DİJİTALLEŞME DÖNÜŞÜM VE DENETİM

Editör
Doç. Dr. Recai AKYEL

T.C. Sayıştay Başkanlığı

DİJİTALLEŞME DÖNÜŞÜM VE DENETİM

Editör
Doç. Dr. Recai AKYEL

Ankara, 2026

Editör
Doç. Dr. Recai AKYEL

Grafik Tasarım
Tahir SÜLEK

ISBN: 978-975-7590-55-2

İÇİNDEKİLER

DİJİTALLEŞME DÖNÜŞÜM VE DENETİM

SUNUŞ

Kamuda hesap verme sorumluluğu ve mali saydamlığa katkı sağlamak üzere denetim, yargılama ve rehberlik görevini yürüten Sayıştayımız, köklü tarihinden aldığı birikimle sürekli yenilenen ve gelişen bir kurum olma vizyonunu benimsemektedir. Bu birikimi, her kuruluş yıl dönümümüzde çeşitli etkinlik ve faaliyetlerle anıyoruz. Bu kapsamda, 164. kuruluş yıl dönümümüzü de 1-3 Haziran 2026 tarihlerinde, geniş bir katılımla gerçekleştirdiğimiz çeşitli programlarla kutladık.

Bu kutlamaları, aynı zamanda çağımızın en belirleyici gündem maddelerinden biri olan dijitalleşmeyi ve onun kamu yönetimine ve denetime olan yansımalarını ele almak için bir vesile olarak değerlendirdik.

Dijital teknolojilerdeki gelişmeler, kamu yönetiminden hizmet sunumuna, karar alma süreçlerinden denetim anlayışına kadar pek çok alanda köklü bir dönüşüme yol açmaktadır. Bu dönüşüm, yalnızca fırsatlar değil, özenle ele alınması gereken yeni sorumluluk alanlarını da beraberinde getirmektedir. Yapay zekâ, bulut bilişim, büyük veri analitiği ve blok zinciri gibi teknolojilerin yaygınlaşması;

veri güvenliği, kişisel verilerin korunması ve dijital hesap verebilirlik gibi konuları kamu yönetiminin ve denetim camiasının gündeminin merkezine taşımaktadır. Bu dönüşümün sağlıklı bir zeminde yönetilebilmesi, hiç şüphesiz, teknik olduğu kadar hukuki ve kurumsal boyutlarıyla da ele alınması gereken çok yönlü bir çabayı gerektirmektedir.

Anayasa Mahkemesi Üyesi ve Sayıştay Onursal Başkanı Doç. Dr. Recai AKYEL'in editörlüğünde hazırlanmış olan bu kitapta; dijitalleşmenin kamu yönetimi, finansal sistemler, kişisel verilerin korunması ve denetim üzerindeki dönüştürücü etkisi ayrıntılı şekilde ele alınmaktadır.

Bilgi ve tecrübeleriyle bizleri aydınlatan değerli yazarlara ve bu kitabın basımında emeği geçen mensuplarımıza teşekkürlerimi sunuyor, bu kıymetli eserin kamu yönetimi ve denetim camiası için faydalı bir kaynak olmasını temenni ediyorum.

DOÇ. DR. RECAİ AKYEL
Anayasa Mahkemesi Üyesi

ÖNSÖZ

Fiziksel biçimdeki bilgi, belge ve iş süreçlerinin bilgisayarlar, internet, bulut bilişim gibi dijital teknolojiler aracılığıyla elektronik ortama aktarılması ve işlenmesi süreci olarak tanımlayabileceğimiz dijitalleşme hızla ilerlemektedir.

Kağıt kullanımını azaltarak zamandan tasarruf sağlayan, veri yönetimini kolaylaştıran dijitalleşmeye kamu kurumları gerekli önemi vermelidir. Devlet dijitalleşme konusunda pozitif yükümlülüğünü ve negatif yükümlülüğünü yerine getirmelidir.

Ülkemizde dijitalleşmenin ne durumda olduğu, nasıl olması gerektiği hususunda değişik kurumlarda kendi görev alanları ile ilgili çalışmalar sürdürülmektedir. Dijitalleşme konusuna dikkat çekmek ve bilgilendirmek amacıyla bu kitap hazırlanmıştır.

Dijitalleşme Dönüşüm ve Denetim Ana Başlıklı bu kitap beş bölümden oluşmaktadır. Her bir bölüm alanında bilgili ve birikimli beş ayrı meslektaşım tarafından yazılmıştır.

Birinci bölümde; dijital teknolojilerin dönüştürücü gücü; dijital devlet ve yansımaları hususunda bilgiler sunulmuştur.

İkinci bölümde; dijital teknolojilerin finansı dönüştürücü etkisi ve finansın geleceği konusunda bilgiler aktarılmıştır.

Üçüncü bölümde; siber güvenlik ihlalleri sebebiyle kişisel verilerin korunmasında Devletin pozitif yükümlülüğünün nasıl olduğu açıklanmıştır.

Dördüncü bölümde; Dijitalleşen denetim ortamında stratejik risk yönetimi, kurumsal dayanıklılık ve yeni nesil denetim konusunda anlatımda bulunulmuştur.

Beşinci bölümde; dijital ekosistemde Sayıştayların dönüşen rolleri: geleneksel denetim anlayışının ötesine geçişin kavramsal ve pratik çerçevesi çizilmeye çalışılmıştır.

T.C. Sayıştayının 164. Kuruluş yıldönümü kutlama faaliyetleri çerçevesinde; dijitalleşme konusunda farkındalık oluşturma amacıyla hazırlanan bu kitabın bölümlerini yazan değerli yazarlara; kitabın basımını yapması nedeniyle Sayıştay Başkanı Metin YENER'e teşekkür ediyorum.

DİJİTAL TEKNOLOJİLERİN DÖNÜŞTÜRÜCÜ GÜCÜ: DİJİTAL DEVLET VE YANSIMALARI

Dr. Ecem Buse SEVİNÇ ÇUBUK
Kıdemli Uzman
T.C. Cumhurbaşkanlığı Siber Güvenlik Başkanlığı

Dr. Atilla AYDIN
Dijital Devlet Düzenlemeleri Daire Başkanı
T.C. Cumhurbaşkanlığı Siber Güvenlik Başkanlığı

ÖZET

Bilgi ve iletişim teknolojilerindeki hızlı gelişmeler, devletlerin kamu hizmetlerini üretme ve yönetme biçimlerinde köklü değişimlere yol açarak geleneksel bürokratik yapıyı stratejik bir dijital devlet modeline dönüştürmüştür. Süreç içerisinde kurumsal otomasyon ve e-devlet uygulamalarından veri odaklı yönetişim, yapay zekâ destekli karar mekanizmaları ve GovTech yaklaşımını içeren modern bir devlet yapısına geçilmiştir. Çalışmanın odak noktası, teknolojik modernizasyonun ötesine geçen bu çok boyutlu kurumsal paradigma değişimini kapsamlı bir biçimde ortaya koymaktadır. Çalışma kapsamında, Türkiye'nin e-Devlet Kapısı ve ulusal bilgi sistemleri ile elde ettiği başarılar uluslararası gelişmeler ışığında incelenmekte ve yeni dönemin veri yönetişimi, dijital ortak hizmetleri, yapay zekâ ve hizmet inovasyonu gibi öncelikleri tartışılmaktadır. Son olarak bu çalışma, dijital devlet modelinin kamu denetimi üzerindeki potansiyel etkilerini ve devletin yeniden tanımlanan işleyiş mantığını teorik ve pratik boyutlarıyla ortaya koymaktadır.

Anahtar Kelimeler: *Dijital Devlet, Dijital Dönüşüm, e-Devlet, Yapay Zekâ, GovTech*

ABSTRACT

Rapid advancements in information and communication technologies have led to fundamental changes in the way governments deliver and manage public services, transforming the traditional bureaucratic structure into a strategic digital government model. Over time, there has been a transition from institutional automation and e-government applications to a modern government structure that incorporates data-driven governance, artificial intelligence-supported decision-making mechanisms, and the GovTech approach. The focus of this study is to comprehensively elucidate this multidimensional shift in the institutional paradigm, which goes beyond mere technological modernization. Within the scope of the study, Türkiye's achievements through its e-Government Portal and national information systems are examined in light of international developments, and the priorities of the new era—such as data governance, digital shared services, artificial intelligence, and service innovation—are discussed. Finally, this study examines the potential impacts of the digital government model on public oversight and elucidates the state's redefined operational logic from both theoretical and practical perspectives.

Keywords: *Digital Government, Digital Transformation, e-Government, Artificial Intelligence, GovTech*

GİRİŞ

Bilgi ve iletişim teknolojilerinde yaşanan hızlı gelişmeler, devletlerin kamu hizmetlerini üretme, sunma ve yönetme biçimlerinde köklü değişimlere yol açmıştır. Başlangıçta yalnızca bürokratik süreçlerin otomasyonu amacıyla kullanılan bilişim teknolojileri, zaman içerisinde kamu yönetiminin örgütlenme yapısını, karar alma mekanizmalarını ve vatandaşlarla kurduğu ilişkiyi yeniden şekillendiren stratejik bir dönüşüm unsuruna dönüşmüştür. Günümüzde dijital dönüşüm, kamu hizmetlerinin elektronik ortama taşınmasının ötesinde; verinin stratejik bir kamu varlığı olarak yönetildiği, kurumlar arasında birlikte çalışabilirliğin sağlandığı, yapay zekâ destekli karar mekanizmalarının geliştirildiği ve kamu değerinin dijital teknolojiler aracılığıyla üretildiği yeni bir devlet modelini ifade etmektedir.

Bu dönüşüm süreci, dijital teknolojilerin gelişimine paralel olarak farklı evrelerden geçmiştir. İlk aşamada bilgisayar teknolojileri kamu kurumlarında işlem kapasitesini artıran teknik araçlar olarak kullanılmış; internet teknolojilerinin yaygınlaşmasıyla birlikte e-devlet uygulamaları gelişmiş ve kamu hizmetleri çevrim içi ortama taşınmıştır. Son yıllarda ise büyük veri, yapay zekâ, bulut bilişim, nesnelerin interneti ve platform teknolojilerinin gelişmesiyle birlikte dijital devlet anlayışı daha bütüncül bir yapıya evrilerek hizmet sunumunun ötesinde veri odaklı yönetişim, kamu değeri üretimi ve proaktif kamu hizmetleri ön plana çıkmıştır. Bu doğrultuda uluslararası kuruluşlar nezdinde kurumsal otomasyon olarak başlayan, e-devlet olarak şekillenen süreç, zaman içerisinde dijital devlet yaklaşımıyla kabuk değiştirmiş ve son yıllarda GovTech perspektifiyle genişletilmiştir. Mevcut haliyle kamunun dijital dönüşümü, teknolojik modernizasyon sürecini aşarak kamu sektörünün kurumsal dönüşümünü hedefleyen ve dijital ekonominin kolaylaştırıcısı olan yeni bir paradigma olarak ele alınmıştır.

Türkiye de bu küresel dönüşüm sürecine erken dönemde uyum sağlayarak özellikle son yirmi yılda dijital devlet alanında önemli ilerlemeler kaydetmiştir. Özellikle e-Devlet Kapısı, ulusal bilgi sistemleri, dijital kimlik altyapıları ve birlikte çalışabilirlik mekanizmaları sayesinde güçlü bir dijital kamu altyapısı

oluşturulmuş; uluslararası endekslerde kayda değer başarılar elde edilmiştir. Bununla birlikte; dijital devlet olgunluğunun artırılması, veri yönetişiminin güçlendirilmesi, yapay zekâ destekli kamu hizmetlerinin yaygınlaştırılması ve kamu değerinin dijital teknolojiler aracılığıyla sürdürülebilir biçimde üretilmesi, Türkiye açısından yeni dönemin temel öncelikleri arasında yer almaktadır.

Bu bölümde, öncelikle devletin dijital dönüşümünün tarihsel gelişimi ele alınmakta; analog devletten dijital devlete uzanan paradigma değişimi açıklanmaktadır. Ardından Türkiye'nin dijital devlet dönüşümü uluslararası gelişmeler ışığında değerlendirilmekte ve dijital devletin kamu değeri üretimine katkısı tartışılmaktadır. Son olarak, bu dönüşümün kamu denetimi üzerindeki potansiyel etkileri tartışılmaktadır. Böylece, dijital devletin yalnızca yeni teknolojilerin kamu sektöründe kullanılması değil; devletin işleyiş mantığını yeniden tanımlayan çok boyutlu bir dönüşüm süreci olduğu ortaya konulmaktadır.

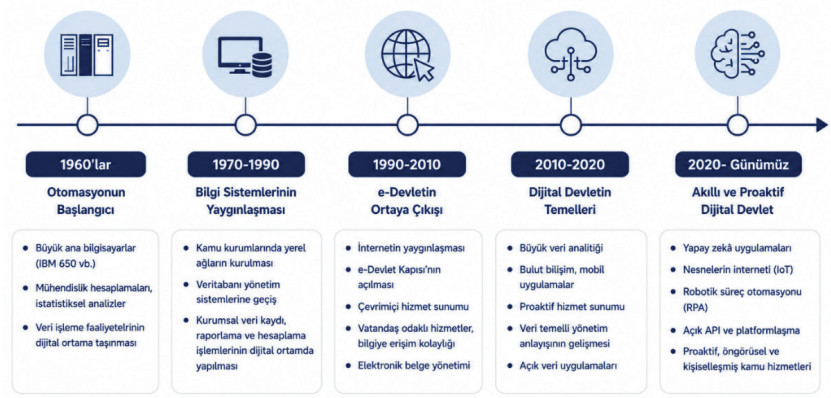
I. DİJİTAL DEVLETİN TARİHSEL EVRİMİ

Devlet; kamu politikalarının oluşturulması ve uygulanmasının yanı sıra, kamu hizmetlerinin planlanması, organize edilmesi, yönlendirilmesi, koordine edilmesi ve denetlenmesi gibi çok boyutlu işlevleri yerine getiren kurumsal bir yapıdır. Bu kapsamda devlet, eğitim, sağlık, güvenlik, adalet ve altyapı gibi temel kamu hizmetlerini belirli bir idari mekanizma içerisinde sunarak toplumsal düzenin sürdürülmesini sağlamaktadır.

Geleneksel devlet anlayışında bu hizmetler büyük ölçüde bürokratik, hiyerarşik ve yüz yüze etkileşime dayalı süreçler aracılığıyla yürütülmüştür (Okçu vd., 2020: 292). Ancak artan nüfus, karmaşıklaşan toplumsal ihtiyaçlar, hızlanan ekonomik ve sosyal yaşam ile vatandaş beklentilerindeki değişim, kamu hizmetlerinin daha etkin, erişilebilir ve vatandaş odaklı bir biçimde sunulmasını zorunlu hâle getirmiştir (OECD, 2026: 10). Bu noktada, devletlerin örgütlenme biçimlerinin, toplumsal ihtiyaçlar kadar teknolojik gelişmeler tarafından da şekillendirildiğini söylemek yanlış olmayacaktır. Yazının icadı, matbaanın yaygınlaşması, telgraf ve telefon gibi iletişim teknolojileri farklı dönemlerde devletlerin idari kapasitesini artırmış; kamu otoritesinin daha geniş coğrafyalarda

etkin biçimde kullanılmasına imkân sağlamıştır. Ancak yirminci yüzyılın ikinci yarısından itibaren bilişim teknolojilerinde yaşanan gelişmeler, önceki teknolojik dönüşümlerden farklı olarak devletin yalnızca kullandığı araçları değil, karar alma süreçlerini, hizmet üretim yöntemlerini ve kurumsal yapısını doğrudan dönüştürmeye başlamıştır.

Bilişim teknolojileri, devletin kurumsal kapasitesinin güçlendirilmesi ve kamu hizmetlerinin dönüştürülmesinde kritik bir araç olarak ortaya çıkmaktadır. Bilginin hızlı işlenmesi, saklanması ve paylaşılmasını mümkün kılan bu teknolojiler, kamu kurumlarının karar alma süreçlerini daha veriye dayalı hâle getirirken, hizmet sunumunu da mekân ve zaman sınırlamalarından büyük ölçüde bağımsızlaştırmaktadır. Böylece dijital teknolojiler ile devlet arasındaki etkileşim, teknik bir bütünleşmenin ötesinde devletin işleyiş anlayışının yeniden şekillenmesini de ifade etmektedir.



Şekil 1. Teknolojinin Tarihsel Akışı ile Devletin Dijital Dönüşümü

Kaynak: Yazarlar tarafından oluşturulmuştur.

Bugün dijital teknolojilerin sunduğu imkânlar sayesinde devlet, yalnızca kamu hizmetlerini daha hızlı, şeffaf ve vatandaş odaklı sunan bir yapıya dönüşmemekte; aynı zamanda veriyi stratejik bir kaynak olarak kullanan, kurumlar arasında bütünleşik

çalışabilen ve politika geliştirme süreçlerini dijital teknolojilerle destekleyen yeni bir yönetim modeline evrilmektedir. Bu dönüşüm doğrusal bir süreçten ziyade birbirini tamamlayan aşamalar halinde gerçekleşmiştir. İlk aşamada bilgisayar teknolojileri kamu kurumlarında rutin hesaplama ve veri işleme faaliyetlerini destekleyen teknik araçlar olarak kullanılmıştır. Zamanla bilgi sistemlerinin yaygınlaşmasıyla birlikte kamu kurumları dijital kayıt sistemleri geliştirmiş, internetin yaygınlaşması kamu hizmetlerinin çevrim içi ortama taşınmasını mümkün kılmış ve e-devlet anlayışı ortaya çıkmıştır. Günümüzde ise dijital dönüşüm yalnızca hizmetlerin elektronik ortama aktarılmasını değil; verinin stratejik bir kamu kaynağı olarak yönetildiği, kurumlar arasında bütünleşik dijital mimarilerin kurulduğu ve yapay zekâ destekli karar mekanizmalarının geliştirildiği yeni bir devlet modelini ifade etmektedir. Bu tarihsel gelişimi beş temel dönem altında incelemek mümkündür (Şekil 1).

Aradan geçen yarım asır sonra gelişen teknoloji ve kurumların uyum süreci doğrultusunda, kamu bilişim sistemlerinin sayısının artması, yürütülen hizmet süreçlerinin çeşitlenmesi ve etkinlik alanının artmasıyla kamu bilişim sistemleri, bilgi işlem birimleri ve bilişim personeli tüm kurumlarımızda vaz geçilemez bir verimlilik ve etkinlik unsuru olarak yer alır hale gelmiştir.

A. Otomasyonun Başlangıcı (1960'Lı Yıllar)

Devletin dijitalleşme yolculuğunun ilk evresi, büyük ölçekli ana bilgisayarların (*mainframe*) kamu kurumlarında kullanılmasıyla başlamıştır. Bu dönemde bilgisayarlar ağırlıklı olarak mühendislik hesaplamaları, istatistiksel analizler ve yoğun veri işleme faaliyetlerinde kullanılmaktadır. Türkiye'de bu sürecin en önemli örneklerinden biri Karayolları Genel Müdürlüğünde kullanılan IBM 650 bilgisayarıdır (Şekil 2). Bu sistem, Avrupa'da ilklerden biri olarak, delikli kartlar aracılığıyla veri girişinin yapıldığı, büyük hacimli ve operatör kontrollü bir yapıya sahip olup, kamu yönetiminde dijital dönüşümün ilk adımını temsil etmektedir.

Şekil 2. Türkiye'nin İlk Bilgisayarı IBM 650

"Elektronik Beyin" olarak adlandırılan IBM 650 Model I adını taşıyan bu sistem, o tarihlerde sadece Türkiye'nin değil, Balkanlar ve Ortadoğu'nun da ilk bilgisayarı olma özelliğini taşımış ve karayolları çalışmalarının modernize edilmesi amacıyla kullanılmıştır (KGM, t.y.). Ankara Balgat'ta bulunan yonca yaprağı tabir edilen kavşağın hesaplamaları IBM 650 ile gerçekleştirilmiştir. Yeni teknolojilerin kamuda iş görme usullerine dâhil edilmesiyle birlikte; bu teknolojileri kullanan yeni roller de oluşmuştur. Bu kapsamda, Türkiye'nin ilk bilgisayar programcısı, Karayolları Genel Müdürlüğü'nün "Elektronik Hesap Makineleri Müdürlüğü" adıyla hizmet veren Türkiye´nin ilk bilgi işlem biriminde çalışmıştır.

Bu dönemde bilişim teknolojileri, mevcut bürokratik süreçleri köklü biçimde dönüştürmekten ziyade, onları hızlandıran ve destekleyen bir araç olarak kullanılmıştır. Veri kayıtlarının fiziksel ortamlardan dijital/elektronik ortama aktarılması, işlem sürelerinin kısalması ve hata oranlarının azalması gibi önemli kazanımlar sağlanmış olsa da sistemler hâlâ yüksek düzeyde insan müdahalesine bağımlı kalmıştır. Bu nedenle söz konusu dönem, tam anlamıyla dijitalleşmeden ziyade "otomasyonun başlangıç aşaması" olarak değerlendirilmektedir.

B. Bilgi Sistemlerinin Yaygınlaşması (1970–1990)

Bilgisayar teknolojilerindeki gelişmeler, kamu kurumlarında bilgi sistemlerinin yaygınlaşmasını beraberinde getirmiştir. Kurumsal veri tabanları oluşturulmuş, elektronik kayıt sistemleri geliştirilmeye başlanmış ve özellikle nüfus, personel, vergi ve mali yönetim gibi yoğun bilgi işleme gerektiren alanlarda dijital uygulamalar kullanılmaya başlanmıştır. Bu dönemde temel amaç, kamu hizmetlerini dönüştürmekten ziyade bürokratik süreçlerin daha hızlı, doğru ve düşük maliyetle yürütülmesini sağlamaktır. Örneğin; 1970'li yıllarda bilgisayarlar, ücret bordrolarının hazırlanması, ambar hesapları, maliyet muhasebesi ve stok kontrolü gibi alanlarda kullanılarak sınırlı alandaki hesaplamaları daha verimli hale getirmiştir (Polatoğlu, 1994: 77). Başka bir ifadeyle teknoloji, kamu yönetiminin karar alma süreçlerinden çok idari operasyonlarını destekleyen bir unsur niteliğindedir.

Bununla birlikte, artan işlem hacmi mevcut bilgi sistemlerinin kapasitesini zorlamaya başlamıştır. Örneğin, ABD Gelir İdaresi (*Internal Revenue Service*-IRS), artan işlem yükünü karşılamak amacıyla 1985 yılında *Service Center Replacement System* programını devreye almıştır. Ancak sistemin yetersiz bilgisayar kapasitesi, vergi beyannamelerinin zamanında işlenmesini engellemiş ve 1985 yılı IRS tarihinde "en kötü beyanname dönemi" olarak anılmıştır. Buna rağmen yaşanan bu deneyim, kurumun bilgi sistemlerini kapsamlı biçimde modernize etmesine yönelik yeni yatırımların ve reformların önünü açmıştır (Internal Revenue Service, 1996: 215).

Bu dönemin önemli bir yansıması gerçek ve tüzel kişiler ile varlık yönetimi yapılan envanterlere yönelik bilgi teknolojilerine uygun bir yaklaşım ile kimlik, vergi, tescil numarası gibi tekil numaralar verilmesidir.

C. E-Devletin Ortaya Çıkışı (1990–2010)

İnternet teknolojilerinin gelişmesi ve son kullanıcılara yönelik cihazların ortaya çıkmasıyla birlikte devletin dijital dönüşümünde yeni bir dönem başlamıştır. Bunun üzerine, 1990'ların başında kamu sektörü bilgi ve hizmet sunmak için elektronik posta (e-posta), *listserv* (ticari e-posta yönetim sistemi) ve *World Wide Web*'i kullanmaya başlamıştır. 1990'ların sonuna gelindiğindeyse,

internet tabanlı hizmetler "e-devlet" girişiminin çoktan ayrılmaz ve önemli bir parçası haline gelmiştir (Ho, 2002: 434). Bu dönemde, e-hizmetlerin hayata geçirilmesine yönelik modellerin oluşturulması eğilimi öne çıkmıştır. Söz konusu modeller, geleneksel hiyerarşiden e-hizmet temelli bir sisteme; bütünleşik ve standartlaştırılmış bir biçimde geçiş yapılmasına katkı sağlamıştır (Bindu, Sankar ve Kumar, 2019: 388).

Kamu hizmetleri ilk kez vatandaşların doğrudan erişebileceği çevrim içi platformlara taşınmış; elektronik belge yönetimi, çevrim içi başvuru sistemleri ve dijital hizmet portalları yaygınlaşmıştır. Ekonomik İş Birliği Kalkınma Teşkilatı (OECD) 2003 yılında yayınladığı raporda; e-devleti, bilgi ve iletişim teknolojilerinin, özellikle de internetin, daha iyi bir yönetim elde etme aracı olarak kullanılması şeklinde tanımlamış; bu sürecin şeffaflık, hesap verebilirlik ve hizmet kalitesi üzerinde olumlu etkiler yarattığını vurgulamıştır.

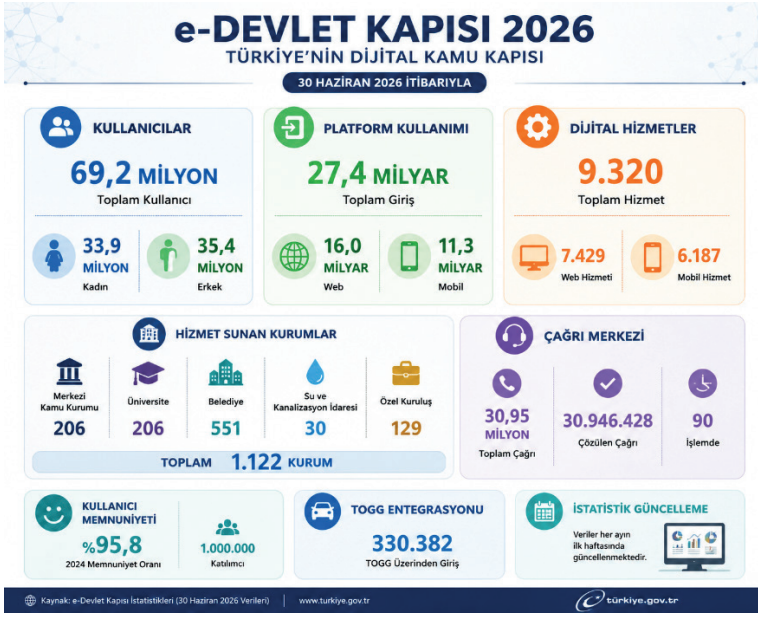
Küresel eğilimlerle paralel olarak; Türkiye'de kamu yönetiminin dijitalleşme vizyonu, 1993 yılında Dünya Bankası ile gerçekleştirilen iş birliği neticesinde somutlaşmaya başlamıştır. Bu dönemde hazırlanan "Bilişim ve Ekonomik Modernizasyon Raporu", kamu sektöründe bilişim teknolojilerinin sadece bir araç değil, ekonomik kalkınmanın ve verimliliğin anahtarı olduğunu vurgulamıştır. E-devlet kavramını çağrıştıran bir ifadenin ilk kez bir kamu politikası metninde kullanımı ise Sekizinci Beş Yıllık Kalkınma Planında (2001-2005) "Kamu Hizmetlerinde Etkinliğin Artırılması" başlığı altında yer bulmuştur. Planın 1844. Paragrafında;

"*Kurum içerisinde düzenli ve süratli bilgi akışı ile işlemlerde basitliğin sağlanabilmesi ve kurumlarda kırtasiyeciliği önleme, evrak, dosyalama ve arşiv sorunlarına köklü çözümler getirmek amacıyla her kurumda Elektronik Bilgi yönetimine önem verilecektir*." politikası yer almaktadır.

E-devlet kavramı ilk kez 2002 Yılı Programında bir kamu politikası metninde "Bilgi ve İletişim Teknolojileri" başlığı altında aşağıdaki paragraflarda yer bulmuş; "*e-Devlet kurma sürecinde, sosyal güvenlik bilgi sistemi, vatandaşlık numarası, vergi numarası gibi diğer bilgi sistemleriyle uyumlu çalışacak bir şekilde tasarlanacaktır*", ifadesine yer everilmiştir (SBB; 2023: 9).

Dokuzuncu Kalkınma Planında (2007-2013) ise e-devlet kavramı ilk kez "Kamu Hizmetlerinde Kalite ve Etkinliğin Artırılması" başlığı altında, bir kalkınma planı metninde münhasır bir alt başlık olarak "e-Devlet Uygulamalarının Yaygınlaştırılması ve Etkinleştirilmesi" şeklinde yer almıştır.

Türkiye'de e-devlet dönüşümünün uygulama alanında en önemli kilometre taşlarından biri ise 2008 yılında e-Devlet Kapısı'nın hayata geçirilmesi olmuştur. Vatandaşların çok sayıda kamu hizmetine tek bir dijital platform üzerinden erişimine olanak sağlayan e-Devlet Kapısı, kamu hizmetlerinin sunumunda zaman ve mekân sınırlamaları önemli ölçüde ortadan kalkmıştır.



Şekil 3. 30 Haziran 2026 itibariyle e-Devlet Kapısı İstatistikleri

E-Devlet Kapısı, Türkiye'de dijital kamu hizmetlerinin en yaygın kullanılan (Şekil 3) altyapılarından biri haline gelmiştir. Sistem bugün 69 milyon kullanıcıya ulaşmış durumdadır. Kullanım yoğunluğu açısından değerlendirildiğinde, e-Devlet Kapısı'na yapılan toplam giriş sayısı 27 milyarın üzerinde olup, bunun önemli bir kısmı web üzerinden gerçekleşirken, 11 milyardan

fazla girişin mobil cihazlar aracılığıyla yapılması dikkat çekmekte; mobil erişimin kamu hizmetlerinde giderek daha merkezi bir rol oynadığı görülmektedir.

Bu dönemde son kullanıcıya ilk önce bilgi almaya yönelik sunulan internet erişimli hizmetler zaman içerisinde gerçek ya da tüzel kişinin durumunda değişikliğin resmi olarak uzaktan yapılabildiği işlemsel hizmetlere evrilmiştir. İşlemsel hizmetleri sunabilmek için kritik olan çevrim içi kimlik doğrulama amacıyla e-imza ve çipli kimlik kartı gibi güven tesis edecek teknolojiler yaygınlaşmaya başlamıştır. Bu gelişmelerin doğal sonucu olarak adli olayların son kullanıcılara yönelik bilişim sistemlerine yansımasıyla siber güvenliğin sağlanması kamu yönetiminin sorumlulukları kapsamına girmiştir. Bu dönemde e-devlet çalışmalarına yön veren kamu yönetimi ilkeleri vatandaş odaklılık ve hizmet etkinliği olmuştur.

D. Dijital Devletin Temelleri (2010–2020)

Bu dönemde dijitalleşme, hizmetlerin elektronik ortama taşınmasının ötesine geçerek devletin kurumsal kapasitesini yeniden şekillendirmeye başlamıştır. Bu doğrultuda, "dijital devlet" yaklaşımı, e-devlet anlayışının ötesine geçerek daha bütüncül, veri temelli ve vatandaş odaklı bir yönetim modelini ifade etmek için kullanılmıştır. Alan yazında e-devlet ve dijital devlet kavramlarını aynı kavramsal zeminde kullanan çalışmalar olmakla birlikte (Demirel, 2006: 84); e-devlet yaklaşımı ağırlıklı olarak mevcut kamu hizmetlerinin dijital kanallar üzerinden sunulmasına odaklanırken, dijital devlet yaklaşımı teknolojiyi devletin politika geliştirme, karar alma, kurumsal koordinasyon ve kamu değeri üretme süreçlerinin ayrılmaz bir parçası olarak ele almaktadır (OECD, 2014).

Bu dönemin en belirgin özelliklerinden biri, verinin kamu yönetiminde stratejik bir kaynak olarak görülmeye başlanmasıdır. Büyük veri analitiği (*big data analytics*), bulut bilişim (*cloud computing*), mobil teknolojiler ve kurumlar arası veri paylaşım mekanizmaları dijital devlet yaklaşımının temel bileşenleri hâline gelmiştir. Kamu kurumları yalnızca dijital hizmet sunan organizasyonlar olmaktan çıkarak ortak veri altyapıları üzerinden

çalışan, birlikte çalışabilir (*interoperable*) ve bütünleşik yapılara dönüşmeye başlamıştır. Böylece farklı kamu kurumlarında tutulan verilerin ortak standartlar çerçevesinde paylaşılması ve yeniden kullanılması mümkün hâle gelmiş; bu durum hem hizmet sunumunda mükerrer veri girişlerini azaltmış hem de politika geliştirme süreçlerinde daha bütüncül analizlerin yapılabilmesine olanak sağlamıştır (Ubaldi, 2013: 22).

Bu dönüşüm sürecinde açık veri (*open data*) ve veri yönetişimi (*data governance*) kavramları da kamu yönetiminin temel gündemlerinden biri hâline gelmiştir. Açık veri yaklaşımı, kamu kurumlarının ürettiği verilerin yeniden kullanılabilir formatlarda kamuoyu, akademi ve özel sektörle paylaşılmasını teşvik ederek şeffaflığın, hesap verebilirliğin ve veri temelli yenilikçiliğin geliştirilmesini amaçlamaktadır (Janssen, Charalabidisve Zuiderwijk, 2012: 260). Açıklık ilkesi, dijital verinin en önemli özelliklerinden birini değiştirerek onu dışlanamaz (*non-excludable*) bir kaynak hâline getirmektedir. Bu sayede dijital veriler, paylaşılan bir kaynak; başka bir ifadeyle kamusal bir mal veya literatürde ifade edildiği şekliyle bir "dijital varlık" niteliği kazanmaktadır (Jetzek, Avital ve Bjorn-Andersen, 2014: 102). Bunun yanında veri yönetişimi; verinin üretilmesi, saklanması, paylaşılması, güvenliği, kalitesi ve etik kullanımına ilişkin kurumsal politika ve mekanizmaları kapsayan stratejik bir yönetim alanı olarak öne çıkmaktadır. Bu gelişmeler, devletlerin yalnızca veri üreten kurumlar olmaktan çıkarak veriyi yöneten ve değer üreten organizasyonlara dönüşmesini sağlamıştır.

Verinin kamu yönetimindeki stratejik öneminin artışıyla birlikte, ulusal düzlemde de konuyla ilgili düzenlemelere gidilmeye başlanmıştır. 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun (KVKK) 2016 yılında yürürlüğe girmesi ile e-devletin en hassas noktaları arasında yer alan "güven" ve "mahremiyet" konuları kanunla hukuksal bir korumaya alınmıştır. Hukuki güvence sağlanarak, vatandaşların kamu kurumlarıyla paylaştığı dijital verilerin (kimlik, sağlık, finans vb.) hangi şartlarda işlenebileceği ve korunacağı netleşmiştir. E-devletin ön şartı olarak "verinin

dijitalleşmesi" ile "kişi haklarının korunması" arasındaki denge kurulmak istenmiştir. Kişisel Verileri Koruma Kurumu kurularak, kamu ve özel sektörün veriyi işleme biçimleri denetim altına alınmıştır.

Dijital devletin temel bileşenlerinin olgunlaşması ve verinin stratejik bir kamu kaynağı hâline gelmesi, dijital dönüşüm sürecinin yeni bir aşamaya taşınmasını sağlamıştır. İlerleyen dönemlerde, dijital teknolojiler aracılığıyla kamu hizmetlerinin öngörülebilir, kişiselleştirilmiş ve proaktif bir yapıya dönüştürülmesi mümkün hale gelmiştir. Dijital hizmet sunumunda uçtan uca son kullanıcının deneyimini önceliklendiren, kurumlar üstü bir anlayış söz konusu olmaya başlamıştır.

Bu dönemde artan mobil cihaz kullanımı ve özel sektörün sunduğu dijital hizmetlerin yaygınlaşması mevcut hizmetlerde sunum kanallarını çeşitlendirmiştir. Farklı paydaşların süreçlere dahil olmasıyla yönetişim ve etkileşim kavramları dijital devlet çalışmalarında ön plana çıkmıştır.

F. Akıllı ve Proaktif Dijital Devlet (2020 Ve Sonrası)

Veri altyapısının güçlendirilmesi, kurumlar arası dijital entegrasyonun geliştirilmesi ve veri yönetişimine ilişkin hukuki ve kurumsal çerçevenin büyük ölçüde oluşturulması, dijital devlet anlayışının yeni bir evreye geçişini mümkün kılmıştır. Böylece 2020'li yıllarla birlikte dijital devlet, yalnızca veriyi yöneten bir yapıyı değil; veriyi analiz eden, öğrenen, öngören ve karar alma süreçlerinde etkin biçimde kullanan "akıllı ve proaktif dijital devlet" anlayışına doğru evrilmeye başlamıştır.

Bu yeni dönemde yapay zekâ, büyük veri analitiği, nesnelerin interneti (IoT), robotik süreç otomasyonu (RPA), açık API mimarileri ve platform yaklaşımı gibi teknolojiler, kamu hizmetlerinin sunum biçimini köklü şekilde değiştirmektedir. Devletler artık yalnızca vatandaşlardan gelen taleplere cevap veren kurumlar değil; farklı veri kaynaklarını analiz ederek ihtiyaçları önceden öngörebilen, karar alma süreçlerini veriyle destekleyen ve hizmetleri proaktif

biçimde sunabilen organizasyonlara dönüşmektedir (Nikiforova vd., 2025: 396).

Bir kamu hizmetinin proaktiflik düzeyi, iki temel unsura bağlıdır. Bunlardan ilki, hizmetin başlatılmasını sağlayan aktördür. Hizmeti başlatan aktör vatandaşın kendisi, bir kamu görevlisi veya yapay zekâ tabanlı bir sistem olabilmektedir (Erlenheim, Draheim ve Taveter, 2020: 457). İkinci unsur ise vatandaşlardan talep edilen bilgi ile etkileşim düzeyidir (Lindgren ve Melin, 2017: 96). Kamu hizmetleri, yalnızca reaktif veya proaktif olmak üzere iki ayrı kategoriye ayrılmamakta; aksine, vatandaşın aktif başvurusunu gerektiren tamamen reaktif hizmetlerden, hak sahipliğinin otomatik olarak belirlenmesi ve hizmetin herhangi bir başvuru gerektirmeden sunulduğu tamamen proaktif hizmetlere kadar uzanan bir süreklilik üzerinde konumlanmaktadır. Örneğin, pasaport başvurusu veya inşaat ruhsatı gibi hizmetlerde vatandaşın başvuru yapması, gerekli belgeleri sunması ve süreci takip etmesi gerektiğinden bu hizmetler büyük ölçüde reaktif nitelik taşımaktadır. Buna karşılık, birçok ülkede uygulanan çevrim içi vergi beyannamesi sistemlerinde verilerin önemli bir kısmı kamu kurumları tarafından önceden doldurulmakta, vatandaş yalnızca bilgileri kontrol ederek onay vermektedir. Bu tür uygulamalar kısmen proaktif hizmetlere örnek oluşturmaktadır. Örneğin; Finlandiya Sosyal Güvenlik Kurumu Kela tarafından geliştirilen yapay zekâ platformu, sosyal yardım başvurularına eklenen belgelerin kabulü ve işlenmesi süreçlerini büyük ölçüde otomatikleştirerek belge formatlarının dönüştürülmesi, optik karakter tanıma, görüntü iyileştirme, barkod okuma ve belge sınıflandırması gibi işlemleri tek bir iş akışı içerisinde gerçekleştirmektedir (OECD, 2025: 22). Böylelikle, sistem doğrudan sosyal yardım hak sahipliğinin belirlenmesi veya hak sahibi olduğu hâlde hizmetlerden yararlanmayan bireylerin (*non-take-up*) tespit edilmesi sorunlarını çözmeye yönelik olmasa da kısmen proaktif hizmet sunmaktadır. Dolayısıyla, uygulamada kamu hizmetlerinin büyük bölümü bu iki uç nokta arasında yer almakta ve vatandaşlardan farklı düzeylerde bilgi veya onay

alınmasını gerektirmektedir. Bir hizmetin hangi düzeyde proaktif olduğu, büyük ölçüde vatandaşların kendi verileri üzerindeki kontrol düzeyi ile hizmete ilişkin tercihlerini belirleme imkânına bağlı olarak değişmektedir.

Tam proaktif yaklaşıma en yakın örneklerinden biri Estonya'nın yaşam olayları (*life events*) temelli dijital hizmet modelidir. *X-Road* altyapısı ve dijital kimlik sistemi sayesinde farklı kamu kurumlarında bulunan veriler güvenli biçimde paylaşılabilmekte, böylece birçok kamu hizmeti vatandaşın yeniden bilgi sunmasına gerek kalmadan otomatik olarak gerçekleştirilebilmektedir. Ancak, Estonya Sayıştayı (*National Audit Office*), 2024 yılı itibarıyla hiçbir kamu hizmetinin henüz en üst dijital olgunluk seviyesine (tam proaktif model) ulaşmadığını, ancak bu hedefe ulaşılmasını sağlayacak güçlü bir kurumsal ve teknik altyapının oluşturulduğunu belirtmiştir. Buna göre Estonya modelinde dahi mevcut hizmetler; bir hizmete elektronik başvuru (e-form) eklenmesi, başka bir hizmette otomatik tetikleme mekanizmalarının devreye alınması gibi küçük müdahalelerle işleyen bir yapıdadır (OECD OPSI, 2024).

Bu dönemin dikkat çeken bir diğer gelişmesi ise "Platform Olarak Devlet (*government as a platform*) yaklaşımıdır. Bu modelde devlet, tüm hizmetleri doğrudan üreten merkezi bir yapı olmaktan ziyade, ortak dijital altyapılar, API servisleri, kimlik doğrulama sistemleri ve veri paylaşım platformları sağlayan bir ekosistem yöneticisi olarak konumlanmaktadır. Böylece kamu kurumları, yerel yönetimler ve hatta özel sektör aynı dijital altyapılar üzerinden güvenli ve standartlaştırılmış biçimde hizmet geliştirebilmektedir. Tim O'Reilly'nin (2010: 15) ortaya koyduğu platform devlet yaklaşımı ve bunu izleyen akademik çalışmalar, dijital devletin geleceğinin ortak platformlar ve açık dijital ekosistemler üzerine inşa edileceğini vurgulamaktadır (Brown vd., 2017: 175).

Akıllı dijital devlet yaklaşımının bir diğer önemli bileşeni yapay zekâ destekli kamu yönetimidir. Kamu sektöründe yürütülen yapay zekâ girişimleri, büyük ölçüde 2017 yılı sonrasında hız kazanmıştır

ve ağırlıklı olarak ulusal düzeyde uygulanmaktadır. Bu projelerin önemli bir kısmı, bağımsız yapay zekâ girişimleri olmaktan ziyade daha geniş kapsamlı dijital dönüşüm programlarının bir parçası olarak geliştirilmektedir (Sevinç Çubuk, 2026: 125). Bu kapsamda yapay zekâ; sosyal yardım programlarında risk analizi, vergi denetimlerinde usulsüzlük tespiti, sağlık hizmetlerinde kaynak planlaması, afet yönetiminde erken uyarı sistemleri ve ulaştırma politikalarında trafik optimizasyonu gibi çok sayıda alanda karar destek aracı olarak kullanılmaktadır. Makine öğrenmesi algoritmaları, tahmine dayalı analitik yöntemler ve üretken yapay zekâ sayesinde kamu kurumları geleceğe yönelik eğilimleri öngörebilmekte ve politika seçeneklerini veri temelli değerlendirebilmektedir. Bu durum, dijital devlet anlayışını yalnızca hizmet sunumuna odaklanan bir yapı olmaktan çıkararak veri temelli yönetişim modeline dönüştürmektedir.

Bununla birlikte, yapay zekânın kamu yönetimindeki uygulama alanları hızla genişlemesine rağmen, hükümetlerin bu teknolojiden hangi alanlarda ve ne ölçüde yararlanabileceğine ilişkin bilgi birikimi hâlen sınırlıdır. Bu çerçevede, yapay zekânın kamu sektöründeki kullanım potansiyelini somutlaştırmak amacıyla Wirtz ve diğerleri (2018: 600-601), geliştirilen uygulamaları incelemiş ve kamu yönetiminde öne çıkan yapay zekâ kullanım alanlarını örneklerle değerlendirmiştir (Tablo 1).

Dünya genelinde birçok kamu kurumu ve devlet kuruluşu, yapay zekâ uygulamalarını farklı hizmet alanlarında test etmeye başlamış olmakla birlikte, bu teknolojilerin geliştirilmesi ve uygulanması konusunda özel sektörün ulaştığı hızın gerisinde kalmaktadır (Mehr, 2017: 6). Bununla birlikte, özel sektörde olgunlaşan yapay zekâ uygulamalarından elde edilen bilgi birikimi ve deneyimin kamu hizmetlerine aktarılması önemli bir fırsat sunmaktadır. Nitekim son yıllarda kamu sektöründe yürütülen yapay zekâ pilot uygulamaları, özellikle kamu hizmetlerinin sunumunun iyileştirilmesi, idari süreçlerin etkinleştirilmesi ve vatandaşlara sunulan destek mekanizmalarının güçlendirilmesi amacıyla hayata geçirilmektedir.

Tablo 1: Kamu Sektöründe Yapay Zekâ Uygulama Alanları, Sağladığı Değer ve Kullanım Örnekleri

Yapay Zekâ Uygulama Alanı	**Sağladığı Değer ve Temel Fonksiyon**	**Kamu Sektöründe Kullanım Örnekleri**
Yapay Zekâ Tabanlı Bilgi Yönetim Sistemleri	Bilginin üretilmesi, sınıflandırılması, depolanması ve kurum içinde paylaşılması; kurumsal bilgi yönetiminin desteklenmesi	Yapay zekâ destekli klinik dokümantasyon sistemleri; kurumsal bilgi tabanlarının oluşturulması
Yapay Zekâ Destekli Süreç Otomasyonu	Tekrarlayan ve kural tabanlı iş süreçlerinin otomatikleştirilmesi; iş akışlarının hızlandırılması, robotik süreç otomasyonu (RPA)	Göçmenlik başvurularının otomatik işlenmesi, veri giriş süreçleri, tıbbi görüntü analizi
Sanal Asistanlar ve Sohbet Botları	Doğal dil işleme ile vatandaşlarla etkileşim kurulması, bilgi sağlanması ve görevlerin yerine getirilmesi	Sığınmacılar için belge hazırlama chatbotları, sanal hemşire asistanları, akıllı insan kaynakları uygulamaları
Tahmine Dayalı Analitik ve Veri Görselleştirme	Büyük verinin analiz edilmesi, öngörü modellerinin geliştirilmesi ve karar destek mekanizmalarının oluşturulması	Su seviyelerinin tahmini, suç yoğunluk analizleri, terör risk haritaları, toplu taşıma güvenlik analizleri
Kimlik Analitiği	Kimlik doğrulama, erişim yönetimi ve dolandırıcılık tespiti	Yüz tanıma sistemleri, kamu verilerinde dolandırıcılık tespiti, risk temelli kimlik doğrulama
Bilişsel Robotik ve Otonom Sistemler	Öğrenebilen ve çevreye uyum sağlayabilen otonom sistemlerin geliştirilmesi	Otonom toplu taşıma araçları, robot destekli cerrahi uygulamaları
Öneri Sistemleri	Kullanıcı tercihlerini analiz ederek kişiselleştirilmiş öneriler sunulması	Kamu personeline kişiselleştirilmiş bilgi ve hizmet önerileri

Yapay Zekâ Uygulama Alanı	Sağladığı Değer ve Temel Fonksiyon	Kamu Sektöründe Kullanım Örnekleri
Akıllı Dijital Asistanlar (IDA)	Ses tabanlı kullanıcı arayüzleri üzerinden bilgiye erişim ve işlem gerçekleştirme	Vatandaşların kamu hizmetlerine sesli erişimi, başvuru süreçlerinde dijital rehberlik
Konuşma Analitiği	Konuşmanın metne dönüştürülmesi, doğal dilin anlaşılması ve çok dilli iletişim	Çağrı merkezi konuşmalarının otomatik çözümlenmesi, sesli yazım, anlık çeviri hizmetleri
Bilişsel Siber Güvenlik Analitiği ve Tehdit İstihbaratı	Yapay zekâ ile güvenlik olaylarının analiz edilmesi, tehditlerin tespit edilmesi ve karar desteği sağlanması	Siber güvenlik analiz platformları (örn. Watson for Cybersecurity), tehdit istihbaratı sistemleri

Kaynak: Wirtz, Weyerer ve Geyer, 2019'dan uyarlanmıştır.

Sonuç olarak devletin dijital dönüşümü, bilgisayarların kamu kurumlarına girmesiyle başlayan teknik bir otomasyon sürecinden, yapay zekâ destekli, veri odaklı ve proaktif dijital devlet modeline uzanan çok katmanlı bir paradigma değişimini ifade etmektedir. Her dönem bir önceki aşamanın üzerine inşa edilmiş; devletin örgütlenme biçimini, kamu hizmetlerinin tasarımını ve vatandaşla kurduğu ilişkiyi de yeniden şekillendirmiştir. Bu nedenle günümüzde dijital dönüşüm, teknolojik yeniliklerin kamu sektörüne uyarlanmasından ziyade devletin işleyiş mantığının yeniden tanımlandığı kapsamlı bir dönüşüm süreci olarak değerlendirilmelidir.

II. DİJİTAL DEVLET DÖNÜŞÜMÜNDE PARADİGMA DEĞİŞİMİ VE TÜRKİYE'NİN GELİŞİMİ

Kamu yönetiminde bilişim teknolojilerinin kullanımı; Weberyen bürokrasinin katı ve hiyerarşik yapısından, esnek, katılımcı ve veri odaklı dijital devlet modeline doğru evrilen çok katmanlı

bir dönüşümü ifade etmektedir. Dijital teknolojilerin kamu yönetiminde kullanılmaya başlanmasıyla birlikte devletin işleyişinde yaşanan asıl dönüşüm, devletin vatandaşla kurduğu ilişkinin, hizmet üretim biçiminin ve yönetişim anlayışının yeniden tanımlanmasında ortaya çıkmaktadır.

OECD, kamu sektöründeki dijital paradigma değişimini, analog devlet anlayışından e-devlet'e ve oradan dijital devlete uzanan bir dönüşüm süreci olarak tanımlamaktadır (OECD, 2021: 22). Geleneksel (analog) devlet yapısında kamu hizmetleri büyük ölçüde kâğıt tabanlı, kapalı ve kurum içi süreçlere dayanmakta; vatandaş ile devlet arasındaki etkileşim ise sınırlı, yavaş ve bürokratik bir nitelik taşımaktadır. 2000'li yıllarda bilgi ve iletişim teknolojilerinin yaygınlaşması ile birlikte kamu yönetiminde ortaya çıkan e-devlet anlayışı, kamu hizmetlerinin elektronik ortama taşınmasını, bilgiye erişimin kolaylaşmasını, işlem süreçlerinin hızlanmasını ve kamu yönetiminde şeffaflık ile etkinliğin artmasını ifade etmektedir. Dijital devlet, dijital teknolojilerin yalnızca hizmet sunumunda değil; aynı zamanda politika yapım süreçlerinde, kurumsal işleyişte ve karar alma mekanizmalarında bütünleşik bir şekilde kullanılmasını kastetmektedir. Bu modelde veri odaklılık, kullanıcı merkezli hizmet tasarımı, açık veri politikaları ve paydaş katılımı ön plana çıkmakta; kamu yönetimi daha esnek, bütünleşik ve proaktif bir yapıya dönüşmektedir.

Dünya Bankası ise bu kavramsal çerçeveyi bir adım ileri taşıyarak "GovTech" yaklaşımını geliştirmiştir (Şekil 4). Dünya Bankası'na göre (2020: 3) GovTech, dijital devlet anlayışının üzerine inşa edilen ve kamu sektörünün dijital dönüşümünde yeni sınırı temsil eden bütüncül bir kamu modernizasyonu yaklaşımıdır. GovTech, dijital devletin oluşturduğu kurumsal ve teknolojik temeli esas almakta; bunun üzerine yapay zekâ, bulut bilişim, nesnelerin interneti, açık veri platformları, dijital kamu altyapıları, açık API ekosistemleri ve kamu-özel sektör iş birlikleri gibi yeni nesil bileşenleri ekleyerek kamu yönetiminin yenilik üretme kapasitesini artırmayı hedeflemektedir. Bu yönüyle GovTech, dijital devletin alternatifi değil; onu tamamlayan ve daha ileri bir olgunluk seviyesine taşıyan yeni bir paradigma olarak değerlendirilmektedir.

Şekil 4: Dijital Devlette Paradigma Değişimi ve Türkiye'nin Konumu

Şekil 4'te gösterildiği gibi Türkiye, bugün büyük ölçüde e-devlet aşamasını tamamlayarak dijital devlet yaklaşımına geçiş sürecini yaşayan ülkeler arasında yer almaktadır. Özellikle e-Devlet Kapısı'nın kamu hizmetleri için ortak erişim noktası hâline gelmesi, dijital kimlik doğrulama mekanizmalarının yaygınlaştırılması ve MERNİS, TAKBİS, UYAP, e-Nabız ile Merkezi Hekim Randevu Sistemi (MHRS) gibi ulusal bilgi sistemlerinin bütünleşik biçimde çalışmaya başlaması, Türkiye'nin dijital devlet altyapısının temel yapı taşlarını oluşturmuştur.

Türkiye'nin bu dönüşüm sürecindeki en önemli avantajlarından biri, merkezi yönetim ve kurumsal koordinasyon kapasitesidir. Pek çok ülkede dijital dönüşüm çalışmaları farklı kurumlar arasında dağınık biçimde yürütülürken, Türkiye'de Cumhurbaşkanlığı Siber Güvenlik Başkanlığı'nın koordinasyon rolü ve TÜRKSAT'ın teknik işletim kapasitesi sayesinde dijital dönüşüm politikaları büyük ölçüde merkezi bir anlayışla hayata geçirilmektedir. Bu yapı; ortak standartların belirlenmesi, dijital kimlik altyapısının geliştirilmesi, güvenlik politikalarının bütüncül biçimde uygulanması ve kurumlar arası birlikte çalışabilirliğin sağlanması açısından önemli avantajlar sunmaktadır. Özellikle e-Devlet Kapısı'nın tüm kamu kurumları için ortak hizmet platformu olarak işletilmesi, farklı kurumlar tarafından geliştirilen hizmetlerin ortak bir kullanıcı deneyimi altında bütünleştirilmesini mümkün kılmıştır.

Ayrıca, Türkiye'nin öne çıkan bir diğer güçlü yönü ise kamu hizmetlerinin kapsamlı biçimde bütünleştirilmiş olmasıdır. Birçok ülkede vatandaşlar farklı kamu kurumlarının ayrı dijital platformlarını kullanmak zorunda kalırken, Türkiye'de kamu kurumlarının sınırlarını aşan hizmet entegrasyonu sayesinde binlerce farklı işlem tek bir dijital platform üzerinden sunulabilmektedir. Bu durum yalnızca kullanıcı deneyimini iyileştirmemekte; aynı zamanda kamu kurumları arasında veri paylaşımını kolaylaştırarak mükerrer belge talebini azaltmakta ve işlem süreçlerini hızlandırmaktadır. OECD'nin dijital devlet yaklaşımında öne çıkan "Platform Olarak Devlet" ilkesi açısından değerlendirildiğinde, e-Devlet Kapısı'nın Türkiye'de oluşturduğu ortak dijital hizmet altyapısı önemli bir kurumsal kapasiteyi yansıtmaktadır.

Dijital devlet dönüşümünün başarısını belirleyen temel göstergelerden biri de vatandaşların dijital hizmetleri benimseme düzeyidir. Hizmetlerin tek platform altında sunulması ve kullanıcı dostu ara yüzlerin oluşturulması sayesinde e-Devlet Kapısı milyonlarca vatandaş tarafından günlük yaşamın ayrılmaz bir parçası hâline gelmiştir. Yüksek kullanıcı memnuniyeti oranları ve sürekli artan kullanım istatistikleri, dijital devlet dönüşümünün yalnızca teknolojik bir başarı olmadığını, aynı zamanda vatandaş güvenini tesis eden bir yönetişim başarısı olduğunu göstermektedir.

Türkiye'nin dijital devlet alanındaki ilerlemesi uluslararası değerlendirmelere de yansımaktadır. Türkiye'nin son yıllardaki performansı incelendiğinde, özellikle Birleşmiş Milletler endekslerinde önemli ilerlemeler kaydettiği, buna karşılık OECD ve Dünya Bankası tarafından değerlendirilen daha ileri dijital devlet bileşenlerinde gelişime açık alanların bulunduğu görülmektedir.

Birleşmiş Milletler tarafından yayımlanan 2024 E-Devlet Gelişmişlik Endeksi (EGDI) sonuçlarına göre Türkiye, 193 ülke arasında 27. sıraya yükselerek 2018 yılına kıyasla 26 basamaklık önemli bir ilerleme kaydetmiştir. Aynı dönemde endeks puanı 0,7112'den 0,8913'e yükselmiş ve yaklaşık %25'lik bir gelişim sağlanmıştır. Bu sonuç, Türkiye'nin dijital kamu hizmetleri altyapısı, telekomünikasyon kapasitesi ve insan sermayesi alanlarında istikrarlı bir gelişim gösterdiğini ortaya koymaktadır.

Benzer şekilde, Çevrim İçi Hizmet Endeksi (*Online Service Index*-OSI) sonuçları Türkiye'nin en güçlü olduğu alanlardan birini oluşturmaktadır. Türkiye, 27. sıradan 13. sıraya yükselerek dünyanın en gelişmiş çevrim içi kamu hizmetlerini sunan ülkeleri arasına girmiştir. Bu başarı, özellikle e-Devlet Kapısı'nın tek erişim noktası olarak geliştirilmesi, kurumlar arası hizmet entegrasyonunun sağlanması ve vatandaş odaklı dijital hizmet tasarımının yaygınlaştırılmasıyla yakından ilişkilidir. Kamu kurumlarının binlerce hizmeti ortak bir platform üzerinden sunabilmesi, uluslararası değerlendirmelerde Türkiye'nin güçlü yönlerinden biri olarak öne çıkmaktadır.

Bir diğer dikkat çekici gelişme ise E-Katılım Endeksi'nde (*E-Participation Index*-EPI) görülmektedir. Türkiye'nin 37. sıradan 22. sıraya yükselmesi, dijital teknolojilerin yalnızca hizmet sunumunda değil; vatandaşların bilgiye erişimi, karar alma süreçlerine katılımı ve dijital etkileşim mekanizmalarının geliştirilmesi açısından da önemli ilerlemeler kaydedildiğini göstermektedir. Özellikle kamu kurumlarının dijital iletişim kanallarını yaygınlaştırması ve çevrim içi katılım mekanizmalarının çeşitlenmesi bu gelişmede etkili olmuştur.

Türkiye'nin dijital devlet alanındaki başarısı yalnızca Birleşmiş Milletler tarafından değil, Dünya Bankası tarafından da doğrulanmaktadır. Dünya Bankası'nın GovTech Olgunluk Endeksi (*GovTech Maturity Index*-GTMI) 2025 sonuçlarında Türkiye, A Grubu ülkeler arasında yer almıştır. Bu grup, dijital kamu altyapıları, kamu hizmetlerinin dijitalleşmesi, vatandaş odaklılık ve kurumsal dijital kapasite bakımından en yüksek olgunluk düzeyine sahip ülkeleri ifade etmektedir. Türkiye'nin 0,812 puan alarak A Grubu içerisinde değerlendirilmesi, dijital devlet altyapısı bakımından uluslararası ölçekte güçlü bir konuma ulaştığını göstermektedir.

Bununla birlikte, OECD Dijital Devlet Endeksi (*Digital Government Index*-DGI) sonuçları farklı bir perspektif sunmaktadır. Türkiye, 38 OECD ülkesi arasında 31. sırada yer almaktadır. İlk bakışta bu sonuç diğer uluslararası endekslere kıyasla daha düşük görünmekle birlikte, OECD Dijital Devlet Endeksi'nin ölçtüğü boyutlar dikkate alındığında bu durum daha anlamlı hâle

gelmektedir. Birleşmiş Milletler endeksleri ağırlıklı olarak dijital hizmet sunumu ve erişilebilirlik kapasitesini değerlendirirken, OECD Dijital Devlet Endeksi; veri yönetişimi, platform olarak devlet yaklaşımı, açık veri politikaları, dijital tasarım (*digital by design*), proaktif kamu hizmetleri ve kullanıcı odaklı yönetişim gibi daha ileri düzey dijital devlet bileşenlerini ölçmektedir (OECD, 2024; OECD, 2026). Dolayısıyla OECD endeksindeki görece düşük performans, Türkiye'nin temel dijital altyapısının yetersiz olduğunu değil; dijital devletin yeni nesil yönetişim bileşenlerinde gelişime açık alanlarının bulunduğunu göstermektedir.

Nitekim OECD'nin *Digital Government Outlook* 2026 raporu da bu değerlendirmeyi desteklemektedir. Rapora göre Türkiye, Kanada, Estonya, Fransa, Güney Kore, Birleşik Krallık ve İsveç gibi ülkelerle birlikte veri stratejilerinin tüm temel bileşenlerini (vizyon, yönetişim, uygulama ve izleme mekanizmaları) bütüncül biçimde geliştiren ülkeler arasında yer almaktadır. Bu değerlendirme, Türkiye'nin yalnızca veri stratejisi hazırlayan ülkeler arasında değil, bu stratejilerin uygulanmasını izleyen ve yöneten kurumsal mekanizmaları da oluşturan ülkeler arasında yer aldığını göstermektedir. Raporda ayrıca, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'nun (TÜBİTAK) kamu kurumları, özel sektör ve araştırma kuruluşlarını aynı araştırma-geliştirme ekosisteminde buluşturan yapay zekâ odaklı konsorsiyum modeli (TÜBİTAK 1711 Yapay Zekâ Ekosistem Çağrısı), Türkiye'nin yapay zekâ kapasitesini geliştiren iyi uygulama örneklerinden biri olarak değerlendirilmektedir (OECD, 2026: 117)[1].

Türkiye'nin dijital devlet dönüşümünü destekleyen bir diğer unsur ise teknolojik kapsayıcılık kapasitesidir. Son yıllarda geniş bant internet altyapısının yaygınlaşması, mobil internet kullanım oranlarının artması, akıllı telefon penetrasyonunun yükselmesi ve teknoloji kullanımına yatkın genç nüfusun varlığı, dijital kamu hizmetlerinin toplumun geniş kesimleri tarafından benimsenmesini kolaylaştırmıştır. Böylece dijital devlet uygulamaları yalnızca teknik olarak geliştirilen sistemler olmaktan çıkmış; vatandaşların günlük yaşamında yoğun olarak kullanılan temel kamu hizmeti kanallarına dönüşmüştür.

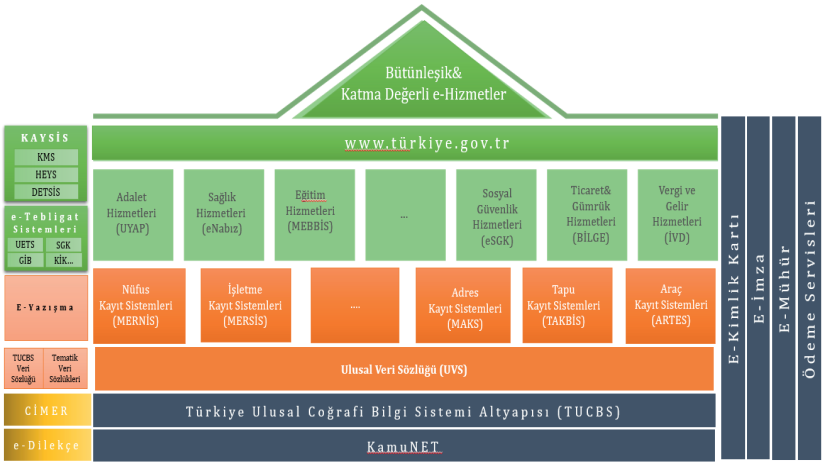
1 https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/06/digital-government-outlook_4585678e/0496b2bc-en.pdf

Bununla birlikte, Bununla birlikte, OECD ve Dünya Bankası raporları birlikte değerlendirildiğinde Türkiye açısından bir sonraki dönüşüm aşamasının dijital hizmetlerin yaygınlaştırılmasından çok dijital yönetişimin güçlendirilmesi olduğu görülmektedir. Türkiye'nin dijital devlet alanında kaydettiği ilerlemeye rağmen, dijital dönüşümün tam potansiyeline ulaşabilmesi için geliştirilmesi gereken bazı alanlar da bulunmaktadır. Öncelikle, açık veri politikalarının kapsamının genişletilmesi ve uluslararası iyi uygulamalarla uyumlu şeffaflık standartlarının daha da güçlendirilmesi önem taşımaktadır. Dijital devlet yaklaşımında veri kamu kurumları arasında paylaşılan operasyonel bir kaynaktan öte, aynı zamanda akademi, özel sektör ve sivil toplum tarafından yeniden kullanılabilen stratejik bir kamu varlığı olarak değerlendirilmektedir. Bu nedenle, verinin güvenlik ve kişisel verilerin korunması ilkeleri gözetilerek yeniden kullanıma açılması, veri temelli inovasyonun desteklenmesi, kamu politikalarının etkinliğinin artırılması ve hesap verebilirliğin güçlendirilmesi açısından kritik öneme sahiptir.

Diğer taraftan, Türkiye'nin dijital devlet ekosistemi güçlü kurumsal bileşenlere sahip olmakla birlikte, bu bileşenlerin bütüncül bir yönetişim anlayışı içerisinde daha etkin şekilde bütünleştirilmesine ihtiyaç bulunmaktadır. E-Devlet Kapısı, dijital kimlik altyapısı, ortak hizmet standartları, veri paylaşım mekanizmaları ve kurumsal bilgi sistemleri önemli bir olgunluk seviyesine ulaşmış olsa da bu unsurların kamu politikalarının tasarımından hizmet sunumuna kadar tüm süreçlerde ortak değer üreten entegre bir yapıya dönüştürülmesi gerekmektedir. Başka bir ifadeyle, Türkiye açısından temel dönüşüm alanı, güçlü fakat zaman zaman birbirinden bağımsız ilerleyen dijital kapasite unsurlarını ortak veri yönetişimi, kurumsal mimari ve yapay zekâ destekli karar mekanizmaları etrafında bütünleştirerek sistem düzeyinde sinerji oluşturabilmektir.

Şekil 5'te gösterilen mevcut Türkiye e-Devlet Kurumsal Mimarisi, son yirmi yılda oluşturulan dijital devlet altyapısının temel bileşenlerini ortaya koymaktadır. Mimarinin merkezinde e-Devlet Kapısı (www.turkiye.gov.tr) yer almakta; vatandaşların farklı kamu kurumları tarafından sunulan hizmetlere tek noktadan

erişebilmesi sağlanmaktadır. Bu yapının altında adalet, sağlık, eğitim, sosyal güvenlik, ticaret ve vergi gibi temel kamu hizmetleri yer alırken, hizmetlerin temelini MERNİS, TAKBİS, MERSİS, MAKS ve ARTES gibi ulusal kayıt sistemleri oluşturmaktadır. Bu sistemler; KamuNET, Türkiye Ulusal Coğrafi Bilgi Sistemi (TUCBS), Ulusal Veri Sözlüğü ve veri yönetişimi bileşenleriyle desteklenmekte; e-Kimlik, e-İmza, e-Mühür ve dijital ödeme servisleri ise tüm mimarinin güven katmanını oluşturmaktadır. Bu yapı, Türkiye'nin dijital devlet dönüşümünde ortak dijital altyapılar, merkezi kimlik doğrulama, birlikte çalışabilirlik ve ortak hizmet sunumu açısından önemli bir kurumsal kapasite geliştirdiğini göstermektedir.



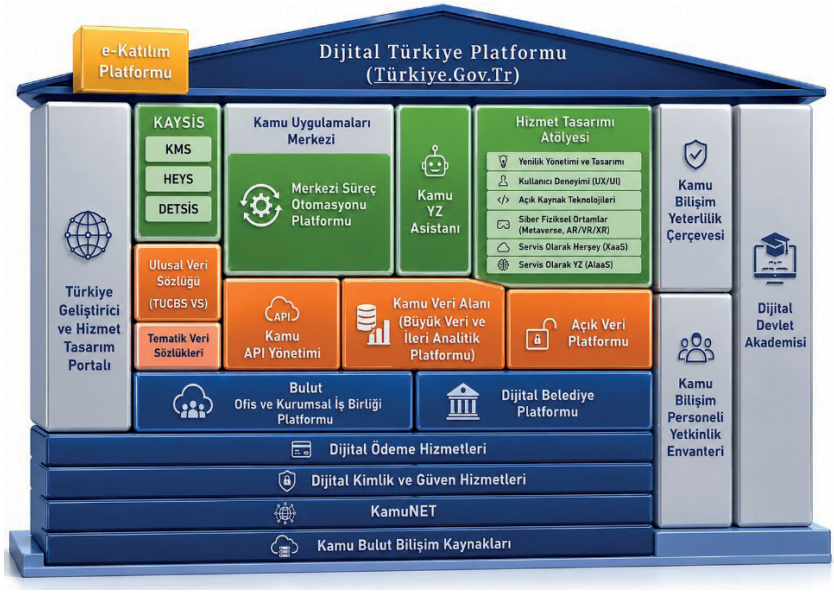
Şekil 5: Türkiye'de e-Devlet Kurumsal Mimarisi

Bununla birlikte mevcut mimari ağırlıklı olarak mevcut kamu hizmetlerinin dijital ortamda bütünleştirilmesine odaklanmaktadır. Başka bir ifadeyle mimari, kamu kurumları arasında veri paylaşımını ve ortak hizmet sunumunu büyük ölçüde mümkün kılmakla birlikte, veri temelli yönetişim, yapay zekâ destekli karar mekanizmaları, açık veri ekosistemi ve platform ekonomisi gibi yeni nesil dijital devlet bileşenlerini sınırlı ölçüde içermektedir. Bu nedenle dijital dönüşümün sürdürülebilirliği açısından yalnızca mevcut hizmetlerin dijitalleşmesi yeterli olmayıp, bu hizmetlerin

veri odaklı ve akıllı sistemler üzerinden yeniden tasarlanması gerekmektedir.

Yeni dönemde mevcut bilişim sistemleri ve merkezi veri tabanlarının birlikte çalışabilmesinin ötesinde büyük veriden değer üretmeye, yeni nesil teknolojilere daha hızlı uyum sağlamaya, hizmet sunum ve politika geliştirmede son kullanıcı katılımı kolaylaştırmaya öncelik verilmektedir.

Bu ihtiyaç doğrultusunda ön plana çıkan yeni nesil Dijital Devlet Hedef Mimarileri (Şekil 6), mevcut yapının devamı niteliğinde olmakla birlikte, dijital devlet anlayışını yeni nesil teknolojiler ve yönetişim mekanizmalarıyla genişleten bütünleşik bir dönüşüm modelini ortaya koymaktadır. Hedef mimaride e-Devlet Kapısı, yalnızca hizmet sunan bir portal olmaktan çıkarılarak Dijital Türkiye Platformu anlayışıyla tüm kamu dijital ekosisteminin merkezi platformu hâline getirilmektedir. Böylece kamu kurumları arasındaki dikey ve yatay veri akışları tek bir dijital mimari içerisinde bütünleştirilmekte; kurum merkezli yapılardan platform merkezli kamu yönetimine geçiş hedeflenmektedir.



Şekil 6: Dijital Devlet Hedef Mimarisi

Hedef mimarinin en önemli yeniliklerinden biri, verinin kamu yönetiminin stratejik bir varlığı olarak yeniden konumlandırılmasıdır. Bu doğrultuda Kamu Veri Alanı (Data Space), Büyük Veri ve İleri Analitik Platformu, Ulusal Veri Sözlüğü, Tematik Veri Sözlükleri, Kamu API Yönetimi ve Açık Veri Platformu gibi yeni bileşenler mimariye dâhil edilmektedir. Böylece verinin yalnızca kurumlar arasında paylaşılması değil; ortak standartlarla yönetilmesi, yeniden kullanılabilir hâle getirilmesi ve kamu politikalarının geliştirilmesinde etkin biçimde değerlendirilmesi amaçlanmaktadır.

Bir diğer önemli dönüşüm ise yapay zekâ ve otomasyon teknolojilerinin mimarinin ayrılmaz bir parçası hâline gelmesidir. Mevcut mimaride yer almayan Kamu Yapay Zekâ Asistanı, Merkezi Süreç Otomasyon Platformu ve Kamu Uygulamaları Merkezi gibi bileşenler sayesinde yalnızca vatandaşlara sunulan hizmetlerin değil, kamu kurumlarının iç iş süreçlerinin de akıllı sistemlerle desteklenmesi öngörülmektedir. Böylece yapay zekâ; belge işleme, karar destek, süreç otomasyonu, vatandaş etkileşimi ve kamu politikalarının geliştirilmesi gibi alanlarda kurumsal kapasiteyi artıran temel teknolojilerden biri hâline gelmektedir.

Hedef mimarinin dikkat çeken bir diğer yönü ise ekosistem yaklaşımını benimsemesidir. Türkiye Geliştirici ve Hizmet Tasarım Portalı, Hizmet Tasarım Atölyesi, Dijital Devlet Akademisi, Kamu Bilişim Yetkinlik Çerçevesi ve Kamu Bilişim Personeli Yetkinlik Envanteri gibi yeni bileşenler, dijital dönüşümün yalnızca teknoloji yatırımlarıyla değil; insan kaynağı, hizmet tasarımı ve kurumsal kapasite geliştirme süreçleriyle birlikte ele alındığını göstermektedir. Böylece dijital devlet yalnızca bilgi sistemlerinin değil; aynı zamanda yönetişim modellerinin, kamu personelinin ve hizmet geliştirme kültürünün de dönüştürülmesini hedeflemektedir.

Ayrıca hedef mimari, bulut bilişim, ortak ofis ve kurumsal iş birliği platformları, dijital belediye platformu, dijital ödeme hizmetleri ve kamu bulut bilişim kaynakları gibi ortak dijital altyapılarla ölçek ekonomisi oluşturmayı amaçlamaktadır. Bu yaklaşım sayesinde mükerrer yatırımların azaltılması, kurumlar arasında standartlaşmanın sağlanması ve dijital çözümlerin kamu genelinde yeniden kullanılabilir hâle getirilmesi mümkün olacaktır.

Mevcut yapı ağırlıklı olarak hizmet entegrasyonu üzerine kuruluyken, hedef mimari veri odaklı yönetişim, platform yaklaşımı, yapay zekâ destekli kamu yönetimi, açık veri ekosistemi, ortak dijital altyapılar ve kurumsal kapasite geliştirme ekseninde bütünleşik bir dijital devlet modeli önermektedir. Başka bir ifadeyle Türkiye'nin dijital dönüşümünde hedeflenen değişim, kurumlar arasında izole biçimde çalışan dijital yapılardan; verinin merkezde olduğu, platformlar üzerinden birlikte çalışan, yapay zekâ ile desteklenen ve kamu değeri üreten katmanlı bir ulusal dijital mimariye geçişi ifade etmektedir. Bu dönüşüm, yalnızca teknolojik modernizasyonu değil, kamu yönetiminin işleyişini ve yönetişim anlayışını yeniden şekillendirecek stratejik bir paradigma değişimini temsil etmektedir.

Mevcut kurumsal mimariden hedef dijital devlet mimarisine geçiş, kamu yönetiminin işleyişini, yönetişim anlayışını ve değer üretme biçimini yeniden tanımlayan kapsamlı bir paradigma değişimini ifade etmektedir. Başka bir ifadeyle dönüşümün odağında artık yeni bilgi sistemleri geliştirmek değil, bu sistemleri ortak standartlar doğrultusunda yöneten, veriyi stratejik bir kamu varlığı olarak değerlendiren ve tüm dijital bileşenleri bütüncül biçimde yönlendirebilen bir dijital devlet ekosistemi oluşturmak yer almaktadır. Bu nedenle hedef mimarinin başarısı, teknolojik yatırımlardan çok yönetişim kapasitesinin güçlendirilmesine bağlıdır.

Bu dönüşümün ilk bileşeni dijital devlet yönetişim mekanizmasının oluşturulmasıdır. Dijital devlet uygulamalarının çok sayıda kurumun sorumluluk alanına girmesi nedeniyle dönüşümün yalnızca merkezi koordinasyonla değil, aynı zamanda her kurumun kendi dijital dönüşümünden sorumlu olduğu çok katmanlı bir yönetişim modeliyle yürütülmesi gerekmektedir. Böyle bir yapı, ortak standartların geliştirilmesini, kurumsal sorumlulukların netleştirilmesini ve dijital dönüşüm projelerinin ulusal önceliklerle uyumlu biçimde yönetilmesini mümkün kılacaktır. OECD de dijital devlet stratejilerinin başarısının güçlü koordinasyon mekanizmalarına ve kurumlar arası ortak yönetişime bağlı olduğunu vurgulamaktadır (OECD, 2024; OECD, 2026).

Paradigma değişiminin ikinci boyutunu kurumsal mimari yaklaşımının olgunlaştırılması oluşturmaktadır. Hedeflenen yapı, her kurumun kendi teknolojik çözümlerini bağımsız olarak geliştirdiği silo yaklaşımından uzaklaşarak ortak teknoloji bileşenleri, yeniden kullanılabilir servisler ve birlikte çalışabilir bilgi sistemleri üzerine kurulu ulusal bir dijital mimariyi esas almaktadır. Böylece kamu kurumları benzer teknolojileri tekrar tekrar geliştirmek yerine ortak platformlardan yararlanabilecek, uygulamalar daha düşük maliyetle geliştirilebilecek ve yeni dijital hizmetlerin hayata geçirilme süresi önemli ölçüde kısalacaktır.

Üçüncü dönüşüm alanı ise veri yönetişiminin kamu yönetiminin merkezine yerleştirilmesidir. Dijital devlet olgunluğu artık yalnızca kurumlar arasında veri paylaşımının sağlanmasıyla değil; verinin ortak standartlar çerçevesinde tanımlanması, veri kalitesinin güvence altına alınması, yaşam döngüsünün yönetilmesi ve büyük veri analitiği ile kamu politikalarının geliştirilmesinde kullanılabilmesiyle ölçülmektedir. Bu kapsamda ortak veri sözlükleri, API yönetimi, kamu veri alanları ve ileri analitik platformları, kamu verisinin stratejik bir üretim faktörüne dönüşmesini sağlayacak temel bileşenler olarak öne çıkmaktadır.

Dijital devlet anlayışındaki paradigma değişimi, yalnızca teknolojik altyapıyı değil, kamu bilişim projelerinin geliştirilme biçimini de değiştirmektedir. Geleneksel yaklaşımda kurumlar kendi ihtiyaçları doğrultusunda bağımsız projeler geliştirirken, yeni yaklaşım ortak mimari ilkelerine uygun, yeniden kullanılabilir, güvenli ve sürdürülebilir çözümlerin geliştirilmesini öngörmektedir. Aynı zamanda kamu kurumlarının teknoloji şirketleri, girişimler ve araştırma kuruluşlarıyla daha yakın iş birliği kurması, yenilikçi çözümlerin kamu sektörüne daha hızlı aktarılmasını sağlayacaktır. Bu yaklaşım, Dünya Bankası'nın GovTech modelinde öne çıkan kamu-özel sektör inovasyon ekosistemi anlayışıyla da örtüşmektedir (World Bank, 2021: 3).

Paradigma değişiminin vatandaş tarafından en görünür yansıması ise dijital kamu hizmetlerinin sunum ilkelerinde gerçekleşmektedir. Hizmetlerin yalnızca çevrim içi sunulması artık yeterli görülmemekte; hizmetlerin yaşam olayları ekseninde tasarlanması, proaktif biçimde sunulması, dijital dayanıklılık ilkelerine

uygun geliştirilmesi, algoritmik şeffaflığın sağlanması ve yeni teknolojilerin kontrollü ortamlarda test edilmesi beklenmektedir. Böylece kamu hizmetleri vatandaşların başvurusunu bekleyen reaktif yapılardan, ihtiyaçları önceden tahmin ederek hizmet sunabilen akıllı sistemlere dönüşmektedir.

Bu dönüşümün sürdürülebilirliği açısından kritik öneme sahip bir diğer unsur insan kaynağıdır. Dijital devletin başarısı yalnızca güçlü teknolojik altyapılarla değil; bu altyapıları tasarlayabilecek, yönetecek ve sürekli geliştirebilecek nitelikli kamu personelinin yetiştirilmesine bağlıdır. Bu nedenle kamu bilişim personeli için ortak yetkinlik çerçevelerinin oluşturulması, uzmanlık ağlarının geliştirilmesi ve sürekli eğitim mekanizmalarının kurulması dijital devlet stratejisinin ayrılmaz bir parçası hâline gelmektedir.

Son olarak paradigma değişimi, ortak dijital hizmet ve altyapıların yaygınlaştırılmasını gerekli kılmaktadır. Dijital kimlik, dijital ödeme sistemleri, elektronik tebligat, güvenli veri paylaşımı, ortak bulut altyapıları ve ortak servis platformları gibi bileşenler, tüm kamu kurumlarının üzerinde hizmet geliştirebildiği temel dijital kamu altyapıları hâline gelmektedir. Böylece kamu kurumları kendi temel altyapılarını yeniden oluşturmak yerine ortak platformlar üzerinde yenilikçi hizmetler geliştirebilmekte; bu durum hem kaynak kullanımında verimlilik sağlamakta hem de vatandaşlara sunulan hizmetlerde standartlaşmayı artırmaktadır.

Bütün bu dönüşüm alanları birlikte değerlendirildiğinde, hedeflenen paradigma değişimi Türkiye'nin uluslararası dijital devlet endekslerindeki konumunu güçlendirecek stratejik bir çerçeve sunmaktadır. Bugün Türkiye, e-devlet başarısını büyük ölçüde tamamlamış; dijital devlet olgunluğunu ise veri yönetişimi ve GovTech ekseninde derinleştirme aşamasına geçmiş ülkeler arasında yer almaktadır. Türkiye'nin bir sonraki dijital dönüşüm aşaması; dijital hizmetlerin sayısını artırmaktan ziyade, açık veri, proaktif kamu hizmetleri, kurumlar arası gerçek zamanlı veri paylaşımı, güvenilir yapay zekâ uygulamaları ve vatandaş katılımını güçlendiren dijital yönetişim mekanizmaları gibi yeni nesil dijital devlet bileşenlerinin geliştirilmesine odaklanmalıdır. Bu dönüşümün başarısı ise güçlü kurumsal koordinasyon, veri yönetişimi ve kamu değeri üretimini merkeze alan bütüncül bir dijital devlet vizyonunun

sürdürülebilir biçimde hayata geçirilmesine bağlıdır.

III. DİJİTAL DEVLETTE HİZMET SUNUMUNDAN KAMU DEĞERİ ÜRETİMİNE

Dijital devlet anlayışı, kamu hizmetlerinin elektronik ortama aktarılmasının ötesinde, kamu yönetiminin değer üretme süreçlerini yeniden tanımlayan kapsamlı bir dönüşümü ifade etmektedir. Bu dönüşüm; kamu hizmetlerinin tasarlanma, üretilme, sunulma ve yönetilme biçimlerinin dijital teknolojiler ekseninde yeniden şekillendirilmesini gerektirmektedir. Dolayısıyla dijital devlette dönüşüm; süreçlerin, hizmetlerin ve ürünlerin dışsal ihtiyaçlara göre sık sık uyarlanmasını gerektiren sürekli bir süreçtir (Mergel vd., 2019: 10). Geleneksel e-devlet yaklaşımında temel amaç hizmetlerin çevrim içi sunulması iken, dijital devlet yaklaşımında asıl hedef, dijital teknolojiler aracılığıyla kamu değeri (*public value*) üretmektir (Twizeyimana ve Andersson, 2019: 168). Bu doğrultuda dijital devletin başarısı, sunulan hizmet sayısından çok; hizmetlerin vatandaşlar açısından oluşturduğu değer, kamu kaynaklarının etkin kullanımı ve kamu yönetiminin yönetişim kapasitesi üzerinden değerlendirilmektedir.

Bu yaklaşım çerçevesinde kamu değeri üç temel unsurun dengeli biçimde gerçekleştirilmesine bağlıdır. Bunlardan ilki verimlilik (*efficiency*) olup kamu kaynaklarının en uygun şekilde kullanılmasını, mükerrer yatırımların azaltılmasını ve hizmet maliyetlerinin düşürülmesini ifade etmektedir. İkinci unsur etkinlik (*effectiveness*) olup kamu hizmetlerinin doğru hedef kitleye, doğru zamanda ve beklenen kalite düzeyinde ulaştırılmasını kapsamaktadır. Üçüncü unsur ise iyi yönetişim (*good governance*) olup şeffaflık, hesap verebilirlik, katılımcılık, güven ve etik ilkeler çerçevesinde kamu hizmetlerinin yönetilmesini ifade etmektedir. Dijital devletin temel amacı, bu üç boyutu birlikte gerçekleştirerek dijital hizmetleri kamu değeri üreten stratejik araçlara dönüştürmektir.

Bu hedefe ulaşılabilmesi için öncelikle kamu kurumlarının ortak veri standartları üzerinden çalışması gerekmektedir. Bu kapsamda kurumların ürettiği verilerin ortak bir Ulusal Veri Sözlüğü, metaveri yönetimi ve API yönetimi yaklaşımıyla tanımlanması büyük önem

taşımaktadır. Böylece farklı kurumlar aynı kavramları aynı şekilde tanımlayabilecek, veri paylaşımı standartlaşacak ve yeni dijital hizmetlerin geliştirilmesi önemli ölçüde hızlanacaktır. Açık API mimarileri sayesinde kamu bilgi sistemleri birbirleriyle güvenli ve standart biçimde haberleşebilecek; yeni uygulamaların mevcut sistemler üzerine kolaylıkla inşa edilmesi mümkün olacaktır.

Dijital hizmet sunumunun ikinci temel bileşeni, kurumlarda BT yönetişimi ve kurumsal mimari anlayışının yaygınlaştırılmasıdır. Ortak teknoloji standartlarının benimsenmesi, bilgi sistemlerinin merkezi ilkelere göre geliştirilmesi ve dijital envanter yönetiminin oluşturulması, kamu kurumlarının benzer teknolojileri tekrar geliştirmesini önleyecek ve bilişim yatırımlarında ölçek ekonomisi sağlayacaktır. Böylece dijital dönüşüm, bağımsız bilgi sistemlerinin geliştirilmesinden ortak dijital platformların yönetimine doğru evrilecektir.

Yeni nesil dijital devlet yaklaşımında ortak hizmetlerin mümkün olduğunca otomatik yürütülmesi de önemli bir öncelik hâline gelmektedir. Özellikle izin, onay, doğrulama ve belge dolaşımı gibi çok sayıda kurum tarafından yürütülen ortak süreçlerin Merkezi Süreç Otomasyon Platformları üzerinden yönetilmesi hem işlem sürelerini kısaltacak hem de vatandaşların aynı bilgileri farklı kurumlara tekrar tekrar sunma zorunluluğunu azaltacaktır. Bu süreçler, düşük kod (*low-code*) ve hızlı uygulama geliştirme altyapıları sayesinde değişen ihtiyaçlara daha hızlı uyarlanabilecektir.

Yapay zekâ ve Robotik Süreç Otomasyonu (RPA) teknolojileri ise dijital devlet hizmetlerinin daha akıllı hâle gelmesini sağlayan temel bileşenlerden biridir. Kurum içi ve kurumlar arası iş akışlarının otomatikleştirilmesi, belge işleme süreçlerinin hızlandırılması, rutin kararların desteklenmesi ve vatandaş taleplerinin daha kısa sürede sonuçlandırılması sayesinde kamu hizmetlerinde önemli verimlilik kazanımları elde edilebilecektir. Bunun yanında yapay zekâ ajanlarının kullanımı, kamu görevlilerinin rutin işlemler yerine daha yüksek katma değer üreten faaliyetlere odaklanmasına imkân sağlayacaktır.

Dijital devlet yaklaşımının en önemli yeniliklerinden biri de Kamu

Veri Alanı (*Public Data Space*) anlayışıdır. Kurumlar arasında yetkilendirilmiş veri paylaşımı sayesinde büyük veri analitiği ve yapay zekâ modellerinin kamu verileri üzerinde güvenli biçimde eğitilmesi mümkün olacaktır. Böylece politika yapıcılar, gerçek zamanlı veriler üzerinden eğilimleri analiz edebilecek, kamu hizmetlerinin performansını ölçebilecek ve karar alma süreçlerini bilimsel verilere dayandırabilecektir. Bu yaklaşım, OECD'nin veri odaklı kamu sektörü (*data-driven public sector*) ilkesinin somut karşılığını oluşturmaktadır.

Dijital hizmetlerin sürdürülebilirliği açısından dijital dayanıklılık (*digital resilience*) ve dijital egemenlik (*digital sovereignty*) de yeni dönemin vazgeçilmez unsurları arasında yer almaktadır. Siber tehditlerin artması, kritik kamu hizmetlerinin kesintisiz sunulmasını stratejik bir gereklilik hâline getirmiştir. Bu nedenle yalnızca güvenlik önlemlerinin artırılması değil; aynı zamanda kriz senaryoları, iş sürekliliği planları ve düzenli dayanıklılık tatbikatlarıyla kamu kurumlarının olası kesintilere karşı hazırlıklı olması gerekmektedir.

Dijital devletin başarısı, yalnızca hizmetlerin işletilmesiyle değil, bu hizmetlerin sürekli geliştirilmesiyle de yakından ilişkilidir. Bu doğrultuda gerçek zamanlı karar destek panelleri, politika yapıcıların kamu hizmetlerinin performansını anlık olarak izleyebilmesini sağlayacak; vatandaş geri bildirimleri ve kullanım verileri ise hizmetlerin sürekli iyileştirilmesine katkıda bulunacaktır. Bunun yanında dijital hizmet tasarım atölyeleri, kamu kurumları, özel sektör, akademi ve vatandaşların birlikte çözüm geliştirebildiği yenilikçi ortamlar oluşturarak kamu hizmetlerinde kullanıcı odaklı inovasyonu destekleyecektir.

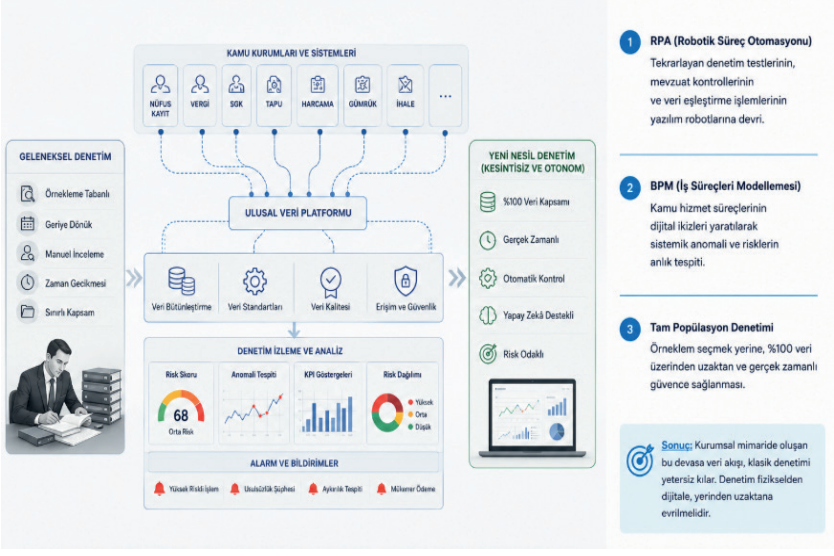
Sonuç olarak dijital devlet anlayışında hizmet sunumunun amacı artık yalnızca işlemleri elektronik ortama taşımak değildir. Asıl hedef; ortak veri altyapıları, kurumsal mimari, yapay zekâ, otomasyon, veri analitiği ve güçlü yönetişim mekanizmalarını bir araya getirerek dijital hizmetlerden sürdürülebilir kamu değeri üretmektir. Bu dönüşüm sayesinde kamu hizmetleri daha verimli, daha etkin ve daha güvenilir hâle gelirken; devlet de veriyi stratejik bir kaynak olarak yöneten, vatandaş ihtiyaçlarını öngören ve sürekli öğrenen bir organizasyona dönüşmektedir. Bu yaklaşım,

Türkiye'nin dijital devlet dönüşümünde ulaşmayı hedeflediği yeni yönetim paradigmasını temsil etmektedir.

V. DİJİTAL DEVLETİN DENETİM PARADİGMASINA ETKİSİ

Dijital devlet anlayışının yaygınlaşması yalnızca kamu hizmetlerinin sunumunu değil, kamu yönetiminin temel fonksiyonlarından biri olan denetim mekanizmalarını da köklü biçimde dönüştürmektedir. Geleneksel kamu yönetiminde denetim faaliyetleri büyük ölçüde belge incelemesine, örnekleme yöntemlerine ve geçmişe dönük kontroller üzerine kurulmuştur. Denetim bulguları çoğu zaman işlemler tamamlandıktan sonra tespit edilmekte, fiziksel belge incelemeleri nedeniyle süreçler uzun zaman almakta ve sınırlı sayıdaki işlemin incelenebilmesi nedeniyle hata veya usulsüzlüklerin tamamına ulaşmak mümkün olamamaktadır.

Ancak dijital devlet mimarisinin oluşturduğu ortak veri altyapıları, kurumlar arası birlikte çalışabilirlik ve gerçek zamanlı veri paylaşımı, denetim anlayışını da temelden değiştirmektedir. Kamu kurumlarının ürettiği verilerin Ulusal Veri Platformu üzerinden bütünleşik biçimde yönetilmesi; veri standartlarının oluşturulması, veri kalitesinin güvence altına alınması ve güvenli veri paylaşım mekanizmalarının geliştirilmesi sayesinde denetim faaliyetleri artık yalnızca belge odaklı olmaktan çıkarak veri odaklı bir yapıya dönüşmektedir



(Şekil 7). Böylece denetçiler, farklı kurumlardan gelen verileri aynı platform üzerinde ilişkilendirebilmekte, işlemleri gerçek zamanlı izleyebilmekte ve risk analizlerini sürekli güncelleyebilmektedir.

Şekil 7: Dijital Devlette Denetim Paradigmasının Dönüşümü

Bu dönüşümün en önemli bileşenlerinden biri Robotik Süreç Otomasyonu (RPA) teknolojileridir. RPA uygulamaları sayesinde tekrar eden denetim testleri, mevzuat kontrolleri, veri eşleştirme işlemleri ve belge doğrulama süreçleri yazılım robotları tarafından otomatik olarak gerçekleştirilebilmektedir. Böylece denetçilerin önemli ölçüde zaman alan rutin kontroller yerine yüksek riskli alanlara ve analitik değerlendirmelere odaklanması mümkün hâle gelmektedir. RPA'nın sağladığı otomasyon, denetim süreçlerinde hem hız hem de doğruluk düzeyini artırırken, insan hatalarından kaynaklanan riskleri de önemli ölçüde azaltmaktadır.

Denetimde paradigma değişimini destekleyen ikinci önemli unsur ise İş Süreçleri Modellemesi (*Business Process Management*-BPM) yaklaşımıdır. Dijital devlet mimarisinde kamu hizmetlerinin iş akışları dijital ortamda modellenebilmekte ve süreçlerin dijital ikizleri oluşturulabilmektedir. Böylece yalnızca gerçekleşen işlemler değil, iş süreçlerinin tamamı sürekli izlenebilmekte; süreç içerisinde oluşabilecek darboğazlar, mevzuata aykırı işlemler veya olağan dışı hareketler daha gerçekleşme aşamasında tespit edilebilmektedir. Denetim, belirli dönemlerde gerçekleştirilen bağımsız bir faaliyet olmaktan çıkarak süreçlerin doğal bir bileşeni hâline gelmektedir.

Bu dönüşümün en önemli sonuçlarından biri de örneklem temelli denetim anlayışından tam popülasyon denetimine geçiştir. Geleneksel denetim yaklaşımında zaman ve kaynak kısıtları nedeniyle işlemlerin yalnızca belirli bir örneklemi incelenebilmekteydi. Oysa dijital devlet altyapılarında bütün işlemler elektronik ortamda kayıt altına alındığından ve büyük veri analitiği araçlarıyla işlenebildiğinden, teorik olarak tüm işlem evreninin (%100 popülasyonun) analiz edilmesi mümkün hâle gelmektedir. Böylece risk analizleri yalnızca geçmiş verilere değil, sürekli güncellenen işlem verilerine dayanmakta; anomali tespiti, olağan dışı davranışların belirlenmesi ve usulsüzlük

göstergelerinin erken aşamada ortaya çıkarılması mümkün olmaktadır.

Yapay zekâ teknolojilerinin denetim süreçlerine entegre edilmesi ise bu dönüşümü daha ileri bir aşamaya taşımaktadır. Makine öğrenmesi algoritmaları büyük veri kümeleri içerisindeki olağan dışı örüntüleri tespit edebilmekte, farklı veri kaynakları arasında ilişki kurabilmekte ve yüksek risk taşıyan işlemleri otomatik olarak önceliklendirebilmektedir. Bunun yanında gerçek zamanlı gösterge panelleri sayesinde yöneticiler ve denetim birimleri, kurumların performansını, risk dağılımını ve kritik uyarıları anlık olarak takip edebilmektedir. Böylece denetim, geçmişte yaşanan hataları raporlayan bir mekanizma olmaktan çıkarak, karar alma süreçlerini destekleyen dinamik bir yönetişim aracına dönüşmektedir.

Bu yeni yaklaşımın ortaya çıkabilmesi ise önceki bölümlerde ele alınan kurumsal mimari, veri yönetişimi, ortak dijital altyapılar ve kamu veri alanı gibi bileşenlerin etkin biçimde işletilmesine bağlıdır. Çünkü yapay zekâ destekli analizler, süreç otomasyonu ve gerçek zamanlı denetim ancak standartlaştırılmış, güvenilir ve kurumlar arasında paylaşılabilir veri altyapıları üzerinde çalışabilmektedir. Başka bir ifadeyle dijital devlet mimarisinde oluşturulan veri ekosistemi, yalnızca kamu hizmetlerinin iyileştirilmesini değil; aynı zamanda denetim kapasitesinin de köklü biçimde yeniden şekillenmesini sağlamaktadır.

Sonuç olarak dijital devlet çağında denetimin temel amacı artık yalnızca mevzuata uygunluğu sonradan kontrol etmek değildir. Yeni paradigma; gerçek zamanlı, risk odaklı, veri temelli ve yapay zekâ destekli sürekli güvence (*continuous assurance*) anlayışını esas almaktadır. Bu dönüşüm sayesinde denetim faaliyetleri fiziksel belge incelemesine dayalı reaktif bir yapıdan; kurumlar arası veri paylaşımını kullanan, tüm işlem evrenini analiz edebilen ve karar vericilere anlık iç görüler sağlayan proaktif bir yönetişim mekanizmasına dönüşmektedir. Dolayısıyla dijital devletin başarısı yalnızca vatandaşlara sunulan hizmetlerin dijitalleşmesiyle değil, bu hizmetlerin şeffaflığını, güvenilirliğini ve hesap verebilirliğini güvence altına alan yeni nesil dijital denetim anlayışının kurumsallaştırılmasıyla mümkün olacaktır.

SONUÇ

Bu bölümde ele alınan gelişmeler, dijital devletin teknolojik araçların kamu yönetiminde kullanılmasından ibaret olmadığını; devletin kurumsal kapasitesini, yönetişim anlayışını ve kamu değeri üretme biçimini yeniden tanımlayan stratejik bir dönüşüm modeli olduğunu göstermektedir. Günümüzde dijital devletin olgunluğu, çevrim içi hizmetlerin sayısından çok, verinin stratejik bir kamu varlığı olarak yönetilmesi, kurumlar arasında birlikte çalışabilirliğin sağlanması, yapay zekâ destekli karar mekanizmalarının geliştirilmesi ve vatandaş odaklı hizmetlerin kamu değeri üretecek şekilde tasarlanabilmesiyle değerlendirilmektedir.

Bu çerçevede Türkiye, e-Devlet Kapısı, dijital kimlik altyapıları, ulusal bilgi sistemleri ve kurumlar arası entegrasyon alanlarında önemli bir kurumsal kapasite oluşturmuş; uluslararası endekslerde dikkat çekici ilerlemeler kaydetmiştir. Bununla birlikte dijital devlet olgunluğunun bir üst seviyeye taşınabilmesi; veri yönetişiminin güçlendirilmesi, açık veri ve hizmet inovasyonu ekosisteminin gelişmesi, yapay zekâ destekli kamu hizmetlerinin yaygınlaştırılması ve ortak dijital platformların bütüncül bir yönetişim anlayışı içerisinde işletilmesine bağlıdır. Bu doğrultuda önerilen hedef dijital devlet mimarisi, yalnızca yeni teknolojilerin sisteme eklenmesini değil; kamu kurumlarının ortak veri, ortak mimari ve ortak yönetişim ilkeleri etrafında bütünleşmesini amaçlamaktadır.

Bu dönüşümün doğal sonuçlarından biri de kamu denetiminin yeniden şekillenmesidir. Ortak veri altyapıları, süreç otomasyonu ve yapay zekâ destekli analiz yetenekleri sayesinde denetim faaliyetleri, geçmişe dönük belge incelemelerinden gerçek zamanlı, risk odaklı ve sürekli güvence sağlayan bir yapıya evrilmektedir. Böylece dijital devlet, yalnızca kamu hizmetlerinin etkinliğini artıran bir model değil; aynı zamanda şeffaflığı, hesap verebilirliği ve kurumsal güveni güçlendiren yeni bir yönetişim paradigması hâline gelmektedir.

Dolayısıyla dijital devletin geleceği, yeni teknolojilerin kamu sektörüne aktarılmasından ziyade; bu teknolojilerin güçlü

yönetişim mekanizmaları, veri temelli karar alma süreçleri ve kamu değeri odaklı bir yönetim anlayışıyla bütünleştirilmesine bağlıdır. Başarı ölçütü artık ne kadar hizmetin dijitalleştiği değil, dijital teknolojiler aracılığıyla vatandaş, kamu kurumları ve toplum için ne ölçüde sürdürülebilir kamu değeri üretilebildiğidir.

KAYNAKÇA

Bindu, N., Sankar, C.P. ve Kumar, K.S. (2019). From conventional governance to e-democracy: Tracing the evolution of e-governance research trends using network analysis tools. Government Information Quarterly, 36(3), 385-399.

Brown, A., Fishenden, J., Thompson, M. ve Venters, W. (2017). Appraising the impact and role of platform models and Government as a Platform (GaaP) in UK Government public service reform: towards a Platform Assessment Framework (PAF). Government Information Quarterly, 34(2), 167-182.

Demirel, D. (2006). E-Devlet ve Dünya Örnekleri. Sayıştay Dergisi, 61, 83-118.

Erlenheim, R., Draheim, D. ve Taveter, K. (2020). Identifying design principles for proactive services through systematically understanding the reactivity-proactivity spectrum. Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance (ICEGOV '20). New York: Association for Computing Machinery.

Ho, A. T. (2002). Reinventing Local Governments and the E-Government Initiative. Public Administration Review, 62(4), 434-444.

Internal Revenue Service (1996). IRS Historical Fact Book: A Chronology 1646-1992. Chamblee: IRS FOIA Request.

Janssen, M., Charalabidis, Y. ve Zuiderwijk, A. (2012). Benefits, Adoption Barriers and Myths of Open Data and Open Government. Information Systems Management, 29, 258–268.

Jetzek, T., Avital, M. ve Bjorn-Andersen, N. (2014). Data-Driven Innovation through Open Government Data. Journal of Theoretical and Applied Electronic Commerce Research, 9(2), 100-120.

KGM (t.y.). Türkiye'de Kullanılan İlk Bilgisayar. https://www.kgm.gov.tr/sayfalar/kgm/sitetr/galeri/ilkbilgisayar.aspx, Erişim: 14.04.2026.

Lindgren, I. ve Melin, U. (2017). Time to Refuel the Conceptual Discussion on Public e-Services – Revisiting How e-Services Are Manifested in Practice. Proceedings of the 16th International Conference on Electronic Government (EGOV). St. Petersburg: EGOV.

Mehr, H. (2017). Artificial Intelligence for Citizen Services and Government. Cambridge: Ash Center for Democratic Governance and Innovation

Mergel, I., Edelmann, N. ve Haug, N. (2019). Defining digital transformation: Results from expert interviews. Government Information Quarterly, 36(4), 1-16.

Nikiforova, A., Rodriguez Müller, A.P., Tangi, L. ve Martin-Bosch, J. (2026). Proactive Public Services in the Age of Artificial Intelligence: Towards Post-Bureaucratic Governance. Electronic Government (EGOV 2025) Lecture Notes in Computer Science, vol 15944. Cham: Springer.

OECD. (2014). Recommendation of the Council on Digital Government Strategies. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406/, Erişim: 13.07.2026.

OECD (2021). The E-Leaders Handbook on the Governance of Digital Government, OECD Digital Government Studies. Paris: OECD Publishing.

OECD (2024). 2023 OECD Digital Government Index. https://www.oecd.org/en/publications/2023-oecd-digital-government-index_1a89ed5e-en.html, Erişim: 12.05.2026.

OECD (2025). Harnessing Artificial Intelligence in Social Security: Use Cases, Governance and Workforce Readiness, OECD Digital Government Studies. Paris: OECD Publishing.

OECD (2026). Digital Government Outlook 2026: From Foundations to Transformational Impact. Paris: OECD Publishing.

OECD OPSI (2024). Life event-based services in Estonia. https://oecd-opsi.org/innovations/life-event-based-services-in-estonia/, Erişim: 13.07.2026.

Okçu, M., Usta, S. ve Ceyhan, H. (2020). Değişen Kamu Yönetimi Anlayışı ve Bürokrasi ve Kültürü. KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi, 22(39), 291-311.

O'Reilly, T. (2011). Government as a Platform. Innovations: Techno-

logy, Governance, Globalization, 6, 13-40.

Polatoğlu, A. (1994). Türk Kamu Yönetiminde Bilgisayar Kullanma Alanları ve Sorunlar. Amme İdaresi Dergisi, 27(4), 63-81.

Sevinç Çubuk, E. B. (2026). Human and Institutional Capacity in Public Sector AI Adoption: Evidence from OECD OPSI Cases. Iğdır Üniversitesi Sosyal Bilimler Dergisi, 42, 108-128.

T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı [SBB] (2023). On İkinci Kalkınma Planı (2024-2028) e-Devlet Hizmetlerinin Geliştirilmesi Çalışma Grubu Raporu. Ankara: SBB.

T.C. Başbakanlık Devlet Planlama Teşkilatı (2000). Sekizinci Beş Yıllık Kalkınma Planı (2001-2005). Ankara: DPT.

Twizeyimana, J.D. ve Andersson, A. (2019). The public value of E-Government – A literature review. Government Information Quarterly, 36(2), 167-178.Ubaldi, B. (2013). Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives. OECD Working Papers on Public Governance, 22.

Wirtz, B.W., Weyerer, J.C. ve Geyer, C. (2019). Artificial Intelligence and the Public Sector—Applications and Challenges. International Journal of Public Administration, 42(7), 596-615.

World Bank (2020). GovTech: The New Frontier in Digital Government Transformation. https://documents1.worldbank.org/curated/en/898571612344883836/pdf/GovTech-The-New-Frontier-in-Digital-Government-Transformation.pdf, Erişim: 14.07.2026.

https://www.turkiye.gov.tr/edevlet-istatistikleri

DİJİTAL TEKNOLOJİLERİN FİNANSI DÖNÜŞTÜRÜCÜ ETKİSİ VE FİNANSIN GELECEĞİ

Gürdoğan YURTSEVER
Mevzuat Uyum Derneği Kurucu ve Onursal Başkanı

ÖZET

Dijital teknolojilerde son yıllarda yaşanan gelişmeler tüm dünyayı, ekonomik ve toplumsal hayatı derinden etkilemekte ve hızla değişmesine neden olmaktadır. Geleneksel iş modelleri kökten değişmekte, bazı meslekler ortadan kalkmakta, yeni iş yapış şekilleri ve meslekler ortaya çıkmaktadır. Finans; bu teknolojilerin en fazla etkilediği ve değiştirdiği alanlardan birisi olarak büyük bir değişim ve dönüşüm geçirmektedir. Yeni geliştirilen finansal teknoloji çözümleri, finansal hizmetleri derinden etkilemektedir. Bu etki yalnızca bir veya bir kaç teknolojiye indirgenemeyecek şekilde geniş boyutludur. Birçok yeni teknoloji finansal hizmetlerin şeklini değiştirmekte ve bu dönüşümün merkezinde yer almaktadır. Bu gelişmeler dünya ekonomisinin en önemli itici güçlerinden olan finansın geleneksel değer yapısına yenilerinin eklenmesine, genişlemesine ve yeni değer alanlarının ortaya çıkmasına neden olmaktadır. Finansı etkileyen dijital teknolojiler ve bunlardan hareketle finansın geleceğine yönelik değerlendirmeler yapılması, bu sürecin doğru bir şekilde anlaşılmasına ve geleceğe yönelik bakış açısının genişletilmesine katkı sağlayabilecektir. Bu nedenle bu çalışmada finansı etkileyen dijital teknolojiler ortaya konulmaya ve bunlardan hareketle finansın geleceğine yönelik değerlendirmelerde bulunulmaya çalışılacaktır.

Anahtar Kelimeler: Dijital Teknolojiler, Finansal Teknolojiler, FinTech, Finansın Geleceği

GİRİŞ

Bilişim ve iletişim teknolojileri başta olmak üzere dijital teknolojilerde yaşanan baş döndürücü gelişmeler, ekonomik ve toplumsal hayatın hemen her alanında köklü değişimlere yol açmaktadır. Geleneksel iş modelleri kökten değişmekte, bazı meslekler ortadan kalkmaktadır. Yeni iş yapış şekilleri ve meslekler ortaya çıkmaktadır. İnternet, mobil teknolojiler, bulut bilişim, büyük veri, veri analitiği, yapay zeka, robotik teknolojiler, makine öğrenmesi, otonom araçlar, üç boyutlu yazıcılar, nesnelerin interneti, giyilebilir teknolojiler, sanal/arttırılmış gerçeklik teknolojileri, kripto paralar/varlıklar, blockchain, nanoteknoloji, genetik, uzay araştırmaları, kuantum bilgisayar gibi alanlarda önemli gelişmeler yaşanmaktadır. Dijital teknolojilerdeki gelişmeler, birbirini besleyen yeniliklerin etkisiyle giderek hızlanan ve üstel nitelik taşıyan bir büyüme eğilimi sergilemektedir.

Bütün bu gelişmeler ürün ve hizmetlerin yanı sıra üretim, dağıtım, karar verme, gözetim ve kullanıcı deneyimi gibi tüm alanların değişmesine neden olmaktadır. Finans alanı ise bu büyük değişimin en yoğun hissedildiği ve doğrudan etkilediği sektörlerin başında gelmektedir. Yeni geliştirilen finansal teknoloji çözümleri, finansal hizmetleri derinden etkilemektedir. Bu etkinin yalnızca bir veya bir kaç teknolojiye indirgenemeyecek şekilde geniş boyutlu olduğunu ifade etmek yanlış olmayacaktır. Bu dönüşümün merkezinde FinTech ve InsurTech girişimleri, TechFin platformları, blokzincir ve merkeziyetsiz finans, açık bankacılık ve açık finans uygulamaları, servis modeli bankacılığı/finansı, gömülü/görünmez finans, kripto varlıklar ve tokenizasyon, büyük veri ve bulut bilişim mimarileri, yapay zeka ve makine öğrenmesi, nesnelerin interneti, merkez bankası dijital paraları, RegTech çözümleri, süper uygulamalar, sosyal medya finansı, kitle fonlaması ve kuantum finans gibi teknolojiler, iş modelleri ve uygulama yaklaşımlarının yer aldığı görülmektedir.

Bu teknolojiler ve bunların birlikte oluşturduğu yeni mimari finansın geleneksel yapısını derinden etkilemekte ve değiştirmektedir. Bu gelişmeler dünya ekonomisinin en önemli itici güçlerinden olan finansal hizmetlerin geleneksel değer yapısına yenilerinin eklenmesine ve yeni değer alanlarının

ortaya çıkmasına neden olmaktadır. Bu teknolojilerden hareketle finansın geleceğine yönelik değerlendirmeler yapılması, bu sürecin daha iyi anlaşılabilmesine ve finansal alandaki bu değişimin yakalanabilmesine önemli katkılar sağlayabilecektir. Bu nedenle bu çalışmada finansı değiştiren dijital teknolojiler ortaya konulmaya ve bunlardan hareketle finansın geleceğine yönelik değerlendirmelerde bulunulmaya çalışılacaktır. Bu kapsamda çalışmanın ilk bölümünde finansı etkileyen dijital teknolojiler ortaya konulacak, ikinci bölümde ise bu gelişmelerden hareketle finansın geleceğine yönelik değerlendirmeler yapılacak ve finansın geleceğine yönelik öngörülerde bulunulacaktır.

I. Finansı Dönüştüren Dijital Teknolojiler

Başta bankacılık, sigortacılık, sermaye piyasaları olmak üzere finansal sistem; üretim, yatırım, ticaret ve tüketim faaliyetlerini birbirine bağlayarak küresel ekonominin işleyişinde merkezi bir rol üstlenmekte ve ekonominin temel itici güçlerinden birisini oluşturmaktadır. Bilişim ve iletişim teknolojileri başta olmak üzere dijital teknolojilerde yaşanan baş döndürücü gelişmeler, ekonomik ve toplumsal hayatın hemen her alanında köklü değişimlere yol açtığı gibi finansı da derinden etkilemekte ve dönüştürmektedir. Bu etkinin yalnızca bir veya bir kaç teknolojiye indirgenemeyecek şekilde geniş boyutlu olduğunu ifade etmek yanlış olmayacaktır. Bu dönüşümün merkezinde yer alan dijital teknolojilere ve bu teknolojilere dayalı olarak ortaya çıkan iş modeli ve uygulama yaklaşımlarına aşağıda yer verilecektir. **Dijitalleşme:** Bankalar, sigorta şirketleri, aracı kurumlar ve diğer finans kuruluşları tarihsel olarak ürün ve hizmetlerini büyük ölçüde fiziksel şubeler, acenteler, temsilciler ve yüz yüze müşteri ilişkileri üzerinden sunan kurumsal yapılar olarak gelişmiştir. Bununla birlikte bilişim teknolojilerinde yaşanan gelişmeler finans kuruluşlarını doğrudan etkilemiş ve bu kuruluşların hem iç operasyonlarında hem de müşteriye sundukları ürün, hizmet ve dağıtım kanallarında hızlı bir dijitalleşme yaşanmıştır. İnternet ve mobil bankacılık, ATM, telefon bankacılığı, kartlı ödemeler gibi başta bankacılık alanında görülen ve daha sonra diğer finans kuruluşlarını da içine alan dijitalleşme sayesinde bu şirketlerin dijital süreçleri ve hizmet kanalları giderek çeşitlenmiş ve kullanımı hızla artmıştır

(Gomber, Koch ve Siering, 2017). Bu eğilim günümüzde de devam etmektedir. Finansta dijitalleşme, finansal ürünlerin elektronik ortama taşınmasından ibaret olmayıp müşteri ediniminden kimlik doğrulamaya, ödemeden tasarrufa, krediden sigortaya kadar tüm süreçlerin veri temelli ve yazılım ağırlıklı hale gelmesini içermektedir. Dijitalleşme ile birlikte finans kuruluşlarının yüz yüze hizmet kanallarının kullanımı giderek azalmakta ve yüz yüze olmayan dijital kanalların kullanımı artmaktadır. Bunların yanı sıra finans kuruluşlarının dijital ürün ve hizmetleri artmakta, her geçen gün yeni ürün ve hizmetler geliştirilmektedir. Bu şekilde başta bankalar olmak üzere finans kuruluşları giderek dijital organizasyonlara dönüşmektedir.

FinTech ve InsurTech: Finansal teknoloji (Financial Technology) kavramının kısaltması olan "FinTech (Fintek)", finansal ürün ve hizmetlerin teknoloji kullanılarak yenilikçi biçimde kullanıcı ve müşterilere sunulmasını ifade etmektedir. FinTech yaklaşımının sigortacılık sektöründeki yansıması, sigorta teknolojileri (Insurance Technology) anlamına gelen "InsurTech" kavramıyla ifade edilmektedir. Bu kavramları finansta bilgi üretim süreçleri, maliyet yapısı ve rekabet mantığını değiştiren bir paradigma olarak ifade etmek de yanlış olmayacaktır. Finansal teknolojiler alanında giderek hızlanan inovasyon sayesinde FinTech büyük bir endüstri haline dönüşmüştür (Eric, 2022). FinTech ve InsurTech girişimleri ile geliştirilen finansal teknoloji çözümleri finansal hizmetlerin bankalar ve sigorta şirketleri dışından daha hızlı, kolay ve düşük maliyetle gerçekleştirilmesine katkı sağlamakta, finans ve sigortacılığı dijital bir kanalın ötesine taşıyarak dönüştürmektedir. FinTech ve InsurTech sayesinde alışageldiğimiz geleneksel finansal sistemler yerlerini yeni, hızlı, dinamik ve aracısız sistemlere bırakmakta ve bu girişimler geleneksel finansa çok önemli bir alternatif olarak karşımıza çıkmaktadır (Yurtsever, 2017, Ekim). Değişen makroekonomik ve düzenleyici ortam, teknolojinin hızlı evrimi ile değişen müşteri beklentileri FinTech alanında yaşanan bu hızlı değişimin temel katalizörleri olarak karşımıza çıkmaktadır (Arslanian ve Fischer, 2019).

TechFin: TechFin kavramı, finans kökenli şirketlerin teknolojiyi kullanmasından farklı olarak, başlangıç noktası teknoloji ve veri

olan şirketlerin finans alanına girmesini ve finansal hizmetler vermesini ifade etmektedir. Teknoloji, telekomünikasyon ve e-ticaret gibi sektörlerde faaliyet gösteren firmalar kendi iş kollarından topladıkları verileri ve yanı sıra teknoloji yetkinliklerini finansal hizmetler alanında avantaja çevirmekte ve finansal hizmetler vermektedir. Apple, Google, Amazon, Alibaba, Uber, Tencent gibi büyük teknoloji firmalarını bu kapsamda belirtmek mümkündür. Bu firmalar tarafından platformları üzerinden ödeme, kredi ve diğer finansal hizmetler vermektedirler (Zetzsche vd., 2017). Bu şekilde teknoloji firmaları bankacılık, sigortacılık gibi finansal hizmetler alanında da faaliyetlerini genişletmektedir. Bu şekilde teknoloji şirketleri bankalara, sigorta şirketlerine ve diğer finans şirketlerine rakip olmakta, hatta hızlı ve çevik yapıları nedeniyle rekabette öne geçmektedirler (Yurtsever, 2021).

Blockchain ve merkeziyetsiz finans: Blockchain (Blokzincir) teknolojisi, kayıt tutma, mutabakat ve transfer süreçlerini merkezi bir otoriteye bağımlı kalmadan gerçekleştirmeye imkan sağlayan bir teknolojidir (Catalini ve Gans, 2019). Blockchain değer paylaşımı dönemini başlatan önemli bir teknoloji olarak karşımıza çıkmaktadır. Pek çok alanda kullanımı mümkün olan bu teknolojinin özellikle finans alanında büyük bir dönüşüme neden olacağı öngörülmektedir (Yurtsever, 2018, Mart). Blockchain ile birlikte merkeziyetsiz finans (Decentralized Finance-DeFi) uygulamaları ön plana çıkmaya başlamıştır. DeFi, geleneksel finansal hizmetlerin banka, borsa veya aracı kurum gibi merkezi yapılar yerine blokzincir üzerinden gerçekleştirmesine imkan sağlayan bir yaklaşım ve uygulama ekosistemidir. Bir anlamda blokzincir temelli yeni bir finansal altyapı olarak ifade etmek mümkündür. Bu yapıda ödeme, borç verme/alma, yatırım, sigorta gibi finansal anlaşmalar akıllı sözleşmeler (smart contracts) yoluyla kod ile yapılmakta, işlemler güvenli ve doğrulanabilir bir şekilde gerçekleştirilmece ve blok zincirinde kalıcı hale gelmektedir (Schar, 2021).

Açık finans (open finance), açık bankacılık (open banking) ve açık sigortacılık (open insurance): Finansal hizmetleri dönüştüren teknoloji ve yaklaşımlardan birisini de açık bankacılık, açık sigortacılık ve daha geniş çerçevede "açık finans (open finance)"

olarak ifade etmek yanlış olmayacaktır. Açık finans, finans şirketlerinin müşterilerine ilişkin bilgileri, yine müşterilerinin izinleri ile üçüncü taraf niteliğindeki fintek şirketlerinin kullanımına açması anlamına gelmektedir. (Yurtsever, 2019, Temmuz). Verinin kuruma değil müşteriye ait olduğu ve kurumların yalnızca müşteri izniyle o verilere erişebildiği bir gelecek açık finans ile mümkün hale gelmektedir. Açık finans, müşteri izniyle finansal verilerin standartlaştırılmış uygulama programlama arayüzleri (Application Programming Interface, API'ler) üzerinden üçüncü taraflarla güvenli şekilde paylaşılmasını mümkün kılmaktadır (Babina vd., 2025). API'ler, farklı yazılım sistemlerinin ortak bir dille birbiriyle iletişim kurmasını sağlayan, teknolojik birlikte çalışabilirliği ve modülerliği mümkün kılan araçlardır (Zachariadis ve Özcan, 2017). API geliştirme ve iş birlikleri yeni hizmet modellerini desteklemektedir (Stefanelli, Manta ve Toma, 2022). Bu şekilde fintek şirketleri elde ettikleri müşteri verilerini etkili bir şekilde kullanarak yeni, daha düşük maliyetli ve hızlı ürün ve hizmetler geliştirme imkanı bulmaktadır. Bu durum da finansal hizmetlerde rekabeti, yenilikçiliği, müşteri kontrolü ve kişiselleştirilmiş hizmet verilmesini güçlendirmektedir.

Servis modeli finans/bankacılık/sigortacılık (Banking-as-a-Servis): Servis modeli, bankaların ve diğer finansal kuruluşların ürün ve altyapılarını yalnızca kendi kapalı kanalları üzerinden sunmaları yerine, API'ler, platformlar ve üçüncü taraf iş birlikleri aracılığıyla modüler hizmetler halinde dış ekosistemlere açmalarını ifade etmektedir. Bu şekilde fintek şirketleri bankacılık ve finans lisansına sahip olmadan bu lisansa sahip firmalardan aldıkları API'ler vasıtasıyla finansal hizmetler verebilme imkanına kavuşmaktadır. Bu model finansal hizmetlerde yeni örgütsel yapılar ve platform iş modelleri ortaya çıkarmaktadır (Zachariadis ve Özcan, 2017). Servis modeli bankacılık finansal ürün ve hizmetlerin çeşitlendirilmesine ve müşteri deneyiminin iyileştirilmesine katkı sağlamaktadır (Stefanalli, Manta ve Toma, 2022). Servis modeli, finansal hizmetlerin kurum odaklı kapalı yapılardan ekosistem, platform, iş birliği ve gömülü/görünmez finans mantığına dayalı daha açık, esnek ve ölçeklenebilir yapılara dönüşmesinde kritik bir rol üstlenmektedir. Bir anlamda finansal

hizmetler kuruma ait bir ürün olmaktan çıkıp farklı platformlara dağıtılmış modüler servisler haline dönüşmektedir.

Gömülü/görünmez finans (Embedded/Invisible Finance): Gömülü/görünmez finans, finansal hizmetlerin ayrı bir banka veya finans kuruluşu kanalı üzerinden değil, müşterinin günlük dijital deneyimi içinde fark edilmeden, kesintisiz ve gömülü/görünmez biçimde sunulmasını ifade etmektedir. Bir anlamda finansal kuruluşlar fintek ve API ortaklıkları ile müşterilerine her zamankinden daha fazla yakın hale gelmekte fakat fiziksel olarak görünmez hale dönüşmektedir (Stefanelli, Manta ve Toma, 2022). Bu sayede müşteriler örneğin bir e- ticaret sitesinden ürün satın alırken aynı zamanda alış veriş kredisi kullanabilir ve ürüne kredili olarak sahip olabilir. Bu şekilde kredi hizmeti bankanın kendi kanalından değil e- ticaret platformunun alışveriş sürecine gömülmüş olarak sunulmaktadır. Buna benzer şekilde alışveriş, seyahat, ulaşım, sağlık, eğitim, oyun, sosyal medya gibi birçok alanda ödeme, kredi, sigorta, yatırım gibi finansal hizmetler işlem akışına görünmez şekilde entegre edilmektedir. Gömülü/görünmez finansı müşterinin finansal hizmete ayrıca başvurmasını gerektirmeden ihtiyaç anında, uygun kanalda ve kişiselleştirilmiş biçimde sunulduğu yeni bir finansal hizmet paradigması olarak değerlendirmek mümkündür (Zachariadis ve Özcan, 2017).

Kripto varlıklar, kripto paralar ve tokenizasyon: Son dönemlerde giderek yaygınlaşan kripto varlıklar, kripto paralar ve tokenizasyon da finansı doğrudan ve çok boyutlu olarak etkileyen en önemli teknolojiler arasında yer almaktadır. Kripto varlıklar; kriptografik güvenlik, blokchain ve ağ katılımcıları arasında sağlanan mutabakat mekanizmaları aracılığıyla oluşturulan, transfer edilen ve saklanan dijital değer temsilleri olarak tanımlanabilir (Böhme, Christin, Edelman ve Moore, 2015). Bitcoin başta olmak üzere kripto paralar ise kripto varlıkların ödeme ve değer transferi işlevi öne çıkan alt türünü oluşturmaktadır. Volatilitesine ve risklerine rağmen kripto paralar bir çok işletme tarafından tıpkı kağıt ve madeni paralar gibi geçerli bir ödeme ve yatırım aracı olarak kabul edilmekte ve giderek yaygınlaşmaktadır (Yurtsever, 2014, Ocak). Tokenizasyon ise fiziksel veya finansal bir varlığın, hakkın

ya da ekonomik değerin blokzincir üzerinde dijital token olarak temsil edilmesi sürecidir (Barnes, 2020). Bu şekilde gayrimenkul, menkul kıymet, emtia veya sanat eseri gibi gerçek varlıklar NFT gibi değiştirilemez tokenler sayesinde dijital olarak da temsil edilebilmekte, alım ve satıma konu edilebilmektedir.

Büyük veri, veri analitiği ve bulut bilişim teknolojileri: Son yıllarda finansı derinden etkileyen alanlardan birisi de büyük/mega veri, veri analitiği ve bulut bilişim teknolojileridir. Finansal sektörde büyük veri; müşteri işlemleri, ödemeler, kredi başvuruları, piyasa verileri, çağrı merkezi kayıtları, mobil uygulama davranışları, sosyal medya izleri ve açık bankacılık verileri gibi yapılandırılmış ve yapılandırılmamış çok sayıda kaynaktan beslenmektedir (Chen, Chiang ve Storey, 2012; Zachariadis ve Özcan, 2017). Bu büyük veri kümeleri yeni teknolojiler, istatistiksel yöntemler, veri madenciliği gibi yöntemlerle çok daha etkili bir şekilde işlenmekte, finansal hizmetlerde verimliliğin artmasına etkide bulunmaktadır. Bulut bilişim teknolojileri ise büyük teknoloji yatırımlarına ihtiyaç duyulmadan internet üzerinden büyük verinin kullanımına imkan sağlamakta ve veri analitiği çalışmalarını güçlendirmektedir (Yurtsever, 2015, Şubat). Bu şekilde finansal alanda veri temelli ve hızlı kararlar alınabilmekte, finansal ürünlerin etkinliği artırılmakta, yeni finansal ürün ve hizmetlerin geliştirilmesi mümkün olabilmektedir.

Yapay zeka, makine öğrenmesi ve robotik teknolojiler: Bugüne kadarki en önemli dönüşümlerden birisi olarak yaşamımızı her geçen gün daha da derinden etkileyen yapay zeka, makine öğrenmesi, derin öğrenme, doğal dil işleme, robotik vb. teknolojiler finansal hizmetleri de hızla değiştirmekte ve dönüştürmektedir. Bankacılık, sigortacılık, ödeme hizmetleri, yatırım, risk yönetimi gibi finansal hizmet süreçlerinde yapay zeka kullanımı hızla artmaktadır. Kredi değerlendirme, risk analizi ve ölçümü, portföy yönetimi, dolandırıcılık ve anomali tespiti, robo-danışmanlık gibi finansal hizmetlerin pek çok alanında yapay zeka ve makine öğrenmesi teknolojileri yoğun şekilde kullanılmaktadır. Yatırım ve varlık yönetimi alanında robo-danışmanlık uygulamaları, algoritmalar aracılığıyla müşterinin risk profili, yatırım hedefi ve davranışsal tercihlerini analiz ederek daha düşük

maliyetli, ölçeklenebilir ve kişiselleştirilmiş yatırım tavsiyesi sunabilmektedir (Alsabah, Capponi, Lacedelli ve Stern, 2019). Yapay zeka teknolojileri finansal ürün ve hizmetlerin verimliliğinin artırılması, risklerin daha etkili yönetilmesi, karar kalitesinin yükseltilmesi, kayıpların azaltılması, müşteri güvenliğinin güçlendirilmesi, kişiselleştirilmiş finansal yeni ürün ve hizmetlerin geliştirilmesi gibi pek çok alanda finansı derinden etkilemektedir (Yurtsever, 2016, Temmuz). İnsan müdahalesi olmadan otonom finans (Autonomous finance) şeklinde tasarruf/yatırım kararları verilmesi gibi yeni yaklaşımlar ortaya çıkmaktadır. Bunun yanı sıra finans kuruluşlarında kullanılan yapay zekanın açıklanabilir, yorumlanabilir, şeffaf, sorumlu, hesap verebilir ve güvenilir olması da hem risk yönetimi bağlamında hem de gözetim ve denetim çalışmaları bakımından önem taşımaktadır. Bu bağlamda açıklanabilir yapay zeka (Explainable AI-XAI) yaklaşım ve uygulamaları önem kazanmaktadır (Arrieta vd., 2020).

Nesnelerin interneti (internet of things, IoT) ve metaverse: Nesnelerin interneti; fiziksel nesnelerin sensörler ve internet aracılığıyla veri üretmesi, paylaşması ve çevresi ile etkileşime geçmesi olarak ifade edilmektedir (Yurtsever, 2016, Haziran). Büyük verinin oluşmasına önemli etkide bulunan nesnelerin interneti finansal hizmetlerde de önemli değişikliklere neden olmaktadır. IoT cihazları davranışsal, çevresel ve operasyonel veriler toplama konusunda benzersiz bir altyapı sunmaktadır (Gubbi vd., 2013). Bu şekilde elde edilen veriler kişiselleştirilmiş finansal ürünler, kullanım bazlı sigorta, dinamik fiyatlama, dolandırıcılık tespiti, teminat izleme ve müşteri risk profilinin daha doğru belirlenmesi gibi alanlarda önemli faydalar sağlayabilecek niteliktedir. Bu kapsamda sanal asistanlar, giyilebilir teknolojiler, sanal gerçeklik (VR) ile artırılmış gerçeklik (AR) çözümleri, hologram ve chatbot teknolojileri de finanstaki değişime etkide bulunmaktadır (Yurtsever, 2021). Metaverse ise fiziksel ve sanal alanların birleştiği, kullanıcıların avatarlar aracılığıyla eş zamanlı etkileşime girebildiği, artırılmış gerçeklik, sanal gerçeklik, blokzincir, yapay zeka ve ağ teknolojileriyle desteklenen dijital ortamlar bütünü olarak tanımlanmaktadır (Mystakidis, 2022). Yakın zaman önce çok popüler hale gelen metaverse ile ilgili başlangıçtaki hızlı gelişimin yavaşladığı görülse de finansal

hizmetleri etkileyebilecek önemli alanlardan birisi olarak karşımıza çıkmaktadır. Sanal banka şubeleri, dijital müşteri temsilcileri, sanal yatırım danışmanlığı, finans eğitim simülasyonları gibi çok çeşitli alanlarda finansı etkilemesi olası görünmektedir.

Sürdürülebilirlik/Yeşil Finans: Tüm dünyayı derinden etkileyen iklim krizi, bununla bağlantılı sürdürülebilirlik çalışmaları ve bu kapsamda geliştirilen teknolojiler de geleneksel finansı temelden değiştiren bir başka önemli faktör olarak karşımıza çıkmaktadır. Bir şirketin yalnızca finansal performansının değil çevresel, sosyal ve yönetişimsel (Environmental, Social, Governance-ESG) sorumluluklarını da değerlendirmeyi içeren ESG performansı yatırımcılar ve kredi verenler açısından giderek daha önem verilen ve belirleyici bir unsur haline gelmektedir. Çevresel sürdürülebilirliği destekleyen ve iklim değişikliğiyle mücadeleye katkı sağlayan proje, faaliyet ve yatırımların finansmanı olarak ifade edilen sürdürülebilir ve yeşil finans uygulamaları giderek artmaktadır. Etki yatırımları hızla genişleyen bir alan olarak dikkat çekmektedir. Bu kapsamda yeşil kredi, karbon kredisi, yeşil tahvil, yenilenebilir enerji finansmanı, enerji verimliliği finansmanı, temiz ulaşım finansmanı, ESG temelli yatırım fonları gibi uygulamalar gelişmektedir. Bunun yanı sıra Green FinTech ve Sustainable FinTech ile bu alanda teknolojik çözümler geliştirilmektedir. Puschmann, Hoffmann ve Khmarskyi (2020) tarafından yapılan çalışmada incelenen örnekler ve sektörel bulgular; Green FinTech uygulamalarının büyük veri, yapay zeka, blokzincir ve açık finans platformlarından yararlanarak ESG veri analitiği, iklim riski ölçümü, sürdürülebilir portföy yönetimi ve robo-danışmanlık gibi alanlarda düşük maliyetli ve yenilikçi çözümler geliştirdiğini göstermektedir. Bu nedenle sürdürülebilirlik ve yeşil finans, başta bankacılık olmak üzere finansın her alanını etkileyen dönüştürücü bir paradigma haline gelmiştir.

Merkez Bankası Dijital Parası (Central Bank Digital Currency, CBDC): Finansı etkileyen önemli gelişmelerden birisini de dijital merkez bankası parası olarak ifade etmek mümkündür. Bir devletin merkez bankası tarafından ihraç edilen ve güvence altına alınan, ulusal para biriminin tamamen dijital formu olarak ifade edilebilecek Merkez Bankası Dijital Parası (Central

Bank Digital Currency-CBDC) finansta dijitalleşmenin yeni bir aşamasını oluşturmaktadır. Birçok ülkede bu konuda çalışmalar yürütülmektedir. Kağıt veya madeni paraların dijital hali olan merkez bankası dijital parası, finanstaki dijitalleşmenin ileri aşamaya geçmesine, finansal teknolojiler alanındaki inovasyonun artmasına, yeni finansal ürün ve hizmetlerin ortaya çıkmasına katkı sağlayabilecek ve finansın geleceğine etkide bulunabilecek nitelikte bir gelişmedir (Yurtsever, 2025, Eylül). Merkez bankası dijital parası ödeme sistemlerinde ulusal paranın dijital ekonomideki rolünü güçlendirebilecek, daha hızlı, düşük maliyetli ve kapsayıcı ödeme altyapıları sağlayarak finansal sistemin işleyişine dönüştürücü etkide bulunabilecektir (Auer ve Böhme, 2020).

Regülasyon teknolojileri (RegTech): Finansı etkileyen düzenlemeler giderek artmakta ve sıkılaşmaktadır. Bu düzenlemeleri takip etmek ve etkili bir şekilde finansal kuruluşlarda hayata geçirmek giderek zorlaşmaktadır. Bunun yanı sıra kişisel verilerin korunması, bilgi güvenliği gibi alanlarda gizlilik gereksinimleri giderek artmaktadır. Ayrıca dijitalleşmenin artmasıyla birlikte suistimal, dolandırıcılık, suç gelirlerinin aklanması, terörizmin finansmanı, siber saldırılar, deepfake, yapay zeka destekli kimlik sahtecilikleri gibi finansal riskler ve suçlar giderek artmaktadır. Bu nedenlerle hem düzenlemelere uyum sağlanması, hem de finansal suçlarla etkili mücadele edilmesi için geleneksel kural bazlı yöntemler yeterli gelmemektedir. Bunun için yapay zeka, makine öğrenmesi tabanlı erken uyarı sistemleri, anomali tespiti, davranış analizi gibi yöntemler kullanılması büyük önem kazanmaktadır. Bu kapsamda regülasyon teknolojileri (RegTech) ve hukuk teknolojileri (LegalTech) finansı etkileyen bir alan olarak hızla gelişim göstermektedir. Artan, sıkılaşan ve giderek karmaşıklaşan yasal düzenlemeler nedeniyle finans şirketleri regülasyon teknolojileri kullanmaya yönelmektedirler (Yurtsever, 2020 Temmuz). Regülasyon teknolojileri, finansal kuruluşların raporlama, gözetim ve mevzuat uyum yükümlülüklerini teknolojiden yararlanarak daha hızlı, izlenebilir ve düşük maliyetli yerine getirmelerine imkan sağlayan yeni bir finansal teknoloji alanı olarak ortaya çıkmıştır (Arner, Barberis ve Buckley, 2017). Düzenlemelerin takibi, uygulanması, kimlik tespiti, müşterini tanı (know your customer, KYC), suç gelirlerinin aklanmasının

önlenmesi (anti-money laundering, AML), yaptırım taraması, işlem izleme, dolandırıcılık tespiti, uzaktan kimlik tespiti, dijital müşteri edinimi, düzenleyici otorite raporlaması gibi çok çeşitli alanlarda RegTech çözümleri giderek yaygınlaşmaktadır. Bunların yanı sıra düzenleyici ve denetleyici otorite teknolojileri olan (Supervisory Technology, SupTech) ise düzenleyici kurumların finansal kuruluşlardan gelen büyük hacimli verileri daha etkin analiz etmesine, uzaktan gözetim yapmasına, risk temelli denetim modelleri geliştirmesine ve piyasa bütünlüğünü gerçek zamanlıya yakın biçimde izlemesine imkan sağlamaktadır (Broeders ve Prenio, 2018). Bu şekilde regülasyon teknolojileri destekleyici bir teknoloji olmaktan çıkarak mevzuat uyum, finansal suçlarla mücadele, veri yönetişimi, dijital kimlik, yapay zeka denetimi, gerçek zamanlı gözetim ve risk temelli düzenleme anlayışının merkezinde yer alan temel bir finansal altyapı unsuruna dönüşmektedir (Arner, Barberis ve Buckley, 2017).

Diğer teknolojiler ve gelişmeler: Bunların yanı sıra kitle fonlaması gibi yeni finansal fonlama modelleri, süper uygulamalar, sosyal medya finansı/bankacılığı, paylaşım ekonomisi, kuantum teknolojisi ve kuantum finans, uzay ekonomisi, uzay finansı, uzay muhasebesi gibi yeni teknolojiler ve gelişmeler de finansı doğrudan ve dolaylı olarak etkilemektedir. **Kitle fonlaması (crowdfunding)**, dijital platformlar aracılığıyla girişimlerin ve projelerin çok sayıda bireysel yatırımcıdan fon toplamasına imkan sağlamaktadır. Bu şekilde girişimciler banka kredisi dışında alternatif finansman kaynaklarına ulaşabilmekte ve sermaye tabanı genişlemektedir (Yurtsever, 2019, Ocak). Farklı sektörlerde çok sayıda hizmeti tek bir mobil veya dijital arayüzde sunan uygulamalar olarak ifade edilen ve farklı ülkelerde hızla gelişen **süper uygulamalar (SuperApps)** finansı da etkilemektedir. Bu uygulamalar üzerinden ödeme, transfer, kredi, sigorta gibi pek çok finansal işlem gerçekleştirilmektedir. Bunun yanı sıra farklı finansal hizmetleri bir araya getiren "finansal süper uygulamalar" da gelişmektedir (Yurtsever, 2024, Şubat). Giderek gelişen **sosyal medya** kanalları üzerinden finansal hizmet kanalları oluşmakta ve finansal işlemler yapılabilmektedir (Yurtsever, 2013, Şubat). Bunun yanı sıra hızla büyüyen **paylaşım ekonomisinin** temelini de finansal işlemler oluşturmakta ve bu durum finansal ürün, hizmet ve işlem

akışlarının yeniden tasarlanmasına neden olmaktadır. Kuantum bilgisayar teknolojisi ise mevcut bilgisayarların sınırlarını aşan finansal hesaplama ve problemlere çözüm üretme kapasitesi ile yeni bir dünyanın kapılarını açma (Yurtsever, 2019, Şubat) hatta mevcut finansı alt üst etme ve **kuantum finans** denilen yeni bir finans alanını ortaya çıkarma potansiyeli taşımaktadır (Orûs, Mugel ve Lizaso, 2018). Bunların yanı sıra Yapay zeka destekli yeni nesil uzay roketleri, uydular, uzay istasyonları ile hızlanan yeni uzay çağı büyük bir **uzay ekonomisinin** de ortaya çıkmasına neden olmaktadır. Uzay madenciliği, uzay turizmi, uzay otelleri, üs kurulması, uzay kolonileri gibi alanlarda çok önemli gelişmeler yaşanmaktadır. Uzay muhasebesi gibi yeni çalışma alanları çıkmaktadır (Yurtsever, 2026, Ocak). Bütün bu gelişmeler de yakın gelecekte finansın niteliğinin dönüşümüne etkide bulunacak ve uzay finansı gibi yeni alanların çıkmasına neden olabilecek bir başka faktör olarak karşımızda durmaktadır.

II. FİNANSIN GELECEĞİ

Önceki kısımda yer verilen yeni teknolojiler, yaklaşım ve modeller finansın her alanı doğrudan veya dolaylı olarak çok boyutlu bir şekilde etkilemektedir. Bu etkinin yalnızca bir veya bir kaç teknolojiye indirgenemeyecek şekilde geniş boyutlu olduğunu ifade etmek yanlış olmayacaktır. Bu teknolojiler ve bunların birlikte oluşturduğu yeni mimari finansın geleneksel yapısını değiştirmekte ve dönüştürmektedir. Bütün bu gelişmelerin finansal alanda neden olduğu makro ve mikro düzeyde değişimlere ve bunlarla bağlantılı olarak finansın geleceğine yönelik değerlendirmelere aşağıda yer verilmiştir.

Dijitalleşmenin ve dijital finans kuruluşlarının yükselişi: Finansal alanda yaşanan dijitalleşme ile finans kuruluşlarının şube, acente gibi fiziksel hizmet mekanları hızla azalırken, dijital kanalları ve bunların kullanımı hızla artmaktadır. Finansal ürünler dijital kanallara taşınmakta ve yeni dijital ürün ve hizmetler faaliyete alınmaktadır. Mobil bankacılık, dijital cüzdanlar, uzaktan kimlik tespiti, temassız ödemeler, elektronik para, çevrim içi yatırım platformları, dijital sigorta satış kanalları ve yapay zeka destekli müşteri temsilcileri gibi dijital uygulamalar, finansal hizmetin şube veya fiziksel ofis gerektirmeden sunulmasını mümkün kılmaktadır.

Ayrıca yeni finansal ürün ve hizmetlerin ortaya çıkmasına neden olmaktadır. Bunların yanı sıra fiziksel mekanı olmayan dijital banka (neobank) ve dijital finans kuruluşları faaliyete geçmektedir. Dijital finans kuruluşları, geleneksel finans kuruluşlarına göre daha hızlı ürün geliştirebilmekte ve daha düşük maliyetli hizmet sunabilmektedirler. Bu gelişimin hızlanarak sürmesi olasıdır. Finans kuruluşlarının büyük kısmı tam dijital kuruluşlar haline dönüşürken bir kısmının ise hibrit yapılara evrilerek karmaşık ürünler, ihtilaf yönetimi ve güven inşası gibi nedenlerle sınırlı fiziksel temas noktalarını korumaları olası görünmektedir. Bu dönüşüm, finansal kuruluşlar açısından yalnızca teknolojik yatırım ihtiyacı doğurmayacak; aynı zamanda organizasyon yapısı, insan kaynağı, risk yönetimi, mevzuat uyum, denetim, müşteri ilişkileri, strateji ve rekabet anlayışını da değiştirecektir.

Finansal aracılığa olan ihtiyacın azalması ve finansal aracıların niteliğinde değişim: Dijitalleşme ve teknolojik gelişmeler ile finansal aracıların niteliği de değişmektedir. Blokzincir teknolojisi ve merkeziyetsiz finans (DeFi) uygulamaları, banka, aracı kurum, takas kuruluşu veya merkezi borsa gibi geleneksel aracıların bazı işlevlerinin akıllı sözleşmeler ve protokoller aracılığıyla yerine getirilmesine imkan sağlamaktadır. Bu çerçevede borç verme, borçlanma, teminatlandırma, alım satım, likidite sağlama ve türev işlemler belirli ölçüde doğrudan kullanıcılar arasında ve yazılımsal protokoller üzerinden gerçekleşebilmektedir. Bu mekanizmalar mevcut durumda aracıları tamamen ortadan kaldırmak için yeterli olmasa da aracılara olan ihtiyacın giderek azaldığı bir finansal mimariye doğru geçiş yaşanmaktadır. Finansal aracılık kurumsal ve hukuki bir nitelikten daha çok teknoloji, veri ve protokol temelli bir aracılığa doğru evrilecektir.

Kurum odaklı kapalı yapıdan servis odaklı açık yapıya geçiş: Açık bankacılık, açık finans, servis modeli bankacılık gibi teknoloji ve uygulamalar finansal hizmetlerin "kurum içinde üretilen nihai ürün" kimliğini aşındırmaktadır. Bu durum bankacılığı ve finansı yalnızca bankaların veya finans kurumlarının sunduğu bir "ürün" olmaktan çıkarıp farklı sektörlerdeki platformların içine yerleşen bir "servis" katmanına dönüştürmektedir. Bankacılık ve finans hizmetleri artık e-ticaret sitesinde ödeme, seyahat uygulamasında sigorta, muhasebe yazılımında tahsilat, pazaryeri platformunda

satıcı finansmanı veya mobil uygulama içinde dijital cüzdan olarak karşımıza çıkabilmektedir. Böylece finansal hizmetin görünür yüzü banka ve finansal kuruluşlar değil, müşterinin işlem yaptığı platform olmakta ve müşteri işlem yaparken finansal hizmetleri bir servis olarak almaktadır. Geleceğin finansında kurumdan çok servis, tekil uygulamadan çok API, sahiplikten çok erişim mantığının ağır basacağı görülmektedir. Servis modelinin finansın geleceğinde önemli bir yaklaşım olarak hızla gelişmeye devam edeceğini ifade etmek yanlış olmayacaktır. Bu durum aynı zamanda finansal kuruluşlar için içe kapalı stratejilerden dışa açık stratejilere geçmelerini zorunlu hale getirecektir. Açık bankacılık ve API temelli servis modelleri, finansal kuruluşların ürün ve altyapılarını üçüncü taraf platformlara entegre etmesine imkan vererek bankacılığı kapalı kurum yapısından ekosistem temelli bir hizmet mimarisine dönüştürecektir (Zachariadis ve Özcan, 2017).

Ekosistem ve platform temelli yapıya dönüşüm: Açık bankacılık ve açık finans, müşteri verisini finans kuruluşlarının kendi kapalı sistemlerinde tutan tekil kurumlar olmaktan çıkararak API'ler üzerinden üçüncü taraflarla etkileşim kuran platformlara dönüşmesini hızlandırmaktadır. API ekonomisi finansal hizmetlerde dijital dönüşümün temel unsurlarından birisi haline gelmiştir ve açık bankacılık platform temelli iş modellerini güçlendirmektedir. (Zachariadis ve Özcan, 2017). Geleneksel finansal modelde bankalar, ödeme kuruluşları, sigorta şirketleri ve yatırım kuruluşları çoğunlukla kendi ürünlerini kendi kanallarından sunarken, yeni modelde farklı aktörler birlikte değer üretmektedir. Bankalar, Fintekler, büyük teknoloji şirketleri, e-ticaret platformları, telekom şirketleri, sosyal medya platformları, sigorta şirketleri, veri sağlayıcıları ve RegTech firmaları aynı finansal ekosistemin parçaları haline gelmektedir. Bu yapı, rekabetin yanında "rekaberlik" olarak ifade edilebilecek rekabet ve iş birliğinin aynı anda yürüdüğü hibrit ilişkileri artıracaktır. Bankalar ve finans kuruluşları Finteklerle rekabet ederken aynı zamanda onların teknolojik çevikliğinden yararlanacak; Fintekler ise bankaların ve finans kuruluşlarının lisans, güven, müşteri tabanı, bilanço ve uyum altyapısından faydalanacaktır. Bu şekilde teknoloji şirketleri, Fintekler ve finansal kuruluşlar arasında ortak bir üretim biçimi gelişecektir. Bu nedenle gelecekte başarılı finansal

kuruluşlar, her şeyi kendi içinde geliştiren kapalı kurumlar değil, dış paydaşlarla hızlı entegrasyon kurabilen, açık ve dinamik stratejiler geliştirebilen ve ekosistem yönetebilen kuruluşlar olacaktır. Süper uygulamalar ise mesajlaşma, alışveriş, ulaşım gibi hizmetleri ödeme, kredi, sigorta, yatırım gibi finansal hizmetler ile tek bir dijital ekosistemde birleştirerek platform içi bir deneyim haline dönüştürmektedir.

Finans kuruluşlarının giderek teknoloji kuruluşlarına dönüşümü: Gelecekte bankaların ve finans kuruluşlarının en kritik varlıkları yalnızca sermaye, mevduat, şube ağı veya bilanço büyüklüğü olmayacak; veri altyapısı, algoritmalar, yazılım geliştirme kapasitesi, siber güvenlik dayanıklılığı, bulut mimarisi, API yönetimi, yapay zeka yetkinliği gibi teknoloji odaklı hususlar rekabet avantajının merkezine yerleşecektir. Bu nedenle finansal kuruluşlar klasik anlamda finans kurumu olmanın yanında aynı zamanda veri işleyen, yazılım geliştiren, algoritmik karar sistemleri kuran, müşteri deneyimi tasarlayan ve teknoloji operasyonu yöneten kuruluşlara dönüşecektir. Rekabetin ekseni mevduat toplama kabiliyeti ile şube ağı olmaktan çıkıp, yazılım geliştirme hızı, veri işleme kapasitesi, siber dayanıklılık, ürün mimarisi ve kullanıcı deneyimi yetkinliğine kaymaktadır. Bu dönüşümü gerçekleştiremeyen kurumların yalnızca yeni Fintek girişimleriyle değil, finansal hizmetleri kendi platformlarına gömen teknoloji şirketleriyle de rekabet etmesi zorlaşacaktır.

Kişiye özel ürün ve hizmetlerin gelişimi, ihtiyaç bazlı kullanım ve kişiselleştirilmiş fiyatlama: Dijitalleşme ve teknolojik gelişim standartlaşmış ürün ve hizmetlerin yerine kişiye özgü, kişiselleştirilmiş ve terzi usulü ürün ve hizmetlerin ön plana çıkmasına neden olmaktadır. Geleneksel finansal sistemde ürünler çoğu zaman standartlaştırılmış durumdadır. Kredi, mevduat, sigorta, kredi kartı veya yatırım fonları gibi finansal ürünler genellikle standart olarak finansal kuruluşlar tarafından sunulmakta ve bunların müşteriye satış ve pazarlaması gerçekleştirilmektedir. Oysa büyük veri, yapay zeka, açık finans gibi teknolojiler ve veri analitiği sayesinde müşterinin gelir, harcama, risk, tercih, yaşam evresi, dijital davranış ve finansal

hedeflerine göre daha kişiselleştirilmiş ürünler sunulabilmesi mümkün hale gelmiştir. Müşteriden elde edilen çok kanallı veriler detaylı olarak analiz edilebilmekte ve müşteri ihtiyaç ve beklentileri daha doğru bir şekilde anlaşılabilmektedir. Buna göre de müşterinin ihtiyaçlarına uygun ürün ve hizmetler sunulması mümkün hale gelmektedir. İhtiyaç ve kullanım bazlı modeller gelişmektedir. İsteğe bağlı ve esnek, istenildiğinde başlatılabilen, durdurulabilen veya sonlandırılabilen finansal ürün ve hizmetler geliştirilmektedir. Bu kapsamda müşterinin anlık nakit ihtiyacına göre kredi kullanması, kullandığı kadar sigorta primi ödemesi, kullanıcı alışkanlıklarına göre otomatik indirimler yapılması gibi kişiselleştirilmiş ve modüler ürün ve hizmetler giderek daha fazla yaygınlaşacaktır. Kişiselleştirilmiş fiyatlama da geleceğin finansının önemli unsurlarından biri olacaktır. Finansal kuruluşlar, müşterinin kredi riski, ödeme davranışı, işlem geçmişi, gelir istikrarı, harcama örüntüsü, sigorta riski ve yatırım tercihlerine göre daha dinamik fiyatlama yapabilecektir. Bu durum iyi risk profiline sahip müşteriler için daha uygun finansman maliyeti, daha ucuz sigorta primi veya daha kişisel yatırım hizmetine imkan sağlayacaktır. Bunlar da müşteri deneyiminin zenginleşmesine katkı sağlayacaktır.

Finansın görünmez ve otonom hale dönüşmesi: Ödeme, kredi, sigorta, yatırım gibi finansal hizmetlerin dijital platformlara gömülmesi, müşterinin finansal işlem yapmak için ayrıca banka veya finansal kuruluşun uygulamasına girmesini gerektirmeyen görünmez finans deneyimini güçlendirmektedir. Bu şekilde finansal hizmetler, müşterinin ayrıca talep ettiği ürünler olmaktan çıkarak ihtiyaç anında, doğru kanalda ve en uygun koşulla sunulan bir hizmete dönüşecektir. Açık bankacılık ve dijital finansal hizmetler bankaların müşteriyle doğrudan temas eden görünür yüzünü azaltırken, arka planda güven, veri, ödeme ve işlem altyapısı sağlayan bir role yönelmelerine neden olmaktadır (Stefanelli, Manta ve Toma, 2022). Bunun yanı sıra otonom finans uygulamaları daha da gelişecektir. Müşterilerin finansal kararlarını manuel olarak kendisinin vermesinden ziyade, yapay zeka destekli sistemlerin müşterinin risk tercihleri ve hedefleri doğrultusunda öneriler sunması ve bazı finansal işlemlerin otomatik olarak

gerçekleştirilmesi ile daha fazla karşılaşılacaktır. Günümüzde karşılaşılan robo-danışmanlık bu dönüşümün erken örneklerinden biridir. Alsabah ve diğerleri, robo-danışmanların yatırımcının risk tercihlerini zaman içinde portföy seçimlerinden öğrenebileceğini ve yatırım kararlarını algoritmik biçimde destekleyebileceğini göstermektedir (Alsabah, Capponi, Lacedelli ve Stern, 2019). Benzer şekilde bütçe yönetimi, borç yönetimi, vergi optimizasyonu, emeklilik planlaması, sigorta ihtiyacı, nakit akışı tahmini, ESG tercihleri gibi çok geniş bir alanda kişisel finans yönetiminin giderek otonom hale dönüşmesi mümkün olacaktır.

Finansal kapsayıcılığın genişlemesi ve finansın demokratikleşmesi: Dijital finans teknolojileri, mobil ve dijital cüzdanlar, mikro kredi, düşük maliyetli yatırım platformları, kitle fonlaması ve robo-danışmanlık gibi araçlar, daha önce finansal sisteme sınırlı erişimi olan bireylerin ve küçük işletmelerin finansal hizmetlere ulaşmasını kolaylaştırmaktadır. Bu da finansal hizmetlerden daha geniş kesimlerin faydalanmasına ve bir açıdan finansal kapsayıcılığın genişlemesine ve finansın demokratikleşmesine etkide bulunmaktadır. Anlık ve gerçek zamanlı finansal işlemler geleceğin finansının bir başka belirleyici özelliği olacaktır. Ödeme sistemleri, para transferleri, menkul kıymet takası, kredi kararı, dolandırıcılık izleme ve risk yönetimi giderek gerçek zamanlı altyapılara taşınmaktadır. Müşteri açısından bu durum, bekleme sürelerinin azalması ve finansal hizmetin daha akışkan hale gelmesine katkıda bulunmaktadır. Sosyal medya artık yalnızca iletişim ve pazarlama aracı değil, aynı zamanda ödeme, bağış, abonelik, mikro gelir, topluluk finansmanı ve sosyal ticaret altyapısına dönüşmektedir. Gelişen teknolojiler varlık sahipliği yerine varlık kullanımının ön plana çıkmasına neden olmaktadır. Bu şekilde paylaşım ekonomisi ve abonelik içeren sistemler ön plana çıkmaktadır (Yurtsever, 2021). Paylaşım ekonomisi platformları, kullanıcıların araç, konut, zaman, beceri veya dijital içerik gibi varlıklarını gelir getirici faaliyetlere dönüştürmesini sağlamaktadır. Bu platformların içinde ödeme, sigorta, teminat, puanlama, mikro kredi ve gelir avansı gibi finansal hizmetlerin sunulması, finansın günlük dijital yaşam akışı ile iç içe geçmesine yol açacaktır.

Sürdürülebilir ve yeşil finansın belirleyici rolü: Sürdürülebilir ve yeşil finans, finansın geleceğini şekillendiren en önemli yapısal dönüşümlerden birisi olarak önemini daha da artıracak görünmektedir. İklim değişikliği, karbon emisyonları, enerji dönüşümü ve sürdürülebilir kalkınma hedefleri, sermaye tahsis kararlarının yalnızca getiri ve risk üzerinden değil, çevresel ve sosyal etki üzerinden de değerlendirilmesini gerektirmektedir. ESG göstergeleri, yatırım kararları, kredi tahsisi, sermaye maliyeti, risk primi ve kurumsal değerleme süreçlerinde giderek daha fazla kullanılacaktır. Gelecekte bankalar, kredi verirken müşterinin karbon yoğunluğunu; yatırımcılar portföy oluştururken şirketin iklim riskini; sigorta şirketleri ise doğal afet ve geçiş risklerini daha fazla dikkate almak durumunda kalacaktır. Kurumsal sosyal sorumluluk yaklaşımlarının önemi daha da artacaktır. Green FinTech uygulamaları ise karbon ayak izi takibi, etki verisinin güvenli bir şekilde toplanması, ESG veri analitiği, yeşil yatırım danışmanlığı, karbon piyasalarına erişim, sürdürülebilirlik raporlaması gibi alanlarda sürdürülebilir finansın dijital altyapısını güçlendirecektir.

Artan riskler ve finansal suçlarla mücadele ile finans mevzuatına uyumun teknolojik dönüşümü: Finanstaki dijitalleşme ve dönüşüm olumlu nitelikteki değişimlerin yanı sıra bu alandaki risklerin de hızla artmasına, niteliğinin değişmesine ve yeni risklerin ortaya çıkmasına neden olmaktadır. Veri mahremiyeti, siber güvenlik, algoritmik şeffaflık ve açıklanabilirlik gibi konular finansal kuruluşlar açısından stratejik risk alanlarına dönüşmektedir. Düzenleyici kuruluşlar bu hızlı gelişime ayak uydurmakta zorlanabilmekte ve bu nedenle yasal açıdan belirsizlikler ve gri alanlar oluşabilmektedir (Liang, 2023). Yapay zeka destekli finansal suçlar, deepfake, sentetik kimlik, siber saldırılar, sosyal mühendislik, hesap ele geçirme, sahte müşteri edinimi, otomatik bot işlemleri, kripto varlık dolandırıcılıkları gibi suçlar atmakta ve karmaşık hale gelmektedir. Yapay zeka ve teknolojiyi yalnızca kişi ve kurumlar değil suç örgütleri de yaygın olarak kullanmaktadır. Suç örgütleri yapay zeka ve diğer teknolojik imkanları kullanarak finansal suçları kolayca işleyebilmekte ve gizleyebilmektedir. Bu nedenle hızlı ve etkili anomali tespiti, gerçek zamanlı uyarı ve önleme sistemleri bir

ihtiyaç olarak ortaya çıkmaktadır. Finansal ürün ve hizmetlerin kişiselleştirmesi ile mahremiyetin ve güvenliğin korunması arasındaki denge geleceğin finansında ana gündem alanlarından birisi olarak önemini koruyacaktır. Yine artan ve sıkılaşan finansal düzenlemelere teknolojiden destek almadan uyum sağlanması giderek zorlaşmaktadır. Bütün bunlar da uyum maliyetlerinin artmasına neden olmaktadır. Bu nedenlerle regülasyon teknolojileri (RegTech) giderek gelişmekte ve kullanımı artmaktadır. Bu sürecin hızlanarak devam etmesi olası görünmektedir. Finansal suçlarla mücadele ve mevzuat uyum süreçleri, giderek manuel, kural bazlı ve parçalı kontrollerden uzaklaşarak yapay zeka, veri analitiği ve RegTech çözümleriyle desteklenen entegre, otomatik ve sürekli izleme esaslı bir yapıya evrilecektir. Bütün bu gelişmeler düzenleyici kurumların gözetim ve denetim mekanizmalarını da doğrudan etkilemekte, gözetim yükü büyümekte, yeni riskler ortaya çıkmakta ve bu alanda da teknolojinin ve yapay zekanın kullanımı bir zorunluluk olarak genişlemektedir. Bu çerçevede teknolojik çözümler finansın geleceğini de etkileyen ve belirleyen stratejik bir alan olarak önemini artıracaktır.

III. SONUÇ

Dijitalleşme ve teknolojik dönüşüm tüm sektörleri olduğu gibi finansı da derinden etkilemektedir. Dijital teknolojiler finansı tek bir çizgide değil, eşzamanlı birçok eksende ve çok katmanlı olarak dönüştürmektedir. Birçok teknolojik gelişme finansı doğrudan ve dolaylı olarak etkilemekte, değişmesi ve dönüşmesine etkide bulunmaktadır. Bu çalışmada ele alınan FinTech ve InsurTech, TechFin, blokzincir ve merkeziyetsiz finans, açık bankacılık ve açık finans, servis modeli bankacılığı/finansı, gömülü/görünmez finans, kripto varlıklar, tokenizasyon, büyük veri, bulut bilişim, veri analitiği, yapay zeka, makine öğrenmesi, robotik teknolojiler, nesnelerin interneti, giyilebilir teknolojiler, sanal gerçeklik, merkez bankası dijital paraları, regülasyon teknolojileri, süper uygulamalar, sosyal medya finansı, kitle fonlaması ve kuantum finans gibi teknolojiler, iş modelleri ve uygulama yaklaşımlarının yer aldığı görülmektedir. Bunlar ve bunların birlikte oluşturduğu yeni mimari finansın geleneksel yapısını hızla değiştirmektedir.

Basel Bankacılık Gözetim Komitesi (Basel Komite) dijitalleşmenin açık finans, blockchain, bulut, yapay zeka ve tokenizasyon gibi farklı teknolojileri tek bir dönüşüm dalgası içinde birleştirerek finansal mimariyi yeniden şekillendirdiğini ortaya koymaktadır. Dijitalleşme; finansın üretimi, sunumu ve yönetiminin tüm aşamalarını ve değer zincirini değiştirmektedir (BCBS Report, 2024). Bu değişim, finansal ürünlerin kimden alındığının yanı sıra bu ürünlerin tasarlanması, üretilmesi, satın alınması ve teslim edilme biçimlerini de etkilemektedir (Arslanian ve Fischer, 2019). Bunların etkisiyle finansta dijitalleşme hızlanmakta, finansal kuruluşların fiziksel hizmet mekanları azalırken dijital kanalların kullanımı hızla artmakta, her geçen gün yeni dijital ürün ve hizmetler geliştirilmekte, dijital bankalar ve finans kuruluşları faaliyete geçmekte, servis ve platform bazlı yaklaşımlar ön plana çıkmakta, kapalı kurum stratejileri açık ekosistemlere dönüşmekte, standart ürünlerin yerine kişiselleştirilmiş, modüler, gerçek zamanlı ve ihtiyaç/kullanım bazlı ürün ve hizmetler almaktadır. Kurum merkezli platformlar yerlerini insan merkezli platformlara bırakmaktadır (Yurtsever, 2019, Temmuz). Finans giderek görünmez, gömülü ve otonom hale gelmektedir.

Finansta dinamik risk yönetimi, veri yönetişimi, siber dayanıklılık ve mevzuat uyum önem kazanmaktadır.

Her geçen gün karşımıza çıkan yeni teknolojiler ve yaklaşımlarla bu dönüşüm daha da hızlanmaktadır. Bir anlamda finans sistemi yeni paradigmalar ile yeniden tanımlanmakta, sınırları genişlemekte, finansın geleceği teknoloji, dijitalleşme, veri ve yapay zeka odağında şekillenmektedir. Gelecekte bu değişimin daha da hızlanacağı ve genişleyeceği açıktır. Bütün bunlar sayesinde finansal işlemler daha hızlı, kolay ve daha ucuza yapılabilmektedir. Finansal aracılara olan ihtiyaç azalmakta ve karşılıklı doğrudan finansal hizmetler yapılabilmesi mümkün hale gelmektedir. Finansal hizmetlere erişim kolaylaşmakta, kapsayıcı hale gelmekte ve demokratikleşmektedir. Kullanıcıların seçenekleri çoğalmakta ve kullanıcı deneyimi zenginleşmekte, şeffaflık artmaktadır. Müşteri ve müşteri verisi merkeze oturmakta, müşterilerin özellikleri, ihtiyaçları ve beklentileri ile uyumlu kişiselleştirilmiş ve

özelleştirilmiş ürün ve hizmetler artmaktadır. Bu şekilde finansal hizmetler günlük yaşama daha derinlemesine etkide bulunmakta ve finansın toplumsal faydası artmaktadır.

Bütün bu gelişmeler finansın geleceğine ilişkin önemli ipuçları barındırmaktadır. Bu dönüşüm sürecinde finansın rolü ve önemi daha da artmaktadır. Finans, değişen dünya dinamiklerine kendisi de değişerek uyum sağlamakta ve hızla dönüşen dünya ekonomisinin can damarı olma özelliğini pekiştirmektedir. Bu sayede finansın geleneksel işlevleri yeni işlevler ile zenginleşmekte, finansın değer zinciri ve katma değer fonksiyonu gelişmektedir. Finanstaki bu değişim dünyadaki ekonomik faaliyetlerin de çeşitlenmesine ve genişlemesine etki etmekte ve bir açıdan katalizör rolü görmektedir. Bunun da etkisiyle girişimcilik genişlemekte, ulusal ve uluslararası ticaretteki büyüme ve entegrasyon hızlanmaktadır (Yurtsever, 2021).

Geleceğin finansı, günümüzün kurumsal, teknolojik ve operasyonel sınırlarının çok ötesine geçerek daha dijital, veri odaklı, platform temelli, görünmez, sürdürülebilir ve müşteri merkezli bir yapıya evrilecektir. Bu şekilde finans, gelecekte de dünya ekonomisinin temel taşı olmayı sürdürecek; ancak bu rolünü daha güçlü biçimde yerine getirebilmesi, teknolojik yeniliklerin güven, sürdürülebilirlik, etik, şeffaflık ve toplumsal fayda ilkeleriyle birlikte yönetilmesine bağlı olacaktır. Bu çerçevede finansal kuruluşların, düzenleyici otoritelerin, teknoloji şirketlerinin ve finans profesyonellerinin değişimi yalnızca izleyen değil, öngören, yöneten ve şekillendiren bir yaklaşım benimsemeleri gerekmektedir. Finansın geleceğine hazırlanmak için yeni teknolojilere uyum sağlamanın yanı sıra kurumsal stratejileri, iş modellerini, insan kaynağını, risk yönetimini ve yönetişim anlayışını bu yeni gerçekliğe göre yeniden tasarlamak önem taşımaktadır.

KAYNAKÇA

Alsabah, Humoud ve Capponi, Agostino ve Ruiz Lacedelli, Octavio ve Stern, Matt. (2019). Robo-advising: Learning Investors' Risk Preferences via Portfolio Choices. Journal of Financial Econometrics, https://ssrn.com/abstract=3228685.

Arner, Douglas W. ve Barberis, Janos ve Buckley, Ross. P. (2017). FinTech, RegTech, and the Reconceptualization of Financial Regulation. Northwestern Journal of International Law & Business, 37(3), 371-413.

Arrieta, Alejandro Barredo ve Diaz-Rodriguez, Natalia ve Del Ser, Javier ve Bennetot, Adrien ve Tabik, Siham ve Barbado, Alberto ve Garcia, Salvador ve Gil-Lopez, Sergio ve Molina, Daniel ve Benjamins, Richard ve Chatila, Raja ve Herrera, Francisco. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. Information Fusion, 58, 82-115.

Arslanian, Henri; Fischer, Fabrice. (2019). The Future of Finance (The Impact of Fintech, AI, and Crypto on Financial Services), Hong Kong. Palgrave Macmillan.

Auer, Raphael ve Böhme, Rainer. (2020). The Technology of Retail Central Bank Digital Currency. BIS Quarterly Review, March, 85-100.

https://www.bis.org/publ/qtrpdf/r_qt2003j.htm.

Babina, Tania ve Bahaj, Saleem ve Buchak, Greg ve De Marco, Filippo ve Foulis, Angus ve Gornall, Will ve Mazzola, Francesco ve Yu, Tong. (2025). Customer Data Access and Fintech Entry: Early Evidence from Open Banking. Journal of Financial Economics. Volume 169.

Barnes, Richard. (2020). Factors in the Portability of Tokenized Assets on Distributed Ledgers. https://doi.org/10.48550/arXiv.2005.07461.

Basel Committee on Banking Supervision (BCBS). (2024). Digitalisation of Finance. BCBS Report.

Böhme, Rainer ve Christin, Nicolas ve Edelman, Benjamin ve Moore, Tyler. (2015) Bitcoin: Economics, Technology, and Governance. Journal of Economic Perspectives, 29, 213-238.

Broeders, Dirk ve Prenio, Jeremy. (2018). Innovative technology in financial supervision (SupTech): The experience of early users. FSI Insights on Policy Implementation No. 9. Bank for International Settlements (BIS).

Catalini, Christian ve Gans, Joshua S. (2019). Some Simple Economics of the Blockchain. Rotman School of Management Working Paper No. 2874598, MIT Sloan Research Paper No.

5191-16

Chen, Hsinchun ve Chiang, Roger H. L., ve Storey, Veda. C. (2012). Business Intelligence and Analytics: From Big Data to Big impact. MIS Quarterly, 36(4), 1165-1188.

Eric, Dejan. (2022). Innovation and Fintech. İçinde: Vukovic, Darko B. ve Maiti, Moinak ve Grigorieva, Elena M. (Ed.). Digitalization and the Future of Financial Services. Springer.

Gomber, Peter ve Koch, Jascha-Alexander ve Siering, Michael. (2017). Digital Finance and Fintech: Current Research and Future Research Directions. Journal of Business Economics, 87, 537-580.

Gubbi, Jayavardhana ve Buyya, Rajkumar ve Marusic, Slaven ve Palaniswami, Marimuthu. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Future Generation Computer Systems, 29(7), 1645-1660.

Liang, Shihan. (2023). The Future of Finance: Fintech and Digital Transformation. Highlights in Business, Economics and Management. Volume 15.

Mystakidis, Stylianos. (2022). Metaverse. Encyclopedia, 2(1), 486-497.

https://doi.org/10.3390/encyclopedia2010031.

OECD. (2024). Tokenisation of Assets and Distributed Ledger Technologies in Financial Markets. OECD Report.

Orûs, Roman ve Mugel, Samuel ve Lizaso, Enrique. (2018). Quantum computing for finance: Overview and prospects. Reviews in Physics. https://doi.org/10.1016/j.revip.2019.100028.

Puschmann, Thomas ve Hoffmann, Christian H. ve Khmarskyi, Valentyn. (2020). How Green FinTech Can Alleviate the Impact of Climate Change-The Case of Switzerland. Sustainability, 12(24), 1-30.

Schar, Fabian. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. Federal Reserve Bank of St. Louis Review, 103(2), 153-174.

Stefanelli, Valeria ve Manta, Francesco ve Toma, Pierluigi. (2022). Digital Financial Services and Open Banking Innovation: Are Banks Becoming 'Invisible'?. Global Business Review. https://doi.org/10.48550/arXiv.2210.01109.

Yazıcı, Selim. Ed. (2021). FinTech ve InsurTech İle Finansın Dönüşümü: Dijital Ekonomide Geleceği Şekillendiren Beş Temel Yapıtaşı.

Yurtsever, Gürdoğan. (2021). Finansal Teknolojilerle Bankacılık ve Sigortacılıkta Değer Zincirinin Yeniden Tanımlanması, Ed. Selim Yazıcı. FinTech ve InsurTech İle Finansın Dönüşümü: Dijital Ekonomide Geleceği Şekillendiren Beş Temel Yapıtaşı.

Yurtsever, Gürdoğan. (2013, Şubat). Sosyal bankacılık gelişiyor. Turcomoney Dergisi. http://www.turcomoney.com.

Yurtsever, Gürdoğan. (2014, Ocak). Sanal para bitcoin gerçek paranın yerini mi alıyor? Turcomoney Dergisi. http://www.turcomoney.com.

Yurtsever, Gürdoğan. (2015, Şubat). Bulut teknolojisi nasıl kullanılmalı? Turcomoney Dergisi. http://www.turcomoney.com.

Yurtsever, Gürdoğan. (2016, Haziran). Akıllı nesneler geleceği şekillendirecek. Turcomoney Dergisi. http://www.turcomoney.com.

Yurtsever, Gürdoğan. (2016, Temmuz). Yapay zeka insan zekası ile yarışıyor. Turcomoney Dergisi. http://www.turcomoney.com.

Yurtsever, Gürdoğan. (2017, Ekim). Finans teknolojileri nereye gidiyor? Turcomoney Dergisi. http://www.turcomoney.com.

Yurtsever, Gürdoğan. (2018, Mart). Blockchain devrimi neler getiriyor? Turcomoney Dergisi. http://www.turcomoney.com.

Yurtsever, Gürdoğan. (2019, Ocak). Yaygınlaşan Finansman Yöntemi: Kitle Fonlaması. Turcomoney Dergisi. http://www.turcomoney.com.

Yurtsever, Gürdoğan. (2019, Şubat). Kuantum bilgisayarlar geleceğimizi şekillendirecek. Turcomoney Dergisi. http://www.turcomoney.com.

Yurtsever, Gürdoğan. (2019, Temmuz). Açık bankacılık ile finansal hizmetlerdeki teknolojik gelişim hızlanıyor. Turcomoney Dergisi. http://www.turcomoney.com.

Yurtsever, Gürdoğan. (2020 Ağustos). Uzaktan müşteri edinimi ile finansal hizmetlere erişim kolaylaşıyor. Turcomoney Dergisi. https://www.turcomoney.com.

Yurtsever, Gürdoğan. (2020 Temmuz). Regülasyon Teknolojilerinin (RegTech) Önemi Artıyor. Turcomoney Dergisi. https://www.turcomoney.com.

Yurtsever, Gürdoğan. (2024, Şubat). Süper uygulamalar yaygınlaşıyor ve yaşamı kolaylaştırıyor. Turcomoney Dergisi. http://www.turcomoney.com.

Yurtsever, Gürdoğan. (2025, Eylül). Dijital TL ne getirecek? Turcomoney Dergisi. http://www.turcomoney.com.

Yurtsever, Gürdoğan. (2026, Ocak). Uzayın sınır tanımayan ekonomisi ne getirecek? Turcomoney Dergisi. http://www.turcomoney.com.

Zetzsche, Dirk Andreas ve Buckley, Ross P. ve Arner, Douglas W. ve Barberis, Janos Nathan. (2017). From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance. New York University Journal of Law and Business, Forthcoming, University of Hong Kong Faculty of Law Research Paper No. 2017/007.

Zachariadis, Markos ve Özcan, Pınar. (2017). The API Economy and Digital Transformation in Financial Services: The Case of Open Banking. SWIFT Institute Working Paper No. 2016001.

SİBER GÜVENLİK İHLALLERİ SEBEBİYLE KİŞİSEL VERİLERİN KORUNMASINDA DEVLETİN POZİTİF YÜKÜMLÜLÜĞÜ

The State's Positive Obligation to Protect Personal Data in the Face of Cyber Security Breaches

Doç. Dr. Recai AKYEL
Anayasa Mahkemesi Üyesi

Dr. Habip OĞUZ
Anayasa Mahkemesi Raportörü

ÖZET

Bilgi toplumunda kişiliğin maddi ve manevi unsurları giderek artan ölçüde veri sorumlularının elindeki kayıt sistemlerinde yoğunlaşmış, siber güvenlik ihlâlleri ise bu birikimi tek bir saldırıyla kitlesel ölçekte savunmasız bırakabilen yapısal bir tehdit hâline gelmiştir. Devletin yalnızca müdahaleden kaçınmasını öngören klasik negatif yükümlülük anlayışı, tehdidin ağırlıkla üçüncü kişilerden kaynaklandığı bu alanda hakkı boş bir güvenceye dönüştürmektedir. Bu çalışma, kişisel verilerin korunmasında devletin pozitif yükümlülüğünü; ihlali önleyecek pratik ve etkili tedbirleri alma *(koruma/önleme)*, ihlâl hâlinde etkili soruşturma ve etkili başvuruyu sağlama *(usul)* ve fiilen işleyen bir hukuki çerçeve kurma *(düzenleme)* şeklindeki üç katmanlı bir yapıyı çözümler. Bu incelemede; öğreti, normatif değerlendirme, AİHM ve Anayasa Mahkemesi kararları çerçevesinde anılan yükümlülükler ele alınır.

Çalışmanın ulaştığı temel sonuç, bu üç katmanın hem Avrupa İnsan Hakları Mahkemesi hem Anayasa Mahkemesi içtihadında somut karşılık bulduğu; söz konusu yapının esasen, hakkın özel hukuk ilişkilerine devletin pozitif yükümlülükleri aracılığıyla ulaştığı dolaylı yatay etkinin somutlaşmış hâli olduğudur. Koruma/önleme yükümlülüğü, her ihlâli engellemeyi garanti eden bir sonuç yükümlülüğü değil, riskle ve verinin hassasiyetiyle ağırlaşan bir özen yükümlülüğüdür. Türk hukukunda üzerinde durulması gereken husus, mevzuatın yokluğu değil etkinliğidir. İspat asimetrisi, etkili soruşturmadaki eksiklikler, düzenlemenin fiilî işleyişindeki boşluklar ve manevi zararın kapsamına ilişkin belirsizlik, biçimsel altyapının güçlü olduğu bir sistemde dahi korumayı zayıflatır.

Anahtar kelimeler: kişisel verilerin korunması, devletin pozitif yükümlülüğü, siber güvenlik, özel hayata saygı, yatay etki

ABSTRACT

In the information society, the material and immaterial aspects of the individual are increasingly concentrated in the record-keeping systems controlled by data controllers, while cybersecurity breaches have become a structural threat capable of leaving this accumulated data vulnerable on a massive scale with a single attack. The classical understanding of negative obligations, which merely requires the state to refrain from intervention, renders this right a hollow guarantee in this field where the threat primarily originates from third parties. This study examines the state's positive obligation in the protection of personal data through a three-tiered framework: taking practical and effective measures to prevent violations *(protection/prevention)*, ensuring effective investigation and recourse in the event of a violation *(procedure)*, and establishing a functioning legal framework *(regulation)*. In this analysis, the aforementioned obligations are examined within the framework of doctrine, normative evaluation, and decisions of the European Court of Human Rights *(ECHR)* and the Constitutional Court.

The study's primary conclusion is that these three layers find concrete expression in the case law of both the European Court of Human Rights and the Constitutional Court; essentially, this structure represents the concrete manifestation of the indirect horizontal effect through which the right is realized in private law relationships via the state's positive obligations. The duty to protect/prevent is not a result-oriented obligation guaranteeing the prevention of every violation, but rather a duty of care that intensifies with the level of risk and the sensitivity of the data. The key point to emphasize in Turkish law is not the absence of legislation but its effectiveness. The burden of proof asymmetry, deficiencies in effective investigations, gaps in the practical operation of the regulation, and uncertainty regarding the scope of non-pecuniary harm weaken protection even within a system with a strong formal framework.

Keywords: protection of personal data, positive obligations of the state, cybersecurity, right to respect for private life, horizontal effect

GİRİŞ

Bilgi toplumunun olgunlaşmasıyla birlikte kişiliğin maddi ve manevi unsurları giderek artan ölçüde dijital ortama taşınmış, bireyin sağlık durumundan siyasi tercihlerine, iletişim içeriğinden konum bilgisine kadar uzanan geniş bir kişilik alanı, veri sorumlularının elinde tutulan kayıt sistemlerinde yoğunlaşmıştır. Bu yoğunlaşma, kişisel verinin yalnızca bireysel mahremiyetin değil, aynı zamanda toplumsal güvenin de taşıyıcısı hâline gelmesine yol açmıştır. Siber güvenlik ihlalleri ise bu birikimi tek bir saldırıyla kitlesel ölçekte savunmasız bırakabilen, sonuçları geri alınamayan ve çoğu zaman failin dahi tespit edilemeyen yapısal bir tehdit olarak ortaya çıkar. Veri güvenliği, teknik düzlemde verinin gizliliği, bütünlüğü ve erişilebilirliği ekseninde tanımlanırken[1], hukuki düzlemde bu üç boyutun korunması doğrudan özel hayata saygı hakkının fiilî güvencesiyle örtüşür[2].

Klasik temel hak anlayışı, devleti hak ve özgürlüklere müdahale etmekten kaçınmakla yükümlü kılan negatif bir konumda tasavvur edilir. Ne var ki kişisel verilerin korunmasında devletin yalnızca kendi organları eliyle gerçekleşecek müdahalelerden kaçınması, hakkın etkili biçimde kullanılmasını sağlamaya yetmez. Verinin esas tehdidi çoğu kez devletten değil, siber saldırganlar, ihmalkâr veri sorumluları, yetkisiz erişim sağlayan özel kişiler gibi üçüncü kişilerden kaynaklanır. Bu durum, devletin edilgen tutumunu aşan, hakkın gerçekleşmesi için etkin edimde bulunmayı gerektiren pozitif yükümlülükleri gündeme getirir[3].

Negatif yükümlülük, en genel anlamıyla devletin insan haklarına keyfî biçimde müdahale etmeme ödevini ifade eder. Pozitif yükümlülük ise hakların pratikte ve etkin biçimde kullanılması için gerekli tedbirlerin alınmasını gerektirir[4]. Öğretide isabetle

1 **Wang**, Anyu: Data Security and Privacy Protection: A Comprehensive Guide, Eo.1, Singapore 2025, p.14.

2 **Gündüz**, Mehmet Şükrü: Uluslararası İnsan Hakları Açısından Kişisel Veri Güvenliği, B.1, Ankara 2022, s.66-67.

3 **Yüzer Eltimur**, Dilara: AİHS Kapsamında Özel Hayatın ve Aile Hayatının Korunmasında Devletin Pozitif Yükümlülükleri, B.1, İstanbul 2019, s.106.

4 **Hazar**, Zeynep: *"Yatay Etki Kavramının Avrupa İnsan Hakları Sözleşmesi Sistemi Bağlamında Değerlendirilmesi"*, AYD, C.41, S.1, y.2024, s.393.

vurgulandığı üzere, devlet bir hakkı korumak için *"evvela ihlali önlemeli, önleyemediyse soruşturmalı, gerektiğinde yargılamalı ve yargılama neticesinde ortaya çıkan tazminat ve telafiyi içeren korumayı sağlamalı"*dır[5]. Bu kademeli yapı, kişisel verilerin korunmasında devletin pozitif yükümlülüğünün de iskeletini oluşturur.

Devletin pozitif yükümlülüğü; ihlâli baştan engelleyecek pratik ve etkili tedbirleri alma *(koruma/önleme yükümlülüğü)*, ihlâl gerçekleştiğinde etkili soruşturma yürütme ve etkili bir hukuki yollara erişim sağlama *(usuli yükümlülük)* ve güvenceleri kâğıt üzerinde bırakmayıp fiilen işleyen bir hukuki çerçeve kurma *(düzenleyici yükümlülük)* şeklinde üç katmanlı bir yapı içinde okunabilir. Bu üçlü ayrım, insan hakları öğretisinde devletin yükümlülüklerini saygı gösterme, koruma ve yerine getirme biçiminde tasnif eden üçlü tipolojiyle de örtüşür[6].

I. KAVRAMSAL VE KURAMSAL ÇERÇEVE

A. Kişisel Veri ve Kişisel Verilerin Korunması Hakkı

1. Kişisel Veri Kavramı ve Özel Nitelikli Veri Ayrımı

Kişisel verilerin korunmasına ilişkin her çözümleme, korunan menfaatin sınırlarını belirleyen kişisel veri kavramının tanımıyla başlamak zorundadır. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun *(KVKK)* 3'üncü maddesine göre kişisel veri, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi ifade eder. Tanımın genişliği, korumanın kapsamını, verinin türüne göre değil, bir gerçek kişiyle ilişkilendirilebilir olması ölçütüne göre belirleyen bilinçli bir tercihtir[7]. Bu geniş çerçeve içinde kanun koyucu, niteliği gereği ifşası bireyi daha ağır biçimde

5 **Bayra**, Adem Ersin: *"İnsan Haklarının Yatay Etkisi: Temel Haklarının Korunma Düzeyi Bakımından Devletin Konumunu Yeniden Düşünmek"*, AYD, C.41, S.1, y.2024, s.186; **Doğru**, Osman: *"Devletin Sorumluluğu: İnsan Hakları Avrupa Sözleşmesi'nde Pozitif Yükümlülükler"*, Danıştay ve İdari Yargı Günü: 139. Yıl, Ed. Danıştay Başkanlığı, B.1, Ankara 2008, s.208-209; **Yüzer Eltimur**, s. 181; **Hoşgül**, Batuhan: Etkin Soruşturma Yükümlülüğü, B.1, Ankara 2019, s.21.

6 **Hazar**, s. 392.

7 Elbette tanımın geniş olması sınırsız olduğu anlamına gelmez. Sınırlamalar için bkz. Elbette tanımın geniş olması sınırsız olduğu anlamına gelmez. Sınırlamalar için bkz. **Çekin**, Mesut Serdar: Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, B.3, İstanbul 2020, s.44-45.

mağdur edebilecek bir veri grubunu ayrıca güvenceye almıştır. KVKK'nın 6'ncı maddesi kapsamında özel nitelikli *(hassas)* kişisel veriler olarak nitelenen sağlık, cinsel hayat, ırk, etnik köken, siyasi düşünce, din ve mezhep, biyometrik ve genetik veriler ile ceza mahkûmiyetine ilişkin veriler, işlenme rejimi bakımından daha sıkı koşullara bağlanmıştır[8].

Bu ayrımın siber güvenlik bağlamındaki önemi yapısaldır. Sağlık verisi gibi özel nitelikli verilerin yetkisiz erişime açılması, yalnızca soyut bir mahremiyet ihlâli değil, bireyin sosyal kimliğini ve hayatını doğrudan tehdit eden somut bir zarardır. Nitekim AİHM de tıbbi verinin gizliliğinin korunmasını, AİHS'in *(Sözleşme)* güvence altına aldığı özel hayata saygı hakkının çekirdeğinde konumlandırmıştır[9]. Özel nitelikli veriye ilişkin bu yüksek korunma beklentisi, devletin güvenlik tedbirleri bakımından üzerine düşen özen ölçütünü de yükseltir.

2. Kişisel Verilerin Korunmasını İsteme Hakkının Özerk Niteliği

Kişisel verilerin korunmasını isteme hakkı, tarihsel olarak özel hayatın gizliliği hakkından türemiş olmakla birlikte, bugün kendine özgü güvenceleri olan özerk bir temel hak olarak kabul edilir[10]. Anayasa Mahkemesi, bu hakkı yalnızca verinin gizli tutulmasıyla sınırlamayan, bireye verisi üzerinde aktif denetim yetkileri tanıyan bir çerçeve içinde yorumlamaktadır. Mahkemeye göre bu hak, özel hayata saygı hakkı kapsamında değerlendirilmekle birlikte, kişinin verisi hakkında bilgilenmesinden bu verilere erişmesine ve düzeltilmesini istemesine kadar uzanan bağımsız bir yetkiler demetini içerir[11]. Hakkın bu özerk niteliği, korunmasının da pasif bir gizlilik beklentisinin ötesine geçerek devletin aktif edimlerini gerektirmesinin kavramsal temelini oluşturur.

---

8 **Yılmaz**, Sabire Sanem: Tıp Alanında Kişisel Verilerin Korunması, B.6, Ankara 2022, s.14.

9 AİHM, *Z /Finlandiya,* B. No: 22009/93, 25/02/1997, § 95.

10 **Doğan**, Bayram: Karşılaştırmalı Hukukta Anayasal Bir Hak Olarak Kişisel Verilerin Korunması Hakkı, B.1, Ankara 2022, s.45. Uluslararası belgelerde ise müstakil düzenlemelerden ziyade özel hayatın korunması hakkı kapsamında değerlendirildiği görülür. Bkz. **Oğuz**, Habip: Kişiliğin Korunması Bağlamında Unutulma Hakkı, B.1, Ankara 2025, s.131.

11 AYM, *Aylin Nazlıaka (2)*, B. No: 2018/24439, 15/6/2021, § 23.

3. Mahremiyet, Veri Güvenliği ve Hakkın Fiilî Korunması Arasındaki İlişki

Kişisel verilerin korunması hukukunun teknik ve hukuki katmanları, veri güvenliği kavramında kesişir. Teknik olarak veri güvenliği, çoğunlukla gizlilik, bütünlük ve erişilebilirlik üçlüsü *(CIA Triad)* ekseninde tanımlanır. Bu üç unsur, verinin yetkisiz erişime, değiştirilmeye ve kullanılamaz hâle getirilmeye karşı korunmasını ifade eder[12]. Veri güvenliğinin etkili biçimde sağlanması, korumanın verinin tek bir anına değil, toplanmasından imhasına kadar uzanan tüm yaşam döngüsüne yayılmasını gerektirir[13]. Bu teknik çerçevenin hukuki anlamı şudur: Kişisel verilerin korunmasını isteme hakkı, ancak verinin fiilen güvende tutulmasıyla içeriğine kavuşur. Güvenlik tedbirlerinin yetersizliği nedeniyle gerçekleşen bir yetkisiz erişim, doğrudan özel hayata saygı hakkının ihlâline dönüşebilir. Bu husus veri güvenliğini salt teknik bir uyum meselesi olmaktan çıkarıp anayasal bir yükümlülük hâline getirir.

B. Hakkın Pozitif Hukuktaki Temelleri

Hakkın doğrudan anayasal dayanağı, 2010 değişikliğiyle Anayasa'nın 20'nci maddesine eklenen fıkradır[14]. Bu hüküm herkese kendisiyle ilgili kişisel verilerin korunmasını isteme hakkını tanır. Bu hak, bilgilendirilme, erişim, düzeltme ve silme yetkilerini de kapsar. Maddeye göre kişisel veriler ancak kanunda öngörülen hâllerde veya açık rızayla işlenebilir. Maddenin kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceğine ilişkin son cümlesi devletin düzenleyici yükümlülüğünün anayasal kaynağını oluşturur.

Kişisel verilerin korunması, bireyin manevi varlığını koruma ve geliştirme hakkıyla doğrudan bağlantılıdır. Verinin yetkisiz ifşası, çoğu zaman bireyin onurunu, sosyal itibarını ve manevi bütünlüğünü zedeler. Bu nedenle Anayasa'nın 17'nci maddesi

12 **Wang**, p. 14.

13 **Wang**, p. 13.

14 **Tahmazoğlu Üzeltürk**, Sultan: *"Kişisel Verilerin Korunması Hakkında Anayasa Değişikliği"*, LHD, y.2010, S.93, s.3151.

hakkın manevi boyutunu besleyen tamamlayıcı bir güvence işlevi görür[15].

Devletin pozitif yükümlülüğünün en genel anayasal dayanağını ise 5'inci madde oluşturur. Bu hüküm, devleti kişinin temel hak ve hürriyetlerini sınırlayan engelleri kaldırmaya ve insanın maddî ve manevî varlığının gelişmesi için gerekli şartları hazırlamaya görevli kılar. Devlete edilgenliği değil, etkin bir koruma faaliyetini emreden bu düzenleme, kişisel verilerin korunmasında üç katmanlı pozitif yükümlülüğün anayasal omurgasını oluşturur.

Kişisel verilerin korunmasını isteme hakkına yapılacak her müdahale, Anayasa'nın 13'üncü maddesindeki güvence sistemine tabidir. Buna göre müdahale ancak kanunla, hakkın özüne dokunmadan, meşru bir amaca dayalı ve ölçülü olabilir. Bu hüküm, devletin yükümlülüklerinin yalnızca koruma yönünü değil, koruma adına getirilen tedbirlerin de sınırını belirler.

Avrupa İnsan Hakları Sözleşmesi'nin özel hayata ve aile hayatına saygı hakkını düzenleyen 8'inci maddesi, kişisel verilerin korunmasına ilişkin pozitif yükümlülük içtihadının asıl gelişim alanıdır. Mahkemenin pozitif yükümlülükleri ve dolayısıyla Sözleşme'nin yatay etkisini en geniş biçimde işlediği alanın 8'inci madde olması, bu maddenin koruduğu menfaatlerin kapsamının olağanüstü genişliğinden kaynaklanır[16]. Sözleşmenin 8'inci maddesi, bireyi yalnızca kamu makamlarının keyfî müdahalelerine karşı korumakla kalmaz, özel hayata etkili biçimde saygı gösterilmesinin doğasında yer alan, üçüncü kişilerin müdahalelerine karşı koruyucu tedbirleri de içeren pozitif yükümlülükleri devlete yükler.

Anayasal ve sözleşmesel güvencelerin yasal düzlemdeki karşılığı Kişisel Verilerin Korunması Kanunudur. Kanunun 12'nci maddesi hükmü, veri sorumlusuna, kişisel verilere hukuka aykırı erişimi önlemek ve verilerin muhafazasını sağlamak için uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri

15 **Eren**, Fikret: Borçlar Hukuku Genel Hükümler, B.25, Ankara 2020, s.884.

16 **Doğru**, Derya: *"İnsan Haklarının Yatay Etkisi ve Avrupa İnsan Hakları Hukukundaki İz Düşümü: Pozitif Yükümlülük Doktrini"*, AYD, C.41, S.1, y.2024, s.260 *(**Doğru**, D.)*.

alma yükümlülüğü getirir. Aynı maddenin beşinci fıkrası, işlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde veri sorumlusunu, durumu en kısa sürede Kişisel Verileri Koruma Kurulu'na ve ilgili kişiye bildirmekle yükümlü tutar. KVKK'nın Avrupa Birliği veri koruma müktesebatından esinlenerek hazırlanmış olması, yapılacak karşılaştırmalı çözümlemenin de meşru zeminini oluşturur.

C. Negatif Yükümlülük - Pozitif Yükümlülük Ayrımı

1. Müdahaleden Kaçınma Yükümlülüğün Sınırları

İnsan haklarının korunmasında devletin yükümlülüklerini belirleyen temel ayrımlardan biri, AİHM'in de benimsediği negatif ve pozitif yükümlülük ayrımıdır[17]. Negatif yükümlülük, devletin haklara hukuka aykırı biçimde müdahale etmeme ödevini ifade eder ve geleneksel olarak medeni ve siyasi haklarla ilişkilendirilir[18]. Ne var ki kişisel verilerin korunmasında negatif yükümlülük tek başına yetersiz kalır. Zira devletin kendi eliyle gerçekleştirmediği, üçüncü kişilerden kaynaklanan ihlâller karşısında salt müdahaleden kaçınma, hakkı boş bir güvenceye dönüştürür[19]. Bu yetersizlik, pozitif yükümlülük doktrininin doğuşunun temel saikidir.

2. Pozitif Yükümlülük Kavramının Doğuşu ve Gelişimi

Avrupa İnsan Hakları Sözleşmesi'nin 8'inci maddesi kapsamında devletin pozitif yükümlülüğüne işaret eden ilk kararlardan biri *Airey/İrlanda* kararıdır[20]. Eşinden şiddet gören başvurucunun fiili ayrılık kararı alabilmesi için gereken adli yardım sisteminin bulunmaması nedeniyle açılan davada AİHM, Sözleşme'nin günümüz koşulları ışığında yorumlanması ve bireyleri gerçek ve etkili biçimde koruması gerektiğini vurgulamış, 8'inci maddenin negatif yükümlülüğün yanında, özel ve aile hayatına etkili biçimde saygı gösterilmesinin doğasında yer alan pozitif yükümlülükleri

17 **Hazar**, s. 392.

18 **Hazar**, s. 393.

19 **Doğru**, s. 193-194; **Yüzer Eltimur**, s. 118-119.

20 AİHM, *Airey/İrlanda*, B. No: 6289/73, 09/10/1979, § 32.

de içerdiğini saptayarak ihlal kararı vermiştir[21]. Bu karar, *"gerçek ve etkili koruma"* ölçütünü Sözleşme yorumunun merkezine yerleştirmesi bakımından kurucu niteliktedir.

Mahkemenin 8'inci madde kapsamında devletin üçüncü kişilere karşı koruma yükümlülüğünü, başka bir deyişle yatay etkiyi açıkça uyguladığı ilk karar ise *X. ve Y./Hollanda* kararıdır[22]. Zihinsel engelli bir gencin uğradığı cinsel saldırının, ulusal ceza usul hukukundaki bir boşluk nedeniyle etkili biçimde kovuşturulamaması üzerine Mahkeme, pozitif yükümlülüklerin kişiler arası ilişkileri de kapsayacak şekilde özel hayata saygıyı güvence altına almak için tedbir alınmasını gerektirdiğini belirtmiş, cezai soruşturmanın usuli engellere takılarak somut ve etkili bir koruma sağlayamaması nedeniyle ihlâl kararı vermiştir[23]. Bu içtihat, ihlâl özel hukuk kişisi tarafından gerçekleştirilmiş olsa dahi, ulusal hukuk sisteminin yeterli koruma güvencelerini sağlayamaması hâlinde devletin sorumluluğunun doğacağını ortaya koyar[24].

D. Devletin Pozitif Yükümlülüğünün Üç Katmanlı Yapısı

Yatay etkiye ilişkin pozitif yükümlülük doktrini, temel olarak devletin bireyleri diğer bireylerin müdahalelerine karşı koruma yükümlülüğüne odaklanır. Ancak devlet, bireyleri üçüncü kişilerin ihlâllerinden korumakla kalmayıp, korunan hakların etkili biçimde kullanılabilmesi için gerekli yasal, mali, yargısal ve idari önlemleri de almak zorundadır[25]. Bu çok yönlü içerik, kişisel verilerin korunmasında devletin pozitif yükümlülüğünün üç katman hâlinde çözümlenmesini mümkün kılar.

Birinci katman, devletin üçüncü kişilerin haksız müdahalelerini ve veri ihlâllerini daha en baştan önleyecek pratik ve etkili tedbirleri alma ödevini ifade eder. Esasa ilişkin bu yükümlülük, ihlâl gerçekleşmeden önce devreye giren önleyici bir koruma mantığına dayanır.

21 **Doğru**, D., s. 260-261.

22 AİHM, *X. ve Y./Hollanda*, B. No. 8978/80, 26/03/1985, § 23.

23 **Doğru**, D., s. 261.

24 **Doğru**, D., s. 262.

25 **Bayra**, s. 187.

İkinci katman, ihlâl gerçekleştiğinde etkili bir soruşturma yürütme ve etkili bir hukuki yola erişim sağlama ödevini kapsar. Devletin koruma görevi, ihlâli önleyemediği durumda soruşturma, gerektiğinde yargılama ve nihayetinde tazmin ve telafiyi içeren bir süreçle tamamlanır[26].

Üçüncü katman ise, güvenceleri kâğıt üzerinde bırakmayıp, aykırılıkları yaptırıma bağlayan ve fiilen işleyen bir hukuki çerçeve kurma ödevidir. Anayasa'nın 20'nci maddesinin son cümlesindeki *"kanunla düzenlenir"* hükmü, bu yükümlülüğün anayasal kaynağıdır. KVKK ve Kişisel Verileri Koruma Kurulu'nun denetim ve yaptırım yetkisi ise bu maddeden dayanağını alır.

II. SİBER GÜVENLİK İHLALİNİN HAK İHLALİNE DÖNÜŞÜMÜ

A. Siber Güvenlik İhlali Kavramı ve Başlıca Türleri

Siber güvenlik ihlali, en yalın tanımıyla, verinin teknik güvenlik niteliklerinden birinin yetkisiz biçimde zedelenmesidir. Veri güvenliğinin gizlilik, bütünlük ve erişilebilirlik üçlüsü ekseninde tanımlandığı dikkate alındığında[27], ihlal türleri de bu üç boyuta göre tasnif edilebilir. Gizliliğin ihlali, yalnızca erişim yetkisi olanların ulaşması gereken bilginin yetkisiz kişilerce ele geçirilmesini ifade eder. Verinin yetkisiz erişimle elde edilmesi hâlinde ihlal, kapsamı ve niteliğine göre sınıflandırılır[28]. Bütünlüğün ihlali, verinin yaşam döngüsü boyunca izinsiz biçimde değiştirilmesi ya da tahrip edilmesidir. Yetkisiz erişimle gerçekleşen her değişiklik aynı zamanda bir bütünlük ihlali oluşturur[29]. Erişilebilirliğin ihlali ise verinin meşru kullanıcılar bakımından kullanılamaz hâle getirilmesini kapsar. Dolayısıyla her siber güvenlik olayı aynı tür ve ağırlıkta bir hak tehdidi doğurmaz. Gizlilik ihlali doğrudan mahremiyeti hedeflerken, bütünlük ve erişilebilirlik ihlalleri farklı menfaatleri zedeleyebilir.

İhlallerin doğuş biçimleri de çeşitlidir. Fidye yazılımı, saldırı karmaşıklığının her yıl arttığı, sürekli gelişen bir tehdit hâline

26 **Bayra**, s. 1867.

27 **Wang**, p. 14.

28 **Wang**, p. 17.

29 **Wang**, p. 18.

gelmiştir. Özellikle hassas verileri önce sızdırıp ardından fidye ödenmezse çevrimiçi yayımlamakla tehdit eden çifte gasp *(double extortion)* kampanyaları, sağlık, eğitim ve yerel yönetim sektörlerini öncelikli hedef hâline getirmektedir[30]. Bunun yanında yetkili kullanıcıların erişim ve ayrıcalıkları gözetildiğinde içeriden gelen tehditler büyük önem taşır. Nitekim 2020 yılındaki ihlallerin dörtte birinden fazlasının içeridekilerden kaynaklanması, kötü niyetli veya ihmalkâr çalışanların oluşturduğu riskin boyutunu göstermek açısından önemlidir[31]. Bu tablo, devlet bakımından özel bir vurguyu gerektirir. Zira çok sayıda vatandaş verisini merkezî veri tabanlarında toplayan idareler, saldırganlar için âdeta bir *"bal küpü"* oluşturur ve birbirine bağlı eski sistemler, çevre savunmaları aşıldığında saldırganların yanal hareketine olanak tanır[32].

B. İhlalin Hak İhlaline Dönüşüm Eşiği

1. İhlalin Hangi Anda Doğacağı Meselesi

Siber güvenlik ihlalinin teknik bir olay olmaktan çıkıp anayasal bir hak ihlaline dönüştüğü anın belirlenmesi, çözümlemenin kilit sorunudur. Burada teknik olay ile hukuki ihlali ayırt etmek gerekir. Bir güvenlik açığının istismar edilmesi teknik bir vakadır, bu vakanın kişisel verilerin korunmasını isteme hakkını ihlal edip etmediği ise ayrı bir hukuki değerlendirmeyi gerekli kılar. Klasik yaklaşım, failin fiilen kötüye kullandığı anda ihlalin gerçekleştiğinin kabulü yönündedir. Oysa Avrupa Birliği Adalet Divanı, bu eşiği belirgin biçimde öne çekmiştir. Bulgaristan Ulusal Gelir İdaresi'nin bilişim sistemlerine yönelik ve altı milyondan fazla kişiyi etkileyen siber saldırıya ilişkin kararında Divan, ele geçirilen kişisel verilerin gelecekte kötüye kullanılacağına dair duyulan korkunun tek başına bir manevi zarar oluşturabileceğini kabul etmiştir[33]. Bu yaklaşımın mantıksal sonucuna göre, verinin gerçekten kötüye kullanılmasını beklemeye gerek yoktur. Yetkisiz

30 **Rustambekov**, İslambek/**Gulyamov**, Said/**Bozgeyik**, Hayri/**Sharipova**, Hilola: Dijital Devlet Yönetişiminin Teorik ve Hukuki Temelleri, B.1, Ankara 2024, s.44.

31 **Rustambekov/Gulyamov/Bozgeyik/Sharipova**, s. 45.

32 **Rustambekov/Gulyamov/Bozgeyik/Sharipova**, s. 44-45.

33 ABAD, *Natsionalna agentsia za prihodite*, C-340/21, 14/12/2023.

erişimin gerçek ve ciddi bir kötüye kullanım riskine neden olması, hakkın ihlal alanına girilmesi için yeterli olabilir. Nitekim verinin yetkisiz erişimle elde edilmesi hâlinde ihlalin kapsam ve niteliğine göre derhal sınıflandırılması ve buna uygun giderim tedbirlerinin uygulanması, teknik literatürde de korumanın bir parçası sayılır[34].

2. Dönüşüm Ölçütleri

İhlalin hak ihlaline dönüşümünde ilk ölçüt, tehdidin öngörülebilir olup olmadığıdır. Devletin yatay düzlemdeki bir ihlalden sorumlu tutulabilmesinin kriterlerinden biri, devletin ya da yetkili makamların söz konusu tehdidi biliyor veya bilmesi gerekiyor olmasıdır[35]. Siber güvenlik bağlamında bu ölçüt, bilinen ve giderilmemiş güvenlik açıklarının istismarıyla gerçekleşen bir ihlalin, öngörülebilir bir riskin gerçekleşmesi olduğu yönünde özel bir anlam kazanır. Nitekim eski sistemlerin yeterince güçlendirilmemesi ve tespit edilen yazılım açıklarının derhal giderilmemesi, saldırganlar için geniş bir saldırı yüzeyi sunmaya devam eder[36]. Öngörülebilir bir açığa karşı tedbir alınmaması, ihlalin devlete ya da veri sorumlusuna yüklenebilirliğini güçlendirir.

İkinci ölçüt, ihlalin ağırlığı ve etkilediği verinin niteliğidir. Özel nitelikli verilerin, özellikle sağlık verisinin ifşası, niteliği gereği daha ağır bir hak ihlali oluşturur. Tıbbi verinin gizliliği, AİHM tarafından özel hayata saygının çekirdeğinde konumlandırılmıştır[37]. Türk hukukunda da bu veriler KVKK'nın 6'ncı maddesi kapsamında ayrıca güvenceye başlanmıştır. Ağırlık değerlendirmesinde ihlalin ölçeği de belirleyicidir. Gerçekten de altı milyonu aşan kişiyi etkileyen ve verileri internette yayımlanan bir saldırı ile sınırlı sayıda kaydı etkileyen bir olay, aynı hukuki ağırlıkta değerlendirilemez. Kötüye kullanım riskinin somutluğu, etkilenen veri kategorisi ile ölçeğin birlikte değerlendirilmesiyle belirlenir.

34 **Wang**, p. 17.

35 **Hazar**, s. 391.

36 **Rustambekov/Gulyamov/Bozgeyik/Sharipova**, s. 44-45.

37 AİHM, *Z./Finlandiya*, § 95.

Üçüncü ölçüt, güvenlik açığı ile zarar arasındaki nedensellik bağı ve ihlalin devlete isnat edilebilirliğidir. Yatay düzlemde gerçekleşen bir ihlalden devletin sorumlu tutulabilmesi için, devletten beklenebilecek bir negatif veya pozitif edimi ya da ona atfedilebilir bir yükümlülüğü yerine getirmede noksanlık bulunması gerekir[38]. Bu ölçüt, devletin her siber ihlalden otomatik olarak sorumlu olmadığını ortaya koyar. Sorumluluk, ancak bir pozitif yükümlülüğün yerine getirilmemesiyle ihlal arasında nedensel bir bağ kurulabildiğinde doğar. İsnat edilebilirlik ölçütü, böylece devletin sorumluluğunu sınırsız bir sonuç sorumluluğuna dönüştürmeyen, ölçülü bir çerçeve sunar.

C. Veri Güvenliği ile Özel Hayata Saygı Arasındaki İlişki

Yukarıdaki ölçütler, veri güvenliği ile özel hayata saygı hakkı arasındaki bağı görünür kılar. Bu bağ, en açık biçimde AİHM'in kişisel veri güvenliğine ilişkin temel kararında kurulmuştur. Kamu hastanesinde çalışan ve aynı zamanda orada tedavi gören, HIV pozitif teşhisi konmuş bir kişinin hasta kayıtlarının yetkisiz erişime karşı yeterince korunmadığı olayda Mahkeme, hakkın ihlalinin yalnızca devletin doğrudan müdahalesiyle değil, yetkisiz erişimi en baştan önleyecek pratik ve etkili koruma tedbirlerinin alınmamasıyla da gerçekleşebileceğini saptamıştır[39]. Buna göre ihlal sonrasında dava açma imkânının varlığı, mahremiyeti en baştan korumakla aynı şey değildir. Gereken şey, yetkisiz erişimin gerçekleşme ihtimalini en baştan dışlayacak somut korumadır. Bu tespit, veri güvenliği tedbirlerinin yetersizliğini salt bir teknik uyumsuzluk olmaktan çıkarıp doğrudan Sözleşmenin 8'inci ve Anayasa 20'nci maddesi kapsamındaki hakkın ihlaline dönüştürür. Böylece veri güvenliği, devletin koruma yükümlülüğünün teknik karşılığı, koruma yükümlülüğü ise veri güvenliğinin hukuki karşılığı hâline gelir.

38 **Hazar**, s. 391.

39 AİHM, *I./Finlandiya*, B. No. 20511/03, 17/07/2008, § 49.

III. KORUMA ve ÖNLEMEYE İLİŞKİN POZİTİF YÜKÜMLÜLÜK

A. Pratik ve Etkili Koruma Standardı

Devletin pozitif yükümlülüğünün ilk katmanı, ihlali daha en baştan önlemeye yönelen esasa ilişkin bir koruma ödevidir. AİHM içtihadında hakların yatay etkisi, esas olarak *"gerçek ve etkili bir koruma"* düşüncesinin bir sonucu olarak ortaya çıkar. Bir ihlal ister devlet eyleminden ister bir bireyin davranışından kaynaklansın, devlet etkili bir güvence sistemi kurmakla yükümlüdür[40]. Mahkeme, pozitif yükümlülüğün hangi alt yükümlülüklerden oluştuğuna dair kapalı bir sınıflandırma yapmamış, böylece gerçek ve etkili koruma fikrinin gerektirdiği esnekliği korumayı tercih etmiştir[41]. Bununla birlikte öğretide bu yükümlülükler tasnif edilmiştir. Buna göre, gerekli normatif düzenlemeleri yapmak ve güvenceleri getirmek, uygulamaya dönük işlevsel tedbirler almak ve denetim görevlerini yerine getirmek, ihlal hâlinde başvurulabilecek hak arama yollarını oluşturmak ile etkin soruşturma yürütmek ve etkili yaptırımlar uygulamak, bu sınıflandırmaların ortak unsurlarıdır[42].

B. Avrupa İnsan Hakları Mahkemesinin Yaklaşımı

Koruma/önleme yükümlülüğünün kişisel veriler bağlamındaki karşılığı *I./Finlandiya* kararıdır. Başvurucu, bir kamu hastanesinin göz kliniğinde sözleşmeli hemşire olarak çalışmakta iken aynı zamanda HIV pozitif teşhisiyle aynı hastanenin bir başka kliniğinde tedavi görmektedir. İş yerindeki bazı imalardan hareketle meslektaşlarının hastalığından haberdar olduğunu fark eden başvurucu, hasta kayıtlarına yetkisiz biçimde erişildiğinden şüphelenir. Olayın belirleyici teknik özelliği, hastanenin kayıt sisteminin kime erişildiğini geriye dönük olarak tespit etmeye imkân vermemesi, dahası mevcut erişim denetimlerinin göz kliniğindeki meslektaşların kayda ulaşmasını engelleyememesidir[43]. Hastane devlet denetimi altında bulunduğundan, olaydan doğan sorumluluk Finlandiya'ya isnat edilmiş, Mahkeme uyuşmazlığı

40 **Hazar**, s. 388.

41 **Hazar**, s. 404.

42 **Hazar**, s. 404.

43 AİHM, *I./Finlandiya*, § 45.

Sözleşmenin 8'inci maddesi kapsamındaki pozitif yükümlülük çerçevesinde ele almıştır.

Mahkeme, iç hukukun başvurucuya, verisinin hukuka aykırı biçimde ifşa edildiği iddiasıyla tazminat talep etme imkânı tanımış olmasının, özel hayatını korumak bakımından tek başına yeterli olmadığını saptamıştır. Burada gereken şey, yetkisiz erişimin gerçekleşme ihtimalini en baştan dışlayacak pratik ve etkili bir korumanın sağlanmasıdır. Mahkemeye göre iç hukuk, sağlık verilerinin 8'inci maddenin güvenceleriyle bağdaşmayan biçimde ifşasını engelleyecek uygun güvenceleri sağlamak zorundadır[44]. Bu gerekçeyle Mahkeme, devletin yetkisiz erişime karşı koruma yükümlülüğünü yerine getirmediği sonucuna vararak 8'inci maddenin ihlal edildiğine hükmetmiştir. Kararın hukuki ağırlığı, korumanın odağını ihlal sonrası giderimden ihlal öncesi önlemeye kaydırmasında yatar. Tazminat davası açma imkânı bir telafi yoludur ancak pozitif yükümlülüğün esasa ilişkin katmanı, zararın hiç doğmamasını sağlayacak önleyici tedbirler almaktır.

I./Finlandiya kararının sağlık verisine ilişkin yüksek koruma beklentisi, daha önce verilen Z./Finlandiya kararına dayanır. Bu kararda Mahkeme, bir kişinin HIV durumuna ilişkin bilginin ifşasının onun özel ve aile hayatını, sosyal ve mesleki durumunu çarpıcı biçimde etkileyebileceğini, bireyi dışlanma ve damgalanma riskine açabileceğini, hatta kişileri teşhis ve tedaviden caydırarak salgınla mücadele çabalarını dahi zayıflatabileceğini vurgulamıştır[45]. Sağlık verisinin bu istisnai hassasiyeti, devletin önleyici koruma yükümlülüğünün ölçütünü yükselten bir etken olarak değerlendirilmelidir. Zira ifşa hâlinde doğacak zarar ne kadar ağırsa, beklenen güvenlik tedbirinin düzeyi de o ölçüde yükselir.

C. Pozitif Yükümlülüğün Türk Hukukundaki Yansıması

Anayasa Mahkemesi de kişisel verilerin korunmasını isteme hakkı bakımından devlete önleyici nitelikte pozitif yükümlülükler yüklendiğini kabul eder. Mahkemeye göre bu hak, devletin

44 AİHM, *I./Finlandiya*, §38.

45 AİHM, *Z./Finlandiya*, §96.

yalnızca kişilerin özel hayatına keyfî biçimde müdahale etmekten kaçınmasını değil, yetki alanındaki bireyleri gerek kamusal makamların gerek diğer bireylerin eylemlerinden kaynaklanabilecek risklere karşı koruyacak tedbirleri almasını da gerektirir[46]. Bu yaklaşım, AİHM'in I./Finlandiya kararındaki önleme mantığını Türk anayasa hukukuna taşır ve devletin koruma görevini, üçüncü kişilerden kaynaklanan ihlalleri kapsayacak biçimde genişletir.

Önleme yükümlülüğünün yasal düzlemdeki somut karşılığı KVKK'nın 12'nci maddesidir. Hüküm, veri sorumlusunu, kişisel verilere hukuka aykırı erişimi önlemek ve verilerin muhafazasını sağlamak için uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almakla yükümlü kılar[47]. Bu tedbirlerin teknik içeriği, veri güvenliği yönünden somutlaşır. Gerçekten de gizliliğin sağlanmasında veri şifreleme ve çok faktörlü kimlik doğrulama yaygın yöntemlerdir. Aşırı hassas veriler bakımından fiziksel yalıtım gibi ek önlemler de gerekebilir[48]. İdari ve örgütsel boyutta ise en az ayrıcalıklı erişimin zorunlu kılınması, anormallikleri tespit etmek için davranışsal analizlerin uygulanması, günlük kayıtlarının ve yetkilerin düzenli denetlenmesi ve ağ güvenliğinde *"sıfır güven"* yaklaşımının benimsenmesi öne çıkar[49]. *I./Finlandiya* kararındaki erişim kaydının tutulmaması ve erişim denetimlerinin yetersizliği şeklindeki eksikliğin tam da bu idari ve teknik tedbirlerdeki boşluğa karşılık geldiği görülür.

D. "Due Diligence" mi, Sonuç Yükümlülüğü mü?

Koruma/önleme yükümlülüğünün hukuki niteliği, eleştirel bir değerlendirmeyi gerektirir. Devlet, hiçbir ihlalin gerçekleşmemesini garanti eden bir sonuç yükümlülüğü altında mıdır, yoksa makul tedbirleri almakla sınırlı bir özen *(davranış)* yükümlülüğü yeterli görülür mü? AİHM'in içtihadı, ikinci yorumu destekler niteliktedir. Mahkeme, önleyici operasyonel yükümlülüğün ihlal

46 AYM, *Aylin Nazlıaka (2)*, § 40.

47 **Çekin**, s. 186-187.

48 **Wang**, p. 17.

49 **Rustambekov/Gulyamov/Bozgeyik/Sharipova**, s. 45.

edilip edilmediğini değerlendirirken üç temel unsur üzerinde durmaktadır. Bu kapsamda öncelikle gerçek ve yakın bir tehdidin bulunup bulunmadığı incelenmekte, ardından resmî makamların bu tehditten haberdar olup olmadığı veya koşullar gereği haberdar olmalarının beklenip beklenemeyeceği değerlendirilmektedir. Son olarak resmî makamların söz konusu tehdidi bertaraf etmek veya etkilerini önlemek amacıyla durumun gerektirdiği makul tedbirleri alıp almadığı araştırılmaktadır[50]. Bu çerçevede ulusal makamlardan beklenen, bildikleri ya da bilmeleri gereken gerçek ve yakın tehlikeyi bertaraf etmek için kendilerinden makul olarak beklenebilecek her şeyi yapmalarıdır[51]. Bu standart, yaşam hakkı ve maddi-manevi bütünlük bağlamında geliştirilmiş olmakla birlikte, kişisel verilerin korunmasına da uyarlanabilir niteliktedir.

Bu uyarlama ışığında *I./Finlandiya* kararı, esasen makul önleyici tedbir ölçütünün veri güvenliğine uygulanmasıdır. Meslektaşların kayda erişme ihtimali öngörülebilir bir risk iken, hastanenin erişim denetimi ve kayıt mekanizması kurmaması, kendisinden makul olarak beklenebilecek tedbirleri almadığını gösterir. Buradan çıkan sonuç, koruma/önleme yükümlülüğünün bir sonuç değil, bir özen yükümlülüğü olduğudur. Devlet her siber ihlalin mutlak güvencesi değildir. Ancak riskle orantılı ve makul tedbirleri almakla yükümlüdür. Bu yorumun pratik sonucu, özen ölçütünün sabit değil değişken olduğudur. Eklenen tedbir düzeyi, verinin hassasiyetiyle ve tehdidin öngörülebilirliğiyle birlikte yükselir. Bu nedenle, çok sayıda vatandaş verisini merkezi sistemlerde toplayan ve bu yönüyle saldırganlar için yüksek değerli bir hedef oluşturan idareler bakımından makul özen eşiği de daha yüksektir.

IV. ETKİLİ SORUŞTURMA ve ETKİLİ BAŞVURU YÜKÜMLÜLÜĞÜ

Devletin pozitif yükümlülüğünün ikinci katmanı, ihlal gerçekleştikten sonra devreye giren usuli yükümlülüktür. Pozitif yükümlülükler, devletten beklenen edimin niteliğine göre maddi ve usuli olmak üzere ikiye ayrılmaktadır. Maddi yükümlülükler, bireylerin haklardan etkin biçimde yararlanabilmesi için gerekli

50 **Hazar**, s. 410.

51 **Hazar**, s. 410.

hukuki düzenlemeleri ve tedbirleri içerirken, usuli yükümlülükler, oluşturulan yasal ve idari çerçevenin doğru uygulanmasını, bir ihlal gerçekleştiğinde ihlalin sonlandırılıp sorumluların cezalandırılmasını sağlayacak yeterli adli ve idari tepkilerin verilmesini gerektirir[52]. Bu adli ve idari tepkilerin tipik ve en önemli görünüm biçimi etkin soruşturma yükümlülüğüdür[53]. Maddi ve usuli boyut arasında kesin bir ayrım çizmek çoğu zaman güç olsa da bu ayrımın belirsizliği korumanın etkililiği bakımından ikincil önemdedir. Zira AİHM'in asıl ilgilendiği, yükümlülüğün etiketi değil, hakkın fiilen korunup korunmadığıdır[54].

A. Etkili Soruşturma Ödevi

Usuli yükümlülüğün dijital ortamda ihlal edilmesine ilişkin karar, *K.U./Finlandiya* kararıdır. Olayda, on iki yaşındaki bir çocuk adına, onun bilgisi dışında bir buluşma sitesine, yaşını ve fiziksel özelliklerini bildiren ve onu kendisiyle yakınlık kuracak kişiler için hedef hâline getiren bir ilan yerleştirilmiştir. Çocuğun babası faili belirlemek üzere kolluğa başvurmuş, ancak internet servis sağlayıcısı, telekomünikasyonun gizliliğini gerekçe göstererek ilanı veren kişinin kimliğini açıklamayı reddetmiş, o tarihte yürürlükteki iç hukuk da bu suç bakımından abonelik verisinin elde edilmesine izin vermediği için fail tespit edilememiştir[55]. Mahkeme, bir suçun soyut olarak var olmasının, asıl faili belirleyip adalet önüne çıkaracak bir araç bulunmadığında sınırlı bir caydırıcılığa sahip olduğunu belirtmiştir[56]. Mahkemeye göre 8'inci madde kapsamındaki pozitif yükümlülük, devlet görevlilerinin cezai sorumluluğunun söz konusu olmadığı hâllerde dahi, bir ceza soruşturmasının etkililiğine ilişkin sorunları kapsayacak biçimde genişleyebilir[57]. Bu çerçevede başvurucunun pratik ve etkili biçimde korunması, faili belirleyip kovuşturacak etkili adımların atılmasını gerektirir. Somut olayda bu koruma sağlanamadığından 8'inci madde ihlal edilmiştir.

52 **Hazar**, s. 395.

53 **Hazar**, s. 396.

54 **Hazar**, s. 396.

55 AİHM, *K.U./Finlandiya*, B. No. 2872/02, 02/12/2008, § 26.

56 AİHM, *K.U./Finlandiya*, § 46.

57 AİHM, *Osman/Birleşik Krallık, 28/10/1998*, § 128.

Bununla birlikte kararın, usuli yükümlülüğün sınırlarına ilişkin de önemli bir kaydı vardır. Mahkeme, pozitif yükümlülüğün makamlara ya da yasa koyucuya imkânsız veya orantısız bir yük yükleyecek biçimde yorumlanamayacağını[58], suçu önleme ve soruşturma yetkilerinin, failin de dayanabileceği 8'inci ve 10'uncu madde güvenceleri dâhil olmak üzere usule ilişkin güvencelere tam saygı gösterilerek kullanılması gerektiğini vurgulamıştır[59]. Mahkeme, 8'inci madde ihlali tespit edildiğinden, etkili başvuru hakkına ilişkin 13'üncü madde iddiasını ayrıca incelemeyi gerekli görmemiştir.

K.U./Finlandiya kararının Türk hukukundaki benzeri, Anayasa Mahkemesi'nin *Cem Özberk* başvurusuna ilişkin kararıdır. Başvurucu, yıllar önce kendisini tedavi etmiş olan psikiyatri uzmanı hekimin, tedavi sürecine ilişkin sağlık verilerini içeren raporu, açık rızası olmaksızın annesine vermesi üzerine Cumhuriyet başsavcılığına suç duyurusunda bulunmuş, neticeten açılan davanın sonunda hekim hakkında beraat kararı verilmiştir[60]. Mahkeme başvuruyu, Anayasa'nın 20'nci maddesi kapsamında kişisel verilerin korunmasını isteme hakkı çerçevesinde değerlendirmiş ve bu hakkın korunmasının devletin pozitif yükümlülükleri kapsamında ele alınması gerektiğini, bu yükümlülüğün yalnızca kamu makamlarına karşı değil, özel kişilerin eylemlerine karşı da geçerli olduğunu özellikle vurgulamıştır. Başvurucunun sağlık verilerinin KVKK'nın 6'ncı maddesi anlamında özel nitelikli kişisel veri olduğu ve bu verilerin aktarılmasının açık rızaya bağlı bulunduğu tespit edilmiştir. Mahkemeye göre olayın aydınlatılmasına yönelik esaslı iddiaların araştırılmaması, soruşturmanın derinleştirilmemesi ve yasal dayanağı gösterilmeyen gerekçelerle sonuca ulaşılması nedeniyle etkili ve özenli bir soruşturma yürütüldüğü söylenemez. Verilen kararlar, kişisel verileri ve hasta haklarını koruyacak şekilde Anayasa'nın 20'nci maddesinin son fıkrasındaki gerekliliklere uygun, ilgili ve yeterli gerekçeler içermemektedir. Bu gerekçelerle Mahkeme hakkın ihlal edildiğine hükmetmiş ve yeniden

58 AİHM, *K.U./Finlandiya*, § 48.

59 AİHM, *K.U./Finlandiya*, § 49.

60 AYM, *Cem Özberk*, B. No. 2020/15944, 20/03/2025, § 9.

soruşturma yapılması için kararı ilgili başsavcılığa göndermiştir. Karar, etkili soruşturma ve kovuşturma yapma ödevinin Türk hukukunda da kişisel verilerin korunmasının ayrılmaz bir bileşeni olduğunu ortaya koyması bakımından dikkate değerdir.

B. Etkili Başvuru Hakkı

Usuli yükümlülüğün ikinci ayağı, etkili başvuru hakkıdır. AİHS'in 13'üncü maddesi Sözleşmede tanınan hak ve özgürlükleri ihlal edilen herkese, ihlal resmî bir hizmetin ifası için davranan kişilerce gerçekleştirilmiş olsa dahi, ulusal bir merci önünde etkili bir yola başvurma hakkı tanır[61]. Öğretide, maddedeki *"resmî bir hizmetin ifası için davranan kişiler tarafından gerçekleştirilmiş olsa dahi"* ifadesinin, tersi yorumla ihlalin bir özel hukuk kişisi tarafından da işlenebileceğini gösterdiği belirtilir. Özel hukuk kişilerinin Sözleşmedeki haklara saygı göstermesini sağlayacak etkili bir başvuru yolunun bulunmaması da 13'üncü maddenin ihlaline yol açabilir[62]. Nitekim AİHM, sınırlı bir denetim yetkisinin bulunduğu özel bir okulda şiddet gördüğünü ileri süren başvurucunun iddialarını dile getirebileceği bir başvuru yolunun bulunmamasını 13'üncü maddenin ihlali olarak değerlendirmiştir[63]. Türk hukukunda bu güvencenin karşılığı, temel hak ve hürriyetlerin korunmasını düzenleyen ve etkili başvuru hakkını içeren Anayasa'nın 40'ıncı maddesidir. Bununla birlikte *K.U./Finlandiya* ve benzeri kararlarda görüldüğü üzere, Mahkeme esasa ilişkin hakkın usuli boyutunun ihlal edildiğini saptadığında 13'üncü maddeyi çoğu kez ayrıca incelemez. Bu durum, etkili başvuru güvencesinin hem özerk bir hak hem esasa ilişkin hakkın usuli bir bileşeni olarak iki yönlü işlediğini gösterir.

C. Mahkemeye Erişim ve Adil Yargılanma

Usuli korumanın yargısal düzlemdeki tamamlayıcısı, adil yargılanma hakkı kapsamındaki mahkemeye erişim hakkı ve hak arama hürriyetidir. Bu güvenceler, esasa ilişkin ve usuli

61 **Tanrıkulu**, M. Sezgin: İnsan Hakları Avrupa Sözleşmesi ve Etkili Başvuru Hakkı, B.1, Ankara 2012, s.130.

62 **Doğru**, D., s. 247.

63 **Doğru**, D., s. 384-385.

korumanın yargı önünde fiilen ileri sürülebilmesini sağlar. Ne var ki mahkemeye erişimin biçimsel olarak tanınmış olması, korumanın etkili olduğu anlamına gelmez. *I./Finlandiya* kararında başvurucu, ilgili sağlık idaresi aleyhine hukuk davası açabilmiş, ancak kayıtlara kimin eriştiğini gösteren bir mekanizma bulunmadığından, verisine hukuka aykırı biçimde erişildiğine dair kesin delil ortaya konulamamış ve derece mahkemeleri talebi reddetmiştir. Bu olgu, mahkemeye erişim hakkının tek başına yetersiz kalabildiğini gösterir. Zira dava açma imkânı, ihlalin maddi gerçeğini ortaya koyacak etkili bir soruşturma ve kayıt altyapısı ile desteklenmediğinde içeriksiz bir güvenceye dönüşür. Bu nedenle mahkemeye erişim, etkili soruşturma ödevinden bağımsız değil, onunla birlikte işleyen bir güvence olarak değerlendirilmelidir.

D. Usuli Yükümlülüğün İspat Yükü Üzerindeki Etkisi

Usuli yükümlülüğün kişisel veriler bağlamındaki asıl önemi, salt usule ilişkin bir gereklilik olmasının ötesinde, esasa ilişkin hakkı fiilen var eden yapısal işlevinde yatar. Veri ihlallerinde mağdur, çoğu zaman verisine kimin, nasıl eriştiğini ya da ihlalin hangi mekanizmayla gerçekleştiğini ispatlayacak konumda değildir. Zira veriye ve erişim kayıtlarına ilişkin teknik unsurlar, mağdurun değil veri sorumlusunun ya da saldırganın elindedir. Bu yapısal ispat asimetrisi, *I./Finlandiya* kararında somutlaşır. Zira erişim kaydı tutulmadığı için başvurucu hukuka aykırı erişimi ispatlayamamış ve esasa ilişkin talebi delil yokluğundan başarısız olmuştur. Dolayısıyla etkili bir soruşturma ve onu mümkün kılan kayıt altyapısı bulunmadığında, esasa ilişkin hak uygulanamaz hâle gelir. Etkili soruşturma ödevi tam da bu asimetriyi giderir. Çünkü ihlalin maddi gerçeğini ortaya koyma külfetini, çaresiz durumdaki mağdurdan devletin soruşturma aygıtına kaydırır.

Karşılaştırmalı hukukta bu asimetriye verilen yanıt daha da ileri gider. Avrupa Birliği veri koruma rejiminde ispat yükü, ihlale katıldığı karine olarak kabul edilen veri sorumlusu üzerindedir[64]. Sorumlu ancak uygun tedbirleri aldığını ispatlayarak sorumluluktan kurtulabilir. Türk hukuku bakımından usuli

64 **Çelikel**, Serdar: Kişisel Verilerin Korunması Kanunu Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri, B.1, Ankara 2022, s.114.

yükümlülüğün bu külfet kaydırıcı işlevi, esas olarak devletin etkili soruşturma ödevi üzerinden işler.

Son olarak, usuli yükümlülüğün sınırsız olmadığı vurgulanmalıdır. Gerçekten de *K.U./Finlandiya* kararının ortaya koyduğu üzere, bu yükümlülük makamlara ya da yasa koyucuya imkânsız veya orantısız bir yük yükleyecek biçimde yorumlanamaz ve soruşturma yetkileri, şüphelinin kendi temel hakları dâhil olmak üzere usule ilişkin güvencelere saygı çerçevesinde kullanılmalıdır[65]. Bu nedenle usuli yükümlülük, esasa ilişkin hakkı fiilen var eden güçlü ve kurucu bir güvence olmakla birlikte, ölçülülük ilkesi ve üçüncü kişilerin çatışan menfaatleriyle dengelenmek zorundadır.

V. ETKİN BİR HUKUKİ ÇERÇEVE KURMA YÜKÜMLÜLÜĞÜ

A. Yükümlülüğün İçeriği

Devletin pozitif yükümlülüğünün üçüncü katmanı, hakkı etkili biçimde koruyacak bir hukuki çerçeve kurma ödevidir. AİHM içtihadında yatay düzlemdeki ihlallerin önlenmesi, her şeyden önce Sözleşmede yer alan hakların etkili korunması için gerekli yasal çerçevenin taraf devletlerce oluşturulmasına bağlıdır. Bu gereklilik kimi hakta doğrudan Sözleşme metninden de kaynaklanabilir[66]. Ne var ki biçimsel bir hukuki çerçevenin varlığı, düzenleyici yükümlülüğün yerine getirildiği anlamına gelmez. Bu yükümlülüğün ayırt edici niteliği, güvenceyi kâğıt üzerinde bırakmayıp fiilen işler kılmasıdır. *I./Finlandiya* kararında AİHM, yalnızca yasal koruma ve giderim imkânının var olmasının yeterli olmadığını, gereken şeyin yetkisiz erişimi en baştan dışlayacak pratik ve etkili koruma olduğunu vurgulamıştır. Aynı doğrultuda *K.U./Finlandiya* kararında, bir suçun soyut olarak var olmasının, faili belirleyip adalet önüne çıkaracak etkili bir araç bulunmadığında sınırlı bir caydırıcılığa sahip olduğu belirtilmiştir[67]. Düzenleyici yükümlülük, bu nedenle yalnızca kural ihdasını değil, kuralların fiilen uygulanabilir ve yaptırıma bağlı olmasını da gerektirir. Türk hukukunda bu yükümlülüğün anayasal kaynağı, Anayasa'nın

65 AİHM, *K.U./Finlandiya*, §§ 48-49.

66 **Hazar**, s. 404.

67 AİHM, *K.U./Finlandiya*, § 46.

20'nci maddesinin son cümlesindeki *"kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir"* hükmüdür.

B. Türk Hukukunda Düzenleyici Yükümlülük

Anayasa Mahkemesi'nin yerleşik içtihadı, kişisel verilerin korunmasını isteme hakkının korunmasında etkin bir hukuki çerçeve aramaktadır. Mahkemeye göre, kişisel verilerin korunması hakkına müdahale teşkil ettiği ve kaldırılması gerektiği konusunda ileri sürülecek iddiaların esasının incelenmesine imkân sağlayan ve gerektiğinde uygun bir telafi yöntemi sunan etkili hukuk yollarının bulunması, ilgililere etkili başvuru hakkının sağlanması bakımından bir gerekliliktir[68]. Bu içtihadın somut bir uygulaması Cem Özberk kararında görülür. Anılan kararda Mahkeme, kişisel verilerin hukuka aykırı biçimde ele geçirilmesi ve açıklanmasının mevzuatta suç olarak düzenlendiğini, KVKK'nın kişisel verilerin aktarılmasını açık rızaya bağladığını ve sağlık verisinin 6'ncı madde anlamında özel nitelikli veri saydığını tespit etmiştir. Mahkemenin bu tespiti, düzenleyici yükümlülüğün özünü ortaya koyar. Zira temel hakların korunması bakımından yalnızca bir hukuki çerçevenin oluşturulmuş olması yeterli görülmez. Bu çerçevenin yargı makamlarınca etkili bir şekilde uygulanması ve verilen kararların ilgili hakkın korunmasını sağlayacak nitelikte, ilgili ve yeterli gerekçelere dayanması da gerekir. Aksi hâlde, mevcut yasal düzenlemelere rağmen hak ihlali söz konusu olur.

C. Kişisel Verileri Koruma Kanununun Düzenleyici İşlevi

Düzenleyici yükümlülüğün asli aracı KVKK'dır. Kanunun 12'nci maddesi hükmü, veri sorumlusunu, kişisel verilere hukuka aykırı erişimi önlemek ve verilerin hukuka aykırı işlenmesini engellemek amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli teknik ve idari tedbirleri almakla yükümlü kılar. Bu hüküm, koruma/önleme katmanının somut içeriğini oluşturmakla birlikte, aynı zamanda düzenleyici çerçevenin veri sorumlularına yüklediği pozitif bir edim ödevidir. Zira yükümlülüğün muhatabı yalnızca devlet değil, veriyi işleyen tüm gerçek ve tüzel kişilerdir.

Düzenleyici çerçevenin siber ihlallere özgü en önemli aracı,

68 AYM, *Ümit Eyüpoğlu*, B. No. 2018/6161, 28/06/2022, § 53.

KVKK'nın 12'nci maddesinin 5'inci fıkrasında öngörülen ihlali bildirim yükümlülüğüdür. Bu hükme göre, işlenen kişisel verilerin hukuka aykırı yollarla başkaları tarafından elde edilmesi hâlinde veri sorumlusu, durumu en kısa sürede Kişisel Verileri Koruma Kurulu'na ve ilgili kişiye bildirmekle yükümlüdür. Bildirim yükümlülüğü, ihlalin gizlenmesini engelleyerek hem ilgili kişinin kendi verisini koruyacak tedbirleri alabilmesini hem denetim makamının zamanında müdahalesini mümkün kılar. Bu yönüyle ispat asimetrisini de bir ölçüde gidererek bilgi yükünü veri sorumlusuna kaydırır.

Düzenleyici yükümlülüğün kurumsal karşılığı, KVKK ile kurulan Kişisel Verileri Koruma Kurumu ve onun karar organı olan Kuruldur. Kurul, veri sorumlularının yükümlülüklerine uyumunu denetleme ve aykırılıklar hâlinde Kanunun 18'inci maddesi hükmü uyarınca idari para cezası uygulama yetkisine sahiptir. Bu denetim ve yaptırım yetkisi, düzenleyici çerçeveyi salt bir kurallar bütünü olmaktan çıkarıp fiilen işleyen bir koruma mekanizmasına dönüştüren unsurdur[69]. Etkin bir denetim ve yaptırım düzeni bulunmadığında, kâğıt üzerindeki kurallar *K.U./Finlandiya* kararında işaret edilen *"soyut yaptırım"* niteliğine indirgenir.

Düzenleyici yükümlülüğün eleştirel çözümlemesi, düzenlemenin varlığı ile etkinliği arasındaki açığa odaklanmalıdır. Türk hukuku, kapsamlı bir kişisel verilerin korunması mevzuatına ve bağımsız bir denetim otoritesine sahiptir. Bu yönüyle düzenleyici çerçevenin biçimsel unsurları mevcuttur. Ancak düzenleyici yükümlülük, yalnızca kuralların yokluğuyla değil, var olan kuralların etkisiz biçimde işletilmesiyle de ihlal edilebilir. Cem Özberk kararı bu açığı somutlaştıran bir karardır. Kişisel verilerin hukuka aykırı ele geçirilmesini suç sayan ceza normları ve KVKK yürürlükteyken dahi, çerçeve etkili biçimde işletilmediği için hak ihlali söz konusu olmuştur. Dolayısıyla düzenleyici yükümlülüğün asıl sınandığı yer, mevzuatın varlığı değil, etkinliğidir.

Bu tespitin siber güvenlik bağlamındaki sonucu da ortadadır. Zira etkin bir düzenleyici çerçeve, yalnızca soyut kurallar koymakla yetinemez, uygulanabilir güvenlik standartları, fiilî sonuç doğuran

69 **Çelikel**, s. 162.

bir ihlal bildirim rejimi ve denetim ile yaptırım kapasitesine sahip bir otorite öngörmek zorundadır. Aksi hâlde çerçeve, koruma sağlamayan bir biçimsel cephe olarak kalır. Karşılaştırmalı hukukta bu etkinlik sorununa verilen caydırıcı yaptırımlar ve ispat yükünün veri sorumlusuna kaydırılması gibi yanıtlar Türk hukukuna karşılaştırmalı bir referans olarak aktarılabilir.

VI. AVRUPA BİRLİĞİ VERİ KORUMA REJİMİ ve ABAD İÇTİHADI

A. Yöntemsel Çerçeve ve Sınır

Avrupa Birliği Genel Veri Koruma Tüzüğü *(GDPR)*, Türkiye'de doğrudan uygulanan bir hukuk kaynağı değildir. Bu nedenle ne GDPR hükümleri ne de Avrupa Birliği Adalet Divanı kararları, Türk hukukunda bağlayıcı norm olarak ileri sürülebilir. Bu kaynaklar yalnızca karşılaştırmalı hukuk ve KVKK'nın yorumunda referans değeri taşır. Karşılaştırmanın meşru zeminini, 6698 sayılı KVKK'nın Avrupa Birliği veri koruma müktesebatından esinlenerek hazırlanmış olması oluşturur. Bu esinlenme, GDPR'ın merkezindeki hesap verebilirlik *(accountability)* ilkesini de kapsayan kavramsal bir yakınlık doğurur. Nitekim hesap verebilirlik, GDPR'ın kurucu bir unsuru olarak veri sorumlusunun yükümlülüklerinin eksenine yerleştirilmiştir[70].

B. Çekirdek İçtihat: Natsionalna agentsia za prihodite (C-340/21)

Siber güvenlik ihlalleri bakımından AB hukukunun en önemli kararı, ABAD'ın Bulgaristan Ulusal Gelir İdaresi'ne *(NAP)* yönelik siber saldırıya ilişkin C-340/21 kararıdır. Kamu borçlarının tespiti ve tahsiliyle görevli ve bu kapsamda veri sorumlusu sıfatını taşıyan NAP'ın bilişim sistemine 2019 yılında sızılmış, saldırı sonucunda altı milyonu aşkın kişinin kişisel verileri internette yayımlanmıştır. Etkilenen kişilerden biri, verilerinin ileride kötüye kullanılacağı endişesine dayanarak manevi tazminat talebiyle ulusal mahkemeye

70 **Taal**, Amie: The GDPR Challenge: Privacy, Technology and Compliance in an Age of Accelerating Change, Eo.1, Boca Raton 2022, p.5; **Voigt**, Paul/**Von Dem Bussche**, Axel: The EU General Data Protection Regulation (GDPR), Eo.1, Cham 2017, p.31.

başvurmuş, uyuşmazlık ön karar usulüyle Divan'a taşınmıştır[71]. Divan'ın kararı üç eksende çözümlenebilir.

Divan, *Österreichische Post* kararındaki yaklaşımını geliştirerek, bir kişinin GDPR ihlali sonucunda verilerinin üçüncü kişilerce kötüye kullanılabileceğine dair duyduğu korkunun tek başına manevi zarar oluşturabileceğini kabul etmiştir. Bu tespit, zararın doğumunu fiilî kötüye kullanım anına bağlayan dar anlayıştan ayrılır. Bununla birlikte Divan, korkunun soyut ve varsayımsal olmamasını arar. Korkunun gerçekten mevcut olup olmadığı ve somut koşullarda temellendirilip temellendirilemeyeceği ulusal mahkemece belirlenir, salt varsayımsal bir gelecekteki zarar riski tazminat hakkı doğurmaz. Böylece manevi zarar, mevcut bir korkuya dayanmakla birlikte ispata tabi tutulmuş ne tümüyle soyutlaştırılmış ne de fiilî kötüye kullanım koşuluna indirgenmiştir.

Kararın ikinci ekseni, ispat yükünün dağılımına ilişkindir. Divan, ihlalin üçüncü kişilerin *(saldırganların)* eyleminden kaynaklanmasının, veri sorumlusunu sorumluluktan kurtarmadığını belirtmiştir. Tazminat davasında, uygulanan teknik ve idari tedbirlerin uygun olduğunu ispat yükü, ilgili kişiye değil veri sorumlusuna düşer. Bu dağılım, GDPR'ın hesap verebilirlik ilkesinin doğal bir sonucudur. Tedbirlerin uygunluğunu kanıtlayacak bilgi ve belge, mağdurda değil veri sorumlusunda bulunduğundan, ispat yükü de ona yüklenmiştir. Bu yaklaşım, yapısal ispat asimetrisine doğrudan bir yanıttır.

Üçüncü eksen, tedbirlerin uygunluğuna ilişkin yargısal denetimin kapsamıdır. Divan'a göre teknik ve idari tedbirlerin uygunluğu, somut biçimde ve ilgili düzenlemelerde sayılan ölçütler ile söz konusu işlemenin özellikleri gözetilerek değerlendirilmelidir. Bu değerlendirmenin iki yönlü bir denge içerdiği görülür. Bir yandan bir ihlalin gerçekleşmiş olması tek başına tedbirlerin uygun olmadığı sonucuna varmak için yeterli değildir. Öte yandan, ulusal mahkeme yalnızca verinin yetkisiz bir üçüncü kişiye ifşa edildiği olgusuna odaklanamaz, veri sorumlusunun tedbirlerinin uygunluğunu kanıtlamak için sunduğu tüm delilleri

71 ABAD, *Natsionalna agentsia za prihodite*, C-340/21, 14/12/2023.

değerlendirmek zorundadır. Dolayısıyla yargısal denetim, tedbirlerin yalnızca biçimsel varlığını ya da ihlalin salt gerçekleşmiş olmasını saptamakla yetinemeyen, esasa ilişkin ve somut bir denetimdir.

C. Österreichische Post (C-300/21) ve Manevi Zarar Eşiği Tartışması

C-340/21 kararının dayandığı temel, daha önce verilen Österreichische Post kararıdır. Bu kararda Divan, GDPR'ın tazminat hükmü kapsamında tazminata hak kazanabilmek için, bir GDPR ihlali, bir zarar ve bu ikisi arasında nedensellik bağını içeren üç kümülatif koşul aramıştır[72]. Divan, salt bir ihlalin varlığının tek başına tazminat hakkı doğurmadığını, ancak manevi zararın tazmin edilebilmesi için belirli bir asgari ağırlık eşiğini aşmasını arayan hiçbir ulusal kuralın da GDPR ile bağdaşmadığını belirtmiştir. Bu yaklaşım, manevi zararın kapısını ne sonuna kadar açar ne de bir ağırlık eşiğiyle kapatır. Zarar ispatlanmak zorundadır, ancak ispatlandığında önemsizliği gerekçesiyle tazminattan yoksun bırakılamaz. Kötüye kullanım korkusunu manevi zarar sayan bu yaklaşım, eşiksiz ama ispata bağlı çerçeve içinde anlam kazanır.

D. Kişisel Verilerin Korunması Kanunu ile Karşılaştırmalı Değerlendirme

Avrupa Birliği rejimi ile KVKK arasındaki karşılaştırma hem yakınlıkları hem de farkları ortaya koyar. Kavramsal düzlemde önemli bir koşutluk vardır. GDPR, kişisel veri ihlalini geniş biçimde tanımlar ve ihlalleri gizlilik, erişilebilirlik ve bütünlük ihlalleri olarak tasnif eder[73]. Bu üçlü tasnif, teknik temelde kurulan ayrımla örtüşür. Veri güvenliğinin gizlilik, bütünlük ve erişilebilirlik ekseninin hem teknik hem hukuki kaynaklarda ortak bir zemine oturduğunu gösterir. Benzer biçimde GDPR'ın risk

72 ABAD, *Österreichische Post*, C-300/21, 04/05/2023, § 32.

73 **Long**, William R.M./**Blythe**, Francesca/**Raul**, Alan Charles: *"The Privacy, Data Protection and Cybersecurity Law Review: Chapter 2 - EU Overview=Gizlilik, Veri Koruma ve Siber Güvenlik Hukuku İncelemesi: Bölüm 2 - Avrupa Birliği Genel Bakışı"*, The Privacy, Data Protection and Cybersecurity Law Review=Gizlilik, Veri Koruma ve Siber Güvenlik Hukuku İncelemesi, Ed. Alan Charles Raul, Eo.7, London 2020, p.15.

temelli güvenlik yükümlülüğü ile KVKK'nın 12'nci maddesinin *"uygun güvenlik düzeyini temin etme"* ölçütü, aynı düşünsel kökten beslenir.

İhlal bildirimi bakımından da koşutluk belirgindir. GDPR, veri sorumlusunu, ilgili kişinin hak ve özgürlükleri bakımından risk doğurması muhtemel ihlalleri gecikmeksizin ve mümkünse ihlalden haberdar olduktan sonra en geç yetmiş iki saat içinde denetim makamına bildirmekle yükümlü tutar[74]. KVKK'nın 12/5'inci maddesi ise bildirimi *"en kısa sürede"* yapılması gereken bir yükümlülük olarak düzenler. Bu sürenin somutlaştırılması Kurul kararlarına bırakılmıştır. İki rejim arasındaki fark, bildirim yükümlülüğünün varlığında değil, süre standardının kanun düzeyinde sayısallaştırılıp sayısallaştırılmadığındadır.

Asıl ayrışma, sorumluluk rejiminde ortaya çıkar. GDPR, açık bir tazminat hükmü öngörür ve C-340/21 kararıyla ispat yükünü veri sorumlusuna kaydırır. Türk hukukunda ise veri ihlalinden doğan tazminat, kural olarak genel haksız fiil sorumluluğu üzerinden işletilir. KVKK'da, GDPR'ın tazminat hükmüne ve ona bağlı ispat yükü karinesine birebir karşılık gelen açık bir düzenleme bulunmamaktadır[75]. Bu durumun pratik sonucu, ispat asimetrisinin Türk hukukunda daha belirgin biçimde sürmesidir. Zira mağdur, kural olarak haksız fiilin şartlarını ve özellikle kusur ile nedenselliği ispatla yükümlüdür. C-340/21'in kötüye kullanım korkusunu manevi zarar sayan yaklaşımı ile ispat yükünü kaydıran karinesi, Türk hukuku bakımından bağlayıcı olmamakla birlikte, manevi tazminata ilişkin TBK'nın 58 ve haksız fiil sorumluluğuna ilişkin 49'uncu maddeleri hükümlerinin yorumunda dikkate alınabilecek karşılaştırmalı bir perspektif sunar.

Son olarak vurgulanmalıdır ki bu karşılaştırma, KVKK'nın yorumunu zenginleştirmeye yönelik bir referans çerçevesidir. GDPR hükümleri ve ABAD kararları, Türk hukukunda doğrudan uygulanabilir kurallar değil, KVKK'nın AB müktesebatıyla

74 **Long/Blythe/Raul**, p. 16; **Taal**, p. 5; **Voigt/Von Dem Bussche**, p. 65-67.

75 **Demirboğa**, Dursun Ali: *"Avrupa Veri Koruma Tüzüğünün (GDPR) Sınıraşan Sorumluluk Hükümlerinin Türk Hukuku Kapsamında Değerlendirilmesi"*, ÇÜHFD, C.4, S.7, Haziran 2017, s.46.

paylaştığı ortak kavramsal zemin sayesinde yorumda yol gösterici olabilecek karşılaştırmalı kaynaklardır.

VII. VERİ İHLALİNDEN DOĞAN ZARARIN TAZMİNİ

Devletin pozitif yükümlülüğü, ihlalin önlenmesi ve etkili biçimde soruşturulmasıyla tamamlanmaz, ihlal sonucunda doğan zararın giderilmesi de bu yükümlülüğün ayrılmaz bir halkasıdır. Nitekim devletin koruma görevi, ihlali önleyemediği durumda soruşturma, gerektiğinde yargılama ve nihayetinde tazminat ile telafiyi içeren bir korumayı sağlamayı gerektirir[76]. Türk hukukunda veri ihlalinden doğan zararın tazmini, esas olarak kişilik hakkının korunmasına ilişkin koruyucu davalar *(TMK m. 24-25)* ve genel haksız fiil sorumluluğu *(TBK m. 49, m. 58)* eksende işler. Kişisel verilerin korunmasını isteme hakkının, anayasal olarak Anayasa'nın 20'nci maddesinde güvenceye alınmış olmakla birlikte, özel hukuk düzleminde kişilik hakkının bir görünümü olarak korunduğu kabul edilmelidir.

A. Kişilik Hakkının Korunması ve Koruyucu Davalar

Bir siber güvenlik ihlali sonucunda kişisel verilerin yetkisiz biçimde ele geçirilmesi veya ifşa edilmesi, kural olarak kişilik hakkına hukuka aykırı bir saldırı oluşturur. TMK m. 24 uyarınca, kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır. Bu çerçevede, hukuka uygunluk sebebi bulunmadan gerçekleşen bir veri ifşası, hukuka aykırılık unsurunu kural olarak karşılar.

Türk Medeni Kanunu'nun 25'inci maddesi, kişilik hakkı saldırıya uğrayan kişiye bir dizi koruyucu dava imkânı tanır. Davacı hâkimden, saldırı tehlikesinin önlenmesini *(önleme davası)*, sürmekte olan saldırıya son verilmesini *(durdurma davası)* ve sona ermiş olsa bile etkileri devam eden saldırının hukuka aykırılığının tespitini *(tespit davası)* isteyebilir. Bunlarla birlikte maddî ve manevî tazminat ile hukuka aykırı saldırı dolayısıyla elde edilen kazancın vekâletsiz iş görme hükümlerine göre kendisine

76 **Bayra**, s. 186.

verilmesini talep etme hakkı da saklıdır[77]. Bu davalar içinde önleme davası, koruma/önleme yükümlülüğünün özel hukuk düzlemindeki tamamlayıcısıdır. Birey, henüz gerçekleşmemiş bir veri ihlali tehlikesini önlemek için yargısal koruma isteyebilirken, devletin düzenleyici yükümlülüğü de bu yolun fiilen işler olmasını gerektirir. Durdurma davası ise verilerin internette yayımlanması gibi etkisi süren ifşalar bakımından özel bir öneme sahiptir. Zira böyle bir durumda zarar, tek seferlik bir olay değil, devam eden bir nitelik arz eder.

B. Haksız Fiil Sorumluluğu

Veri ihlalinden doğan tazminat talebinin temel hukuki dayanağı, haksız fiil sorumluluğunu düzenleyen TBK'nın 49'uncu maddesidir. Hükme göre, kusurlu ve hukuka aykırı bir fiille başkasına zarar veren, bu zararı gidermekle yükümlüdür. Siber güvenlik ihlalleri bağlamında genel sorumluluğun unsurları somut olay düzeyinde belirginleşir[78]. Bu çerçevede fiil, çoğu durumda gerekli teknik ve idari güvenlik tedbirlerinin alınmaması şeklindeki ihmali bir davranıştan oluşur. Hukuka aykırılık, veri sorumlusunun KVKK'nın 12'nci maddesinde öngörülen veri güvenliğini sağlama yükümlülüğünü ihlal etmesi veya kişisel verilerin hukuka aykırı biçimde işlenmesiyle ortaya çıkar. Kusur unsuru ise veri sorumlusunun gerekli dikkat ve özeni göstermemesinde; örneğin bilinen güvenlik açıklarını gidermemesi, güncel koruma önlemlerini uygulamaması ya da etkili erişim kontrol mekanizmaları oluşturmamasında somutlaşır. Zarar, olayın özelliklerine göre maddi veya manevi nitelik taşıyabilir. Nedensellik bağı ise meydana gelen zararla güvenlik açığı ya da ihmal edilen güvenlik tedbiri arasındaki ilişkinin ortaya konulmasıyla kurulur.

Bu unsurların ispatı, uygulamada en zorlu sorunu oluşturur. Mağdur, kural olarak kusuru ve nedenselliği ispatla yükümlüdür. Oysa tedbirlerin yeterliliğine ve ihlalin mekanizmasına ilişkin

77 **Oğuz**, s. 235-238; **Eren**, s. 885-886; **Oğuz**, Habip: İnternet Ortamında Kişilik Haklarının İhlâli ve Korunması, B.2, Ankara 2012, s.151 vd. *(**Oğuz**, Kişilik Hakkı)*

78 **Eren**, s. 584.

bilgi ve belge, mağdurda değil veri sorumlusunda bulunmaktadır. Karşılaştırmalı hukukta bu güçlük, ispat yükünün veri sorumlusuna kaydırılmasıyla aşılmıştır. Ne var ki bu çözüm Türk hukuku bakımından bağlayıcı değildir ve genel haksız fiil rejiminde ispat yükü kural olarak mağdurda kalmaya devam eder. KVKK'nın veri sorumlusu için özel bir sorumluluk türü ya da kusur karinesi öngörüp öngörmediği konusunda doktrinde çeşitli görüşler bulunmaktadır[79].

C. Manevi Tazminat

Veri ihlallerinde zararın ağırlıklı olarak manevi nitelik taşıdığı dikkate alındığında, TBK m. 58 merkezî bir öneme sahiptir. Hükme göre, kişilik hakkının zedelenmesinden zarar gören kişi, uğradığı manevi zarara karşılık manevi tazminat isteyebilir[80]. Hâkim, bu tazminat yerine veya buna ek olarak başka bir giderim biçimi kararlaştırabilir, özellikle saldırıyı kınayan bir karar verebilir ve bu kararın yayımlanmasına hükmedebilir. Özel nitelikli verilerin, özellikle sağlık verisinin ifşası, niteliği gereği kişinin onurunu ve sosyal itibarını zedeleyen bir manevi zarar doğurmaya elverişlidir. Hâkime tanınan alternatif giderim yetkisi, veri ihlalleri bakımından işlevseldir. Salt para ödenmesi yerine, hukuka aykırı içeriğin silinmesine ya da düzeltilmesine ve kararın yayımlanmasına hükmedilmesi, sürmekte olan bir ifşanın etkilerini bertaraf etmede çoğu kez daha etkili bir telafi sağlar.

D. Sorumluluğun Sınırları ve İspat Sorunları

1. Zararın İspatı ve Kötüye Kullanım Endişesinin Türk Hukukundaki Yeri

Manevi tazminat bakımından eşik sorun, zararın fiilî bir kötüye kullanımı mı gerektirdiği, yoksa gelecekteki kötüye kullanıma ilişkin temellendirilmiş bir korkunun yeterli olup olmadığıdır. Karşılaştırmalı hukukta Divan, kötüye kullanım korkusunun tek başına manevi zarar oluşturabileceğini, ancak bu korkunun

79 **Çekin**, s. 172-173; **Badur**, Emel/**Kurt Konca**, Nesibe: *"Kişisel Verilerin Hukuka Aykırı İşlenmesinden Doğan Zararların Tazmini ve Görevli Mahkeme"*, İnÜHFD, C.13, S.2, y.2022, s.482; **Demirboğa**, s. 46.

80 **Eren**, s. 888-889.

soyut ve varsayımsal olmaması gerektiğini kabul etmiş, manevi zararın asgari bir ağırlık eşiğini aşmasını aramayı reddetmekle birlikte zararın ispatlanmasını şart koşmuştur. Türk hukukunda manevi tazminat, kişilik hakkının zedelenmesini gerektirir. Verinin yetkisiz biçimde ele geçirilmesiyle kişinin verisi üzerindeki denetimini yitirmesinin ve bundan doğan kaygının kişilik hakkını zedeleyip zedelemediği, özellikle özel nitelikli veriler bakımından savunulabilir bir tartışmadır. Bu konuda öğretide çeşitli görüşler bulunmaktadır. C-340/21'in yaklaşımı, TBK m. 58'in yorumunda dikkate alınabilecek karşılaştırmalı bir perspektif sunmakla birlikte bağlayıcı değildir. Herhâlde manevi zararın varlığını ispat külfeti, Türk hukukunda zarar görene düşmektedir.

2. Veri Sorumlusunun Sorumluluğu ile Devletin Sorumluluğunun Ayrışması

Veri ihlallerinde sorumluluk, birbirinden ayrılması gereken iki ayrı hat üzerinde işler. Birinci hat, ihlalden doğrudan doğan veri sorumlusunun sorumluluğudur. Veri sorumlusu özel bir kişi ise, sorumluluk genel haksız fiil hükümleri *(TBK m. 49, m. 58)* ve kişilik hakkının korunmasına ilişkin davalar *(TMK m. 24-25)* çerçevesinde adlî yargıda, veri sorumlusu bir kamu kurumu ise, idarenin sorumluluğu *(kural olarak hizmet kusuru)* çerçevesinde idarî yargıda gündeme gelir. Her iki hâlde de sorumluluk, ihlalin kendisine ilişkindir.

İkinci hat, devletin koruma, usul ve düzenleme yükümlülüklerini yerine getirmemesinden doğan sorumluluğudur. Bu sorumluluk, devletin veri sorumlusu sıfatından bağımsızdır ve niteliği gereği genel haksız fiil mekanizmasıyla değil, anayasal ve insan hakları koruma mekanizmalarıyla işler. Nitekim *Cem Özberk* kararında ihlalin tespiti üzerine yeniden soruşturma kararı verilmiş, *I./Finlandiya* ve *K.U./Finlandiya* kararlarında ise devletin pozitif yükümlülüğünü yerine getirmemesi, Sözleşme ihlali olarak tespit edilmiştir. İki hat kimi zaman örtüşebilir. Örneğin bir kamu kurumunda gerçekleşen ihlal, hem o kurumun veri sorumlusu sıfatıyla sorumluluğunu hem devletin pozitif yükümlülük sorumluluğunu birlikte gündeme getirebilir. Ne var ki bu iki sorumluluk farklı temellere dayanır ve farklı yollarla takip edilir. Bu ayrımın pratik sonucu, sorumluluğun sınırlarına ilişkindir.

Devlet her ihlalin mutlak güvencesi olan bir sonuç sorumlusu değildir. Veri sorumlusunun sorumluluğu da haksız fiilin genel şartlarıyla, özellikle kusur ve nedensellik unsurlarıyla sınırlıdır.

VIII. TEMEL HAKLARIN ÖZEL HUKUKA ETKİSİ (YATAY ETKİ)

Kişisel verilerin korunmasını isteme hakkı yalnızca devlete karşı dikey biçimde değil, özel hukuk ilişkilerine de etki eden bir haktır. Belirtmek gerekir ki siber güvenlik ihlallerinin failleri çoğunlukla devlet değil, özel veri sorumluları, siber saldırganlar ve ihmalkâr çalışanlardır. Klasik anlayış, insan haklarını birey-devlet ilişkisinde hiyerarşik olarak üstte yer alan devlete karşı dikey biçimde konumlandırmış, ihlaller karşısında taleplerin yalnızca devlete yöneltilebileceğini kabul etmiştir[81]. Oysa veri ihlalleri ağırlıkla yatay düzlemde, yani özel kişiler arasında gerçekleşir. O hâlde temel sorun, anayasal hakkın bu yatay ilişkilere hangi mekanizmayla ulaştığıdır.

A. Doğrudan ve Dolaylı Yatay Etki

İnsan haklarının özel hukuka etkisi, iki temel model çerçevesinde tartışılır. Doğrudan yatay etki *(direct horizontal effect)* modeline göre temel haklar, eşit düzeydeki özel hukuk kişileri arasındaki ilişkilerde, yasalara ve yorum gerektiren ara basamaklara dayanmaya gerek olmaksızın doğrudan uygulanır. Bu model, esasa ilişkin *(bir özel hukuk kişisinin diğerine karşı doğrudan anayasal hakka dayanabilmesi)* ve usule ilişkin *(temel hakkın yargı önünde doğrudan dava yoluyla ileri sürülebilmesi)* iki bileşen içerir[82]. Ne var ki uluslararası insan hakları hukukunda doğrudan yatay etkiden söz edilemez. Çünkü uluslararası merciler önünde şikâyetler yalnızca devletler aleyhine yapılabilir[83].

Dolaylı yatay etki *(indirect horizontal effect / mittelbare Drittwirkung)* modeli ise, temel hakların özel kişilere doğrudan yükümlülük getirdiği anlayışını reddeder[84]. Bu modelin başlıca savunucusu

81 **Doğru**, D., s. 222.

82 **Doğru**, D., s. 230.

83 **Doğru**, D., s. 231.

84 **Bozbayındır**, Ali Emrah: *"İşkence ve Kötü Muamele Yasağının Yatay Etkisi (Drittwirkung)"*, THD, C.13, S.145, Eylül 2018, s.48.

Dürig'e göre, temel hakların özel kişilere doğrudan etkisi yoktur. Bu etki, devlet aracılığıyla, yani yasama organının özel hukuka ilişkin yaptığı yasalar ve yargı organının özel hukuk yargılamalarında temel haklara uygun yorum faaliyeti yoluyla gerçekleşir[85]. Bu modelde kamu hukuku ile özel hukuk özerk iki alan olarak kalır. İrade özerkliği korunur ve hak ihlallerinden dolayı devletin sorumluluğu sürer. Modelin Alman hukukundaki klasik dayanağı *Lüth* kararıdır. Bu kararla Alman içtihadı doğrudan yatay etkiden dolaylı etkiye kaymış ve dolaylı etki, temel hakların *"değer ve yayılma etkisi" (Ausstrahlungswirkung)* üzerinden kurulmuştur. Bu anlayışa göre temel haklar aynı zamanda objektif bir değerler düzeni teşkil eder ve bu düzen tüm hukuk sistemine yayılır. Mahkemelerin görevi, hakkın kendisini değil temsil ettiği değerleri yasanın yorumunda dikkate almaktır. Böylece anayasa yasanın yorumunda kullanılsa dahi, dava hem maddî hem usulî olarak bir özel hukuk davası olarak kalır[86]. Karşılaştırmalı hukukta, bu modellerin yanında, anayasal güvencelerin uygulanması için devlet eyleminin varlığını arayan Amerikan *"devlet eylemi doktrini"* gibi farklı yaklaşımlar da bulunmaktadır[87].

Avrupa İnsan Hakları Sözleşmesi sistemi, bu modeller karşısında özgün bir konum benimsemiştir. Mahkeme, yatay etkiyi işaret eden tek tip bir kavram geliştirmek yerine, onu *"gerçek ve etkili bir koruma"*nın bir sonucu olarak ve pozitif yükümlülük doktrini içinde eriterek ele almayı tercih etmiştir[88]. Buna göre, Sözleşme özel kişilere doğrudan yükümlülük yüklemez. Bunun yerine, hakkın yatay ilişkilerdeki korunmasını devletin pozitif yükümlülükleri aracılığıyla sağlar. Dolayısıyla AİHS sistemi ve Türk anayasa yargısı dolaylı yatay etki modeli benimsemektedir.

B. Özel Hukuk Normlarının Temel Haklara Uygun Yorumlanması

Dolaylı yatay etki modelinin işleyiş mekanizması, özel hukuk ilişkilerinin insan hakları normlarına uygun yorumlanmasıdır. Bu modelde temel haklar, özel hukuk yargılamalarında bir

85 **Doğru**, D., s. 235.

86 **Bayra**, s. 181-182.

87 **Bayra**, s. 182.

88 **Hazar**, s. 390.

yorum aracı olarak kullanılır ve mahkemeler özel hukuka ilişkin yasaları insan hakları normları ışığında yorumlayıp uygular[89]. Bu mekanizma, hakkın yasanın yerine geçmediği, yalnızca onun yorumunda kullanıldığı bir tekniğe dayanır[90]. Anayasal normların hiyerarşik üstünlüğü ve bağlayıcılığı, yargı organını yasaları temel haklara uygun biçimde yorumlamakla yükümlü kıldığından, bu yorum faaliyeti yalnızca bir imkân değil, anayasal bir gerekliliktir[91].

Bu yorum faaliyetinin kişisel verilere uygulanması somut sonuçlar doğurur. Veri ihlallerine ilişkin kişilik hakkının korunmasına ilişkin TMK m. 24-25, haksız fiil sorumluluğuna ilişkin TBK m. 49 ve manevi tazminata ilişkin TBK m. 58 gibi özel hukuk normları, Anayasa m. 20 ve AİHS m. 8'in güvence altına aldığı değerler ışığında yorumlanmalıdır. Örneğin TMK m. 24 ve TBK m. 49 bağlamındaki hukuka aykırılık değerlendirmesi, kişisel verilerin korunmasının anayasal değerini, TBK m. 58 kapsamındaki kişilik hakkının zedelenmesi ölçütü ise verinin, özellikle özel nitelikli verinin ifşasının ağırlığını gözetecek biçimde yorumlanmalıdır. Yorum yönteminin kendisi de bu uyumu destekler. Lafzî yorumun yetersiz kaldığı yerlerde, yasa koyucunun ve yasanın amacına amaçsal yorum yöntemiyle ulaşılabilir[92]. KVKK ile ilgili TMK ve TBK hükümlerinin amacı, kişiliğin ve kişisel verinin korunması anayasal amacını da içerdiğinden, amaçsal yorum bu hükümlerin temel haklara uygun biçimde uygulanmasını sağlar. Böylece hak, özel hukuka, irade özerkliğini ortadan kaldırmadan ve özel hukukun bağımsızlığını zedelemeden yayılır.

C. Veri İhlalleri Bağlamında Yatay Etkinin İşlevi

Veri ihlalleri ağırlıkla yatay düzlemde gerçekleşir. Çünkü doğrudan ihlal eden, çoğu zaman bir özel veri sorumlusu, bir saldırgan ya da içeriden bir aktördür. Oysa anayasal hak öncelikle devleti muhatap alır. Yatay etki, bu iki olgu arasındaki köprüdür.

Bu köprü, AİHS ve Türk hukuku sisteminde pozitif yükümlülük

89 **Doğru**, D., s. 236.

90 **Bayra**, s. 181.

91 **Doğru**, D., s. 236.

92 **Kaya**, Asım: *"Amaçsal Yorum"*, ABD, y.72, S.2014/4, s.365.

doktrini aracılığıyla kurulur. Yatay etkiye ilişkin pozitif yükümlülük doktrini, temel olarak devletin bireyleri diğer bireylerin müdahalelerine karşı koruma yükümlülüğüne odaklanır[93]. Dolayısıyla koruma/önleme, usul ve düzenleme yükümlülükleri şeklindeki üç katmanlı yapı esasen dolaylı yatay etkinin somutlaşmış hâlidir. Devlet, bu üç katman aracılığıyla, özel kişilerden kaynaklanan veri ihlallerine karşı hakkı korur. İhlalin özel hukuk düzlemindeki tasfiyesi ise, özel hukuk yolları *(TMK m. 2425, TBK m. 49, m. 58)* aracılığıyla ve bu yolların temel haklara uygun yorumlanmasıyla gerçekleşir.

Bu çerçevede kişisel verilerin korunmasını isteme hakkı, yatay ilişkilerde *"gerçek ve etkili koruma"*ya özel kişileri doğrudan bağlayarak değil, devletin pozitif yükümlülükleri ile özel hukukun temel haklara uygun yorumunun birleşimi aracılığıyla kavuşur. Bu yapı, neden bir özel aktörün gerçekleştirdiği siber ihlalin hem o aktörün özel hukuk sorumluluğunu hem de devletin pozitif yükümlülük sorumluluğunu birlikte gündeme getirebildiğini açıklar. Aynı yapı, devletin etkili bir koruma çerçevesi sağlamamasının başlı başına bir hak ihlali sayılmasının da kuramsal temelini oluşturur. Nitekim *I./Finlandiya*, *K.U./Finlandiya* ve *Cem Özberk* kararlarında ihlal, doğrudan failin eyleminden çok, devletin yatay düzlemdeki koruma, soruşturma ve düzenleme ödevlerini yerine getirmemesinden doğmuştur. Yatay etki, böylece soyut bir kuramsal kategori olmaktan çıkıp, kişisel verilerin korunmasının fiilen işleyen koruma mantığına dönüşür.

IX. TÜRK HUKUKUNUN DEĞERLENDİRİLMESİ

A. Mevcut Hukuki Durum

Türk hukuku, kişisel verilerin korunmasında çok katmanlı bir koruma çerçevesine sahiptir. Anayasal düzlemde hak, m. 20'de doğrudan güvenceye alınmış; m. 5, m. 13 ve m. 17 ile desteklenmiştir. Yasal düzlemde 6698 sayılı KVKK kapsamlı bir veri koruma rejimi kurmuş; ceza

93 **Kaya**, s. 187.

hukuku düzleminde TCK m. 135-136 kişisel verilere ilişkin fiilleri suç saymış; özel hukuk düzleminde TMK m. 24-25 ile TBK m. 49 ve m. 58 koruyucu ve tazmin edici yolları sağlamıştır. Kurumsal düzlemde ise Kişisel Verileri Koruma Kurumu ve Kurul, denetim ve yaptırım işlevini üstlenmiştir. Anayasa Mahkemesi içtihadı, kişisel verilerin korunmasını isteme hakkının devlete pozitif yükümlülükler yüklediğini; bu yükümlülüğün üçüncü kişilerin müdahalelerini önlemeyi, etkili soruşturma yürütmeyi ve etkin bir hukuki çerçeve sağlamayı kapsadığını ortaya koymuştur. Dolayısıyla koruma/önleme, usul ve düzenleme şeklindeki üç katmanlı yapı Türk hukukunun pozitif düzenlemelerinde ve içtihadında ilke düzeyinde karşılık bulmaktadır. Bu yönüyle Türk hukukunun biçimsel altyapısı, AİHM'in I./Finlandiya ve K.U./Finlandiya kararlarındaki standartlarla büyük ölçüde uyumlu, AB veri koruma rejimiyle de kavramsal olarak yakındır.

B. Uygulamada Ortaya Çıkan Sorunlar

Bu biçimsel uyuma rağmen, bir dizi yapısal sorun da mevcuttur. Birincisi, ispat asimetrisidir. Veri ihlallerinde mağdur, kural olarak haksız fiilin kusur ve nedensellik unsurlarını ispatla yükümlüyken, tedbirlerin yeterliliğine ve ihlalin mekanizmasına ilişkin bilgi veri sorumlusunun ya da saldırganın elindedir. Türk hukuku ise bu asimetriyi gideren açık bir ispat yükü kuralından yoksundur. İkincisi, etkili soruşturma açığıdır. Cem Özberk kararının gösterdiği üzere, veri ihlallerine ilişkin ceza soruşturmaları her zaman etkili ve özenli biçimde yürütülmemekte, kovuşturmaya yer olmadığına dair kararların gerekçeleri çoğu kez Anayasa m. 20'nin gerektirdiği ilgili ve yeterli gerekçe ölçütünü karşılamamaktadır. Üçüncüsü, düzenlemenin etkinliği sorunudur. Mevzuat ve denetim otoritesi mevcut olmakla birlikte, çerçevenin fiilî işleyişi yeknesak değildir. Düzenlemenin varlığı ile etkinliği arasında bir açık sürmektedir. Dördüncüsü, manevi zararın kapsamına ilişkin belirsizliktir. Verinin yetkisiz ele geçirilmesiyle doğan denetim kaybının ve gelecekteki kötüye kullanıma ilişkin temellendirilmiş korkunun tazmin edilebilir bir manevi zarar oluşturup oluşturmadığı netleşmemiştir. Beşincisi, merkezi veri tabanlarına özgü risktir. Çok sayıda vatandaş verisini merkezi sistemlerde toplayan idareler, saldırganlar için yüksek değerli bir hedef oluşturmakta,

ne var ki önleyici güvenlik standartlarının bu yükselmiş riskle her zaman orantılı olmadığı görülmektedir.

C. Yargıtay İçtihatlarının Görünümü

Yargıtay'ın kişisel verilere ilişkin ceza içtihadı, korumanın kapsamını belirleyen yerleşik bir eğilim ortaya koymaktadır. Bu içtihada göre, TCK m. 135 ve m. 136 yalnızca sır niteliğindeki kişisel verileri değil, gerçek kişiyle ilgili her türlü bilgiyi kapsar. Zira m. 135'in gerekçesinde gerçek kişiyle ilgili her türlü bilginin kişisel veri sayılması gerektiği belirtilmiştir. Dolayısıyla her türlü kişisel verinin hukuka aykırı biçimde verilmesi, yayılması veya ele geçirilmesi, m. 136'daki 30 suçu oluşturabilmektedir. Yargıtay'ın yerleşik içtihadında bu suçla korunan hukuki yarar, genel olarak kişilerin özel hayatı ve hayatın gizli alanı, özelde ise kişisel verilerdir[94]. İçtihatta ayrıca bir nitelendirme ölçütü gelişmiştir. Buna göre, hukuka aykırı biçimde ele geçirilen veya yayılan verinin doğrudan özel hayata ilişkin olması hâlinde, fiilin kişisel verilere ilişkin suç tipinden çok özel hayatın gizliliğini ihlal suçu *(TCK m. 134)* kapsamında değerlendirilebileceği kabul edilmektedir. Bunların yanında Yargıtay, somut olayda failin kastını ve mağdurun makul gizlilik beklentisini de değerlendirir. Örneğin eşlerin ortak yaşam alanındaki cihaz kullanımına ilişkin uyuşmazlıklarda makul gizlilik beklentisinin zayıflayabileceğini gözetmektedir. Özel hukuk düzleminde ise Yargıtay'ın yerleşik yaklaşımı, kişilik hakkının hukuka aykırı veri ve mahremiyet müdahaleleriyle zedelenmesi hâlinde manevi tazminata hükmedilmesi yönündedir. Bu içtihat eğilimi, koruma mantığını destekler ancak ceza içtihadının ağırlıkla bireysel failler üzerinden geliştiği, sistemik ve kitlesel siber ihlallere özgü ölçütlerin ise henüz aynı olgunlukta yerleşmediği gözlemlenebilir.

D. Çözüm ve Reform Önerileri

Yukarıda tespit edilen sorunlar, üç katmanlı yükümlülük yapısını fiilen güçlendirecek reform önerilerine işaret etmektedir. Birinci öneri, ispat yüküne ilişkindir. Veri güvenliği kaynaklı

94 **Çağlar**, İsmail: Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu (TCK m.136), B.1, Ankara 2024, s.109-110.

sorumlulukta, uygun teknik ve idari tedbirlerin alındığını ispat külfetinin veri sorumlusuna yüklenmesini öngören bir kusur karinesinin benimsenmesi değerlendirilmelidir. Karşılaştırmalı hukukta bu çözüm, ispat yükünü veri sorumlusuna kaydıran içtihatla hayata geçirilmiştir. Bu yaklaşım Türk hukuku bakımından bağlayıcı olmamakla birlikte, ispat asimetrisini gidermeye yönelik bir model olarak yol gösterici olabilir.

İkinci öneri, etkili soruşturma standardının güçlendirilmesidir. Veri ihlallerine ilişkin ceza soruşturmalarının etkili ve özenli biçimde yürütülmesi, kovuşturmaya yer olmadığına dair kararların Anayasa m. 20'nin gerektirdiği ilgili ve yeterli gerekçe ölçütünü karşılaması ve soruşturma makamlarının siber ihlalleri aydınlatacak teknik kapasiteyle donatılması gerekmektedir.

Üçüncü öneri, düzenleyici çerçevenin etkinleştirilmesidir. KVKK m. 12'deki güvenlik yükümlülüğünün, özellikle merkezi ve kamusal veri tabanları bakımından, uygulanabilir ve riskle orantılı somut standartlara dönüştürülmesi; m. 12/5'teki *"en kısa sürede"* ölçütünün açık bir süreyle netleştirilmesi, Kurul'un denetim kapasitesinin ve yaptırımların caydırıcılığının güçlendirilmesi önerilebilir.

Dördüncü öneri, manevi tazminatın kapsamına ilişkin belirsizliğin giderilmesidir. Verinin yetkisiz ele geçirilmesiyle doğan denetim kaybının ve temellendirilmiş kötüye kullanım korkusunun tazmin edilebilir manevi zarar oluşturup oluşturmadığı, doktrin ve içtihat eliyle ya da yasal düzeyde açıklığa kavuşturulmalıdır.

Beşinci ve son öneri, önleyici güvenlik standartlarına ilişkindir. Şifreleme, erişim denetimi ve erişim kayıtlarının tutulması gibi asgari güvenlik tedbirlerinin, verinin hassasiyeti ve ölçeğiyle orantılı biçimde zorunlu kılınması, *"tasarımda güvenlik"* yaklaşımının ve erişim kaydı tutma yükümlülüğünün benimsenmesi, ispat asimetrisini de yapısal olarak azaltacaktır. Bu kapsamda ilk olarak önleyici standartların güçlendirilmesi suretiyle koruyucu mekanizmaların geliştirilmesi amaçlanmalı, ikinci olarak etkili soruşturma süreçleri aracılığıyla ispat asimetrisinin azaltılması ve hak arama imkânlarının güçlendirilmesini öngören tedbirler alınmalı, son olarak ise etkili yaptırımlarla desteklenen kapsamlı

bir düzenleyici çerçevenin oluşturulması hedeflenmelidir. Bu üç unsur birlikte değerlendirildiğinde, bireylerin siber güvenlik risklerine karşı daha etkin şekilde korunmasına hizmet eden bütüncül bir koruma sistemi ortaya çıkmar.

SONUÇ

Bu çalışma, siber güvenlik ihlallerinde devletin kişisel verilerin korunmasına ilişkin pozitif yükümlülüklerini ne ölçüde yerine getirebildiği sorusunu, devletin yükümlülüğünün üç katmanlı bir yapı içinde okunabileceği varsayımı üzerinden incelemiştir. Ulaşılan ilk sonuç, kişisel verilerin korunmasında klasik negatif yükümlülük anlayışının tek başına yetersiz kaldığıdır. Verinin esas tehdidi çoğu kez devletten değil, üçüncü kişilerden kaynaklandığından, devletin yalnızca müdahaleden kaçınması hakkı boş bir güvenceye dönüştürür; hakkın fiilen korunması, devletin etkin edimini gerektiren pozitif yükümlülükleri zorunlu kılar.

İkinci sonuç, bu pozitif yükümlülüğün üç katmanının da hem Avrupa İnsan Hakları Mahkemesi hem de Anayasa Mahkemesi içtihadında somut karşılık bulduğudur. Koruma/önleme yükümlülüğü, I./Finlandiya kararında *"yetkisiz erişim ihtimalini en baştan dışlayacak pratik ve etkili koruma"* ölçütüyle ifade edilmiş, ihlal sonrası dava açma imkânının, mahremiyeti baştan korumakla aynı şey olmadığı saptanmıştır. Usuli yükümlülük, K.U./ Finlandiya kararında soyut yaptırım tehdidinin yetersizliği ve etkili soruşturma zorunluluğu üzerinden temellendirilmiş, Türk hukukunda ise Cem Özberk kararı, etkili ceza kovuşturmasının yokluğunu doğrudan bir hak ihlali saymıştır. Düzenleyici yükümlülük ise, güvenceleri kâğıt üzerinde bırakmayan, fiilen işleyen bir

hukuki çerçeve kurma ödevi olarak, Anayasa m. 20'nin *"kanunla düzenlenir"* buyruğunda ve KVKK'nın kurumsal yapısında karşılığını bulmuştur.

Üçüncü sonuç, bu üç katmanlı yapının esasen dolaylı yatay etkinin somutlaşmış hâli olduğudur. Veri ihlalleri ağırlıkla özel kişiler arasında, yani yatay düzlemde gerçekleşir; oysa anayasal hak

öncelikle devleti muhatap alır. AİHS ve Türk hukuku sistemi, bu boşluğu özel kişilere doğrudan yükümlülük yükleyerek değil, yatay etkiyi pozitif yükümlülük doktrini içinde eriterek ve özel hukuk normlarını temel haklara uygun yorumlayarak kapatmaktadır. Böylece kişisel verilerin korunmasını isteme hakkı, yatay ilişkilerde gerçek ve etkili korumaya, devletin pozitif yükümlülükleri ile özel hukukun temel haklara uygun yorumunun birleşimi aracılığıyla kavuşur.

Dördüncü sonuç, koruma/önleme yükümlülüğünün hukuki niteliğine ilişkindir. Bu yükümlülük, hiçbir ihlalin gerçekleşmemesini garanti eden bir sonuç yükümlülüğü değil, riskle orantılı ve makul tedbirleri almayı gerektiren bir özen yükümlülüğüdür. Devlet, her siber ihlalin mutlak güvencesi değildir; ancak beklenen özen ölçütü sabit olmayıp, verinin hassasiyetiyle ve tehdidin öngörülebilirliğiyle birlikte yükselir. Bu nedenle, çok sayıda vatandaş verisini merkezi sistemlerde toplayan idareler bakımından özen eşiği de buna koşut olarak ağırlaşır.

Bu tespitler, reform yönünü de belirlemektedir. Veri güvenliği sorumluluğunda ispat külfetini veri sorumlusuna kaydıran bir kusur karinesinin değerlendirilmesi, etkili soruşturma standardının güçlendirilmesi, KVKK m. 12'deki güvenlik yükümlülüğünün özellikle merkezi veri tabanları için uygulanabilir ve riskle orantılı somut standartlara dönüştürülmesi, ihlal bildirim süresinin netleştirilmesi, manevi zararın kapsamının açıklığa kavuşturulması ve şifreleme, erişim denetimi ile erişim kaydı tutma gibi asgari önleyici tedbirlerin zorunlu kılınması, üç katmanlı pozitif yükümlülüğü fiilen işlevsel kılacak başlıca adımlardır.

Nihai değerlendirmede, kişisel verilerin korunması artık salt bir gizlilik beklentisi ya da teknik bir uyum meselesi değil, devletin önleme, soruşturma ve düzenleme ödevlerini kapsayan, anayasal düzeyde temellenmiş bir pozitif yükümlülükler bütünüdür. Siber güvenlik ihlalleri çağında bu yükümlülüğün ölçütü, kuralların varlığı değil, korumanın fiilen ve etkili biçimde gerçekleşip gerçekleşmediğidir. Hakkın geleceği, bu üç katmanın kâğıt üzerinde değil uygulamada birlikte işletilmesine bağlıdır.

KAYNAKÇA[95]

Badur, Emel/**Kurt Konca**, Nesibe: *Kişisel Verilerin Hukuka Aykırı İşlenmesinden Doğan Zararların Tazmini ve Görevli Mahkeme*, İnÜHFD, C.13, S.2, y.2022, s476-490

Bayra, Adem Ersin: *İnsan Haklarının Yatay Etkisi: Temel Haklarının Korunma Düzeyi Bakımından Devletin Konumunu Yeniden Düşünmek*, AYD, C.41, S.1, y.2024, s151-212

Bozbayındır, Ali Emrah: *İşkence ve Kötü Muamele Yasağının Yatay Etkisi (Drittwirkung)*, THD, C.13, S.145, Eylül 2018, s45-60

Çağlar, İsmail: Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu (TCK m.136), B.1, Ankara 2024

Çekin, Mesut Serdar: Avrupa Birliği Hukukuyla Mukayeseli Olarak 6698 Sayılı Kanun Çerçevesinde Kişisel Verilerin Korunması Hukuku, B.3, İstanbul 2020

Çelikel, Serdar: Kişisel Verilerin Korunması Kanunu Kapsamında Veri Sorumlusu ve Veri Sorumlusunun Yükümlülükleri, B.1, Ankara 2022

Demirboğa, Dursun Ali: *Avrupa Veri Koruma Tüzüğünün (GDPR) Sınıraşan Sorumluluk Hükümlerinin Türk Hukuku Kapsamında Değerlendirilmesi*, ÇÜHFD, C.4, S.7, Haziran 2017, s29-52

Doğan, Bayram: Karşılaştırmalı Hukukta Anayasal Bir Hak Olarak Kişisel Verilerin Korunması Hakkı, B.1, Ankara 2022

Doğru, Osman: *Devletin Sorumluluğu: İnsan Hakları Avrupa Sözleşmesi'nde Pozitif Yükümlülükler*, Danıştay ve İdari Yargı Günü: 139. Yıl, Ed. Danıştay Başkanlığı, B.1, Ankara 2008, s193-210

Doğru, Derya: *İnsan Haklarının Yatay Etkisi ve Avrupa İnsan Hakları Hukukundaki İz Düşümü: Pozitif Yükümlülük Doktrini*, AYD, C.41, S.1, y.2024, s213-294 *(**Doğru**, D.)*

Eren, Fikret: Borçlar Hukuku Genel Hükümler, B.25, Ankara 2020

Gündüz, Mehmet Şükrü: Uluslararası İnsan Hakları Açısından Kişisel Veri Güvenliği, B.1, Ankara 2022

95 Dipnotlarda geçen eserlerde yazarların soyadlarına göre atıf yapılmıştır. Aynı yazarın birden çok eserine yapılan atıflar ile aynı soyadı taşıyan yazarların eserlerine yapılan atıflar, kısaltılış şekilleriyle parantez içerisinde gösterilmiştir.

Hazar, Zeynep: *Yatay Etki Kavramının Avrupa İnsan Hakları Sözleşmesi Sistemi Bağlamında Değerlendirilmesi*, AYD, C.41, S.1, y.2024, s367-441

Hoşgül, Batuhan: Etkin Soruşturma Yükümlülüğü, B.1, Ankara 2019

Kaya, Asım: *Amaçsal Yorum*, ABD, y.72, S.2014/4, s363-383

Long, William R.M./**Blythe**, Francesca/**Raul**, Alan Charles: *The Privacy, Data Protection and Cybersecurity Law Review: Chapter 2 - EU Overview=Gizlilik, Veri Koruma ve Siber Güvenlik Hukuku İncelemesi: Bölüm 2 - Avrupa Birliği Genel Bakışı*, The Privacy, Data Protection and Cybersecurity Law Review=Gizlilik, Veri Koruma ve Siber Güvenlik Hukuku İncelemesi, Ed. Alan Charles Raul, Eo.7, London 2020, p5-40

Oğuz, Habip: Kişiliğin Korunması Bağlamında Unutulma Hakkı, B.1, Ankara 2025

Oğuz, Habip: İnternet Ortamında Kişilik Haklarının İhlâli ve Korunması, B.2, Ankara 2012 *(**Oğuz**, Kişilik Hakkı)*

Rustambekov, İslambek/**Gulyamov**, Said/**Bozgeyik**, Hayri/**Sharipova**, Hilola: Dijital Devlet Yönetişiminin Teorik ve Hukuki Temelleri, B.1, Ankara 2024

Taal, Amie: The GDPR Challenge: Privacy, Technology and Compliance in an Age of Accelerating Change=GDPR Zorluğu: Hızlanan Değişim Çağında Mahremiyet, Teknoloji ve Uyum, Eo.1, Boca Raton 2022

Tahmazoğlu Üzeltürk, Sultan: *Kişisel Verilerin Korunması Hakkında Anayasa Değişikliği*, LHD, y.2010, S.93, s3151-3156

Tanrıkulu, M. Sezgin: İnsan Hakları Avrupa Sözleşmesi ve Etkili Başvuru Hakkı, B.1, Ankara 2012

Voigt, Paul/**Von Dem Bussche**, Axel: The EU General Data Protection Regulation (GDPR)=AB Genel Veri Koruma Tüzüğü (GDPR), Eo.1, Cham 2017

Wang, Anyu: Data Security and Privacy Protection: A Comprehensive Guide=Veri Güvenliği ve Gizlilik Koruması: Kapsamlı Bir Kılavuz, Eo.1, Singapore 2025

Yılmaz, Sabire Sanem: Tıp Alanında Kişisel Verilerin Korunması, B.6, Ankara 2022

Yüzer Eltimur, Dilara: AİHS Kapsamında Özel Hayatın ve Aile Hayatının Korunmasında Devletin Pozitif Yükümlülükleri, B.1, İstanbul 2019

KISALTMALAR CETVELİ

AB : Avrupa Birliği

ABAD : Avrupa Birliği Adalet Divanı

AİHM : Avrupa İnsan Hakları Mahkemesi

AİHS : Avrupa İnsan Hakları Sözleşmesi

AYM : Anayasa Mahkemesi

B. No. : Başvuru Numarası

CIA Triad : Confidentiality, Integrity and Availability

ECHR : European Court of Human Rights

GDPR : General Data Protection Regulation

KVKK : Kişisel Verilerin Korunması Kanunu

m. : madde

NAP : Bulgaristan Gelir İdaresi

TBK : Türk Borçlar Kanunu

TCK : Türk Ceza Kanunu

TMK : Türk Medeni Kanunu

DİJİTALLEŞEN DENETİM ORTAMINDA STRATEJİK RİSKYÖNETİMİ, KURUMSAL DAYANIKLILIK VE YENİ NESİL DENETİM

Strategic Risk Management, Organizational Resilience and Next-Generation Audit in the Digitalized Audit Environment

Ehtiram İSMAYİLOV
KPMG Türkiye Şirket Ortağı,
Bilgi Sistemleri Risk Yönetimi; ISACA İstanbul, Başkan

ÖZET

Dijitalleşme, denetimi örneklem temelli ve dönemsel bir güvence faaliyetinden, büyük veri, yapay zekâ, sürekli izleme ve teknoloji güvencesiyle desteklenen daha dinamik bir yönetişim fonksiyonuna dönüştürmektedir. Bu çalışma, dijital denetim ortamında ortaya çıkan siber güvenlik, veri yönetişimi, yapay zekâ, üçüncü taraf ve düzenleyici uyum risklerini stratejik risk yönetimi ve kurumsal dayanıklılık bağlamında incelemektedir. Çalışma, denetim fonksiyonunun yalnızca kontrol uygunluğunu doğrulayan bir yapı olmaktan çıkarak risk iştahı, karar alma, iş sürekliliği, teknoloji güvenilirliği ve ESG güvencesi alanlarında değer üreten bir güvence mimarisine dönüşmesi gerektiğini savunmaktadır. Sonuç olarak yeni nesil denetim yaklaşımı, insan muhakemesi ile otomasyonun dengelendiği, açıklanabilir, veri odaklı ve stratejiyle bütünleşik bir model olarak ele alınmalıdır.

A**nahtar Kelimeler:** Dijital denetim, stratejik risk yönetimi, kurumsal dayanıklılık, yapay zekâ, teknoloji güvencesi.

ABSTRACT

Digitalization is transforming audit from a sample-based and periodic assurance activity into a more dynamic governance function supported by big data, artificial intelligence, continuous monitoring and technology assurance. This article examines cybersecurity, data governance, artificial intelligence, third-party and regulatory compliance risks emerging in the digital audit environment through the lenses of strategic risk management and organizational resilience. It argues that the audit function should move beyond verifying control compliance and become an assurance architecture that creates value in risk appetite, decision-making, business continuity, technology reliability and ESG assurance. Accordingly, next-generation audit should be designed as an explainable, data-driven and strategy-integrated model that balances human judgment with automation.

Keywords: Digital audit, strategic risk management, organizational resilience, artificial intelligence, technology assurance.

GİRİŞ

Dijitalleşme, kurumların değer üretme biçimini değiştirdiği kadar denetim, risk yönetimi ve kurumsal yönetişim fonksiyonlarının çalışma mantığını da dönüştürmektedir. İş süreçleri artık yalnızca muhasebe kayıtları, onay akışları ve dönem sonu raporları üzerinden izlenmemekte; bulut altyapıları, uygulama programlama arayüzleri, uzaktan erişim çözümleri, veri gölleri, yapay zekâ modelleri, tedarikçi platformları ve sürekli akan operasyonel veri setleri üzerinden şekillenmektedir (ISACA, 2018; NIST, 2024a). Bu durum, denetim için iki yönlü bir sonuç doğurur. Bir yandan veri analiz kapasitesi artmakta, kontrol testleri genişlemekte ve anomali tespiti daha erken yapılabilmektedir (Appelbaum vd., 2017: 1-27; IAASB, 2020a). Diğer yandan denetim evreni daha karmaşık, daha hızlı değişen ve sınırları daha belirsiz bir yapıya kavuşmaktadır. Bu makalenin temel çıkış noktası, denetimin bu iki sonucu aynı anda yönetmesi gerektiğidir: daha fazla veriyle daha hızlı güvence üretmek, fakat bunu daha kırılgan ve daha karmaşık bir kontrol ortamında yapmak.

Geleneksel denetim yaklaşımı çoğunlukla belirli dönemlerde seçilen örneklemlere, geçmişe dönük belge incelemelerine ve finansal veri ağırlıklı değerlendirmelere dayanır (Vasarhelyi vd., 2004: 1-21; Alles vd., 2008: 64-80). Dijital ve sürekli denetim yaklaşımı ise veri evreninin daha geniş bölümünü kapsamayı, riskleri gerçek zamana yakın göstergelerle izlemeyi ve denetim kanıtını yalnızca kayıtların doğruluğu olarak değil, süreçlerin güvenilirliği ve teknoloji ortamının kontrol edilebilirliği olarak ele almayı gerektirir (IAASB, 2020a; IAASB, 2020b). Sürekli denetim literatürü, bu dönüşümün yalnızca daha fazla teknoloji kullanımı anlamına gelmediğini; güvence üretiminin zamanlamasını, kapsamını ve karar alma süreçleriyle ilişkisini değiştirdiğini göstermektedir (Vasarhelyi vd., 2004: 1-21; Alles vd., 2008: 64-80).

Bu çalışmanın temel amacı, dijitalleşen denetim ortamında yeni nesil risklerin nasıl yönetilmesi gerektiğini stratejik risk yönetimi, kurumsal dayanıklılık ve yeni nesil denetim perspektifleriyle tartışmaktır. Çalışma, bir uygulama raporu ya da ampirik saha araştırması olmaktan ziyade, güncel standartlar, akademik literatür ve kurumsal risk raporları üzerinden kavramsal bir

çerçeve kurmaktadır. Bu çerçeve, özellikle kamu kurumları, yüksek düzenleme baskısı altındaki kuruluşlar ve büyük ölçekli işletmeler açısından denetim fonksiyonunun yeni rolünü anlamaya yöneliktir. Çünkü dijitalleşen ortamlarda risk yönetimi artık yalnızca "risk gerçekleşti mi?" sorusuna değil, "hangi riskler stratejik amaçları, hizmet sürekliliğini ve paydaş güvenini etkileyebilir?" sorusuna yanıt aramak zorundadır (COSO, 2017; ISO, 2018). Bu soru değişimi, çalışmanın özgün katkısının da merkezindedir: denetim, geçmiş kontrol sonuçlarını raporlayan bir faaliyet olmaktan çok, kurumun gelecekteki dayanıklılık kapasitesini görünür kılan bir yönetişim pratiği olarak ele alınmalıdır.

Dijital denetim ortamını tartışırken teknik kapasite ile yönetişim kapasitesini birlikte ele almak gerekir. Büyük veri analitiği, yapay zekâ destekli sınıflandırma, istisna raporlaması ve otomasyon araçları denetçilere daha geniş veri setleri üzerinde çalışma olanağı sunar (Appelbaum vd., 2017: 1-27; Fedyk vd., 2022: 938-985). Ancak algoritmik kararların açıklanabilirliği, veri kalitesi, model yanlılığı, siber güvenlik, kişisel verilerin korunması, üçüncü taraf bağımlılığı ve düzenleyici uyum sorunları çözülmeden bu araçlar güvenilir bir denetim zemini oluşturmaz (DAMA International, 2017; NIST, 2020; NIST, 2023). NIST'in yapay zekâ risk yönetimi yaklaşımı, yapay zekâ sistemlerinde yönetişim, ölçme, yönetme ve haritalama faaliyetlerinin birlikte ele alınmasını önerirken; NIST Siber Güvenlik Çerçevesi 2.0 siber risk yönetimini kurumsal yönetişim düzeyine taşıyan "Govern" fonksiyonunu çerçeveye eklemektedir (NIST, 2023; NIST, 2024a). Bu nedenle çalışmada teknoloji, denetimin dışsal bir aracı değil, denetim nesnesinin ve denetim metodolojisinin aynı anda dönüştüğü bir alan olarak görülmektedir.

Bu çalışma beş bölümden oluşmaktadır. İlk bölüm dijitalleşen denetim ortamının geleneksel denetimden farklarını ve denetim kanıtı üzerindeki etkilerini incelemektedir. İkinci bölüm siber güvenlik, veri kalitesi, yapay zekâ, üçüncü taraf ve düzenleyici uyum risklerini ele almaktadır. Üçüncü bölüm stratejik risk yönetimine geçişi, risk iştahı ve entegre risk yönetimi bağlamında tartışmaktadır. Dördüncü bölüm kurumsal dayanıklılığı, yalnızca bilgi teknolojileri sürekliliği değil, kurum genelinde karar alma ve operasyonel sürdürülebilirlik disiplini olarak değerlendirmektedir.

Beşinci bölüm ise yapay zekâ, büyük veri, sürekli denetim, teknoloji güvencesi ve ESG güvencesi başlıklarını yeni nesil denetim yaklaşımı altında birleştirmektedir.

I. DİJİTALLEŞEN DENETİM ORTAMI

A. Geleneksel Denetimden Sürekli ve Veri Odaklı Denetime

Dijital denetim ortamının en belirgin etkisi, denetimin kapsam ve zaman boyutunda görülür. Geleneksel denetimde kanıt toplama süreci çoğunlukla örneklem, belge incelemesi ve dönemsel testler üzerinden ilerler (Vasarhelyi vd., 2004: 1-21). Bu yaklaşım, denetim kaynaklarının sınırlı olduğu dönemlerde rasyonel bir seçimdir; ancak yüksek hacimli işlem verisinin gerçek zamanlı üretildiği dijital ortamlarda tek başına yeterli değildir (Cao vd., 2015: 423-429; Appelbaum vd., 2017: 1-27). Büyük veri analitiği ve otomatik kontrol testleri, denetçinin yalnızca seçilmiş işlemlerle değil, işlem evreninin tamamına yakın bir bölümüyle çalışma olasılığını artırmaktadır (Cao vd., 2015: 423-429; IAASB, 2020b). Bu dönüşüm, örnekleme dayalı makul güvence yaklaşımını ortadan kaldırmaz; fakat riskli alanların belirlenmesi, istisnaların önceliklendirilmesi ve kanıtın zamanında üretilmesi açısından denetim kalitesini güçlendirebilir. Burada önemli olan, "daha çok veriye bakmak" ile "daha güçlü denetim kanıtı üretmek" arasındaki farkı koruyabilmektir.

Sürekli denetim, denetim faaliyetinin periyodik kapanış döngülerinden ayrılarak süreç içi göstergelere, otomatik kontrollerin işleyişine ve erken uyarı mekanizmalarına yaklaşmasıdır (Vasarhelyi vd., 2004: 1-21; Alles vd., 2008: 64-80). Bu yaklaşımda denetçi, yalnızca işlemler gerçekleştikten sonra hata ve usulsüzlük arayan bir kontrolör değil, risk göstergelerini yorumlayan ve yönetim için karar destek bilgisi üreten bir güvence uzmanı haline gelir. Literatürde sürekli denetim ve sürekli izleme ayrımı önemlidir: sürekli izleme yönetimin kontrol sorumluluğunun parçası iken, sürekli denetim bu izleme mekanizmalarının bağımsız güvence perspektifiyle değerlendirilmesini içerir (Alles vd., 2008: 64-80; IIA, 2020). Bu ayrım, denetçinin yönetime yakınlaşırken yönetimin yerine geçmemesi gerektiğini gösterir.

Dijital denetimde zaman ve kapasite kısıtlarının azalması, denetimin daha kolay hale geldiği anlamına gelmez. Aksine denetçi, veri kaynaklarının bütünlüğünü, sistem arayüzlerini, yetkilendirme kontrollerini, veri dönüşüm kurallarını, istisna algoritmalarının doğruluğunu ve raporlama zincirini birlikte değerlendirmek zorundadır (DAMA International, 2017; IAASB, 2020b). Bir analitik testin anlamlı olması için, yalnızca çıktının sıra dışı görünmesi yeterli değildir; kullanılan veri setinin eksiksizliği, değişmezliği, uygun şekilde yetkilendirilmiş sistemlerden alınması ve analiz varsayımlarının denetim amacıyla uyumlu olması gerekir (IAASB, 2020a; IAASB, 2020b). IAASB'nin otomatik araç ve tekniklere ilişkin destek materyalleri, teknolojinin denetim prosedürlerinde kullanılmasının mesleki muhakemeyi ortadan kaldırmadığını, aksine araçların uygunluğu, veri güvenilirliği ve prosedürün amaca uygunluğu hakkında daha açık değerlendirme gerektirdiğini vurgular (IAASB, 2020a; IAASB, 2020b).

Bu noktada dijital denetimin organizasyonel koşulları da önem kazanır. Analitik araçların kuruma değer katması için denetim fonksiyonunun veri erişim yetkileri, veri mühendisliği desteği, çalışma kağıdı standardı ve kalite güvence süreçleri önceden tasarlanmalıdır (DAMA International, 2017; IAASB, 2020b). Aksi halde denetçiler teknik olarak güçlü araçlara sahip olsalar bile, her denetimde veri setini yeniden temizlemek, sistem sahiplerinden manuel dosya istemek veya sonuçları yeterince belgeleyememek zorunda kalabilir. Bu durum, dijital denetimi sürdürülebilir bir kapasite olmaktan çıkarıp kişisel beceriye bağlı geçici uygulamalara dönüştürür. Kurumsal düzeyde standartlaştırılmış veri katalogları, onaylı analitik prosedürler ve denetim izleri, sürekli denetim yaklaşımının kurumsallaşması için temel altyapıdır (DAMA International, 2017; Alles vd., 2008: 64-80). Bu çalışmanın yorumu, dijital denetimin başarısının tek tek araçlardan çok bu araçları taşıyan kurumsal çalışma disiplinine bağlı olduğudur.

Bu nedenle dijital denetim ortamında "tam denetim" kavramı dikkatli kullanılmalıdır. İşlem evreninin tamamını analiz etmek teknik olarak mümkün olsa bile, bu analiz her zaman tam güvence anlamına gelmez (Cao vd., 2015: 423-429; IAASB, 2020b). Verinin kaynağı eksikse, log kayıtları manipüle edilebiliyorsa, kritik

sistemlerde yetki matrisi doğru tasarlanmamışsa veya yapay zekâ modeli yanlış sınıflandırma yapıyorsa, bütün veri üzerinde çalışmak dahi yanlış sonuçları daha hızlı üretmeye yol açabilir (DAMA International, 2017; NIST, 2023). Denetim kalitesini belirleyen unsur, veri hacminden çok veri yönetişimi, kontrol tasarımı, algoritmanın açıklanabilirliği ve denetçinin bulguları iş bağlamında yorumlayabilme kapasitesidir. Başka bir ifadeyle dijitalleşme, denetimde niceliksel kapsama sorununu azaltırken niteliksel yorumlama sorumluluğunu artırmaktadır.

B. Denetim Kanıtının Teknoloji Ortamıyla Birlikte Değerlendirilmesi

Dijitalleşme, denetim kanıtının doğasını da genişletir. Denetim kanıtı artık yalnızca fatura, sözleşme, banka mutabakatı veya muhasebe fişi gibi statik belgelerden oluşmaz (IAASB, 2020b). Sistem logları, işlem zaman damgaları, erişim kayıtları, iş akışı onayları, API çağrıları, veri aktarım izleri, model çıktıları, otomasyon kuralları ve bulut yapılandırmaları da denetim kanıtı zincirinin parçası haline gelir (DAMA International, 2017; ISACA, 2018). Bu genişleme, denetçinin bilgi sistemleri kontrolleriyle finansal ve operasyonel kontroller arasındaki ilişkiyi daha iyi anlamasını gerektirir (ISACA, 2018; IAASB, 2020a). ISACA'nın COBIT çerçevesi de kurumsal bilgi ve teknoloji yönetişiminin yalnızca BT departmanının görevi olmadığını, kurumsal hedeflerle uyumlu değer üretimi ve risk optimizasyonu gerektirdiğini belirtir (ISACA, 2018).

Teknoloji ortamıyla bütünleşik kanıt yaklaşımı, denetimde risk temelli planlamayı güçlendirir. Denetçi artık yalnızca hangi hesap kaleminin riskli olduğunu değil, bu riski üreten işlem akışının hangi sistemlerden geçtiğini, hangi dış servis sağlayıcıya bağımlı olduğunu, hangi veri alanlarının manuel değiştirilebildiğini ve hangi kontrollerin otomatik çalıştığını da analiz etmelidir (IAASB, 2020a; NIST, 2024a). Bu bağlamda dijital denetim, finansal denetim, iç denetim, BT denetimi, siber güvenlik değerlendirmesi ve veri yönetişimi kontrolleri arasında daha geçirgen bir ilişki kurar. Yeni nesil denetim yaklaşımında güvence, ayrı ayrı raporlanan kontrol testlerinin toplamı değil, uçtan uca süreç görünürlüğü üzerinden üretilen bütünleşik bir değerlendirmedir. Bu yorum,

çalışmanın denetimi parçalı kontrol testlerinden ziyade süreç ve teknoloji mimarisini birlikte okuyan bir güvence faaliyeti olarak konumlandırmasının temelini oluşturur.

Denetim kanıtının dijitalleşmesi aynı zamanda etik ve hukuki boyutları da güçlendirir (NIST, 2020; NIST, 2023). Kişisel veri içeren logların kullanımı, çalışan davranış verilerinin analizi, yapay zekâ modeliyle risk puanlaması, veri saklama süreleri ve sınır ötesi veri aktarımı gibi konular, denetim planlamasında göz ardı edilemeyecek uyum alanlarıdır (NIST, 2020; European Union, 2024). NIST Gizlilik Çerçevesi, mahremiyet risklerini yalnızca mevzuata uyum meselesi olarak değil, veri işleme faaliyetlerinin bireyler ve kurumlar üzerindeki etkilerini yönetme disiplini olarak ele alır (NIST, 2020). Bu nedenle dijital denetim kapasitesi artarken, veri minimizasyonu, amaçla sınırlılık, erişim kontrolü ve denetim izinin korunması ilkeleri daha fazla önem kazanır (NIST, 2020; DAMA International, 2017).

Bu dönüşümün kurumsal etkisi, denetim fonksiyonunun beceri setinde de görülür. Denetçiler için muhasebe ve mevzuat bilgisi halen temel yetkinliktir; ancak veri analitiği, süreç madenciliği, bilgi sistemleri kontrolleri, siber risk, model riski ve teknoloji yönetişimi bilgisi giderek daha kritik hale gelmektedir (Appelbaum vd., 2017: 1-27; ISACA, 2018). Yapay zekâ araçları denetim prosedürlerini hızlandırabilir; fakat denetçinin profesyonel şüpheciliği, bağımsızlığı ve muhakemesi yerini otomasyona bırakmamalıdır (Fedyk vd., 2022: 938-985; NIST, 2023). Fedyk vd. (2022: 938-985), yapay zekânın denetim sürecine etkisini incelerken teknolojinin denetim kalitesi ve verimliliği açısından potansiyel taşıdığını, ancak bu potansiyelin doğru örgütsel kullanım ve insan denetimiyle anlamlı hale geldiğini göstermektedir.

II. DİJİTAL ORTAMDA YENİ NESİL RİSKLER

A. Siber Güvenlik, Kimlik ve Veri İhlali Riskleri

Dijitalleşen denetim ortamında siber güvenlik riski, teknik bir olay riski olmaktan çıkıp stratejik ve finansal etkileri olan bir kurumsal risk alanına dönüşmüştür (NIST, 2024a; Verizon, 2026). Kimlik bilgilerinin ele geçirilmesi, çok faktörlü kimlik doğrulamanın zayıf uygulanması,

oltalama saldırıları, bulut yapılandırma hataları, fidye yazılımı, tedarik zinciri saldırıları ve yetkili kullanıcıların kötüye kullanımı, hem hizmet sürekliliğini hem de denetim kanıtının güvenilirliğini doğrudan etkiler (NIST, 2024a; Verizon, 2026). NIST Siber Güvenlik Çerçevesi 2.0, siber güvenliği tanımlama, koruma, tespit, yanıt ve iyileştirme fonksiyonlarına ek olarak yönetişim düzeyiyle bütünleştirir; bu da siber riskin yönetim kurulu ve üst yönetim gündeminin parçası olması gerektiğine işaret eder (NIST, 2024a).

Siber riskin denetim açısından özel önemi, güvenilir veri ve güvenilir sistem varsayımını zayıflatmasından kaynaklanır. Denetçi bir veri setini analiz ederken, bu verinin doğru sistemden geldiğini, yetkisiz değişikliğe uğramadığını, işlem izlerinin silinmediğini ve raporlama katmanında manipüle edilmediğini varsaymak zorundadır (IAASB, 2020a; IAASB, 2020b). Siber olaylar bu varsayımları doğrudan hedef alır (NIST, 2024a; Verizon, 2026). Verizon'un veri ihlali araştırmaları, kimlik bilgileri, insan unsuru, zafiyetlerin kötüye kullanımı ve üçüncü taraf bağlantılarının ihlal örüntülerinde önemli yer tuttuğunu göstermektedir (Verizon, 2026). Dolayısıyla dijital denetimde siber güvenlik kontrolleri, yalnızca BT denetiminin alt başlığı değil, bütün denetim güvenilirliğinin altyapısıdır. Bu nedenle siber bulgular denetim raporunda teknik risk olarak değil, kanıt güvenilirliği ve kurumsal güven sorunu olarak da okunmalıdır.

Yapay zekâ, siber risk profilini iki yönlü etkilemektedir (NIST, 2024b; Verizon, 2026). Savunma tarafında güvenlik olaylarının sınıflandırılması, anomali tespiti, saldırı yüzeyi izleme ve güvenlik operasyon merkezi süreçlerinde otomasyon sağlayabilir (NIST, 2024b). Saldırı tarafında ise sosyal mühendislik, kimlik avı, deepfake, otomatik zafiyet tarama ve hedefli kötü amaçlı yazılım üretimi gibi alanları güçlendirebilir (NIST, 2024b; Verizon, 2026). NIST'in üretken yapay zekâ profili, üretken modellerin yanlış bilgi üretimi, içerik manipülasyonu, veri sızıntısı, kötüye kullanım ve insan güveni üzerindeki etkileri nedeniyle özel risk yönetimi gerektirdiğini belirtir (NIST, 2024b). Bu bağlamda denetim fonksiyonu, yapay zekâyı yalnızca verimlilik aracı olarak değil, aynı zamanda yeni saldırı ve kontrol zafiyeti kaynağı olarak değerlendirmelidir.

Siber güvenlik riskleri kurumların itibarını, finansal performansını ve paydaş güvenini etkilediğinden, denetim raporlamasında teknik bulguların iş etkisiyle ilişkilendirilmesi gerekir (NIST, 2024a; COSO, 2017). Örneğin zayıf parola politikası ya da ayrıcalıklı hesap kontrol eksikliği tek başına teknik bir bulgu gibi görünebilir; ancak kritik ödeme sistemi, vatandaş verisi, müşteri bilgileri veya finansal raporlama sistemiyle ilişkili olduğunda stratejik düzeyde bir risk haline gelir. Bu nedenle yeni nesil denetim, kontrol zafiyetlerini yalnızca olasılık ve etki matrisine yerleştirmekle yetinmemeli; bu zafiyetlerin hangi stratejik amaçları, hizmet yükümlülüklerini ve yasal sorumlulukları etkilediğini göstermelidir. Bu, yazarın denetim raporlamasına ilişkin temel önerilerinden biridir.

B. Yapay Zekâ, Gölge Yapay Zekâ ve Üçüncü Taraf Riskleri

Yapay zekâ riskleri, yalnızca modellerin hatalı tahmin üretmesinden ibaret değildir. Modelin hangi veriyle eğitildiği, hangi varsayımlarla çalıştığı, hangi karar süreçlerine entegre edildiği, çıktısının kim tarafından onaylandığı, modelin zaman içinde performansının nasıl izlendiği ve yanlış kararın hangi iş sonucunu doğuracağı birlikte değerlendirilmelidir (NIST, 2023; NIST, 2024b). NIST AI RMF, yapay zekâ risk yönetimini yönetişim, haritalama, ölçme ve yönetme fonksiyonlarıyla ele alarak teknik ölçütlerle kurumsal sorumluluklar arasında bağ kurar (NIST, 2023). Bu yaklaşım, denetim fonksiyonu açısından model envanteri, sorumluluk matrisi, performans izleme, açıklanabilirlik ve insan gözetimi kontrollerinin test edilmesini gerektirir (NIST, 2023; European Union, 2024).

Gölge yapay zekâ, kurumun resmi onay ve kontrol mekanizmaları dışında kullanılan yapay zekâ araçlarını ifade eder (NIST, 2024b; McKinsey & Company, 2025). Çalışanların ücretsiz veya ticari üretken yapay zekâ araçlarına kurumsal veri yüklemesi, hassas bilgileri model çıktısıyla işlemesi veya resmi süreçleri kayıt dışı otomasyonlarla desteklemesi, veri sızıntısı, fikri mülkiyet, yanlış karar ve uyum risklerini artırır (NIST, 2023; NIST, 2024b). Bu risk, klasik gölge BT sorununa benzer; fakat üretken yapay zekânın doğal dil arayüzü, kullanım kolaylığı ve hızlı yayılımı nedeniyle daha geniş bir kullanıcı tabanına ulaşır (McKinsey & Company, 2025; NIST, 2024b). McKinsey'nin yapay zekâ kullanımına ilişkin

küresel araştırmaları, üretken yapay zekânın kurumlarda hızla benimsendiğini, buna karşılık yönetişim, risk ve değer realizasyonu mekanizmalarının aynı hızda olgunlaşmasının kritik olduğunu göstermektedir (McKinsey & Company, 2025).

Üçüncü taraf ve dış kaynak riskleri dijital ortamda daha karmaşık hale gelmiştir. Bulut sağlayıcıları, yazılım servisleri, ödeme altyapıları, veri işleme platformları, yapay zekâ servisleri ve dış güvenlik operasyon merkezleri kurumun kontrol alanını genişletir; ancak doğrudan kontrol gücünü azaltabilir (NIST, 2024a; ISACA, 2018). Üçüncü tarafın güvenlik zafiyeti, veri işleme hatası veya hizmet kesintisi, kurumun kendi hizmet kalitesini ve denetim kanıtı güvenilirliğini etkileyebilir (NIST, 2024a; BCBS, 2021). NIST CSF 2.0'ın yönetişim fonksiyonu tedarik zinciri siber risk yönetimini açık biçimde kurumsal risk yönetimiyle ilişkilendirir (NIST, 2024a). Bu nedenle denetim, üçüncü taraf sözleşmelerini yalnızca hizmet seviyesi ve maliyet açısından değil, veri erişimi, olay bildirimi, süreklilik, denetim hakkı ve alt yüklenici zinciri açısından da değerlendirmelidir.

Yapay zekâ ve üçüncü taraf riskleri birlikte düşünüldüğünde sorumluluk sınırları daha da belirsizleşir. Bir kurum dış sağlayıcının modelini kullanıyor, veriyi bulut ortamında işliyor, karar önerisini kendi personeli onaylıyor ve sonucu vatandaşa, müşteriye ya da yatırımcıya yansıtıyorsa, hatanın kaynağını ve sorumluluğunu belirlemek kolay değildir (NIST, 2023; European Union, 2024). Avrupa Birliği Yapay Zekâ Yasası'nın risk temelli yaklaşımı, yüksek riskli yapay zekâ sistemlerinde yönetişim, kayıt tutma, insan gözetimi ve şeffaflık gibi yükümlülüklere vurgu yapmaktadır (European Union, 2024). Bu eğilim, denetim fonksiyonunun yapay zekâ kullanımını yalnızca verimlilik veya inovasyon başlığı altında değil, hesap verebilirlik ve kontrol edilebilirlik başlığı altında da incelemesini gerektirir.

Bu risk alanında denetim için pratik başlangıç noktası, yapay zekâ kullanım envanteridir. Kurum hangi modellerin kullanıldığını, bu modellerin hangi iş kararlarını etkilediğini, hangi veri kaynaklarına eriştiğini, model sahibinin kim olduğunu ve çıktının hangi kontrolle onaylandığını bilmiyorsa güvence üretmek mümkün değildir (NIST, 2023; European Union, 2024). Envanterin bulunması

tek başına yeterli değildir; kullanım amaçları, risk sınıfları, veri hassasiyeti, tedarikçi bağımlılığı ve insan gözetimi mekanizmaları da kayıt altına alınmalıdır (NIST, 2023; NIST, 2024b). Böyle bir envanter, denetim planlamasında yüksek etkili ve düşük olgunluklu yapay zekâ kullanım alanlarının önceliklendirilmesini sağlar. Bu çalışma açısından envanter, bir uyum listesi değil, denetim evreninin yeniden kurulmasını sağlayan analitik bir başlangıç noktasıdır.

C. Veri Kalitesi, Veri Yönetişimi ve Düzenleyici Uyum

Dijital denetimin en kritik girdisi veridir. Veri kalitesi düşük olduğunda en gelişmiş analitik araçlar bile güvenilir sonuç üretmez (DAMA International, 2017; Appelbaum vd., 2017: 1-27). Eksik, mükerrer, tutarsız, güncel olmayan, yanlış sınıflandırılmış veya bağlamından koparılmış veri, denetim bulgularını yanıltabilir (DAMA International, 2017; IAASB, 2020b). Veri yönetişimi bu nedenle yalnızca veri ambarı ya da raporlama ekibinin teknik meselesi değildir; veri sahipliği, veri sözlüğü, kalite kuralları, erişim yetkileri, saklama politikaları, veri soy ağacı ve değişiklik izlerinin kurumsal düzeyde yönetilmesini gerektirir (DAMA International, 2017; OECD, 2021). DAMA-DMBOK, veri yönetişimini veri yönetimi disiplinlerinin merkezinde konumlandırarak kalite, güvenlik, mimari ve metaveri yönetimiyle bütünleştirir (DAMA International, 2017).

Denetim açısından veri yönetişimi, kanıtın güvenilirliği ve tekrar üretilebilirliği için zorunludur. Denetçi bir bulguya ulaşırken hangi veri setini kullandığını, bu verinin hangi sistemden alındığını, hangi dönüşümlerden geçtiğini, hangi filtrelerin uygulandığını ve analizin hangi sürümle yapıldığını belgeleyebilmelidir (IAASB, 2020a; IAASB, 2020b). Bu gereklilik, özellikle yapay zekâ ve büyük veri analitiği kullanılan denetimlerde daha da önemlidir (NIST, 2023; Appelbaum vd., 2017: 1-27). Çünkü algoritmik analizler, denetim raporunda görünen basit sonuçların arkasında çok sayıda teknik tercih barındırır. IAASB'nin otomatik araç ve tekniklere ilişkin değerlendirmeleri, denetim prosedürünün amaca uygunluğu ile kullanılan verinin güvenilirliğinin birlikte belgelenmesi gerektiğini ortaya koyar (IAASB, 2020a; IAASB, 2020b).

Düzenleyici uyum riski de dijitalleşmeyle birlikte çok boyutlu hale gelmiştir (NIST, 2020; European Union, 2024). Kişisel verilerin korunması, siber olay bildirimi, finansal raporlama, yapay zekâ yönetişimi, sürdürülebilirlik raporlaması, bulut lokasyonu ve üçüncü taraf veri işleme gibi alanlar farklı düzenleyici rejimlerin kesişiminde yer alır (NIST, 2020; European Union, 2024; European Commission, 2026). Kurumlar, dijital dönüşüm projelerini yalnızca operasyonel verimlilik açısından değil, düzenleyici beklentilerin izlenebilirliği ve kanıtlanabilirliği açısından da tasarlamalıdır (OECD, 2021; NIST, 2020). OECD'nin veri erişimi ve paylaşımına ilişkin politika çerçeveleri, veriden değer üretimi ile güven, sorumluluk ve koruma mekanizmalarının birlikte düşünülmesi gerektiğini vurgular (OECD, 2021).

Bu noktada denetim fonksiyonunun katkısı, düzenleyici gereklilikleri kontrol listesine indirgemeden süreç tasarımıyla ilişkilendirmektir. Bir uyum kontrolü yalnızca "politika var mı?" sorusuyla sınırlı kalırsa, dijital risklerin gerçek etkisini yakalayamaz (ISACA, 2018; NIST, 2024a). Denetim, politikanın sistem yapılandırmasına, erişim akışına, veri saklama kuralına, tedarikçi sözleşmesine, model onay sürecine ve olay müdahale prosedürüne nasıl yansıdığını test etmelidir (IAASB, 2020a; ISACA, 2018). Bu yaklaşım, uyum denetimini statik belge incelemesinden çıkararak teknoloji mimarisi ve iş süreciyle bütünleştirir.

III. STRATEJİK RİSK YÖNETİMİNE GEÇİŞ

A. Strateji, Risk İştahı ve Performans

Dijital ortamda risk yönetiminin stratejiyle entegre edilmesi zorunludur. Geleneksel yaklaşımda risk yönetimi çoğu zaman gerçekleşmiş olayları değerlendiren, finansal ve uyum odaklı, silo bazlı bir fonksiyon olarak görülebilir. Oysa dijitalleşme, risklerin etkileşimini ve hızını artırır (NIST, 2024a; ISO, 2018). Bir siber olay operasyonel kesintiye, veri ihlaline, düzenleyici yaptırıma, itibar kaybına ve stratejik proje gecikmesine aynı anda yol açabilir (NIST, 2024a; BCBS, 2021). COSO'nun kurumsal risk yönetimi çerçevesi, riskin strateji ve performansla bütünleşmesini merkeze alır; risk yönetimini ayrı bir raporlama yükümlülüğü değil, karar alma ve değer yaratma sürecinin parçası olarak konumlandırır (COSO,

2017). Bu çalışmanın yorumu, dijital risklerin hızının ve bileşik etkisinin, risk yönetimini stratejinin sonradan kontrol edilen bir eki olmaktan çıkarıp strateji tasarımının parçası haline getirdiğidir.

Risk iştahı, bu dönüşümün temel araçlarından biridir (COSO, 2017; ISO, 2018). Dijital projelerde kurumların tüm riskleri sıfırlaması mümkün değildir; ancak hangi riskleri hangi sınırlar içinde kabul edeceğini, hangi risklerin stratejik hedefleri tehdit edeceğini ve hangi göstergelerin erken uyarı sayılacağını belirlemesi gerekir. Örneğin buluta geçiş stratejisi maliyet ve ölçeklenebilirlik avantajı sunabilir; fakat veri lokasyonu, üçüncü taraf bağımlılığı, erişim yönetimi ve hizmet sürekliliği risklerini artırabilir (NIST, 2024a; BCBS, 2021). Yapay zekâ kullanımı karar destek kapasitesini artırabilir; fakat açıklanabilirlik, model yanlılığı ve veri mahremiyeti risklerini doğurabilir (NIST, 2023; NIST, 2024b). Risk iştahı bu tercihleri görünür hale getirir ve yönetimin hangi risk-getiri dengesini kabul ettiğini açıklar. Bu nedenle risk iştahı, dijital dönüşümde yalnızca risk limitlerini değil, kurumun ne tür bir belirsizlik içinde değer üretmek istediğini de tanımlar.

Stratejik risk yönetimi, yalnızca risklerin listelenmesiyle değil, risk göstergelerinin performans göstergeleriyle ilişkilendirilmesiyle anlam kazanır (COSO, 2017; ISO, 2018). Kritik risk göstergeleri (KRI) ile kilit performans göstergeleri (KPI) birlikte izlenmediğinde, kurum kısa vadeli performans hedeflerine ulaşırken dayanıklılığını zayıflatabilir (COSO, 2017; BCBS, 2021). Örneğin dijital hizmet kanalının kullanım oranı artarken kimlik doğrulama hataları, sistem kesinti süreleri veya müşteri şikayetleri artıyorsa, performans başarısı risk birikimini maskeleyebilir (NIST, 2024a; COSO, 2017). ISO 31000, risk yönetiminin kurumun tüm faaliyetlerine entegre, yapılandırılmış, kapsayıcı, dinamik ve sürekli iyileşen bir süreç olması gerektiğini belirtir (ISO, 2018). Bu ilkeler dijital risk yönetimi için de geçerlidir.

Stratejiyle bütünleşik risk yönetimi, denetim fonksiyonunun raporlama dilini de değiştirir. Denetim raporu yalnızca kontrol eksikliği, bulgu derecesi ve öneri formatında kalmamalı; bulgunun hangi stratejik hedefi etkilediğini, hangi risk iştahı sınırını zorladığını ve hangi karar noktasında yönetim dikkatine sunulması gerektiğini göstermelidir. Bu yaklaşım, denetimin yönetime daha

fazla değer sunmasını sağlar. Denetim, geçmiş uyumsuzlukları tespit eden bir kontrol mekanizması olmaktan çıkarak, stratejik kararların risk sonuçlarını görünür kılan bir güvence fonksiyonuna dönüşür. Bu dönüşüm, makalenin savunduğu yeni nesil denetim anlayışının ana omurgasını oluşturur.

B. Entegre Risk Yönetimi, Üç Hat Modeli ve Teknoloji Yönetişimi

Entegre risk yönetimi, dijital risklerin farklı fonksiyonlar arasında dağılmasını önlemek için gereklidir. Siber güvenlik ekibi teknik zafiyetleri, hukuk birimi sözleşme ve mevzuat risklerini, veri yönetişimi ekibi veri kalitesini, iş birimleri süreç risklerini, iç denetim ise güvence ihtiyaçlarını takip edebilir (IIA, 2020; ISACA, 2018). Ancak bu fonksiyonlar ortak bir risk dili ve yönetişim mekanizmasıyla çalışmadığında, kurumun gerçek risk profili parçalı görünür (COSO, 2017; IIA, 2020). IIA'nın Üç Hat Modeli, yönetim, risk ve uyum fonksiyonları ile iç denetim arasındaki rolleri daha esnek ve yönetişim odaklı biçimde tanımlar; değer yaratma, koruma ve güvence sorumluluklarının açıklaştırılmasını amaçlar (IIA, 2020).

Dijitalleşen kurumlarda üç hat modeli statik bir organizasyon şemasından çok, sorumlulukların tasarlanması için kullanılmalıdır. Birinci hat olan iş birimleri dijital süreçlerin sahipliğini üstlenmeli, kontrolleri süreç içine yerleştirmeli ve risk göstergelerini günlük yönetim pratiğine dahil etmelidir (IIA, 2020; COSO, 2017). İkinci hat fonksiyonları, risk metodolojisi, siber güvenlik politikaları, uyum çerçeveleri, veri yönetişimi standartları ve teknoloji risk limitlerini belirlemelidir (IIA, 2020; NIST, 2024a). Üçüncü hat olan iç denetim ise bu yapıların tasarım ve işleyiş etkinliğine bağımsız güvence sağlamalıdır (IIA, 2020). Bu ayrım, denetimin teknoloji projelerine ya çok geç dahil olmasını ya da yönetim sorumluluğunu üstlenmesini önler.

Teknoloji yönetişimi, entegre risk yönetiminin uygulama zemini olarak görülebilir. ISACA COBIT çerçevesi, kurumsal bilgi ve teknolojinin yönetimi ile yönetişimini değer üretimi, risk optimizasyonu ve kaynak optimizasyonu hedefleriyle ilişkilendirir (ISACA, 2018). Bu yaklaşım, BT yatırımlarının yalnızca proje teslim

tarihi ve bütçe performansı üzerinden değil, kurumun stratejik hedeflerine katkısı, risk seviyesini düşürme kapasitesi, kontrol edilebilirliği ve sürdürülebilirliği üzerinden değerlendirilmesini gerektirir (ISACA, 2018). Dijital denetim fonksiyonu, teknoloji projelerinin iş gerekçesi, veri mimarisi, kontrol tasarımı, güvenlik gereksinimleri ve fayda realizasyonu arasındaki bağlantıyı test etmelidir.

Stratejik risk yönetimine geçişte yönetim kurulu ve üst yönetimin rolü belirleyicidir (COSO, 2017; ISO, 2018). Risk iştahı, teknoloji yatırımlarının önceliği, yapay zekâ kullanım sınırları, veri paylaşımı, üçüncü taraf kabul kriterleri ve kriz yönetimi sorumlulukları üst düzey karar gerektirir (COSO, 2017; NIST, 2023; BCBS, 2021). Bu kararlar net değilse, denetim bulguları tekrar eden teknik eksikliklere dönüşür; çünkü temel yönetişim boşluğu kapanmamıştır. Yeni nesil denetim yaklaşımı bu nedenle yalnızca kontrol sahiplerine değil, strateji ve yönetişim sahiplerine de hitap etmelidir. Denetim komitesi, risk komitesi ve üst yönetim, dijital risklerin stratejik etkilerini aynı raporlama dilinde görebilmelidir. Bu noktada denetimin değeri, bulgu sayısından çok yönetimin daha iyi karar almasını sağlayan risk anlatısını kurabilmesinde ortaya çıkar.

Bu raporlama dilinin etkili olabilmesi için bulguların finansal olmayan etkileri de görünür kılınmalıdır. Dijital riskler çoğu zaman hizmet kalitesi, vatandaş veya müşteri güveni, operasyonel itibar, regülasyon karşısındaki güvenilirlik ve çalışanların karar alma kapasitesi üzerinde etki yaratır (NIST, 2024a; BCBS, 2021). Bu etkiler parasal olarak hemen ölçülemese bile, stratejik öncelikler açısından kritik olabilir (COSO, 2017; ISO, 2018). Denetim fonksiyonu, bulgularını yalnızca yüksek, orta ve düşük risk derecelerine indirmek yerine, riskin hangi stratejik hedefi geciktirdiğini, hangi kritik süreci kırılgan hale getirdiğini ve hangi paydaş beklentisini zedelediğini açıklamalıdır.

IV. KURUMSAL DAYANIKLILIK VE DENETİMİN ROLÜ

A. Dayanıklılık Operasyonel Bir Yeterlilik Olarak

Kurumsal dayanıklılık, kurumun kesinti, kriz, siber olay, tedarikçi arızası, doğal afet, mevzuat şoku veya teknoloji hatası karşısında kritik hizmetlerini kabul edilebilir seviyede sürdürebilme ve olay

sonrası öğrenerek güçlenebilme kapasitesidir (BCBS, 2021; ISO, 2019). Bu kavram iş sürekliliği, operasyonel risk, kriz yönetimi, siber dayanıklılık, tedarik zinciri yönetimi ve kurumsal yönetişim disiplinlerinin kesişiminde yer alır (BCBS, 2021; ISO, 2019). Basel Komitesi'nin operasyonel dayanıklılık ilkeleri, kurumların kritik operasyonlarını tanımlamasını, etki toleranslarını belirlemesini, senaryolarla test etmesini ve üçüncü taraf bağımlılıklarını yönetmesini önermektedir (BCBS, 2021). ISO 22301 ise iş sürekliliği yönetim sistemleri için gereklilikleri ortaya koyar (ISO, 2019).

Dijitalleşme dayanıklılık ihtiyacını artırmıştır; çünkü birçok kurumun hizmet üretimi artık birbirine bağlı platformlara, dış servis sağlayıcılara, gerçek zamanlı veri akışlarına ve otomasyon kurallarına bağlıdır (NIST, 2024a; BCBS, 2021). Tek bir uygulama arızası, kimlik sağlayıcısı kesintisi, bulut bölgesi problemi ya da tedarikçi API hatası birden fazla iş sürecini durdurabilir (BCBS, 2021; ISO, 2019). Bu nedenle dayanıklılık yalnızca bilgi teknolojileri biriminin felaket kurtarma planı olarak görülemez (BCBS, 2021; ISO, 2019). Kurumun kritik süreçleri, karar alma zinciri, iletişim planı, alternatif çalışma senaryoları, veri kurtarma hedefleri ve müşteri/vatandaş hizmet yükümlülükleri birlikte tasarlanmalıdır (BCBS, 2021; ISO, 2019).

Dayanıklılık yaklaşımının zayıf olduğu kurumlarda süreklilik planları çoğu zaman "dekoratif" belgeye dönüşür. Planlar vardır; ancak gerçek risk profiline, güncel sistem mimarisine, üçüncü taraf bağımlılıklarına ve kriz anındaki karar hiyerarşisine uymaz. Testler düzenli yapılmadığında planların uygulanabilirliği bilinmez (BCBS, 2021; ISO, 2019). Test sonuçları süreçlere yansıtılmadığında ise kurum aynı zafiyetleri korur. Kurumsal dayanıklılık bu nedenle sürekli iyileştirme mantığı gerektirir (ISO, 2019). Kritik göstergeler, erken uyarı mekanizmaları, masa başı tatbikatlar, teknik kurtarma testleri, tedarikçi kesinti senaryoları ve olay sonrası öğrenme döngüleri bu yapının parçası olmalıdır (BCBS, 2021; ISO, 2019). Bu çalışma açısından dayanıklılık, planların varlığından çok bu planların kriz anında davranışa dönüşebilme kapasitesidir.

Dayanıklılık, kamu kurumları açısından ayrıca hesap verebilirlik ve hizmet sürekliliği boyutu taşır (INTOSAI, 2004; ISO, 2019). Kamu hizmetlerinin kesintiye uğraması yalnızca finansal kayıp

değil, vatandaş güveni, kamu düzeni ve temel haklara erişim üzerinde de etki yaratabilir (INTOSAI, 2004; BCBS, 2021). INTOSAI'nin kamu sektörü iç kontrol standartları, kontrol ortamı, risk değerlendirme, kontrol faaliyetleri, bilgi-iletişim ve izleme bileşenlerini kamu kaynaklarının etkili, ekonomik ve verimli kullanımıyla ilişkilendirir (INTOSAI, 2004). Dijital kamu hizmetlerinin yaygınlaştığı ortamda bu ilkeler teknoloji altyapısı, veri güvenilirliği ve hizmet sürekliliğiyle birlikte yorumlanmalıdır (INTOSAI, 2004; NIST, 2024a).

B. Denetim Perspektifinden Kritik Sorular

Denetim fonksiyonunun kurumsal dayanıklılığa katkısı, yalnızca süreklilik planının varlığını kontrol etmekle sınırlı olmamalıdır. Denetim, kurumun kritik süreçlerini gerçekten tanımlayıp tanımlamadığını, bu süreçler için kabul edilebilir kesinti süreleri ve veri kaybı toleransları belirleyip belirlemediğini, alternatif çalışma senaryolarını test edip etmediğini, üçüncü taraf bağımlılıklarını izleyip izlemediğini ve kriz anındaki karar mekanizmasını netleştirip netleştirmediğini sorgulamalıdır (BCBS, 2021; ISO, 2019). Bu sorular, denetimin "kontrol var mı?" yaklaşımından "kriz altında sürdürülebilirlik sağlanabilir mi?" yaklaşımına geçmesini sağlar. Bu ayrım, makalenin denetim odağına ilişkin en önemli önerilerinden biridir.

Kritik süreçlerin tanımlanması, dayanıklılık denetiminin başlangıç noktasıdır. Kurumun tüm süreçleri aynı önemde değildir; bazı süreçler hizmet sürekliliği, mevzuat yükümlülüğü, finansal raporlama veya güvenlik açısından daha kritiktir (BCBS, 2021). Bu süreçler belirlenmeden süreklilik kaynakları doğru önceliklendirilemez (BCBS, 2021; ISO, 2019). Denetim, kritik süreç listesinin güncel strateji, hizmet portföyü, dijital kanal kullanımı ve dış bağımlılıklarla uyumunu test etmelidir (IIA, 2020; BCBS, 2021). Ayrıca bu süreçlerin sahipleri, sistem bağımlılıkları, veri girdileri, üçüncü taraf bağlantıları ve manuel alternatifleri açıkça belgelenmelidir (ISO, 2019; BCBS, 2021).

Kesinti senaryolarının test edilmesi, planların gerçekçiliğini ortaya çıkarır. Masa başı tatbikatlar, kriz kararlarını ve iletişim akışını; teknik kurtarma testleri, sistemlerin geri dönüş kapasitesini;

tedarikçi senaryoları, dış bağımlılıkların etkisini; siber olay tatbikatları ise güvenlik ve operasyon ekipleri arasındaki koordinasyonu test eder (BCBS, 2021; NIST, 2024a). Denetim, testlerin yalnızca yapılıp yapılmadığını değil, test kapsamını, başarısızlık noktalarını, iyileştirme aksiyonlarını ve üst yönetim raporlamasını değerlendirmelidir (IIA, 2020; BCBS, 2021). Dayanıklılık olgunluğu, plan dokümanlarının sayısıyla değil, testlerden öğrenme ve aksiyonları kapatma disiplininin gücüyle ölçülür.

Üçüncü taraf izleme ve teknoloji bağımlılığı analizi de dayanıklılık denetiminin kritik alanlarıdır. Kurumlar birçok hizmeti dış sağlayıcılar üzerinden yürüttüğünde, kendi süreklilik kapasitesi tedarikçinin dayanıklılığına bağlı hale gelir (BCBS, 2021; NIST, 2024a). Sözleşmelerde olay bildirimi, denetim hakkı, veri erişimi, alt yüklenici kullanımı, hizmet seviyesi, kurtarma hedefleri ve çıkış planı hükümleri bulunmadığında kurum kriz anında kontrol gücünü kaybedebilir (BCBS, 2021; ISO, 2019). Denetim, üçüncü taraf risk yönetimini yalnızca satın alma veya sözleşme uygunluğu olarak değil, operasyonel dayanıklılık ve veri güvenliği açısından değerlendirmelidir.

V. YENİ NESİL DENETİM YAKLAŞIMI

A. Denetimde Yapay Zekâ ve İnsan Muhakemesi

Yapay zekâ denetimi yalnızca hızlandırmaz; doğru tasarlandığında daha derin analiz, daha anlamlı örüntü keşfi ve daha güçlü karar destek bilgisi sağlayabilir (Fedyk vd., 2022: 938-985; NIST, 2023). Anomali tespiti, belge sınıflandırma, doğal dil işleme, sözleşme inceleme, işlem kümeleme, risk puanlama ve sürekli kontrol izleme gibi alanlarda yapay zekâ araçları denetçinin çalışma kapasitesini artırır (Fedyk vd., 2022: 938-985; IAASB, 2020b). Ancak bu artış, denetçinin yerini alan bir otomasyon anlayışıyla değil, denetçinin muhakemesini güçlendiren bir yardımcı sistem anlayışıyla ele alınmalıdır. Fedyk vd. (2022: 938-985), yapay zekânın denetim süreçlerinde verimlilik ve kalite potansiyeli taşıdığını gösterirken, bu etkinin insan uzmanlığı ve kurumsal uygulama kalitesiyle ilişkili olduğunu ortaya koymaktadır. Bu nedenle makalenin yaklaşımı, yapay zekâyı denetçinin ikamesi değil, denetçinin soru

sorma, istisna seçme ve bulgu yorumlama kapasitesini genişleten bir yardımcı katman olarak ele almaktadır.

Yapay zekâ destekli denetimlerde açıklanabilirlik kritik bir ilkedir (NIST, 2023; NIST, 2024b). Denetçi, bir modelin neden belirli işlemleri riskli gördüğünü, hangi değişkenlerin sonucu etkilediğini ve modelin hangi sınırlara sahip olduğunu anlayamazsa, model çıktısını güvenilir denetim kanıtı olarak kullanmak zorlaşır (NIST, 2023; IAASB, 2020b). Açıklanabilirlik yalnızca teknik şeffaflık değildir; denetim raporunun yönetim ve denetim komitesi tarafından anlaşılabilir olmasını da sağlar (NIST, 2023; IIA, 2020). NIST AI RMF ve üretken yapay zekâ profili, yapay zekâ sistemlerinde güvenilirlik, emniyet, güvenlik, mahremiyet, açıklanabilirlik ve hesap verebilirlik gibi boyutların birlikte yönetilmesini önerir (NIST, 2023; NIST, 2024b). İnsan muhakemesi özellikle üç alanda vazgeçilmezdir. Birincisi, denetim hedefinin ve risk hipotezinin doğru kurulmasıdır; yanlış soru soran bir model doğru cevap üretse bile denetim değerini düşürür. İkincisi, model çıktılarının bağlamsal yorumudur; istisna olarak görünen bir işlem yasal, operasyonel veya mevsimsel nedenlerle makul olabilir. Üçüncüsü, etik ve yönetişim değerlendirmesidir; bir analitik test teknik olarak mümkün olsa bile mahremiyet, ayrımcılık veya çalışan güveni açısından uygun olmayabilir (NIST, 2020; NIST, 2023). Bu nedenle yapay zekâ destekli denetim, otomasyon ile mesleki şüpheciliğin dengelendiği bir çalışma modeli gerektirir. Bu çalışma, denetçinin değerini algoritmanın ürettiği cevaptan çok hangi sorunun sorulacağına ve cevabın hangi bağlamda anlamlı olduğuna karar verme kapasitesinde görmektedir.

Denetim fonksiyonlarının yapay zekâdan değer üretmesi için veri, süreç ve yetkinlik olgunluğu gerekir. Dağınık veri kaynakları, tutarsız kodlama, zayıf metaveri, yetersiz erişim kontrolü ve belirsiz süreç sahipliği olan kurumlarda yapay zekâ denetimi beklenen sonucu üretmez (DAMA International, 2017; NIST, 2023). Ayrıca denetim ekiplerinin yalnızca aracı kullanması değil, aracın sınırlamalarını, hata türlerini, eğitim verisi etkilerini ve güvence ihtiyacını anlaması gerekir (NIST, 2023; IAASB, 2020b). Bu nedenle yapay zekâ yatırımları, denetim metodolojisi, kalite güvence programı, veri yönetişimi ve eğitim planıyla birlikte tasarlanmalıdır.

B. Sürekli Denetim, Büyük Veri ve Analitik Güvence

Sürekli denetim, dijital ortamın doğal tamamlayıcısıdır (Vasarhelyi vd., 2004: 1-21; Alles vd., 2008: 64-80). Kurumlar işlemlerini gerçek zamanlı platformlarda yürütürken denetimin yalnızca yıl sonu veya dönemsel kapanış sonrasında güvence üretmesi yeterli olmayabilir (Vasarhelyi vd., 2004: 1-21; Appelbaum vd., 2017: 1-27). Sürekli denetim yaklaşımı, kritik kontrollerin, işlem örüntülerinin ve risk göstergelerinin düzenli ve otomatik olarak izlenmesini sağlar (Alles vd., 2008: 64-80; IAASB, 2020b). Bu model, denetçiyi işlem sonrası hata bulma rolünden çıkararak risk sinyallerini zamanında yorumlayan bir yönetişim aktörüne dönüştürür (Vasarhelyi vd., 2004: 1-21; IIA, 2020). Vasarhelyi vd. (2004: 1-21), analitik izleme ve sürekli güvence yaklaşımının denetim zamanlamasını ve kapsamını dönüştürdüğünü vurgular.

Büyük veri denetimde yalnızca hacim artışı anlamına gelmez (Appelbaum vd., 2017: 1-27; Cao vd., 2015: 423-429). Verinin çeşitliliği, hızı, doğruluğu ve iş bağlamı önemlidir (DAMA International, 2017; Appelbaum vd., 2017: 1-27). Yapılandırılmış finansal veriler, yapılandırılmamış metinler, çağrı merkezi kayıtları, sistem logları, sensör verileri, e-posta akışları ve dış veri kaynakları birlikte analiz edildiğinde daha zengin risk sinyalleri üretilebilir (Appelbaum vd., 2017: 1-27; Cao vd., 2015: 423-429). Ancak bu çeşitlilik, veri hazırlama, sınıflandırma, kalite kontrol, mahremiyet ve yorumlama zorluklarını artırır (DAMA International, 2017; NIST, 2020). Appelbaum vd. (2017: 1-27), büyük veri ve analitiğin modern denetimde araştırma ve uygulama ihtiyacını artırdığını; Cao vd. (2015: 423-429) ise finansal tablo denetimlerinde büyük veri analitiğinin kanıt değerlendirmesini değiştirebileceğini belirtmektedir.

Analitik güvence yaklaşımında denetim metodolojisinin açık olması gerekir (IAASB, 2020a; IAASB, 2020b). Hangi veri kaynakları kullanıldı, hangi istisna kuralları uygulandı, eşikler nasıl belirlendi, hatalı pozitif ve hatalı negatif sonuçlar nasıl yönetildi, model performansı nasıl izlendi ve bulgular iş birimleriyle nasıl doğrulandı? Bu sorular yanıtlanmadan analitik çıktılar denetim raporunda güçlü bir kanıt haline gelemez (IAASB, 2020b; NIST, 2023). Denetim kalitesi, aracın teknik karmaşıklığından çok,

metodolojinin şeffaflığı ve sonuçların tekrarlanabilirliğiyle ilgilidir. Bu nedenle denetim ekipleri analitik çalışma kağıtlarını, veri soy ağacını ve model varsayımlarını düzenli biçimde belgelemelidir (DAMA International, 2017; IAASB, 2020b). Yazarın burada vurguladığı nokta, analitik denetimin "kara kutu" bir uzmanlık alanına dönüşmemesi; denetlenebilir, açıklanabilir ve tekrar üretilebilir bir mesleki yöntem olarak kurulmasıdır.

Sürekli denetim uygulamalarının başarısı, yönetimle denetim arasındaki sınırın doğru kurulmasına da bağlıdır (IIA, 2020; Alles vd., 2008: 64-80). Sürekli izleme araçlarını yönetim kullanır; sürekli denetim ise bu izleme sistemlerinin tasarım ve işleyişine güvence sağlar (Alles vd., 2008: 64-80; IIA, 2020). İç denetim yönetimin kontrol sorumluluğunu üstlenirse bağımsızlığı zayıflar; hiç dahil olmazsa da dijital risklerin erken aşamada yönetilmesine katkı veremez (IIA, 2020). Bu denge, üç hat modeli, denetim komitesi gözetimi ve açık rol tanımlarıyla kurulmalıdır (IIA, 2020).

C. Teknoloji Güvencesi ve ESG Güvencesi

Teknoloji güvencesi, dijital dönüşüm projelerinin güvenilir, kontrol edilebilir ve kurumsal hedeflerle uyumlu olup olmadığını değerlendiren bir güvence alanıdır (ISACA, 2018; IIA, 2020). Bu yaklaşım, analitik çözümlerin nerede kullanıldığını, işe etkisinin ve risklerinin ne olduğunu, yapay zekâ ve veri analitiği kaynaklı risklerin nasıl yönetildiğini, yönetişim sorumluluklarının tanımlanıp tanımlanmadığını ve çıktılarının denetlenebilir olup olmadığını sorgular (ISACA, 2018; NIST, 2023). Denetim fonksiyonu, teknoloji güvencesiyle dijital dönüşümün hızını yavaşlatmayı değil, güvenli ve sürdürülebilir biçimde değer üretmesini sağlamayı hedeflemelidir.

Teknoloji güvencesi özellikle yapay zekâ kullanımında önemlidir (NIST, 2023; European Union, 2024). Bir kurumun yapay zekâ model envanteri yoksa, veri kaynakları belirsizse, model onay süreci tanımlanmamışsa, performans izleme yapılmıyorsa ve model çıktılarının hangi kararları etkilediği bilinmiyorsa, yapay zekâ kullanımı kurumsal risk haline gelir (NIST, 2023; NIST, 2024b). Denetim, yapay zekâ kullanımını yalnızca algoritmanın doğruluğuyla sınırlı görmemeli; yönetişim, veri kalitesi, etik,

mahremiyet, siber güvenlik, insan gözetimi ve olay müdahalesi boyutlarını birlikte incelemelidir (NIST, 2023; European Union, 2024). Bu yaklaşım, düzenleyici beklentilerin artmasıyla daha da önemli hale gelmektedir (European Union, 2024; NIST, 2023).

ESG ve sürdürülebilirlik güvencesi de teknolojiyle giderek daha fazla bütünleşmektedir (IAASB, 2024; European Commission, 2026). Sürdürülebilirlik raporlaması, yalnızca metin beyanlarından oluşan gönüllü bir açıklama alanı olmaktan çıkıp veri yoğun, kontrol gerektiren ve denetlenebilir süreçlere dayalı bir raporlama alanına dönüşmektedir (IFRS Foundation, 2023a; IFRS Foundation, 2023b; European Commission, 2026). IFRS S1 ve IFRS S2 sürdürülebilirlikle ilgili finansal bilgilerin ve iklimle ilgili açıklamaların yatırımcı odaklı raporlama çerçevesini güçlendirmiştir (IFRS Foundation, 2023a; IFRS Foundation, 2023b). Avrupa Birliği Kurumsal Sürdürülebilirlik Raporlama Direktifi ise sürdürülebilirlik raporlamasının kapsamını ve güvence ihtiyacını genişletmiştir (European Commission, 2026). IAASB tarafından yayımlanan ISSA 5000, sürdürülebilirlik güvence denetimleri için genel gereklilikleri ortaya koyarak bu alandaki güvence ihtiyacının uluslararası standartlaşmasına katkı sağlar (IAASB, 2024). Bu gelişmeler denetim fonksiyonu açısından önemli sonuçlar doğurur. ESG verileri çoğu zaman farklı sistemlerden, tedarikçilerden, manuel girişlerden ve tahmin modellerinden gelir (IFRS Foundation, 2023a; IAASB, 2024). Enerji tüketimi, emisyon verisi, tedarik zinciri bilgisi, insan kaynakları göstergeleri ve sosyal etki metrikleri finansal raporlama verileri kadar olgun kontrol ortamına sahip olmayabilir (IFRS Foundation, 2023b; IAASB, 2024). Bu nedenle teknoloji destekli ESG güvencesi, veri soy ağacı, hesaplama metodolojisi, sistem kontrolleri ve yönetim beyanlarının tutarlılığını birlikte test etmelidir (IAASB, 2024; DAMA International, 2017).

Yeni nesil denetim yaklaşımı, yapay zekâ, sürekli denetim, büyük veri, teknoloji güvencesi ve ESG güvencesini ayrı projeler olarak değil, tek bir güvence mimarisinin bileşenleri olarak görmelidir. Bu mimaride denetim planı stratejik risklerle başlar, veri ve teknoloji ortamını değerlendirir, kritik süreçlere odaklanır, sürekli izleme sinyallerini kullanır ve yönetim için karar destek değeri üretir (COSO, 2017; IIA, 2020; Vasarhelyi vd., 2004: 1-21). Böyle bir

modelde denetim raporu yalnızca geçmiş uyumsuzlukları değil, kurumun gelecekteki dayanıklılık ve güvenilirlik kapasitesini de görünür kılar. Makalenin özgün çerçevesi, bu farklı güvence alanlarını tek bir "stratejik güvenilirlik" problemi altında bir araya getirmesidir.

Bu mimarinin uygulanması aşamalı bir olgunlaşma gerektirir. İlk aşamada denetim evreni dijital süreçler, veri varlıkları, kritik sistemler, yapay zekâ kullanımları ve üçüncü taraf bağımlılıklarını kapsayacak şekilde güncellenmelidir. İkinci aşamada veri kalitesi ve erişim kontrolleri güvence altına alınmalı, tekrar kullanılabilir analitik testler geliştirilmelidir (DAMA International, 2017; IAASB, 2020b). Üçüncü aşamada sürekli denetim göstergeleri risk iştahı ve stratejik hedeflerle ilişkilendirilmelidir (COSO, 2017; Vasarhelyi vd., 2004: 1-21). Son aşamada ise teknoloji, ESG, siber güvenlik ve operasyonel dayanıklılık bulguları tek bir yönetim raporlaması içinde bütünleştirilmelidir. Böylece denetim fonksiyonu dijital dönüşümü dışarıdan izleyen değil, güvenilir dönüşüm için gerekli geri bildirim döngüsünü kuran bir aktör olur. Bu aşamalı yaklaşım, makalenin uygulamaya dönük öneri setini oluşturmaktadır.

SONUÇ VE ÖNERİLER

Bu çalışma, dijitalleşen denetim ortamında stratejik risk yönetimi, kurumsal dayanıklılık ve yeni nesil denetim yaklaşımını bütünleşik bir çerçevede ele almaktadır. Dijitalleşme, denetimin yalnızca kullanılan araçlarını değil, denetim kanıtının niteliğini, risklerin oluşma hızını, kontrol ortamının sınırlarını ve denetçinin kurumsal yönetişim içindeki rolünü dönüştürmektedir. Geleneksel denetim yaklaşımı, belirli dönemlerde seçilen örneklemlere ve geçmişe dönük analizlere dayanırken; dijital ve sürekli denetim yaklaşımı daha geniş veri evrenlerinin incelenmesini, risk göstergelerinin gerçek zamana yakın izlenmesini ve uçtan uca süreç görünürlüğünü mümkün kılmaktadır. Ancak bu olanaklar, veri kalitesi, sistem güvenilirliği, siber güvenlik, model açıklanabilirliği ve insan muhakemesiyle desteklenmediğinde güvenilir güvence üretmek için yeterli değildir.

Çalışmanın ilk sonucu, dijital denetimin teknik bir modernizasyon projesi olarak değil, kurumsal yönetişim meselesi olarak görülmesi

gerektiğidir. Büyük veri, yapay zekâ, otomatik kontrol testleri ve sürekli izleme araçları denetim fonksiyonuna hız ve kapsam kazandırabilir. Buna karşılık veri kaynağının güvenilirliği, veri soy ağacı, erişim kontrolü, algoritmik kararların açıklanabilirliği ve analitik metodolojinin tekrarlanabilirliği güvence kalitesinin temel koşullarıdır. Denetçinin rolü, araç çıktısını raporlamakla sınırlı değildir; denetçi, çıktının iş bağlamını, risk anlamını ve kontrol etkisini yorumlamak zorundadır.

İkinci sonuç, dijital ortamda yeni nesil risklerin birbirinden bağımsız yönetilemeyeceğidir. Siber güvenlik, kimlik yönetimi, veri ihlali, gölge yapay zekâ, üçüncü taraf bağımlılığı, veri kalitesi ve düzenleyici uyum riskleri çoğu zaman aynı süreç içinde kesişir. Bu nedenle risk yönetimi, finansal ve uyum odaklı silo yaklaşımından çıkarak strateji, performans ve teknoloji yönetişimiyle bütünleşmelidir. Risk iştahı, kritik risk göstergeleri ve performans göstergeleri birlikte ele alınmadığında, kurumlar kısa vadeli dijital verimlilik kazanımları elde ederken uzun vadeli dayanıklılıklarını zayıflatabilir.

Üçüncü sonuç, kurumsal dayanıklılığın yalnızca bilgi teknolojileri sürekliliği olarak değerlendirilemeyeceğidir. Kritik süreçlerin tanımlanması, kabul edilebilir kesinti sürelerinin belirlenmesi, alternatif çalışma senaryolarının test edilmesi, üçüncü tarafların izlenmesi, kriz karar hiyerarşisinin netleştirilmesi ve test sonuçlarına göre sürekli iyileştirme yapılması tüm kurumun sorumluluğudur. Denetim fonksiyonu bu alanda planların varlığını değil, kriz altında sürdürülebilirlik kapasitesini değerlendirmelidir.

Son olarak çalışma, yeni nesil denetim yaklaşımının yapay zekâ, sürekli denetim, büyük veri analitiği, teknoloji güvencesi ve ESG güvencesini tek bir güvence mimarisinde birleştirmesi gerektiğini savunmaktadır. Bu mimaride insan muhakemesi otomasyonun yerine geçmez; otomasyon insan muhakemesini güçlendirir. Denetim fonksiyonu stratejik riskleri anlayan, dijital süreçlerin kontrol mantığını değerlendiren, kurumsal dayanıklılığı sorgulayan ve yönetim için güvenilir içgörü üreten bir yönetişim aktörü haline gelmelidir. Bu dönüşümün başarısı, kurumun veri yönetişimi olgunluğu, risk kültürü, teknoloji yönetişimi ve denetim metodolojisinin açıklığına bağlıdır.

Bu kapsamda çalışma, uygulayıcılar için dört öncelikli eylem alanı önermektedir. İlk olarak kurumlar dijital denetim evrenlerini güncellemeli ve kritik sistemler, veri varlıkları, yapay zekâ kullanımları, dış servis sağlayıcılar ve ESG veri süreçlerini aynı risk haritasında göstermelidir. İkinci olarak denetim fonksiyonları, veri analitiği kullanımını kişisel beceri düzeyinden kurumsal metodoloji düzeyine taşımalıdır; bunun için standart veri talep süreçleri, onaylı analitik testler, kalite kontrolleri ve tekrar üretilebilir çalışma kağıtları gereklidir. Üçüncü olarak üst yönetim, risk iştahını dijital stratejiyle açık biçimde ilişkilendirmeli ve kritik risk göstergelerini performans göstergeleriyle birlikte izlemelidir. Dördüncü olarak dayanıklılık denetimleri, planların varlığını değil, test edilmiş senaryolar, kapatılmış aksiyonlar ve kriz anındaki karar kapasitesini esas almalıdır.

Çalışmanın özgün katkısı, denetimde dijitalleşmeyi yalnızca araç ve verimlilik meselesi olarak değil, strateji, risk, dayanıklılık ve güvence mimarisi meselesi olarak konumlandırmasıdır. Bu bakış açısı, denetim fonksiyonunun gelecekteki rolünü daha geniş bir kurumsal yönetişim sorumluluğu içinde değerlendirmeyi mümkün kılar. Kurumlar için temel mesele, daha fazla veri toplamak veya daha fazla otomasyon kullanmak değildir; asıl mesele, bu teknolojileri güvenilir karar alma, hesap verebilirlik ve sürdürülebilir değer üretimi için kontrol edilebilir bir yapıya kavuşturmaktır.

Dijitalleşen denetim ortamında başarı, teknoloji araçlarının sayısıyla değil, bu araçların strateji, risk iştahı, veri yönetişimi ve kurumsal dayanıklılık hedefleriyle ne kadar tutarlı biçimde kullanıldığıyla ölçülmelidir. Bu ölçüt, kurumların güvenilir dönüşüm kapasitesini de görünür kılar.

Dijitalleşen denetim ortamı, denetim fonksiyonuna hem önemli fırsatlar hem de yeni sorumluluklar getirmektedir. Veri analiz kapasitesinin artması, örneklem sınırlamalarının azalması, sürekli denetim uygulamaları, yapay zekâ destekli analizler ve teknoloji güvencesi, denetimin kapsamını ve etkisini güçlendirebilir. Ancak bu fırsatlar, veri kalitesi, siber güvenlik, model riski, üçüncü taraf bağımlılığı, düzenleyici uyum ve etik yönetişim sorunları çözülmeden sürdürülebilir güvenceye dönüşmez. Dijital denetim,

yalnızca daha fazla araç kullanmak değil, güvence mantığını dijital süreçlerin gerçek risk profilini kapsayacak şekilde yeniden tasarlamaktır.

Çalışmanın temel sonucu, risk yönetiminin stratejiyle entegre edilmesi gerektiğidir. Dijital riskler finansal, operasyonel, teknolojik ve itibari etkileri aynı anda üretebildiğinden, silo bazlı risk değerlendirmesi yetersiz kalır. Kurumlar risk iştahını dijital stratejiyle ilişkilendirmeli, kritik risk göstergelerini performans göstergeleriyle birlikte izlemeli, üç hat modelindeki sorumlulukları netleştirmeli ve teknoloji yönetişimini kurumsal yönetişimin ayrılmaz parçası olarak ele almalıdır. Denetim fonksiyonu da bulgularını stratejik hedefler, risk iştahı sınırları ve paydaş değeriyle ilişkilendiren bir raporlama diline geçmelidir.

Kurumsal dayanıklılık, bu yeni yaklaşımın merkezinde yer almalıdır. Dijital hizmetlerin sürekliliği, bulut ve tedarikçi bağımlılıkları, siber olaylar ve veri güvenilirliği, kurumların yalnızca teknik altyapısını değil, karar alma ve kriz yönetimi kapasitesini de sınar. Denetim fonksiyonu kritik süreçlerin tanımlanması, kesinti senaryolarının test edilmesi, üçüncü tarafların izlenmesi, IT bağımlılıklarının analiz edilmesi ve kriz karar mekanizmalarının netleştirilmesi konularında güvence sağlamalıdır. Bu güvence, kontrol listelerinin ötesine geçerek kriz altında sürdürülebilirlik sorusuna odaklanmalıdır.

Bu yaklaşımın hayata geçirilmesi için denetim planlarının yıllık statik dokümanlar olarak değil, risk profilindeki değişime göre güncellenen yaşayan belgeler olarak ele alınması gerekir. Yeni bir bulut geçişi, kritik tedarikçi değişikliği, yapay zekâ projesi, sürdürülebilirlik raporlama yükümlülüğü veya siber olay sonrası ortaya çıkan bulgular denetim evrenine hızlı biçimde yansıtılmalıdır. Böylece denetim fonksiyonu yalnızca geçmiş yıl risklerine göre hareket eden bir yapı olmaktan çıkar; kurumun dijital dönüşüm hızına uyum sağlayan daha çevik ve stratejik bir güvence kapasitesi kazanır.

Yeni nesil denetim için beş öneri öne çıkmaktadır. Birincisi, denetim planlaması dijital strateji, risk iştahı ve kurumsal dayanıklılık hedefleriyle birlikte yapılmalıdır. İkincisi, veri yönetişimi denetim

metodolojisinin temel bileşeni haline getirilmeli; veri kaynağı, veri soy ağacı, kalite kuralları ve erişim kontrolleri açıkça test edilmelidir. Üçüncüsü, yapay zekâ kullanımı açıklanabilirlik, insan gözetimi, model performansı, etik ve mahremiyet ilkeleriyle birlikte denetlenmelidir. Dördüncüsü, sürekli denetim ve analitik güvence uygulamalarında metodoloji, eşikler, hata oranları ve bulgu doğrulama süreçleri belgelendirilmelidir. Beşincisi, ESG ve teknoloji güvencesi alanları finansal ve operasyonel denetim planlarıyla bütünleştirilmelidir.

Sonuç olarak dijitalleşen denetim ortamında denetçinin rolü daralmamakta, aksine genişlemektedir. Denetçi, teknoloji araçlarını kullanan bir veri analisti olmanın ötesinde; stratejik riskleri anlayan, dijital süreçlerin kontrol mantığını değerlendiren, kurumsal dayanıklılığı sorgulayan ve yönetim için güvenilir içgörü üreten bir yönetişim aktörüne dönüşmektedir. Bu dönüşümün başarısı, teknoloji yatırımlarından çok, kurumun risk kültürü, veri yönetişimi, denetim metodolojisi ve insan muhakemesiyle otomasyonu dengeli biçimde birleştirme kapasitesine bağlıdır.

KAYNAKÇA

Alles, M. G., Kogan, A. ve Vasarhelyi, M. A. (2008). Continuous monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemens. International Journal of Accounting Information Systems, 9(2), 64-80. https://doi.org/10.1016/j.accinf.2007.11.004

Appelbaum, D., Kogan, A. ve Vasarhelyi, M. A. (2017). Big data and analytics in the modern audit engagement: Research needs. Auditing: A Journal of Practice & Theory, 36(4), 1-27. https://doi.org/10.2308/ajpt-51684

Basel Committee on Banking Supervision (BCBS). (2021). Principles for operational resilience. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.htm, Erişim: 06.07.2026.

Cao, M., Chychyla, R. ve Stewart, T. (2015). Big data analytics in financial statement audits. Accounting Horizons, 29(2), 423-429. https://doi.org/10.2308/acch-51068

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). Enterprise risk management: Integrating with strategy and performance. COSO. https://www.coso.org/erm-framework, Erişim: 06.07.2026.

DAMA International. (2017). DAMA-DMBOK: Data management body of knowledge (2. Baskı). Technics Publications.

European Commission. (2026). Corporate sustainability reporting. https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company- reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en, Erişim: 10.07.2026.

European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. Official Journal of the European Union. https://eur- lex.europa.eu/eli/reg/2024/1689/oj, Erişim: 07.07.2026.

Fedyk, A., Hodson, J., Khimich, N. ve Fedyk, T. (2022). Is artificial intelligence improving the audit process? Review of Accounting Studies, 27, 938-985. https://doi.org/10.1007/s11142-022-09697-x

IFRS Foundation. (2023a). IFRS S1 General requirements for disclosure of sustainability- related financial information. IFRS Foundation. https://www.ifrs.org/issued-standards/ifrs- sustainability-standards-navigator/ifrs-s1-general-requirements/, Erişim: 08.07.2026.

IFRS Foundation. (2023b). IFRS S2 Climate-related disclosures. IFRS Foundation. https://www.ifrs.org/issued-standards/ifrs-sustainability-standards-navigator/ifrs-s2- climate-related-disclosures/, Erişim: 08.07.2026.

Institute of Internal Auditors (IIA). (2020). The IIA's three lines model: An update of the Three Lines of Defense. The Institute of Internal Auditors. https://www.theiia.org/en/content/position-papers/2020/the-iias-three-lines-model-an- update-of-the-three-lines-of-defense/, Erişim: 07.07.2026.

International Auditing and Assurance Standards Board (IAASB). (2020a). The use of automated tools and techniques when identifying and assessing risks of material misstatement in accordance with ISA 315 (Revised 2019). IAASB. https://www.iaasb.org/publications/use-automated-tools-and-techniques-when-identifying-and-assessing-risks-material-misstatement, Erişim: 08.07.2026.

International Auditing and Assurance Standards Board (IAASB). (2020b). The use of automated tools and techniques in performing audit procedures. IAASB. https://www.iaasb.org/publications/use-automated-tools-techniques-performing-audit- procedures, Erişim: 08.07.2026.

International Auditing and Assurance Standards Board (IAASB). (2024). International Standard on Sustainability Assurance 5000: General requirements for sustainability assurance engagements. IAASB. https://www.iaasb.org/publications/international- standard-sustainability-assurance-5000-general-requirements-sustainability-assurance, Erişim: 09.07.2026.

International Organization for Standardization (ISO). (2018). ISO 31000:2018 Risk management - Guidelines. ISO. https://www.iso.org/standard/65694.html, Erişim: 06.07.2026.

International Organization for Standardization (ISO). (2019). ISO 22301:2019 Security and resilience - Business continuity management systems - Requirements. ISO. https://www.iso.org/standard/75106.html, Erişim: 07.07.2026.

International Organization of Supreme Audit Institutions (INTOSAI). (2004). Guidelines for internal control standards for the public sector. INTOSAI. https://www.intosai.org/fileadmin/downloads/documents/open_access/intosai_guidance/i ssai_1000_to_2999/

INTOSAI_GOV_9100_E.pdf, Erişim: 07.07.2026.

ISACA. (2018). COBIT 2019 framework: Governance and management objectives. ISACA.

McKinsey & Company. (2025). The state of AI: How organizations are rewiring to capture value. McKinsey & Company. https://www.mckinsey.com/capabilities/quantumblack/our- insights/the-state-of-ai, Erişim: 09.07.2026.

National Institute of Standards and Technology (NIST). (2020). NIST Privacy Framework: A tool for improving privacy through enterprise risk management, Version 1.0. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.01162020, Erişim: 06.07.2026.

National Institute of Standards and Technology (NIST). (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1, Erişim: 07.07.2026.

National Institute of Standards and Technology (NIST). (2024a). The NIST Cybersecurity Framework (CSF) 2.0. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29, Erişim: 07.07.2026.

National Institute of Standards and Technology (NIST). (2024b). Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.600-1, Erişim: 09.07.2026.

Organisation for Economic Co-operation and Development (OECD). (2021). Recommendation of the Council on enhancing access to and sharing of data. OECD/LEGAL/0463. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463, Erişim:

08.07.2026.

Vasarhelyi, M. A., Alles, M. G. ve Kogan, A. (2004). Principles of analytic monitoring for continuous assurance. Journal of Emerging Technologies in Accounting, 1(1), 1-21. https://doi.org/10.2308/jeta.2004.1.1.1

Verizon. (2026). 2026 Data Breach Investigations Report. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/, Erişim: 10.07.2026.

DİJİTAL EKOSİSTEMDE SAYIŞTAYLARIN DÖNÜŞEN ROLLERİ: GELENEKSEL DENETİM ANLAYIŞININ ÖTESİNE GEÇİŞİN KAVRAMSAL VE PRATİK ÇERÇEVESİ

İhsan ÇULHACI
BT Denetimi Grup Başkanı
T.C. Sayıştay Başkanlığı

ÖZET

Dijitalleşme ve beraberinde getirdiği dönüşüm, kamu yönetiminin işleyişini derinden etkilemekte; kamu hizmetlerinin sunumunu, kamu kaynaklarının yönetimini ve bunlar üzerindeki denetim mekanizmalarını köklü biçimde değiştirmektedir. Bu çalışma, söz konusu dönüşümün Sayıştaylar için açtığı yeni katma değer alanlarını ele almaktadır. Odak noktası, dijitalleşmenin sağladığı imkânların denetim süreçlerinde araç olarak kullanılması değil; yaşanan dönüşüm ortamında kamu yönetiminin sağlıklı bir çerçevede ilerletilmesi, iyi yönetişime katkı sağlanması ve muhtemel risklerin öngörülerek yapıcı öneriler getirilmesi bağlamında Sayıştayların üstlenebileceği proaktif rollerdir. Dijital devlet, veri, yapay zekâ, dijital egemenlik, siber güvenlik, hukuk ve finansal teknolojiler eksenlerinde yürütülen analizin bulguları, Sayıştayların geleneksel "harcama odaklı" denetim anlayışının ötesine geçen; kamu kesiminin bütününe dışarıdan bakan, öngören, rehberlik eden ve örnek olan bir aktör rolüne kavuşabileceğini; kamu genelinde eşgüdümü teşvik etmede benzersiz bir konuma sahip olduğunu ortaya koymaktadır. Çalışmada bu dönüşümün kavramsal çerçevesi çizilmiş, uluslararası Sayıştay pratiklerinden somut örneklerle

desteklenmiş ve Sayıştayların dijital ekosistemde yaratabilecekleri özgün katma değerin parametreleri tanımlanmıştır.

Anahtar Kelimeler: Yüksek Denetim Kurumları, Dijital Dönüşüm, Kamu Denetimi, Dijital Egemenlik, Yapay Zekâ Denetimi

ABSTRACT

Digitalisation and its accompanying transformation profoundly affect public administration, fundamentally altering the delivery of public services, the management of public resources, and the oversight mechanisms governing them. This article examines the new value-creation opportunities that this transformation opens up for Supreme Audit Institutions (SAIs). The focus is not on leveraging digital capabilities as tools in audit processes, but rather on the proactive roles SAIs can assume in ensuring that public governance advances on sound foundations, contributing to good governance, and anticipating potential risks while offering constructive recommendations. Analysis across the dimensions of digital government, data, artificial intelligence, digital sovereignty, cybersecurity, law, and financial technologies reveals that SAIs can move well beyond the traditional "expenditure-focused" audit paradigm, evolving into proactive actors that look at the public sector as a whole from an independent external vantage point -foreseeing, guiding, and setting an example- and that are uniquely positioned to foster the whole-of-government coordination that digital transformation requires. The article outlines the conceptual framework of this transformation, supports it with concrete examples from international SAI practices, and defines the parameters of the distinct value SAIs can create within the digital ecosystem.

Keywords: Supreme Audit Institutions, Digital Transformation, Public Audit, Digital Sovereignty, Artificial Intelligence Audit

GİRİŞ

İçinde bulunduğumuz dönem, kamu yönetimi açısından köklü bir paradigma dönüşümünü temsil etmektedir. Dijitalleşme; geniş bir yelpazede, devletin vatandaşla ilişkisini, kurumların birbirleriyle etkileşimini, kamunun politikalarının bileşimini ve kamu kaynaklarının yönetimini temelden dönüştürmektedir. Bu dönüşümün somut tezahürleri günlük kamu yönetimi pratiğinde açıkça görülmektedir: vatandaşlar artık kamu hizmetlerinin büyük bölümüne dijital kapılar üzerinden erişmekte, kamu kurumları kararlarını giderek artan ölçüde büyük veriye ve veri analitiğine dayandırmakta; yapay zekâ destekli sistemler, vergi denetiminden sosyal yardım yönetimine uzanan geniş bir alanda kamu idarelerinin işleyişine dahil olmaktadır. Bu dönüşüm bir yandan büyük fırsatlar sunarken bir yandan da üzerinde titizlikle durulması gereken yeni ve özgün konuları beraberinde getirmektedir: silolar halinde tutulan verinin yönetişimi, büyük ölçekli BT projelerine harcanan kaynakların etkin kullanımı, yapay zekâ sistemlerinin kullandığı algoritmaların adil ve tarafsız olması ve kritik kamu altyapılarının güvenliği, dijitalleşmenin yönetilmesi gereken yüzünü oluşturmaktadır.

Tüm bu gelişmeler, kamu denetimini de doğrudan ilgilendirmektedir. Bütçe hakkının tarihsel bekçileri olarak kurulan Sayıştaylar, bugün yalnızca geçmiş işlemleri denetlemekle değil, kamu kesiminin dijital dönüşümünün sağlıklı bir zemine oturmasını güvence altına almak gibi yeni ve zorlu bir misyonla da yüz yüzedir. Dünyada yüksek denetim kurumları üzerine yapılan çalışmalar, bu kurumların geleneksel "bekçi köpek" (watchdog) rolünden giderek "rehber köpek" (guidedog) rolüne evrildiğini göstermektedir (Lagos, 2026; Pollitt ve Summa, 1997). Bu evrim, denetimi salt bir geriye dönük inceleme işlevi olmaktan çıkarmakta; kamusal değer yaratan, iyi yönetişimi pekiştiren ve geleceğe yönelik öngörü sunan proaktif bir işleve dönüştürmektedir (INTOSAI-P 12, 2019; Köse ve Polat, 2021).

Bu dönüşümün Sayıştaylar için taşıdığı önem, yalnızca akademik bir merak konusu değildir. Kamu kurumlarının dijital dönüşüme ayırdığı kaynakların hacmi her geçen yıl artmakta; yapay zekâ, veri yönetişimi ve siber güvenlik gibi alanlardaki kamu yatırımları, geleneksel kamu yönetimi harcama kalemleriyle kıyaslanamayacak

bir hızla büyümektedir (Damar vd., 2024; Asiloğulları Ayan, 2026). Bu büyüme, denetimin de aynı hızla ve aynı derinlikte bu alanlara nüfuz etmesini zorunlu kılmaktadır. Aksi hâlde, kamu kaynaklarının önemli bir bölümü bağımsız bir gözün erişemediği bir alanda harcanmaya devam edecek; bu durum hem hesap verebilirlik hem de kamu güveni açısından giderek büyüyen bir açık yaratacaktır.

Bu çalışma, söz konusu dönüşüm bağlamında Sayıştayların üstlenebileceği yeni rolleri, öncü Sayıştay uygulamalarında somutlaşan uluslararası örnekler üzerinden ele almaktadır. Önemle vurgulanmalıdır ki çalışmanın odak noktası, dijitalleşmenin sunduğu araçların denetim süreçlerinde nasıl kullanılabileceği değildir; bu başlı başına ayrı ve kapsamlı bir inceleme konusudur. Araştırmanın temel sorusu şudur: Yaşanan dönüşüm ortamında Sayıştaylar, kamu yönetiminin sağlıklı bir çerçevede ilerlemesine nasıl katkı sunabilir, iyi yönetişimi nasıl güçlendirebilir, riskleri öngörerek yapıcı öneriler nasıl getirebilir? Bu soruyu yanıtlamak amacıyla çalışma; dijital devlet, veri, yapay zekâ, dijital egemenlik, siber güvenlik, hukuk ve finansal teknolojiler eksenlerini sistematik biçimde incelemekte; her eksen için Sayıştayların özgün katma değerini tartışmakta ve bu tartışmayı uluslararası Sayıştay pratiklerinden somut örneklerle beslemektedir.

Çalışmanın yapısı şu şekildedir: Birinci bölüm, Sayıştayların tarihsel evrimini ve güncel kavramsal çerçeveyi ele almaktadır. İkinci bölüm, dijital ekosistemin temel bileşenlerini ve Sayıştayların bu bileşenler karşısındaki rollerini irdelemektedir. Üçüncü bölüm, tüm bu analizleri bütünleşik bir çerçevede sentezlemektedir. Çalışma, sonuç bölümüyle tamamlanmaktadır.

I. KURAMSAL VE TARİHSEL ÇERÇEVE

A. Sayıştayların Doğuşu ve Geleneksel Misyon

Tarihsel kökleri itibarıyla bütçe hakkının güvencesi olarak doğan ve parlamentoların yürütme organı üzerindeki denetim yetkisini kullanmasının somut aracı olan Sayıştaylar, geleneksel olarak, kamu gelirlerinin toplanmasında ve harcamaların yapılmasında bütçe kanununa uygun şekilde hareket edilip edilmediğini ve kamu

hesaplarının doğru tutulup tutulmadığını denetlemiştir. Türk kamu yönetimi geleneğinde Sayıştay, 1862 yılında kuruluşundan bu yana bu misyonu üstlenmiş; yargı yetkisiyle donatılmış, özgün yapısıyla hesap yargısı işlevini de üstlenmiştir (Akyel, 2016).

Sayıştayın denetim kapsamı, kamu yönetiminin karmaşıklaşmasına ve genişlemesine paralel olarak tarihsel süreç içinde genişlemiştir. 1967 yılında yürürlüğe giren ve kimi değişikliklerle yaklaşık kırk üç yıl yürürlükte kalan 832 sayılı Sayıştay Kanunu döneminde, kurumun denetim alanının ve yetkilerinin çeşitli düzenlemelerle kademeli olarak genişletildiği görülmektedir (Ergen ve Durak, 2020). 2010 yılında kabul edilen 6085 sayılı Sayıştay Kanunu ise hem denetim kapsamını daha da genişletmiş hem de kuruma Türkiye Büyük Millet Meclisi'ne düzenli raporlama yapma görevini yüklemiştir. Raporlama görevinin kurumsallaşması, Sayıştayın hesapları kesin hükme bağlayan bir yargı mercii olmanın ötesine geçip, bulgularını kamuoyu ve yasama organıyla düzenli biçimde paylaşan şeffaf bir kurum kimliğine büründüğünü göstermektedir. Bu tarihsel örüntü, Sayıştayın sabit bir denetim alanıyla ve anlayışıyla sınırlı kalmadığını; kamu yönetiminde ortaya çıkan yeni kurumsal yapılar ve yeni işlevler karşısında kapsamını ve araçlarını sürekli yeniden tanımlayan dinamik bir kurum olduğunu göstermektedir. Bu çalışmada ele alınan veri, yapay zekâ, dijital egemenlik ve siber güvenlik gibi dijital ekosistem bileşenleri, Sayıştayın denetim kapsamındaki genişlemenin en güncel halkasını oluşturmaktadır.

Uluslararası alanda ise Sayıştayların bağımsızlığı ve temel görevleri, 1977 Lima Deklarasyonu ile belirlenmiştir. Uluslararası Yüksek Denetim Kurumları Teşkilatı INTOSAI'nin kurucu belgesi niteliğindeki bu deklarasyon (INTOSAI-P 1), bağımsız dış denetimi demokratik yönetimin vazgeçilmez bir unsuru olarak konumlandırmaktadır. Bağımsızlık, yalnızca kurumsal bir ayrıcalık değil; denetim bulgularının güvenilirliğinin ve toplumsal meşruiyetin ön koşuludur. Deklarasyon, Sayıştayların yürütme organından bağımsız biçimde faaliyet göstermesini, denetim programını özgürce belirleyebilmesini ve bulgularını kamuoyuyla serbestçe paylaşabilmesini güvence altına almıştır (INTOSAI-P 1, 2019).

Geleneksel denetim anlayışı içinde Sayıştaylar üç temel işlev üstlenmiştir: mali denetim, uygunluk denetimi ve performans denetimi. Mali denetimde, kamu hesaplarının gerçek durumu doğru olarak yansıtıp yansıtmadığı; uygunluk denetiminde, harcama ve işlemlerin ilgili mevzuata uygunluğu; performans denetiminde ise kamu kaynaklarının ekonomiklik, verimlilik ve etkililik ilkeleri çerçevesinde kullanılıp kullanılmadığı sorgulanmaktadır. Bu üçlü yapı, onlarca yıl boyunca Sayıştayların denetim gündemini belirlemiştir (Köse, 2007; Akyel ve Köse, 2010).

B. Geleneksel Anlayışın Sınırları ve Dönüşümün Zorunluluğu

Yirminci yüzyılın son çeyreğinden itibaren kamu yönetimi anlayışında yaşanan köklü dönüşümler -Yeni Kamu İşletmeciliğinden (New Public Management) Yeni Kamu Yönetişimine (New Public Governance) uzanan paradigma değişiklikleri (Uzun, 2024; Önder, 2023)- Sayıştayların işlevlerine ilişkin beklentileri de etkilemiştir. Bir yanda hesap verebilirlik ve şeffaflık talebi artarken, öte yanda kamu kurumlarının performansını ve yarattıkları toplumsal değeri ölçme ihtiyacı güçlenmektedir (Otia ve Bracci, 2022; Şaşmaz ve Özen, 2026). Bu bağlamda yalnızca "para nereye harcandı?" sorusunu soran bir denetim anlayışı yetersiz kalmaya başlamış; "harcanan para gerçekten değer yarattı mı?" sorusu denetimin odağına yerleşmiştir.

Bu dönüşümü en net biçimde ortaya koyan akademik değerlendirmelerden biri, Sayıştayların "bekçi köpek" (watchdog) rolünden "rehber köpek" (guidedog) rolüne evrilmesi olgusudur (Lagos, 2026). Pollitt ve Summa'nın (1997) öncü çalışmasında temelleri atılan bu kavramsal ayrım, günümüzde daha da belirginleşmiştir: geleneksel denetim anlayışı, hataları tespit edip raporlamakla yetinen reaktif bir yapıyı tanımlarken; yeni denetim anlayışı, riskleri oluşmadan önce gören, kamu yönetimine stratejik içgörüler sunan ve politika yapıcılara yol gösteren proaktif bir kurumu ön plana çıkarmaktadır.

INTOSAI'nin bu dönüşümü en açık biçimde tescil ettiği belge, INTOSAI-P 12: "Yüksek Denetim Kurumlarının Değer ve Faydaları - Vatandaşların Yaşamında Fark Yaratma" başlıklı ilke belgesidir. Bu belge, Sayıştayların misyonunu üç temel eksen etrafında

tanımlamaktadır: (i) merkezi yönetim ve kamu kurumlarının hesap verme sorumluluğunu, şeffaflığını ve doğruluğunu güçlendirmek; (ii) vatandaşlar, parlamento ve diğer paydaşlarla ilgili olma durumunun sürdüğünü göstermek; (iii) davranışlarıyla örnek teşkil ederek model bir kuruluş olmak (INTOSAI-P 12, 2019). Özellikle üçüncü eksen, Sayıştayların kendi kurumsal davranışlarıyla kamu sektörünün bütününe model oluşturma sorumluluğunu vurgulamaktadır. Bu çerçeve, Sayıştayların yalnızca geçmişin hesabını soran değil, gelecekteki kamu yönetiminin kalitesini yükselten kurumlar olduğunu açıkça ilan etmektedir.

Öte yandan, teknolojinin denetime sunduğu imkânlar, bahse konu dönüşümü gerçekleştirme ihtimalini güçlendiren bir etken niteliği taşımaktadır. Blok zinciri, makine öğrenmesi ve yapay zekâ temelli teknolojiler, denetimin büyük veri analizine, gelişmiş prosedürlere ve risk değerlendirmelerine dayalı olarak yürütülmesini mümkün kılarak sonuçların isabetini ve güvenilirliğini artırmaktadır (Köse, 2023). Veri hacminin, çeşitliliğinin ve üretim hızının sürekli artması, büyük verinin etkin biçimde analiz edilmesini birçok sektörde olduğu gibi denetimde de verimlilik ve etkinliğin ön koşulu haline getirmiştir; bu doğrultuda toplanan ve anlamlandırılan verilerden elde edilecek çıktıların değer katma potansiyeli yüksektir. Yakın gelecekte denetimin, algoritmaların hesap verebilirliği gibi ileri teknolojilere dayalı sistemlerin güvenilirliğini konu alan yeni işlevler üstlenmesi beklenmektedir (Köse, 2023). Bu beklenti, Sayıştayların, ilerleyen bölümlerde ele alınan Veri ve Yapay Zekâ eksenlerindeki rollerinin kavramsal zeminini de oluşturmaktadır.

C. Gözetim, İçgörü ve Öngörü: Üç Boyutlu Bir Çerçeve

Günümüzde Sayıştayların işlevini kavramsallaştırmanın en işlevsel yollarından biri, gözetim (oversight), içgörü (insight) ve öngörü (foresight) eksenlerinde üç boyutlu bir çerçeve kurmaktır (OECD, 2016). Bu üçlü yapı, Sayıştayların denetim faaliyetinin derinliğini ve kapsamını bütünsel olarak görmemizi sağlamaktadır.

Gözetim boyutu, Sayıştayların geleneksel çekirdeğini oluşturmaktadır: kamu kaynaklarının yasal çerçeve ve bütçe kanunları uyarınca kullanılıp kullanılmadığının bağımsız bir gözle denetlenmesi. İçgörü boyutu, denetim bulgularının yalnızca

uyumsuzlukları kayıt altına almakla kalmayıp, kamu yönetimindeki sistemik sorunları, yapısal zayıflıkları ve iyileştirme alanlarını derinlemesine analiz etmesini gerektirir. Öngörü boyutu ise en ileri adımı temsil eder: denetim faaliyetinin yalnızca geçmişe ve bugüne değil, geleceğe de yönelmesi; riskleri önceden belirlemesi, politika yapıcılara erken uyarılar iletmesi ve kamu kurumlarının sağlıklı bir gelecek inşa etmesine katkı sunması (Köse ve Polat, 2021).

Bu üçlü çerçeve, OECD'nin ABD, Brezilya, Fransa, Güney Afrika, Güney Kore, Hollanda, Kanada, Polonya, Portekiz ve Şili Sayıştaylarını kapsayan 2016 tarihli raporunda kavramsallaştırılmış ve "iyi yönetişime katkı sunan bir Sayıştay modeli" olarak uluslararası düzeyde bilinirlik kazanmıştır (OECD, 2016). Burada, bahse konu çerçevenin yalnızca akademik bir kurgu ya da soyut bir kavramsallaştırma olmadığını belirtmek yerinde olacaktır: ABD Sayıştayı (GAO), bu çerçeveyi kendi kurumsal kimliğinin merkezine yerleştirmiş; kongreye sunduğu hizmeti 2007 yılında bu üç kavramla -gözetim, içgörü ve öngörü- tanımlamaya başlamış (GAO, 2007), 2021 yılındaki yüzüncü kuruluş yıldönümü etkinliklerinde de bu üç boyutun kurumun geleceği açısından taşıdığı önemi vurgulamıştır (GAO, 2021a).

Bu üç boyutun tek bir denetim faaliyeti içinde nasıl bir arada işleyebileceğini büyük ölçekli bir kamu bilişim projesinin denetimi üzerinden somutlaştırmak, çerçevenin soyut kalmasını önlemek açısından faydalı olacaktır: gözetim boyutu, projeye ayrılan kaynağın bütçe mevzuatına uygun kullanılıp kullanılmadığını sorgularken; içgörü boyutu, projenin ilerleyişini teknik ve idari açıdan derinlemesine inceleyerek altyapı kısıtları, kurumlar arası eşgüdüm eksiklikleri veya risk yönetimi zafiyetleri gibi yapısal sorunları ortaya çıkarmakta; öngörü boyutu ise bu bulgulardan hareketle projenin başarısızlıkla sonuçlanma riskini daha proje tamamlanmadan tespit ederek karar vericileri zamanında uyarmakta ve gerekli durumlarda projenin sürdürülebilirliği için stratejik çözüm önerileri sunmaktadır. İlerleyen bölümlerde ele alınacak olan Smart-eID vakası, üç boyutun bir arada işletilmesi sayesinde önemli bir kamu kaynağı kaybının önlenebileceğini göstermesi bakımından öğreticidir.

Dijitalleşme, bu üç boyutun eş zamanlı olarak ele alınabileceği bir derinliğe sahiptir. Kamu kurumlarının dijital dönüşüm süreçleri, yapay zekâya yaptıkları yatırımlar, veri yönetişim yapıları ve siber güvenlik kapasiteleri; hem gözetim (mevzuata uyum sağlanmış mı?), hem içgörü (sistemler amaçlandığı şekilde çalışıyor ve beklenen fayda sağlanıyor mu?) hem de öngörü (hangi riskler ufukta görünüyor?) perspektifi ile sorulan soruların odağına girmektedir. Bu nedenle dijitalleşme ve beraberinde getirdiği dönüşüm, Sayıştaylar için yalnızca kritik öneme sahip yeni bir denetim konusu değil, toplumsal değer yaratma kapasitesini sınayan ve genişleten bir dönüşüm fırsatıdır. Bu bağlamda, çalışmanın ikinci bölümünde ele alınan dijital devlet, veri, yapay zekâ, dijital egemenlik, siber güvenlik, hukuk ve finansal teknolojiler eksenlerinin her biri, bu üç boyutun somut uygulama alanları olarak okunabilir: her eksende Sayıştayların üstlenebileceği rol, ilgili alandaki mevzuata uyumun gözetimi, mevcut uygulamaların işlerliğine dair içgörü üretimi ve gelecekteki risklerin öngörülmesi sorularının bir bileşimidir.

II. DİJİTAL EKOSİSTEMİN BİLEŞENLERİ VE SAYIŞTAYLARIN ROLLERİ

A. Dijital Devlet: Aktarım mı, Dönüşüm mü?

Kamu hizmetlerinin dijitalleşmesi, onlarca yıldır hükümetler tarafından açıklanan stratejik hedeflerin odağında yer almaktadır. Bu süreçte yinelenen bir örüntü dikkat çekmektedir: hükümetler her yeni dönemde yenilikçi dijital dönüşüm stratejilerini açıklarken pratikte mevcut süreçlerin dijital ortama aktarılmasıyla yetinmektedir. Birleşik Krallık Sayıştayı (NAO), 1996'dan 2024'e uzanan yaklaşık otuz yıllık dönemi kapsayan tarihsel analizinde, "eski sistemlerin modernize edilmesi" ve "bütünleşik veri yönetimi" gibi hedeflerin hükümetlerin dijital stratejilerinde tekrar tekrar yer aldığını belgeleyen çarpıcı bir tablo ortaya koymuştur. Bu tablo, dijital dönüşümün söylemde ne kadar kolay, pratikte ne kadar zorlu olduğunun açık göstergesidir (NAO, 2024).

Ülkeler arasındaki performans farkları bu zorlu durumu somutlaştırmaktadır. 33 ülkenin karşılaştırmalı olarak değerlendirildiği OECD 2023 Dijital Devlet Endeksi'nde Güney Kore 0,935 puanla listenin zirvesinde yer alırken, OECD ortalamasının

0,605'te kaldığı görülmektedir (OECD, 2024). Ancak endeksin asıl dikkat çekici bulgusu, ülke sıralaması değildir: OECD, hükümetlerin dijital dönüşüm yatırımlarına ilişkin yönetişim düzenlemelerinin, yetki ve gözetim mekanizmalarının güçlendirilmesi gerektiğini özellikle vurgulamaktadır (OECD, 2024). Bu bulgu, doğrudan Sayıştaylara atıfta bulunmasa da, dijital dönüşüm yönetişiminde bağımsız bir dış gözün oynayabileceği role dair önemli bir bağlam sunmaktadır. Kamu kurumlarının kendi iç yönetişim yapıları kadar, bu yapıları dışarıdan değerlendirebilecek bağımsız bir denetim mekanizmasının varlığı da dijital dönüşümün sağlıklı ilerlemesi açısından belirleyici olmaktadır.

Bu tabloyu kavramsal olarak açıklamaya yardımcı olan üç yapısal sorun öne çıkmaktadır: ön-yüz odaklılık, silo tipi düşünce yapısı ve dış kaynak bağımlılığı. Ön-yüz odaklılık; süreçleri iyileştirerek dönüştürmek yerine mevcut uygulamayı dijital ortama olduğu gibi aktarmayı ifade eder. Silo tipi düşünce yapısı; birbirleriyle konuşmayan ve bütçesel açıdan dağınık sistemlerin varlığını sürdürmesine -kimi durumlarda ise bu nitelikte sistemlerin ortaya çıkmasına- yol açmaktadır. Dış kaynak bağımlılığı ise projelerde geçici olarak çalıştırılan kurum dışı danışmanlara aşırı güven ve teslimiyeti, dolayısıyla kurumsal dijital hafıza ile yetkinliğin kaybını beraberinde getirir. Almanya Sayıştayı (Bundesrechnungshof - BRH) tarafından hazırlanan raporlar, bu üç sorunu sistematik biçimde belgeleyen zengin bulgular sunmaktadır: federal kurumların paralel / birbirinin ikamesi sistemler ve yazılımlar geliştirmesi (BRH bu durumu "vahşi büyüme" olarak adlandırmaktadır), dijitalleşmenin arka plandaki süreçlere değil yalnızca kullanıcıların karşısına çıkan arayüzlere uygulanması ve milyarlarca avroluk BT yatırımlarının vadedilen verimliliği sağlayamaması (BRH, 2025a; BRH, 2024).

Bu bağlamda Sayıştayların temel sorusu, "harcama odaklı" değil, "etki odaklı" bir bakışla, şunlar olmalıdır: Kurumlar ve işler gerçekten daha verimli hale geldi mi? Vatandaşın hayatı somut olarak kolaylaştı mı? BRH, bu soruyu yanıtlamak için "dijital temettü" kavramını denetim çerçevesinin merkezine taşımıştır. Dijital temettü, tasarım ve mevzuat hazırlığı aşamasında harcanan her ek çalışma saatinin, uygulama aşamasında gerçek bir zaman ve maliyet tasarrufu yaratıp yaratmadığını sorgular (BRH, 2025b).

Bu kavram, Sayıştayın salt harcama denetimi yapan bir kuruluş değil, kamu yatırımlarının toplumsal getirisini ölçen stratejik bir aktör olduğunu açıkça ortaya koymaktadır. BRH'nin bu çerçevede geliştirdiği ve yasama sürecine proaktif katılım sağlayan bir diğer özgün araç olan Digitalcheck uygulaması ise çalışmanın Siber Güvenlik ve Hukuk başlıkları altında ele alınmaktadır.

Sayıştayların değer üretebileceği alanlar bu örneklerle sınırlı değildir: ekonomik fizibilite çalışması yapılmadan başlatılan kamu bilişim projelerini tespit edip parlamento ve hükümeti zamanlı şekilde uyarmak, kurumlar arası eşgüdümü sağlayacak mekanizmalar önermek ve kamu kurumlarını harici bağımlılıktan kurtaracak iç yetkinlik stratejileri için öneriler geliştirmek de Sayıştayların katkı sunabileceği kritik alanlardır.

Almanya'da yürütülen Smart-eID Projesi bu konuda ders çıkarılabilecek önemli bir vaka sunmaktadır. Ekonomik fizibilite analizi yapılmadan başlatılan, risk yönetimi ihmal edilen ve teknik kısıtları baştan öngörülemeyen bu proje, 90 milyon avroyu aşan bir kamu kaynağı harcanmasının ardından 2024 yılında durdurulmak zorunda kalınmıştır. BRH, projenin başarısızlık riskini 2021 yılında tespit etmiş ve uyarmış; ancak yürütme organı gerekli önlemleri zamanında almamıştır (BRH, 2025c). Bu vaka, Sayıştay uyarılarının ciddiye alındığında kamu zararını önleyebileceğinin açık bir göstergesidir.

Sayıştaylar bu alanda özgün metodolojiler de geliştirmektedir. İsviçre Sayıştayı'nın (SFAO) geliştirdiği DigiTrans modeli; dijital dönüşüm projelerini uçtan uca süreç verimliliği perspektifiyle ele almakta ve müşteri, strateji, teknoloji, operasyon ile organizasyon ve kültür olmak üzere beş boyutta tanımlanmış 19 kriter üzerinden kurumların dijital yetkinliklerini ve risklerini bütüncül biçimde değerlendirmektedir (SFAO, 2023).

B. Veri: Yeni Para Birimi

"Veri, dijital çağda karar almanın yeni para birimidir." Kaynağını Avrupa Komisyonu Tüketici Komiseri Meglena Kuneva'nın 2009 yılında dile getirdiği "kişisel veri, internetin yeni petrolü ve dijital dünyanın yeni para birimidir" sözünden alan ve Dünya Ekonomik

Forumu'nun kişisel veriyi yeni bir ekonomik varlık sınıfı olarak tanımlayan raporuyla yaygınlaşan bu yaklaşım (WEF, 2011), kamu yönetiminde yaşanan köklü bir dönüşümü özetlemektedir: kararlar artık sezgi ya da deneyimden değil, büyük veri setlerinin analizinden beslenmektedir. "Veri odaklı devlet" vizyonu, kamu hizmetlerinin tasarımından politika değerlendirmesine, kaynak planlamasından performans ölçümüne kadar geniş bir alanda kamu kurumlarının veri üretme, saklama, paylaşma ve analiz etme kapasitesini belirleyici bir yetkinlik olarak öne çıkarmaktadır (OECD, 2022; Kahyaoğlu vd., 2026).

Ancak bu vizyonun hayata geçirilmesinin önünde ciddi güçlükler bulunmaktadır. Kamu kurumlarında verinin; eksik, tutarsız, erişilmesi güç ve paylaşılması sorunlu biçimde tutulduğu sıklıkla belgelenmektedir. NAO'nun tespitlerine göre birçok kamu kurumunda veriler silolar halinde yönetilmekte, sistemler birbiriyle konuşamamaktadır; bu durum hem verimliliği zedelemekte hem de bütünleşik kamu hizmetlerinin sunumunu güçleştirmektedir (NAO, 2024). Dijital Devlet başlığı altında değinilen OECD endeksine göre, ülkeler bu alanda orta düzey bir olgunluk bandında seyretmektedir ve veriye dayalı yönetim kapasitesinin geliştirilmesinde önemli bir potansiyel henüz değerlendirilememektedir (OECD, 2024).

Sayıştayların bu tablodaki özgün rolü iki boyutta ele alınabilir. Birinci boyut, verinin doğruluğuna ve güvenilirliğine ilişkin bağımsız güvence sağlamaktır. Kamu kararları giderek daha fazla veriye dayandığında, bu verinin bağımsız bir gözle doğrulanması demokratik hesap verebilirlik açısından zorunlu hale gelmektedir. Açık kamu verisinin kalitesi, kamu kurumlarının performans göstergelerinin güvenilirliği ve algoritmik karar sistemlerinin dayandığı veri tabanlarının tamlığı ve doğruluğu; Sayıştayların etki odaklı değerlendirme süreçlerine doğrudan giren konulardır. Bunun somut bir örneği, GAO'nun bir raporunda görülmektedir. GAO, 2024 tarihli söz konusu denetiminde; 2019-2023 yılları arasında gerçekleşen 335 sözleşme feshinin ve 52 idari anlaşmanın başka kaynaklarda raporlanmasına rağmen, federal kurumlar tarafından potansiyel yüklenicilerin geçmiş performans ve dürüstlük kayıtlarını değerlendirmek için başvurulan resmi veri tabanına hiç işlenmediğini tespit etmiştir. Bu durum, ihale

kararlarına doğrudan esas teşkil eden resmî bir kamu veri tabanının dahi önemli ölçüde eksik kalabildiğini ve bu tür eksikliklerin çoğunlukla ancak bağımsız bir denetim mekanizmasıyla gün yüzüne çıkarılabildiğini göstermektedir (GAO, 2024b). İkinci boyut ise kurumlar arası eşgüdüm işlevidir. Kamu kesiminin bütününe yönelik denetim yetkisine sahip olan Sayıştaylar, farklı kurumların veri yönetim pratiklerini karşılaştırabilmekte, normalizasyon ve standartlaştırma süreçlerini değerlendirebilmekte ve silolardan kurtarılmış bütünleşik veri yönetimini teşvik edebilmektedir (Akyel ve Köse, 2010).

Veri etiği boyutu da bu alanda giderek önem kazanmaktadır. Kamu kurumlarının topladığı verilerin kamu yararına kullanılıp kullanılmadığı, kişisel veri mahremiyetinin korunup korunmadığı ve yapay zekâ sistemlerini besleyen kamu verilerinin mülkiyetinin kim tarafından nasıl kullanıldığı; Sayıştayların gündemine girmeye başlayan sorulardır. Nitekim, Avustralya Sayıştayı'nın (ANAO) yayımladığı raporlarda, veri koruma mevzuatına uyumun kâğıt üzerinde kaldığına ve kurumların veri etiği çerçevelerini yeterince hayata geçiremediğine dair tespitlere yer verilmektedir (ANAO, 2025).

Açık devlet verisinin kalitesi ve erişilebilirliği, bu tartışmanın bir başka boyutunu oluşturmaktadır. Yakın dönem araştırmalar, açık devlet verisi uygulamalarının yolsuzlukla mücadele ve demokratik hesap verebilirlik üzerinde olumlu bir etki yaratabildiğini, ancak bu etkinin verinin gerçek anlamda erişilebilir, güncel ve kullanılabilir olmasına bağlı olduğunu ortaya koymaktadır (Koçdemir ve Atan, 2026). Bu tespit, Sayıştayların yalnızca verinin varlığını değil, niteliğini de denetlemesi gerektiğine işaret etmektedir.

C. Yapay Zekâ: Harcama, Yönetişim ve İlkeler

Yapay zekâ (YZ), kamu sektöründe hızla yaygınlaşmaktadır. OECD'nin 2024 tarihli raporuna göre hükümetler, kamu hizmetlerinin tasarımından iç operasyonlara, vergi denetiminden sosyal yardım yönetimine kadar uzanan geniş bir alanda YZ uygulamalarını hayata geçirmektedir. Kurumlar bu konuda büyük bir hevesle hareket etmektedir; çok sayıda YZ projesi başlatılmakta ve yüksek miktarda kamu kaynağı bu alanda harcanmaktadır (OECD, 2024a; Ateş, 2025).

Peki harcanan para gerçekten değer yaratıyor mu? Bu soru, Sayıştaylar için öncelikli bir denetim gündemine dönüşmektedir. YZ kullanımı gerçekten gerekli mi? Amaçlar ve çıktılar somut biçimde belirlenmiş mi? Kaynak ve zaman planlaması yapılmış mı? Sayıştayların denetim bulgularına bakıldığında, bu temel proje yönetişim sorularının yanıtlarının çoğunlukla hayal kırıklığı yarattığı görülmektedir. ANAO'nun 2025 tarihli Avustralya Vergi Dairesi denetiminde, kurumun otomasyon ve YZ stratejisi için uygulama düzenlemelerinin kurulmadığı, kurumsal roller ve sorumlulukların tanımlanmadığı, YZ'ye özgü risk yönetimi mekanizmalarının oluşturulmadığı tespit edilmiştir (ANAO, 2025). NAO'nun 2024 tarihli raporunda ise ankete katılan hükümet kuruluşlarının yüzde 70'inin YZ kullanımına geçtiği ya da bunu planladığı; ancak açık hesap verebilirlik ve yönetişim mekanizmalarının kurulmasında ciddi eksiklikler bulunduğu belgelenmiştir (NAO, 2024a).

Sayıştayların bu alandaki denetim sorumluluğu, harcamaların değer yaratıp yaratmadığının sorgulanmasıyla sınırlı kalmamaktadır. Kamu kurumları tarafından kullanılan YZ sistemlerinin etik ve hesap verebilirlik boyutları, Sayıştayların gündemine giderek daha fazla girmektedir. Bu boyut üç temel soruyla özetlenebilir: Sistem şeffaf mı - YZ'nin nasıl çalıştığı, hangi faktörleri dikkate aldığı ve kararlarını nasıl verdiği açıklanabilir mi? Adil mi - YZ algoritması ayrımcılık yapıyor mu, önyargı içeriyor mu? Güvenli mi - veri mahremiyeti korunuyor mu, üretilen verinin mülkiyetinin kime ait olduğu belirlenmiş mi? Kamu kurumlarının sosyal yardım, vergi cezası veya istihdam gibi -Avrupa Birliği Yapay Zekâ Yasası'nın "yüksek riskli" olarak sınıflandırdığı- alanlarda kullandığı YZ sistemlerinde insan gözetiminin fiilen sağlanıp sağlanmadığı ise ayrıca sorgulanması gereken kritik bir unsurdur (Avrupa Parlamentosu ve Konseyi, 2024).

Bu son sorunun -insan gözetiminin fiilen var olup olmadığının- ne denli kritik olduğunu, Hollanda'da yaşanan çocuk bakım yardımı skandalı çarpıcı biçimde göstermektedir. Hollanda Vergi ve Gümrük İdaresi'nin sahtecilik tespiti amacıyla kullandığı risk skorlama algoritması, sonuçları anlamlı bir insan incelemesine tabi tutulmadığı için on binlerce aileyi haksız yere sahtecilikle suçlamış; bu ailelerden yardımların tamamının geri ödenmesi talep

edilmiş ve pek çoğu ağır mali güçlüklere sürüklenmiştir. Hollanda Veri Koruma Otoritesi'nin incelemesi, uygulamanın hukuka aykırı ve ayrımcı olduğunu tespit etmiş; skandal Ocak 2021'de hükümetin toplu istifasıyla sonuçlanmıştır (Hadwick ve Lan, 2021). Bu vaka, "insan gözetimi" ilkesinin yalnızca kâğıt üzerinde var olmasının yeterli olmadığını; gözetimin anlamlı, yani kararı fiilen değiştirebilecek nitelikte olması gerektiğini göstermesi bakımından öğreticidir.

YZ sistemlerinin sorumlu kullanımı, yalnızca sistemin kendi tasarımına değil, kurumların bu sistemleri kullanan personelinin yeterliliğine de bağlıdır. NAO'nun 2024 tarihli incelemesi, ankete katılan kamu kurumlarının önemli bir bölümünde YZ okuryazarlığının ve veri kültürünün yetersiz kaldığını; bu eksikliğin YZ sistemlerinin amaçlandığı gibi kullanılmasını ve olası risklerin öngörülmesini güçleştirdiğini ortaya koymaktadır (NAO, 2024a). Bu bulgu, Sayıştaylar açısından, YZ denetiminin yalnızca sistemin teknik özelliklerine değil, kurumların bu sistemleri kullanma kapasitesine de yönelmesi gerektiğine işaret etmektedir.

Brezilya, Finlandiya, Almanya, Hollanda, Norveç ve Birleşik Krallık Sayıştayları tarafından ortaklaşa geliştirilen "YZ Sistemlerinin Denetimi" konulu rehber, bu alana ilişkin değerli bir kaynak niteliğindedir. Bu çerçeve; proje yönetişimi, veri kalitesi, model geliştirme, şeffaflık ve açıklanabilirlik, adillik ve zarar minimizasyonu ile güvenlik gibi başlıkları kapsayan bütüncül bir denetim metodolojisi sunmaktadır. Rehber, Sayıştayların YZ sistemleri karşısında sormak durumunda olduğu soruları sistematize ederek bir başlangıç noktası oluşturmaktadır (SAI of Brazil vd., 2025). GAO ise bir yandan büyük dil modellerini kendi iç süreçlerinde -özellikle raporlamada- bir kalite kontrol aracı olarak kullanırken (GAO, 2024), aynı zamanda federal kurumların YZ kullanımını geliştirmiş olduğu metodoloji doğrultusunda denetlemekte ve sonuçlarını raporlamaktadır (GAO, 2021b).

D. Dijital Egemenlik: Veri, Altyapı ve Yazılım

Dijital egemenlik kavramı, son yıllarda kamu yönetiminin ve uluslararası ilişkilerin gündeminde önemli bir yer işgal etmeye başlamıştır. Teknoloji artık yalnızca bir verimlilik aracı

olarak değerlendirilmemektedir; ulusal güvenliğin, ekonomik bağımsızlığın ve devlet-vatandaş ilişkisinin önemli bir boyutu olarak ele alınmaktadır. Günümüzde, veri ve yazılım katmanının oluşturduğu dijital sınırlar, fiziksel sınırlar kadar hayati görülmekte; yazılım ve donanımda dışa bağımlılık yalnızca operasyonel bir risk olarak değil, stratejik bir zafiyet olarak da kabul edilmektedir.

Dijital egemenlik üç temel sütun üzerinde yükselmektedir. Birinci sütun, kamu kurumlarının topladığı ve işlediği verinin ulusal sınırlar içindeki egemen altyapılarda güvenle saklanmasını gerekli kılan veri egemenliğidir. Sağlık, eğitim ve vergi gibi kritik kamu verilerinin yerelde değil küresel bulut hizmet sağlayıcılarının altyapılarında tutulması, ekstrateritoryal yasal düzenlemeler nedeniyle (bu düzenlemeler somut örnekleriyle birlikte Hukuk başlığı altında ele alınacaktır) bir egemenlik riski doğurmaktadır. İkinci sütun, altyapı egemenliğidir. Kullanılan altyapı bileşenlerinin güvenilirliği sorusu ve tedarik zincirlerindeki bağımlılık riskleri, kritik kamu bilişim altyapılarında güvenlik ve sürdürülebilirlik konusunu gündeme taşımakta, bu çerçevede "arka kapı" güvencesinin sağlanması ve yabancı kaynaklı donanıma olan bağımlılığın azaltılması bu boyutun temel odak noktaları olarak öne çıkmaktadır. Üçüncü sütun, yazılım egemenliğidir. Bu boyut, kamu kurumlarının yazılım ekosisteminde kendi kendine yetme kapasitesi ve yerli ya da açık kaynak kodlu alternatiflerin kullanım oranı ile yakından ilgilidir.

Sayıştaylar bu üç sütunun her birinde özgün katkılar sunabilmektedir. Veri egemenliği alanında, bulut hizmetleri sözleşmelerinde verilerin sahibi olan ülkede bulundurulmasını zorunlu tutan veri yerelleştirme koşullarının (Kaya, 2026) yerine getirilip getirilmediğini denetlemek ve kritik kamu verilerinin ekstrateritoryal erişim risklerine karşı korunup korunmadığını değerlendirmek, Sayıştayların bu alanda yürütebileceği çalışmalar olarak öne çıkmaktadır. Hollanda Sayıştayı'nın (NCA) 2025 yılında gerçekleştirdiği denetim, Sayıştaylar tarafından bu alanda yürütülebilecek faaliyetlere ilişkin somut bir örnek teşkil etmektedir. NCA, merkezi hükümetin almakta olduğu 1.588 bulut hizmetinin dörtte birinden fazlasının hangi bulut modeline (kamu, özel ya da hibrit bulut) ait olduğunun dahi bilinmediğini, en kritik 126 bulut

hizmetinin ise yarısından fazlasının yabancı ülke uyruğuna tabi sağlayıcılardan temin edildiğini, bu hizmetlerin üçte ikisi için ise hiçbir stratejik risk değerlendirmesi yapılmadığını tespit etmiştir. Denetim, hükümetin buluta "yeterince düşünmeden" geçtiğini ve olası zararın toplumsal işleyişi aksatabilecek boyutta olduğunu vurgulamıştır (NCA, 2025). Bu bulgular, veri egemenliği risklerinin yalnızca soyut hukuki bir kavram değil, sistematik bir denetimle somut biçimde ortaya konabilecek ölçülebilir bir olgu olduğunu göstermektedir. Altyapı egemenliği alanında ise Sayıştayların, kritik bilişim tedarik zincirlerindeki bağımlılık risklerini raporladığı görülmektedir: GAO, 2020-2023 döneminde yaşanan küresel yarı iletken (çip) krizinin ardından hükümetin yerli üretim kapasitesini güçlendirmek amacıyla başlattığı ve 2025 yılı itibarıyla 40 projeye 30,9 milyar dolar kaynak aktarılan destek programının proje seçim kriterlerini ve ilerleyişini denetlemiştir (GAO, 2026). Yazılım egemenliği alanında da GAO'nun denetim bulguları öğretici bir nitelik taşımaktadır. GAO, 2024 yılında 24 federal kurumun yazılım lisans harcamalarını incelemiş, tek bir yazılım sağlayıcısının en yüksek tutarlı lisans harcamalarının yüzde 31,3'ünü oluşturduğunu; kurumların lisans kullanım verilerini tutarlı ve eksiksiz biçimde takip edemedikleri için gereğinden fazla veya az lisans satın alıp almadıklarını dahi belirleyemediklerini tespit etmiştir (GAO, 2024c). Bu bulgu, yazılım egemenliği olgusunun yalnızca stratejik bir tercih meselesi olmadığını; aynı zamanda somut bir mali izlenebilirlik ve disiplin konusu olduğunu göstermektedir. Kamu kurumlarında stratejik açıdan önemli olan yazılımlarda belirli tedarikçilere yoğunlaşılmasını bir performans göstergesi olarak izlemek ve bu yoğunlaşmanın yarattığı mali ve operasyonel riskleri raporlamak, Sayıştayların bu alanda sunabileceği somut bir katkı olarak ortaya çıkmaktadır. Ulaşılan denetim bulguları, yalnızca tekil olarak kurumları değil kamu sektörünün genelini etkileyen sistemik riskleri gün yüzüne çıkarma kapasitesi taşımaktadır.

E. Siber Güvenlik: Kâğıt Üzerinde Uyumdan Gerçek Dayanıklılığa

Siber güvenlik, kamu kurumlarının karşı karşıya olduğu en kapsamlı ve hızla büyüyen risk alanlarından birini oluşturmaktadır.

Bu kurumlarda işlenen hassas verinin hacmi ve kritikliği, kamunun siber saldırılar için cazip bir hedef haline gelmesine yol açmaktadır.

Peki kamu kurumları bu tehdide gerçekten hazır mı? Sayıştaylar bu soruyu yanıtlarken kritik bir ayrımı ön plana çıkarmak durumundadır: mevzuata kâğıt üzerinde uyum ile gerçek siber dayanıklılık aynı şey değildir. Bir kurum, bilgi güvenliği mevzuatının tüm gerekliliklerini belgeleyen raporlar üretebilir; ancak gerçek dünya koşullarında saldırıya karşı savunmasız kalıyor olabilir. BRH bu ayrımı "güvenlik freni" kavramıyla somutlaştırmıştır. BT projelerinde hız baskısı nedeniyle güvenlik standartlarının esnetilmesi gündeme geldiğinde, yasama ve uygulama süreçlerinde bu esnetmelere karşı uyarı görevi üstlenmiş; hız uğruna güvenlikten taviz verilmemesi gerektiğini savunmuştur. Bu yaklaşımla Sayıştaylar, kurumların güvenlik mevzuatına kâğıt üzerinde değil, pratikte uyum sağlayıp sağlamadığını sorgulamaktadır (BRH, 2025a). Bu perspektif, salt uyum denetimini aşan ve etkinlik denetimine uzanan bir anlayışı yansıtmaktadır.

Bu bağlamda Sayıştayların odaklanabileceği somut denetim sorularının şunlar olduğu görülmektedir: Siber güvenliğe ayrılan bütçeler verimli kullanılıyor mu? Kurumların siber dayanıklılık olgunluğu, standart bir endeks çerçevesinde ölçülebilir düzeyde mi? Kritik altyapıların güvenliği ve sürekliliği güvence altında mı? Bir siber saldırı sonrasında kurumların iş sürekliliği ve toparlanma kapasitesi yeterli mi? Kullanılan yazılımların bileşen listeleri (Software Bill of Materials - SBOM) tutulmakta mı?

Farklı ülke Sayıştaylarının bulgularının bu alandaki görünüme ilişkin ortaya koyduğu tablo kaygı vericidir. GAO, 2010'dan bu yana federal siber güvenlik alanında 1.610 öneri yapmıştır ancak Mayıs 2024 itibarıyla bu önerilerin 567'si hâlâ uygulanmayı beklemektedir. Bu durum, Sayıştay bulgularının takibinin ve hesap verebilirlik döngüsünün sağlıklı işleyip işlemediğinin de ayrıca sorgulanması gerektiğini göstermektedir (GAO, 2024a). ANAO'nun bulguları da benzer bir tablo ortaya koymaktadır: Avustralya kamu kurumlarında BT kontrol ortamına ilişkin bulgular yıllar içinde tekrarlanmakta; özellikle bilgi güvenliği, değişiklik yönetimi ve kullanıcı erişim kontrolleri alanlarında kronik zayıflıklar sürmektedir (ANAO, 2024).

Bu alandaki dikkat çekici uygulamalardan biri Birleşik Krallık'ta görülmektedir: 2023'ten bu yana kamu kurumlarının kritik BT sistemlerinin siber dayanıklılığı, GovAssure adı verilen yıllık bir güvence programı çerçevesinde bağımsız doğrulamaya tabi tutulmaktadır. NAO ise bu mekanizmanın kendisini ve ürettiği sonuçları incelemektedir. Kurum, 2025 tarihli raporunda, değerlendirilen kritik sistemlerde temel kontrollerin olgunluk düzeyinin düşük kaldığını ve çok sayıda eski sistemin siber riskinin belirlenemediğini ve bilinemediğini tespit etmiştir (NAO, 2025). Bu iki katmanlı yapı -yürütmenin kendi ölçüm mekanizmasını kurması ve Sayıştayın bu mekanizmayı ve çıktılarını bağımsız biçimde denetlemesi- siber dayanıklılık alanında hesap verebilirlik döngüsünün nasıl işletilebileceğine dair öğretici bir örnek sunmaktadır.

Burada, BRH tarafından geliştirilen özgün araçlardan biri olan Digitalcheck uygulamasına değinmek yerinde olacaktır. 1 Ocak 2023'te kabul edilerek hayata geçen bu mekanizma sayesinde bir yasa veya düzenleme taslak aşamasındayken "dijital olarak uygulanabilir mi?" sorusu test edilmekte, böylece "tasarımdan itibaren güvenlik" (security by design) ilkesi yasama sürecine entegre edilmektedir (BRH, 2025b). Sayıştayların yasama sürecine proaktif biçimde müdahil olduğu ve siber güvenliği kurum içi teknik bir mesele olmaktan çıkarıp yasama sürecinin başından itibaren gözetilmesi gereken sistemik bir politika önceliği olarak konumlandıran bu yaklaşım, denetimin yalnızca geçmişi değerlendiren değil geleceği de şekillendiren bir işlev üstlendiğinin somut kanıtı olmaktadır.

F. Hukuk: Sınır Ötesi Veri Erişimi ve Yasaların Dijital Uygulanabilirliği

Dijitalleşme, hukuki çerçeveyi iki farklı boyutta zorlayan yeni gerilimler yaratmaktadır. Birinci boyut, ulusal mevzuatın, küresel teknoloji şirketlerinin faaliyetleri üzerindeki etkisinin sınırlarını çizen "sınır ötesi" hukuktur. Kritik kamu verilerinin küresel bulut devlerinin altyapılarında tutulması, yabancı devletlere bu verilere erişim hakkı tanıyan ekstrateritoryal hukuki düzenlemeler aracılığıyla egemenlik riskine dönüşebilmektedir.

Bu risk artık yalnızca teorik değildir: Türkçe karşılığı "Yurt Dışında Verilerin Yasal Kullanımını Açıklığa Kavuşturma Yasası" olan ve kısaca US CLOUD Act olarak bilinen yasa, ABD kolluk kuvvetlerinin, ABD yargı yetkisine tabi bulut bilişim ve teknoloji şirketleri tarafından tutulan verilere -verilerin nerede depolandığına ya da verilerin sahipliğinin hangi ülkeye ait olduğuna bakmaksızın- mahkeme kararıyla erişmesine olanak tanımaktadır. Başka bir ifadeyle, ABD kolluk kuvvetleri, bu yasa sayesinde, ABD uyruğundaki şirketler tarafından fiziksel olarak diğer ülkelerin topraklarında tutulmakta olan verilere o ülkenin adli makamlarına haber vermeden erişebilmektedir. Bu durum, "Dijital Egemenlik" başlığı altında bahsi geçen ekstrateritoryal yasal düzenlemeler nedeniyle ortaya çıkan risklere somut bir örnek teşkil etmektedir.

NAO tarafından hazırlanan Bulut Hizmetleri Rehberi, bu risklerin nasıl denetlenebileceğine dair somut bir metodoloji ortaya koymaktadır. Rehber, kamu kurumlarının denetim komitelerinin bulut hizmeti sözleşmelerini değerlendirirken sorması gereken sorular arasında, hizmet sağlayıcının altyapısının hangi ülkede bulunduğunu, verinin hangi ülkenin yargı yetkisi altında tutulduğunu ve sözleşmenin Birleşik Krallık hukukuna tabi olup olmadığını açıkça saymaktadır (NAO, 2019). Bu yaklaşım, ekstrateritoryal erişim risklerinin yalnızca akademik bir tartışma konusu değil, Sayıştayların denetlenen kurumlara sistematik olarak yönelttiği somut bir soru haline geldiğini göstermektedir.

İkinci boyut, dijital yasama kalitesidir, daha açık bir ifadeyle, mevcut ve yeni çıkarılan yasaların dijital gerçeklikle uyumluluğu. Hazırlanan yasalar ve düzenlemeler, dijital ortamda uygulanabilir mi? Siber güvenlik ve veri egemenliği standartlarını yeterince güvence altına alıyor mu? Yukarıda da değinildiği üzere, bu sorular, Almanya'da Digitalcheck uygulaması aracılığıyla yanıtlanmaya çalışılmaktadır. Avrupa Birliği'nde ise Yapay Zekâ Yasası (EU AI Act, Regulation 2024/1689), yüksek riskli YZ uygulamalarına getirilen şeffaflık, hesap verebilirlik ve insan gözetimi zorunlulukları aracılığıyla kamu kurumlarının YZ kullanımına kapsamlı bir hukuki çerçeve çizmektedir (Avrupa Parlamentosu ve Konseyi, 2024). Sayıştaylar, kamu kurumlarının bu düzenlemelere fiilen uyum sağlayıp sağlamadığını bağımsız bir gözle değerlendirme konumundadır.

Bu hukuki çerçevelerin nihai amacı, algoritmik sistemlerin kamu yönetiminde kullanımının demokratik denetime fiilen tabi kalmasını güvence altına almaktır. Kamu yönetimi literatüründe klasikleşmiş bir çalışma, bilgi ve iletişim teknolojilerinin kamu kurumlarını memurların bireysel takdir yetkisi kullandığı "sokak düzeyi bürokrasiden" (street-level bureaucracy) sistemlerin karar verdiği "sistem düzeyi bürokrasiye" (system-level bureaucracy) dönüştürdüğünü; bu dönüşümün idari takdir yetkisini ve anayasal denetim mekanizmalarını köklü biçimde etkilediğini ortaya koymaktadır (Bovens ve Zouridis, 2002). Bu çerçeve, algoritmik sistemlerin kullanımının yaygınlaştığı ve karar alma süreçlerinin sistemlere devredildiği günümüz kamu yönetimi pratiklerine uygulandığında, demokratik hesap verebilirlik açısından üzerinde durulması gereken yeni bir alanın ortaya çıktığı görülmektedir: Bu sistemleri anlayıp denetleyebilecek teknik uzmanlık ile sistemlerin tabi olması gereken demokratik gözetim mekanizmaları arasında bir boşluk doğabilmektedir. Sayıştaylar, hem bu boşluğu tespit edebilecek teknik kapasiteyi geliştirme hem de kamu adına hesap sorma yetkisine sahip olmaları bakımından, yukarıda örnekleri verilen hukuki çerçevelerin öngördüğü demokratik denetimin kâğıt üzerinde kalmayıp fiilen işlemesine katkı sağlayacak kilit aktörlerden biri olarak öne çıkmaktadır.

G. Finansal Teknolojiler: Yeni Araçlar, Yeni Sorular

Blok zinciri, akıllı sözleşmeler, kripto varlıklar ve dijital merkez bankası paraları (CBDC), kamu maliyesinin geleneksel yapısını dönüştürme potansiyeli taşıyan finansal teknolojilerdir. Kamu harcamalarının ve gelirlerinin bu yeni araçlar aracılığıyla gerçekleşmeye başladığı bir tabloda Sayıştayların sormak zorunda olduğu sorular şunlardır: Blok zincirinin sunduğu değiştirilemez işlem kaydı, denetim izini nasıl dönüştürecek? Akıllı sözleşmeler aracılığıyla gerçekleştirilen kamu harcamaları nasıl izlenir ve kodu kim denetler? Kamu kurumlarının kripto varlık ya da token kullandığı durumlarda denetim nasıl yürütülür? CBDC'nin kamu maliyesine etkileri nasıl değerlendirilir? Bunlar, şu an için tam anlamıyla cevaplanamamış olmakla birlikte, Sayıştayların yakın gelecekte yanıtlamak durumunda kalacağı sorulardır.

Köse ve Polat (2021), finansal teknolojilerin dönüştürücü etkisini blok zinciri odağında ele almakta ve denetim açısından yol açtığı sonuçlara iki yönden dikkat çekmektedir: bir yandan blok zincirinin sunduğu değiştirilemez kayıt yapısı, sahte ve yanıltıcı işlemlerin gerçekleştirilmesini engelleyerek denetim izinin güvenilirliğini artırmakta; öte yandan dönemsel denetim raporlamasından sürekli denetim yaklaşımına geçişi mümkün kılmaktadır.

Çoğu ülkede olduğu gibi Türkiye'de de bu alanda somut düzenleyici adımlar atılmaktadır. 5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanunun 3 ve 9/A maddelerinde düzenlenen müşterinin tanınması, şüpheli işlem bildirimi ve bilgi/belge verme yükümlülükleri, 1 Mayıs 2021 tarihli bir yönetmelik değişikliğiyle kripto varlık hizmet sağlayıcılarını da kapsayacak şekilde genişletilmiş; Temmuz 2024'te 6362 sayılı Sermaye Piyasası Kanununda yapılan değişiklikle bu kuruluşlar ayrıca Sermaye Piyasası Kurulunun doğrudan düzenleme ve denetim yetkisi altına alınmıştır. Bu gelişme, kripto varlık ekosisteminin devletin finansal istihbarat ve denetim ağına kademeli olarak entegre edildiğini göstermektedir. Bu tür düzenlemelerin kâğıt üzerinde kalmayıp fiilen uygulanıp uygulanmadığının, yani hizmet sağlayıcıların gerçekten etkin bir izleme, raporlama ve uyum altyapısı kurup kurmadığının denetlenmesi, Sayıştayların bu alanda katkı sunabileceği bir nokta olarak ortaya çıkmaktadır.

Akıllı sözleşmeler aracılığıyla gerçekleştirilen kamu harcamalarının denetimi ise akıllı sözleşmelerin doğası gereği geleneksel denetimden farklı bir yaklaşıma ihtiyaç duyulduğunu göstermektedir: mevcut durumda bir harcama işlemi gerçekleştikten sonra belgeler üzerinden geriye dönük olarak incelenebilirken, akıllı sözleşmeler blok zincirine yerleştirildikten sonra değiştirilemez hale gelmekte, bu da hatalı veya kötü niyetle yazılmış bir kodun sonradan düzeltilmesini imkânsız kılmaktadır. Bu nedenle akıllı sözleşmelerin denetimi, kod devreye alınmadan önce yürütülmesi gereken bir ön denetim faaliyetine dönüşmekte; bu amaçla geliştirilen biçimsel doğrulama (formal verification) yöntemi, sözleşmenin kodunu matematiksel kanıt teknikleriyle inceleyerek tasarlandığı gibi çalışacağına dair önceden güvence elde edilmesini amaçlamaktadır (Bhargavan vd., 2016).

Yeni finansal teknolojilerin denetim süreçlerine entegrasyonu çeşitli fırsatlar sunmaktadır; ancak görüleceği üzere bu potansiyelin gerçeğe dönüşmesi için Sayıştayların bu alandaki teknik yetkinliklerini yeniden şekillendirerek geliştirmesi ve mevcut denetim metodoloji ve standartlarının bu teknolojiler doğrultusunda güncellenmesi gerekmektedir. Bu çerçevede Sayıştayların, yeni finansal teknolojilerin uygulama alanlarını ve sınırlarını ele alan teknoloji değerlendirme raporları yayımladığı görülmektedir (GAO, 2022). Bu tür çalışmalar, Sayıştayların yeni teknolojiler karşısında yalnızca denetleyen konumunda kalmadığını, politika yapıcıları bilgilendiren bir işlev de üstlenebildiğini göstermektedir.

III. SAYIŞTAYLARIN DÖNÜŞEN ROLLERİ: BÜTÜNLEŞİK BİR ÇERÇEVE

Önceki bölümlerde, dijital ekosistemin temel bileşenlerinde Sayıştayların katma değer üretebileceği alanlar ortaya konmaya çalışılmıştır. Bu tespitler bir araya getirildiğinde, geleneksel denetim anlayışının ötesine geçen yeni bir denetim anlayışına yönelen köklü bir dönüşümün parametreleri netleşmektedir.

Geleneksel anlayış, denetimde ağırlıklı olarak şu soruları sormuştur: Para nereye harcandı? Harcama mevzuata uygun muydu? Kayıt doğru mu? Şüphesiz ki, bu sorular hâlâ geçerliliğini korumaktadır; ancak dijital çağın yönetim güçlüklerini karşılamak için tek başlarına yetersiz kalmaktadır. Yeni denetim anlayışı bu sorulara şunları eklemektedir: BT yatırımları hedeflenen değeri yarattı mı? Dijital dönüşüm gerçek mi, yoksa yalnızca bir arayüz değişikliği mi yapıldı? Kamu verisi güvenilir mi, güvenli mi ve kamu yararına mı kullanılıyor? YZ sistemleri adil, şeffaf ve hesap verebilir mi? Kritik altyapılar gerçekten güvende mi, yoksa güvenlik yalnızca kâğıt üzerinde mi? Dijital egemenlik riskleri yönetiliyor mu? Sayıştaylar, bu sorular doğrultusunda dijital dönüşümün temel bileşenleri ile ilgili özgün denetim metodolojileri geliştirmekte (SFAO, 2023; GAO, 2021b) ve bu alanlarda uluslararası iş birliği ağları oluşturmaktadır (SAI of Brazil vd., 2025; Yener vd., 2025).

Bu dönüşümün merkezinde, Sayıştayların sahip olduğu ve başka hiçbir kurumun ikame edemeyeceği bir kurumsal konum yatmaktadır: kamu kesiminin bütününe dışarıdan, bağımsız ve yapıcı bir bakış açısıyla bakabilme kapasitesi. Teknik uzmanlar belirli

sistemleri, iç denetçiler kendi kurumlarını incelemektedirler; ancak tek tek kurumların denetlenmesi ile görülemeyecek olan sistemik sorunları, silo yapılar arasındaki boşlukları ve kurumlar arası koordinasyon eksikliklerini yalnızca, kamu sektörünün tamamına yönelik denetim yetkisine sahip Sayıştaylar tespit edebilmektedir (Akyel ve Köse, 2010; Otia ve Bracci, 2022).

Bu özgün konumdan hareketle Sayıştayların dijital ekosistemde üstlenebileceği roller, "öngören, rehberlik eden ve örnek olan" şeklinde özetlenebilir. Öngörü boyutunda Sayıştaylar; dijitalleşme süreçlerindeki riskleri oluşmadan önce tespit etme, büyük ölçekli kamu BT projelerinin başarısızlık sinyallerini erken dönemde raporlama ve politika yapıcılara stratejik uyarılar iletme işlevi üstlenmektedir. Rehberlik boyutunda; iyi uygulamaları karşılaştırmalı olarak değerlendirip yaygınlaştırma, kamu kurumlarına dijital olgunluk ekseninde bir referans çerçevesi sunma ve mevzuat ile strateji belgelerinin dijital gerçeklikle uyumunu denetleme işlevini yerine getirmektedir. Örnek olma boyutunda ise kurumsal davranışını en yüksek şeffaflık, hesap verebilirlik ve etik standartlarıyla şekillendirerek kamu sektörü için bir model teşkil etmektedirler (INTOSAI-P 12, 2019).

Bu üç boyutun çalışmamızda ele alınan örneklerde nasıl tezahür ettiğini hatırlamak, çerçeveyi somutlaştırmak açısından faydalı olacaktır. Öngörü boyutu, BRH'nin Smart-eID projesindeki başarısızlık riskini proje devam ederken tespit edip uyarmasında somutlaşmaktadır. Rehberlik boyutu, NAO'nun kamu kurumlarının denetim komitelerine bulut hizmetleri sözleşmelerinin incelenmesinde hangi soruların sorulması gerektiğini gösteren rehberinde ve SFAO'nun DigiTrans modelinin kurumlara sunduğu somut değerlendirme çerçevesinde görülmektedir; bu araçlar, Sayıştayların denetledikleri kurumları yalnızca süreç sonunda değerlendirmekle kalmayıp, süreç boyunca yönlendirdiğini de ortaya koymaktadır. Örnek olma boyutu ise GAO'nun kendi iç süreçlerinde büyük dil modellerinden faydalanırken "sorumlu kullanım" ilkesini ön plana almasında somutlaşmaktadır; GAO, kendi kurumsal pratiğinde bu teknolojiyi nasıl sorumlu biçimde kullanacağını göstererek, denetlediği kurumlardan beklediği standartları önce kendi bünyesinde uygulamaktadır.

Tüm bu gelişmeler, denetimin sınırlarının değiştiğini; izleme ve değerlendirme işlevlerinin tek tek kurumları değil sistemleri, tek tek projeleri değil politikaları, tek tek harcamaları değil kamu değeri yaratımını kapsadığını göstermektedir (Lagos, 2026). Bu dönüşüm aynı zamanda Sayıştayların kendi kapasitelerini geliştirme zorunluluğunu da beraberinde getirmektedir: siber güvenlik, veri analitiği, YZ yönetişimi ve finansal teknolojiler gibi alanlarda uzmanlaşmış insan kaynağı oluşturmak (Hamdouche vd., 2026); uluslararası iyi uygulamalardan ve yeni metodolojilerden etkin şekilde yararlanmak ve kurumun denetim stratejisini dijital dönüşümün hızına uygun biçimde güncellemek bu zorunluluğun uygulamaya yansıyan boyutlarını oluşturmaktadır.

SONUÇ

Dijitalleşme, kamu yönetiminin işleyişini derinden dönüştürmektedir ve bu süreç Sayıştaylar için hem büyük fırsatlar hem de zorlu sorular barındırmaktadır. Bu çalışma, söz konusu dönüşüm ortamında Sayıştayların katma değeri yüksek alanlara odaklanmak suretiyle iyi yönetişime daha fazla katkı sunma potansiyelini analiz ederek, geleceğe dönük stratejilerinin şekillenmesinde yönlendirici olabilecek bir çerçeveyi teori ve uygulama boyutuyla ortaya koymayı amaçlamıştır.

Kamu kurumlarının dijital dönüşüme ayırdığı kaynakların hacminin hızla büyümesi, denetimin de aynı hızla ve aynı derinlikte bu alanlara nüfuz etmesini gerektirmektedir. Ortaya konulan mevcut tablo, bu ihtiyacın hâlihazırda tam olarak karşılanmadığını; Sayıştayların bu alanda sağlayabileceği potansiyel katma değerin henüz tam anlamıyla üretilemediğini göstermektedir.

Yapılan analizler sonucunda ulaşılan temel bulgular şu şekilde özetlenebilir: Dijital devlet alanında, Sayıştaylar "etki odaklı" bir bakışla BT yatırımlarının hedeflenen değeri yaratıp yaratmadığını sorgulamakta; proaktif mekanizmalar aracılığıyla hatalı tasarlanmış projelere karşı erken uyarı işlevi görebilmektedir. Veri alanında, bir kamu kaynağı olarak konumlanmakta olan kamu verisinin doğruluğuna ve kamu yararına kullanımına ilişkin bağımsız güvence sağlamayı Sayıştaylar özgün bir işlev haline getirmektedir. Yapay zekâ alanında, YZ harcamalarının hedeflenen değeri üretip

üretmediği ile YZ sistemlerinin şeffaflığı, adaleti ve güvenliği üzerindeki denetim iki ayrı ancak birbirini tamamlayan görev olarak öne çıkmaktadır. Dijital egemenlik alanında, veri, altyapı ve yazılım egemenliğine yönelik sistematik denetim, tüm boyutlarını kapsayacak haliyle yalnızca Sayıştaylar tarafından yürütülebilecek niteliktedir. Siber güvenlik alanında, kâğıt üzerinde uyumla gerçek dayanıklılık arasındaki ayrım, Sayıştayların etkinlik odaklı denetim anlayışı ile somut şekilde örtüşmektedir. Hukuk ve finansal teknolojiler alanlarında ise yeni düzenleyici çerçeveler ve yeni finansal araçlar, denetim metodolojisinin sürekli güncellenmesini zorunlu kılmaktadır.

Tüm bu eksenler ortak bir noktada birleşmektedir: Sayıştayları benzersiz kılan, kamu kesiminin bütününe dışarıdan, bağımsız ve yapıcı bir bakış açısıyla bakabilme kapasitesi dijital dönüşüm çağında kendiliğinden değer üretmemektedir. Çalışmanın ortaya koyduğu tablo, bu konumun ancak tutarlı ve sistematik bir denetim stratejisi, uzmanlaşmış insan kaynağı ve sürekli güncellenen metodolojilerle katma değere dönüştüğünü göstermektedir. Sistemik sorunları tespit etmek, politika yapıcılara stratejik içgörüler sunmak ve vatandaşın dijital kamu hizmetlerinden gerçekten yararlanıp yararlanmadığını güvence altına almak; bu dönüşümün somut çıktılarıdır.

Bu noktada altı çizilmesi gereken husus, dijital dönüşümün doğası gereği tekil kurumların çabasıyla değil, kamu kesiminin bütününde eşgüdümlü bir çabayla sağlıklı biçimde ilerleyebileceğidir. Veri standartlarının uyumlaştırılması, siber güvenlik olgunluğunun kamu genelinde eşit düzeye getirilmesi, yapay zekâ yönetişiminin tutarlı ilkeler etrafında şekillendirilmesi; bunların hiçbirinin tek bir kurumun kendi başına çözebileceği meseleler olmadığı görülmektedir. Kamu kesiminin bütününe yönelik denetim yetkisine sahip olan ve tekil kurumların göremediği sistemik boşlukları görebilen Sayıştaylar, bu eşgüdümü teşvik edecek ve kolaylaştıracak benzersiz bir konumda bulunmaktadır. Bu bakımdan, dijitalleşme ile hedeflenen katma değere ulaşılmasında Sayıştaylar tarafından üstlenilecek rolün sahip olduğu kritik önem ortaya çıkmaktadır. Dolayısıyla tarihsel gelişim süreçlerinde yeni bir aşamayı teşkil edecek şekilde Sayıştayımızın ve diğer ülke

Sayıştaylarının bu alana özel bir ağırlık verecekleri ve vizyonlarının bu yönde yeniden şekilleneceği kolaylıkla söylenebilir.

İleride yapılacak araştırmalar açısından bakıldığında, farklı ülke Sayıştaylarının bu dönüşüme verdiği yanıtların karşılaştırmalı olarak incelenmesi, ulusal hukuki çerçevelerin Sayıştayların dijital denetim kapasitesi üzerindeki etkisinin değerlendirilmesi ve yeni denetim metodolojilerinin geliştirilmesine ilişkin ampirik çalışmaların, bu alandaki bilgi birikimine önemli katkılar sunacağı düşünülmektedir. Sayıştayların bu alanda hazırladıkları raporların etkisinin ölçülmesi amacıyla parlamentolar nezdinde oluşturduğu etki ve denetlenen kamu kurumlarının bu raporlarda sunulan bulgu ve önerileri hayata geçirme kapasiteleri ya da yaklaşımları da araştırılmasında yarar görülen konulardır.

KAYNAKÇA

Akyel, R. (2016). Sayıştay Raporlarının Kamu Mali Yönetimine Katkısı. Amme İdaresi Dergisi, 49(1), 119-145.

Akyel, R. ve Köse, H. Ö. (2010). Kamu Yönetiminde Etkinlik Arayışı: Etkin Kamu Yönetimi İçin Etkin Denetimin Gerekliliği. Türk İdare Dergisi, (466), 9-45.

ANAO (2024). ANAO Annual Report 2023-24. Australian National Audit Office, Canberra.

ANAO (2025). Governance of Artificial Intelligence at the Australian Taxation Office. Auditor-General Report No. 26, 2024-25. Australian National Audit Office, Canberra.

Asiloğulları Ayan, M. (2026). Kamu Kurumlarında Bilgi Sistemleri ve Dijital Denetim: Sayıştay Dergisi Üzerine Bir Metin Madenciliği Analizi. Sayıştay Dergisi, 37(141), 253-283.

Ateş, H. (2025). Algorithmic Systems and Democratic Oversight in Public Auditing. TCA Journal/Sayıştay Dergisi, 36(139), 681-709.

Avrupa Parlamentosu ve Konseyi (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act). Avrupa Birliği Resmî Gazetesi, 12 Temmuz 2024.

Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Gollamudi, A., Gonthier, G., Kobeissi, N., Rastogi, A., Sibut-Pinote, T., Swamy, N. ve Zanella-Béguelin, S. (2016). Formal Verification of Smart Contracts: Short Paper. Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security (PLAS '16), 91-96.

BRH - Bundesrechnungshof (2024). Digitalstrategie der Bundesregierung — Ausrichtung und Ziele. Bundesrechnungshof, Bonn.

BRH - Bundesrechnungshof (2025a). Verwaltungsdigitalisierung: Empfehlungen für die 21. Legislaturperiode. Bundesrechnungshof, Bonn.

BRH - Bundesrechnungshof (2025b). Digitalcheck im Rechtsetzungsverfahren. Bundesrechnungshof, Bonn.

BRH - Bundesrechnungshof (2025c). Digitale Identitäten: Ressortübergreifende Steuerung und Umsetzung der Vorhaben. Bundesrechnungshof, Bonn.

Damar, M., Köse, H. Ö., Cagle, M. N. ve Özen, A. (2024). Mapping the Digital Frontier: Bibliometric and Machine Learning Insights into Public Administration Transformation. Sayıştay Dergisi, 132, 9-41. https://doi.org/10.52836/sayistay.1455036

Ergen, Z. ve Durak, B. (2020). Tarihsel Süreç İçerisinde Türk Sayıştayı. Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 29(1), 298-307.

GAO (2007). United States Government Accountability Office: Supporting the Congress through Oversight, Insight, and Foresight. GAO-07-644T. U.S. Government Accountability Office, Washington D.C.

GAO (2021a). Anniversary Events: A Hundred Years of GAO. U.S. Government Accountability Office, Washington D.C. https://www.gao.gov/about/what-gao-does/hundred-years-of-gao/anniversary-events

GAO (2021b). Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities. GAO-21-519SP. U.S. Government Accountability Office, Washington D.C.

GAO (2022). Blockchain: Emerging Technology Offers Benefits for Some Applications but Faces Challenges. GAO-22-104625. U.S. Government Accountability Office, Washington D.C.

GAO (2024). Artificial Intelligence: GAO's Work to Leverage Technology and Ensure Responsible Use. GAO-24-107237. U.S. Government Accountability Office, Washington D.C.

GAO (2024a). High Risk Series: Cybersecurity. GAO-24-107231. U.S. Government Accountability Office, Washington D.C.

GAO (2024b). Federal Contractors: Actions Needed to Improve Quality of Performance and Integrity Data. GAO-24-106911. U.S. Government Accountability Office, Washington D.C.

GAO (2024c). Federal Software Licenses: Agencies Need to Take Action to Achieve Additional Savings. GAO-24-105717. U.S. Government Accountability Office, Washington D.C.

GAO (2026). Semiconductors: Information on Projects Funded to Strengthen U.S. Supply Chain. GAO-26-107882. U.S. Government Accountability Office, Washington D.C.

Hadwick, D. ve Lan, S. (2021). Lessons to Be Learned from the Dutch Childcare Allowance Scandal: A Comparative Review of Algorithmic Governance by Tax Administrations in the Netherlands, France and Germany. World Tax Journal, 13(4), 609-645.

Hamdouche, R., Bouchetara, M., Yoruk, E. ve Zerouti, M. (2026). Artificial Intelligence and the Future of Management: Evidence from Algeria on Redefining Roles, Skills, and Human-Machine Collaboration. Sayıştay Dergisi, 37(140), 1-34.

INTOSAI (2019). INTOSAI-P 1: Lima Deklarasyonu. Uluslararası Yüksek Denetim Kurumları Örgütü, Viyana. https://www.issai.org

INTOSAI (2019). INTOSAI-P 12: Yüksek Denetim Kurumlarının Değeri ve Faydaları — Vatandaşların Hayatında Fark Yaratmak. Uluslararası Yüksek Denetim Kurumları Örgütü, Viyana. https://www.issai.org

Kahyaoğlu, S., Arslan, Y. ve Özçakır, M. (2026). Türkiye'de KVKK Düzenlemeleri Çerçevesinde Otomasyona Uyum Algısının Analizi. Sayıştay Dergisi, 37(140), 65-96.

Kaya, M. B. (2026). Kişisel Verileri Türkiye'de Barındırma Zorunluluğu: Türk Hukukunda Veri Lokalizasyon Hükümleri. https://mbkaya.com/veri-lokalizasyon-turkiye-kvkk/ (Erişim Tarihi: 6 Temmuz 2026).

Köse, H. Ö. (2007). Dünyada ve Türkiye'de Yüksek Denetim. T.C. Sayıştay Başkanlığı 145. Yıl Yayınları, Ankara.

Köse, H. Ö. ve Polat, N. (2021). Dijital Dönüşüm ve Denetimin Geleceğine Etkisi. Sayıştay Dergisi, 32(123), 9-41. https://doi.org/10.52836/sayistay.1068328

Köse, H. Ö. (2023). Kamu Yönetiminde Denetimin İşlevleri, Dinamikleri ve Geleceği. Eds. Önder, M. ve Köse, H. Ö., Kamu Yönetiminde Denetim: Temel Paradigmalar, Değişim ve Yeni Yönelişler, Sayıştay Yayınları, 37-68.

Lagos, N. (2026). How Have the Transformations of Supreme Audit Institutions Shaped Contemporary Public Auditing? A Professional, Process, and Stakeholder Perspective. Financial Accountability & Management. https://doi.org/10.1111/faam.70030

NAO (2019). Guidance for Audit Committees on Cloud Services. National Audit Office, Londra.

NAO (2024). Digital Transformation in Government: A Guide for Senior Leaders and Audit and Risk Committees. National Audit Office, Londra. https://www.nao.org.uk/wp-content/uploads/2024/02/digital-transformation-in-government.pdf

NAO (2024a). Use of Artificial Intelligence in Government. HC 612, 15 Mart 2024. National Audit Office, Londra. https://www.nao.org.uk/reports/use-of-artificial-intelligence-in-government/

NAO (2025). Government Cyber Resilience. HC 545, Session 2024-25. National Audit Office, Londra. https://www.nao.org.uk/reports/government-cyber-resilience/

NCA - Netherlands Court of Audit (2025). Het Rijk in de cloud: Donkere wolken pakken samen [Dutch central government in the cloud: Dark clouds gathering]. Netherlands Court of Audit, The Hague. https://english.rekenkamer.nl/documents/2025/01/15/dutch-central-government-in-the-cloud

OECD (2016). Supreme Audit Institutions and Good Governance: Oversight, Insight and Foresight. OECD Public Governance Reviews, OECD Publishing, Paris. https://doi.org/10.1787/9789264263871-en

OECD (2022). Going Digital to Advance Data Governance for Growth and Well-being. OECD Publishing, Paris. https://doi.org/10.1787/e3d783b0-en

OECD (2024). 2023 OECD Digital Government Index. OECD Public Governance Policy Papers. OECD Publishing, Paris.

OECD (2024a). Governing with Artificial Intelligence. OECD Publishing, Paris.

Otia, J. E. ve Bracci, E. (2022). Digital Transformation and the Public Sector Auditing: The SAI's Perspective. Financial Accountability

& Management, 38(2), 252-280. https://doi.org/10.1111/faam.12317

Önder, M. (2023). Kamu Yönetiminde Güncel Eğilimler. Eds. Önder, M. ve Köse, HÖ, Kamu Yönetiminde Denetim: Temel Paradigmalar, Değişim ve Yeni Yönelişler, Sayıştay Yayınları.

Pollitt, C. ve Summa, H. (1997). Comparative and International Administration: Reflexive Watchdogs? How Supreme Audit Institutions Account for Themselves. Public Administration, 75(2), 313-336.

SAI of Brazil, Finland, Germany, the Netherlands, Norway and the UK (2025). Auditing Machine Learning Algorithms: A White Paper for Public Auditors. https://www.auditingalgorithms.net (Erişim Tarihi: 13 Haziran 2026).

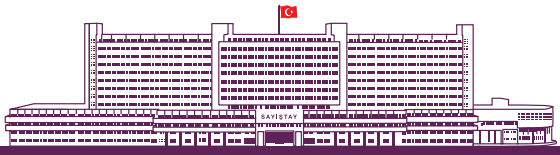
SFAO - Swiss Federal Audit Office (2023). Digital Transformation: Summary Report on Past Audits. Swiss Federal Audit Office, Bern. https://www.efk.admin.ch

Şaşmaz, M. Ü. ve Özen, A. (2026). Dijital Teknoloji ve Hesap Verebilirlik İlişkisi: G20 Ülkeleri Üzerine Ampirik Bir İnceleme. Sayıştay Dergisi, 37(140), 35-63.

Uzun, H. (2024). Kamu Yönetiminde Paradigma Değişimi: Yeni Kamu Yönetişimi. Ankara Hacı Bayram Veli Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 26(2), 647-672. https://doi.org/10.26745/ahbvuibfd.1437097

WEF - World Economic Forum (2011). Personal Data: The Emergence of a New Asset Class. World Economic Forum, Cenevre.

Yener, M., Charoenpol, M., Suntharanurak, S. ve Köse, H. Ö. (2025). Strategic Cooperation of Supreme Audit Institutions of Thailand and Türkiye for Digital Transformation and Innovation in Public Sector Auditing. Sayıştay Dergisi, 36(136), 9-34.



Sayıştay, Türk Kamu Mali Sisteminin Müeyyidesidir.

Sayıştay, Türk Kamu Mali Sisteminin sağlıklı çalışmasının teminatıdır ve güvencesidir.

Sayıştay, Osmanlı yönetim sisteminden Divan Modelinin günümüzde yaşayan tek örneğidir.

Sayıştay, üç bağımsız kurumu tek ad altında, tek çatı altında, tek başkanlık altında toplayan, ancak her üç kurumun da fonksiyonel anlamda bağımsız çalıştıkları bir örnektir. Birincisi bağımsız Yüksek Kamu Denetim Kurumu, İkincisi İlk Derece Hesap Mahkemesi, Üçüncüsü Temyizen Yüksek Hesap Mahkemesi.

Yüksek Kamu Denetim Kurumu fonksiyonu ile Sayıştay, Türk Kamu Yönetiminin verimli, ekonomik ve etkin çalışmasına ve iyi yönetişimin gerçekleşmesine katkı sunmaktadır.

Dijitalleşme ile yaşanan dönüşüm ortamında Kamu Yönetimin Sağlıklı bir çevrede çalışması, iyi yönetişime katkı sağlanması, risklerin öngörülerek çözüm için öneriler geliştirmek sayışların faaliyetleri arasındadır.

Sayıştayların dijital ekosistemde gerçekleştireceği katma değer kamu yönetimi için önemli ve büyük olacaktır.

ISBN: 978-975-7590-55-2

İnönü Bulvarı (Eskişehir Yolu) No: 45
06520 Balgat Çankaya / ANKARA

Tel: (+90) 312 295 30 00
sayistay@sayistay.gov.tr