının olduğu göz ardı edilmemelidir.

Yapay zekâ sistemlerinin tasarımına ve mevcut sistemlerin dönüşümüne yönelik stratejilerin geliştirilmesi konusunda teknoloji ve hukuksal düzenlemelere uyumlu olarak hazırlanmış standartlar bulunmamaktadır. Bu nedenle bilgi saklama süreçlerine yönelik olarak

hazırlanan politika ve prosedürler içinde bu tür risklere karşı alınacak önlemler ve sorumlulukların paylaşımına yer verilmelidir. Yapay zekâ sistemlerinin bilgi saklama süreçlerinde kullanımına bağlı olarak meydana gelebilecek risk ve tehditlerin görülebilmesi amacıyla, sistem dönüşüm süreçlerinde mümkün olduğunca pilot dönüşüm stratejisinin tercih edilmesi önem taşımaktadır. Dönüşüm süreçlerinde insan denetim ve kontrolü de sağlanmalıdır. Bununla beraber, bu sistemleri kullanan ya da sistem üzerinde bilgileri işlenen kişilerin güveninin sağlanması amacıyla, mümkün olduğu ölçüde şeffaf ve açıklanabilir tasarımların geliştirilmesine özen gösterilmelidir.

Kaynakça

5070 Sayılı Kanun. (2004). Elektronik İmza Kanunu. Erişim adresi: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5070.pdf

5237 Sayılı Kanun. (2004). Türk Ceza Kanunu. Erişim adresi: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf

5651 Sayılı Kanun. (2007). İnternet Ortamında Yapılan Yeyınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun. Erişim adresi: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf

6100 Sayılı Kanun. (2011). Hukuk Muhakemeleri Kanunu. Erişim adresi: http://www.resmigazete.gov.tr/eskiler/2011/02/20110204-2.htm

6698 Sayılı Kanun. (2016). Kişisel Verilerin Korunması Kanunu. Erişim adresi: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf

Aletras, N., Tsarapatsanis, D., Preoţiuc-Pietro, D. ve Lampos, V. (2016). Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective. *PeerJ Computer Science, 2*. doi: https://doi.org/10.7717/peerj-cs.93

Bhuvaneswari, M. S., Vasuki, K. A. ve Kumar, J. Karthik. (2017). Homomorphic Encryption in Cloud. *International Journal of Recent Engineering Research and Development, 2*(5), 84-89. Erişim adresi: http://www.ijrerd.com/papers/v2-i5/part-II/14-IJRERD-B205.pdf

BTK. (2005a). Elektronik İmza İle İlgili Süreçlere ve Teknik Kriterlere İlişkin Tebliğ. Erişim adresi: https://www.btk.gov.tr/uploads/pages/eimza-teblig-5a33fe9b1f2a2.pdf

BTK. (2005b). Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmelik. Erişim adresi: https://www.btk.gov.tr/uploads/pages/eimza-yonetmelik-5a33fe7fe7d86.pdf

BTK. (2017). Elektronik İmza Mevzuatı. Erişim adresi: https://www.btk.gov.tr/elektronik-imza-mevzuati

Chinnikatti, S. K. (2018). Artificial intelligence in forensic science. *Forensic Science & Addiction Research, 2*(5), 182-183. doi: 10.31031/FSAR.2018.03.000554

Conway, M. O. H. (2015). Taking stock and making hay: Archival collections assessment. J. Michalko (Ed.), *Making archival and special collections more accessible* içinde (s. 17-39). Dublin: OCLC Research.

Davenport, T. H. ve Prusak, L. (2000). *Working knowledge: How organizations manage what they know*. Boston: Harvard Business Review Press.

Dursun, S. A. (2008). *Borçlar Hukukunda hakimin sözleşmeyi tamamlaması* (Yayımlanmamış Doktora tezi). İstanbul Üniversitesi, İstanbul. Retrieved from

https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=wBmNpkQC9Nhi90NLW7E7-dTxxRiDxyYLewLAgjV-4tAtb_KWKO0a_TPlaxs8npu1

ETSI. (2002). ETSI TS 102 023: Policy requirements for time-stamping authorities. Erişim adresi: https://www.etsi.org/deliver/etsi_ts/102000_102099/102023/01.01.01_60/ts_102023v010101p.pdf

European Commission. (2019a). A definition of AI: Main capabilities and disciplines. Erişim adresi: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60651

European Commission. (2019b). Ethics guidelines for trustworthy AI. Erişim adresi: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

EY. (2018). Managing integrity risks with AI: Enabled by EY virtual analytics infrastructure. Erişim adresi: https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/assurance/assurance-pdfs/ey-forensics-managing-integrity-risks-with-ai-enabled-by-ey-virtual-analytics-infrastructure.pdf

Ganesan, R. (2019). Data integrity key to a secure, AI-driven enterprise - ManageEngine. Erişim adresi: https://itbrief.com.au/story/data-integrity-key-to-a-secure-ai-driven-enterprise-manageengine

Google. (2019). Perspectives on Issues in AI Governance. Erişim adresi: https://ai.google/static/documents/perspectives-on-issues-in-ai-governance.pdf

Gringras, C., Stevens, I., Tench, D. ve Free, R. (2019). Integrity and transparency: Ethical considerations for the evolving AI landscape. Erişim adresi: https://cms.law/en/GBR/Publication/Integrity-and-transparency

Hey, J. (2004). The data, information, knowledge, wisdom chain: The metaphorical link. Erişim adresi: http://www.dataschemata.com/uploads/7/4/8/7/7487334/dikwchain.pdf

IRIS. (2017). How can artificial intelligence affect courts? Erişim adresi: http://irisbh.com.br/en/how-can-artificial-intelligence-affect-courts/

Karliuk, M. (2018). The ethical and legal issues of artificial intelligence. *RIAC*. Erişim adresi: https://russiancouncil.ru/en/analytics-and-comments/analytics/the-ethical-and-legal-issues-of-artificial-intelligence/

Laudon, K. C. ve Laudon, J. P. (2014). *Management information systems: Managing the digital firm* (13 bs.). London: Pearson Education Limited.

McDermott, R. (1999). Why information technology inspired but cannot deliver knowledge management. *California Management Review, 41*(4), 104-119. Erişim adresi: http://www.moderntimesworkplace.com/good_reading/GRKnowledgeWork/IT___Knowledge_Management.McDermott.1999.pdf

Rolan, G., Humphries, G., Jeffrey, L., Samaras, E., Antsoupova, T. ve Stuart, K. (2019). More human than human? Artificial intelligence in the archive. *Archives and Manuscripts, 47*(2), 179-203. doi: 10.1080/01576895.2018.1502088

Rowley, J. (2007). The wisdom hierarchy: representations of the DIKW hierarchy. *Journal of Information Science, 33*(2), 163-180. Erişim adresi: https://journals.sagepub.com/doi/abs/10.1177/0165551506070706?casa_token=FIHTYDa3zsMAAAAA%3AJJqMuTL6xr9NaR81g1R1jGicPFD9yh7I1qFYGM4j2VFV2B4fZPutDTdMEuIF5F9TfjHZdLTQxm63&

Tomek, M. (2019). 5 Challenges automation rates face today within RPA projects. Erişim adresi: https://www.minit.io/blog/explore-the-true-value-of-automation-rates-and-associated-challenges-in-rpa

UK National Archives. (2017). Digital strategy. Erişim adresi: https://www.nationalarchives.gov.uk/documents/the-national-archives-digital-strategy-2017-19.pdf

UNCITRAL. (2007). *United Nations Convention on the Use of Electronic Communications in International Contracts*. New York: United Nations Publication.

Villaronga, E. F., Kieseberg, P. ve Li, T. (2018). Humans forget, machines remember: Artificialintelligence and the Right to Be Forgotten. *Computer Law & Security Review, 34*(2), 304-313. doi: 10.1016/j.clsr.2017.08.007

Wolf, K. (2019). AI, data integrity, & the life sciences: Let's not wait until someone dies. Erişim adresi: https://www.pharmaceuticalonline.com/doc/ai-data-integrity-the-life-sciences-let-s-not-wait-until-someone-dies-0001

Yargıtay. (2015). *T.C. Yargıtay 8. Ceza Dairesi, Bilişim Suçu, Esas No:2014/29566, Karar No:2015/13421*.