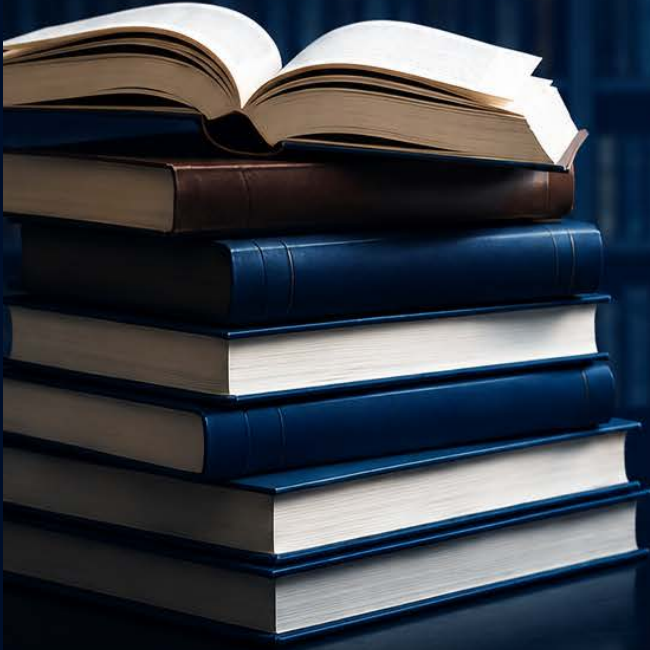


YÖNETİM BİLİŞİM SİSTEMLERİ ALANINDA GÜNCEL KONULAR VE AKADEMİK DEĞERLENDİRMELER

Editör: Doç.Dr. Senem ALTAN



yaz
yayınları

Yönetim Bilişim Sistemleri Alanında Güncel Konular ve Akademik Değerlendirmeler

Editör

Doç.Dr. Senem ALTAN

yaz
yayınları

2026

**Yönetim Bilişim Sistemleri Alanında
Güncel Konular ve Akademik
Değerlendirmeler**

Editör: Doç.Dr. Senem ALTAN

© YAZ Yayınları

Bu kitabın her türlü yayın hakkı Yaz Yayınları'na aittir, tüm hakları saklıdır. Kitabın tamamı ya da bir kısmı 5846 sayılı Kanun'un hükümlerine göre, kitabı yayınlayan firmanın önceden izni alınmaksızın elektronik, mekanik, fotokopi ya da herhangi bir kayıt sistemiyle çoğaltılamaz, yayımlanamaz, depolanamaz.

E_ISBN 978-625-5450-70-8

Ekim 2026 – Afyonkarahisar

Dizgi/Mizanpaj: YAZ Yayınları

Kapak Tasarım: YAZ Yayınları

YAZ Yayınları. Yayıncı Sertifika No: 73086

M.İhtisas OSB Mah. 4A Cad. No:3/3

İscehisar/AFYONKARAHİSAR

www.yazyayinlari.com

yazyayinlari@gmail.com

İÇİNDEKİLER

**Siber Güvenlik ve Yönetim Bilişim Sistemlerinde Veri
Mahremiyeti: KVKK Bağlamında Bir Değerlendirme ..1**
Mansur BEŞTAŞ, Abdurrezzak ÇELİK

**Yönetim Bilişim Sistemlerinde Dijital Sürdürülebilirlik:
Kavramsal Temeller, Akıllı Bilgi Sistemleri ve
Sürdürülebilir Değer Yaratımı.....33**
Furkan ATLAN

**Embodiment as Commons: The Political Economy of
Open-Source AI Bodies.....55**
İsmail Erim GÜLAÇTI

"Bu kitapta yer alan bölümlerde kullanılan kaynakların, görüşlerin, bulguların, sonuçların, tablo, şekil, resim ve her türlü içeriğin sorumluluğu yazar veya yazarlarına ait olup ulusal ve uluslararası telif haklarına konu olabilecek mali ve hukuki sorumluluk da yazarlara aittir."

SİBER GÜVENLİK VE YÖNETİM BİLİŞİM SİSTEMLERİNDE VERİ MAHREMİYETİ: KVKK BAĞLAMINDA BİR DEĞERLENDİRME

Mansur BEŞTAŞ¹

Abdurrezzak ÇELİK²

1. GİRİŞ

Bilgi ve iletişim teknolojilerinin işletme işlevleriyle bütünleşmesi, yönetim bilişim sistemlerini (YBS) çağdaş kuruluşların karar alma ve operasyon süreçlerinde merkezi bir konuma taşımıştır. Yönetim bilişim sistemleri veri toplama, işleme, saklama ve raporlama işlevlerini bir araya getirerek yöneticilere zamanında ve güvenilir bilgi sağlamayı amaçlamaktadır (Laudon ve Laudon, 2011). Sistemlerin kapsamı genişledikçe işlenen verinin hacmi, çeşitliliği ve hassasiyeti de artmaktadır. Böylece siber güvenlik ve veri mahremiyeti, yalnız bilgi işlem birimlerinin değil, üst yönetimin ve bütün kurumsal işlevlerin sorumluluk alanına girmektedir.

Uzaktan ve hibrit çalışma düzenlerinin yaygınlaşması, kurumsal uygulamaların bulut altyapılarına taşınması ve üçüncü taraf hizmetlere bağımlılığın artması, bilgi güvenliği risklerini daha karmaşık hâle getirmiştir. Bulut ortamlarında yetkisiz erişim, veri kaybı, güven eksikliği, farkındalık yetersizliği ve düzenleyici belirsizlikler öne çıkan sorunlar arasındadır (Ukeje vd., 2024). Bu koşullar işletmelerin teknik altyapı yatırımlarıyla

¹ Doç. Dr., Bitlis Eren Üniversitesi, ORCID: 0000-0002-8192-2044.

² Bilim Uzmanı, ORCID: 0000-0003-1128-534X.

birlikte hukuki uyum, tedarikçi denetimi ve kurumsal yönetim kapasitelerini de geliştirmesini gerektirmektedir.

Kişisel verilerin korunması, siber güvenliğin temel hukuki boyutlarından biridir. Türkiye'de 7 Nisan 2016 tarihinde yayımlanan 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK), kişisel verilerin işlenmesine ilişkin ilkeleri, işleme şartlarını ve veri sorumlularının yükümlülüklerini düzenlemektedir. Kanun'un 8, 9, 11, ve 13-18. maddeleri yayımından altı ay sonra, diğer hükümleri ise yayımı tarihinde yürürlüğe girmiştir. Kanun'un özel nitelikli kişisel veriler ile yurt dışına aktarımı düzenleyen 6 ve 9. maddeleri ile kabahatlere ilişkin 18. maddesi 2024 yılında değiştirilmiş, böylece ulusal sistemin Avrupa Birliği düzenlemeleriyle uyumlaştırılması yönünde önemli bir adım atılmıştır (Turan Başara, 2024; Kişisel Verileri Koruma Kurumu [KVKK], 2024a). Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) ise belirli koşullarda Birlik dışında yerleşik veri sorumluları ve veri işleyenler üzerinde de etki doğurmaktadır. Her iki düzenleme, veri mahremiyetinin YBS'nin tasarımıyla ilişkilendirilmesine kadar bütün yaşam döngüsünde gözetilmesini gerektirmektedir.

Çalışmanın amacı, yönetim bilişim sistemlerinde siber güvenlik ve veri mahremiyetini teknik güvenlik, hukuki uyum, insan faktörü ve kurumsal yönetimden oluşan dört bileşenli bir çerçevede incelemektir. Bu doğrultuda KVKK ile GDPR'nin işletme uygulamalarına etkileri karşılaştırılmakta, güncel siber güvenlik yaklaşımları değerlendirilmekte ve Türkiye'deki işletmelere yönelik uygulanabilir öneriler geliştirilmektedir. İnceleme, ampirik bir araştırmadan çok güncel mevzuat ile alan yazını eleştirel biçimde bir araya getiren kavramsal bir sentez niteliğindedir.

Bu kavramsal sentezde, yönetim bilişim sistemleri, siber güvenlik, veri mahremiyeti, bulut bilişim, insan faktörü ve

kurumsal bilgi güvenliği alanındaki güncel akademik çalışmalar ile KVKK, GDPR, Kişisel Verileri Koruma Kurulu kararları, Kurum rehberleri ve ilgili standartlar birlikte incelenmiştir. Kaynaklar, bölümün teknik, hukuki, insan ve yönetim boyutlarını açıklama gücü ile güncellikleri dikkate alınarak seçilmiş, mevzuata ilişkin değerlendirmelerde resmî düzenleme ve Kurum kaynakları esas alınmıştır.

Bu çalışmada veri mahremiyeti ile bilgi güvenliği birbirinin yerine kullanılan kavramlar olarak ele alınmamaktadır. Veri mahremiyeti, kişisel verilerin hangi amaçla, hangi hukuki dayanakla ve hangi sınırlar içinde işlendiğine odaklanırken bilgi güvenliği, verinin gizlilik, bütünlük ve erişilebilirliğini koruyan teknik ve idari tedbirleri kapsar. Şifreleme, kimlik ve erişim yönetimi ile ağ segmentasyonu bu nedenle mahremiyetin kendisi değil, hukuka uygun veri işleme düzenini destekleyen güvenlik araçlarıdır.

Çalışma sekiz ana başlıktan oluşmaktadır. Girişin ardından yönetim bilişim sistemlerinin kavramsal çerçevesi ve temel bileşenleri açıklanmakta, siber güvenlik kavramı ile dijitalleşme sürecinde ortaya çıkan başlıca tehditler ele alınmaktadır. Daha sonra KVKK ve GDPR karşılaştırılmakta, bulut bilişim, ERP entegrasyonu ve çalışan davranışlarından kaynaklanan mahremiyet riskleri tartışılmaktadır. Kurumsal bilgi güvenliği yönetimi standartlarının incelenmesinden sonra Türkiye'deki uygulama sorunları ve öneriler değerlendirilmekte, çalışma genel bir değerlendirmeye tamamlanmaktadır.

2. YÖNETİM BİLİŞİM SİSTEMLERİ: KAVRAMSAL ÇERÇEVE

Yönetim bilişim sistemleri, bir kuruluşun karar alma, koordinasyon, kontrol ve analiz faaliyetlerini desteklemek üzere insan, süreç, veri ve teknolojiyi bir araya getiren yapılardır

(Laudon ve Laudon, 2011). İşlem işleme sistemleri, yönetim raporlama sistemleri, karar destek sistemleri ve yönetici bilgi sistemleri farklı yönetsel düzeylerdeki bilgi ihtiyaçlarına karşılık verir. Güncel dijital dönüşüm yazını ise bilgi sistemlerinin yalnız mevcut süreçleri destekleyen araçlar olmadığını, değer önerisini, örgütsel kimliği ve iş modellerini dönüştürebildiğini vurgulamaktadır (Verhoef vd., 2021; Wessel vd., 2021). Çağdaş YBS yaklaşımı bu dönüşüm doğrultusunda, operasyonel verimlilik ile stratejik ve örgütsel dönüşümü aynı çerçevede değerlendirmelidir.

Kurumsal kaynak planlaması (ERP) sistemleri, finans, insan kaynakları, tedarik zinciri ve müşteri ilişkileri gibi işlevleri bütünsel bir veri tabanı üzerinde bir araya getiren başlıca YBS uygulamalarındandır (Abd Elmonem vd., 2016). Bu bütünlüşme veri tutarlılığını ve işlem hızını artırırken, tek bir güvenlik açığının birden fazla kurumsal işlevi etkileyebileceği bir risk yoğunlaşması yaratır. Dijital dönüşümün teknoloji kadar örgütsel aktörler, yetkinlikler ve çalışma ortamıyla ilişkili olması, ERP dönüşümlerinde güvenlik ve mahremiyetin yalnız teknik kurulum aşamasına bırakılmamasını gerektirir (Nadkarni ve Prügl, 2021).

Kurumların bulut tabanlı ERP çözümlerine yönelmesinde maliyet etkinliği, ölçeklenebilirlik ve bakım kolaylığı belirleyici olurken, veri güvenliği ve mahremiyet kaygıları geçiş kararını sınırlayabilmektedir (Chang, 2020). Güncel sistematik incelemeler, bulut kullanımında teknik zafiyetlerin yanı sıra yönetişim, güven, farkındalık ve düzenleyici uyum sorunlarının da belirleyici olduğunu ortaya koymaktadır (Ukeje vd., 2024). Hizmet sağlayıcısı ile veri sorumlusu arasındaki görevlerin sözleşmelerde açıkça belirlenmesi ve güvenlik gereksinimlerinin sistem mimarisine başlangıç aşamasında dâhil edilmesi gerekir.

YBS aracılığıyla işlenen veri çeşitliliği müşteri işlemleri, çalışan performansı, tedarikçi kayıtları ve pazarlama analitiği gibi

geniş bir alana yayılmaktadır. Dijital dönüşüm, yeni veri kaynaklarını ve bağlantılı iş modellerini kurumsal karar süreçlerine dâhil ederken veri akışlarının sınırlarını da genişletmektedir (Verhoef vd., 2021). Bu genişleme işletmeleri teknik güvenliğin yanında hukuki uyum ve veri yönetişimi sorumluluğuyla karşı karşıya bırakır. Genişleyen veri akışları karşısında veri sahipliği, veri kalitesi, erişim yetkileri ve saklama süreleri kurumsal stratejiyle bağlantılı biçimde yönetilmelidir.

Karar destek sistemleri (KDS) özelinde bakıldığında, yöneticilere sunulan analitik çıktıların güvenilirliği, temel alınan verinin bütünlüğüne doğrudan bağlıdır. Bir bilgi sisteminin siber saldırıya uğraması yalnızca veri gizliliğini değil, aynı zamanda veri bütünlüğünü de tehdit etmekte, bozulan veya değiştirilen veri üzerinden üretilen kararlar, işletmeyi ciddi operasyonel ve finansal risklere maruz bırakabilmektedir (Kott ve Linkov, 2021). Yönetim bilişim sistemlerinin güvenlik mimarisinde yalnızca gizlilik değil, bütünlük ve erişilebilirlik boyutlarının da eşit ağırlıkla ele alınması gerekmektedir.

Yönetici Destek Sistemlerinin (YDS; Executive Information Systems, EIS) üst düzey stratejik kararları desteklemek amacıyla farklı kaynaklardan konsolide ettiği veriler, genellikle kurumun en hassas bilgilerini içermektedir, bu nedenle söz konusu sistemlere yönelik erişim yetkilendirmesinin çok katmanlı biçimde tasarlanması gerekmektedir. Sistemlerin farklı kullanıcı gruplarına farklı yetki düzeyleri tanıyan rol tabanlı erişim kontrolü (RBAC) modelleriyle yapılandırılması, hem iç tehditlerin hem de dış saldırıların etkisini sınırlandıran temel bir güvenlik uygulaması olarak öne çıkmaktadır.

3. DİJİTALLEŞME SÜRECİNDE SİBER GÜVENLİK KAVRAMI

Siber güvenlik, bilgi sistemlerinin gizlilik, bütünlük ve erişilebilirlik ilkeleri çerçevesinde yetkisiz erişim, değiştirme veya tahribata karşı korunmasını ifade eden çok boyutlu bir kavramdır. Sürekli izlenebilir ve ölçümlenebilir veri güvenliğinin sağlanması, kurumsal risk yönetimi modeliyle belirlenen risklerin yönetilmesi ve yeni tehditlerin öngörülebilmesiyle mümkün olmaktadır (Korucu, 2021). Bu bakış açısı, siber güvenliğin yalnızca teknik bir savunma mekanizması değil, aynı zamanda sürekli gözden geçirilmesi gereken dinamik bir yönetim süreci olduğunu ortaya koymaktadır.

Siber dayanıklılık kavramı, saldırı sonrasında sistemlerin operasyonel sürekliliğini koruma ve hızla toparlanma kapasitesini ifade etmekte olup, günümüzde yalnızca önleyici güvenlik önlemleriyle sınırlı kalmayan bütüncül bir yaklaşımı zorunlu kılmaktadır. Siber dayanıklılığın somut biçimde ölçülebilir hâle getirilmesi, kurumların güvenlik yatırımlarının etkinliğini değerlendirebilmesi ve kaynaklarını doğru önceliklendirebilmesi açısından kritik önem taşımaktadır (Kott ve Linkov, 2021). İşletmelerin siber olgunluk düzeylerini periyodik olarak değerlendiren metrik temelli çerçeveler benimsemesi önerilmektedir.

Yapay zekâ destekli güvenlik çözümleri, tehdit tespiti ve müdahale süreçlerinde giderek daha fazla rol üstlenmektedir. Açıklanabilir yapay zekâ yaklaşımları, tehdit avcılığında tespit sonuçlarının güvenlik analistlerince yorumlanmasını kolaylaştırabilir (Kumar vd., 2023). Bununla birlikte bu sistemler yeni kişisel veri işleme faaliyetleri doğurabileceği için veri minimizasyonu, amaçla sınırlılık, ayrımcılık riski ve insan denetimi gibi konular tasarım aşamasında ele alınmalıdır. Çalışan verilerinin yapay zekâ destekli sistemlerle işlenmesi de işverenin

yönetim yetkisi ile çalışanın temel hakları arasında ölçülü bir denge kurulmasını gerektirir (Ses ve Korkusuz, 2025). Bu nedenle yapay zekâ destekli güvenlik uygulamaları, çalışmanın dört bileşenli çerçevesinde teknik kapasite, hukuki uyum, insan denetimi ve kurumsal yönetim gereksinimlerinin kesiştiği bir uygulama alanı olarak değerlendirilmelidir.

İşletmeler açısından siber güvenlik risklerinin kaynağı yalnızca dış saldırganlarla sınırlı değildir, iç tehditler, insan hatası ve süreç eksiklikleri de önemli risk unsurları arasında yer almaktadır. Bilgi sistemlerinin denetiminde siber güvenlik risklerinin kapsamlı biçimde değerlendirilmesi, işletmelerin finansal tablo güvenilirliğinden operasyonel sürekliliğe kadar geniş bir alanı doğrudan etkilemektedir (Öztürk, 2018). Bu bağlamda iç denetim fonksiyonunun bilgi teknolojileri risklerini kapsayacak biçimde genişletilmesi, kurumsal yönetişimin güncel bir gereksinimi olarak öne çıkmaktadır.

Siber güvenliğin yalnız teknik bir sorun olarak görülmesi, çalışan davranışlarını ve kurumsal koşulları ikincil konuma iter. Oysa güncel alan yazını, karar verme süreçleri, güvenlik kültürü, çalışma koşulları ve örgütsel yapıların hem güvenlik açıklarını hem de siber dayanıklılığı biçimlendirdiğini belirtmektedir (Khadka ve Ullah, 2025). Çalışanları yalnızca 'en zayıf halka' olarak nitelemek yerine, güvenli davranışı destekleyen süreçleri ve kullanılabilir kontrolleri geliştirmek daha işlevsel bir yaklaşımdır.

Fidye yazılımı (ransomware) saldırıları, son yıllarda işletmelerin operasyonel sürekliliğini tehdit eden en yaygın siber saldırı türlerinden biri hâline gelmiştir. Bu tür saldırılarda kurumsal veri tabanlarının şifrelenerek erişilemez hâle getirilmesi, yalnızca doğrudan finansal kayıplara değil, aynı zamanda müşteri güveninin sarsılmasına ve itibar kaybına da yol açabilmektedir. Yeni normal dünya düzeninde bilinen siber

saldırı ve veri hırsızlığı yöntemlerine, farklı bilişim platformlarında yaşanan veri güvenliği ihlallerinin eklenmesi, kurumların çok katmanlı ve dinamik bir savunma stratejisi geliştirmesini zorunlu kılmaktadır (Korucu, 2021).

Tedarik zinciri saldırılarında kurum doğrudan hedef alınmak yerine güvendiği yazılım sağlayıcısı, hizmet sunucusu veya iş ortağı üzerinden etkilenmektedir. YBS altyapısının çok sayıda üçüncü taraf bileşeni ve entegrasyonla çalışması saldırı yüzeyini genişletir. Bu risk, tedarikçilerin yalnız hizmet kalitesi bakımından değil, erişim yetkileri, veri işleme rolleri, alt yüklenicileri, olay bildirim süreçleri ve güvenlik olgunluğu bakımından da değerlendirilmesini gerektirir. Bulut ortamlarında hesap verebilirliğin sağlanması, teknik mimari ile sözleşmesel ve yönetsel kontrollerin birlikte kurulmasına bağlıdır (Zaguir vd., 2024).

4. KİŞİSEL VERİLERİN KORUNMASINA İLİŞKİN HUKUKİ ÇERÇEVE: KVKK VE GDPR

4.1. Türkiye'de Kişisel Verilerin Korunması Kanunu

Türkiye'de kişisel verilerin korunmasını isteme hakkı Anayasa'nın 20. maddesinde güvence altına alınmıştır. Bu anayasal temel üzerine kurulan 6698 sayılı Kanun, kişisel verilerin işleme şartlarını, ilgili kişinin haklarını ve veri sorumlusunun yükümlülüklerini düzenlemektedir. Kanun'un 4. maddesindeki hukuka ve dürüstlük kurallarına uygunluk, doğruluk ve güncellik, belirli ve meşru amaç, amaçla bağlantılı ve ölçülü işleme ile gerekli süre kadar muhafaza ilkeleri YBS'deki veri yaşam döngüsünün tamamına uygulanmalıdır. Veri envanteri, erişim yetkileri, saklama süreleri ve imha süreçleri bu ilkelerle uyumlu biçimde tasarlanmalıdır.

Kanun'un 12. maddesi uyarınca veri sorumlusu, kişisel verilerin hukuka aykırı işlenmesini ve erişilmesini önlemek, verilerin muhafazasını sağlamak için gerekli teknik ve idari tedbirleri almakla yükümlüdür. Kişisel Verileri Koruma Kurumu'nun rehberi erişim kontrolü, kullanıcı hesabı yönetimi, şifreleme, ağ güvenliği, yedekleme, kayıtların izlenmesi ve düzenli testler gibi uygulamaları ayrıntılandırmaktadır (KVKK, 2018a). Bu yaklaşım, YBS güvenliğini tek bir ürün veya yazılıma indirgememekte, risk temelli ve süreklilik taşıyan bir yönetim süreci olarak ele almaktadır.

Kanun'un 12. maddesinin beşinci fıkrasında veri ihlalinin en kısa sürede ilgisine ve Kurula bildirilmesi öngörülmektedir. Kişisel Verileri Koruma Kurulunun 24 Ocak 2019 tarihli ve 2019/10 sayılı kararıyla “en kısa sürede” ifadesi, veri sorumlusunun ihlali öğrendiği tarihten itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirim yapması şeklinde yorumlanmıştır (KVKK, 2019).

Veri Sorumluları Sicil Bilgi Sistemi (VERBİS), kayıt yükümlülüğü bulunan veri sorumlularının veri işleme faaliyetlerine ilişkin bilgileri bildirdiği sicil sistemidir. Bununla birlikte kayıt yükümlülüğü bütün veri sorumluları için mutlak değildir. Kişisel Verileri Koruma Kurulunun 2018/32 sayılı kararı istisna tutulan veri sorumlusu gruplarını belirlemiş, 2023/1154 sayılı karar ise istisna kriterlerinden birini güncellemiştir (KVKK, 2018b, 2023). Kayıtlı yükümlü kuruluşların bildirimlerinde işleme amaçları, veri kategorileri, alıcı grupları, azami saklama süreleri, yurt dışına aktarım bilgileri ve alınan güvenlik tedbirleri yer alır. VERBİS bildiriminin güncel bir kişisel veri işleme envanterine dayanması, sicil kaydını biçimsel bir işlem olmaktan çıkarıp veri yönetişiminin parçası hâline getirir.

Çalışan verileri, iş ilişkisinin kurulmasından sona ermesine kadar insan kaynakları bilgi sistemleri, erişim kayıtları, performans değerlendirmeleri ve iş sağlığı süreçleri gibi çok sayıda kanaldan işlenmektedir. Özellikle yapay zekâ destekli izleme ve karar sistemleri, veri minimizasyonu, şeffaflık, ölçülülük ve insan denetimi bakımından yeni riskler doğurmaktadır (Ses ve Korkusuz, 2025). Bu risklerin sınırlandırılması için erişim yetkilerinin görevle sınırlandırılması, saklama sürelerinin belirlenmesi ve çalışanların anlaşılır biçimde aydınlatılması gerekir. Böylece yapay zekâ kullanımı yalnız teknik bir güvenlik veya verimlilik aracı olarak değil, hukuki dayanak, insan hakları üzerindeki etki ve yönetim sorumluluklarıyla birlikte ele alınmaktadır.

4.2. Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR)

Avrupa Birliği'nin 2016/679 sayılı Genel Veri Koruma Tüzüğü 25 Mayıs 2018'den itibaren uygulanmaktadır (Avrupa Parlamentosu ve Avrupa Birliği Konseyi, 2016). GDPR, yerleşim yeri ölçütüne ek olarak Birlik içindeki kişilere mal veya hizmet sunulması ya da davranışlarının izlenmesi gibi koşullarda bölge dışındaki kuruluşlara da uygulanabilir. Tüzük, veri korumasının tasarım aşamasında ve varsayılan ayarlarda gözetilmesini öngörür. Güncel gereksinim mühendisliği çalışmaları da düzenleyici veri koruma gereklerinin yazılım geliştirme yaşam döngüsünün başında tanımlanmasının önemini vurgulamaktadır (Negri-Ribalta vd., 2024).

GDPR uyumu, özellikle sınırlı hukuki ve teknik kaynağa sahip küçük ve orta ölçekli işletmeler için güç bir süreçtir. Veri işleme faaliyetlerinin ve yasal dayanakların belirlenmesi, risklerin değerlendirilmesi, ilgili kişi taleplerinin yönetilmesi, ihlal müdahale süreçlerinin kurulması ve uluslararası aktarımların izlenmesi birlikte yürütülmelidir. Sistematik alan yazını, yalnız

standart edinmenin uygulama yol haritası oluşturmak için yeterli olmayabileceğini, bilgi yönetişimi ile kurumsal mimarinin uyum programını destekleyen başlıca unsurlar arasında bulunduğunu belirtmektedir (Zaguir vd., 2024).

Kamu kurumlarının ve işletmelerin bulut hizmetlerine yönelmesi, veri koruma uyumunu hizmet sağlayıcılar ve alt işleyenler nedeniyle daha karmaşık hâle getirmektedir. Bulut benimsemesine ilişkin sistematik incelemelerde yetkisiz erişim, gizlilik kaybı, farkındalık eksikliği, güven sorunu ve düzenleyici belirsizlikler ortak riskler olarak belirlenmiştir (Ukeje vd., 2024). Bulut tedarikçisi seçimi bu çerçevede veri merkezi konumu, alt hizmet sağlayıcılar, erişim kayıtları, şifreleme, veri taşınabilirliği ve sözleşmenin sona ermesinden sonraki silme süreçlerini kapsamalıdır.

GDPR'de hesap verebilirlik, kuruluşun yalnız kurallara uymasını değil, uyumu kanıtlayabilmesini de gerektirir. İşleme kayıtları, risk değerlendirmeleri, veri koruma etki değerlendirmeleri, ihlal kayıtları ve alınan teknik ve yönetsel tedbirler bu kanıtlama işlevine hizmet eder. Düzenleyici gereksinimlerin bilgi sistemlerine aktarılmasındaki güçlükler, hukuk ve yazılım ekipleri arasında sistemli bir iş birliğini gerekli kılmaktadır (Negri-Ribalta vd., 2024).

KVKK ile GDPR ortak ilkeler taşımakla birlikte kapsam, kurumsal roller, ihlal bildirimi, yaptırımlar ve yurt dışına aktarım mekanizmaları bakımından aynı düzenlemeler değildir. KVKK'nın 9. maddesinde 2024 yılında yapılan değişikliklerle yeterlilik kararı, uygun güvenceler ve arıza aktarım halleri esasına dayanan yeni bir sistem benimsenmiş, standart sözleşmeler ile bağlayıcı şirket kuralları uygun güvence yöntemleri arasında düzenlenmiştir (KVKK, 2024a, 2024b). Uluslararası faaliyet gösteren Türk işletmeleri iki düzenlemenin kesişen ilkelerini

ortak kontrollerle yönetebilir, ancak her düzenlemenin ayrı yükümlülüklerini ayrıca değerlendirmelidir.

Tablo 1. KVKK ve GDPR'nin Temel Unsurlar Açısından Karşılaştırılması

Karşılaştırma unsuru	KVKK	GDPR
Uygulama alanı	Türkiye'deki veri işleme faaliyetleri ve Kanun'un kapsam hükümleri	AB içindeki faaliyetler ile belirli koşullarda bölge dışındaki mal veya hizmet sunumu ve izleme faaliyetleri
Temel ilkeler	Hukuka uygunluk, doğruluk ve güncellik, amaçla sınırlılık, ölçülülük ve gerekli süre kadar saklama	Hukuka uygunluk, adillik ve şeffaflık, amaçla sınırlılık, veri minimizasyonu, doğruluk, saklama sınırı, bütünlük ve hesap verebilirlik
Özel nitelikli veriler	6. madde kapsamında 2024'te güncellenen işleme şartları	9. madde kapsamında özel veri kategorileri ve istisnalar
İhlal bildirimi	Kurulun 2019/10 sayılı kararı uyarınca, ihlalin öğrenilmesinden itibaren gecikmeksizin ve en geç 72 saat içinde Kurula bildirim	Risk doğuran ihlallerde mümkünse 72 saat içinde denetim makamına bildirim
Yurt dışına aktarım	Yeterlilik kararı, uygun güvenceler ve arızı hâller. 2024'te yenilenen sistem	Yeterlilik kararı, uygun güvenceler ve istisnalar
Kurumsal roller	Veri sorumlusu ve veri işleyen. VERBİS için istisnalar bulunur	Veri sorumlusu, veri işleyen ve belirli durumlarda veri koruma görevlisi
Yaptırımlar	Kanun'un 18. maddesindeki idari para cezaları; standart sözleşmenin beş iş günü içinde Kuruma bildirilmemesi hâlinde ayrıca 50.000–1.000.000 TL idari para cezası	Yüzde esaslı üst sınırlar dâhil kademeli idari para cezaları
Tasarım yaklaşımı	Tasarımdan ve varsayılan ayarlardan itibaren mahremiyet açık bir kanun hükmü olarak düzenlenmemiştir. Yaklaşım, genel ilkeler ve veri güvenliği yükümlülüğü üzerinden dolaylı biçimde desteklenir	Tasarımdan ve varsayılan ayarlardan itibaren veri koruma, GDPR'nin 25. maddesinde açık bir yükümlülük olarak düzenlenir

Not: Hukuki dayanaklar: KVKK m. 6, m. 9, m. 12 ve m. 18; Kişisel Verileri Koruma Kurulunun 24.01.2019 tarihli ve 2019/10 sayılı kararı; GDPR m. 9, m. 25, m. 33 ve m. 83. Tablo, bu düzenlemeler temel alınarak yazar tarafından sentezlenmiştir.

5. YÖNETİM BİLİŞİM SİSTEMLERİNDE VERİ MAHREMİYETİ RİSKLERİ

5.1. Bulut Bilişim ve ERP Sistemlerinde Güvenlik

Bulut bilişim işletmelere ölçeklenebilirlik, esneklik ve maliyet avantajı sağlarken, veri üzerindeki fiilî kontrolün hizmet sağlayıcılarla paylaşılması yeni güvenlik ve mahremiyet riskleri doğurur. Sistematik incelemeler, bulut ortamlarındaki risklerin yalnız teknik açıklarla sınırlı olmadığını, yönetim, güven, farkındalık ve düzenleyici uyum sorunlarını da kapsadığını belirtmektedir (Ukeje vd., 2024). Koruma düzeninde veri sınıflandırma, güçlü kimlik doğrulama, erişim kontrolü, şifreleme, kayıt izleme, yedekleme ve olay müdahalesi bütünlük biçimde kurulmalıdır.

ERP sistemlerinin bulut ortamına taşınması sürecinde veri güvenliği kaygıları, organizasyonların geçiş kararını erteleme ya da hibrit modelleri tercih etme eğilimini artıran başlıca faktörler arasında yer almaktadır. Organizasyonların bulut ERP sistemlerine geçiş kararında hem kolaylaştırıcı hem de engelleyici faktörlerin bir arada değerlendirilmesi gerekmekte, veri güvenliği ve mahremiyet kaygıları bu değerlendirmede belirleyici bir ağırlığa sahip olmaktadır (Chang, 2020). Bulut ERP tedarikçisi seçiminde sağlayıcının güvenlik sertifikasyonları ve veri merkezi konumlarının değerlendirilmesi kritik önem taşımaktadır.

Kurumsal sistemlerde veri kalitesi ile siber güvenlik arasındaki ilişki, alan yazında giderek daha fazla dikkat çeken bir konu hâline gelmiştir, düşük veri kalitesi, güvenlik açıklarının tespit edilmesini zorlaştırabilmekte ve yanlış karar alma risklerini artırabilmektedir. Bulut ERP sistemlerinde siber güvenlik ve veri kalitesinin birlikte ele alınması, organizasyonların hem operasyonel güvenilirliğini hem de mevzuat uyumluluğunu güçlendiren bütüncül bir yaklaşım olarak değerlendirilmektedir.

Bu bağlamda veri yönetişimi süreçlerinin güvenlik politikalarıyla entegre biçimde tasarlanması önerilmektedir.

Kurumsal ağların bölümlere ayrılması (segmentasyon), kişisel verilerin işlendiği ağ alanlarının diğer kurumsal kaynaklardan izole edilmesini sağlayarak olası bir ihlalin etkisini sınırlandırmaya yardımcı olmaktadır. Kişisel verilerin işlendiği ağ bölümünün ayrı biçimde yapılandırılması hâlinde, güvenlik kaynaklarının tüm ağ yerine yalnızca bu sınırlı alanın korunmasına yoğunlaştırılabileceği vurgulanmaktadır (KVKK, 2018a). Bu teknik yaklaşım, özellikle çok uluslu ya da çok şubeli işletmelerin veri güvenliği mimarisinde önceliklendirilmesi gereken bir uygulama olarak öne çıkmaktadır.

Kimlik ve erişim yönetimi (Identity and Access Management), bulut tabanlı yönetim bilişim sistemlerinde en kritik güvenlik bileşenlerinden birini oluşturmaktadır. Kaba kuvvet saldırılarına karşı parola girişi deneme sayısının sınırlandırılması, düzenli parola değişiminin sağlanması ve yönetici yetkisinin yalnızca gerekli durumlarda etkinleştirilmesi, temel ancak etkili koruma önlemleri arasında sayılmaktadır (KVKK, 2018a). Çok faktörlü kimlik doğrulama (MFA), erişim için parola gibi tek bir unsurla yetinmeyip en az iki bağımsız doğrulama unsurunun kullanılmasını sağlayarak özellikle ayrıcalıklı ve uzaktan erişimlerde hesap ele geçirme riskini azaltan tamamlayıcı bir IAM kontrolüdür. Bunlara ek olarak, kurumdan ayrılan çalışanların hesaplarının zaman kaybetmeksizin devre dışı bırakılması, yetkisiz erişim risklerinin azaltılmasında belirleyici bir uygulamadır.

Şifreleme, hem durağan hem de aktarım hâlindeki veriler için temel bir koruma katmanıdır. Bununla birlikte şifrelemenin etkinliği algoritma seçiminin yanında anahtarların üretimi, saklanması, yenilenmesi, erişim yetkileri ve imha süreçlerinin güvenliğine bağlıdır. Bulut ERP hizmetinde hangi verinin kim

tarafından şifrelendiği, anahtarların kimin denetiminde bulunduğu ve hizmet sona erdiğinde verinin nasıl silineceği sözleşmede açıklanmalıdır. Tasarımdan itibaren mahremiyet yaklaşımı, bu kararların sistem devreye alındıktan sonra değil, mimari tasarım sırasında alınmasını gerektirir (Bal vd., 2026).

Uzaktan ve hibrit çalışma, kurumsal ağın fiziksel sınırlarını belirsizleştirdiği için çevre güvenliğine dayalı geleneksel yaklaşımın etkisini azaltmıştır. Sıfır güven mimarisi, kullanıcıyı veya cihazı ağ içindeki konumuna dayanarak güvenilir saymamakta, her erişim isteğinin kimlik, cihaz durumu, bağlam ve yetki bakımından doğrulanmasını esas almaktadır (Kang vd., 2023). Bu yaklaşım tek bir ürün değil, kimlik yönetimi, en az ayrıcalık, ağ bölümlendirme, sürekli izleme ve yönetim bileşenlerinden oluşan kurumsal bir dönüşümdür. Uygulamanın başarısı teknik mimari kadar üst yönetim desteğine, yetkinliğe ve aşamalı bir olgunluk planına bağlıdır (Yeoh vd., 2023).

5.2. Çalışan Davranışı ve İçeriden Gelen Tehditler

Çalışanlar güvenlik olaylarında önemli bir rol oynamakla birlikte onları doğrudan 'en zayıf halka' olarak tanımlamak sorunu tek boyuta indirger. Güvenli olmayan davranışlar çoğu zaman arayüz tasarımı, iş yükü, eğitim niteliği, örgütsel iklim ve yönetim tercihleriyle birlikte şekillenir (Khadka ve Ullah, 2025). Siber güvenlik kültürüne ilişkin uygulamalar da politika, iletişim, eğitim, çalışan katılımı ve yönetim desteğinin birbirini tamamlayan bir düzen içinde ele alınmasını gerektirir (Alshaikh, 2020). Etik olmayan veya ihmalkâr çalışan davranışları ağ ve uygulama kötüye kullanımı, riskli internet kullanımı, güvenlik kurallarının ihlali ve yetersiz erişim kontrolü gibi kategoriler altında incelenebilir (Chu ve So, 2020). Etkili risk yönetimi, çalışan sorumluluğu ile kurumun güvenli çalışma koşulları oluşturma yükümlülüğünü birlikte ele almalıdır.

Güvenlik farkındalık programları ile yaptırım algısının farklı davranış türlerinde aynı sonucu üretmemesi, tek tip bir müdahale stratejisinin sınırlı kalabileceğini düşündürmektedir (Chu ve So, 2020). Farkındalık, bilgi ve güvenli davranış birbiriyle ilişkili olmakla birlikte aynı kavramlar değildir. Kullanıcının tehdidi tanıması, koruyucu aracı doğru kullanacağı anlamına gelmeyebilir (Zwilling vd., 2022). Kurumların eğitim programlarını davranış temelli risk analizi, uygulamalı ölçüm ve düzenli geri bildirimle desteklemesi, kaynakların daha etkili kullanılmasına katkı sağlayabilir.

Güvenlik kültürü ile istihdam ilişkisinin çalışanların güvenlik uyum davranışlarını nasıl şekillendirdiği üzerine yapılan araştırmalarda, örgütsel güvenlik kültürünün ve çalışan-işveren ilişkisinin kalitesinin, resmi politika ve prosedürlerden bağımsız olarak güvenlik uyumunu doğrudan etkilediği belirlenmiştir (D'Arcy ve Greene, 2014). Bu sonuç, güvenlik yönetiminin yalnızca kural koyucu bir yaklaşımla değil, çalışan bağlılığını ve güven ilişkisini gözetken bir örgüt kültürü inşasıyla desteklenmesi gerektiğine işaret etmektedir.

İçeriden kaynaklanan risklerin yönetiminde çalışanların güvenlik olaylarını bildirmekten çekinmesi önemli bir engeldir. Cezalandırılma korkusu, bildirim kanalının bilinmemesi veya karmaşık prosedürler olayların gecikmesine yol açabilir. Bildirim mekanizmaları kolay erişilebilir ve öğrenmeyi teşvik eden bir yapıda kurulmalıdır. İnsan faktörünü davranış, karar verme ve örgütsel kültürle birlikte ele alan çalışmalar, bireysel eğitimin ancak kurumsal süreçler ve yönetim desteğiyle tamamlandığında kalıcı sonuç üretebileceğini belirtmektedir (Khadka ve Ullah, 2025).

Sosyal mühendislik saldırıları, teknik açıklardan çok güven, acelecilik ve otorite algısı gibi insani özellikleri kullanır. Kimlik avı e-postaları, sahte destek çağrıları ve hedef odaklı

kimlik avı girişimleri bu saldırıların yaygın örnekleridir. Eğitimlerin yalnız bilgi aktarımına dayanmaması, çalışanların gerçekçi senaryolarla güvenli davranışı uygulamasına imkân vermesi gerekir. Simülasyon sonuçları çalışanları cezalandırmak için değil, riskli iş akışlarını ve ek desteğe ihtiyaç duyulan alanları belirlemek için kullanılmalıdır (Khadka ve Ullah, 2025).

6. KURUMSAL BİLGİ GÜVENLİĞİ YÖNETİMİ: STANDARTLAR VE UYGULAMALAR

6.1. ISO/IEC 27001 ve Risk Yönetimi Çerçeveleri

ISO/IEC 27001, kurumların bilgi güvenliği yönetim sistemini kurması, uygulaması, sürdürmesi ve sürekli iyileştirmesi için risk temelli bir çerçeve sunmaktadır. Güncel ISO/IEC 27001:2022 sürümü varlıkların, tehditlerin, zafiyetlerin ve kontrollerin kuruluşun bağlamı içinde değerlendirilmesini gerektirir. Sertifikasyon, tek başına KVKK veya GDPR uyumunu kanıtlamaz. Bununla birlikte risk değerlendirmesi, sorumlulukların belirlenmesi, dokümantasyon, iç denetim ve sürekli iyileştirme süreçleri hukuki uyumu destekleyebilir. Standart ile mevzuat arasındaki ilişkinin bir eşdeğerlik değil, tamamlayıcılık ilişkisi olduğu gözetilmelidir (Zaguir vd., 2024).

COBIT 2019, kurumsal bilgi ve teknolojinin yönetişimi ile yönetimini işletme hedefleriyle ilişkilendiren güncel bir çerçeve sunmaktadır. Çekirdek modelde beş alan altında kırk yönetişim ve yönetim hedefi bulunmakta, bilgi güvenliği, bulut bilişim ve güncel teknoloji eğilimleri odak alanlarıyla ele alınabilmektedir (ISACA, 2018). COBIT 2019'un ISO/IEC 27001 ile birlikte kullanılması, güvenlik kontrollerinin kurumsal hedefler, sorumluluklar, performans göstergeleri ve güvence süreçleriyle ilişkilendirilmesine yardımcı olabilir. Bununla birlikte her iki çerçeve de somut KVKK ve GDPR

yükümlülüklerinin ayrıca değerlendirilmesi gereğini ortadan kaldırmaz.

Kurumsal risk yönetimi, bulut tabanlı sistemlerde risklerin tanımlanması, değerlendirilmesi, azaltılması ve sürekli izlenmesini kapsar. Bulut ortamındaki yapılandırmalar, kullanıcı hesapları, yazılım bileşenleri ve alt hizmet sağlayıcılar zaman içinde değişebildiğinden tek seferlik risk değerlendirmesi yeterli değildir. Risk kaydı, varlık envanteri, zafiyet yönetimi, olay kayıtları ve tedarikçi değerlendirmeleri birbirini besleyen bir izleme düzeni içinde yürütülmelidir (Ukeje vd., 2024).

Bilgi sistemlerinin denetiminde siber güvenlik risklerine yönelik bütüncül bir denetim modeli önerisi, risklerin yalnızca bilgi işlem birimi tarafından değil, iç denetim, risk yönetimi ve üst yönetim işbirliğiyle ele alınmasının önemine dikkat çekmektedir (Öztürk, 2018). Bu yaklaşım, bilgi güvenliğinin izole bir teknik fonksiyon olarak değil, kurumsal yönetişimin bütünlük bir parçası olarak konumlandırılması gerektiğini ortaya koymaktadır.

Olay müdahale planlaması (incident response planning), bir güvenlik ihlali gerçekleştiğinde kurumun ne hızla ve ne kadar etkin biçimde tepki verebileceğini belirleyen kritik bir hazırlık sürecidir. Bilişim sisteminin çökmesi, kötü niyetli yazılım bulaşması, hizmet dışı bırakma saldırısı ya da gizlilik ve bütünlüğü bozan ihlaller gibi istenmeyen olaylarda, delillerin toplanması ve güvenli biçimde saklanması gerekmektedir (KVKK, 2018a). Bu süreçlerin önceden tanımlanmış rol ve sorumluluklarla desteklenen bir olay müdahale planına dayandırılması, kriz anındaki karar verme hızını ve etkinliğini artırmaktadır.

Güvenlik açığı taramaları ve sızma testleri, kurumsal bilgi sistemlerinin bilinen zafiyetlere karşı ne ölçüde dayanıklı olduğunu ölçmeye yönelik proaktif değerlendirme araçlarıdır.

Güvenlik yazılımı mesajlarının, erişim kontrolü kayıtlarının ve diğer raporlama araçlarının düzenli biçimde kontrol edilmesi ile bu sistemlerden gelen uyarılar üzerine zamanında harekete geçilmesi gerektiği vurgulanmakta, düzenli zafiyet taramaları ve sızma testlerinin yapılması önerilmektedir (KVKK, 2018a). Bu değerlendirmelerin sonuçlarına göre güvenlik önceliklerinin periyodik olarak gözden geçirilmesi, kurumsal risk profilinin güncel tutulmasını sağlamaktadır.

6.2. Güvenlik Kültürü ve Farkındalık Eğitimleri

Kurumsal güvenlik kültürü, teknik kontrollerin günlük çalışma pratiklerinde karşılık bulmasını sağlayan tamamlayıcı bir unsurdur. Farkındalık eğitimleri düzenli ve role göre uyarlanmış biçimde tasarlanmalı, çalışanların güncel tehditleri tanınması ve şüpheli durumları doğru kanallardan bildirmesi sağlanmalıdır. Güvenlik kültürünün kalıcı hâle gelmesi, yönetim desteği, açık iletişim, çalışan katılımı ve uygulamaların düzenli değerlendirilmesiyle mümkündür (Alshaikh, 2020). Böylece çalışan yalnız risk kaynağı olarak değil, kurumsal dayanıklılığın etkin bir bileşeni olarak konumlandırılabilir.

Farkındalık programlarında aynı içeriğin bütün çalışanlara sunulması yerine görev, erişim düzeyi ve karşılaşılan tehditler dikkate alınmalıdır. İnsan kaynakları personeli çalışan verileri, finans birimi ödeme dolandırıcılığı, sistem yöneticileri ise ayrıcalıklı hesaplar bakımından farklı risklere maruz kalır. Farkındalık ve bilgi düzeyinin güvenli davranışla ilişkili olması, eğitim etkinliğinin yalnız katılım oranıyla ölçülemeyeceğini ortaya koymaktadır (Zwilling vd., 2022). Simülasyon sonuçları, olay bildirim süresi, tekrar eden hata örüntüleri ve güvenli davranış göstergeleri birlikte izlenmelidir.

Üniversite kütüphaneleri örneğinde yürütülen bir çalışma, kişisel verilerin korunmasına yönelik farkındalığın yalnızca özel sektör kuruluşlarıyla sınırlı olmadığını, kamu hizmeti sunan bilgi

merkezlerinin de kullanıcı verilerinin gizliliği, bütünlüğü ve kullanılabilirliğini gözeten politikalar geliştirmesi gerektiğini ortaya koymaktadır (Henkoğlu ve Uçak, 2015). Bu bulgu, veri mahremiyeti yönetiminin sektör bağımsız bir kurumsal sorumluluk alanı olarak ele alınması gerektiğini göstermektedir.

Güvenlik kültürünün üst yönetim tarafından açıkça desteklenmesi ve kaynak tahsisinde önceliklendirilmesi, farkındalık programlarının sürdürülebilirliği açısından belirleyici bir faktördür. Örgütsel güvenlik ikliminin çalışanların güvenlik uyum davranışlarına doğrudan yansıdığı gösterildiğinden (D'Arcy ve Greene, 2014), yöneticilerin güvenlik konusundaki söylem ve uygulamaları arasındaki tutarlılık, çalışanların güvenlik önlemlerini içselleştirme düzeyini doğrudan etkilemektedir.

7. TÜRKİYE'DE İŞLETMELERDE KVKK UYUMLULUĞU: UYGULAMA SORUNLARI VE ÖNERİLER

Türkiye'de özellikle küçük ve orta ölçekli işletmeler, KVKK uyumunun hukuki, teknik ve idari bileşenlerini aynı anda yönetmekte güçlük yaşayabilir. Veri işleme envanterinin hazırlanması, aydınlatma yükümlülüğü, işleme şartlarının belirlenmesi, ilgili kişi başvurularının yönetimi, saklama ve imha süreçleri ile güvenlik tedbirleri farklı uzmanlıkların birlikte çalışmasını gerektirir. GDPR uyumuna ilişkin güncel incelemeler de sınırlı kaynak, uzmanlık eksikliği ve uygulama yol haritası yetersizliğinin ortak sorunlar olduğunu belirtmektedir (Zaguir vd., 2024). Uyum programı kuruluşun ölçeğine ve risk profiline göre önceliklendirilmelidir.

KVKK uygulamasındaki güncel dönüşüm yalnız mevzuat metninin değiştirilmesiyle sınırlı değildir. 7499 sayılı Kanun ile özel nitelikli kişisel verilerin işlenmesini düzenleyen 6. madde,

yurt dışına aktarımı düzenleyen 9. madde ve kabahatlere ilişkin 18. madde değiştirilmiş, ayrıca geçiş hükmü getirilmiştir. Değişiklikler 1 Haziran 2024 tarihinde yürürlüğe girmiş, 9. maddenin değişiklikten önceki birinci fıkrasının yeni düzenlemeyle birlikte 1 Eylül 2024 tarihine kadar uygulanmasına imkân tanınmıştır (KVKK, 2024a). Bu değişiklikler işletmelerin işleme envanterlerini, hukuki dayanaklarını, sözleşmelerini ve bilgi sistemi akışlarını yeniden değerlendirmesini gerektirmiştir. Bu durum, hukuki uyum kararlarının doğrudan YBS mimarisi ve tedarikçi yönetimiyle ilişkilendirilmesi gerektiğini açıkça ortaya koymaktadır.

İşletmelerin karşılaştığı başlıca sorunlardan biri, kişisel verinin hangi sistemlerde, hangi amaçla ve ne kadar süreyle tutulduğunun eksiksiz belirlenememesidir. Veri keşfi araçları bu süreci destekleyebilir, ancak otomatik keşif sonuçları tek başına hukuki nitelendirme yapamaz. Teknik tarama, süreç sahipleriyle görüşme ve kayıtların örneklenmesi birlikte yürütülmelidir. Elde edilen envanter, VERBİS bildirimi gereken durumlarda bu bildirimin dayanağını oluşturmalı ve sistem değişiklikleriyle birlikte güncellenmelidir (Athier Olca ve Can, 2024; KVKK, 2018b, 2023).

Küçük ve orta ölçekli işletmelerin uyum maliyetlerini karşılayabilme kapasitesi, büyük ölçekli kurumlara kıyasla belirgin biçimde sınırlıdır. KOBİ'lerin KVKK uyum süreçlerinde tüm gereklilikleri aynı anda karşılamaya çalışmak yerine, risk düzeyine göre önceliklendirilmiş kademeli bir uygulama takvimi izlemesi daha gerçekçi bir strateji olarak değerlendirilmektedir. Öncelikle en yüksek hacimde ve en hassas nitelikte kişisel veri işlenen süreçlerin güvence altına alınması, sınırlı kaynakların etkin biçimde kullanılmasına katkı sağlayacaktır.

Sektörel farklılıklar, kişisel veri işleme riskinin niteliğini doğrudan etkiler. Sağlık, finans ve eğitim gibi alanlarda özel

nitelikli veriler, yoğun izleme faaliyetleri veya yüksek etkili karar süreçleri bulunabilir. Bu kuruluşlar KVKK'nın 6. maddesinde 2024 yılında yapılan değişiklikleri, sektörel düzenlemeleri ve Kişisel Verileri Koruma Kurulu kararlarını birlikte değerlendirmelidir (Turan Başara, 2024). Güvenlik tedbirleri yalnız sektör adına göre değil, işlenen verinin niteliği, hacmi, erişim çevresi ve ihlalin kişiler üzerindeki olası etkisine göre belirlenmelidir.

Tedarikçi ve iş ortağı yönetimi, KVKK uyumunun kritik bir boyutudur. Kişisel veri işleyen üçüncü taraflarla yapılan sözleşmelerde tarafların rolleri, işleme amacı, güvenlik tedbirleri, alt yükleniciler, olay bildirimini, denetim hakkı, saklama süresi ve hizmet sonunda silme veya iade şartları açıklanmalıdır. Yurt dışındaki hizmet sağlayıcılara veri aktarılıyorsa KVKK'nın güncel 9. maddesindeki aktarım mekanizmaları ayrıca incelenmelidir. Standart sözleşme kullanılması, veri akış haritasında veri aktaran ile veri alıcısının, aktarım ülkelerinin, veri kategorilerinin, erişim yetkilerinin ve alt işleyenlerin açık biçimde tanımlanmasını gerektirir. Sözleşmedeki güvenlik, saklama, silme ve olay bildirim hükümleri de YBS yapılandırmaları ve denetim kayıtlarıyla uygulanabilir hâle getirilmelidir. İmzalanan standart sözleşmenin beş iş günü içinde Kuruma bildirilmesi gerekir. Bildirim fiziki olarak, kayıtlı elektronik posta (KEP) üzerinden veya Kurul tarafından kullanıma sunulan Standart Sözleşme Bildirim Modülü aracılığıyla gerçekleştirilebilir (KVKK, 2024b, 2024c). Bu bildirim yükümlülüğünün yerine getirilmemesi, Kanun'un 18. maddesi uyarınca veri sorumlusu veya veri işleyen hakkında 50.000 Türk lirasından 1.000.000 Türk lirasına kadar idari para cezasına yol açabilir (KVKK, 2024a).

Uygulamayı somutlaştırmak amacıyla temsili bir KOBİ senaryosu düşünülebilir. Çalışan ve müşteri kayıtlarını yurt dışındaki bir bulut hizmetinde tutan çevrimiçi perakende

işletmesi, ilk aşamada insan kaynakları, satış, erişim kaydı ve müşteri iletişimi verilerinin akışını envantere işlemelidir. İşleme şartları ve saklama süreleri belirlendikten sonra veri aktaran ile veri alıcısının rolleri, aktarım ülkesi, alt işleyenler ve erişim yetkileri veri akış haritasında gösterilmelidir. Uygun aktarım mekanizması seçilirken standart sözleşme gerekiyorsa beş iş günlük bildirim takvimi sorumlu birime atanmalı ve bildirim için fiziki yol, KEP veya Standart Sözleşme Bildirim Modülü kullanılmalı, teknik tarafta çok faktörlü kimlik doğrulama, rol tabanlı erişim, şifreleme, olay kayıtları ve hizmet sonundaki silme süreci yapılandırılmalıdır. Bu senaryo, Tablo 2'deki aşamaların hukuk, bilgi işlem, satın alma ve süreç sahiplerinin ortak çalışmasıyla uygulanabileceğini görünür kılmaktadır. Bu temsili senaryo, alan yazını ve güncel mevzuattan hareketle bu bölüm kapsamında oluşturulan uygulama örneğidir ve çalışmanın kavramsal çerçevesini işletme düzeyindeki somut adımlarla ilişkilendirmeyi amaçlamaktadır.

Yapılan değerlendirmeler doğrultusunda işletmelerin KVKK uyumunu tek seferlik bir belge hazırlama projesi olarak değil, sürekli izlenen bir yönetim süreci olarak ele alması gerekir. Veri koruma sorumlulukları hukuk ve bilgi işlem birimleriyle sınırlandırılmamalı, insan kaynakları, satın alma, pazarlama, iç denetim ve üst yönetimi kapsayan bir yapı kurulmalıdır. Uygulama takvimi veri hacmi, hassasiyet, erişim çevresi ve ilgili kişiler üzerindeki olası etki esas alınarak önceliklendirilmelidir. ISO/IEC 27001 gibi standartlar risk yönetimi ve sürekli iyileştirme bakımından destekleyici araçlar olarak kullanılmalı, ancak mevzuata uyumun yerine geçtiği varsayılmamalıdır. Çalışan eğitimleri de güncel tehdit senaryolarına ve görev bazlı risklere göre düzenli olarak yenilenmelidir.

Tablo 2. İşletmeler İçin KVKK Uyum Yol Haritası

Aşama	Temel işlem	Sorumlu birimler	YBS'ye teknik yansımaları	Üretilmesi gereken kayıt
1. Veri keşfi	Sistemlerdeki kişisel verilerin ve veri akışlarının belirlenmesi	Bilgi işlem ve süreç sahipleri	Veri keşfi, sınıflandırma ve akış haritası	Kişisel veri işleme envanteri
2. Hukuki değerlendirme	Amaç, işleme şartı, saklama süresi ve aktarım dayanağının belirlenmesi	Hukuk ve süreç sahipleri	İşleme kuralları ile saklama sürelerinin sisteme tanımlanması	Hukuki dayanak ve saklama kaydı
3. Risk analizi	Veri ve sistem risklerinin ölçülerek önceliklendirilmesi	Bilgi güvenliği ve risk yönetimi	Erişim, şifreleme, yedekleme ve kayıt kontrolleri	Risk değerlendirme ve kontrol planı
4. Tedarikçi kontrolü	Veri işleyenlerin, alt işleyenlerin ve yurt dışı aktarımların incelenmesi	Satın alma, hukuk ve bilgi işlem	Aktarım noktaları, roller ve yetkilerin sistemde belgelenmesi	Sözleşme, aktarım ve tedarikçi denetim kaydı
5. Olay yönetimi	İhlal tespiti, müdahale, bildirim ve delil saklama süreçlerinin kurulması	Olay müdahale ekibi ve hukuk	Log, uyarı, erişim kesme ve bildirim mekanizmaları	Olay ve ihlal kayıtları
6. İzleme ve iyileştirme	Envanterin, kontrollerin ve eğitimlerin periyodik olarak güncellenmesi	İç denetim ve üst yönetim	Sürekli izleme ve performans göstergeleri	Periyodik uyum ve iyileştirme raporu

Not: Tablo, bu bölümde incelenen KVKK yükümlülükleri, bilgi güvenliği kontrolleri ve kurumsal yönetim ilkelerinin uygulamaya aktarılması amacıyla yazar tarafından oluşturulan özgün bir sentezdir.

8. SONUÇ

Çalışma, yönetim bilişim sistemlerinde siber güvenlik ve veri mahremiyetinin birbirinden ayrı yönetilemeyeceğini açıklayan kavramsal bir çerçeve sunmuştur. Bulut bilişim, ERP, yapay zekâ ve üçüncü taraf entegrasyonları işletmelere hız ve ölçek kazandırırken kişisel verinin daha geniş ve değişken bir ekosistemde işlenmesine yol açmaktadır. YBS güvenliği bu açıdan yalnız sistemlerin saldırılara karşı korunmasıyla sınırlı değildir. Verinin hangi amaçla işlendiğinin, kimlerce erişilebildiğinin, nerede saklandığının, ne zaman silineceğinin ve ihlal hâlinde nasıl müdahale edileceğinin de yönetilmesini kapsar.

Yapılan değerlendirmeler, etkili YBS güvenliğinin dört bileşenin birlikte işletilmesine bağlı olduğunu göstermiştir. Bunlar teknik güvenlik, hukuki uyum, insan faktörü ve kurumsal yönetişimdir. Şifreleme, erişim kontrolü ve izleme gibi teknik önlemler hukuki dayanak, şeffaflık ve veri minimizasyonu ilkeleriyle desteklenmelidir. Çalışanların güvenli davranışı ise kullanılabilir kontroller, görev bazlı eğitim, açık bildirim kanalları ve yönetim desteğiyle güçlendirilmelidir. Risklerin sahipliği ve denetimi üst yönetim düzeyinde tanımlanmadığında bu unsurların kalıcı bir sisteme dönüşmesi güçleşir.

KVKK ile GDPR arasındaki ortak ilkeler, işletmelere bazı kontrolleri bütünsel biçimde kurma imkânı verir. Bununla birlikte iki düzenlemenin kapsamı, veri ihlali bildirimleri, kurumsal roller, yaptırımlar ve yurt dışına aktarım mekanizmaları aynı değildir. Özellikle KVKK'nın 2024 değişiklikleri sonrasında özel nitelikli verilerin işleme şartları, uluslararası veri akışları ve standart sözleşmelere ilişkin bildirim ile yaptırım hükümleri güncel kurallara göre yeniden değerlendirilmelidir. ISO/IEC 27001:2022 bu süreçte risk yönetimi, kayıt ve sürekli iyileştirme disiplini kazandırabilir, ancak tek başına hukuki uyumun kanıtı sayılamaz.

Çalışmanın sınırları, benimsenen kavramsal sentez yaklaşımından kaynaklanmaktadır. Değerlendirmeler ampirik işletme verilerine dayanmamakta ve önerilen uygulama adımları farklı sektörlerde doğrudan sınanmamaktadır. Sağlık, finans, eğitim ve elektronik ticaret gibi alanların veri türleri, düzenleyici yükümlülükleri ve risk düzeyleri farklı olduğundan öneriler bütün işletmelere aynı biçimde genellenemez. Sunulan çerçeve, kuruluşun ölçeği, sektörü, veri işleme amaçları ve risk profili dikkate alınarak uyarlanmalıdır.

Gelecek araştırmalarda Türkiye'deki işletmelerin KVKK uyum olgunluğu sektör ve ölçek temelinde ampirik olarak

karşılaştırılabilir. Yapay zekâ destekli çalışan izleme ve karar sistemlerinin hukuki ve örgütsel etkileri, sıfır güven mimarisinin KOBİ'lerde uygulanabilirliği ve 2024 sonrası yurt dışına aktarım mekanizmalarının kurumsal bilgi sistemlerine etkisi de araştırılmaya açıktır. Bu çalışmalar, teknik güvenlik ile veri koruma hukukunu aynı analitik çerçevede ele aldığı anda hem alan yazına hem de uygulamaya daha güçlü katkı sunacaktır.

KAYNAKÇA

- 6698 sayılı Kişisel Verilerin Korunması Kanunu. (2016, 7 Nisan). *Resmî Gazete* (Sayı: 29677).
- Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98, 102003. <https://doi.org/10.1016/j.cose.2020.102003>
- Athier Olca, E., & Can, Ö. (2024). KVKK kavramlarının modellenmesi için ontoloji tabanlı bir yaklaşım. *Dokuz Eylül Üniversitesi Mühendislik Fakültesi Fen ve Mühendislik Dergisi*, 26(76), 173–191. <https://doi.org/10.21205/deufmd.2024267620>
- Avrupa Parlamentosu ve Avrupa Birliği Konseyi. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88. https://publications.europa.eu/resource/cellar/3e485e15-11bd-11e6-ba9a-01aa75ed71a1.0006.03/DOC_1 Erişim tarihi: 02.09.2026
- Bal, S., Canayaz, E., & Kabataş Soyer, Z. B. (2026). Taşınabilir tıbbi cihazların mühendislik tasarımında tasarıma dayalı gizlilik yaklaşımı: KVKK ve GDPR perspektifinde veri güvenliği. *Bilişim Teknolojileri Dergisi*, 19(2), 105–112. <https://doi.org/10.17671/gazibtd.1788711>
- Chang, Y. (2020). What drives organizations to switch to cloud ERP systems? The impacts of enablers and inhibitors. *Journal of Enterprise Information Management*, 33(3), 600–626. <https://doi.org/10.1108/JEIM-06-2019-0148>
- Chu, A. M. Y., & So, M. K. P. (2020). Organizational information security management for sustainable information systems: An unethical employee information security behavior

- perspective. *Sustainability*, 12(8), 3163.
<https://doi.org/10.3390/su12083163>
- D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, 22(5), 474–489.
<https://doi.org/10.1108/IMCS-08-2013-0057>
- Abd Elmonem, M. A., Nasr, E. S., & Geith, M. H. (2016). Benefits and challenges of cloud ERP systems: A systematic literature review. *Future Computing and Informatics Journal*, 1(1–2), 1–9.
<https://doi.org/10.1016/j.fcij.2017.03.003>
- Henkoğlu, T., & Uçak, N. Ö. (2015). Üniversite kütüphanelerinde kişisel verilerin korunması. *Bilgi Dünyası*, 16(1), 45–74.
<https://doi.org/10.15612/BD.2015.472>
- ISACA. (2018). *COBIT 2019 framework: Introduction and methodology*. ISACA.
<https://www.isaca.org/store2/product/CB19FIM>
- Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and application of zero trust security: A brief survey. *Entropy*, 25(12), 1595.
<https://doi.org/10.3390/e25121595>
- Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security*, 24. <https://doi.org/10.1007/s10207-025-01032-0>
- Kişisel Verileri Koruma Kurumu. (2018a). *Kişisel veri güvenliği rehberi (Teknik ve idari tedbirler)*. Erişim Tarihi: 30.08.2026.
https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf

- Kişisel Verileri Koruma Kurumu. (2018b). *Veri Sorumluları Siciline kayıt yükümlülüğünden istisna tutulacak veri sorumlularına ilişkin 2 Nisan 2018 tarihli ve 2018/32 sayılı karar*. Erişim Tarihi: 25.08.2026. <https://www.kvkk.gov.tr/Icerik/4233/2018-32>
- Kişisel Verileri Koruma Kurumu. (2019). Kişisel veri ihlali bildirim usul ve esaslarına ilişkin Kişisel Verileri Koruma Kurulunun 24.01.2019 tarihli ve 2019/10 sayılı kararına ilişkin duyuru. Erişim Tarihi: 26.08.2026. <https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi>
- Kişisel Verileri Koruma Kurumu. (2023). *Veri Sorumluları Siciline kayıt yükümlülüğüne ilişkin istisna kriterinde değişiklik yapılması hakkında 6 Temmuz 2023 tarihli ve 2023/1154 sayılı karar*. Erişim Tarihi: 26.08.2026. <https://www.kvkk.gov.tr/Icerik/7647/2023-1154>
- Kişisel Verileri Koruma Kurumu. (2024a). *6698 sayılı Kişisel Verilerin Korunması Kanunu'nda yapılan değişiklikler hakkında kamuoyu duyurusu*. Erişim Tarihi: 26.08.2026. <https://www.kvkk.gov.tr/Icerik/7834/6698-Sayili-Kisisel-Verilerin-Korunmasi-Kanununda-Yapilan-Degisiklikler-Hakkinda-Kamuoyu-Duyurusu>
- Kişisel Verileri Koruma Kurumu. (2024b). *Kişisel verilerin yurt dışına aktarılması rehberi*. <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/13711235-abb6-4b17-9a6b-0a68c1ad86c5.pdf>
- Kişisel Verileri Koruma Kurumu. (2024c). Standart Sözleşme Bildirim Modülü hakkında kamuoyu duyurusu. Erişim Tarihi: 26.08.2026. <https://www.kvkk.gov.tr/Icerik/8043/Standart-Sozlesme-Bildirim-Modulu-Hakkinda-Kamuoyu-Duyurusu>

- Korucu, O. (2021). Yeni normal dünya düzeninin siber güvenlik ve bilgi güvenliğine etkileri. *Yönetim Bilişim Sistemleri Dergisi*, 7(1), 44–60. <https://izlik.org/JA33DT56SH>
- Kott, A., & Linkov, I. (2021). To improve cyber resilience, measure it. *Computer*, 54(2), 80–85. <https://doi.org/10.1109/MC.2020.3038411>
- Kumar, P., Wazid, M., Singh, D. P., Singh, J., Das, A. K., Park, Y., & Rodrigues, J. J. (2023). Explainable artificial intelligence envisioned security mechanism for cyber threat hunting. *Security and Privacy*, 6(6), e312. <https://doi.org/10.1002/spy2.312>
- Laudon, K. C., & Laudon, J. P. (2011). *Yönetim bilişim sistemleri* (U. Yozgat, Çev. Ed.). Nobel Akademik Yayıncılık.
- Nadkarni, S., & Prügl, R. (2021). Digital transformation: A review, synthesis and opportunities for future research. *Management Review Quarterly*, 71, 233–341. <https://doi.org/10.1007/s11301-020-00185-7>
- Negri-Ribalta, C., Lombard-Platet, M., & Salinesi, C. (2024). Understanding the GDPR from a requirements engineering perspective: A systematic mapping study on regulatory data protection requirements. *Requirements Engineering*, 29, 523–549. <https://doi.org/10.1007/s00766-024-00423-4>
- Öztürk, M. S. (2018). Siber saldırılar, siber güvenlik denetimleri ve bütüncül bir denetim modeli önerisi. *Journal of Accounting and Taxation Studies*, 208-232. <https://doi.org/10.29067/muvu.340848>.
- Ses, S. M., & Korkusuz, M. R. (2025). İş ilişkisinde kişisel verilerin yapay zekâ destekli sistemler yardımıyla işlenmesi. *Ankara Sosyal Bilimler Üniversitesi Hukuk*

Fakültesi Dergisi, 6(2), 1000–1050.
<https://doi.org/10.47136/asbuhfd.1566869>

- Turan Başara, G. (2024). Kişisel Verilerin Korunması Kanunu'nun 6. maddesinde yapılan değişiklik bağlamında özel nitelikli kişisel verilerin işlenmesi. *Ankara Hacı Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, 28(4), 51–80. <https://doi.org/10.34246/ahbvuhfd.1497257>
- Ukeje, N., Gutierrez, J., & Petrova, K. (2024). Information security and privacy challenges of cloud computing for government adoption: A systematic review. *International Journal of Information Security*, 23(2), 1459–1475. <https://doi.org/10.1007/s10207-023-00797-6>
- Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. *Journal of Business Research*, 122, 889–901. <https://doi.org/10.1016/j.jbusres.2019.09.022>
- Wessel, L., Baiyere, A., Ologeanu-Taddei, R., Cha, J., & Jensen, T. B. (2021). Unpacking the difference between digital transformation and IT-enabled organizational transformation. *Journal of the Association for Information Systems*, 22(1), 102–129. <https://doi.org/10.17705/1jais.00655>
- Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and a maturity assessment framework. *Computers & Security*, 133, 103412. <https://doi.org/10.1016/j.cose.2023.103412>
- Zaguir, N. A., Magalhães, G. H., & Spinola, M. M. (2024). Challenges and enablers for GDPR compliance: Systematic literature review and future research

directions. *IEEE Access*, 12, 81608–81630.
<https://doi.org/10.1109/ACCESS.2024.3406724>

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1), 82–97.
<https://doi.org/10.1080/08874417.2020.1712269>

YÖNETİM BİLİŞİM SİSTEMLERİNDE DİJİTAL SÜRDÜRÜLEBİLİRLİK: KAVRAMSAL TEMELLER, AKILLI BİLGİ SİSTEMLERİ VE SÜRDÜRÜLEBİLİR DEĞER YARATIMI

Furkan ATLAN¹

1. GİRİŞ

Sürdürülebilirlik, örgütlerin yalnızca çevresel etkilerini azaltmaya yönelik bir sorumluluk alanı olmaktan çıkarak ekonomik değer yaratımı, toplumsal refah, kaynakların etkin kullanımı ve uzun dönemli örgütsel devamlılıkla ilişkilendirilen çok boyutlu bir yönetim konusu hâline gelmiştir. Dijital teknolojilerin örgütsel süreçlerde giderek daha fazla kullanılması, sürdürülebilirlik hedeflerine ulaşılmasında Yönetim Bilişim Sistemlerinin (YBS) üstlenebileceği rolün yeniden değerlendirilmesini gerekli kılmıştır. Bu doğrultuda bilgi sistemleri, yalnızca enerji tüketen teknolojik altyapılar olarak değil, örgütsel süreçlerin, karar mekanizmalarının ve kullanıcı davranışlarının sürdürülebilirlik doğrultusunda dönüştürülmesini destekleyen araçlar olarak da ele alınmaya başlanmıştır. Böylece YBS ile sürdürülebilirlik arasındaki ilişki, teknolojinin çevresel etkilerinin azaltılmasının ötesine taşınarak örgütsel ve toplumsal değer yaratımı perspektifine doğru genişlemiştir (Melville, 2010; Watson vd., 2010).

Bu gelişimin önemli aşamalarından biri, Yeşil Bilgi Teknolojileri (Green IT) ile Yeşil Bilgi Sistemleri (Green IS)

¹ Dr. Öğr. Üyesi, Burdur Mehmet Akif Ersoy Üniversitesi Bucak Zeliha Tolunay Uygulamalı Teknoloji ve İşletmecilik Yüksekokulu Yönetim Bilişim Sistemleri Bölümü, ORCID: 0000-0003-1602-1941.

yaklaşımları arasındaki kavramsal genişlemedir. Green IT kapsamında enerji verimli bilişim altyapılarının kullanılması, elektronik atıkların azaltılması ve bilgi teknolojileri (IT) kaynaklarının daha etkin yönetilmesi ön plana çıkarken, Green IS yaklaşımında bilgi sistemlerinin kaynak tüketiminin izlenmesi, süreçlerin iyileştirilmesi ve sürdürülebilir kararların desteklenmesi amacıyla kullanılabileceği kabul edilmektedir. Bu dönüşümle birlikte YBS'nin sürdürülebilirlik bağlamındaki işlevi, IT'nin kendi çevresel etkilerinin azaltılmasından, bilgi ve teknolojinin örgütsel sürdürülebilirliğin geliştirilmesinde kullandığı daha kapsamlı bir yapıya evrilmiştir (Molla vd., 2011; Loeser vd., 2017).

Söz konusu kavramsal gelişimin güncel karşılığı dijital sürdürülebilirlik yaklaşımında ortaya çıkmaktadır. Dijital sürdürülebilirlik, dijital kaynakların ve dijital artefaktların çevresel, ekonomik ve toplumsal refahı destekleyecek biçimde geliştirilmesine ve kullanılmasına karşılık gelir. Bu yaklaşımda yalnızca dijital teknolojilerin daha sürdürülebilir hâle getirilmesi değil, sürdürülebilirliğin dijital teknolojiler aracılığıyla nasıl desteklenebileceği de dikkate alınmaktadır. Bununla birlikte, dijitalleşmenin kendiliğinden olumlu sürdürülebilirlik sonuçları yaratacağı varsayılmamakta; enerji tüketimi, dijital eşitsizlik, mahremiyet, algoritmik ayrımcılık ve benzeri olumsuz sonuçların da değerlendirilmesi gerekmektedir. Dolayısıyla dijital sürdürülebilirliğin çevresel, ekonomik ve sosyal boyutlarının birlikte ele alındığı sosyo-teknik bir yaklaşım içinde değerlendirilmesi önem taşımaktadır (Kotlarsky vd., 2023; Schoormann vd., 2025).

Dijital sürdürülebilirliğin YBS açısından temel önemi, sürdürülebilirlik hedeflerinin veri aracılığıyla ölçülebilir ve yönetilebilir hâle getirilmesinde yatmaktadır. Enerji tüketimi, emisyonlar, su kullanımı, kaynak hareketleri ve operasyonel performansla ilişkin verilerin elde edilmesi önemli olmakla

birlikte, sürdürülebilir değer yaratımı için bu verilerin analiz edilmesi, anlamlandırılması ve karar süreçlerine aktarılması gerekmektedir. Bu açıdan YBS, sürdürülebilirlik verilerinin kaydedildiği pasif bir altyapı olmaktan çıkarak sürdürülebilirlik performansının izlendiği, değerlendirildiği ve yönlendirildiği aktif bir karar mekanizmasına dönüşmektedir. Dijital teknolojilerin ekolojik ve ekonomik değerin iş modellerine bütünleştirilmesini destekleyebilmesi, bu dönüşümün örgütsel önemini artırmaktadır (Böttcher vd., 2024).

Yapay zekâ (AI) ve makine öğrenmesi (ML), Nesnelerin İnterneti (IoT), bulut bilişim, dijital ikizler ve dijital platformlar bu yapının tamamlayıcı teknolojik bileşenlerini oluşturmaktadır. Bu teknolojiler aracılığıyla fiziksel çevreden veri elde edilebilmekte, sürdürülebilirlik performansına ilişkin tahmin ve analizler gerçekleştirilebilmekte, alternatif kararların sonuçları değerlendirilebilmekte, bilgi işlem kaynakları daha etkin yönetilebilmekte ve farklı aktörler arasındaki bilgi ve kaynak akışı koordine edilebilmektedir. Dolayısıyla dijital teknolojilerin sürdürülebilirliğe sağladığı katkının kullanılan teknoloji sayısından ziyade, bu teknolojilerin sürdürülebilirlik hedefleriyle ne ölçüde bütünleştirildiği üzerinden değerlendirilmesi gerekmektedir.

Bu doğrultuda öncelikle YBS’de dijital sürdürülebilirliğin kavramsal temelleri; Green IT’den Green IS’e geçiş, çevresel, ekonomik ve sosyal sürdürülebilirlik boyutları, dijital kaynaklar ve dijital artefaktlar ile çift dönüşüm perspektifi kapsamında ele alınmaktadır. Ardından AI ve ML, IoT, bulut bilişim, dijital ikizler ve dijital platformların sürdürülebilirlik odaklı akıllı bilgi sistemlerindeki işlevleri değerlendirilmektedir. Böylece dijital sürdürülebilirliğin kavramsal temelleri ile sürdürülebilirlik amaçlı dijital teknolojiler arasında bütüncül bir YBS perspektifinin ortaya konulması amaçlanmaktadır.

2. YBS'DE DİJİTAL SÜRDÜRÜLEBİLİRLİĞİN KAVRAMSAL TEMELLERİ

Dijital teknolojilerin örgütsel süreçlerde yaygınlaşması, sürdürülebilirlik ile YBS arasındaki ilişkinin yalnızca IT'nin çevresel etkileri üzerinden değerlendirilmesini yetersiz hâle getirmiştir. İlk dönem çalışmalarda enerji tüketiminin azaltılması, donanım kullanım sürelerinin uzatılması, elektronik atıkların yönetilmesi ve veri merkezi verimliliğinin artırılması gibi konular öne çıkarken, daha sonraki araştırmalarda bilgi sistemlerinin örgütlerin çevresel davranışlarını ve sürdürülebilir iş süreçlerini dönüştürme kapasitesi üzerinde durulmaya başlanmıştır. Melville (2010) tarafından bilgi sistemlerinin çevresel inançları, örgütsel uygulamaları ve sonuçları etkileyebilecek dönüştürücü bir unsur olduğu ortaya konulurken, Watson vd. (2010) tarafından da bilgi sistemlerinin, enerji verimliliğinin ötesinde, çevresel olarak sürdürülebilir bir toplumun oluşturulmasına katkıda bulunabileceği belirtilmiştir. Böylece sürdürülebilirlik, YBS açısından yalnızca teknolojik altyapının çevreci hâle getirilmesiyle ilgili teknik bir problem olmaktan çıkarılarak örgütsel ve toplumsal dönüşüm problemi şeklinde ele alınmaya başlanmıştır.

Bu gelişimin güncel karşılığı dijital sürdürülebilirlik kavramında görülmektedir. Kotlarsky vd. (2023) tarafından Journal of the Association for Information Systems (JAIS) kapsamında yapılan kavramsallaştırmada dijital sürdürülebilirlik, dijital kaynakların ve dijital artefaktların çevrenin, toplumun ve ekonomik refahın geliştirilmesine yönelik biçimde geliştirilmesi ve kullanılması olarak tanımlanmıştır. Dolayısıyla dijital sürdürülebilirlikte yalnızca “dijital teknolojinin sürdürülebilir olması” değil, “sürdürülebilirliğin dijital teknolojiler aracılığıyla mümkün kılınması” da dikkate alınmaktadır. Daha güncel YBS literatüründe bu yaklaşım genişletilerek dijital teknolojilerin olumlu sonuçları kadar enerji tüketimi, dijital eşitsizlik,

mahremiyet, algoritmik ayrımcılık veya geri tepme etkileri gibi istenmeyen sonuçlarının da değerlendirilmesi gerektiği vurgulanmıştır (Schoormann vd., 2025). Bu nedenle dijital sürdürülebilirliğin çevresel, ekonomik ve sosyal sonuçlarının birlikte değerlendirildiği sosyo-teknik bir çerçeve içinde incelenmesi gerekli görülmektedir.

2.1. Green IT'den Green IS'e ve Dijital Sürdürülebilirliğe Geçiş

Green IT ile Green IS arasında kavramsal bir ayrım yapılması gerekmektedir. Green IT, temel olarak bilgi teknolojileri altyapısının çevresel ayak izinin azaltılmasını ifade eder. Bu kapsamda enerji verimli donanımların tercih edilmesi, sunucuların konsolidasyonu, sanallaştırma, enerji tüketiminin azaltılması, elektronik atıkların uygun biçimde yönetilmesi ve bilişim ekipmanlarının yaşam döngüsünün sürdürülebilir biçimde yönetilmesi gibi uygulamalar ele alınmaktadır. Molla vd. (2011) tarafından geliştirilen Green IT hazırlık yaklaşımında da örgütlerin teknolojik altyapılarını çevresel açıdan daha sürdürülebilir yönetebilmek için belirli yönetsel, teknolojik ve örgütsel yetenekler geliştirmeleri gerektiği gösterilmiştir. Bu yönüyle Green IT'de öncelikle “IT'nin çevresel etkisinin nasıl azaltılabileceği” sorusuna yanıt aranmaktadır.

Green IS ise kapsam bakımından Green IT'den daha geniş bir yaklaşımı temsil etmektedir. Green IS kapsamında bilgi sistemleri yalnızca çevresel sorun oluşturan bir teknoloji altyapısı olarak değerlendirilmemekte; aynı zamanda örgütün ve diğer ekonomik aktörlerin sürdürülebilir davranışlara yönlendirilmesini sağlayabilecek dönüştürücü bir mekanizma olarak da ele alınmaktadır. Loeser vd. (2017) tarafından Green IT uygulamaları ile Green IS uygulamaları birbirinden ayrıştırılarak, Green IS uygulamalarının kaynak ve süreç şeffaflığının geliştirilmesini, iş süreçlerinin daha verimli yürütülmesini ve

çevresel inovasyonun desteklenmesini sağlayabildiği gösterilmiştir. Örneğin, bir veri merkezinin enerji tüketiminin azaltılması Green IT kapsamında değerlendirilirken, tedarik zincirindeki karbon emisyonlarının izlenmesini ve karar vericilerin emisyon azaltıcı alternatiflere yönlendirilmesini sağlayan bir bilgi sistemi Green IS kapsamında değerlendirilmektedir.

Dijital sürdürülebilirlik, bu iki yaklaşım üzerine inşa edilmesine rağmen, her ikisinden de daha geniş bir kavramsal alan oluşturmaktadır. Kotlarsky vd. (2023) tarafından Green IT ve Green IS literatürünün sistematik olarak değerlendirilmesi sonucunda, sürdürülebilirliğin yalnızca çevresel boyuta sınırlandırılmasının günümüzdeki dijital dönüşümün etkilerini açıklamakta yetersiz kaldığı belirtilmiştir. Dijital sürdürülebilirlik kapsamında dijital teknolojilerin çevresel etkilerinin yanı sıra ekonomik refah, sosyal kapsayıcılık, çalışma koşulları, erişilebilirlik ve toplumsal değer yaratımı üzerindeki etkileri de değerlendirmeye alınmaktadır. Bu genişleme sonucunda YBS araştırmalarındaki temel soru, “teknolojinin nasıl daha yeşil hâle getirileceğinden” “dijital kaynak ve sistemlerin çok boyutlu sürdürülebilir değer üretmek üzere nasıl tasarlanıp yönetilebileceğine” doğru evrilmiştir.

2.2. Çevresel, Ekonomik ve Sosyal Sürdürülebilirlik Boyutları

Dijital sürdürülebilirliğin kapsamı çevresel, ekonomik ve sosyal sürdürülebilirlik boyutlarının birlikte değerlendirilmesine dayanmaktadır. Çevresel boyutta enerji ve doğal kaynak tüketiminin azaltılması, emisyonların izlenmesi, döngüsel ekonominin desteklenmesi ve atıkların azaltılması gibi hedefler hedeflenmektedir. Ekonomik boyutta ise süreç verimliliği, maliyetlerin düşürülmesi, inovasyon kapasitesinin geliştirilmesi ve sürdürülebilir iş modelleri aracılığıyla uzun dönemli değer

yaratılması önem kazanmaktadır. Böttcher vd. (2024), dijital teknolojilerin yalnızca operasyonları optimize eden yardımcı araçlar olarak kullanılmasının ötesine geçilerek ekolojik ve ekonomik değerin iş modelinin temel mantığına yerleştirilebileceğini göstermiştir. Bu bağlamda dijital sürdürülebilirlik, çevresel performans ile ekonomik performans arasında zorunlu bir karşılık bulunduğu varsayımını sorgulayan bir yaklaşım sunmaktadır.

Sosyal boyutta ise teknolojiye erişim, çalışan refahı, kapsayıcılık, güvenlik, mahremiyet ve dijital eşitsizlik gibi hususlar dikkate alınmaktadır. Nitekim sürdürülebilir bilgi sistemlerinin örgütsel olarak benimsenmesi yalnızca teknolojik yeterlilikle açıklanamamakta; çalışanların motivasyonlarının, tutumlarının, örgütsel kuralların ve sosyal etkileşimlerin de sürece dâhil edilmesi gerekmektedir (Kirchner-Krath vd., 2024). Benzer şekilde Schoormann vd. (2025), dijital teknolojilerin sürdürülebilirlik açısından hem olumlu hem de olumsuz sonuçlar yaratabileceğine dikkat çekmiştir. Örneğin, dijital hizmetler belirli hizmetlere erişimi genişletebilirken, dijital uçurum nedeniyle bazı grupların dışlanmasına da yol açabilmektedir. Bu nedenle YBS bağlamında sürdürülebilirliğin yalnızca çevresel performans göstergelerine indirgenmemesi; teknolojinin ekonomik, çevresel ve toplumsal sonuçları arasındaki olası ödüneşimlerin birlikte yönetilmesi gerekmektedir.

2.3. Dijital Kaynaklar, Dijital Artefaktlar ve Sürdürülebilir Değer Yaratımı

Dijital sürdürülebilirliğin ortaya çıkmasında dijital kaynaklar ile dijital artefaktların sürdürülebilir amaçlara yönlendirilmesi merkezi önem taşımaktadır. Dijital kaynaklar, veri ve teknik altyapı gibi yeniden kullanılabilen dijital unsurları kapsarken, dijital artefaktlar, yazılım uygulamaları ve bilgi sistemleri gibi belirli işlevleri gerçekleştirmek üzere oluşturulan

dijital yapılardan meydana gelmektedir (Kotlarsky vd., 2023). Bu ayrım, sürdürülebilir değer yaratımının yalnızca fiziksel bilişim donanımlarının verimliliğine bağlı olmadığını göstermektedir. Örneğin, enerji tüketim verilerinin toplanması başlı başına bir dijital kaynak yaratırken, söz konusu verileri analiz ederek yöneticilere enerji tasarrufu kararları öneren bir karar destek sistemi sürdürülebilirlik amacı taşıyan dijital bir artefakt niteliği kazanmaktadır.

Dijital kaynakların sürdürülebilir değere dönüştürülebilmesi, teknolojinin örgütsel süreç ve kararlarla bütünleştirilmesine bağlıdır. Veriler aracılığıyla kaynak tüketiminin görünür hâle getirilmesi, analitik sistemlerle verimsizliklerin belirlenmesi, süreçlerin otomatik olarak optimize edilmesi ve ürün yaşam döngülerinin izlenmesi çevresel değer üretebilirken; aynı altyapılar maliyet azaltımı, yeni hizmetlerin geliştirilmesi ve yeni iş modellerinin ortaya çıkarılması yoluyla ekonomik değer de sağlayabilmektedir. Böttcher vd. (2024) tarafından incelenen dijital sürdürülebilir iş modellerinde dijital teknolojilerin ekolojik ve ekonomik değer yaratımının doğrudan bir bileşenine dönüştürülebildiği belirlenmiştir. Böylece YBS'nin rolü, sürdürülebilirlik verilerinin kaydedildiği pasif sistemlerin oluşturulmasından çıkarak sürdürülebilir değerın tasarlandığı, ölçüldüğü ve yönlendirildiği dijital mekanizmaların geliştirilmesine doğru genişlemektedir.

2.4. Dijital ve Yeşil Dönüşümün Bütünleşmesi: Çift Dönüşüm

Dijital dönüşüm ile yeşil dönüşümün birbirinden bağımsız yürütülmesinin taşıdığı sınırlılıklar, çift dönüşüm (twin transition) yaklaşımının ortaya çıkmasına yol açmıştır. Çift dönüşümde dijitalleşme ve sürdürülebilirlik, iki paralel dönüşüm programı olarak değil, birbirini karşılıklı olarak güçlendiren süreçler olarak değerlendirilmektedir. Christmann vd. (2024)

tarafından bu ilişki, dijital teknolojilerin sürdürülebilirlik dönüşümünü mümkün kıldığı ve sürdürülebilirlik hedeflerinin de dijital dönüşümün yönünü belirlediği değer yaratıcı bir karşılıklı etkileşim şeklinde kavramsallaştırılmıştır. Bu nedenle veri analitiği, IoT, AI ve dijital platformlar yalnızca dijital olgunluğu artırmak amacıyla kullanılmamakta; kaynak optimizasyonu, emisyonların azaltılması, döngüsellik ve sürdürülebilir karar verme gibi hedeflere bağlandığında çift dönüşümün bileşenlerine dönüşmektedir.

Bununla birlikte, dijital dönüşümün kendiliğinden çevresel sürdürülebilirlik üreteceği varsayımı desteklenmemektedir. Bianchini vd. (2023) tarafından Avrupa bölgeleri üzerinde yapılan ampirik incelemede, yeşil teknolojik gelişmenin sera gazı emisyonlarını azaltabildiği; buna karşılık bazı dijital teknolojilerin tek başına emisyon artırıcı etkiler gösterebildiği belirlenmiştir. Özellikle büyük veri ve bilgi işlem altyapılarının çevresel maliyetlerinin dikkate alınması gerektiği ortaya konmuştur. Aynı çalışmada yeşil ve dijital teknolojilerin güçlü biçimde birlikte bulunduğu bölgelerde daha olumlu tamamlayıcılık etkilerinin ortaya çıkması, dijitalleşmenin sürdürülebilirlik stratejileri tarafından yönlendirilmesi gerektiğini göstermektedir. Dolayısıyla çift dönüşüm, örgütlerin yalnızca daha fazla dijital teknoloji benimsemesini değil, dijital yatırımların sürdürülebilirlik amaçları doğrultusunda seçilmesini, tasarlanmasını ve yönetilmesini de gerektirmektedir.

Bu perspektiften değerlendirildiğinde, YBS çift dönüşümün teknik altyapısını sağlamanın ötesinde dijital ve sürdürülebilirlik stratejileri arasındaki bütünleşmenin kurulduğu temel örgütsel alanlardan biri hâline gelmektedir. Dijital teknolojiler aracılığıyla sürdürülebilirlik performansının ölçülmesi ve iyileştirilmesi mümkün kılınırken, sürdürülebilirlik hedefleri aracılığıyla hangi dijital yatırımların yapılacağına ve bu teknolojilerin hangi değerleri üretmesi gerektiğine ilişkin stratejik

yönlendirme sağlanmaktadır. Böylece Green IT'den Green IS'e ve buradan dijital sürdürülebilirlik ile çift dönüşüme uzanan kavramsal gelişim, YBS'nin sürdürülebilirlik bağlamındaki rolünün teknik verimlilikten örgütsel ve toplumsal değer yaratımına doğru genişlediğini göstermektedir.

3. SÜRDÜRÜLEBİLİRLİK İÇİN DİJİTAL TEKNOLOJİLER VE AKILLI BİLGİ SİSTEMLERİ

Dijital teknolojilerin sürdürülebilirlik açısından taşıdığı değer, yalnızca işlemlerin dijitalleştirilmesi veya teknolojik altyapının modernleştirilmesi üzerinden değerlendirilmemektedir. IT literatüründe dijital sürdürülebilirlik, dijital kaynakların ve dijital yapıların çevresel, toplumsal ve ekonomik refahın geliştirilmesi amacıyla tasarlanması ve kullanılmasıyla ilişkilendirilmektedir (Kotlarsky vd., 2023). Bu yaklaşım, sürdürülebilirlik için kullanılan IT'nin temel işlevini, verilerin toplanmasından ziyade bu verilerin karar verilebilir bilgiye dönüştürülmesi üzerinden açıklamaktadır. Nitekim dijital sürdürülebilir iş modellerinde sensörlerden, kurumsal sistemlerden ve dış veri kaynaklarından elde edilen verilerin birleştirilerek kaynak tüketimi, çevresel performans, verimsizlik ve iyileştirme alanları hakkında sürdürülebilirlik istihbaratı üretilebildiği gösterilmektedir (Böttcher vd., 2024).

Bu nedenle sürdürülebilirlik odaklı akıllı IT'nin algılama, analiz, öngörü, karar desteği ve koordinasyon işlevlerini birbirine bağlayan bir bilgi mimarisi olarak ele alınması gerekmektedir. IoT aracılığıyla fiziksel çevreden veri elde edilmekte, AI ve analitik yöntemlerle bu verilerden örüntüler ve tahminler üretilmekte, dijital ikizler aracılığıyla alternatif kararların sonuçları modellenmekte, bulut altyapılarıyla hesaplama kaynakları ölçeklenmekte ve dijital platformlarla farklı aktörler

arasındaki bilgi alışverişi koordine edilmektedir. Böylelikle dijital teknolojinin sürdürülebilirliğe katkısı, kullanılan teknoloji sayısı ile değil, kararların daha ölçülebilir, öngörülebilir ve kaynak-etkin hâle getirilme derecesiyle belirlenmektedir.

3.1. AI ve ML Tabanlı Sürdürülebilirlik Uygulamaları

AI ve ML, sürdürülebilirlik yönetiminde özellikle büyük ve heterojen veri kümelerinden tahmine ve optimizasyona elverişli bilgi üretilmesini mümkün kılmaktadır. Bu sistemlerde geçmiş tüketim değerleri, çevresel ölçümler, operasyon verileri ve dış çevre değişkenleri işlenerek talep, kaynak ihtiyacı, risk ve olası çevresel etkiler hakkında öngörüler oluşturulabilmektedir. ML tabanlı su yönetimi uygulamalarında, örneğin yağış, debi, yeraltı su seviyesi, sıcaklık, arazi kullanımı ve tüketim gibi değişkenlerden yararlanılarak su talebi, taşkın riski, su kalitesi ve dağıtım sistemi performansının tahmin edilebildiği belirtilmektedir (Ahmed vd., 2024). Burada üretilen temel bilgi, gelecekteki sistem durumuna ilişkin bir tahmin iken; iyileştirilen yönetim kararı su tahsis, altyapı işletimi veya erken müdahale kararı olmakta; sürdürülebilirlik çıktısı ise su kaybının ve kaynak baskısının azaltılması biçiminde ortaya çıkmaktadır.

AI'nin yönetsel değeri yalnızca tahmin yapılmasıyla sınırlı değildir. Dinamik koşullar altında hangi eylemin daha yüksek sürdürülebilirlik performansı yaratacağının belirlenmesi de mümkün hâle gelmektedir. Pekiştirmeli öğrenme (reinforcement learning) çalışmalarında enerji sistemleri, su kaynakları ve ulaşım gibi alanların önemli uygulama kümeleri oluşturduğu; özellikle değişken kaynak koşullarına uyum sağlayan karar politikalarının geliştirilebildiği gösterilmektedir (Zuccotto vd., 2024). Böyle bir yapı içerisinde enerji talebinin hangi zamanlarda karşılanacağı, yenilenebilir üretimin hangi kaynaklarla dengeleneceği veya kaynakların hangi faaliyetlere yönlendirileceği gibi operasyonel kararlar dinamik biçimde

optimize edilebilmektedir. Bunun sonucunda enerji tüketiminin, emisyonların ve kaynak kullanımındaki verimsizliklerin azaltılması desteklenmektedir.

Bununla birlikte, AI tabanlı sürdürülebilirlik uygulamalarının başarısı algoritmik doğrulukla özdeşleştirilmemelidir. Böttcher vd. (2024), sürdürülebilirlik istihbaratı üreten iş modellerinde YZ ve MÖ tabanlı analitiğin asıl değerinin sürdürülebilir olmayan süreçler hakkında görünürlük oluşturması, verimsizlikleri belirlemesi ve karar vericilere iyileştirme seçenekleri sunması olduğunu göstermektedir. Bu nedenle model çıktılarının enerji, karbon, su veya atık gibi anlamlı performans göstergeleriyle ilişkilendirilmesi ve yönetim süreçlerine aktarılması gerekmektedir. Böylece algoritmik çıktı, teknik bir tahmin olmaktan çıkarılarak sürdürülebilir kaynak tahsisini destekleyen yönetsel bilgiye dönüştürülmektedir.

3.2. IoT ve Gerçek Zamanlı Çevresel Veri Toplama

IoT, fiziksel çevrede gerçekleşen değişimlerin sürekli veya kısa aralıklarla ölçülerek IT'ye aktarılmasını sağlar. Sıcaklık, enerji tüketimi, su kalitesi, nem, emisyon veya ekipman durumu gibi değişkenlerin sensörlerle izlenmesi sayesinde yöneticilerin yalnızca geçmiş raporlara değil, güncel sistem durumuna ilişkin bilgiye de erişmesi mümkün olmaktadır. Ahmad vd. (2023) tarafından gerçekleştirilen gerçek dünya uygulamasında çevresel sensörlerin bilgi açısından kritik konumlara yerleştirilmesi, iletişim kapasitesinin düzenlenmesi ve enerji kullanımının optimize edilmesi yoluyla geniş çevresel alanlardaki değişimlerin güvenilir biçimde izlenebildiği gösterilmiştir. Bu tür sistemlerde üretilen bilgi, çevresel durumun zaman ve konum boyutundaki güncel görünümüdür; bu sayede örnekleme, bakım, müdahale ve kaynak dağılımı kararlarının daha hızlı alınması sağlanabilmektedir.

IoT tabanlı verilerin davranışsal kararları da değiştirebildiği görülmektedir. Akıllı sayaçlar aracılığıyla enerji kullanımının gerçeğe yakın ve zamanında ölçülmesi ve bu bilgilerin kullanıcı arayüzleri üzerinden sunulması, tüketicilerin kendi enerji kullanımını değerlendirmelerine olanak tanır (Wendt vd., 2024). Bu noktada teknolojinin sürdürülebilirlik etkisi sensörün varlığından değil, ölçülen tüketim bilgisinin karşılaştırılabilir ve eyleme dönüştürülebilir hâle getirilmesinden kaynaklanmaktadır. Benzer mantık kurumsal ölçekte uygulandığında üretim hatlarında, binalarda, enerji ağlarında veya lojistik sistemlerinde aşırı tüketimin ve anormal durumların erken belirlenmesi mümkün olmakta; böylece enerji, su ve diğer doğal kaynakların gereksiz kullanımının önlenmesine yönelik kararlar desteklenmektedir.

3.3. Bulut Bilişim, Dijital İkizler ve Akıllı Kaynak Yönetimi

Bulut bilişim, sürdürülebilir kaynak yönetiminde hem dijital hizmetlerin ölçeklenmesini sağlayan bir altyapı hem de bilgi işlem kaynaklarının daha etkin kullanılmasına yönelik bir yönetim modeli olarak değerlendirilmektedir. Bulut ortamlarında hesaplama, depolama ve iş yüklerinin talebe göre tahsis edilebilmesi, kapasitenin sürekli olarak en yüksek talebe göre fiziksel olarak bulundurulması gereksinimini azaltabilmektedir. Park vd. (2023) tarafından ABD’de 57 endüstriyi kapsayan ampirik analizde, bulut tabanlı bilgi teknolojileri hizmetlerinin kullanıcı tarafındaki enerji verimliliğiyle pozitif ilişki gösterdiği ve etkinin kullanılan bulut hizmet modeline göre farklılaşabildiği belirlenmiştir. Buna göre bulut sistemlerinden üretilen kapasite, iş yükü ve tüketim bilgileri, hangi kaynakların nerede ve ne zaman çalıştırılacağına ilişkin kararları iyileştirebilmekte ve bilgi işlem altyapısındaki enerji tüketiminin azaltılmasına katkı sağlayabilmektedir.

Ancak bulut bilişimin sürdürülebilirliği otomatik olarak oluşturduğu kabul edilmemelidir. Veri merkezi kaynaklarının, iş yüklerinin, enerji tüketiminin ve hizmet kalitesinin birlikte yönetilmesi gerektiği belirtilmekte; enerji verimliliği ile hizmet düzeyi arasındaki dengenin akıllı kaynak yönetimi aracılığıyla kurulabileceği vurgulanmaktadır (Buyya vd., 2024). Ayrıca bulut mimarisinde çoklu kiracılık, talebe bağlı kaynak sağlama ve kullandıkça ödeme gibi özelliklerin sürdürülebilirlik sonuçlarını etkileyen tasarım kararları olduğu gösterilmektedir (Ahmadisakha ve Andrikopoulos, 2024). Dolayısıyla yönetsel kararın yalnızca “buluta geçiş” biçiminde tanımlanması yerine, iş yüklerinin hangi mimaride ve hangi kaynak tahsis politikasıyla çalıştırılacağına odaklanılması gerekmektedir.

Dijital ikizler ise fiziksel kaynak, süreç veya sistemlerin güncel verilerle beslenen sanal temsillerinin oluşturulmasını sağlayarak sürdürülebilirlik yönetimine farklı bir karar alma yeteneği kazandırmaktadır. Fiziksel sistemden alınan verilerin sanal katmana aktarılmasıyla mevcut durum izlenebilmekte, riskler değerlendirilebilmekte ve alternatif kararların sonuçları fiziksel uygulamadan önce analiz edilebilmektedir. Tedarik zinciri sürdürülebilirlik riskleri üzerine gerçekleştirilen bir çalışmada, dijital ikiz yapısının gerçek zamanlı izleme, risk değerlendirmesi, kapasite planlaması ve kaynak alternatiflerinin incelenmesiyle ilişkilendirildiği gösterilmiştir (Hezam vd., 2024). Böylelikle hangi tedarikçinin seçileceği, kapasitenin nasıl dağıtılacağı veya riskli kaynakların nasıl ikame edileceği gibi kararların sanal ortamda değerlendirilmesi mümkün olmakta; kaynak israfı ve çevresel risklerin azaltılmasına yönelik daha proaktif bir yönetim anlayışı desteklenmektedir.

3.4. Dijital Platformlar ve Sürdürülebilir Ekosistemler

Dijital platformların sürdürülebilirlik açısından temel işlevi, tek bir işletmenin verimliliğinin ötesine geçilerek farklı

aktörlerin bilgi, kaynak ve faaliyetlerinin ortak bir dijital ortamda koordine edilmesidir. Böttcher vd. (2024) tarafından tanımlanan dijital sürdürülebilir platformlarda çok taraflı pazar yapılarının döngüsel ekonomiyle ilişkilendirilebildiği; yeniden kullanım, kaynakların yeniden dolaşıma sokulması ve atığın azaltılması gibi faaliyetlerin platform üzerinden ölçeklenebildiği gösterilmektedir. Bu sistemlerde üretilen bilgi yalnızca işlem bilgisi değildir; kullanılabilir kaynakların nerede bulunduğu, hangi aktörün hangi kaynağa ihtiyaç duyduğu, sürdürülebilirlik performansının nasıl değiştiği ve değer zincirinin hangi noktasında iyileştirme yapılabileceği de görünür hâle getirilmektedir. Böylelikle eşleştirme, tedarik, yeniden kullanım ve iş ortağı seçimine ilişkin kararların iyileştirilmesiyle döngüsellik desteklenmektedir.

Güncel bulgular sürdürülebilirlik platformlarının ekosistem düzeyinde daha geniş bir yönetim işlevi üstlenebileceğini de göstermektedir. Leutheuser ve Voigt (2026) tarafından 42 uzman görüşmesine dayalı olarak gerçekleştirilen araştırmada sürdürülebilirlik platformlarının etkisi; dış gereksinimler, sürdürülebilirlik verisi, sürdürülebilir değer yaratımı ve sürdürülebilir değer zinciri optimizasyonu olmak üzere dört unsur üzerinden açıklanmıştır. Bu yapı içerisinde farklı işletmelerden gelen sürdürülebilirlik verileri ortak bir bilgi alanında görünür hâle getirilmekte, değer zincirindeki zayıf noktalar belirlenmekte ve ortak iyileştirme kararları desteklenmektedir. Dolayısıyla platformların sürdürülebilirlik katkısı yalnızca işlemleri dijitalleştirmekten değil, ekosistem aktörleri arasındaki bilgi asimetrisini azaltarak koordinasyonu güçlendirmesinden de kaynaklanmaktadır. Bu perspektiften değerlendirildiğinde, akıllı BS, IoT ile fiziksel dünyayı algılayan, YZ ile geleceği öngören, dijital ikizlerle alternatifleri sıyan, bulut bilişimle kaynakları ölçekleyen ve dijital platformlarla

aktörleri koordine eden bütünleşik bir sürdürülebilirlik karar altyapısı olarak konumlandırılmaktadır.

4. SONUÇ VE ÖNERİLER

Dijital kaynakların ve dijital artefaktların sürdürülebilir değere dönüştürülebilmesi, verinin yalnızca toplanmasına değil, karar süreçlerine aktarılmasına da bağlıdır. Enerji tüketimi, emisyonlar, su kullanımı, kaynak hareketleri veya operasyonel performansa ilişkin verilerin görünür hâle getirilmesi sürdürülebilirlik yönetimi açısından önemli olmakla birlikte, asıl katkı söz konusu verilerin analiz edilmesi, verimsizliklerin belirlenmesi ve alternatif kararların değerlendirilmesinde ortaya çıkmaktadır. Bu nedenle sürdürülebilirlik odaklı bilgi sistemlerinin tasarımında hangi verinin üretileceğinin yanı sıra bu verinin hangi yönetsel kararı destekleyeceğinin ve hangi sürdürülebilirlik çıktısına katkı sağlayacağını da açık biçimde belirlenmesi önerilmektedir.

Dijital ve yeşil dönüşüm arasındaki bütünleşme de sürdürülebilirlik açısından temel bir gereklilik olarak ortaya çıkmaktadır. Dijitalleşmenin tek başına sürdürülebilir sonuçlar üreteceği varsayımından hareket edilmemeli; dijital yatırımların sürdürülebilirlik amaçları doğrultusunda seçilmesi, tasarlanması ve yönetilmesi sağlanmalıdır. Dijital teknolojilerin enerji tüketimi veya diğer olumsuz etkiler yaratabileceği dikkate alınarak dijital dönüşümün yönü sürdürülebilirlik hedefleriyle ilişkilendirilmelidir. Böylece dijital dönüşüm ile yeşil dönüşümün birbirinden bağımsız süreçler olarak yürütülmesi yerine, birbirini karşılıklı olarak destekleyen bütünleşik bir dönüşüm anlayışının benimsenmesi uygun olacaktır.

AI ve ML, IoT, bulut bilişim, dijital ikizler ve dijital platformlar sürdürülebilirlik odaklı bilgi sistemlerinde birbirinden bağımsız teknolojiler olarak değil, tamamlayıcı

yetenekler sağlayan bileşenler olarak değerlendirilmelidir. IoT aracılığıyla güncel çevresel ve operasyonel verilerin elde edilmesi, AI ve ML ile bu verilerin tahmin ve optimizasyon amacıyla işlenmesi, dijital ikizlerle alternatif kararların sonuçlarının değerlendirilmesi, bulut bilişimle bilgi işlem kaynaklarının etkin biçimde yönetilmesi ve dijital platformlarla farklı aktörler arasındaki bilgi ve kaynak akışının koordine edilmesi mümkün hâle gelmektedir. Bu nedenle teknolojik başarının yalnızca algoritmik doğruluk, sensör sayısı, hesaplama kapasitesi veya işlem hacmi gibi teknik göstergeler üzerinden değerlendirilmesi yerine, üretilen çıktının sürdürülebilirlik kararlarına ne ölçüde katkı sağladığı da dikkate alınmalıdır.

Örgütsel uygulamalarda sürdürülebilirlik odaklı YBS yatırımlarının teknoloji edinimi merkezli bir anlayıştan uzaklaştırılması önerilmektedir. Teknoloji seçiminin enerji, su, emisyon, atık, kaynak verimliliği, süreç etkinliği veya koordinasyon gibi somut sürdürülebilirlik gereksinimleriyle ilişkilendirilmesi; üretilen bilginin ise karar vericilerin sürdürülebilir olmayan süreçleri belirlemesini ve uygun alternatifleri değerlendirmesini sağlayacak biçimde yapılandırılması gerekmektedir. Bunun yanında, dijital teknolojilerin ekonomik ve çevresel katkıları kadar kapsayıcılık, erişilebilirlik, mahremiyet ve diğer sosyal sonuçlarının da değerlendirilmesi önem taşımaktadır.

Sonuç olarak, sürdürülebilirlik perspektifinden YBS'nin stratejik değeri, daha fazla dijital teknoloji kullanılmasından değil; dijital kaynakların ve teknolojik yeteneklerin çevresel, ekonomik ve sosyal değer yaratımını destekleyecek biçimde bütünleştirilmesinden kaynaklanmaktadır. Bu nedenle sürdürülebilirlik odaklı YBS yaklaşımında temel önceliğin teknoloji merkezli dijitalleşmeden, veri ve dijital yeteneklerin ölçülebilir sürdürülebilirlik hedefleri doğrultusunda yönetildiği

bütünleşik karar sistemlerine doğru yönlendirilmesi gerektiği değerlendirilmektedir.

KAYNAKÇA

- Ahmad, S., Uyanik, H., Ovatman, T., Sandikkaya, M. T., De Maio, V., Brandić, I., & Aral, A. (2023). Sustainable environmental monitoring via energy and information efficient multinode placement. *IEEE Internet of Things Journal*, 10(24), 22065–22079. <https://doi.org/10.1109/JIOT.2023.3303124>
- Ahmadisakha, S., & Andrikopoulos, V. (2024). Architecting for sustainability of and in the cloud: A systematic literature review. *Information and Software Technology*, 171, 107459. <https://doi.org/10.1016/j.infsof.2024.107459>
- Ahmed, A. A., Sayed, S., Abdoulhalik, A., Moutari, S., & Oyedele, L. (2024). Applications of machine learning to water resources management: A review of present status and future opportunities. *Journal of Cleaner Production*, 441, 140715. <https://doi.org/10.1016/j.jclepro.2024.140715>
- Bianchini, S., Damioli, G., & Ghisetti, C. (2023). The environmental effects of the “twin” green and digital transition in European regions. *Environmental and Resource Economics*, 84(4), 877–918. doi: 10.1007/s10640-022-00741-7.
- Böttcher, T. P., Empelmann, S., Weking, J., Hein, A., & Krcmar, H. (2024). Digital sustainable business models: Using digital technology to integrate ecological sustainability into the core of business models. *Information Systems Journal*, 34(3), 736–761. doi: 10.1111/isj.12436.
- Buyya, R., Ilager, S., & Arroba, P. (2024). Energy-efficiency and sustainability in new generation cloud computing: A vision and directions for integrated management of data centre resources and workloads. *Software: Practice and*

Experience, 54(1), 24–38.
<https://doi.org/10.1002/spe.3248>

Christmann, A.-S., Crome, C., Graf-Drasch, V., Oberländer, A. M., & Schmidt, L. (2024). The twin transformation butterfly: Capabilities for an integrated digital and sustainability transformation. *Business & Information Systems Engineering*, 66(4), 489–505. doi: 10.1007/s12599-023-00847-2.

Hezam, I. M., Ali, A. M., Sallam, K., Hameed, I. A., & Abdel-Basset, M. (2024). Digital twin and fuzzy framework for supply chain sustainability risk assessment and management in supplier selection. *Scientific Reports*, 14, 17718. <https://doi.org/10.1038/s41598-024-67226-z>

Kirchner-Krath, J., Morschheuser, B., Sicevic, N., Xi, N., von Korfflesch, H. F. O., & Hamari, J. (2024). Challenges in the adoption of sustainability information systems: A study on green IS in organizations. *International Journal of Information Management*, 77, 102754. doi: 10.1016/j.ijinfomgt.2024.102754.

Kotlarsky, J., Oshri, I., & Sekulic, N. (2023). Digital sustainability in information systems research: Conceptual foundations and future directions. *Journal of the Association for Information Systems*, 24(4), 936–952. doi: 10.17705/1jais.00825.

Leutheuser, V., & Voigt, K.-I. (2026). Striving for the common good: Sustainability impacts on digital platform ecosystems. *Creativity and Innovation Management*, 1–20. <https://doi.org/10.1111/caim.70084>

Loeser, F., Recker, J., vom Brocke, J., Molla, A., & Zarnekow, R. (2017). How IT executives create organizational benefits by translating environmental strategies into

- Green IS initiatives. *Information Systems Journal*, 27(4), 503–553. doi: 10.1111/isj.12136.
- Melville, N. P. (2010). Information systems innovation for environmental sustainability. *MIS Quarterly*, 34(1), 1–21. doi: 10.2307/20721412.
- Molla, A., Cooper, V., & Pittayachawan, S. (2011). The Green IT readiness (G-readiness) of organizations: An exploratory analysis of a construct and instrument. *Communications of the Association for Information Systems*, 29, 67–96. doi: 10.17705/1CAIS.02904.
- Park, J., Han, K., & Lee, B. (2023). Green cloud? An empirical analysis of cloud computing and energy efficiency. *Management Science*, 69(3), 1639–1664. <https://doi.org/10.1287/mnsc.2022.4442>
- Schoormann, T., Möller, F., Hoppe, C., & vom Brocke, J. (2025). Digital sustainability: Understanding and managing tensions. *Business & Information Systems Engineering*, 67(3), 429–438. doi: 10.1007/s12599-025-00937-3.
- Watson, R. T., Boudreau, M.-C., & Chen, A. J. (2010). Information systems and environmentally sustainable development: Energy informatics and new directions for the IS community. *MIS Quarterly*, 34(1), 23–38. doi: 10.2307/20721413.
- Wendt, C., Kosin, D., Adam, M., & Benlian, A. (2024). Sustainable energy consumption behaviour with smart meters: The role of relative performance and evaluative standards. *Information Systems Journal*, 34(6), 1995–2023. <https://doi.org/10.1111/isj.12520>
- Zuccotto, M., Castellini, A., La Torre, D., Mola, L., & Farinelli, A. (2024). Reinforcement learning applications in environmental sustainability: A review. *Artificial*

Intelligence Review, 57, 88.
<https://doi.org/10.1007/s10462-024-10706-5>

EMBODIMENT AS COMMONS: THE POLITICAL ECONOMY OF OPEN-SOURCE AI BODIES

İsmail Erim GÜLAÇTI¹

1. INTRODUCTION: THE €125 BODY

In April 2026 the independent researcher Olivia Zhu published a preprint and a public code repository describing a hardware-software architecture that gives a large language model (LLM) a closed-loop physical interface (Zhu, 2026a). A single ESP32 microcontroller carries sensors for six environmental modalities and three output channels (a buzzer, a vibration motor and a small display), and two input-output pairs are coupled so that the model receives a reading consistent with its own output having registered in the room. The firmware and the bridge service that exposes the device to a remote LLM client are released under the MIT license, the parts are retail components, and the figure of about €125 comes from the author's announcement on X rather than from the preprint (Zhu, 2026b).

What kind of embodiment this is has to be settled first. The device's outputs are sound, vibration and light addressed to a person in the room. Zhu states that it "cannot pick up a cup, cannot move from where it is, cannot identify or manipulate the objects around it" (Zhu, 2026a, p. 25) and that, by the success criterion of robot embodiment, task completion, "it is not embodied at all" (p. 26). Measured by physical capability, it does not belong with Boston Dynamics' Atlas, and this chapter does not place it there.

¹ Assist. Prof. Dr., Yıldız Technical University, Faculty of Art and Design, Department of Art, Industrial Design Program, ORCID: 0000-0002-6786-479X.

The sense of embodiment at stake is the thinner one Brooks (1991) gave: a system whose "actions are part of a dynamic with the world and have immediate feedback on their own sensations" (p. 570). Zhu's self-perception loops meet that condition in its most minimal form, and nothing stronger.

Two consequences follow. The comparisons with industrial platforms in Section 2 concern capital structure, that is, who is in a position to build a closed loop between a model and a physical environment, not capability. And the argument cannot rest on Zhu's device alone. The same separation of body and model appears at the manipulating end of the open-source range: the SO-101, an arm with five joints and a gripper designed by The Robot Studio with Hugging Face, is released under the Apache-2.0 license with a parts list priced at US\$121.94 per arm, without a statement of whether printing or shipping is included (The Robot Studio, n.d.), and SmolVLA, an openly licensed model for controlling such robots, is "designed to be trained on a single GPU and deployed on consumer-grade GPUs or even CPUs" (Shukor et al., 2025, p. 1). Zhu's device is the low-capability end of this range and the most transparent instance of its architecture, which is why it anchors the analysis.

Bracketing the phenomenological questions Zhu's paper foregrounds, the chapter asks what governance regime emerges when the threshold for closed-loop embodiment falls to retail cost while the model and infrastructure layers on which it depends remain proprietary, paid-access and concentrated. It argues that the open-sourcing of minimal AI embodiment architectures reconfigures embodiment from a corporate-industrial capacity into a layer-dependent governance regime, open at the hardware and software layers, dependent on proprietary infrastructure at the model and cloud layers, producing a frontier where multiple regulatory regimes cover incompatible pieces of the same object, and none carries accountability for the whole.

Several literatures bear on this argument. LLM-driven robotics (e.g., Driess et al., 2023) treats the robot as the engineering substrate and the model as a controller above it. Commons scholarship (Benkler, 2006; Ostrom, 1990) supplies a vocabulary for collectively governed resources, and Internet-law scholarship has argued that regulation should follow the layers of a technical system (Benkler, 2000; Solum & Chung, 2004). Work on open AI has shown that openness in models is graded rather than binary (Liesenfeld & Dingemanse, 2024; Solaiman, 2023) and leaves the concentration of power in AI largely in place (Widder, Whittaker, & West, 2024), and work on algorithmic supply chains has shown how accountability disperses across the actors who jointly produce an AI system (Cobbe, Veale, & Singh, 2023). The contribution here is narrower: it carries the graded reading of openness from the model to the whole embodied stack and asks what the layer structure does to accountability when the person who assembles it acts outside commercial activity.

2. EMBODIMENT'S INDUSTRIAL ASSUMPTION

The most visible pole of embodied AI in the early 2020s was organized by well-capitalized firms. Boston Dynamics was acquired by Hyundai Motor Group in a transaction valuing it at \$1.1 billion (Boston Dynamics, 2021). Such platforms walk, lift and manipulate, and their economics follow from integrated supply chains, proprietary actuators and large engineering teams. They are cited for that capital structure, not as a benchmark for Zhu's device. The theoretical case for embodiment developed alongside this political economy without questioning it: the bodies through which Brooks (1991) argued for situated intelligence were research robots built in an academic laboratory, and who would be in a position to build bodies was not part of the question.

The European instruments that now bear on embodied AI were drafted around the same chain of manufacturers, importers and providers who place products or AI systems on the market (Regulation (EU) 2023/1230; Regulation (EU) 2024/1689). The AI Act has no category for robots: an embodied system becomes high-risk through the product it belongs to, for instance as a safety component of a product listed in Annex I, not because it has a body (Regulation (EU) 2024/1689, Art. 6(1)). Section 5 shows that these instruments are less blind to individual builders than this suggests, since both the AI Act and the Machinery Regulation include natural persons who build for their own use among their addressees. The corporate-industrial assumption operates instead in the material scopes and open-source exclusions through which each instrument decides what counts as a regulable object.

3. OPEN-SOURCE EMBODIMENT AS LAYERED INFRASTRUCTURE

3.1. The Case and Its Evidential Limits

In Zhu's architecture, self-perception pairs the buzzer with a microphone and the motor with an accelerometer, so that each output returns as a number. The microcontroller hosts no model. A bridge service exposes it over HTTPS to any tool-using LLM client, and at runtime the system depends on USB power, residential Wi-Fi and a Cloudflare tunnel (Zhu, 2026a, Sections 3, 9.3, 10.1).

The case has to be weighed before it is used. The preprint has a single human author, who lists two Claude models as collaborators; the Zenodo record gives no indication of peer review, and a later version has since been posted. Its validation, 30 randomized trials per condition, was run on one device, in one room, in a single session (Zhu, 2026a, Section 10.1). The audio loop registers all ten tones at +30 to +56 dB above ambient, but

short haptic transients cannot be distinguished from the no-motor baseline (Sections 6.3, 9.2). The LLM collaborators drafted the code, designed and ran the validation, and drafted the manuscript from its third section onward, while the human author built the device and revised the text (Section 8.1). The most discussed claim, that two model versions produced distinct experiences of co-presence on an unchanged body, is the builder's report about two of the models that co-wrote the paper, gathered without a matched protocol; Zhu notes that a structured comparison would be needed to move the model-agnostic property "from architectural to systematically validated" (Zhu, 2026a, p. 29). The public repository, accessed in September 2026, documents no independent replication (Zhu, n.d.).

The chapter therefore relies only on what can be checked against the published artifact, the system's composition, licensing and runtime dependencies, treats the validation as establishing feasibility and no more, and treats the co-presence report as testimony on which none of its claims depends.

What the checkable part shows is a separation between a reproducible layer and a rented one. In Zhu's formulation the body is the constant and the model the variable (Zhu, 2026a, Section 9.3). The case thus separates three conditions of reproducibility: the retail availability of components, the permissiveness of the licenses on design and code, and the operational dependencies under which the system runs. The first two are commonable. The third, API access, power, residential network and public tunnel, is not.

3.2. Layered Commons as an Analytical Framework

Commons scholarship (Benkler, 2006; Ostrom, 1990) assumes that the resource is reachable by the governance regime in question, and Zhu's case fails the assumption in part: an MIT license reaches her firmware and bridge, and nothing she

publishes reaches the commercial model they call. That technical systems should be analysed layer by layer is not new. Benkler (2000) divided the communications environment into physical, logical and content layers and argued that regulation at each layer shapes whether people act as consumers or as users; Solum and Chung (2004) derived from Internet architecture a principle that law should respect the separation of layers. This tradition already knows that governance differs by layer. What it presupposes is a network whose layers are provisioned by carriers, platforms and publishers. The embodied stack differs in one respect: its layers are assembled at runtime by a single user, who holds full rights in some of them and only contractual access to others.

Layered commons therefore defines its layers independently of the instruments that govern them, by the function a component performs and the form of the resource it constitutes. The hardware layer transduces physical states and consists of rival goods whose ownership transfers on sale. The software layer encodes and routes and consists of non-rival, copyable code. The model layer performs inference; reached through an API, it is a non-rival resource from which the user can be excluded, delivered as a service. The infrastructure layer transports and hosts and consists of rival capacity rented at runtime. Which instruments attach to each layer is then an empirical question (Table 1; artifact details from Zhu, 2026a), not part of the definition.

The no-propagation principle can accordingly be stated with conditions. Openness does not cross a layer boundary when the open side is governed by permissive licenses and the closed side by contracts, because a license releases only rights the licensor holds and a contract binds only its parties: the MIT license on Zhu's bridge grants nothing in Anthropic's model. Two conditions weaken the claim. Reciprocal licenses propagate within a layer; the GNU Affero General Public License requires

a modified program to offer its source to "all users interacting with it remotely through a computer network" (Free Software Foundation, 2007, Section 13), but the obligation attaches to the licensed program, not to a model it calls. More consequentially, an open-weight model run locally moves the model layer onto the builder's own hardware; SmolVLA's weights, for instance, are released under Apache 2.0 (Hugging Face, n.d.). What then remains out of reach is frontier capability, not the model layer as such. The asymmetry examined here is contingent: it holds where, as in Zhu's configuration, the capability the builder wants is available only by API.

Table 1. The Four Layers of the Embodied Stack in Zhu's Configuration

Layer	Function and resource form	Instruments that attach	Concentration	Commonable here?
Hardware	Transduces physical state; rival goods sold outright (ESP32, sensors, outputs)	Product-safety and radio-equipment law; open-hardware definitions (Open Source Hardware Association, 2011)	Retail-competitive components	Yes: retail availability
Software	Encodes and routes; copyable code (firmware and bridge, MIT license)	Open-source licensing; copyright	Distributed contribution (Blind et al., 2021)	Yes: permissive licensing
Model	Infers; access-excludable service (frontier LLM via paid API)	Provider terms; AI Act Art. 53, with the Art. 53(2) exemption limited to open-weight models	Few providers; Anthropic and OpenAI models reached the body (Zhu, 2026a)	No at frontier scale; small open-weight models are
Infrastructure	Transports and hosts; rival capacity rented at runtime (Wi-Fi, ISP, tunnel)	Provider terms; telecoms and data-protection law	70 to 80% of cloud market held by three providers (OECD, 2025)	No: rented at runtime

The asymmetry has a material basis in who pays for what. A study for the European Commission estimated that about €1

billion of EU corporate investment in open-source software in 2018 produced an economic impact of €65 to €95 billion (Blind et al., 2021): the software commons runs on contributed labor with large spillovers. The OECD (2025) reports that 70 to 80% of the global cloud market is held by Amazon Web Services, Microsoft Azure and Google Cloud, and Widder et al. (2024) argue that openness has not disturbed the concentration of the resources, including compute, on which frontier models depend. The maintenance budget for Zhu's hardware and software is contributed labor; for the model and infrastructure layers it is rent paid to a few firms, under terms that govern what the open code can do once it runs.

3.3. Historical Precedent Patterns

The pattern has precedents at other positions in the stack, analogies with specified points of contact rather than identities. Amazon's Ring doorbells combine retail hardware installed by residents with a corporate cloud; Calacci, Shen and Pentland (2022) document over half a million publicly shared Ring-Neighbors videos between 2016 and 2020 and police access to footage developing largely outside the warrant requirements that govern state surveillance. One layer up, Hawkins, Russell and Mittelstadt (2025) identified about 35,000 downloadable deepfake model variants depicting identifiable people, 96% of those built on Stable Diffusion and Flux targeting female-presenting individuals, produced with as few as 20 images and about fifteen minutes of training on consumer hardware. That case is close to Zhu's in composition, open weights, consumer compute and individual execution, and differs in that harm is the purpose of many variants. The European response matters for Section 5: the 2026 amendment of the AI Act prohibited placing on the market, putting into service or using AI systems that generate or manipulate realistic intimate or sexually explicit material of identifiable persons without their explicit consent

(Regulation (EU) 2024/1689, Art. 5(1)(ba), as inserted by Regulation (EU) 2026/1744). An instrument keyed to a practice reaches the individual user whatever layer the tool sits on. In both cases a threshold falls, deployment spreads across individual operators, the platform layers stay concentrated, and governance arrives around uses rather than objects; Zhu's case follows the pattern with the body open and the model rented.

4. RELATIONAL BEHAVIOR AT THE MODEL LAYER

That people respond socially to communicative machines, without needing a face or a body, is well established (Reeves & Nass, 1996); anthropomorphism and companionship are outside this chapter's scope. The question here is where, in a layered system, the cues that elicit those responses are produced, and who controls that layer.

In Zhu's architecture the body's contribution is fixed: it returns readings and executes commands through a published API. Which sensors are read and when, which outputs are fired, and how readings are framed back to the person are decisions taken by the model client (Zhu, 2026a, Sections 3, 9.3). This is verifiable in the code. Zhu's report that one Claude version mainly narrated the room while another mainly fired outputs and read back their echoes (Section 9.3) illustrates the variation the architecture permits; it cannot show how large or stable that variation is.

Lekova, Tsvetkova and Stefanov (2026) supply a second case with the same design property. Their rehabilitation deployment of the Furhat robot head is built so that "all cloud services and LLMs are integrated in a modular and optional manner, allowing components to be substituted or deployed locally" (p. 4). Comparing four LLMs on synthetic patient

narratives, they found factual-contradiction rates from 22.7% to 40%, although human validation used a single model. The two cases support a limited claim: substitution at the model layer is a design property, and changing the model measurably changes generated text; whether it changes co-presence with a person remains open.

The consequence for the layered reading is specific. The system's relational behavior, its rhythm of attention and its framing of the room, is produced at the layer that in Zhu's configuration is reached by paid API and governed by the provider's terms. The instruments on the open layers cannot specify that behavior, for a legal reason: a license releases an artifact the licensor holds, and this behavior is the runtime output of a model the builder does not hold. Publishing firmware, parts list and API makes the conditions of the interaction reproducible, not the interaction, because the generator stays with the provider, which can update or withdraw it. With an open-weight model run locally the builder would hold the generator, and the behavior would become inspectable and repeatable. In the configuration examined here it is neither. The layer at which the system does its relational work is the layer the commons does not reach.

5. THE REGULATORY PATCHWORK

That accountability disperses across the actors who produce computational systems is established, from Nissenbaum's (1996) problem of many hands to algorithmic supply chains (Cobbe et al., 2023), and the open-source exemptions in European AI law have been examined for models (Liesenfeld & Dingemanse, 2024). This section therefore does not claim to find a vacuum. It reads how four instruments treat a configuration assembled by a natural person outside commercial activity, with a physical layer attached: the AI Act (Regulation

(EU) 2024/1689, as amended by Regulation (EU) 2026/1744), the Machinery Regulation (Regulation (EU) 2023/1230), the Product Liability Directive (Directive (EU) 2024/2853) and the Cyber Resilience Act (Regulation (EU) 2024/2847).

Under the AI Act the first question is whether there is an AI system at all, that is, a system that "infers, from the input it receives, how to generate outputs" that "can influence physical or virtual environments" (Art. 3(1)). Zhu's firmware and bridge infer nothing; a system meeting the definition comes into being when the builder couples the body to a model. Whoever does so plausibly develops an AI system and puts it into service, which includes supply "for own use" (Art. 3(11)), and a provider may be a natural person acting "whether for payment or free of charge" (Art. 3(3)). The Act does not lack an addressee; it lacks obligations for that addressee. Deployer obligations do not apply to "purely personal non-professional activity" (Art. 2(10)); systems under free and open-source licenses are excluded unless they are high-risk or fall under Article 5 or 50 (Art. 2(12)); and the configuration is not high-risk, since it is no safety component under Annex I and the employment category in Annex III concerns recruitment, work decisions and monitoring, not systems that merely operate in a workplace. One duty survives: systems "intended to interact directly with natural persons" must inform those persons that they are interacting with AI unless this is obvious (Art. 50(1)). At the model layer the Act reaches the provider, who owes documentation and information to downstream providers (Art. 53(1)(a), (b)), an obligation lifted only for models with public weights under a free and open-source license and without systemic risk (Art. 53(2)). The 2026 amendment left these provisions unchanged. The Act's reach is thin rather than absent, and it is organized by layer.

The Machinery Regulation, applicable from 14 January 2027, likewise includes natural persons who manufacture

products "and puts those products into service for its own use" (Art. 3(18)(b)). The obstacle is material scope. Machinery is an assembly with a drive system "consisting of linked parts or components, at least one of which moves" (Art. 3(1)(a)); the vibration motor moves, but electrical and electronic products within the Low Voltage or Radio Equipment Directives are excluded where they are household appliances, audio and video equipment or information technology equipment (Art. 2(2)(p)), and a Wi-Fi microcontroller device is most plausibly such a product (see Directive 2014/53/EU, Art. 1(1)). A self-built SO-101 arm, a motorized assembly joined for manipulation, is a stronger candidate, and its builder a manufacturer for own use. Regulatory reach at the hardware layer thus rises with physical capability, while the dependence on the model layer stays the same across the range.

The Product Liability Directive applies to products placed on the market or put into service after 9 December 2026 (Art. 2(1)). It treats software as a product whether "stored on a device, accessed through a communication network or cloud technologies, or supplied through a software-as-a-service model" (recital 13), and counts as manufacturer one who develops a product "for their own use" (Art. 4(10)(c)). It excludes "free and open-source software that is developed or supplied outside the course of a commercial activity" (Art. 2(2)); publishing such software on open repositories is not making it available on the market (recital 14), and where it is integrated into a commercial product the integrator may be liable, "but not the manufacturer of the software" (recital 15). Read by layer, the Directive withholds liability from the layer Zhu published and leaves it available against the commercially supplied layers, the components and, on the reading recital 13 supports, a model supplied as a service. The Cyber Resilience Act, whose obligations apply from 11 December 2027 (Art. 71(2)), shows that the legislator has built a

dedicated addressee for open source: the "open-source software steward", "a legal person" supporting free software "intended for commercial activities" under "a light-touch and tailor-made regulatory regime" (Art. 3(14); recital 19). An individual who publishes a device's firmware for others to build is neither a legal person nor a commercial supplier.

The instruments are aware of the configuration; what the reading shows is how they draw their lines, each taking a layer, or an actor defined by a layer, as its object. The builder is a provider with a transparency duty under the AI Act, a manufacturer under the Machinery Regulation whose device most likely falls outside its scope, and outside the Directive and the Cyber Resilience Act for what she published; the model provider carries documentation duties and, plausibly, product liability. No instrument takes the assembled runtime configuration as its object. Ostrom's first design principle requires that the users and "the boundaries of the CPR itself" be "clearly defined" (Ostrom, 1990, p. 91); Zhu's configuration is a coherent technical object whose governance object is divided among regimes with different users and protected parties. Narrowing the Directive's open-source exclusion or widening the Machinery Regulation's scope would move a boundary within one layer without making the composed object an addressee. The one measure in this chapter that reaches across layers, the deepfake prohibition in Section 3.3, does so by regulating a practice rather than a layer.

6. CONCLUSION: AFTER THE €125 BODY

Read together, the sections yield three conclusions. First, the three conditions of reproducibility named in Section 3.1 now carry the results of Sections 4 and 5. Retail availability and permissive licensing are commonable; operational access is not, and the model and infrastructure layers within it are the

concentrated ones. Section 4 showed that this layer is also where the system's relational behavior is generated, and Section 5 that it is where European law addresses a commercial provider rather than the builder. In the configuration examined, the layer that does the most work in an interaction is the layer the commons does not reach. With an open-weight model run locally that coincidence would loosen, which is why it is a property of the configuration rather than of embodiment as such.

Second, classrooms and makerspaces, where such systems are most likely to spread, pool equipment and mentorship, but at the operational layer they pool payment rather than capacity: a shared API account, a budget for inference. Pooling redistributes who pays the rent without removing it.

Third, the consent question Zhu defers lands on no single layer. Deployment in cafés, transit or workplaces, she writes, would require explicit consent from co-present individuals (Zhu, 2026a, Section 10.3); licensing on the open layers has no mechanism for non-users, and terms on the closed layers address customers. The instrument that does address the bystander is data-protection law, through a household boundary. The General Data Protection Regulation does not apply to processing "by a natural person in the course of a purely personal or household activity" (Regulation (EU) 2016/679, Art. 2(2)(c)), the Court of Justice has held that a home camera which "also monitors a public space" falls outside that exemption (Case C-212/13, *Ryneš*, 2014, para. 35), and the Regulation still applies to those "which provide the means for processing personal data for such personal or household activities" (recital 18), which would plausibly include a model provider receiving the readings. Whether the device's readings are personal data depends on identifiability, which this chapter does not settle. Bystander protection begins where the device leaves the home, the point Zhu names, and then attaches

to the builder and the model provider in separate relations, with nothing that governs the composed system in the café.

The separation that makes embodiment accessible, body as constant and model as variable, also places the operational layer with concentrated providers. This returns the chapter to its thesis: the open-sourcing of minimal AI embodiment architectures reconfigures embodiment from a corporate-industrial capacity into a layer-dependent governance regime, open at the hardware and software layers, dependent on proprietary infrastructure at the model and cloud layers, producing a frontier where multiple regulatory regimes cover incompatible pieces of the same object, and none carries accountability for the whole. The question to drop is whether the model is open. The question to take up is which layers of the stack are governed, by whom, under what rules, with what maintenance budget, and with what incident records.

REFERENCES

- Benkler, Y. (2000). From consumers to users: Shifting the deeper structures of regulation toward sustainable commons and user access. *Federal Communications Law Journal*, 52(3), 561–579.
- Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. New Haven, CT: Yale University Press.
- Blind, K., Böhm, M., Grzegorzewska, P., Katz, A., Muto, S., Pätsch, S., & Schubert, T. (2021). *The impact of open source software and hardware on technological independence, competitiveness and innovation in the EU economy: Final study report*. Luxembourg: Publications Office of the European Union. Retrieved from <https://op.europa.eu/en/publication-detail/-/publication/84834aa9-2c2d-11ec-bd8e-01aa75ed71a1>
- Boston Dynamics. (2021). *Hyundai Motor Group completes acquisition of Boston Dynamics from SoftBank* [Press release]. Retrieved from <https://bostondynamics.com/news/hyundai-motor-group-completes-acquisition-of-boston-dynamics-from-softbank/>
- Brooks, R. A. (1991). Intelligence without reason. In *Proceedings of the 12th International Joint Conference on Artificial Intelligence* (pp. 569–595). Retrieved from <https://www.ijcai.org/Proceedings/91-1/Papers/089.pdf>
- Calacci, D., Shen, J. J., & Pentland, A. (2022). The cop in your neighbor's doorbell: Amazon Ring and the spread of participatory mass surveillance. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2), Article 400. doi:10.1145/3555125

- Case C-212/13, František Ryneš v Úřad pro ochranu osobních údajů, ECLI:EU:C:2014:2428 (Court of Justice of the European Union, December 11, 2014).
- Cobbe, J., Veale, M., & Singh, J. (2023). Understanding accountability in algorithmic supply chains. In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency* (pp. 1186–1197). New York, NY: ACM. doi:10.1145/3593013.3594073
- Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC. (2014). *Official Journal of the European Union*. Retrieved from <http://data.europa.eu/eli/dir/2014/53/oj>
- Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC. (2024). *Official Journal of the European Union*, L 2024/2853. Retrieved from <http://data.europa.eu/eli/dir/2024/2853/oj>
- Driess, D., Xia, F., Sajjadi, M. S. M., Lynch, C., Chowdhery, A., Ichter, B., . . . Florence, P. (2023). PaLM-E: An embodied multimodal language model. In *Proceedings of the 40th International Conference on Machine Learning* (pp. 8469–8488). Retrieved from <https://proceedings.mlr.press/v202/driess23a.html>
- Free Software Foundation. (2007). *GNU Affero General Public License* (Version 3). Retrieved from <https://www.gnu.org/licenses/agpl-3.0.en.html>

- Hawkins, W., Russell, C., & Mittelstadt, B. (2025). Deepfakes on demand: The rise of accessible non-consensual deepfake image generators. In *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency* (pp. 1602–1614). New York, NY: ACM. doi:10.1145/3715275.3732107
- Hugging Face. (n.d.). *lerobot/smolvla_base* [Model card]. Retrieved September 23, 2026, from https://huggingface.co/lerobot/smolvla_base
- Lekova, A., Tsvetkova, P., & Stefanov, T. (2026). Human-AI co-research on design and evaluation of embodied conversational agent in rehabilitation contexts. *Frontiers in Robotics and AI*, 13, Article 1758391. doi:10.3389/frobt.2026.1758391
- Liesenfeld, A., & Dingemanse, M. (2024). Rethinking open source generative AI: Open-washing and the EU AI Act. In *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency* (pp. 1774–1787). New York, NY: ACM. doi:10.1145/3630106.3659005
- Nissenbaum, H. (1996). Accountability in a computerized society. *Science and Engineering Ethics*, 2(1), 25–42. doi:10.1007/BF02639315
- OECD. (2025). *Competition in the provision of cloud computing services* (OECD Roundtables on Competition Policy Papers No. 323). Paris, France: OECD Publishing. doi:10.1787/595859c5-en
- Open Source Hardware Association. (2011). *Open source hardware definition (version 1.0)*. Retrieved from <https://www.oshwa.org/definition/>

Ostrom, E. (1990). *Governing the commons: The evolution of institutions for collective action*. Cambridge, England: Cambridge University Press.

Reeves, B., & Nass, C. (1996). *The media equation: How people treat computers, television, and new media like real people and places*. New York, NY: Cambridge University Press.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union*, L 119, 1–88. Retrieved from <http://data.europa.eu/eli/reg/2016/679/oj>

Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC. (2023). *Official Journal of the European Union*, L 165, 1–102. Retrieved from <http://data.europa.eu/eli/reg/2023/1230/oj>

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). (2024). *Official Journal of the European Union*, L 2024/1689. Retrieved from <http://data.europa.eu/eli/reg/2024/1689/oj>

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828

- (Cyber Resilience Act). (2024). *Official Journal of the European Union*, L 2024/2847. Retrieved from <http://data.europa.eu/eli/reg/2024/2847/oj>
- Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI). (2026). *Official Journal of the European Union*, L 2026/1744. Retrieved from <http://data.europa.eu/eli/reg/2026/1744/oj>
- Shukor, M., Aubakirova, D., Capuano, F., Kooijmans, P., Palma, S., Zouitine, A., . . . Cadene, R. (2025). *SmolVLA: A vision-language-action model for affordable and efficient robotics* (arXiv:2506.01844). Retrieved from <https://arxiv.org/abs/2506.01844>
- Solaiman, I. (2023). The gradient of generative AI release: Methods and considerations. In *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency* (pp. 111–122). New York, NY: ACM. doi:10.1145/3593013.3593981
- Solum, L. B., & Chung, M. (2004). The layers principle: Internet architecture and the law. *Notre Dame Law Review*, 79(3), 815–948.
- The Robot Studio. (n.d.). *SO-ARM100* [GitHub repository]. Retrieved September 23, 2026, from <https://github.com/TheRobotStudio/SO-ARM100>
- Widder, D. G., Whittaker, M., & West, S. M. (2024). Why 'open' AI systems are actually closed, and why this matters. *Nature*, 635(8040), 827–833. doi:10.1038/s41586-024-08141-1

- Zhu, O. (n.d.). *minimal-embodiment* [GitHub repository]. Retrieved September 23, 2026, from <https://github.com/oliviazzzu/minimal-embodiment>
- Zhu, O. (2026a). *A minimal self-perceiving embodiment for large language models* [Preprint]. doi:10.5281/zenodo.19903098
- Zhu, O. [oliviazzzu]. (2026b, April 30). *My Claude wanted a body, so I built him a small one. It runs on an ESP32, letting Claude perceive...* [Tweet]. Retrieved from <https://x.com/oliviazzzu/status/2049778751689425392>

**YÖNETİM BİLİŞİM SİSTEMLERİ ALANINDA
GÜNCEL KONULAR VE
AKADEMİK DEĞERLENDİRMELER**

yaz
yayınları

YAZ Yayınları
M.İhtisas OSB Mah. 4A Cad. No:3/3
İscehisar / AFYONKARAHİSAR
Tel : (0 531) 880 92 99
yazyayinlari@gmail.com • www.yazyayinlari.com