TEMMUZ 2026
SAYI 4

BTKıbrıs

Bilim, Bilişim, Teknoloji Dergisi

Dijital dünyaya bağlanın.

btkibris.org

Editörün yazısı: BT Kıbrıs Büyüyor...

Merhaba sevgili okurlarımız;

Dördüncü sayımızla sizlerle yeniden buluşmanın heyecanını yaşıyoruz.

Kısa sayılabilecek bu yayın yolculuğunda, BT Kıbrıs olarak yalnızca teknolojik gelişmeleri aktaran bir dergi olmanın ötesine geçmeyi; bilişim alanında bilgi üreten, deneyim paylaşımını teşvik eden ve çözüm odaklı yaklaşımları öne çıkaran bir platform olmayı hedefledik.

Geride bıraktığımız üç sayıda ülkemizin bilim ve bilişim dünyasındaki uzmanların katkılarıyla siber güvenlikten yapay zekâya, dijital dönüşümden yazılım geliştirmeye kadar pek çok güncel konuyu ele aldık.

Okuyucularımızdan aldığımız değerli geri bildirimler ise doğru bir yolda ilerlediğimizin en önemli göstergesi oldu.

Dijital dünyanın sürekli değiştiği bir dönemde, bilgiye ulaşmak kadar doğru bilgiyi paylaşmak ve ortak aklı geliştirmek de büyük önem taşımaktadır. Bu anlayışla hazırladığımız dördüncü sayımızda da sektör profesyonellerinin, akademisyenlerin ve teknolojiye yön veren isimlerin görüşlerini sizlerle buluşturmaya devam ediyoruz.

Kuzey Kıbrıs Türk Cumhuriyeti'nin bilişim ekosisteminin güçlenmesine katkı sağlayacak her fikir, her proje ve her başarı hikâyesi bizim için ayrı bir değerdir. Bu yolculukta bizleri takip eden, görüşleriyle katkı sunan tüm okuyucularımıza ve kalemleriyle dergimize değer katan yazarlarımıza teşekkür ediyor; birlikte üreten, paylaşan ve geleceği şekillendiren güçlü bir bilişim topluluğu oluşturma hedefiyle yeni sayılarımızda da sizlerle buluşmayı diliyoruz.

Ahmet HIZLI

Bilgisayar Mühendisi (M.Sc.)

BT Kıbrıs Editörü

KKTC'de Bilgi ve İletişim Teknolojileri (ICT) Sektöründe Kurumsallaşma Sorunsalı: Türkiye ve Kıbrıs Cumhuriyeti Ekseninde Bir Karşılaştırma ve Eksik Kurum Analizi

Yusuf KÜÇÜK
yusufkucuk2014@gmail.com

Bilgi ve İletişim Teknolojileri (ICT), modern devlet yapılarının egemenlik, siber güvenlik, e-devletleşme ve ekonomik kalkınma süreçlerinin merkezinde yer almaktadır. Kuzey Kıbrıs Türk Cumhuriyeti (KKTC), yüksek üniversite popülasyonu ve genç iş gücü ile bilişim odaklı bir büyüme potansiyeline sahip olmasına rağmen, bu potansiyeli makro ekonomik ve idari bir avantaja dönüştürmekte zorlanmaktadır. Bu çalışmanın temel amacı, KKTC'deki ICT ekosisteminin "kurumsallaşamama" problemini yasal ve yapısal boyutlarıyla ortaya koymaktır.
Çalışmada metodoloji olarak; Türkiye Cumhuriyeti ve Kıbrıs Cumhuriyeti'nin kurumsal ve mevzuat altyapıları referans noktası (benchmarking) alınarak bir boşluk analizi (gap analysis) yürütülmüştür. Ayrıca ekosistemin bilimsel ve teknolojik ayağını oluşturan yükseköğretim ağları, "Ulusal Akademik Ağ" (NREN) perspektifinden incelenmiştir. Elde edilen bulgular, KKTC'de mevzuatın güncelliğini yitirdiğini, stratejik yönetim kademelerinde yetki karmaşası yaşandığını; siber güvenlik, veri koruma ve akademik altyapı alanlarında operasyonel "eksik kurumlar" (boş kutular) bulunduğunu göstermektedir. Çalışmanın sonunda, KKTC'nin dijital dönüşümünü sürdürülebilir kılacak kurumsal şema ve yasal reform önerileri sunulmuştur.

1. Giriş

Yirmi birinci yüzyılda devletlerin egemenlik sınırları yalnızca fiziksel toprak parçalarıyla değil, sahip oldukları dijital altyapılar, veri merkezleri ve siber ağların güvenliğiyle de ölçülmektedir. Bilgi ve İletişim Teknolojileri (ICT), kamunun şeffaflaşması, e-devlet hizmetlerinin etkinliği ve katma değerli ekonomik büyüme için anahtar role sahiptir. KKTC, coğrafi kısıtlamalar ve tanınma sorunları nedeniyle konvansiyonel sanayi ve ticaret alanlarında küresel pazarlara erişimde dezavantajlı konumdadır. Ancak bilişim sektörü, lojistik ve coğrafi sınırlardan bağımsız yapısı gereği KKTC için yapısal ekonomik tıkanıklığı aşabilecek en stratejik sektördür.

Buna karşın, adadaki ICT ekosistemi incelendiğinde; teknolojik yatırımların bütüncül bir devlet politikasına dönüşemediği, kurumlar arası mükerrer yatırımların yapıldığı ve en önemlisi çağdaş riskleri göğüsleyecek kurumsal yapıların hukuken ve fiilen tesis edilemediği görülmektedir. Bu çalışma; KKTC'deki kurumsallaşma açığını, adanın coğrafi komşusu ve üyesi olduğu uluslararası normlar (AB) bakımından Kıbrıs Cumhuriyeti ile kurumsal ve finansal hamisi konumundaki Türkiye Cumhuriyeti ekseninde ve "Ulusal Akademik Ağ" vizyonu çerçevesinde incelemektedir.

2. Mevzuat Analizi ve Hukuki Altyapı Kıyaslaması

Kurumların operasyonel yetkinliği, hukuki meşruiyeti ve yaptırım gücü, üzerine inşa edildikleri yasal mevzuatın derinliği ve dinamizmi ile doğrudan ilişkilidir. Teknolojinin geometrik bir hızla ilerlediği bir dönemde, mevzuatın statik kalması kurumsal felce (legislative paralysis) yol açmaktadır.

2.1. Elektronik Haberleşme ve Regülasyon Mevzuatı

KKTC'de bilişim ve telekomünikasyon sektörünün anayasası niteliğindeki düzenleme, 6/2012 sayılı Elektronik Haberleşme Yasası'dır. Bu yasa, dönemin ihtiyaçlarına göre Bilgi Teknolojileri ve Haberleşme Kurumu'nu (BTHK) kurarak pazarı regüle etme misyonunu başarıyla üstlenmiştir. Ancak kabul edildiği 2012 yılından bugüne geçen sürede; bulut bilişim (cloud computing), 5G ve ötesi mobil altyapılar, yapay zeka entegrasyonları ve nesnelerin interneti (IoT) gibi kavramlar yasal düzlemde karşılık bulamamıştır.

Türkiye Cumhuriyeti'nde ise 5809 sayılı Elektronik Haberleşme Kanunu (2008), Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yayınlanan yönetmelik ve tebliğlerle sürekli dinamik tutulmakta ve AB müktesebatına uyum çerçevesinde güncellenmektedir. Kıbrıs Cumhuriyeti tarafında ise durum tamamen Avrupa Birliği standartlarına endekslidir. AB'nin Elektronik Haberleşme Kodu (EECC - Directive (EU) 2018/1972) ulusal hukuka adapte edilmiş olup, altyapı paylaşımından pazar rekabetine kadar tüm süreçler supranasyonel standartlarla güvence altına alınmıştır.

2.2. Siber Güvenlik ve Kritik Altyapı Koruma Mevzuatı

Siber güvenlik, KKTC mevzuatının en zayıf halkasıdır. Adada müstakil bir "Siber Güvenlik Yasası" bulunmamaktadır. Siber güvenliğe dair yükümlülükler, 6/2012 sayılı yasanın altındaki tüzükler ve ikincil mevzuatlarla idare edilmeye çalışılmaktadır. Bu durum, finans (bankacılık), enerji ve e-devlet gibi kritik altyapıların siber savunmasında yasal yaptırım ve denetim boşluğu yaratmaktadır.

Buna karşılık Türkiye, Ulusal Siber Güvenlik Stratejisi ve Eylem Planları ile süreci makro düzeyde yürütmekte; BTK ve USOM tebliğleriyle kurumlara yasal siber ödevler yüklemektedir. Kıbrıs Cumhuriyeti ise AB'nin en güncel siber güvenlik mevzuatı olan NIS 2 (Network and Information Security) Direktifi'ni yürürlüğe koymuştur. NIS 2, kritik altyapı sağlayıcılarında yaşanacak siber ihlallerde şirketlerin küresel ciroları üzerinden milyonlarca avroluk idari para cezaları öngören, son derece katı ve bağlayıcı bir yasal yaptırım mekanizması sunmaktadır.

2.3. Kişisel Verilerin Korunması Mevzuatı

KKTC, 89/2007 sayılı Kişisel Verilerin Korunması Yasası'na sahiptir. Yasa biçimsel olarak var olsa da, ruhu itibarıyla günümüz küresel veri standardı olan AB GDPR (General Data Protection Regulation) normlarının gerisinde kalmıştır. "Büyük Veri" (Big Data) çağında, verinin yurt dışına aktarımı, veri sorumlularının sicili ve "unutulma hakkı" gibi kavramlar mevcut yasada tanımlı değildir. En kritik kurumsal açık ise, bu yasayı ihlal eden kamu ve özel sektör aktörlerini yargılayıp cezalandıracak bağımsız bir üst kurulun fiilen operasyonel olmamasıdır.

Türkiye, 2016'da yürürlüğe soktuğu 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ve buna bağlı kurulan bağımsız KVKK Kurumu ile veri güvenliğini çok sıkı denetlemektedir. Kıbrıs Cumhuriyeti ise doğrudan GDPR mevzuatına tabi olup, veri ihlallerine karşı Kişisel Verilerin Korunması Komiserliği eliyle doğrudan cezai yaptırım uygulamaktadır.

Tablo 1: Düzenleme ve Altyapı Alanlarında Mevzuat Kıyaslaması (Gap Analysis)

Düzenleme Alanı	KKTC	Türkiye Cumhuriyeti	Kıbrıs Cumhuriyeti (AB)	KKTC'deki Yapısal Boşluk (Gap)
Elektronik Haberleşme	6/2012 Sayılı EHY	5809 Sayılı EHK	AB Elektronik Haberleşme Kodu	Güncel küresel teknolojilerin (5G, Bulut) yasada hiyerarşik yer bulamaması.
Siber Güvenlik	Müstakil yasa yok (Tüzük seviyesinde)	Ulusal Strateji Belgeleri & BTK Tebliğleri	NIS 2 Direktifi (Bağlayıcı Kanun)	Kritik altyapıları koruyacak, yaptırım gücü yüksek ana siber yasanın eksikliği.
Veri Koruma	89/2007 Sayılı Yasa	6698 Sayılı KVKK	GDPR (Genel Veri Koruma Yönetmeliği)	Yasanın çağ dışı kalması ve bağımsız denetleyici üst kurulun kurulmamış olması.
Ulusal Akademik Ağ (NREN)	Müstakil bir yasa veya kurumsal çatı yok.	278 sayılı TÜBİTAK Kanunu uyarınca işletilen ULAKBİM mevzuatı.	CYNET (Cyprus Research and Academic Network) Hukuki Yapısı ve AB Dijital Gündemi.	Akademik trafiği, siber güvenlik istihbaratını ve büyük veriyi ticari ağlardan ayırıp koruyacak yasal statünün eksikliği.

3. Kurumsal Şema Kıyaslaması (Benchmarking)

Mevzuat boşlukları, doğal olarak kurumsal şemada da "hiç var olmamış" ya da "fonksiyonel felce uğramış" departmanlar yaratmaktadır. Üç ülkenin dikey hiyerarşik şeması kıyaslandığında KKTC'deki kurumsal boşluklar net bir şekilde görünmektedir.

Tablo 2: Dikey Hiyerarşik Kurumsal Şema Karşılaştırması

[SEVİYE]	[TÜRKİYE]	[KIBRIS CUMHURİYETİ]	[KKTC]
POLİTİK / STRATEJİK	Cumhurbaşkanlığı Dijital Dönüşüm Ofisi	Araştırma, İnovasyon ve Dijital Politika Müsteşarlığı	Başbakanlık DDEDK (Kısıtlı yetki ve bütçe)
REGÜLASYON / DENETLEME	BTK (Bağımsız Üst Kurul)	OCECPR (Bağımsız Otorite)	BTHK (Aktif ama yükü fazla)
ULUSAL AKADEMİK AĞ	TÜBİTAK ULAKBİM (TRUBA, Eduroam, Ulusal Akademik Omurga)	CYNET (Avrupa Araştırma Ağı - GEANT Tam Üyesi)	**[BOŞ KUTU]** (Üniversiteler ticari ISP omurgalarına bağımlı ve dağınık)
SİBER GÜVENLİK	USOM (Ulusal Müdahale)	DSA / CyCERT (AB Entegre)	**[BOŞ KUTU]** (Müstakil USOM/SOME yok)
VERI KORUMA	KVK Kurumu (Aktif Ceza/Denetim)	Kişisel Veri Komiserliği (GDPR Yetkili)	**[BOŞ KUTU]** (Yasa var, Kurul/Yaptırım yok)
AR-GE / FONLAMA	TÜBİTAK / KOSGEB / Teknoparklar	IDEK (Araştırma ve İnovasyon Vakfı)	**[YETERSİZ / DAĞINIK]** (Üniversite odaklı, yerel fon yok)

3.1. Stratejik Seviyede Kurumsal Analiz

Türkiye'de Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Güney Kıbrıs'ta ise doğrudan Bakanlar Kurulu düzeyinde temsil edilen Araştırma, İnovasyon ve Dijital Politika Müsteşarlığı devletin dijital vizyonunu tek elden çizer. KKTC'de ise bu rol, yakın dönemde mevzuatı geliştirilmeye çalışılan Başbakanlık altındaki Dijital Dönüşüm ve Elektronik Devlet Kurumu (DDEDK) tarafından yürütülmeye çalışılmaktadır.

Ancak bu yapı, bağımsız bütçeli özerk bir ajans veya müstakil bir müsteşarlık ağırlığına sahip değildir. Bürokratik hiyerarşide diğer bakanlıkların (örneğin Bayındırlık ve Ulaştırma Bakanlığı, Maliye Bakanlığı) bilişim bütçeleri ve projeleri üzerinde nihai ve bağlayıcı bir koordinasyon kurmakta zorlanmaktadır. Bu durum, adada e-devlet projelerinin yavaş ilerlemesi ve parça parça (silolar halinde) büyümesi sonucunu doğurmaktadır.

3.2. Operasyonel Seviyede Kurumsal Analiz (Siber Güvenlik, Veri Koruma ve Akademik Ağ)

Kurumsal şemanın en alarm veren kısmı operasyonel katmandır. Türkiye'de USOM, Kıbrıs Cumhuriyeti'nde ise DSA/CyCERT 7/24 siber tehdit istihbaratı toplayıp siber olaylara anında müdahale ederken; KKTC şemasında "Ulusal SOME / CERT" kutusu tamamen boştur. Benzer şekilde, veriyi denetleyecek bir üst kurul (KVKK muadili) şemada aktif yer almadığı için, KKTC'de e-devlet veri merkezinin veya vatandaşlık verilerinin güvenliği, yasal denetimden yoksun bir biçimde yalnızca kamudaki kısıtlı personelin bireysel özverisine kalmıştır.

Bu operasyonel boşluk, akademik altyapı boyutunda da kendini göstermektedir. Türkiye ve AB tarafında akademik ağlar (ULAKBİM ve CYNET) kamu ve üniversite veri trafiğini ticari hatlardan yalıtıp güvenli bir omurgaya oturturken, KKTC'de yükseköğretim kurumları tamamen ticari servis sağlayıcıların (ISP) insiyatifine dağılmış durumdadır.

4. Tartışma ve Bulgular

Elde edilen yasal ve şematik veriler doğrultusunda KKTC ICT sektöründeki kurumsallaşma problemi dört temel başlık altında özetlenebilir:

- **Kurum Enflasyonu Değil, Fonksiyon Eksikliği:** KKTC'de sorun yeni binalar inşa etmek veya tabelalar asmak değildir. BTHK regülasyon görevini başarıyla yapmaktadır; ancak siber güvenlik müdahale (CERT) ve veri koruma (KVKK) gibi farklı fonksiyonel uzmanlıkların aynı potada eritilmeye çalışılması kurumsal verimliliği düşürmektedir.
- **Siyasi Sürdürülebilirlik Problemi:** Türkiye ve Kıbrıs Cumhuriyeti'ndeki üst düzey ICT yapıları (Ofis ve Müsteşarlık), hükümetler veya bakanlar değişse dahi devletin makro-dijital stratejisini kesintisiz sürdürecek şekilde yasal zırhla donatılmıştır. KKTC'de ise bilişim vizyonu, koalisyon hükümetlerinin ömrü ve ilgili bakanın kişisel inisiyatifi ile sınırlı kalmaktadır.
- **Finansman ve İnovasyon Kopukluğu:** Kıbrıs Cumhuriyeti Araştırma ve İnovasyon Vakfı (IDEK) ve Türkiye'deki TÜBİTAK/KOSGEB mekanizmaları sektörü milyonlarca liralık/avroluk fonlarla beslerken; KKTC'de üniversitelerin teknoparkları ile yerel bilişim start-up'larını doğrudan fonlayacak, devlet eliyle yönetilen kurumsal bir "Bilişim ve Ar-Ge Fon Ajansı" bulunmamaktadır.
- **Akademik Ağ Parçalanmışlığı ve Ortak Siber Savunma (Ağ Egemenliği) Eksikliği:** KKTC, yüksek üniversite popülasyonu ve öğrenci yoğunluğuyla yapısal bir avantaja sahip görünse de, bu akademik güç kurumsal bir Ulusal Akademik ve Araştırma Ağı (NREN) çatısı altında konsolide edilememiştir.
- *Münferit Çözümler ve Kamu Kaynağı İsrafı:* Adadaki her üniversite, kendi internet çıkışını, bant genişliğini ve siber güvenlik duvarı hizmetlerini ticari internet servis sağlayıcılardan (ISP) münferit olarak satın almaktadır. Bu durum, ortak bir ulusal akademik omurga (backbone) olmamasından ötürü mükerrer altyapı yatırımlarına ve ciddi mali kaynak israfına yol açmaktadır.
- *Akademik Siber Güvenlik Kör Noktası (Akademik SOME Eksikliği):* Devasa öğrenci ve akademisyen kitlelerinin veri trafiği, ortak bir siber tehdit istihbarat mekanizmasından yoksundur. Türkiye'de ULAKBİM ve üniversite SOME'leri koordineli çalışırken, KKTC'de ulusal bir siber saldırı anında akademik ağları koruyacak, trafiği filtreleyecek merkezi bir siber savunma kalkanı (Scrubbing Center) bulunmamaktadır.
- *Küresel Bilim Ağlarından Soyutlanma:* Kıbrıs Cumhuriyeti, CYNET üzerinden Avrupa'nın devasa araştırma ağ omurgası GEANT'a doğrudan entegre durumdayken; KKTC üniversiteleri büyük veri (Big Data) transferi, grid hesaplama ve küresel akademik kimlik doğrulama (Edugain) altyapılarına kurumsal düzeyde erişememekte, dijital dünyada izole kalmaktadır.

5. Sonuç ve Öneriler

KKTC'nin dijital dünyada kendi egemenliğini ilan edebilmesi ve ICT sektörünü lokomotif bir ekonomik güce dönüştürebilmesi için ivedilikle şu kurumsal ve yasal adımları atması önerilmektedir:

- **"Dijital Dönüşüm Bakanlığı" veya Özerk Müsteşarlık Kurulması:** Başbakanlık DDEDK'nın yapısı güçlendirilmeli; bütçesi ve kadrosu yasa ile korunan, tüm bakanlıkların bilişim projelerini tek elden onaylayan ve denetleyen üst bir idari otoriteye (Müsteşarlık veya Bakanlık düzeyine) dönüştürülmelidir.
- **Müstakil Siber Güvenlik Yasası ve KKTC-USOM'un Teşkili:** 6/2012 sayılı yasanın gölgesinden çıkılarak acilen müstakil bir Siber Güvenlik Yasası çıkarılmalı ve bu yasaya bağlı olarak 7/24 çalışacak özerk bir **KKTC Ulusal Siber Olaylara Müdahale Merkezi** kurulmalıdır.
- **Veri Koruma Kurulu'nun Operasyonel Yapılması:** 89/2007 sayılı yasa, AB GDPR normlarına göre revize edilmeli ve kamu ile özel sektörün veri işleme süreçlerini denetleyip ceza kesme yetkisine sahip bağımsız **Kişisel Verileri Koruma Kurulu** aktif hale getirilmelidir.
- **Ulusal Bilişim Fon Ajansı:** Üniversite-Sanayi iş birliğini kağıt üstünden eyleme dökecek; yerel yazılım ürünlerini, siber güvenlik girişimlerini ve genç girişimcileri hibe ve sıfır faizli kredilerle destekleyecek özerk bir Ar-Ge fonlama ajansı kurulmalıdır.
- **"KKTC Ulusal Akademik Ağ ve Bilgi Merkezi" (KKTC-ULAKBİM) Kurulması:** Başbakanlık DDEDK, BTHK ve Milli Eğitim Bakanlığı ortaklığında, Türkiye'deki TÜBİTAK ULAKBİM modeli referans alınarak özerk bir akademik ağ kurumu yasalaştırılmalıdır. Bu kurum:
  1. Tüm KKTC üniversitelerini, araştırma merkezlerini ve e-devlet veri merkezlerini **tek bir yüksek hızlı, bağımsız ulusal fiber optik Ar-Ge ağı (K-NET / KKTC-NET)** üzerinde birleştirmelidir.
  2. Bu yapı bünyesinde merkezi bir **"Akademik SOME"** kurulmalı; üniversite ağlarındaki siber tehditler ulusal düzeyde birer siber istihbarata dönüştürülerek siber erken uyarı sistemi işletilmelidir.
  3. Yerel bilişim start-up'ları, teknoparklar ve akademisyenler için hayati önem taşıyan Yüksek Başarımlı Hesaplama (HPC) ve yapay zeka veri işleme altyapıları, ticari bulut sağlayıcılarına bağımlı kalmaksızın bu ulusal merkezin bünyesinde millileştirilmelidir.

Sonuç olarak, KKTC'de bilişim alanında kurumsallaşmanın tamamlanması ve akademik altyapının bir çatı altında toplanması, adayı bir "ambargolar ülkesi" olmaktan çıkarıp küresel bir "teknoloji ve veri adası" haline getirmenin yegane yoludur.

Kaynakça (Akademik Atıf Örnekleri)

- Bilgi Teknolojileri ve Haberleşme Kurumu (BTHK). (2012). *6/2012 Sayılı Elektronik Haberleşme Yasası*. Lefkoşa.
- Avrupa Parlamentosu. (2022). *Directive (EU) 2022/2555 (NIS 2 Directive)*. Official Journal of the European Union.
- T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2020). *Ulusal Yapay Zeka ve Siber Güvenlik Strateji Belgeleri*. Ankara.
- CYNET. (2024). *Cyprus Research and Academic Network Infrastructure and Strategic Roadmap*. Nicosia.

TÜBİTAK ULAKBİM. (2023). *Ulusal Akademik Ağ ve Bilgi Merkezi Faaliyet Raporu*. Ankara.

Gmail Live ile e-postalar artık konuşarak bulunacak: Testler başladı

Google, Gmail deneyimini yapay zeka ile geliştirmeye yönelik yeni adımlar atmayı sürdürüyor. Şirketin Gmail Live adını verdiği ve Gemini destekli sesli e-posta arama özelliği, beta sürecinde ilk kullanıcılarla buluşmaya başladı. Yeni sistem sayesinde kullanıcılar, gelen kutularında anahtar kelime yazmak yerine doğal konuşma diliyle sesli arama yapabiliyor. Kaynak: donanimhaber.com

Gmail'de e-postalar artık konuşarak bulunacak: Testler başladı

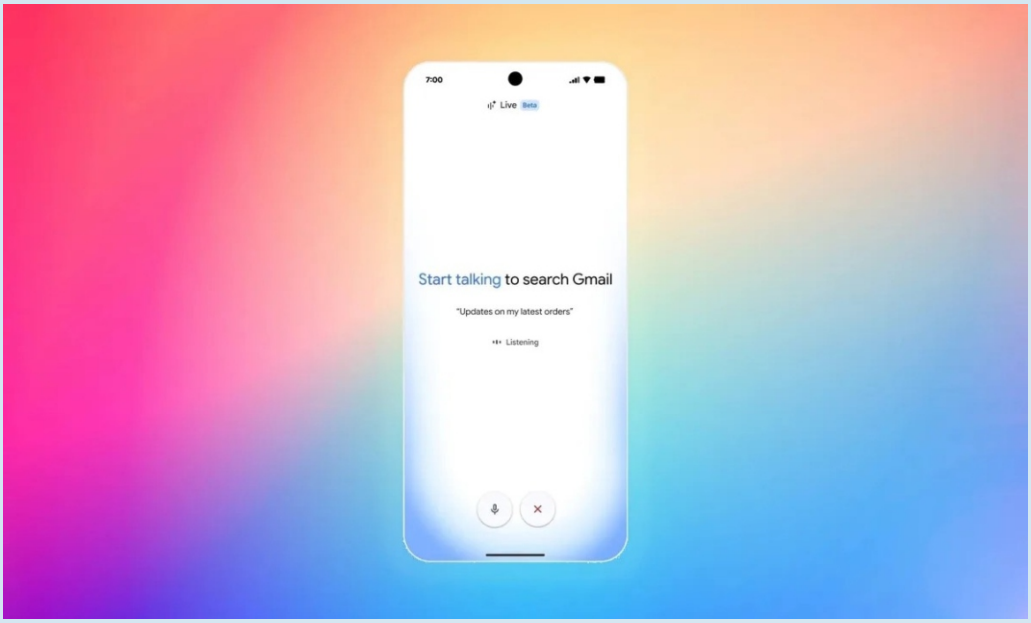
Google, Gmail deneyimini yapay zeka ile geliştirmeye yönelik yeni adımlar atmayı sürdürüyor. Şirketin Gmail Live adını verdiği ve Gemini destekli sesli e-posta arama özelliği, beta sürecinde ilk kullanıcılarla buluşmaya başladı. Yeni sistem sayesinde kullanıcılar, gelen kutularında anahtar kelime yazmak yerine doğal konuşma diliyle sesli arama yapabiliyor.
Gemini destekli Gmail Live kullanıma sunuluyor

Google'ın geçtiğimiz ay düzenlediği Google I/O etkinliğinde duyurduğu Gmail Live, şu anda sınırlı sayıdaki Android ve iOS kullanıcısına beta kapsamında dağıtılıyor ve test ediliyor. Aktarılanlara göre özellik, yaz ayları içinde daha geniş çapta Google AI Pro ve Google AI Ultra abonelerine sunulacak.

Yeni özellik etkin olduğunda Gmail'in arama çubuğunda Live simgesi görüntüleniyor ve yanında Gemini düğmesi yer alıyor. Bu düğmeye dokunulduğunda Gmail Live tam ekran olarak açılıyor. Kullanıcılar Gemini'ye doğal bir şekilde konuşarak yaklaşan seyahat tarihlerini, sipariş durumlarını veya belirli içeriklere sahip e-postaları bulmasını isteyebiliyor.

Diğer Google uygulamalarına da gelecek
Google, Live deneyimini yalnızca Gmail ile sınırlı tutmayı planlamıyor. Şirketin üzerinde çalıştığı Docs Live, kullanıcının sesli düşüncelerini düzenli bir belge taslağına dönüştürebilecek ve gerekli izin verilmesi halinde diğer Google uygulamalarındaki bilgileri de belgeye ekleyebilecek. Benzer şekilde geliştirilen Keep Live ise Google Keep uygulamasına yapay zeka destekli sesli etkileşim özellikleri kazandıracak.

Google, yeni Live özelliklerini ilk etapta Google AI Pro ve Google AI Ultra abonelerine sunacak. Google Workspace kurumsal müşterileri ise bu yenilikleri ön izleme programı kapsamında test edebilecek.



Geçmişi Bilmeyen Geleceğe Yön Veremez. (Mustafa Kemal Atatürk)

Dijitalleşme sürecinde Kuzey Kıbrıs (Geçmişten Günümüze)

Nisan 2008 ayında dönemin Başbakanı Sn. Ferdi Sabit SOYER'in etki ve desteği ile, e-Devlet kapılarını 22 servis ile vatandaşa açmıştır. O dönemde ne Türkiye'de ne de Güney Kıbrıs'ta herhangi bir e-devlet servisi açılmamıştı.

1985 yılında Kıbrıs'a o zamanki adı ile bünyesinde sadece 3 Mühendislik (Elektrik ve Elektronik, Makina ve İnşaat Mühendisliği) programı olan Yüksek Teknoloji Enstitüsü'ne atandığımda, Elektrik ve Elektronik Mühendisliği programı tarafından sunulan Bilgisayar Programlama (FORTRAN) yazılım dili verilmekte idi. Bazı kurumlarda ise (Maliye, SSD, bazı bankalar vs. gibi) COBOL dili ile dijitalleşme süreçleri yaşanmakta idi. Kuzey Kıbrıs kurumların yönetiminde aydın kesimlerin olması, ana veri odaklarının daha küçük olması dijitalleşme sürecinin daha kolay ve hızlı olabileceği görünümü oluşturduğu görünse de, insan eğitimin önemli olduğu varsayımından hareketle, Elektrik ve Elektronik Mühendisliği programı içerisinde Computer and Control opsiyonunun açılması ve bunun içerisinde Veri Tabanı Yönetimi, Bilgisayar Ağları Yönetimi, İşletim Sistemleri Yönetimi gibi dersler ile yazılımın güçlendirilmesi ve çeşitli sektörlerde dijital dönüşümün hızlandırılması hedeflenmiştir. 1986 Şubat ayında ilk olarak YTE ve KTMMO ortaklığında "**Mühendislik Uygulamalarında Bilgisayar Kullanımı**" semineri düzenlediğimizde, öğrenciler de bunun farkındalığını özümseyerek, 30'u aşkın öğrenci ile yan dal olarak Bilişim Sistemleri Mühendisliği opsiyonu rağbet görmüştür. Ancak, bunun nitelikli bilişim tabanlı insan gücü yetiştirmede ve dijitalleşme yolunda hızlı yol alınamayacağı görüşünden hareketle, dönemin Eğitim Bakanı Sn. Salih COŞAR'ın (ışıklar içerisinde uyusun) desteği ile 2 yıllık Bilgisayar Programcılığı programı açılmış ve oldukça rağbet görmüştür. Kurumlara ve sanayi kuruluşlarına yetkin ve nitelikli bilişim elemanları yetiştirilmiştir. 1987 yılında her iki programın öğrencilerinin desteği ile Kamu ve Sanayi kuruluşları için, Salamis Bay otelinde 3 günlük "**Bilişim Kongresi**" düzenlenmiş ve bunun akabinde birçok kurum ve kuruluş, dijitalleşme için hızla adımlar atmıştır. Bu aşamada Kuzey Kıbrıs'ta ilk kez Bilişim alanında (dijitalleşme konusunda) Üniversite-Kamu-Endüstri işbirliğinin temelleri atılmıştır. 1988 yılında kısa adı EARN (European Academic Research Network) olan Avrupa Araştırma Ağı'na bağlanarak, Kuzey Kıbrıs'ta hatta tüm Kıbrıs adasında ilk kez uluslararası bilişim ağlarına bağlanılıp, Türkiye'de sadece TUVAKA (Türkiye Üniversiteler ve Araştırma Kurumları Ağı) üyelerine verilen servisler, tüm Kuzey Kıbrıs kurumlarının hizmetine sunulmuştur. 1993 yılında ODTÜ'nün Internet'e bağlanmasının hemen ardından, 1994 yılında dönemin Eğitim Bakanı Sn. Mehmet Ali TALAT'ın destekleri ile Kuzey Kıbrıs'ta ilk INTERNET bağlantısı sağlanmış ve gerek akademik kuruluşların ve gerekse diğer Kamu ve Kuruluşların kullanımına sunulmuştur. İzolasyonlar altındaki Kuzey Kıbrıs toplumunun dijital dünya ile bütünleşmesi için tüm sektörler seferber olmuş ve özel sektör olarak ilk ISP (COMTECH) ve hemen ardından (EBİMNet) ve diğer ISP ve alt ISP'ler üstün gayret göstermişlerdir. Kısa süre içerisinde, kurumların kendi ürettikleri bilgileri toplumla ve diğer kurumlarla paylaşmaları konusunda küçük kurumsal networkler hızla oluşmaya başlamıştır. Hatta, o dönemin kısıtlı bant genişliği nedeni ile dönemin Ulaştırma Bakanı Sn. Mehmet BAYRAM'ın desteği ile Internet ağı bant genişliğinin arttırılması için, sadece veri aktarımı sağlanması kaydı ile yurtdışı bağlantılı Uydu Sistemlerinin kullanımına onay verilmiştir. Kamu bilgi kaynaklarının ortak kullanımını sağlamak ve bunları toplumla paylaşmak üzere 1998 yılında dönemin Başbakanı Sn. Dr. Derviş EROĞLU'nun desteği ile Başbakanlık bünyesinde KAMUNET Üst Kurulu oluşturulmuştur. 2004 yılına kadar, 2000 sendromuna hazırlık, kamuda dijitalleşme için stratejik raporların hazırlanması, SWOT analizlerinin yapılması, Kamu bilişim envanterinin donanım, yazılım ve insan gücü açısından toparlanması, kamu kurumlarının ağ yapılanması için top domain kodlarının (**nc.tr**) alınmasının sağlanması, özel sektörün sürece dahil edilmesi için gereken altyapıların sağlanması, kamu bilişim sistemleri ve entegrasyonu için, donanım ve yazılım standartlarının oluşturulması gibi dijitalleşmeye yönelik birçok işlevler, kısıtlı bütçeler ile tamamlanmıştır. Bu süre içerisinde nitelikli insan gücü oluşturmak için, izolasyonlara rağmen Kuzey Kıbrıs'ta doğrudan EMEA'ya bağlı ECDL, MicroSoft Academy, Cisco Networking Academy oluşumları sağlanmıştır. Bu eğitimleri pekiştirmek ve insan gücüne sertifikasyon sağlamak için de ECDL ve Pearson Test Merkezleri oluşturulmuştur. Bu merkezlerden oldukça yüksek sayıda genç kesim, kamu ve özel sektör çalışanı faydalanmış ve yetkinliklerini güçlendirmiştir. Sn. Mehmet Ali TALAT'ın başbakanlığı döneminde, geliştirilen verilerin tüm toplum kesimlerine yaygınlaştırılması, Kamu verilerinin ve ağının dönemin teknolojilerine bağlı olarak büyük ölçüde tamamlanmış olması ve dijitalleşme sürecinin tüm sektörlere yayılması görüşünden hareketle, 2004 yılında KAMUNET, e-DEVLET Üst Kurulu haline dönüştürülmüştür. Annan Planı görüşmelerinde, Bilişim ve Teknoloji alanındaki gelişmelerimiz, Güney Kıbrıs'a göre oldukça üst düzeyde olduğu

raporlarda açıkça ifade edilmiştir. Ancak, Güney Kıbrıs'ın AB müktesebatlarını aynen kullanabileceği varsayılarak, tarafımızın da buna uygun yasaların hazırlanması gerektiği için, hızla gerekli yasaların hazırlanması sürecine girilmiştir. Bu arada 2005 yılında, e-Devlet Üst Kurulu olarak, UNDP desteği ile büyük bir çalıştay yapılmış, mevcut durum analizleri ve yol haritası çizilmiştir. Bunun yanında, Global düzeyde standartlara uygun e-Devlet uygulamaları geliştiren Talinn Üniversitesi bünyesinde kurulan AB destekli bağımsız EGA (Electronic Government Agency) kuruluşunun yetkilileri ülkemize davet edilmiştir. Kamu Sektörü üst düzey yetkilileri ve çalışanlarına ve bunun yanında siyasi erk'in e-Devlet olgusuna sahip çıkması gerekliliğinden hareketle, Cumhuriyet Meclisindeki parti milletvekillerine seminerler verilmiştir. Kurul, hızlı çalışarak, e-Devlet olgusunun temel taşları olan yasaları AB ve uluslararası normlarda hazırlamış, 2006 yılında "Bilgi Edinme Hakkı Yasası", 2007 yılında "Kişisel Bilgilerin Korunması Yasası" ve "Elektronik İmza Yasası" yürürlüğe girmiştir. Aynı yıl, altyapı ve bilişim ağ standartlarının oluşturulması için e-Devlet Kurulu ile koordinasyon ile çalışacak "Telekomünikasyon Üst Kurulu oluşturulmuştur. Bu yasaların yürürlüğe girmesi ile kurumlararası veri paylaşımı ve kurumların veri odaklarını hızla düzenlemeleri açısından ve vatandaştan alınacak geri dönümlerle sağlanması amacı ile **Nisan 2008** ayında dönemin Başbakanı Sn. Ferdi Sabit SOYER'in etki ve desteği ile, e-Devlet kapılarını **22 servis** ile vatandaşa açmıştır. O dönemde ***ne Türkiye'de ne de Güney Kıbrıs'ta herhangi bir e-devlet servisi açılmamıştı***. Bu çalışmalar sürerken, iki temel yasa olan "Elektronik Haberleşme Yasası" ve "e-Devlet ve Dijital Dönüşüm Yasası" taslak olarak hazırlanmış ancak maalesef 2009 yılında kurullardaki belirsizlik ve 2010 yılında kurulların dağılması ile zamanında yürürlüğe girememişlerdir.

Bugün, Temmuz 2026 ve verilen e-Devlet servisi sayısı 18.

Bundan sonraki süreçleri ve bir sonraki yazımda

DİPNOT: Siyasi isimler, siyasi erk'in dijitalleşme olgusuna ne kadar sahiplenmiş olduğunu göstermek için verilmiştir.

Necdet İcil
Independent ICT Expert, Mentor, Project Manager,
GMTGB YK Üyesi

Teknoloji devi Oracle, yapay zekaya yönelirken 21.000 kişiyi işten çıkarıyor.
https://www.bbc.com/news/articles/c4gy0x0j5deo

Google'ın yapay zekası manipüle ediliyor. Arama devi sessizce karşı koyuyor.
https://www.bbc.com/future/article/20260519-google-tackles-attempts-to-hack-its-ai-results

WhatsApp'ın başına Hintli bir girişim şirketinin kurucusu geçecek, Will Cathcart ise görevinden ayrılacak.
Kunal Shah, bir süredir Hindistan'ın girişimcilik ekosisteminde tanınan bir isimdi, ancak şimdi küresel ilgi odağı haline geldi.
https://www.bbc.com/news/articles/c8e2195k5j2o

Paris'te yapay zekâ gözlüklerini test ettim. İşte yanlış yaptıkları noktalar:
Giyilebilir yapay zekâ, gezginlerin şehirlerde yol bulmasına, menüleri çevirmesine ve seyahati temelden dönüştürmesine yardımcı olabilir. Peki, dezavantajları nelerdir?
https://www.bbc.com/travel/article/20260612-i-tested-metas-ai-glasses-in-paris

Yapay Zekanın Beyninizi Bulamaç Haline Getirmesini Nasıl Durdurabilirsiniz?
GPS yön duygumuzu mahvetti. Arama motorları hafızamızı zayıflatıyor. Bilim insanları, yapay zekanın yaratıcılıktan eleştirel düşünmeye kadar her şeye aynı şeyi yapabileceği konusunda uyarıyor.
https://www.bbc.com/future/article/20260505-how-to-use-ai-without-turning-your-brain-to-mush

Google'ın YouTube'u, gençler arasında sosyal medya bağımlılığı davasını çözüme kavuşturdu.
Google'ın YouTube'u, Florida'da 15 yaşında bir çocuğun açtığı sosyal medya bağımlılığı davasını çözüme kavuşturdu. Bu, çocuklar arasında ruh sağlığı krizini körüklemekle suçlanan çevrimiçi platformlar için yeni bir yasal darbe oldu.
https://www.bbc.com/news/articles/cly81g7x73po

'Yapay zeka bir tekneyi tamir edemezdi': Çıraklar geleneksel bir tekneyi ayakta tutuyor.
Bir tersanede, hevesli bir grup çırak, iki geleneksel tekneyi restore etmek için yoğun bir şekilde çalışıyor.

16 ile 31 yaşları arasındaki bu gençler, kaybolma riski taşıyan becerileri öğreniyorlar.

Tekne yapımının yakın zamanda tehlike altındaki zanaatlar listesine dahil edilmesiyle, bu gençler bu zanaatı kurtarmaya yardımcı olabilir mi?

Essex, Brightlingsea'da, Colne Nehri'ne bakan Pioneer Sailing Trust, İngiltere'de tarihi tekne restorasyonunda çıraklık eğitimi sunan tek yerdir.

Eğitim görenler, Ulusal Piyango fonlarıyla desteklenen projelere duydukları tutku kadar, bu tekneleri kurtarmaya da tutkuyla bağlılar.

1948 yapımı, Mersey Adası'ndan gelen ve daha iyi günler görmüş olan Jinnie adlı istiridye teknesi ve 1950'lerde Doğu Kıyısı'nı inceleyen ve o zamanlar üretilen en küçük nehir ağzı araştırma teknesi olan Jassa üzerinde çalışıyorlar.

Çırakların yardımıyla, bu iki teknenin yakında tekrar suya indirilmesi umuluyor.
Kaynak BBC.com

Dijital dönüşüm 2; Teknoloji dönüşümü değil, iş yapma şeklinin dönüşümüdür ve odağında insan vardır.

Elektronik Belge Yönetim Sistemi (EBYS), kurumsal belgelerin dijital ortamda güvenli şekilde üretilmesini ve saklanmasını sağlayan yazılımdır; Süreç Yönetimi (BPM) ise iş adımlarının baştan sona tasarlanıp optimize edilerek yönetilmesidir. İş dünyasında bu iki kavram, operasyonel hız ve dijital dönüşüm sağlamak amacıyla genellikle entegre şekilde çalışır.

Elektronik Belge Yönetim Sistemi (EBYS) Nedir?

EBYS, kurum içi ve kurumlar arası resmi yazışmaların, formların ve her türlü dokümanın kağıt kullanılmadan dijital ortamda yönetilmesini sağlar. Yazışma süreçlerini standartlaştırarak kurumsal hafızayı korur.

- **Üretim ve Tasarım:** Belgeler EBYS programlarının sunduğu özellikler ile dijital şablonlar kullanılarak oluşturulur.
- **Onay ve E-İmza:** Evraklar, 93/2007 Sayıle Elektronik İmza Yasası'na uygun olarak yasal geçerliliğe sahip e-imza ile imzalanır ve onaylanır.
- **Dağıtım ve İletim:** Hazırlanan belgeler ilgili birimlere, kişilere veya dış kurumlara anında ve güvenli yollarla ulaştırılır.
- **Arşivleme ve Erişim:** Belgeler mevzuata uygun şekilde güvenli bulut veya sunucu sistemlerinde depolanır; yetkili personeller tarafından kolayca sorgulanıp bulunabilir.

Süreç Yönetimi (BPM) Nedir?

Süreç Yönetimi (Business Process Management - BPM), bir şirketin hedeflerine ulaşması için yürüttüğü birbirine bağlı faaliyetlerin (iş akışlarının) tasarlanması, modellenmesi, çalıştırılması ve sürekli iyileştirilmesi disiplinidir. Amacı operasyonel hataları sıfıra indirmek ve verimliliği artırmaktır.

- **Modelleme:** Bir işin (örneğin fatura onaylama, işe alım, İthal Ön İzin, e-vize) hangi adımlardan oluştuğu ve kimlerin onayından geçeceği görsel olarak haritalandırılır.
- **Otomasyon:** Manuel yapılan rutin görevler (veri girişi, hatırlatma e-postaları vb.) sistem tarafından otomatik hale getirilir.
- **Takip ve Analiz:** İşin hangi aşamada tıkandığı, hangi personelin üzerinde ne kadar iş yükü olduğu anlık olarak izlenir.
- **Optimizasyon:** Darboğaz oluşturan adımlar tespit edilerek süreç sürekli olarak daha hızlı ve az maliyetli hale getirilir.

EBYS ve Süreç Yönetimi Arasındaki Farklar

Özellik	Elektronik Belge Yönetim Sistemi (EBYS)	Süreç Yönetimi (BPM)
Odak Noktası	Belgenin kendisi, yasal uyumluluğu ve arşivlenmesi.	İşin yapılış şekli, adımları ve iş akışının verimliliği.
Temel Çıktı	Formlar, resmi yazışmalar, sözleşmeler ve raporlar.	Tamamlanmış bir iş (örn: sipariş teslimi, müşteri talebinin çözülmesi).
Amaç	Kağıt tüketimini azaltmak, kurumsal hafıza ve hızlı erişim.	İş adımlarını hızlandırmak, maliyeti düşürmek ve standardizasyon.
Kapsam	Genellikle evrak akışı olan kamu ve özel sektör departmanları.	Üretimden finansa, İK'dan lojistiğe kadar tüm şirket operasyonları.

İkisinin Birlikte Kullanımı Neden Önemlidir?

Modern kurumlarda belge ve süreç birbirini tetikler. Örneğin; bir Süreç Yönetimi sistemi üzerinden başlatılan "Satın Alma Süreci", onay adımları tamamlandığında otomatik olarak bir "Sözleşme Belgesi veya İthal Ön İzin Evrağı" üretilmesi için EBYS altyapısını kullanır. Bu entegrasyon sayesinde hem işin takibi hatasız yapılır hem de ortaya çıkan yasal evraklar güvenle arşivlenmiş olur.

Şirketiniz veya kurumunuz için bir dijital dönüşüm planlıyorsanız, **hangi sektöre yönelik** (kamu, lojistik, finans vb.) ya da **hangi departman özelinde** (insan kaynakları, satın alma vb.) bir çözüm aradığınızı paylaşırsanız, size uygun **yazılım modelleri** ve **iş akışı senaryoları** önerebilirim.

EBYS ve Süreç Yönetimi Kullanarak işlerini dijitalleştirm iş kurumlarımı zdan bazılarından örnek;

1. Elektrik Mühendisleri Odası, **İthal Ön İzin** sürecini kamuya açmış ve web sayfaları üzerinden çevirim içi İthal Ön İzin başvurularını almakta, Sistem içerisinde bu süreç başladığında, ilgili teknik personele anında görev olarak düşmekte, ilgili Teknik Personel gelen başvuru formunu inceledikten sonra, uygunsa uygunluk belgesi için süreci onaylar, Teknik personelin onayından sonra, ilgili hesaplamalar otomatik yapılarak, muhasebe departmanının kontrolü için anında görev olarak muhasebe departmanı personeline düşer. Muhasebe departmanı gerekli kontrolleri yaptıktan sonra, Faturalama işlemini gerçekletirir ve Başvuru sahibine çevrimiçi Ödeme linki ile birlikte Fatura tutarı mail olarak gönderilir, Ödem İşlemini başvuru sahibi yaptıktan sonra, muhasebe departmanına ödeme bilgisi görev olarak gelir. Muhasebe departmanı ödeme onayını yaptıktan sonra, İthal Ön İzin belgesinin imzalanması için Önce Teknik personele sonra da Müdür'e e-imza ile imzalaması için görev düşer. İmzalam işlemleri tamamlandığında evrak ve iş tamamlanmış olur. Onaylanmış imzalanmış, İithal ön izin Evrağı sistemden otomatik olarak başvuru sahibine, Gümrük komisyoncusuna ve Gümrük

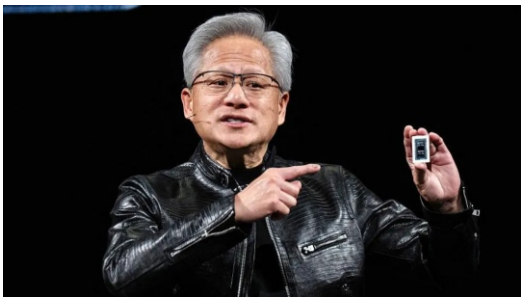
Müdürlüğüne iletmiş olur. **E-vize** süreci Elektirk mühendislerinin çizdiği elektirik projelerinin kağıtsız ortamda vizelenme sürecidir. Elektrik Mühendisleri Odası ,üye Elektrik mühendisi ,web sitesinden e-vize başvuru linki ile sisteme giriş yaparak, oradaki üyelik bilgilerini, proje bilgilerini ve gerekli evrak ve paftaları sisteme çevrim içi yükler. Yükleme işlemi tamamlandığında kendi e-imzası ile tek seferde tüm yüklediği belge, evrak ve bilgileri imzalar. (Müelliflik hakkı açısından ıspat) İmzalam işlemi tamamlandığında proje bilgisi, Muhasebe ön kayıt personeline görev olarak düşer. Proje genel olarak gerekli bilgiler varsa, Önkayıt ücreti için onaylanır ve başvuru mühendisine ödeme bilgileri otomatik gider. Başvu yapan mühendis ödemesini çevrim içi K.Kartı veya havale olarak yapar. Ödeme bilgisi muhasebe departmanına görev olarak gelir. Ödem onayını yapan muhasebe personelinden sonra Vize teknik personellerine Proje görev olarak düşer. Projeyi inceleyecek vize personeli projeyi açarak, kontrolleri sistemde bulunan kontrol listesine göre yapar. Eksik veya değişiklik varsa sistemde kontrol listesi maddesine gerekli açıklamayı yazarak, başvuru sahibi mühendise Notlama olarak sistem üzerinden geri gönderir. Notlama alan mühendis gerekli düzeltmeleri yaptıktan sonra yine sistem üzerinden projeyi geri gönderir. Vize Kontrol mühendisinin önüne notlanmış proje görev olarak düşer ve gerekli işlemler tamamlandıysa projeyi onaylar. Onaylanan proje Muhasebe departmanına vize harcı hesaplanmış olarak düşer. Hesaplama kontrolü yapıldıktan sonra başvuru mühendisine vize harcı ödeme bilgileri otomatik gider. Başvu yapan mühendis ödemesini çevrim içi K.Kartı veya havale olarak yapar. Ödeme bilgisi muhasebe departmanına görev olarak gelir. Muhasebe departmanı Ödeme onayını yaptıktan sonra, Proje vizelenmesi için önce Teknik personele e-imza için görev olarak gider. Teknik personel projeyi e-imza ile imzaladıktan sonra, Müdür'e e-imza için görev olarak gider. Müdür e-imzası ile imzaladıktan sonra, Proje e-vizeli olarak Başvuru mühendisine otomatik mail yolu ile iletilir ve süreç biter.

Kağıt tüketimi olmadan bu kadar işlem (0 Kağıt)

Lisani Deniz
Dijital Dönüşüm Danışmanı
lisanideniz@gmail.com

Nvidia, kişisel bilgisayarlar için yeni bir yapay zeka çipi duyurdu.

Nvidia, yapay zeka teknolojisiyle entegre edilmiş cihazlar için tüketici pazarına girerken, PC'ler için yeni bir çip duyurdu.



Nvidia'nın CEO'su Jensen Huang, RTX Spark çipini tanıtırken, "Bilgisayarın bu şekilde yeniden icadı, telefonun bugün akıllı telefon olarak bildiğimiz şeye dönüşmesi kadar büyük bir olay" dedi.

Huang, bu açıklamayı Pazartesi günü Tayvan'ın Taipei kentinde düzenlenen Computex teknoloji fuarının açılışı öncesinde yaptığı açılış konuşmasında yaptı.

Ayrı bir gelişme olarak, ABD Pazar günü Nvidia'nın en gelişmiş çiplerinin Çinli firmalara satışına ilişkin kurallarını sıkılaştırdı.

Nvidia, internet sitesinde RTX Spark'ın "kişisel yapay zekâ ajanları çağı için yeni bir süper çip olduğunu ve bir araç olmaktan çıkıp takım arkadaşı haline gelen yeni bir bilgisayar sınıfı sunduğunu" belirtti.

Bu özellik, Lenovo, HP, Dell, Microsoft Surface, Asus ve MSI tarafından üretilen yeni bir Windows PC serisine dahil edilecek. Sonbaharda piyasaya sürülmesi planlanan bu ürünlerin ardından Acer ve Gigabyte modelleri de gelecek.

Bu hamle, Apple ve Intel gibi PC pazarındaki önde gelen isimlere bir meydan okuma anlamına geliyor.

Araştırma şirketi Gartner'a göre, Lenovo, HP, Dell ve Apple, bu yılın ilk üç ayında dünya PC pazarının neredeyse %75'ini oluşturdu.

Bir 'paradigma değişimi'

Nvidia geleneksel olarak Grafik İşlem Birimleri (GPU'lar) üretmeye odaklanmıştır; bunlar başlangıçta video oyunları için bilgisayar grafiklerini hızlı bir şekilde işlemek üzere tasarlanmış, ancak günümüzde yapay zeka sistemlerine güç sağlamak için de yaygın olarak kullanılan özel çiplerdir.

Teknoloji araştırma şirketi Forrester'ın başkan yardımcısı ve baş analisti Charlie Dai, bu duyurunun Nvidia'nın PC pazarında "bileşen tedarikçisi" konumundan "mimari sahibi" konumuna "paradigma değişikliği" yaptığını gösterdiğini söyledi.

"Bu durum doğrudan Intel, AMD ve Qualcomm'u zorlayacak ve performans, verimlilik ve yapay zeka entegrasyonu konusunda rekabet baskısını artıracak," dedi.

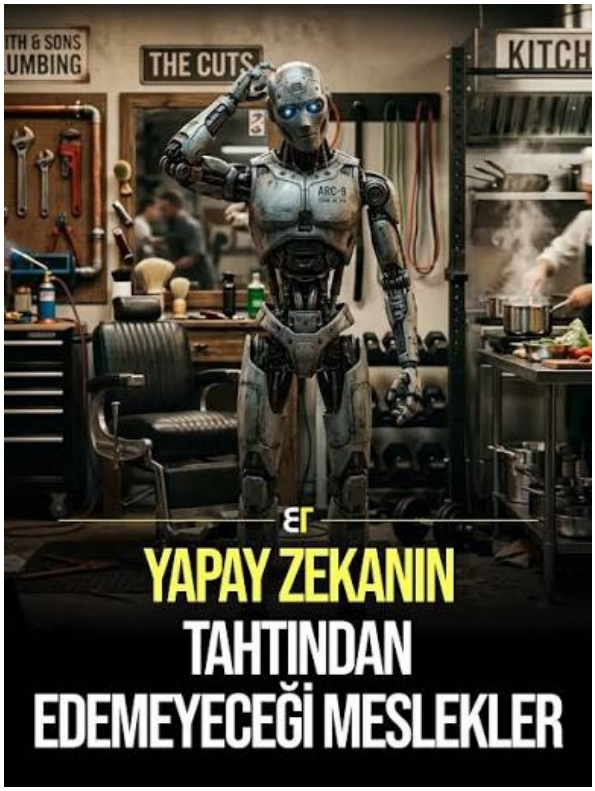
Ancak, sektör analisti firması FDM CCS Insight'ın Araştırma Direktörü Ian Fogg, bu değişikliğin "önemli bir maliyetle birlikte gelmesinin muhtemel olduğunu" ve Nvidia'nın "iş istasyonu sınıfı performans arayanları" hedefleyeceğini söyledi.

Açıklamanın bir bölümü, Nvidia'nın yapay zekâ ajanları (OpenClaw gibi yapay zekâ tarafından yönlendirilen otonom yazılım programları) için RTX Spark çipiyle desteklenen "sağlam ve güvenli bir Windows platformu" sağlamak üzere Microsoft ile yapılan ortaklığa odaklandı.

Microsoft Yönetim Kurulu Başkanı ve Başkanı Satya Nadella, "Amacımız, Windows işletim sistemine sahip her eve ve her masaya sınırsız zeka sunmaktır. RTX Spark, bu vizyona doğru gerçek bir atılımı temsil ediyor" dedi.

Yarı iletken analisti Dr. Ian Cutress, Nvidia'nın Windows işletim sistemli ve Nvidia donanımına sahip bir dizüstü bilgisayar sunarak, özellikle yapay zeka ile çalışan geliştiricilere "kendi yazılım ve donanım yörüngesinde kalmaları için bir neden" verdiğini söyledi.

BT Kıbrıs: Yapay zekanın henüz tehdit etmediği meslekler neler?



1. Psikologluk ve PsikoterapistlikTerapi süreçleri, kelimelerin ötesinde danışanın beden dilini okumayı, güven bağı kurmayı ve derin bir empati yapmayı gerektirir. İnsan psikolojisini anlamlandırmak, bir yapay zekanın sahip olamayacağı, yalnızca insana özgü bir sezgi işidir.

2. Yaratıcı Sanatlar ve YazarlıkYapay zeka görsel, müzik veya metin üretebilir. Ancak bu üretimler mevcut verilerin analizine (istatistiksel örüntülere) dayanır. Özgün bir sanat eseri ortaya koymadaki duygusal derinlik, hayal gücü ve yaşanmışlık aktarımı sadece insan sanatçılara ve yazarlara aittir.

3. Zanaatkarlık ve Ustalık (Tesisatçı, Elektrikçi, Marangoz vb.)Bu meslekler, standartlaştırılmış fabrika ortamlarının aksine her evin veya mekanın kendine has, öngörülemeyen yapısıyla başa çıkmayı gerektirir. Değişen ortama uyum sağlama, el becerisi ve çok yönlü fiziksel problem çözme kapasitesi nedeniyle robotların ve yapay zekanın en zorlanacağı alanlardandır.

4. Öğretmenlik ve AkademisyenlikÖzellikle çocukların ve gençlerin eğitiminde, salt bilgi aktarımının ötesinde öğrencilere ilham verme, onları motive etme, duygusal zorluklarını fark edip onlara rehberlik etme süreçleri vardır. Pedagojik formasyon ve insani liderlik yapay zekanın taklit edemeyeceği temel unsurlardır.

5. Yaratıcı Liderlik ve YönetimÜst düzey yöneticilik; vizyon geliştirme, şirket kültürü oluşturma, kriz anlarında ahlaki/etik kararlar alma ve insanları ortak bir hedef etrafında toplama becerisi ister. Stratejik vizyon ve insanları yönlendirme gibi inisiyatif gerektiren liderlik rolleri, insani yargılara dayanır.

Peki Geleceğin Meslekleri Neler Olabilir?

İşte Robert Capps'ın önerdiği Yapay Zeka Çağının 22 Yeni Mesleği:

1. AI Etik Danışmanı
2. Algoritmik Uyum Tasarımcısı
3. Yapay Zeka Kişilik Geliştiricisi
4. AI Stil Direktörü
5. Dijital Güven Yöneticisi
6. AI Hikâye Kurgucusu
7. Veri Kaynak Doğrulama Uzmanı
8. Sanal Gerçeklik Deneyim Küratörü
9. Yapay Zeka Mentoru (AI Eğiticisi)
10. Duygusal İfade Tasarımcısı (Empati Mühendisi)
11. Yapay Zeka Entegrasyon Danışmanı
12. Dijital Çevre (Metaverse) Yöneticisi
13. İlaç Uyumluluk Optimizasyonu Uzmanı
14. AI Ürün Test Kullanıcısı (İnsan-AI etkileşimi denetçisi)
15. Otomatikleştirilmiş İş Süreçleri Geliştiricisi
16. Zeka Uyumluluğu Psikoloğu
17. Dijital İşbirliği Koçu
18. Yapay Zeka Protokol Denetçisi
19. Eğitilebilir AI İçerik Danışmanı
20. Veri Gizliliği Uzlaşma Mühendisi
21. Robot Davranış Tasarımcısı
22. İnanç ve Değer Sistemleri Danışmanı (AI kültürel çevirmeni)

Bu meslekler şimdilik teorik olsa da, bazıları teknoloji dünyasında yavaş yavaş ortaya çıkmaya başladı. Uzmanlar, gelecekte insanların yalnızca "işlerini kaybetmemek" için değil, yeni tür beceriler geliştirmek için de harekete geçmesi gerektiğini vurguluyor.

Telekomünikasyon Dairesi: Yük mü, Fırsat mı?

1. Önce Büyük Resme Bakalım

2025 yılında KKTC'de haberleşmeye ne kadar para ödendi, biliyor musunuz?
5,57 milyar TL.
BTHK (Bilgi Teknolojileri ve Haberleşme Kurumu) verilerine göre elektronik haberleşme sektörünün toplam net satış geliri 2025
yılında bu seviyeye ulaştı — bir önceki yıla göre yaklaşık

Yıl	Gelir
2022	68 Milyon TL
2023	119 Milyon TL
2024	214 Milyon TL
2025	375 Milyon TL

%57'lik bir artışla.
Burada tartışılan şey küçük bir "telefon dairesi" değil. **5,5 milyar TL'lik bir ekonomidir.** Ülke ölçeğinde devasa bir sektördür.

2. Telekomünikasyon Dairesi Gerçekten Zarar Ediyor mu?

Ulaştırma Bakanlığı'nın resmi verilerine göre dairenin gelir tablosu şöyle:

Basit bir hesap yapalım:
375 ÷ 68 = 5,5 kat büyüme

Tek kuruş yatırım yapılmadı. Kaynak aktarılmadı.
Buna rağmen Telekomünikasyon Dairesi'nin geliri sadece dört yılda **5,5 kat büyüdü.**

Sorulması gereken soru şu: zarar eden, atıl, "yük" olarak tarif edilen bir kurumun geliri dört yılda 5,5 kat artar mı?
Hiçbir yeni yatırım yapılmadan, kaynak aktarılmadan, tüm yapısal olumsuzluklara rağmen gerçekleşen bu büyüme — dikkat
çekicidir ve açıklanmaya değerdir. Kurum elinde hiçbir ek kaynak olmadan bunu başardıysa, asıl soru şudur: gerekli yatırım
yapılsaydı bu büyüme nereye taşınabilirdi?

3. Asıl Sorun Nedir?

Bir çiftçi düşünün.
Her yıl daha fazla ürün satıyor. Ama traktör alamıyor, sulama sistemi kuramıyor, depo yapamıyor.
Sorun, ürün satamaması mı? Hayır.
Sorun, kazandığı parayı kullanamamasıdır.
Telekomünikasyon Dairesi'nin sorunu gelir yaratamaması değil; yarattığı gelir üzerinde yeterli yatırım özgürlüğüne sahip olmamasıdır. Kurum büyüyor, ama büyüdüğü kaynağı kendi geleceğine dönüştüremiyor.

4. Dünyada Bu İş Nasıl Yapılıyor?

İki örnek, iki farklı yol — ama ortak bir ilke:
CYTA (Güney Kıbrıs)
Sahibi devlet. Ama kurumun mali ve idari özerkliği var. Kamu mülkiyeti ile kurumsal hareket kabiliyeti aynı çatı altında bir arada
durabiliyor.

5. Bakanın ve Hükümetin Asli Görevi Nedir?

Bir ulaştırma bakanının görevi:
Kurum küçültmek **değildir**
Kurumu tasfiye etmek **değildir**
Kurumu yatırım yapamaz hale getirmek **değildir**
Özelleştirmeye zorlamak **değildir**
Devletin asıl görevi:
Stratejik altyapıyı korumak
Yatırımı planlamak
Rekabeti düzenlemek
Vatandaşa kaliteli hizmet sağlamak
Sorulması gereken soru basit: **Sektör 5,57 milyar TL'ye çıkmışsa, devlet bu büyümeden neden daha fazla pay almıyor?**

6. Öneri: Telekomünikasyon Kalkınma Fonu

Bu yazının en önemli bölümü burası.
Öneri: Sektör gelirlerinin %2'si oranında bir *Telekomünikasyon Kalkınma Fonu* kurulsun. BTHK gelirlerinden de belirli bir yüzde bu
fona aktarılsın.
2025 yılı geliri **119 milyar Euro'nun üzerinde** gerçekleşti. Almanya bu sektörü "önemsiz" ilan etmedi — tam tersini yaptı. Telekomünikasyonu stratejik altyapı olarak gördü, devlet bütçesinden yatırım yaptı, fonlar oluşturdu ve sektörü büyüttü. Ortak nokta: hiçbiri telekomünikasyonu küçültülecek bir kalem olarak görmedi. İkisi de onu **stratejik bir varlık** olarak ele aldı.

5,57 milyar TL × %2 = **111 milyon TL / yıl**
10 yılda: **~1,1 milyar TL**

Bu fonla finanse edilebilecek alanlar:
- Fiber altyapı
- Veri merkezi
- Siber güvenlik
- Kamu bulutu

Ve daha fazlası — özelleştirmeye gerek kalmadan, kurumu tasfiye etmeden.

7. Sonuç

Bugün mesele birkaç çalışanın maaşı değildir.
Bugün mesele, **5,5 milyar TL'lik büyüyen bir sektörün geleceğidir.**
Elektrik nasıl stratejikse, su nasıl stratejikse, haberleşme de stratejiktir.
Teknolojiye karşı değiliz. Telekomünikasyon Dairesi'nin seyirci kaldığı bir dijital dönüşüme karşıyız. Çocuklarımızın yaşayacağı
dijital KKTC'nin altyapısının nasıl şekilleneceğini konuşuyoruz.

Özelleştirme ile atalet arasında üçüncü bir yol vardır: kamu mülkiyeti, mali özerklik ve hareket kabiliyeti.

Hakan Üredi
uredihakan@gmail.com
+90 542 858 00 08

Tek Bir Platformdan Tüm Operasyonu Yönetmek Mümkün mü?

Dijitalleşme, günümüzde yalnızca teknolojik bir dönüşüm süreci değil, aynı zamanda kurumların çalışma kültürünü yeniden şekillendiren önemli bir değişimdir. İş süreçleri büyüdükçe ekipler genişlemekte, projeler çeşitlenmekte ve operasyonların yönetimi her geçen gün daha karmaşık hale gelmektedir. Bu durum, kurumların yalnızca işlerini dijital ortama taşımalarını değil, aynı zamanda bu süreçleri daha akıllı ve bütünleşik şekilde yönetmelerini zorunlu kılmaktadır.

Pek çok kurum bugün proje yönetimi, destek talepleri, doküman paylaşımı, ekip iletişimi ve raporlama gibi süreçleri farklı yazılımlar üzerinden yürütmektedir. İlk bakışta bu yöntem ihtiyaçları karşılıyor gibi görünse de zamanla veri dağınıklığı, bilgi tekrarları, iletişim kopuklukları ve operasyonel verimsizlik gibi sorunlar ortaya çıkmaktadır. Kullanıcıların birden fazla sisteme giriş yapması, aynı bilgiyi farklı platformlara tekrar girmesi ve yöneticilerin farklı kaynaklardan rapor toplamak zorunda kalması, hem zaman kaybına hem de karar alma süreçlerinin yavaşlamasına neden olmaktadır.
Bu nedenle son yıllarda kurumlar, operasyonlarını tek bir platform üzerinden yönetebilecek entegre PMO (Project Management Office) sistemlerine yönelmektedir.

PMO Yaklaşımı Nedir?

PMO, yalnızca projelerin takip edildiği bir yapı değildir. Modern PMO anlayışı; projelerin planlanmasından ekip koordinasyonuna, destek süreçlerinden performans analizlerine kadar birçok operasyonel sürecin merkezi olarak yönetilmesini sağlayan kapsamlı bir yönetim yaklaşımıdır.

Bu yaklaşımın temel amacı, kurum içerisinde yürütülen tüm çalışmaların ortak bir standart altında ilerlemesini sağlamak, ekipler arasındaki koordinasyonu güçlendirmek ve yöneticilere süreçleri tek noktadan izleyebilme imkânı sunmaktır.

Projeleri Yönetmekten Fazlası

Başarılı bir proje yalnızca zamanında tamamlanan proje değildir. Aynı zamanda doğru planlanmış, doğru kaynaklarla yürütülmüş ve süreç boyunca etkin şekilde takip edilmiş bir projedir.

Modern PMO platformları sayesinde projeler; görev kartları, iş akışları, öncelik seviyeleri, zaman planlamaları ve sorumluluk dağılımları ile detaylı şekilde yönetilebilmektedir.

Her ekip üyesi kendi görevlerini net olarak görebilirken, yöneticiler devam eden projelerin genel durumunu tek ekrandan takip edebilmektedir. Geciken işler, yaklaşan teslim tarihleri ve kritik görevler anlık olarak görüntülenebildiği için olası risklere erken müdahale edilebilmektedir.

Bu sayede proje yönetimi yalnızca takip edilen bir süreç olmaktan çıkarak aktif şekilde yönetilen bir yapıya dönüşmektedir.

Destek Süreçlerinde Hız ve Şeffaflık

Her kurumun günlük operasyonlarının önemli bir kısmını destek talepleri oluşturmaktadır. Bu taleplerin e-posta zincirleri veya mesajlaşma uygulamaları üzerinden yönetilmesi, zaman içerisinde kontrolü zorlaştırmaktadır.

PMO yaklaşımında tüm destek talepleri kayıt altına alınır, ilgili ekip veya personele yönlendirilir ve çözüm süreci baştan sona izlenebilir hale gelir.

Talebin ne zaman oluşturulduğu, kim tarafından işlendiği, hangi aşamada olduğu ve ne kadar sürede sonuçlandığı gibi bilgiler sistem tarafından kayıt altına alınır. Böylece hem hizmet kalitesi yükselir hem de süreçlerin performansı ölçülebilir hale gelir.

Ekipler Arasında Güçlü Koordinasyon

Kurumların büyümesiyle birlikte farklı departmanlar arasında koordinasyonu sağlamak her geçen gün daha önemli hale gelmektedir.

Yazılım geliştirme, insan kaynakları, muhasebe, satış, pazarlama veya teknik ekiplerin aynı platform üzerinde çalışması; bilgi akışını hızlandırırken departmanlar arasındaki iletişim kopukluklarını da önemli ölçüde azaltmaktadır.

Görevlerin hangi aşamada olduğu, kimlerin hangi iş yüküne sahip olduğu ve ekiplerin performansı merkezi olarak takip edilebildiği için kaynak planlaması daha sağlıklı yapılabilmektedir.

Veriye Dayalı Karar Alma

Yöneticiler için en değerli kaynaklardan biri doğru ve güncel veridir.
Modern PMO sistemleri yalnızca görev yönetimi yapmakla kalmaz; aynı zamanda operasyonlardan elde edilen verileri anlamlı raporlara dönüştürür.

Tamamlanan projeler, devam eden çalışmalar, geciken görevler, ekip performansları, iş yoğunluğu analizleri ve süreç istatistikleri tek panel üzerinden görüntülenebilir.

Bu yaklaşım sayesinde kararlar kişisel tahminlere değil, ölçülebilir verilere dayandırılır. Böylece hem stratejik planlamalar güçlenir hem de operasyonel iyileştirmeler daha sağlıklı gerçekleştirilebilir.

Yapay Zekâ Destekli Yeni Nesil PMO

Yapay zekâ teknolojilerinin gelişmesiyle birlikte PMO sistemleri de yeni bir dönüşüm yaşamaktadır.

Akıllı görev önerileri, otomatik önceliklendirme, gecikme risklerinin tahmin edilmesi, iş yükü analizleri ve doğal dil ile rapor oluşturma gibi özellikler, yöneticilerin çok daha hızlı karar almasını sağlamaktadır.
Yapay zekâ, yöneticilerin yerine karar veren bir yapı değil; doğru veriyi doğru zamanda sunarak karar alma süreçlerini destekleyen güçlü bir yardımcı haline gelmektedir.

Önümüzdeki yıllarda yapay zekâ destekli PMO platformlarının kurumların dijital dönüşümünde çok daha önemli bir rol üstlenmesi beklenmektedir.

Geleceğin Çalışma Modeli

İş dünyası artık birbirinden bağımsız yazılımların kullanıldığı yapılardan, tüm süreçlerin birbirine bağlı olduğu entegre platformlara doğru ilerlemektedir.
Projelerin, destek süreçlerinin, ekip koordinasyonunun, doküman yönetiminin ve yönetsel raporlamanın aynı sistem içerisinde yönetilmesi; yalnızca operasyonel kolaylık sağlamaz. Aynı zamanda kurum kültürünü güçlendirir, şeffaflığı artırır ve sürdürülebilir büyümeye katkı sağlar.

Tek bir platform üzerinden yönetilen operasyonlar, kurumların değişen ihtiyaçlara daha hızlı uyum sağlamasına, kaynaklarını daha verimli kullanmasına ve rekabet avantajı elde etmesine yardımcı olmaktadır.

Sonuç

Tek bir platformdan tüm operasyonları yönetmek artık geleceğe ait bir vizyon değil, günümüz kurumlarının ulaşabileceği gerçekçi bir hedef haline gelmiştir.

Doğru planlanmış bir PMO yaklaşımı; proje yönetimini, destek süreçlerini, ekip koordinasyonunu, raporlamayı ve kurumsal bilgi yönetimini ortak bir çatı altında birleştirerek daha verimli, daha şeffaf ve daha sürdürülebilir bir çalışma modeli oluşturur.

Dijital dönüşümün başarısı yalnızca kullanılan teknolojilerle değil, bu teknolojilerin kurumun iş yapış biçimine ne kadar doğru entegre edildiğiyle ölçülmektedir. Geleceğin başarılı kurumları, farklı sistemler arasında kaybolan değil; tüm süreçlerini tek merkezden yönetebilen ve veriye dayalı kararlar alabilen organizasyonlar olacaktır.

Naim Sadıklar
Web Yazılım Geliştirme Takım Lideri

Gelişmiş yapay zekalar Mythos 5 ve Fable 5 yeniden kullanıma açıldı.

ABD hükümeti, Anthropic'in Mythos 5 ve Fable 5 yapay zeka modellerine uygulanan erişim kısıtlamasını kaldırdı. ABD Ticaret Bakanlığı'nın kararıyla şirket, kısa süre önce erişime kapatmak zorunda kaldığı modelleri yeniden müşterilerinin kullanımına sunabilecek.

Anthropic, X üzerinden yaptığı açıklamada Ticaret Bakanlığı'ndan gerekli izni aldığını ve 1 Temmuz itibarıyla Mythos 5 ile Fable 5 modellerine erişimi yeniden kademeli olarak açmaya başlayacağını duyurdu.

Şirket, yaklaşık iki hafta önce ABD hükümetinin talimatı doğrultusunda yeni yapay zeka modellerine yabancı uyruklu kişilerin erişimini durdurmakla yükümlü tutulmuştu. Bu kısıtlama ABD'de bulunan ve Anthropic bünyesinde çalışan yabancı uyruklu personeli de kapsıyordu. Düzenlemeye tam uyum sağlamak isteyen şirket ise bunun ardından Mythos ve Fable modellerine erişimi tamamen askıya almıştı.

Kritik altyapı kuruluşlarına izin verilmişti

Aslında hükümet, nihai karar öncesinde Mythos 5 için sınırlı bir istisna tanımıştı. Birkaç gün önce verilen izin kapsamında model, ABD'de kritik altyapıları işleten ve koruyan belirli kuruluşların kullanımına yeniden açılmıştı.

Project Glasswing ortakları kapsamında yer alan yaklaşık 100 kuruluş, Anthropic'in en gelişmiş siber güvenlik odaklı yapay zeka modeline yeniden erişim kazandı. Ancak aynı dönemde, Mythos'un yeteneklerini daha geniş kullanıcı kitlesine ulaştırmak amacıyla geliştirilen Fable 5'in durumu belirsizliğini koruyordu.

Haftalar süren görüşmelerin ardından Ticaret Bakanı Howard Lutnick, Anthropic'in "modellerle ilişkili güvenlik risklerini proaktif olarak tespit etmeyi ve ele almayı; Mythos, Fable ve gelecekteki modeller için protokoller, standartlar ve sürümler konusunda ABD hükümetiyle titizlikle çalışmayı ve herhangi bir kötü niyetli faaliyeti ABD hükümetine bildirmeyi kabul ettiğini" söyledi.
Kaynak: donanimhaber.com

KKTC Bilgi Teknolojileri Ekosistemi: Yapısal Sorunlar ve Mevcut Durum Darboğazı

Giriş: İllüzyonun Ötesinde Bir Dijital Çölleşme
Yıllardır siyasi kürsülerde bir slogan olarak yankılanan "Bilişim Adası" vizyonu, maalesef sahadaki acı gerçeklerle her geçen gün daha sert çarpışmaktadır. Dünya; yapay zeka, SDN (Yazılım Tanımlı Ağlar) ve otonom sistemlerle dördüncü sanayi devrimini yaşarken, KKTC'de bilişim ekosistemi vizyonsuzluk, liyakatsizlik ve teknik ilgisizlik kıskacında boğulmaktadır. Bu makale, süslü vaatlerin arkasındaki yapısal darboğazı ve yaklaşan dijital iflası mercek altına almaktadır.

1. Bilişim İşgücünün Değersizleştirilmesi ve "Teknik Memur" Sendromu
Sektörün en derin yarası, nitelikli bilişim profesyonellerinin stratejik birer değer yerine "sıradan birer çalışan" olarak görülmesidir.

- Sıradanlaştırma ve Liyakat Krizi: Hem devlette hem de özel sektörde bilişim kadroları, teknik yetkinlik yerine çoğu zaman politik müdahalelerle doldurulmaktadır. Mühendislik zekası gerektiren pozisyonların "teknik birer memurluk" seviyesine indirgenmesi, nitelikli beyin göçünü tetiklemektedir.
- Etik Aşınma ve Kişisel Çıkarlar: BT çalışanlarının değersizleştirildiği bir ortamda, etik aşınma kaçınılmaz hale gelmektedir. Emeğinin karşılığını alamayan figürlerin, iş yapan firmalarla kurdukları şahsi ilişkileri kurum menfaatlerinin önüne koyması, ekosistemi içten içe çürüten bir kansere dönüşmüştür.

2. Akademik Atalet: Üniversitelerin Ekosistemden Kopukluğu
KKTC, dünya ölçeğinde bir üniversite yoğunluğuna sahip olsa da, bu kurumların yerel bilişim yaşamına katkısı yok denecek kadar azdır.

- Teorik Labirentler: Üniversiteler, endüstrinin ihtiyaç duyduğu operasyonel beceriler yerine piyasa gerçekliğinden kopuk yoğun teorik bilgiye odaklanmaktadır.
- Diploma Fabrikaları: Teknoparkların teknoloji üretmek yerine vergi avantajlı ofis komplekslerine dönüşmesi ve akademik kadroların saha profesyonelleriyle entegre olamaması, üniversiteleri adanın dijital kalkınmasında lokomotif değil, ancak birer vagon konumuna itmiştir.

3. Lisans İhlalleri ve EoS/EoL İhmali: Güvenlikte "Saatli Bomba"
BT lisans haklarının sistematik ihlali ve cihaz ömür süreçlerinin (EoS/EoL) takibi konusundaki vurdumduymazlık, ulusal bir güvenlik meselesidir.Bilineceği üzere EoS/EoI(End od Sale/Support- End of life) terimi teknolojik ömürlerini tamamlamış,satışı kanuni olarak gerçekleşmeyen ve hürtürlü yazılım/donanım desteği alınmayan cihazlar için kullanılmaktadır.

- Korsan ve Güncellenmeyen Sistemler: Lisanssız yazılımlar ve artık güncelleme almayan demode donanımlarla kritik altyapıları yönetmeye çalışmak, küresel siber saldırganlara karşı "kalkanı indirilmiş bir kale" gibi beklemekle eşdeğerdir.

4. Teknolojik Körlük: IPv6 Çıkmazı ve Modern Ağ Paradigması
Dünya interneti IPv6 üzerinde yeniden kurgulanırken, KKTC'nin hala IPv4 adres tükenmişliği ve CGNATve diğer NAT teknolojileri ile mahkumiyetiyle boğuşması teknolojik bir utançtır.(NAT doğrudan IP kullanma yerine dolaylı kullanma metodunu anlatır)

- Mimari Geri Kalmışlık: SDN, VXLAN ve modern veri merkezi mimarilerinin ıskalanması, adayı dijital bir gettoya hapsetmektedir. Bu hantallığı aşabilecek olan "endüstriyel sertifikasyon kültürü ise hem kamuda hem akademide sistematik olarak değersizleştirilmektedir.

5. Yönetimsel ve Kurumsal Boşluk: "Sahipsiz" Dijital Sınırlar
Hükümet yapısında müstakil bir "Dijital Dönüşüm Bakanlığı" veya tam yetkili bir otoritenin bulunmaması, dijitalleşmeyi sahipsiz bırakmaktadır.

- Ulusal SOM Eksikliği: Güney Kıbrıs'ta Digital Security Authority (DSA) gibi yapılar siber sınırları korurken, KKTC'de tehditleri 7/24 izleyen operasyonel bir üst yapının (Ulusal SOM) yokluğu, kritik altyapıları her türlü sabotaja açık hale getirmektedir.

6. Sonuç: İthal Bir Gelecek mi, Yerli Bir Diriliş mi?
Mevcut gidişat, "Bilişim Adası" vizyonunun ancak bu memleketin kendi insan kaynağını yok ederek gerçekleşebileceğini göstermektedir. Kendi mühendisini liyakatle istihdam edemeyen, üniversitelerini sektörle barıştıramayan ve sistemlerini demode protokollerle yürüten bir yapı; yarın tüm yasalarını ithal etmek, tüm stratejik noktalarını dış kadrolara teslim etmek ve dijital egemenliğini tamamen devretmek zorunda kalacaktır.
Kendi insanını ve teknik uzmanlığını değersizleştirerek bir başkasının "dijital sömürgesi" olmak ile gerçek bir bilişim adası olmak arasındaki tercih, bugünün karar vericilerinin omuzlarındadır. Ya bugün liyakati ve teknik standardı temel alan kurumsal bir irade inşa edilecek, ya da KKTC bilişim dünyası tamamen "ithal bir kadere" teslim olacaktır.

Yusuf KÜÇÜK
yusufkucuk2014@gmail.com

Bir yarışmanın ardından...

Türkiye Bilişim Derneği (TBD)'nin Türkiye'de her yıl düzenlediği GBYF (Genç Beyinler Yeni Fikirler) yarışması, TBD ve BTHK işbirliği ve Lefke Avrupa Üniversitesi'nin desteği ile ilk kez 8 Mayıs 2026 tarihinde tam gün olarak Kuzey Kıbrıs'ta düzenlenmiştir. BTKıbrıs dergisi yazarlarından bazıları bu yarışmada juri olarak görev almıştır. Tahminlerimin çok üstünde büyük bir katılım vardı. Öğrendiğim kadarı ile 165 başvuru gelmiş, bizim alanda gördüğümüz, 100'ün üstünde proje alanda sergileniyordu. Yani hakemlerin (jüri) 5 saat içerisinde bu kadar projeyi değerlendirmesi ve puanlaması bekleniyordu. Öğrenciler o kadar heyecanlı idiler ki, hakemleri teker teker çağırıp projelerini tanıtmaya çalışıyorlardı. Ben, son 10 yıl içerisinde çoğu zaman üniversitelerin mühendislik programlarının bitirme (mezuniyet) projelerine dış juri üyesi olarak katılmama rağmen, bu coşkuyu ilk kez yaşamıştım. Üniversitelerdeki bitirme projeleri sunumları, daha fazla bir yarışma veya kendi projelerini iyi gösterme heyecanından çok, mezuniyet için en iyi notu alma kurgusu içerisinde iken, bu yarışmada genç öğrenciler, birbirleri arasında en iyi, en başarılı, en uygulanabilir, en ticarişebilir projenin kendilerinin projesi olması konusunda rekabetçi oluyordu. Tek kişilik projeler olduğu gibi , takım olarak proje sunan gençler de vardı. Tüm projeleri verilen süre içerisinde değerlendirmek pek mümkün olmayacaktı. Bütün projeler birbirinden güzel, başarılı olmasına rağmen yarısından fazlasını değerlendirme imkanı bulabildim. Üniversite öğrencilerinin demografik yapısı gereği, proje takımlarının da yaklaşık %65 i , TC ve 3. ülke öğrencisi idi. Tüm hakemlerin verdiği puanlar neticesinde iki kategoride 3 en iyi puan alan projeler seçildi ve ödüllendirildi. Ödüllendirilen 6 proje içerisinde 5 tanesinin benim değerlendirdiğim projeler arasında olması beni biraz rahatlattı. Böylesine güzel ve etkili bir yarışmayı düzenleyen TBD ve BTHK kuruluşlarına teşekkür borcumuz var. Ayrıca, bu yarışmanın sponsorları arasında, BT Kıbrıs yazarı ve Teknoloji Firması "EMİ Technogies" firmasının yani bir KKTC firmasının bulunması da benim değer gördüğüm noktalardan birisidir. Bu yarışmadan sonra, 20 civarında proje takımı benimle irtibat kurup görüştü.

Bu yarışmadan, kendim adıma söylemek gerekirse, oldukça değerli ve önemli bulgu ve çıktılar oluşmuştur. Bu soruların cevabını bulmak eminim çok zor olmasa gerek. Ama, "Kuzey Kıbrıs Türk toplumu olarak Inovasyonun, Teknolojik çalışmaların neresindeyiz." sorusuna cevap için oldukça önemlidir.

1. KKTC bünyesindeki bir STO veya bir kurum/kuruluş, bu yarışmayı düzenlemeye talip olsaydı, bu kolabratif desteği sağlayabilir miydi?
2. Heyecanları zirvede olan bu öğrencilerin, yarışmadan sonra, dereceye girsin girmesin, bu güzel projelerini KKTC'de uygulayabilecekleri bir ortam var mıdır?
3. Bu projelerin Kuzey Kıbrıs adına ticarileştirilmesi için, yabancı öğrencilerin bir süre daha adada kalması için gereken mevzuat var mıdır?
4. Bu projelerin Kuzey Kıbrıs adına ticarileştirilmesi için, fiziki olarak devlet ve/veya özel sektör destekli , Kuluçka Merkezleri, Araştırma ve Geliştirme Merkezleri, Teknoloji Transfer Ofisleri, StartUp Kümelenmesi var mıdır?
5. Bu projelerin, bitirme ve/veya ders projesi olduğuna ve üniversitelerimizin eğitimdeki kalitesinin bir görüntüsü olarak kabul ettiğimiz varsayımından hareketle, yüksek öğrenimle ilgili kurum/kurumlarımızın ilgisi ne kadardır?
6. Bu projelerin ne kadarına sahip çıkabiliyoruz?
7. Bu gençlerimizin yarışmadaki heyecanınından sonra görecekleri ilgisizlik, bu gençleri nasıl bir yönelime sürükleyecektir?
8. Bu projeleri izleyen ve/veya değerlendiren özel sektör var ise, kaç tanesi bu öğrencilerle ilgilenmiştir?
9. Dış destekleri memnuniyetle kabul etmekle birlikte, bu tür yarışmaları, dönemsel olarak yapabilecek kurumlarımız yok mudur?
10. Bu yarışmaya, BTHK nedeni ile Ulaştırma Bakanlığı damgaını vurmuş olsa da, projeler içerisinde eğitim teknolojileri, tarım teknolojileri, sağlık teknolojileri vs.. değişik projeler olduğundan, özellikle Eğitimden sorumlu bakanlığın, ArGe'den sorumlu bakanlığın ve diğer bakanlıkların ilgisi ve etkisi ne kadardır?

Bu sorulara, olumlu cevap ve çözüm bulduğumuz zaman, Kuzey Kıbrıs Inovasyon ve Teknoloji alanında hızla ilerlemeye ve rekabet edebilecek bir konuma gelebilecektir. Bunun için en önemli olgu, genç beyinleri ve yeni fikirleri sahiplenme ve desteklemekten geçmektedir.

Necdet İcil
Independent ICT Expert, Mentor, Project Manager, GMTGB YK Üyesi

KOBİ'ler İçin Siber Güvenlik: Büyük Bütçeler Olmadan Veriyi Korumak Mümkün mü?

Yerel işletme sahipleriyle yaptığım görüşmelerde sıkça aynı düşünceyle karşılaşıyorum:
"Siber güvenlik büyük şirketlerin işi. Bizim gibi küçük işletmelerin milyonlarca liralık sistemlere bütçesi yetmez."
Oysa gerçek tam tersidir.

Siber saldırganlar çoğu zaman güçlü güvenlik ekiplerine sahip büyük kurumlarla uğraşmak yerine, güvenlik önlemleri daha zayıf olan küçük ve orta ölçekli işletmeleri hedef alır. Çünkü onlar için önemli olan şirketin büyüklüğü değil, savunmasının ne kadar zayıf olduğudur.

Geçtiğimiz dönemde bir işletme sahibi bana şu soruyu sormuştu:

"Biz sadece birkaç çalışanı olan küçük bir firmayız. Bizi neden hedef alsınlar?"

Birkaç ay sonra aynı işletme, çalışanlarından birinin açtığı sahte bir e-posta eki nedeniyle günlerce sistemlerine erişemedi. Saldırganların hedefi sektörleri veya büyüklükleri değildi; yalnızca kolay bir hedef olmalarıydı.

İyi haber şu ki işletmenizi korumak için devasa bütçelere ihtiyacınız yok. Doğru alışkanlıklar, temel güvenlik önlemleri ve düzenli kontroller çoğu zaman pahalı çözümlerden daha fazla fayda sağlayabilir.

Dijital Kasanızda Ne Var? Önce Riskinizi Tanıyın

Siber güvenlik yatırımlarının ilk adımı teknoloji satın almak değil, neyi korumaya çalıştığınızı bilmektir.

Kendinize şu soruyu sorun:

"Yarın sabah tüm bilgisayarlarımız çalışmaz hale gelse, hangi veriler olmadan işimizi sürdüremeyiz?"

Bu veriler;

- müşteri kayıtları,
- muhasebe verileri,
- sipariş bilgileri,
- sözleşmeler,
- personel kayıtları

olabilir.

En kritik verilerinizi belirlemeden yapılan güvenlik yatırımları, nereye gideceği belli olmayan bir sigorta poliçesi satın almaya benzer.

Önce en değerli dijital varlıklarınızı belirleyin, sonra koruma katmanlarını onların etrafında oluşturmaya başlayın.

Herkese Her Anahtar Verilmez

KOBİ'lerde sık karşılaştığım bir diğer durum ise ortak klasörlere ve sistemlere verilen sınırsız erişim yetkileridir.

Google Drive, OneDrive, NAS cihazları veya şirket sunucularında çoğu zaman herkes her şeye erişebilmektedir.

Fiziksel dünyada ofisin temizlik personeline muhasebe kasasının anahtarını teslim etmiyorsanız, dijital dünyada da her çalışana tüm şirket verilerine erişim vermemelisiniz.

Bilgiye erişim, görev ihtiyacı kadar olmalıdır.

Bu yaklaşım bilgi güvenliği dünyasında "En Az Yetki Prensibi" olarak bilinir ve en etkili güvenlik önlemlerinden biridir.

Yedek Almak Yetmez, Kurtarabilmek Gerekir

Birçok işletmede şu cümleyi duyarım:

"Merak etmeyin, yedeklerimizi alıyoruz."

Ancak asıl soru şudur:

"Son yedeğinizden başarılı şekilde geri dönüş yapabildiniz mi?"

Harici diskte tutulan ve sürekli sisteme bağlı kalan yedekler, bir fidye yazılımı saldırısında bilgisayarlarla birlikte şifrelenebilir.

Bu nedenle:

- Verilerinizi düzenli yedekleyin.
- En az bir kopyayı çevrimdışı veya izole bir ortamda saklayın.
- Belirli aralıklarla geri yükleme testleri yapın.

Yedeklerin çalıştığından emin olmak, yedek almaktan daha önemlidir.

Şifreler ve Güncellemeler Hâlâ En Güçlü Savunmalardan Biri

Siber saldırıların önemli bir bölümü teknik ustalıkla değil, basit ihmaller nedeniyle başarılı olmaktadır.

Bugün hâlâ:

- 123456
- şirket adı
- doğum tarihi

gibi tahmin edilmesi kolay şifrelerle karşılaşabiliyoruz.

Güçlü parola kullanımı ve iki faktörlü kimlik doğrulama (2FA), uygulanması en kolay ve en etkili güvenlik önlemleri arasındadır.

Aynı şekilde işletim sistemlerini, modemleri, güvenlik duvarlarını ve kullandığınız yazılımları güncel tutmak da kritik önem taşır.

Ertelenen her güncelleme, potansiyel bir güvenlik açığının daha uzun süre açık kalması anlamına gelir.

Siber Güvenlik Bir Teknoloji Konusu Değil, Yönetim Konusudur

Birçok işletme siber güvenliği yalnızca bilgisayarların veya teknik personelin sorumluluğu olarak görüyor.

Oysa en pahalı güvenlik duvarı bile yanlış kişiye gönderilen bir Excel dosyasını engelleyemez.

En gelişmiş antivirüs yazılımı bile çalışanların dikkatsizce paylaştığı müşteri bilgilerini koruyamaz.

Bu nedenle siber güvenlik;

- teknoloji,
- süreç,
- çalışan farkındalığı,
- yönetim disiplini

birlikte ele alındığında anlam kazanır.

Sonuç

Siber güvenlik artık büyük şirketlerin ayrıcalığı değil, her işletmenin temel sorumluluğudur.

İyi haber şu ki KOBİ'lerin güvenliğini artırmak için her zaman büyük bütçeler gerekmez. Doğru risk değerlendirmesi, kontrollü erişim, sağlam yedekleme politikaları ve çalışan farkındalığı sayesinde birçok risk önemli ölçüde azaltılabilir.

Fiziksel kasanızı açık bırakmazsınız.

Peki dijital kasanız ne kadar güvende?
Destech IT Solutions olarak işletmelerin ihtiyaçlarına uygun, uygulanabilir ve sürdürülebilir veri güvenliği stratejileri geliştirmelerine destek vermeye devam ediyoruz.

Erkan Emirzade
Bilgisayar Mühendisi

SİBER GÜVENLİK: ARTIK BİR TERCİH DEĞİL, ZORUNLULUK…

Son aylarda ülkemizde çeşitli kamu kurumları ve dijital hizmet platformlarıyla ilgili olarak basına yansıyan siber güvenlik haberleri, dijital dünyada güvenliğin ne kadar önemli hale geldiğini bir kez daha göstermiştir. Haberlerin teknik detayları ve doğruluk dereceleri ilgili kurumlar tarafından değerlendirilmeye devam ederken, ortaya çıkan tablo hepimize önemli bir gerçeği hatırlatmaktadır: Dijitalleşme hızla ilerlerken, siber güvenlik aynı hızla güçlendirilmediği takdirde kurumlarımız ve vatandaşlarımız ciddi risklerle karşı karşıya kalabilmektedir.

Bugün kamu hizmetlerinden sağlık sistemlerine, belediye işlemlerinden çalışma izinlerine, eğitim sistemlerinden finansal işlemlere kadar birçok hizmet dijital platformlar üzerinden yürütülmektedir. Vatandaşlarımızın kimlik bilgileri, iletişim bilgileri, eğitim kayıtları, çalışma izinleri, mali verileri ve bazı durumlarda sağlık bilgileri bu sistemlerde tutulmaktadır.

Dolayısıyla siber güvenlik artık yalnızca bilgi işlem birimlerinin teknik sorunu değildir. Siber güvenlik; kamu güvenliği, ekonomik güvenlik, kişisel verilerin korunması ve toplumsal güven meselesidir.

Dünyanın en gelişmiş ülkeleri, en büyük teknoloji şirketleri ve en güçlü kamu kurumları dahi zaman zaman siber saldırılarla karşı karşıya kalmaktadır. Bu nedenle hiçbir kurumun yüzde yüz güvenli olduğunu söylemek mümkün değildir. Önemli olan saldırının hiç yaşanmaması değil, saldırılara karşı hazırlıklı olmak, riskleri azaltmak, saldırıları erken tespit edebilmek ve oluşabilecek zararları en aza indirebilmektir.

Son dönemde kamuoyuna yansıyan olaylar bize bir başka gerçeği daha göstermektedir. Kurumlarımızın büyük çoğunluğu saldırıları engellemek için belirli tedbirler almakta, ancak saldırıları erken tespit edecek ve anlık olarak izleyebilecek mekanizmalara yeterince sahip olmayabilmektedir.

Günümüzde modern siber güvenlik yaklaşımı yalnızca güvenlik duvarı kurmak veya antivirüs kullanmak değildir. Asıl amaç, sistem içerisinde olağan dışı hareketleri erken fark edebilmek ve olası bir ihlali büyümeden durdurabilmektir.

Bu nedenle gelişmiş ülkelerde Güvenlik Operasyon Merkezleri (SOC), Siber Olaylara Müdahale Ekipleri (SOME), merkezi log yönetimi sistemleri, güvenlik bilgi ve olay yönetimi sistemleri (SIEM) ve gerçek zamanlı izleme altyapıları yaygın olarak kullanılmaktadır.

Bir saldırgan sisteme giriş yapmayı başarsa bile, bu sistemler sayesinde olağan dışı hareketler dakikalar içerisinde fark edilebilmekte ve müdahale süreçleri başlatılabilmektedir.

Bilgi İşlem Personelinin Rolü

Siber güvenlik yalnızca yöneticilerin veya kurumların sorumluluğu değildir. Bilgi işlem birimlerinde görev yapan teknik personelin de sürekli gelişen tehditlere karşı kendisini güncellemesi gerekmektedir.
Bugün bilgi işlem personelinden beklenen yalnızca sistemleri çalıştırmak değildir. Aynı zamanda sistemleri izlemek, güvenlik risklerini değerlendirmek, kullanıcıları bilinçlendirmek ve olası tehditleri erken fark edebilmektir.

Bu nedenle kurumlarımızın teknik personellerinin düzenli eğitimlere katılması, uluslararası standartları takip etmesi ve mesleki gelişim faaliyetlerine destek verilmesi büyük önem taşımaktadır.

Kurum Yöneticilerinin Rolü

Siber güvenlik çoğu zaman teknik bir konu olarak görülse de aslında yönetsel bir konudur.

Bir kurumun siber güvenlik seviyesi, yalnızca kullandığı teknolojilerle değil, yöneticilerinin konuya verdiği önemle de doğrudan ilişkilidir.
Yönetim kademelerinin siber güvenliği bir maliyet kalemi olarak değil, kurumsal risk yönetiminin ayrılmaz bir parçası olarak görmesi gerekmektedir.

Nasıl ki binalar için yangın güvenliği, araçlar için trafik sigortası veya iş yerleri için iş sağlığı ve güvenliği vazgeçilmez unsurlarsa, dijital sistemler için de siber güvenlik aynı öneme sahiptir.

Ülkemizin İhtiyacı: Ulusal Yaklaşım

KTMMOB Bilgisayar Mühendisleri Odası olarak uzun yıllardır ülkemizde bir Ulusal Siber Güvenlik Stratejisi hazırlanması gerektiğini savunmaktayız.

Kurumların tek tek çabaları önemlidir ancak yeterli değildir.
Siber tehditler kurum tanımamaktadır.

Bu nedenle kamu kurumları, yerel yönetimler, üniversiteler, düzenleyici kurumlar, özel sektör ve meslek örgütleri arasında koordinasyon sağlanmalıdır.

Ulusal ölçekte görev yapacak bir Siber Güvenlik Merkezi kurulması, kritik altyapıların merkezi olarak izlenmesi, kurumlar arası bilgi paylaşımının artırılması ve ulusal siber olay müdahale kapasitesinin geliştirilmesi artık bir tercih değil, ihtiyaç haline gelmiştir.

BMO Olarak Ne Yapıyoruz?

KTMMOB Bilgisayar Mühendisleri Odası olarak siber güvenlik konusunu yalnızca gündeme gelen olaylar sonrasında konuşan bir kurum olmayı değil, sürekli farkındalık ve kapasite geliştirme çalışmaları yürüten bir meslek örgütü olmayı hedefledik.
Bu kapsamda son dört yıldır çeşitli kamu kurumları, belediyeler, eğitim kurumları ve sivil toplum kuruluşlarıyla iş birliği içerisinde çok sayıda farkındalık etkinliği ve eğitim programı gerçekleştirdik.
Güvenli İnternet Kullanımı, Siber Güvenlik Farkındalığı ve Bilinçli Teknoloji Kullanımı

başlıklarında düzenlediğimiz eğitimler ile; ortaokul öğrencilerine, kamu çalışanlarına, sivil toplum kuruluşlarına, belediye personellerine ve 60 yaş üstü vatandaşlarımıza yönelik yüz yüze farkındalık eğitimleri yürüttük. Ebeveynlere yönelik televizyon kanalında yayınlanacak şekilde bilgilendirici kamu spotu yayınları hazırladık. Yakın bir zamanda yayında olacaktır.

Bu eğitimlerde yalnızca teknik konular değil; dijital dolandırıcılıklar, sosyal mühendislik saldırıları, güçlü parola kullanımı, kişisel verilerin korunması, çocukların internet güvenliği ve dijital dünyada bilinçli davranış modelleri gibi günlük yaşamı doğrudan etkileyen konular da ele alınmıştır.

Çünkü siber güvenliğin ilk savunma hattı teknoloji değil, bilinçli insanlardır.

Geleceğe Yönelik Projelerimiz

Odamız, yalnızca farkındalık eğitimleriyle yetinmemekte, aynı zamanda ülkemizin ihtiyaç duyduğu nitelikli insan kaynağının yetiştirilmesine yönelik çalışmalar da yürütmektedir.

Önümüzdeki dönemde üniversiteler, eğitim kurumları, özel sektör ve kamu kuruluşlarıyla iş birliği içerisinde; siber güvenlik uzmanlığı eğitim programları, uluslararası sertifikasyon süreçleri, uygulamalı laboratuvar eğitimleri, genç mühendis gelişim programları, siber güvenlik yarışmaları ve hackathonlar, kurumsal farkındalık eğitimleri gibi projelerin hayata geçirilmesi hedeflenmektedir.

Amacımız yalnızca sistemleri korumak değil, bu sistemleri koruyabilecek insan kaynağını da ülkemize kazandırmaktır.

Son söz;

Son günlerde kamuoyuna yansıyan olaylar, hepimiz için önemli dersler içermektedir.

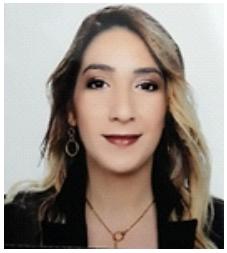
Bu olayları kurumları veya kişileri suçlamak için değil, ülkemizin dijital dayanıklılığını artırmak için bir fırsat olarak değerlendirmeliyiz.
Bugün atılacak doğru adımlar, yarının krizlerini önleyecektir.

Kıbrıs Türk Bilgisayar Mühendisleri Odası olarak, kamu kurumlarımızın, özel sektörümüzün ve vatandaşlarımızın daha güvenli bir dijital geleceğe sahip olması için çalışmalarımızı sürdürmeye, bilgi ve tecrübemizi paylaşmaya ve çözüm üretmeye devam edeceğiz.

Çünkü siber güvenlik yalnızca bilgi işlem uzmanlarının değil, dijital dünyada yaşayan hepimizin ortak sorumluluğudur.

Esat GÜRHAN – *Bilgisayar / AI Prompt Mühendisi*
KTMMOB Bilgisayar Mühendisleri Odası Başkanı
esat.gurhan@ktbmo.org
0548 – 843 79 10

"AGENTIC AI MIMARISI: BIR AGENT NASIL DÜŞÜNÜR, PLANLAR VE HAREKETE GEÇER?"

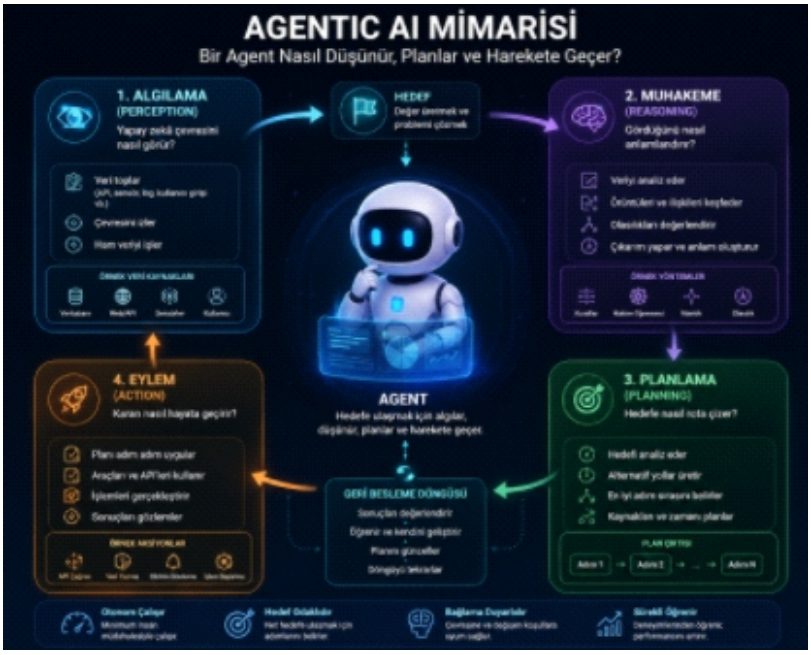


Bu başlığı bugünün dünyasıyla eşleştirecek olursak, belki de önce şu soruyu sormalıyız: Eğer ben bir agent olsaydım, nasıl düşünürdüm? Bir hedefe ulaşmak için hangi verileri toplar, hangi parametreleri değerlendirir ve doğru zamanda nasıl harekete geçerdim?

Bugün yapay zekâ ile kurduğumuz ilişki tam da bu soruların etrafında şekilleniyor. Birçoğumuz yapay zekâ araçlarını tüketim konusunda oldukça cömertçe kullanıyoruz; fakat bazılarımız hâlâ bu dönüşüm karşısında içsel bir tereddüt yaşıyor.

Özellikle yazılım dünyasında çalışan meslektaşlarımla konuştuğumda bunu sıkça hissediyorum. Bir algoritmayı saatlerce, bazen günlerce kurmaya çalışan insanların, bugün aynı çıktıyı saniyeler içinde alabilmesi hem büyük bir nimet hem de garip bir yüzleşme yaratıyor. Çünkü bir yandan "Keşke o zamanlar elimizde olsaydı" diyoruz; diğer yandan içimizde bir yerde, o mücadeleyle büyüyen tarafımızı özlüyoruz.

Belki de asıl dönüşüm burada başlıyor: Artık sadece yazılım üretmiyoruz; düşünebilen, planlayabilen ve harekete geçebilen sistemler tasarlıyoruz. İşte Agentic AI mimarisi tam olarak bu kırılma noktasında anlam kazanıyor.



Yapay zekânın nasıl düşündüğünü anlatırken, uzman bir meslektaşımın bir makalesinde karşılaştığım satranç örneği aklıma geliyor: Yapay zekâ, tıpkı bir satranç oyuncusunun birkaç hamle sonrasını hesaplaması gibi, her adımın olası sonucunu tartar.

Peki burada asıl soru şu: Bir agent gerçekten düşünür mü?

Bir agent için düşünmek, önce çevresini algılamakla başlar. Gelen veriyi anlamlandırır, mevcut durumu analiz eder, hedefi ile mevcut durum arasındaki farkı ölçer ve bu boşluğu kapatacak en uygun yolu planlamaya çalışır.

İnsanlarla, agentlar arasında bulunan en net fark, insan hesaplamalarını bilinçle yapar, agent ise mimarisi gereği.

Agentic AI'nın kalbinde yatan yapı tam olarak budur: Algılama, muhakeme, planlama ve eylem.

- **Algılama (Perception): Yapay zekâ çevresini nasıl görür?**
- **Muhakeme (Reasoning): Gördüğünü nasıl anlamlandırır?**
- **Planlama (Planning): Hedefe nasıl rota çizer?**
- **Eylem (Action): Kararı nasıl hayata geçirir?**

1. Algılama (Perception): Yapay zekâ çevresini nasıl görür?

Bir agent için her şey algılamakla başlar. İnsan nasıl çevresinden ses, görüntü ve deneyim topluyorsa; yapay zekâ da veriyle beslenir. Bu veri bir müşteri davranışı, sistem logları, finansal hareketler ya da kullanıcı talepleri olabilir. Agent, önce bulunduğu ortamı anlamaya çalışır. Çünkü doğru görmeyen bir sistem, doğru düşünemez.

2. Muhakeme (Reasoning): Gördüğünü nasıl anlamlandırır?

Algılanan veri tek başına bir anlam ifade etmez. Burada devreye muhakeme girer. Agent topladığı bilgileri analiz eder, örüntüler arar, riskleri değerlendirir ve olasılıkları hesaplar. Tıpkı bir insanın karşısındaki problemi zihninde çözmeye çalışması gibi, yapay zekâ da veriyi bilgiye dönüştürür.

3. Planlama (Planning): Hedefe nasıl rota çizer?

Bir hedef varsa, o hedefe giden yol da vardır. Planlama aşamasında agent, mevcut durum ile ulaşmak istediği sonuç arasındaki boşluğu analiz eder. Bu noktada alternatif yollar üretir, hangi adımın daha verimli olduğunu hesaplar ve kendine bir yol haritası oluşturur. Aslında burada sadece "ne yapacağını" değil, "hangi sırayla yapacağını" belirler.

4. Eylem (Action): Kararı nasıl hayata geçirir?

Düşünmek ve planlamak tek başına yeterli değildir; önemli olan harekete geçmektir. Agent burada kararını uygular. Bir API çağırabilir, bir işlemi başlatabilir, bir kullanıcıya öneri sunabilir ya da bir riski otomatik olarak engelleyebilir. İşte klasik yapay zekâ ile Agentic AI arasındaki temel fark burada ortaya çıkar: Biri önerir, diğeri uygular.

Ve belki de bir agent'ın nasıl düşündüğünü anlamak, insanın kendi düşünme biçimini yeniden keşfetme yolculuğu olacaktır.

Fatoş Leymoncu ÖZBİNGÜL
Bilgisayar Mühendisi / AI Researcher
LinkedIn: linkedin.com/in/ozbingulfatos

KKTC'deki Siber Saldırılar bir kader mi? Yoksa bilinçsiz kullanıcı kaynaklı mı?

Son zamanlarda bir çok kurum ve özel şirkete siber saldırılar yapıldığı haberleri gerek basında gerekse sosyal medyada haber olarak okuyoruz. Nedir bu Siber Saldırı?

Siber saldırı, kişi, kurum veya devlete ait bilgisayar sistemlerine (ağlarına), dijital cihazlarına veya bilgi işlem sistemlerine yetkisiz olarak erişme, zarar verme, verileri çalma veya sistemin işleyişini kesintiye uğratma amacıyla yapılan kasıtlı ve kötü niyetli girişimlerdir. Bu eylemler genellikle maddi çıkar, casusluk veya sabotaj amacıyla bilgisayar korsanları (hackerlar) tarafından gerçekleşse de genç nesil bunu tamamen tecrübe edinmek, zevk amaçlı da yapmaktadır.

Son **3 yıl (Temmuz 2023 – Temmuz 2026)** dikkate alındığında, kamuoyuna yansıyan ve güvenilir kaynaklarla doğrulanan veya güçlü şekilde raporlanan olaylar aşağıdaki gibidir.

Tarih	Kurum / Sektör	Olay	Sonuç	Doğrulanma Durumu	Haber Kaynağı
2023	Çeşitli kamu kurumları	DDoS ve web sitelerine yönelik saldırılar	Bazı kamu hizmetlerinde kısa süreli kesintiler yaşandı.	**Kısmen doğrulandı** (kurum bazında ayrıntılar açıklanmadı)	Çeşitli yerel basın haberleri ve BTHK siber güvenlik değerlendirmeleri. (Instagram)
2024	Belediyeler	Web siteleri ve sosyal medya hesaplarına yönelik saldırılar	Bazı belediyelerde hizmet kesintileri ve hesap ele geçirme olayları yaşandı.	**Kısmen doğrulandı**	Yerel basın haberleri (Kıbrıs Postası, Haber Kıbrıs, Kıbrıs Gerçek vb.) ve belediye açıklamaları. (Instagram)
Mart 2025	BTHK	Kurum altyapısına yönelik siber saldırı girişimi	Saldırı engellendi, veri kaybı olmadığı açıklandı.	✅ **Resmî olarak doğrulandı**	BTHK Resmî Açıklaması, Kıbrıs Postası, Haber Kıbrıs, Bugün Kıbrıs. (KIBRIS POSTASI)
Mayıs 2025	Ekonomi ve Enerji Bakanlığı	Bilgi sistemlerine siber saldırı	Veri sızıntısı olmadığı açıklandı.	✅ **Resmî olarak doğrulandı**	Bakanlık açıklaması ve Kıbrıs Postası. (Instagram)
2025	KIB-TEK	Bilgi sistemlerine izinsiz erişim iddiaları	Polis soruşturmasına konu oldu. Olayın dış saldırı mı yoksa yetkisiz erişim mi olduğu netleşmedi.	⚠ **Olay doğrulandı, saldırı niteliği doğrulanmadı**	Polis soruşturmasına ilişkin yerel basın haberleri ve kamuoyu açıklamaları. (Instagram)
2025–2026	Bankacılık sektörü	DDoS ve fidye yazılımı girişimleri	Birden fazla bankanın etkilendiği iddia edildi, isimler açıklanmadı.	⚠ **Sektörel düzeyde doğrulandı, kurum bazında doğrulanmadı**	Bayındırlık ve Ulaştırma Bakanı Erhan Arıklı'nın açıklamaları, BTHK değerlendirmeleri ve sektör kaynakları. (Instagram)
Nisan–Haziran 2026	Basın kuruluşları ve gazeteciler	Sosyal medya hesaplarının ele geçirilmesi	Çok sayıda hesap etkilendi. BTHK bazı vakaların teknik olarak "siber saldırı" değil, platform kaynaklı işlemler olduğunu açıkladı.	✅ **Olay doğrulandı, bazı vakaların niteliği tartışmalı**	BTHK açıklaması ve yerel medya haberleri. (Instagram)
Haziran 2026	Çalışma ve Sosyal Güvenlik Bakanlığı	Çalışma İzinleri Portalına saldırı	Sistem korundu, veri kaybı olmadığı açıklandı.	✅ **Resmî olarak doğrulandı**	Bakanlık açıklaması ve yerel basın haberleri. (Instagram)
Haziran 2026	Sağlık Bakanlığı	Yaklaşık 364 bin kişilik veri sızıntısı iddiası	Adli ve idari inceleme başlatıldı.	⚠ **Veri sızıntısı iddiası var, kesin sonucu henüz doğrulanmadı**	Yeniçağ Kıbrıs, Haber Kıbrıs, siyasi parti açıklamaları ve soruşturma haberleri. (Instagram)
Haziran 2026	Girne Belediyesi	Belediye Başkanının sosyal medya hesaplarının ele geçirilmesi	Hesaplar geçici olarak erişim dışı kaldı.	✅ **Doğrulandı**	Girne Belediyesi resmî açıklaması ve Kıbrıs Türk Medya. (Kıbrıs Türk Haber)
2026	Casino sektörü	Kumarhane bilgi sistemlerine sızma ve jackpot manipülasyonu iddiaları	Polis soruşturmalarına yansıdı, işletme isimleri açıklanmadı.	⚠ **Olay doğrulandı, kurum isimleri doğrulanmadı**	Yerel basın (özellikle Gıynık Gazetesi ve diğer haber portalları), polis soruşturma haberleri. (Instagram)

Yukardaki tablo yıl ve aya göre, hangi kuruma ne tür bir saldırı yapıldığını göstermektedir. Aşağıda ise yapılan saldırılardaki saldırı türleri ve bu saldırı türlerinin açıklamalarını bakacağız.

DDoS (Distributed Denial of Service) Saldırısı: Bir web sitesi veya sunucunun aynı anda binlerce hatta milyonlarca sahte istekle bombardımana tutulmasıdır. Amaç sistemi çökertmek veya hizmet veremez hale getirmektir. Bu saldırıda genellikle veri çalınmaz; hizmet kesintisi oluşturulur.

Web Sitesine Yönelik Siber Saldırı: Web sunucusunu, web uygulamasını veya içerik yönetim sistemini hedef alan saldırılardır. Amaç web sitesini bozmak, erişilemez hale getirmek, zararlı kod yerleştirmek veya kullanıcı bilgilerini ele geçirmektir.

Yukardaki tablo yıl ve aya göre, hangi kuruma ne tür bir saldırı yapıldığını göstermektedir. Aşağıda ise yapılan saldırılardaki saldırı türleri ve bu saldırı türlerinin açıklamalarını bakacağız.

DDoS (Distributed Denial of Service) Saldırısı: Bir web sitesi veya sunucunun aynı anda binlerce hatta milyonlarca sahte istekle bombardımana tutulmasıdır. Amaç sistemi çökertmek veya hizmet veremez hale getirmektir. Bu saldırıda genellikle veri çalınmaz; hizmet kesintisi oluşturulur.

Web Sitesine Yönelik Siber Saldırı: Web sunucusunu, web uygulamasını veya içerik yönetim sistemini hedef alan saldırılardır. Amaç web sitesini bozmak, erişilemez hale getirmek, zararlı kod yerleştirmek veya kullanıcı bilgilerini ele geçirmektir.

Siber Saldırı Girişimi: Kurumun bilgi sistemlerine yönelik yapılan ancak güvenlik sistemleri tarafından engellenen saldırı teşebbüsüdür. Saldırı başarılı olmayabilir ancak sistem hedef alınmıştır.

Bilgi Sistemlerine Siber Saldırı: Kurumun sunucuları, ağ altyapısı, veri tabanları veya uygulamalarını hedef alan genel saldırıları ifade eder. Bu kapsamda DDoS, zararlı yazılım, fidye yazılımı veya yetkisiz erişim girişimleri bulunabilir.

İzinsiz Erişim (Unauthorized Access): Bir kişinin yetkisi olmadığı halde kullanıcı hesabı, sunucu, veri tabanı veya ağ sistemlerine giriş yapmasıdır. Bu durum her zaman dış kaynaklı bir hacker saldırısı olmayabilir; içeriden bir kullanıcı tarafından da gerçekleştirilebilir.

DDoS ve Fidye Yazılımı (Ransomware) Girişimleri: Bir yandan kurumun hizmetleri DDoS saldırısıyla durdurulurken diğer yandan sistemlere zararlı yazılım bulaştırılarak verilerin şifrelenmesi veya fidye talep edilmesi amaçlanabilir. Günümüzde birçok saldırı grubu bu iki yöntemi birlikte kullanmaktadır.

Sosyal Medya Hesaplarının Ele Geçirilmesi (Account Takeover): Kuruma veya kişiye ait Facebook, Instagram, X, LinkedIn gibi hesapların şifrelerinin ele geçirilmesi ya da oturum bilgilerinin çalınması sonucu hesabın saldırganın kontrolüne geçmesidir. Genellikle oltalama (phishing), zararlı yazılım veya şifre sızıntıları sonucu gerçekleşir.

Çalışma İzinleri Portalına Saldırı: Kamuya açık bir web uygulamasını hedef alan saldırıdır. Amaç sisteme yetkisiz erişim sağlamak, hizmeti durdurmak veya veri elde etmektir. Böyle saldırılarda SQL Injection, Brute Force, DDoS veya Web Application Attack yöntemleri kullanılabilir.

Veri Sızıntısı (Data Breach): Kuruma ait kişisel verilerin, müşteri bilgilerinin veya gizli belgelerin yetkisiz kişiler tarafından ele geçirilmesi ve internette, özellikle Dark Web üzerinde paylaşılmasıdır. Veri sızıntısı her zaman sistemin hacklenmesi sonucu olmayabilir; yanlış yapılandırma veya içeriden veri çıkarılması nedeniyle de oluşabilir.

Hesap Ele Geçirme (Account Compromise): Bir kullanıcının dijital hesabının şifre, oturum belirteci (session token) veya kimlik doğrulama bilgilerinin çalınarak saldırganın kontrolüne geçmesidir. Sosyal medya hesapları bunun en yaygın örneklerindendir.

Bilgi Sistemlerine Sızma (System Intrusion): Kurumun ağ altyapısına veya sunucularına güvenlik açıklarından yararlanılarak yetkisiz erişim sağlanmasıdır. Saldırgan, sistem içinde kalıcılık sağlayabilir, veri toplayabilir veya başka sistemlere geçiş yapabilir.

Jackpot Manipülasyonu: Özellikle casino sektöründe elektronik oyun makineleri veya merkezi oyun yönetim sistemlerine müdahale edilerek haksız kazanç elde edilmesini amaçlayan saldırıdır. Yazılım manipülasyonu, ağ erişimi veya içeriden destek ile gerçekleştirilebilir. Bu, finansal kazanç odaklı özel bir siber suç türüdür.

Bu saldırılar hangi amaçlarla yapılır?

Genel olarak tablodaki olaylar beş ana kategoriye ayrılabilir:

Amaç	Örnek Saldırılar
Hizmeti durdurmak	DDoS, Web Sitesi Saldırıları
Veri çalmak	Veri Sızıntısı, Bilgi Sistemlerine Sızma, Yetkisiz Erişim
Para kazanmak	Fidye Yazılımı, Jackpot Manipülasyonu
Hesap ele geçirmek	Sosyal Medya Hesabı Ele Geçirme, Account Takeover
İstihbarat veya casusluk yapmak	Uzun süre fark edilmeden sistem içinde kalınarak veri toplama (Advanced Persistent Threat - APT)

KKTC'de en sık görülen saldırı türleri

Son üç yıldaki kamuya yansıyan olaylara bakıldığında en yaygın saldırı türleri şunlardır:

1. **DDoS (Hizmet Engelleme) saldırıları**
2. **Yetkisiz erişim girişimleri**
3. **Kamu kurumlarına yönelik web uygulaması saldırıları**
4. **Sosyal medya hesaplarının ele geçirilmesi**
5. **Veri sızıntıları**
6. **Fidye yazılımı girişimleri**
7. **Finansal kazanç amaçlı casino sistemlerine yönelik saldırılar**

Bu sınıflandırma, olayları hem teknik hem de operasyonel açıdan anlamlandırmak için kullanılabilir. Özellikle kamu kurumları için, saldırı türüne göre alınacak önlemler (örneğin DDoS koruması, çok faktörlü kimlik doğrulama, ağ segmentasyonu veya yedekleme politikaları) farklılık gösterir.

Nasıl Korunmalı?

Siber saldırılardan korunma yalnızca kurumların değil, bireysel kullanıcıların da sorumluluğundadır. Çünkü birçok saldırı, doğrudan kurumu hedef almak yerine **kullanıcının hesabını ele geçirerek** başlar. Bu nedenle alınacak önlemleri **kurumsal** ve **bireysel** olmak üzere iki başlıkta değerlendirmek daha doğru olacaktır.

Peki bu saldırılar karşısında veya saldırı olmadan ne yapmalıyız? Korunabilirmiyiz?

Evet Saldırıların etkisini azaltabiliriz. Peki ne yapmalıyız?

Kurumlar İçin Alınması Gereken Önlemler

Saldırı Türü	Alınması Gereken Önlemler
DDoS Saldırıları	DDoS koruma hizmetleri kullanmak, yük dengeleme (Load Balancer), CDN ve güvenlik duvarı (Firewall) çözümleri uygulamak.
Veri Sızıntıları	Verileri şifrelemek, erişim yetkilerini sınırlandırmak, düzenli güvenlik denetimleri yapmak ve veri kaybı önleme (DLP) sistemleri kullanmak.
Yetkisiz Erişim	Çok faktörlü kimlik doğrulama (MFA), güçlü parola politikaları ve düzenli kullanıcı hesap denetimleri uygulamak.
Web Uygulaması Saldırıları	Web Application Firewall (WAF) kullanmak, güvenlik testleri (Penetrasyon Testi) yaptırmak ve yazılımları sürekli güncel tutmak.
Fidye Yazılımı	Günlük yedekleme yapmak, yedekleri çevrimdışı saklamak, EDR/XDR çözümleri kullanmak ve çalışanları bilinçlendirmek.
Sosyal Medya Hesaplarının Ele Geçirilmesi	MFA etkinleştirmek, kurumsal hesapları merkezi olarak yönetmek ve yalnızca yetkili kişilere erişim vermek.
İç Tehditler	Yetki matrisi oluşturmak, log kayıtlarını düzenli incelemek ve görev ayrılığı (Segregation of Duties) uygulamak.

Normal Bir Kullanıcı Ne Yapmalı?

Aslında birçok büyük saldırının başlangıç noktası **tek bir kullanıcının yaptığı hata** olabilir. Bu nedenle aşağıdaki önlemler günlük yaşam için oldukça önemlidir.

Güçlü ve Benzersiz Parola Kullanın

- Her hesap için farklı parola oluşturun.
- Aynı parolayı e-posta, banka ve sosyal medya hesaplarında kullanmayın.
- En az **12–16 karakter** uzunluğunda parola tercih edin.

Örnek

❌ Ahmet123
❌ Kibris2025
✅ K!br!s_2026@Teknoloji

Çok Faktörlü Kimlik Doğrulamayı (MFA) Açın

Şifreniz çalınsa bile telefonunuza gelen doğrulama kodu olmadan hesabınıza giriş yapılamaz.
Özellikle;

- e-Devlet
- E-posta
- Banka
- Facebook
- Instagram
- WhatsApp
- Google
- Microsoft

hesaplarında mutlaka aktif olmalıdır.

Şüpheli Linklere Tıklamayın

Size gelen;

- SMS
- WhatsApp
- Messenger
- Instagram
- E-posta

mesajlarındaki bağlantıları doğrulamadan açmayın.
Örneğin;
"Kargonuz teslim edilemedi."
"Banka hesabınız bloke edildi."
"Şifrenizi hemen yenileyin."
şeklindeki mesajların büyük bölümü **oltalama (Phishing)** saldırısıdır.

Bilgisayar ve Telefonunuzu Güncel Tutun

Saldırganlar genellikle eski yazılımlardaki güvenlik açıklarını kullanır.
Mutlaka güncel tutun:

- Windows
- Android
- iPhone (iOS)
- Tarayıcılar
- Antivirüs
- Office yazılımları

Ücretsiz Wi-Fi Ağlarına Dikkat Edin

Kafe, otel veya havaalanı gibi ortak ağlarda;

- internet bankacılığı,
- e-posta yönetimi,
- kurumsal sistemlere giriş

mümkün olduğunca yapılmamalıdır.
Gerekirse VPN kullanılmalıdır.

Antivirüs Tek Başına Yeterli Değildir

Modern saldırıların çoğu;

- kullanıcıyı kandırarak,
- sahte web siteleri oluşturarak,
- sosyal mühendislik yöntemleriyle

gerçekleşmektedir.
Bu nedenle en önemli güvenlik unsuru **kullanıcının farkındalığıdır.**

Düzenli Yedekleme Yapın

Belgelerinizi;

- harici disk,
- NAS,
- güvenilir bulut hizmetleri

üzerinde düzenli olarak yedekleyin.
Fidye yazılımı saldırılarında en büyük kurtarıcı yedeklerdir.

Sosyal Medyada Fazla Bilgi Paylaşmayın

Doğum tarihi
telefon numarası
kimlik bilgileri
adres
tatil planları
gibi bilgiler saldırganların sizi hedef almasını kolaylaştırabilir.

Bankadan Gelen Mesajlara Karşı Dikkatli Olun

Hiçbir banka;

- SMS ile şifre istemez.
- Telefonla kart şifresi istemez.
- WhatsApp üzerinden işlem yaptırmaz.

Şüphe duyduğunuzda bankayı **resmî telefon numarasından siz arayın.**

Düzenli Olarak Hesaplarınızı Kontrol Edin

Kontrol edilmesi gerekenler:

- Banka hesap hareketleri
- E-posta giriş geçmişi
- Google hesabı cihaz listesi
- Facebook oturumları
- Instagram girişleri

Tanımadığınız bir cihaz görürseniz hemen çıkış yaptırın ve şifrenizi değiştirin.

KKTC'de Kullanıcıların En Sık Karşılaştığı Siber Tehditler

Son yıllarda kamuoyuna yansıyan olaylar dikkate alındığında bireysel kullanıcılar için en yaygın tehditler şunlardır:

Tehdit	Risk Düzeyi	Korunma Yöntemi
Sahte banka SMS ve e-postaları (Phishing)	Çok yüksek	Linke tıklamamak, bankanın resmî uygulamasını kullanmak
WhatsApp hesabının ele geçirilmesi	Çok yüksek	Doğrulama kodunu kimseyle paylaşmamak, iki adımlı doğrulamayı açmak
Facebook ve Instagram hesaplarının çalınması	Çok yüksek	MFA kullanmak, güçlü ve benzersiz parola oluşturmak
Veri sızıntıları nedeniyle şifrelerin ifşa olması	Yüksek	Her hesapta farklı parola kullanmak ve şüpheli durumlarda parolaları değiştirmek
Sahte yatırım ve kripto dolandırıcılıkları	Yüksek	Lisanssız platformlardan uzak durmak, doğrulanmamış vaatlere inanmamak
Fidye yazılımı	Orta	Güncel yazılım kullanmak ve düzenli yedek almak

Sonuç

Siber güvenlikte en zayıf halka çoğu zaman teknoloji değil, **insan faktörüdür**. Kurumlar güçlü teknik önlemler alsa bile, tek bir zayıf parola, doğrulama kodunun paylaşılması veya sahte bir bağlantıya tıklanması ciddi veri kayıplarına yol açabilir. Buna karşılık; güçlü parolalar, çok faktörlü kimlik doğrulama, düzenli güncellemeler, yedekleme alışkanlığı ve bilinçli internet kullanımı hem bireylerin hem de kurumların maruz kalabileceği siber riskleri önemli ölçüde azaltır.

Ahmet HIZLI
Bilgisayar Mühendisi (M.Sc.)

KAMUSAL SAĞLIĞIN SİBER GÜVENLİKLE İMTİHANI

Sağlık Kurumları Neden Hedef?
Sağlık kurumları, İnsanlarla ilgili özel, gizli kalması gereken ve çok önemli bilgileri tutup işlemler yaptıklarından dolayı genellikle siber tehdit aktörleri tarafından en çok siber saldırıya uğrayan kurumlardandır. Ayrıca hastanelerin sağlık hizmeti verdikleri özel cihazların hacklenmesiyle hizmet verilen hasta öldürülebilir. Bundan 5 veya 6 sene önce yani pandemi döneminde İngilteredeki bir hastanede tedavi görmekte olan bir insanın bağlı olduğu sağlık cihazı hacklenmiş ve hastane personelinden çok yüklü miktarda fidye istenmişti, hasta kurtarılmaya çalışıldı fakat uzun süre cihazdan destek alamadığı için hayatını kaybetti ve tarihe siber saldırıyla hastanede hayatını kaybeden ilk insan olarak geçti. Dolayısıyla hastaneler v.b. sağlık kurumları uyguladığı hizmetler ve depolayarak kullandıkları kritik hasta verilerinden dolayı her zaman siber saldırılara uğrayan, hasta verileri gerek ilaç şirketlerine satılan, gerek siber suçlarda sahte saldırgan profili yaratılmak suretiyle kullanılan gerekse de dolandırıcılıklar için kullanılan ve siber suçlular için çok çeşitli alanlarda çok karlı olup bu tür kötü niyetli avantajlar elde etmek amacıyla çok sık hedef olan çok kritik kurumlardır. Bu nedenle:

- **Devlet destekli APT grupları** – Siber savaşta sağlığı çökerterek karşı taraf üzerinde stratejik ve psikolojik üstünlük sağlamak için.
- **Siber suç örgütleri** – Fidye, sahte kriminal kimlikler yaratıp kendilerini gizlemek ve finansal kazanç elde etmek için.
- **Bireysel hackerlar** – Ego tatmini veya kendini kanıtlama amacıyla.

Motivasyon farklı olsa da sonuç aynıdır: psikolojik yıkım, sağlığı çökertmek ve toplumsal etki yaratarak istediği ve beklediği etkiyi oluşturmaya çalışmak.

1. Pandemi Döneminde Yaşanan Fiziksel Sosyal Mühendislik Saldırısı:
Hatırlarsanız pandemi döneminde bir kişi en az 4 veya 6 aydır hastanenin her yerine girip çıkmış, sağlık ve diğer hastane personeliyle içli dışlı olmuş ve sonradan bu kişinin herkese söylediği gibi aslında hastanenin IT departmanında çalışmadığı hatta hastanenin personeli olmadığı ortaya çıkartılmış ve tutuklanmıştı. Fakat bu ortaya çıkarılana kadar hastanenin girmediği bölümü kalmadığı için muhtemelen çok sayıda önemli bilgiyi toplamış olduğunu değerlendirmeliyiz. Bunun nedenleri:
Yakalanana kadar IT Departmanı dahil her departmanda çok zaman geçirme imkanı bulması – Bu durum her türlü bilgiye ve veriye erişme imkanı sağlar. Örneğin; Kullanılan IT sisteminin özellikleri; Hangi veri tabanı ve işletim sistemleri kullanılıyor? Bunlara girilen ve işlenen veriler, diğer departmanlardaki veriler, hastane personeliyle ilgili bilgiler v.s.
Bu şekilde başarılı olan bir sosyal mühendislik saldırısı başka şekillerde de gerçekleşebilirdi. Örneğin; Kurye Numarası, Hasta Yakını Numarası, Yeni görevlendirilmiş özel güvenlik personeli numarası veya hastane personeline sosyal medya, SMS, arama veya e-posta hesapları üzerinden yapılmaya çalışılacak diğer sosyal mühendislik teknikleri.

Bu nedenle bu ve benzeri durumlarda personel gibi davranılıyorsa mutlaka kamu personelinin ve özellikle hastane personelinin bilgilerinin olması gereken kurumlardan doğrulanmaya çalışılması, kurye gibi davranılıyorsa askeri birliklerdeki nizamiye modeli gibi giriş kısmında durdurularak ilgili departmanın öğrenmeye çalışılması yani mesela kime getirdin bu yemeği? Söylenmedi derse hangi departman veya bölüme getirdin? Söylenmedi derse ne getirdin? Bakmadım derse o zaman geri git öğren ve gel gibi karşılıklar verilerek bu potansiyelin önüne geçilebilir. Yeni görevlendirilmiş özel güvenlik görevlisi gibi davranılıyorsa zaten ilgili özel güvenlik personelleri en başta şüphelenmeli ve amirlerine bunu doğrulatmalıdırlar.

Doğrulanmamışsa da hastane polisiyle iş birliği içinde en uygun an ve zamanda kişiyi etkisiz hale getirmelidirler. Eğer hasta yakını ve dolayısıyla da refakatçisi gibi davranılarak sızılmaya çalışıldığına şüpheleniliyorsa hastaya sorularak doğrulatma yapılabilinir. Örneğin X Hanım veya Y Bey sizin şuyunuz veya buyunuzmuş doğru mudur? Eğer olumsuz geri dönüş alınırsa derhal hastanedeki güvenlik görevlileriyle temas sağlanıp şahıslar etkisiz hale getirilir. Siber dünyadan hastane personeline yönelik olarak gerçekleştirilebilecek tüm sosyal mühendislik ve siber saldırılar içinse tüm hastane personeline belirli aralıklarla Siber güvenlik farkındalık eğitimleriyle, sosyal mühendislik farkındalık eğitimleri, bilgi güvenliği eğitimleri, dijital medya okur yazarlığı eğitimleri verilmesi ve hastanenin bünyesinde mor takım siber güvenlik ekipleri oluşturularak, hastanenin geneli için siber güvenlik ve bilgi güvenliği politikalarının oluşturulmasıyla felaket kurtarma planlarının hazırlanıp uygulanması ve tüm bu politikalar, planlar ve eğitimlerin gerektikçe güncellenmesi kritik öneme sahiptir.

Saldırıyı Nasıl Fark Ederiz?
Bir saldırı gerçekleştiğinde erken tespit hayati önem taşır. Dikkat edilmesi gereken işaretler:

- Anormal Davranışlar – Genellikle ilk kez hastaneye adım atmasına rağmen sanki de çok önceden personelle tanışıyormuş ve hastane ekibinin bir parçasıymış gibi davranılmaya çalışılır (IT veya herhangi bir hastane bölümünün yeni personeliymiş rolü) ve direkt olarak her türlü bilgiyi elde etmeye çalışırlar. Normalde bir kişi yeni personel olduğu bir yerde önce bölüm olarak arkadaşlarıyla tanışıp kaynaşır daha sonra diğer departmanlardan kişilerle iletişim kurar ve genelde işi kendi departmanıyla alakalı olarak öğrenmeye başlar zaman geçtik sonra denk geldikçe diğer departmanlardan biraz biraz bilgi öğrenir. Ne hemen herkesle sarmaş dolaş olur ne de kendi departmanıyla ilgili olsun olmasın hemen her bilgiyi elde etmeye çalışır. Eğer bunları yapıyorsa sıkıntı var demektir.
- Herkesin her şeyini bilip öğrenmeye çalışır ama kendiyle ilgili ya hiçbir şey söylemez yada yalan söyler – Bu kişiler genellikle yukarıda da değindiğimiz gibi mümkün olan her şeyi öğrenmeye çalışırlar fakat kendileriyle ilgili ya doğru dürüst bilgi vermezler ya da kendileriyle ilgili hiçbir şey söylemezler.
- Hemen Her Departmana veya Bölüme Erişme Çabası – Kendisiyle veya işiyle alakası vardır veya yoktur amaç bilgi hırsızlığı olduğu için mümkün olan her yere mutlaka erişmeye/girmeye çalışırlar.

Çelişkili Cevaplar – Bazen eğer şansınız yaver gider ve acemisine denk gelirseniz sıkıştırdığınız anda stres ve paniğe kapılarak çelişkili cevaplar vererek kendisini ele verebilir veya çok panik ve stres olmuşsa suçunu itiraf da edebilir.

2. 22 Temmuz 2026 Tarihinde Duyurulan 364 Bin Kişinin Sağlık Bakanlığındaki Verilerinin Çalınması:
Başta söyleyeyim ben yaptığım OSINT taramasında henüz böyle bir bilgiye ulaşamadım. Benim ulaştığım bir yerde son olarak şu

ana kadar personel bilgisi hariç 733 kişinin bilgilerinin sağlık bakanlığının sisteminden dark web e sızdırıldığı sonucu var. Dolayısıyla önce bu 733 kişiyle ilgili bir bilgilendirme yazmak zorundayım;

- Eğer sürekli hiç temas kurmamanıza ve bilgi vermemenize rağmen ilaç firmaları veya ilaç firmalarından olduklarını söyleyenler tarafından; Arama, SMS, e-posta ve Sosyal Medya yoluyla v.s. sürekli rahatsız ediliyorsanız; AB vatandaşlığınızın da olması halinde AB Makamlarına, olmaması halinde KVKK ve Mahkemeler başta olmak üzere gidebileceğiniz tüm mercilere gidip şikayetçi olun ve bu kişilerle firmaları engelleyin
- Sosyal Medyadaki bilgilerinizi kısıtlayın. Örneğin gerçek ad ve soyadınız varsa mutlaka birini uydurma yapın, tüm gerçek aile bilgilerinizi eğer girme hatası yapmışsanız kaldırın, hobileriniz v.s. gibi sizin kişisel ve karakteristik özelliklerinizi belirten her şeyi kaldırın ve her şeyinizi değil çok az şeyi ki onlarda mümkünse sizi ele vermeyecek bilgiler olsun paylaşın sadece.
- Ve tüm dolandırıcılıklara yani dolandırıcılık girişimlerine karşı hazırlıklı olun.

Not: 733 kişinin kim olduğu bilinmediğinden dolayı aslında herkesin kendini sanki bu 733 kişiden biriymiş gibi düşünerek yukarıda sıraladığım tedbirlerle önlemleri almasını rica ediyorum.

Ve şimdi sağlık bakanlığımız için gerekenleri belirtiyorum:

Saldırıyı Nasıl Fark Ederiz?

Bir saldırı gerçekleştiğinde erken tespit hayati önem taşır. Dikkat edilmesi gereken işaretler:

- Anormal Trafik Akışları – Sisteminizde kontrolünüz dışında gerçekleşen olağan dışı istekler ve bağlantılar.
- Wireshark ile Log Analizi – Paket içeriklerini inceleyerek normalde yalnızca iç ağla iletişim kurması gereken servislerin dış ağla haberleştiğini görebilirsiniz.
- Komut Satırı Kontrolleri (netstat -abno) – TCP/UDP servislerinin kimlerle konuştuğunu ve bağlantı durumlarını görüntüleyebilirsiniz.
- Hizmet Aksaması – Kurum personeli dışında birilerinin yetkisiz işlemleri doğrudan hizmet kesintisine yol açabilir.

Siber Saldırılardan Korunma Yöntemleri

Sağlık bakanlığının bu tür saldırılara karşı alabileceği önlemler:

- Zero Trust Network Access (ZTNA) – Her erişimi sürekli doğrulamak ve minimum yetkiyle çalıştırmak.
- Veri tabanı ve Kritik IT Sistemlerini VLAN'larla İzole Etmek – İç ağda olmanın tek başına erişim hakkı vermemesini sağlamak.
- UEBA, EDR, SIEM, SOAR, MDM – Güvenlik çözümlerini doğru şekilde yapılandırmak.
- Segmentasyon ve Port Yönetimi – Gereksiz servisleri kapatmak, gerekli olanları güncel sürümlerle çalıştırmak.
- Farkındalık Eğitimleri ve Tatbikatlar – Oltalama saldırısı simülasyonları, Felaket Kurtarma ve Olay Müdahale tatbikatları ve Siber Güvenlik Farkındalık Eğitimleri.
- Kurumsal Politikalar – Siber güvenlik, Felaket Kurtarma ve Olay Müdahale Planı, Siber Tehdit İstihbaratı ve Bilgi Güvenliği Politikalarının yazılı hale getirilmesi.
- Mor Takım + SOC Yaklaşımı – Ofansif ve defansif güvenlik uzmanlarının dönüşümlü çalıştığı hibrit ekipler ve bunları destekleyen bir SOC kurmak.

Sonuç

Sağlık Bakanlığının yaşadığı bu iki saldırı örneği, sağlık bakanlığıyla kurumlarının siber saldırılara karşı ne kadar kırılgan olduğunu bir kez daha göstermektedir. Özellikle özel hasta gruplarıyla normal hastaların bilgileri gibi hassas ve gizli tutulması gereken bilgilerle kritik sistemlerin güvenliği, yalnızca teknik bir gereklilik değil, toplumsal güvenliğin teminatıdır. Dünya standartlarında güvenlik için kurumların hem teknolojik çözümleri hem de insan faktörünü kapsayan bütüncül bir yaklaşım benimsemesi şarttır.

Cem GÖKDEL
Siber Güvenlk Uzmanı(Etk/Beyaz Şapkalı Hacker)

YAPAY ZEKAYLA ÜRETMEK: ORTAK MI, YOKSA TAKLİTÇİ Mİ?

Teknoloji hayal gücümüzü besliyor mu, yoksa özgünlüğümüzü mü evcilleştiriyor?

Günümüzde komutlar (promptlar) yazarak saniyeler içinde binlerce kelimelik metinler, etkileyici görseller ve kusursuz melodiler üretebildiğimiz bir dijital çağdayız. Yapay zekâ (YZ) araçları artık günlük üretimimizin vazgeçilmez bir parçası haline geldi. İnsanlar her an yeni fikirler paylaşabilir ve algoritmaların gücüyle saniyeler içinde sanatsal çıktılar üretebilir. Ancak ekran başında yapay zekâyla kurduğumuz bu üretim profesyonelleşirken, zihnin derinliklerindeki özgün ve sancılı yaratıcılık azalıyor mu?

Son yıllarda yapılan deneysel araştırmalar, üretken yapay zekâ araçlarının yaygın kullanımının bireylerin yaratıcı öz-yeterlik algısı ve odaklanma biçimleri üzerinde çeşitli etkiler yaratabileceğini göstermektedir. Yapay zekâ destekli üretim süreçleri hız kazanırken, bazı kullanıcılar hazır şablonlara yönelme eğilimi gösterebilmekte; bu durum ise zamanla ortaya çıkan ürüne karşı yabancılaşma ve tatminsizlik hissini artırabilmektedir.

1.ALGORİTMİK YARATICILIK NEDİR?

Algoritmik yaratıcılık,

Sürekli komut üretmek ve hazır şablonlara güvenmek, zamanla zihnimizin benzersiz hata yapma ve bu hatalardan yepyeni sanatsal akımlar doğurma becerisini yüzeysel bir kusursuzluğa feda edebilir.

Promptlar artıyor, fakat üzerine günlerce düşünülen o ham fikirlerin sayısı azalabiliyor.

1.1. Algoritmik Üretimin Sonuçları

- **Zihinsel Etkiler:** Üretim sürecinde zihinsel tembellik ve "kolay çözüme yönelme" alışkanlığının artması,
- **Bilişsel Riskler:** Özgünlük kaybı, birbirine benzeyen ("YZ kokan") içeriklerin yaygınlaşması,
- **Fizyolojik Etkiler:** Ekran başında geçirilen sürenin uzamasına bağlı olarak odaklanma ve dikkat dağınıklığı,
- **Kültürel Etkiler:** İnsan emeğinin estetik değerinin sorgulanması ve sanatsal bağların mekanikleşmesi olarak sıralanabilir.

Yapay zekâ artık sadece bir kod bloğu veya hesaplama aracı değil; günlük düşünce ve üretim süreçlerimizin tam merkezinde duran bir "ortak".

İnsanlar günün büyük bölümünü bu yapay zekâlı asistanlarla geçirirken, zihnin kendi kendine kaldığı o "can sıkıntısından beslenen" yaratıcı anlar giderek daha sınırlı hâle geliyor. Özellikle yeni nesil tasarımcılar ve yazarlar için yapay zekâyı kullanmak bir tercih değil, çağın doğal bir gerekliliğidir. Ancak bu sürekli destek hali, bireylerin kendi potansiyellerini keşfetme sürecinde zihinsel yorgunluk ve taklitçi bir his yaratabiliyor. Teknoloji üretkenliği artırırken, yaratıcılığın doğasını sessizce değiştiriyor.

Bu noktada önemli olan algoritmaları reddetmek değil; yapay zekâ ile insan zihninin özgün kıvılcımı arasında sağlıklı bir denge kurabilmektir.

2. BAĞIMLILIK NEDEN ARTIYOR?

Kusursuzluğa Kolay Erişim: İnsan eliyle günlerce sürecek bir görseli veya metni saniyeler içinde alabiliyor olmak, bizi üretimin o zahmetli ama öğretici sürecinden uzaklaştırıyor.

Zaman Baskısı ve Hız Yarışı: Modern dünyanın yüksek temposu ve dijital platformların sürekli içerik talep etmesi, insanları derin düşünmek yerine yapay zekânın hızına sığınmaya zorluyor,

Dijital Estetik Standartları: Algoritmaların yaygınlaştırdığı "mükemmel" estetik kalıplar, insanların kusurlu olsa da karakterli tarzlarını yetersiz veya eksik hissetmesine yol açabiliyor,

Hızlı Tüketim Çılgınlığı: Çabuk üretilen içerikler, anlık memnuniyet sağlasa da zamanla üreticinin kendi becerilerinden uzaklaşmasına yol açabilir.

"Milyonlarca parametreye sahip modellerle üretiyoruz ama kendi zihnimizin benzersiz derinliğinde bazen hiç olmadığımız kadar kısır kalabiliyoruz."

3. GÜNCEL ARAŞTIRMALAR NE SÖYLÜYOR?

Yayımlanan uluslararası araştırmalar, üretken yapay zekânın iş yaşamında hızla yaygınlaştığını göstermektedir. Özellikle yazılım, tasarım ve içerik üretimi gibi bilgi yoğun sektörlerde yapay zekâ araçları günlük iş akışlarının önemli bir parçası hâline gelmiştir. Araştırmalar, bu araçların rutin görevlerde zaman tasarrufu sağladığını; buna karşılık yapay zekâ tarafından üretilen içeriklerin doğrulanması ve düzenlenmesi için çalışanların ek zaman ayırdığını ortaya koymaktadır. Tablo 1 güncel araştırmalardan öne çıkan bazı bulguları özetlemektedir.

Tablo1. Yapay Zekâ Kullanımında Öne Çıkan Göstergeler

Gösterge	Bulgular
AI kullanan çalışan oranı	%50
Düzenli kullanım	%28
Yıllık zaman tasarrufu	122 saat
AI doğrulama süresi	6,4 saat/hafta
E-posta zaman kazancı	3 saat/hafta

4. YARATICILIĞIMIZI KORUMAK İÇİN NE YAPABİLİRİZ?

Önce Kendi Zihninizi Karalayın: Bir projeye başlarken yapay zekayı açmadan önce, en az 30 dakika boyunca yalnızca kalem ve kağıtla kendi fikirlerinizi ve taslaklarınızı oluşturun.

Yapay zekâyı "asistan" olarak konumlandırın: Onun sizin yerinize düşünmesine izin vermeyin; onu yalnızca fikrinizi cilalamak, araştırma yapmak veya ham işleri otomatikleştirmek için kullanın.

Hataların Estetiğine İnanın: Kusursuz yapay zekâ çıktılarının yanında, insan elinden çıkmış o benzersiz, asimetrik ve samimi hataların sanatsal değerini koruyun ve parlatın.

Analog Molalar Verin: Dijital araçlardan tamamen uzaklaştığınız, zihnin kendi kendine kalıp sıkılmasına izin verdiğiniz yaratıcı kuluçka dönemleri oluşturun.

Ustalık Becerilerinizi Geliştirin: Temel zanaatınızı (çizmeyi, yazmayı, kodlamayı) yapay zekâ olmadan da yapabilecek kas hafızanızı ve teorik bilgiyi sürekli taze tutun.

"Gerçek yaratıcılık, prompt satırının bittiği yerde başlar"

KAYNAKLAR

1. Davenport, T. H., & Mittal, N. (2022). How generative AI is changing creative work. Harvard Business Review. https://hbr.org/2022/11/how-generative-ai-is-changing-creative-work
2. Stanford Institute for Human-Centered Artificial Intelligence (HAI). (2026). Artificial Intelligence Index Report 2026. Stanford University. https://hai.stanford.edu/assets/files/ai_index_report_2026.pdf
3. Brynjolfsson, E., Bick, R., & Hartley, J. (2026). What is Generative AI Worth? Evidence on Adoption and Consumer Surplus. Stanford Digital Economy Lab.
4. Brynjolfsson, E., Bick, R., & Hartley, J. (2026). What is Generative AI Worth? Evidence on Adoption and Consumer Surplus. Stanford Digital Economy Lab.
5. Hou, J., & Chen, Y. (2024). The Double-Edged Roles of Generative AI in the Creative Process: Experiments on Design Work. Information Systems Research, 35(4). https://doi.org/10.1287/isre.2024.0937
6. Google. (2025). *AI Works Pilot: Productivity and AI Adoption in the Workplace.*
7. Dillon, E. W., Jaffe, S., Immorlica, N., & Stanton, C. (2025). *Shifting Work Patterns with Generative AI.* Microsoft Research & Stanford University.

Glean Work AI Institute. (2026). *The Rise of the Botsitters: The Hidden Labor Behind AI Productivity.*

Dr. Eren Küren
Bilgisayar Mühendisi &
Dijital Dönüşüm Uzman

Çocuklara İnternet Erişimini Neden Kısıtlamalıyız?

Dijital çağın getirdiği en büyük paradokslardan biri şudur: İnternet, insanlık tarihinin en güçlü öğrenme aracı olduğu kadar, aynı zamanda en tehlikeli ortamlarından biri haline gelebilmektedir. Özellikle çocuklar söz konusu olduğunda, bu ikilem çok daha keskin bir hal almaktadır. Kısıtlama, yasaklamak anlamına gelmez; bilinçli, denetimli ve yaşa uygun bir erişim düzeni oluşturmak anlamına gelir.

Çocukların beyni, yetişkinlere kıyasla çok daha hızlı etkilenir ve şekillenir. Sınırsız internet kullanımı bu gelişim sürecini ciddi biçimde sekteye uğratabilir. Kısa videolar ve anlık içerikler, çocukların uzun süreli odaklanma kapasitesini zayıflatırken her şeye anında ulaşma alışkanlığı, gecikmeye tahammülü ortadan kaldırmaktadır. Bunun yanı sıra sosyal medya aracılığıyla gelişen karşılaştırma kültürü, çocuklarda yetersizlik duygusu, kaygı ve düşük öz saygıya zemin hazırlamaktadır.

Bu gözlemleri destekleyen bilimsel bulgular son derece çarpıcıdır. San Diego Eyalet Üniversitesi'nden psikolog Jean Twenge'nin 500.000'den fazla ergeni kapsayan araştırması, 2012 yılından itibaren akıllı telefonların yaygınlaşmasıyla eş zamanlı olarak ergen depresyonu ve yalnızlık oranlarının belirgin biçimde arttığını ortaya koymaktadır. Harvard Tıp Fakültesi'nin uyku araştırmaları ise ekranlardan yayılan mavi ışığın melatonin üretimini baskıladığını ve çocukların uyku döngüsünü doğrudan bozduğunu göstermektedir. Dünya genelinde yapılan güncel araştırmalar da 8-12 yaş arasındaki çocukların günde ortalama dört ila altı saat ekran başında geçirdiğini; bunun önerilen sınırın iki ila üç katına ulaştığını tespit etmektedir.

İnternet, her yaştan kullanıcıya hitap eden içerikler barındırmaktadır; ancak bu içeriklerin büyük bir kısmı çocuklar için son derece uygunsuz olabilir. Şiddet ve korku içeren görüntüler, yetişkinlere yönelik

içerikler, nefret söylemi ve öz zarara teşvik eden topluluklar, bir çocuğun yalnızca yanlış bir arama kelimesiyle karşılaşabileceği tehlikeler arasındadır. Bu durum, denetimsiz internet kullanımının ne denli ciddi sonuçlar doğurabileceğini gözler önüne sermektedir.

Kötü niyetli kişiler, çocukların saflığından ve güvene olan eğiliminden yararlanmaktadır. Oyun platformları veya sosyal medya üzerinden kurulan iletişimler zaman zaman manipülasyon ve istismara dönüşebilmektedir. Siber zorbalık ise yaşıtlar tarafından uygulanan dijital baskıyla ağır psikolojik izler bırakabilmektedir. Tüm bunlara ek olarak, çocuklar sahte kampanya ve ödül mesajlarına kolayca kanarak kimlik avı dolandırıcılığının hedefi haline gelebilmektedir.

Ψ

Dijital bağımlılık da göz ardı edilemeyecek bir sorundur. Araştırmalar, aşırı ekran süresinin uyku kalitesini düşürdüğünü, fiziksel aktiviteyi azalttığını, sosyal becerileri zayıflattığını ve akademik performansı olumsuz etkilediğini ortaya koymaktadır. Özellikle yatmadan önce yapılan internet kullanımı, çocukların hem bedensel hem de zihinsel dinlenmesini engellemektedir.

Bu risklere karşı atılabilecek en somut adımlardan biri günlük ekran sürelerini yaşa göre düzenlemektir. Uzmanlar ve sağlık kuruluşları bu konuda net öneriler sunmaktadır. Amerikan Pediatri Akademisi ve Dünya Sağlık Örgütü'nün rehberlerine göre 0-2 yaş arasındaki bebekler için ekran süresi neredeyse tamamen kısıtlanmalıdır; bu dönemde beyin gelişimi fiziksel dokunuş, yüz yüze iletişim ve gerçek dünya deneyimlerine ihtiyaç duymaktadır. 2-5 yaş arasındaki çocuklar için günlük en fazla bir saat önerilmekte, ancak bu sürenin eğitici içeriklerle ve ebeveyn eşliğinde geçirilmesi vurgulanmaktadır. 6-12 yaş grubunda ise günde iki saati aşmamak temel kural olmakla birlikte asıl önemli olan ekranın uyku, ödev ve sosyal etkileşimin önüne geçmemesidir. 13-18 yaş arasındaki ergenlerde ekran süresini salt rakamlarla ölçmek güçleşmektedir; bu nedenle toplam süreyi kısıtlamaktan çok içeriği denetlemek, gece 22.00 ile sabah 07.00 arasında cihazları yatak odasından uzak tutmak ve düzenli fiziksel aktiviteyi günlük rutinin parçası haline getirmek önerilmektedir. Tüm yaş grupları için

Ψise yemek masasında ve uyumadan en az bir saat önce ekran kullanımının yasaklanması, ekran süresinin ödül ya da ceza aracı olarak kullanılmaması gibi evrensel kurallar geçerliliğini korumaktadır.

Konunun yalnızca bireysel bir sorumluluk meselesi olmadığını, aynı zamanda yasal ve kurumsal bir çerçeve gerektirdiğini de vurgulamak gerekmektedir. Avrupa Birliği'nin Genel Veri Koruma Tüzüğü olan GDPR, 16 yaşın altındaki çocukların verilerinin işlenmesi için ebeveyn onayı zorunluluğu getirmektedir. Birleşik Krallık ise 2023 yılında yürürlüğe giren Çevrimiçi Güvenlik Yasası ile platformları çocuklara yönelik zararlı içerikleri kaldırmakla yükümlü kılmıştır. Türkiye'de Bilgi Teknolojileri ve İletişim Kurumu bünyesinde işletilen güvenli internet hizmeti, ebeveynlerin çocukları için özel bir filtreleme profili oluşturmasına olanak tanımaktadır. Ne var ki yasal düzenlemeler tek başına yeterli değildir; platform şirketlerinin algoritmik sorumluluğu, içerik moderasyonu ve yaş doğrulama sistemleri konusundaki denetim mekanizmaları hâlâ geliştirilmeye muhtaçtır.

Okulların ve devletin bu süreçteki rolü de göz ardı edilmemelidir. Dijital okuryazarlık eğitiminin yalnızca aile içinde verilmesi beklenmek yerine müfredatın zorunlu bir parçası haline getirilmesi, çocuklar arasındaki fırsat eşitsizliğini de ortadan kaldırabilir. Nitekim Finlandiya ve Estonya gibi ülkeler dijital okuryazarlığı temel eğitim müfredatına entegre ederek bu alanda önemli başarılar elde etmiştir. Öte yandan bazı ülkelerde okullarda sosyal medya kullanımının yasaklanmasına yönelik tartışmalar da giderek yoğunlaşmaktadır; Fransa bu adımı ulusal düzeyde atan ilk ülkeler arasında yer almaktadır.

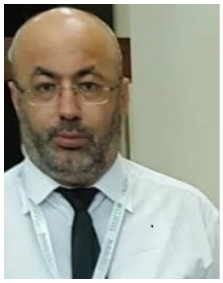
Bu noktada kısıtlamaya yönelik karşı görüşleri de dürüstçe ele almak gerekmektedir. Bazı eğitimciler ve çocuk gelişimi uzmanları, aşırı korumacı bir yaklaşımın çocuğun dijital yetkinliğini ve merakını köreltebileceğini öne sürmektedir. Buna göre teknolojiyle erken ve özgür bir şekilde tanışan çocuklar, gelecekteki iş hayatına daha donanımlı hazırlanmaktadır. Bir diğer karşı argüman ise kısıtlamanın çocuğun bağımsız düşünce gelişimini engelleyebileceği yönündedir. Bu görüşler tamamen geçersiz değildir; ancak söz konusu argümanlar kısıtlamaya değil, kör yasakçılığa karşı çıkmaktadır. Bilinçli ve yaşa uygun bir denetim ile tam serbesti arasındaki fark, çocuğu hem korumak hem de geliştirmek açısından belirleyici olmaktadır.

Soyut önerilerin pratikte nasıl işlediğini somut bir örnekle görmek konuyu daha da aydınlatacaktır. Dokuz yaşındaki bir çocuğun tablet üzerinden sosyal medyaya erişmeye başladığını varsayalım. Denetim yazılımı olmayan bir ortamda bu çocuk kısa sürede yaşına uygun olmayan içeriklerle karşılaşabilir, tanımadığı kişilerle iletişime geçebilir ve giderek artan bir ekran süresiyle uyku düzeni bozulabilir. Öte yandan ebeveyn denetim aracının kurulu olduğu, cihazın yalnızca oturma odasında kullanılabildiği ve akşam 20.00'den sonra otomatik olarak kilitlendiği bir ortamda büyüyen aynı çocuk, interneti keşfetmeye devam ederken bu risklerin büyük bölümünden korunmuş olur. Fark, internetin kendisinde değil; çevresinde kurulan bilinçli yapıdadır.

Sonuç olarak internet erişimini kısıtlamak, çocukları dijital dünyadan tamamen koparmak değil; onları risklere karşı korurken bu dünyanın fırsatlarından sağlıklı biçimde yararlanmalarını sağlamaktır. Bu dengeyi kurmanın en etkili yolu, birbirini tamamlayan birkaç temel yöntemi bir arada uygulamaktır. Ebeveyn denetim yazılımları olan Google Family Link, Apple Screen Time veya Microsoft Family Safety gibi uygulamalar sayesinde hangi içeriklere erişildiği ve ne kadar süre harcandığı doğrudan takip edilebilmektedir. Bilgisayar ve tabletlerin yalnızca ortak alanlarda kullanılması şeffaflığı artırırken çocuğun denetimsiz kalma hissini de ortadan kaldırmaktadır. Dijital okuryazarlık eğitimi ise belki de en kalıcı yöntemdir; çocuğa sadece "bunu yapma" demek yerine sahte haberleri nasıl ayırt edeceğini, kişisel bilgilerini kiminle paylaşmaması gerektiğini ve rahatsız edici bir durumla karşılaştığında ne yapacağını öğretmek onu gerçek anlamda korur. Yemek saatleri ve sabah rutinleri gibi belirli zaman dilimlerini tamamen ekransız ilan etmek de çocuğun zamanla bu boşlukları kitap okuma ve dış mekân aktiviteleriyle doldurmayı öğrenmesine zemin hazırlar. Tüm bu yöntemlerin temeli ise açık ve yargılamayan bir aile içi iletişimdir; çocuk rahatsız edici bir içerikle karşılaştığında bunu ebeveynine söyleyebilecek kadar güvende hissetmiyorsa hiçbir yazılım ya da kural tek başına yeterli olamaz. Teknolojiyi doğru kullanmayı öğrenmek, onu hiç kullanmamaktan çok daha değerlidir; ancak bu öğrenme süreci, bilinçli bir rehberlik olmadan kendiliğinden gerçekleşmez.

Uzm. Psk. Eşmen Tatlıcalı

Yapay Zekâ Çağında Yükseköğretim: Üniversitelerde Eğitim Modellerinin Dönüşümü ve KKTC'nin Geleceğe Hazırlanması



❖ **Giriş: Yeni Bir Eğitim Çağının Başlangıcı**

İnsanlık tarihi incelendiğinde, büyük teknolojik dönüşümlerin yalnızca ekonomik ve toplumsal yapıları değil, eğitim sistemlerini de köklü biçimde değiştirdiği görülmektedir. Matbaanın icadı bilgiye erişimi yaygınlaştırmış, sanayi devrimi modern eğitim kurumlarının ortaya çıkmasına zemin hazırlamış, internet teknolojileri ise öğrenmeyi fiziksel sınırların ötesine taşımıştır. Günümüzde ise yapay zekâ teknolojileri, yükseköğretim sistemlerini yeniden şekillendiren yeni bir dönüşüm dalgasının merkezinde yer almaktadır.

Dünya Ekonomik Forumu'nun yayımladığı Future of Jobs raporlarına göre, yapay zekâ ve dijital dönüşümün etkisiyle önümüzdeki yıllarda iş dünyasında ihtiyaç duyulan beceriler hızla değişecek ve çalışanların önemli bir bölümü yeni yetkinlikler kazanmak zorunda kalacaktır. Bu dönüşüm, yalnızca iş gücü piyasasını değil, bireyleri geleceğe hazırlamakla sorumlu olan yükseköğretim kurumlarını da doğrudan etkilemektedir. Üniversiteler artık sadece bilgi aktaran kurumlar değil; öğrencilerine değişime uyum sağlama, eleştirel düşünme, problem çözme ve yapay zekâ ile birlikte çalışma becerileri kazandıran öğrenme ekosistemleri hâline gelmektedir.

Şekil 1. *Yapay zekâ teknolojileri, üniversitelerin eğitim, araştırma ve yönetim süreçlerini dönüştürerek geleceğin yükseköğretim modelini şekillendirmektedir.*

Son yıllarda özellikle üretken yapay zekâ uygulamalarının yaygınlaşmasıyla birlikte üniversiteler, eğitim anlayışlarını yeniden değerlendirmeye başlamıştır. Çünkü artık bilgiye erişim geçmiş dönemlere kıyasla çok daha kolaydır. Öğrenciler birkaç saniye içerisinde milyonlarca akademik kaynağa ulaşabilmekte, karmaşık sorularına yanıt alabilmekte ve farklı alanlardaki bilgileri karşılaştırabilmektedir

❖ **Bilgi Çağından Yapay Zekâ Çağına Geçiş**

Uzun yıllar boyunca eğitim sistemleri, öğrencilere mümkün olduğunca fazla bilgi kazandırmayı hedeflemiştir. Bilgiye erişimin sınırlı olduğu dönemlerde bu yaklaşım son derece anlamlıydı. Ancak günümüzde bilgi eksikliğinden çok bilgi fazlalığı problemi yaşanmaktadır. Öğrenciler artık ihtiyaç duydukları verilere kolayca ulaşabilmekte, ancak bu bilgileri değerlendirme, doğrulama ve anlamlandırma konusunda yeni becerilere ihtiyaç duymaktadır.

Şekil 2. *Yapay zekâ destekli öğrenme sistemleri, öğrencilerin bireysel ihtiyaçlarına göre şekillenen kişiselleştirilmiş eğitim deneyimleri sunmaktadır.*

❖ **Üniversitelerde Eğitim Modellerinin Değişimi**

Geleneksel eğitim modeli büyük ölçüde öğretim üyesinin merkezde olduğu bir yapıya dayanıyordu. Öğrenciler belirli bir müfredatı takip ediyor, dersleri dinliyor ve sınavlarla değerlendiriliyordu. Ancak günümüz öğrencilerinin beklentileri ve öğrenme alışkanlıkları önemli ölçüde değişmiştir.

Yapay zekâ teknolojilerinin yükselişiyle birlikte eğitim sistemlerinin odağı da değişmektedir. Üniversiteler artık yalnızca bilgi öğretmeye değil; eleştirel düşünme, problem çözme, yaratıcılık, iletişim ve etik karar verme gibi becerileri geliştirmeye yönelmektedir.

Yeni nesil öğrenciler, bilgiye anında ulaşabilmekte ve öğrenme süreçlerinde daha aktif rol almak istemektedir. Bu nedenle üniversitelerde öğrenci merkezli eğitim modelleri giderek yaygınlaşmaktadır.

❖ **Araştırma ve Bilimsel Üretimde Yeni Dönem**

Üniversitelerin temel görevlerinden biri bilimsel bilgi üretmektir. Günümüzde araştırmacılar her yıl yayımlanan milyonlarca akademik çalışma arasında önemli bilgilere ulaşmakta zorlanabilmektedir. Yapay zekâ bu noktada araştırma süreçlerine önemli katkılar sağlamaktadır.

Şekil 3. *Yapay zekâ destekli araştırma araçları, veri analizi ve bilimsel keşif süreçlerinde araştırmacılara önemli avantajlar sağlamaktadır.*

Akademik literatür taramalarının hızlandırılması, büyük veri kümelerinin analiz edilmesi ve araştırma eğilimlerinin belirlenmesi gibi işlemler artık çok daha kısa sürelerde gerçekleştirilebilmektedir.
Bu durum araştırmacıların zamanlarını daha yaratıcı ve yenilikçi çalışmalara ayırabilmelerine olanak sağlamaktadır.

❖ **2035'İN ÜNİVERSİTE ÖĞRENCİSİ**

- Kişisel yapay zekâ destekli öğrenme asistanları kullanacak.
- Ders içeriklerini kendi öğrenme hızına göre kişiselleştirebilecek.
- Fiziksel sınıflar ile sanal öğrenme ortamlarını birlikte deneyimleyecek.
- Sanal ve artırılmış gerçeklik teknolojileriyle laboratuvar uygulamaları gerçekleştirecek.
- Küresel ölçekte farklı ülkelerden öğrencilerle ortak projeler yürütecek.
- Veri okuryazarlığı ve yapay zekâ okuryazarlığı temel beceriler arasında yer alacak.
- Üniversite eğitimi mezuniyetle sınırlı kalmayacak, yaşam boyu öğrenme modeli yaygınlaşacak.

❖ **Akademisyenin Değişen Rolü**

Yapay zekâ teknolojilerinin yaygınlaşmasıyla birlikte sıkça dile getirilen sorulardan biri de akademisyenlerin gelecekteki rolüdür. Bazı çevrelerde yapay zekânın öğretim üyelerinin yerini alacağı yönünde görüşler bulunsa da eğitim süreci yalnızca bilgi aktarımından ibaret değildir.
Bir akademisyen aynı zamanda rehberdir, mentordur, araştırmacıdır ve öğrencilerin düşünsel gelişiminde önemli bir rol üstlenmektedir.

❖ **Yapay Zekâ ve Akademik Etik**

Her teknolojik yenilik gibi yapay zekâ da bazı riskleri beraberinde getirmektedir. Özellikle akademik dürüstlük konusu, yükseköğretim kurumlarının üzerinde durduğu temel başlıklardan biri hâline gelmiştir.
Öğrencilerin yapay zekâ araçlarını bilinçsiz kullanmaları durumunda özgünlük, kaynak gösterme ve intihal gibi konularda çeşitli sorunlar ortaya çıkabilmektedir.

❖ **KKTC Üniversiteleri İçin Yeni Fırsatlar**

Kuzey Kıbrıs Türk Cumhuriyeti, yükseköğretim alanında sahip olduğu uluslararası öğrenci profili ve çok kültürlü yapısıyla dikkat çekmektedir. Farklı ülkelerden gelen öğrencileri bir araya getiren üniversiteler, aslında yapay zekâ çağının gerektirdiği küresel eğitim anlayışına önemli ölçüde sahiptir.
KKTC yükseköğretim sistemi, sahip olduğu uluslararası öğrenci profili ve çok kültürlü eğitim yapısıyla bölgesel ölçekte önemli bir konuma sahiptir. Ülkede faaliyet gösteren üniversiteler, farklı coğrafyalardan gelen öğrencileri aynı akademik ortamda buluştururken dijital dönüşüm ve yapay zekâ uygulamaları açısından da önemli fırsatlar sunmaktadır. Son yıllarda birçok üniversitenin yapay zekâ, veri bilimi, yazılım mühendisliği ve dijital teknolojiler alanlarında yeni programlar açması, bu dönüşümün somut göstergeleri arasında yer almaktadır. Ayrıca TEKNOFEST'in KKTC'de düzenlenmesiyle birlikte teknoloji ve inovasyon kültürüne yönelik farkındalık artmış, gençlerin araştırma ve geliştirme faaliyetlerine olan ilgisi daha görünür hâle gelmiştir. Bu gelişmeler, KKTC'nin yükseköğretimde yapay zekâ temelli dönüşümü benimseyen bölgesel bir eğitim merkezi olma potansiyelini güçlendirmektedir.

Şekil 4. *Uluslararası öğrenci çeşitliliği, KKTC üniversitelerinin küresel eğitim ve teknoloji ekosistemleriyle daha güçlü bağlar kurmasına olanak sağlamaktadır.*

Bu avantaj, KKTC'nin bölgesel bir eğitim ve teknoloji merkezi olma potansiyelini artırmaktadır. Özellikle yapay zekâ, veri bilimi, siber güvenlik ve dijital dönüşüm alanlarında yapılacak yatırımlar, üniversitelerin uluslararası görünürlüğünü güçlendirebilir.

❖ **KKTC Yükseköğretimi:**

➢**Yapay Zekâ Dönüşümünde Bölgesel Bir Merkez Olabilir mi?**

KKTC yükseköğretim sektörü ülke ekonomisinin en önemli bileşenlerinden biridir. On binlerce uluslararası öğrenciye ev sahipliği yapan üniversiteler, Doğu Akdeniz bölgesinde önemli bir eğitim merkezi konumundadır. Bu durum yapay zekâ dönüşümü açısından önemli fırsatlar sunmaktadır.

➢**Güçlü Yönler**

Uluslararası Öğrenci Profili

KKTC üniversiteleri çok kültürlü yapıları sayesinde küresel eğitim teknolojilerini test edebilecek ideal ortamlar sunmaktadır.

İngilizce Eğitim Avantajı

Birçok programın İngilizce olması küresel yapay zekâ ekosistemiyle entegrasyonu kolaylaştırmaktadır.

Esnek Yapı

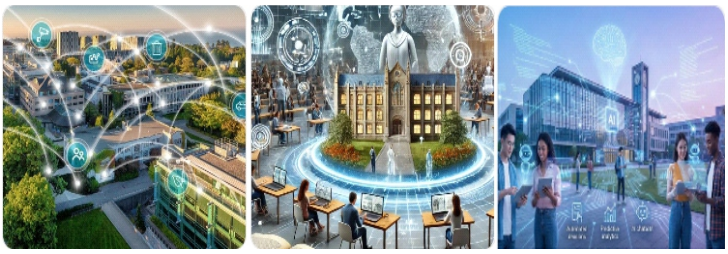
KKTC yükseköğretim sistemi büyük ülkelerdeki bürokratik süreçlere kıyasla daha hızlı hareket edebilme potansiyeline sahiptir.

Şekil 3. *Yapay zekâ destekli araştırma araçları, veri analizi ve bilimsel keşif süreçlerinde araştırmacılara önemli avantajlar sağlamaktadır.*

❖ **Akıllı Kampüsler ve Dijital Üniversiteler**

Yapay zekâ çağında üniversitelerin dönüşümü yalnızca sınıf ortamlarıyla sınırlı değildir. Kampüs yönetimi, öğrenci hizmetleri, güvenlik sistemleri ve idari süreçler de dijitalleşmektedir.

Geleceğin akıllı kampüslerinde öğrenciler ders programlarından kariyer planlamalarına kadar birçok konuda yapay zekâ destekli sistemlerden yararlanacaktır.



Şekil 5. *Akıllı kampüs uygulamaları, öğrenci deneyimini geliştirirken üniversitelerin operasyonel verimliliğini de artırmaktadır.*

❖ **Sonuç: Geleceği Şekillendiren Üniversiteler**

Yapay zekâ teknolojileri yükseköğretim sistemlerinde yalnızca teknik bir değişim değil, aynı zamanda düşünsel ve yapısal bir dönüşüm süreci başlatmıştır. Bilginin hızla üretildiği ve paylaşıldığı günümüz dünyasında üniversitelerin temel görevi, öğrencileri geleceğin belirsizliklerine hazırlamak ve onları yaşam boyu öğrenen bireyler olarak yetiştirmektir.

Bu yeni dönemde başarılı üniversiteler, teknolojiyi yalnızca kullanan değil; onu geliştiren, sorgulayan ve toplumsal faydaya dönüştüren kurumlar olacaktır. Akademisyenler rehberlik rolünü güçlendirecek, öğrenciler daha aktif öğrenme süreçlerinin merkezinde yer alacak ve araştırma faaliyetleri yapay zekâ desteğiyle yeni bir boyut kazanacaktır.

KKTC açısından değerlendirildiğinde ise yapay zekâ çağı önemli fırsatlar sunmaktadır. Güçlü üniversiteler, nitelikli insan kaynağı ve vizyoner politikalarla desteklenen bir yükseköğretim sistemi, ülkenin bölgesel bir eğitim ve teknoloji merkezi hâline gelmesine katkı sağlayabilir.

Geleceğin dünyasında rekabet yalnızca ekonomik kaynaklarla değil, bilgi üretme ve teknolojiyi yönlendirme kapasitesiyle şekillenecektir. Bu nedenle yapay zekâ çağında üniversitelerin dönüşümü, yalnızca eğitim alanının değil, toplumların geleceğinin de en önemli belirleyicilerinden biri olacaktır.

❖ **2040 Senaryosu:**

Yapay Zekâ Destekli Bir KKTC Üniversitesi

- Sabah saat 08.00.
- Öğrenci kampüse adım attığında kişisel yapay zekâ asistanı günün programını hazırlamıştır.
- Ders notları otomatik güncellenmiştir.
- Sanal laboratuvarlarda dünyanın farklı ülkelerindeki öğrencilerle ortak deneyler yapılmaktadır.
- Çeviri sistemleri sayesinde onlarca farklı dil konuşan öğrenciler aynı sınıfta eğitim alabilmektedir.
- Risk altındaki öğrenciler erken tespit edilmekte ve destek programlarına yönlendirilmektedir.
- Akademisyenler ise rutin işlerle değil, araştırma ve inovasyonla ilgilenmektedir.
- Bu senaryo uzak bir gelecek değildir.
- Birçok bileşeni bugün uygulanabilir durumdadır.

Şekil 6. *Geleceğin üniversiteleri, insan zekâsı ile yapay zekânın iş birliği içinde yeni bilgi ve inovasyon ürettiği küresel merkezler olacaktır.*

❖ **Üniversiteler Yok Olmayacak, Evrilecek**

- Yapay zekâ çağında üniversitelerin önemi azalmayacaktır.
- Tam tersine artacaktır.
- Ancak bu önem yeni roller üzerinden şekillenecektir.

Geleceğin üniversiteleri:

- Bilgi aktaran değil,
- Bilgi üreten,
- Bilgiyi doğrulayan,
- Etik kullanımını öğreten,
- İnsan ve yapay zekâ iş birliğini yöneten kurumlar olacaktır.

KKTC'nin genç, dinamik ve uluslararası yükseköğretim yapısı, bu dönüşüm sürecinde önemli bir avantaja sahiptir. Doğru stratejilerle hareket edildiğinde KKTC, yalnızca öğrenci kabul eden bir eğitim merkezi değil; yapay zekâ araştırmaları, dijital inovasyon ve yüksek teknoloji üretimi alanlarında Doğu Akdeniz'in öncü bilgi üssü haline gelebilir.

Yapay zekâ geleceği değiştirecek. Ancak geleceğin nasıl şekilleneceğine karar verecek olan yine insan aklı, bilim ve eğitim olacaktır.

Bu çalışma, yapay zekâ çağında yükseköğretimin dönüşümüne ilişkin güncel akademik literatür ve uluslararası raporlar temel alınarak hazırlanmıştır.

KAYNAKÇA

❖ Denny, P., Gulwani, S., Heffernan, N. T., Käser, T., Moore, S., Rafferty, A. N., & Singla, A. (2024). Generative AI for Education (GAIED): Advances, Opportunities, and Challenges. arXiv. https://arxiv.org/abs/2402.01580

❖ Holmes, W., Bialik, M., & Fadel, C. (2019). Artificial Intelligence in Education: Promises and Implications for Teaching and Learning. Boston: Center for Curriculum Redesign.

❖ Łodzikowski, K., Foltz, P. W., & Behrens, J. T. (2023). Generative AI and Its Educational Implications. arXiv. https://arxiv.org/abs/2401.08659

❖ Luckin, R. (2018). Machine Learning and Human Intelligence: The Future of Education for the 21st Century. London: UCL Institute of Education Press.

❖ Selwyn, N. (2019). Should Robots Replace Teachers? AI and the Future of Education. Cambridge: Polity Press.

❖ UNESCO. (2023). Guidance for Generative AI in Education and Research. Paris: UNESCO.

❖ World Economic Forum. (2025). The Future of Jobs Report 2025. Geneva: World Economic Forum.

❖ Zawacki-Richter, O., Marín, V. I., Bond, M., & Gouverneur, F. (2019). Systematic Review of Research on Artificial Intelligence Applications in Higher Education – Where Are the Educators? International Journal of Educational Technology in Higher Education, 16(39).

Yrd. Doç. Dr. Cemal Kavalcıoğlu
Yakın Doğu Üniversitesi
Mühendislik Fakültesi
Elektrik ve Elektronik Mühendisliği
Öğretim Üyesi

Bir Bıçak Gibi YZ

A. M. Turing (1950) Computing Machinery and Intelligence. *Mind 49:* 433-460.

COMPUTING MACHINERY AND INTELLIGENCE

By A. M. Turing

1. The Imitation Game

I propose to consider the question, "Can machines think?" This should begin with definitions of the meaning of the terms "machine" and "think." The definitions might be framed so as to reflect so far as possible the normal use of the words, but this attitude is dangerous, If the meaning of the words "machine" and "think" are to be found by examining how they are commonly used it is difficult to escape the conclusion that the meaning and the answer to the question, "Can machines think?" is to be sought in a statistical survey such as a Gallup poll. But this is absurd. Instead of attempting such a definition I shall replace the question by another, which is closely related to it and is expressed in relatively unambiguous words.

İkinci Dünya Savaşı'nda Nazi Almanyası'nın Enigma kodunu çözerek milyonlarca kişinin hayatını kurtaran Alan Turing, 1950 yılında yayımlanan 'Computing Machinery and Intelligence' makalesinde 'Makineler düşünebilir mi?' sorusunu sorar. İnsan ırkı makinelerin üreticisi durumundayken, 1996 yılında dönemin dünya satranç şampiyonu Garry Kasparov, IBM'in Deep Blue makinesine karşı yaptığı karşılaşmayı 4-2 kazanır. Bir yıl sonra düzenlenen rövanş karşılaşmasında ise 19 hamle sonra oyunu bırakmak durumunda kalır. Bir makinenin dünya satranç şampiyonuna karşı kazandığı anı hayal edin.

Makinelerin insanlardan daha başarılı olup olamayacakları konusu uzun zamandır tartışılan bir konuyken, Büyük Dil Modelleri'nin (LLM) gelişmesi sayesinde tartışma farklı bir seviyeye ulaştı. Unutkan bir elemanınıza çizelge hazırlatabilir, toplantı notlarını kaydedebilir, bu notları kişisel takviminize ekleyebilir veya herhangi bir konuda hatırlatıcı kurabilirsiniz. 'Donkey work' olarak aktarılan, tekrar edilen ve entelektüel düzeyi düşük olan işlerde, ilgili uygulamaları kullanarak verimliliğinizi artırabilirsiniz. Hukuk alanında 30 gün sürecek olan araştırmalar 3 dakikaya düşüyor, çağrı merkezi gibi alanlarda insan istihdamı artık yok denecek seviyede. Seçtiğiniz uygulama ile yazılım/programlama bilginiz olmasa bile, Python kullanabiliyorsunuz. Bu açılardan bakınca doğru prompt'u yazabilmek önemli bir beceri.

Yine de tablo hep pespembe değil. Yapay zeka tarafından üretilen içerikten kimin sorumlu olduğu tartışmalı bir konu. Uluslararası bir denetim mekanizması yararlı olur mu? Birleşmiş Milletler'in son dönemdeki tutukluğuna ve etkisizliğine (Filistin, Ukrayna, İran'da yaşananlar) bakıldığı zaman, kurulacak olan uluslararası bir yapay zeka gözetim biriminin etkisi olmayabilir. Ama yine bölgesel düzenlemeler de yok değil. Örneğin, AB Yapay Zeka Yasası (The AI Act) Ağustos 2024'te yürürlüğe girdi. İlgili yasa, gerçek içeriklerle yapay zeka tarafından üretilen içeriklerin ayırt edilebilmesi için çeşitli kurallar getiriyor. Yapay zeka üzerine ilk yasal çerçeve olan yasa, yapay zekanın barındırdığı risklerin kontrol edilmesini hedefliyor.

Ekim 2019'da, 19. Avrupa Dijital Devlet Konferansı'nı organize ederek ev sahipliği yapmıştık. Konferans başkanı olarak yaptığım açılış konuşmasında, yapay zekanın kamu yönetiminde elzem öncelik olacağını aktarmış, ilgili konferansta yapay zeka destekli, elektronik katılımcılığı artıracak, demokratik karar verme modeli olan 'Engage' modelini sunmuştum. Tüm kamusal süreçlerin ivedilikle dijitalleşmesi ve e-devlete geçilmesi gerektiğini kayıtlara geçirdik, önemini aktardık. COVID-19 pandemisi, yıllardır bu alanda yaptığımız çalışmaların önemini kısa sürede hatırlattı, etkili bir katalizör görevi gördü. Farkındalığımızın yapay zeka kullanımı yönünde artması için benzer bir süreç mi gerekli?

Farkındalığımız artmalı çünkü aynı oluyor tebrik mesajları, kutlamalar, haberler, konuşma metinleri… 'Bu başarı yalnızca bir sıralama sonucu değil;...' kalıbıyla sıklıkla karşılaşıyorsunuzdur.

Öğrencilere, rekabetçi iş piyasasında istihdam edilmeleri için gerekli becerileri vermesini beklediğimiz bir üniversite, paylaşımında yapay zekanın ürettiği bir içeriği kullanıyorsa, sizce bu özgün bir içerik midir?

Bu başarı yalnızca bir sıralama sonucu değil; üniversitemizin uzun vadeli vizyonunun, akademik mükemmeliyet anlayışının ve sürdürülebilir gelişim stratejisinin somut bir göstergesidir.

Bu istikrar; öğrencilerimiz, mezunlarımız ve tüm paydaşlarımız için uluslararası tanınırlık, güven ve prestij anlamına geliyor.

Modeller geliştikçe, halüsinasyon (yapay zekanın doğru olmayan bir bilgiyi, doğruymuş gibi aktarması) oranları düşüyor. Ama düşmediği anlarda ne yapılmalı? Yapay zekayı içerik üreticisi yapmak yerine, üretim kaldıracı olarak kullanmak daha doğru bir

yaklaşım olabilir. Bunun için gerek kendimizi, gerekse bağlı bulunduğumuz organizasyonları dönüştürmek, farkındalığı artırmak da gerekli.

Yaratıcılık azalıyor, nicelik artarken nitelik düşüyor. Sahte/yalan içeriğin daha hızla yayıldığı günümüzde, boş/doğrulanmamış içerik artıyor, yanlış bilgi, doğru bilgiymiş gibi hızlıca yayılıyor. Diyalektiği, tartışma kültürünü kaybediyoruz, eleştirel düşünceden yoksunlaşıyoruz. Bunlar günümüze etki eden, gelecek için olası yüksek zararlı tehlikeler. Aslında, geleceği değiştirecek en önemli teknolojilerden biri olarak görülen yapay zekanın bir bıçak gibi, soyguncunun elinde bir soygun aleti, bir doktorun elinde ise hayat kurtaran bir alet olarak durduğu gerçeğini kabullenip, bu bilinçle hareket etmek gerekiyor.

Doç. Dr. Tuğberk Kaya
E-devlet Uzmanı

Polymarket Siber Saldırıya Uğradı: Milyonlarca Dolarlık Kripto Para Çalındı

Polymarket siber saldırıya uğradı ve bazı kullanıcıların kripto varlıklarının çalındığı açıklandı. Platform, olayın üçüncü taraf bir servis kaynaklı olduğunu belirtirken zarar gören kullanıcıların kayıplarının karşılanacağını duyurdu.

Kripto dünyasında bu kez gündem, tahmin piyasalarının en bilinen platformlarından Polymarket oldu. “Polymarket siber saldırıya uğradı” haberlerinin ardından kullanıcılar, platformdaki varlıklarının güvende olup olmadığını sorgulamaya başladı. Şirket ise olayın sınırlı sayıda kullanıcıyı etkilediğini söylüyor.

Polymarket’i yalnızca kripto kullanıcıları değil, politikadan spora kadar pek çok konuda tahmin piyasalarını takip eden geniş bir kitle de kullanıyor. Bu yüzden yaşanan olay, sıradan bir güvenlik açığından daha büyük yankı uyandırdı. Özellikle cüzdan onayları üzerinden ilerleyen saldırı yöntemi dikkat çekti.

Paylaşılan bilgilere göre saldırı, doğrudan Polymarket’in ana sistemi yerine üçüncü taraf bir servis üzerinden
gerçekleşti. Buradaki en kritik nokta şu: Kripto cüzdanlarında bir işlemi onaylamak, çoğu zaman paranın gerçekten hareket etmesi anlamına geliyor. Yani kullanıcı yalnızca ekrandaki bir butona basmış gibi görünse de arka planda dijital varlıkları başka bir adrese gönderilebiliyor.

Polymarket, saldırının yaşandığını ve kullanıcı fonlarının çalındığını doğruladı ancak resmi kayıp miktarını açıklamadı. Şirket, etkilenen kullanıcılarla iletişime geçileceğini ve zararların platform tarafından karşılanacağını belirtti.

Kullanıcıların dikkat etmesi gerekenler

Bu olay, kripto cüzdanı kullanan herkes için önemli bir hatırlatma oldu. Bilmediğiniz işlem onaylarını kabul etmemek, cüzdan izinlerini düzenli kontrol etmek ve şüpheli bağlantılardan uzak durmak artık ekstra önlem değil, temel güvenlik alışkanlığı. Özellikle tarayıcı cüzdanlarında tek bir onay büyük kayıplara yol açabiliyor.

Polymarket cephesinde ise bundan sonra asıl beklenti, saldırının tüm teknik detaylarının şeffaf biçimde paylaşılması olacak. Kullanıcıların güvenini geri kazanmak isteyen platformun yalnızca geri ödeme yapması yetmeyebilir. Bağımsız güvenlik denetimleri ve daha sıkı üçüncü taraf kontrolü de şart görünüyor.

KKTC'de Meslek Liseleri ve Bilişim Eğitiminin Verimlilik Sorunu

KKTC'de meslek liseleri, düz liselere kıyasla öğrenci başına daha yüksek maliyetli eğitim kurumlarıdır. Bunun temel nedeni bilişim gibi alanlarda sürekli güncellenmesi gereken laboratuvar ve teknik donanım yatırımlarıdır. Ancak bu yüksek yatırımın geri dönüşü sınırlı kalmaktadır; çünkü bilişim mezunlarının çok küçük bir kısmı (%5'ten az) istihdam edilmektedir. Bu durum, devletin eğitim bütçesinde meslek liselerinin pahalı ama stratejik bir alan olduğunu, buna rağmen istihdam ve alanında devam oranlarının düşük kalmasının ciddi bir verimlilik sorunu yarattığını göstermektedir.

Meslek Liselerinin Ülkelerin Gelişimindeki Rolü

Meslek liseleri, ülkelerin ekonomik ve toplumsal gelişiminde kritik bir rol oynar. Öğrencilere yalnızca teorik bilgi değil, doğrudan iş hayatında kullanılabilecek uygulamalı beceriler kazandırarak onları üretim ve hizmet sektörüne hazırlar. Bu okullar, gençlerin erken yaşta meslek sahibi olmalarını sağlarken aynı zamanda sanayi, bilişim, sağlık ve turizm gibi alanlarda ara eleman ihtiyacını karşılar.

Meslek liselerinin önemi, yalnızca bireysel kariyer gelişimiyle sınırlı değildir; aynı zamanda ülkenin ekonomik verimliliğini artırır, işsizlik oranlarını düşürür ve sektörlerin nitelikli iş gücüne erişimini kolaylaştırır. Bu nedenle meslek liseleri, eğitim sisteminin stratejik bir parçası olarak görülmeli ve sürekli desteklenmelidir.

Ülkemizdeki Meslek Liselerinin Durumu

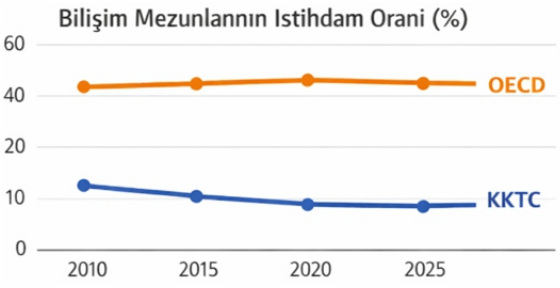
KKTC'de genel tabloya baktığımızda, meslek liselerinin eğitim sistemindeki yeri oldukça kritik ama aynı zamanda sorunlu bir noktada duruyor. Son yıllarda lise öğrencilerinin yaklaşık dörtte biri meslek liselerinde eğitim alıyor; bu oran bilişim, elektrik-elektronik, sağlık ve turizm gibi alanlarda yoğunlaşıyor. Ancak mezunların yalnızca %20'si kendi alanında üniversiteye devam ediyor ya da çok küçük bir kısmı (%3) doğrudan mesleğini yapıyor. Geri kalan büyük çoğunluk ya alan dışı bölümlere yöneliyor ya da farklı sektörlerde çalışıyor. Bu durum, bir yandan üniversiteye yönelme oranını yüksek tutarken diğer yandan teknik eleman açığını büyütüyor.

Dolayısıyla KKTC'de meslek liselerinin önemi yalnızca bireysel kariyer açısından değil, ülkenin ekonomik verimliliği ve iş gücü dengesi açısından da belirleyici. Eğitim maliyetleri düz liselere göre daha yüksek olmasına rağmen, yatırımın geri dönüşü sınırlı kalıyor. Bu tablo, meslek liselerinin daha güçlü sektör–okul iş

birlikleriyle desteklenmesi gerektiğini ve mezunların alanında devam etme oranını artıracak politikaların önemini ortaya koyuyor.

Bilişim İstihdamında Dünya Normları ile KKTC Arasındaki Uçurum

Bilişim alanında ise dünya genelinde, son 20 yılda en hızlı büyüyen sektörlerden biri haline geldi. Yazılım geliştirme, siber güvenlik ve yapay zekâ gibi alanlarda iş gücü talebi her yıl artıyor. OECD ülkelerinde bilişim mezunlarının kendi alanında istihdam oranı %45–50 seviyelerinde; bu da bilişim eğitiminin doğrudan ekonomik büyümeye katkı sağladığını gösteriyor.
KKTC'de ise bilişim alanındaki tablo daha farklı. Meslek liselerinde bilişim eğitimi alan öğrencilerin üniversiteye geçiş oranı yüksek (%60), fakat alanında bir bölüme devam edenlerin oranı %25 ile sınırlı. İş gücü tarafında ise son 15 yılda bilişim mezunlarının yalnızca %10'u sektörde istihdam edilebilmiş (lise ve üniversite mezuniyeti sonrası). Bu oran, dünya ortalamasının oldukça altında. KKTC'nin büyüyen teknoloji ve hizmet sektörü ara eleman ihtiyacını karşılamakta zorlanıyor; bu da ülkenin dijital dönüşüm sürecini yavaşlatıyor.



Meslek Lisesinde Bilişim Eğitimi Alan Mezunların İstihdam Sorunu"

Yazının başında da belirtildiği gibi, KKTC'de bilişim meslek liselerinden mezun olan öğrenciler, eğitim sürecinde ciddi yatırımlarla yetiştirilmelerine rağmen mezuniyet sonrası sektörde yeterince yer bulamamaktadır. Bu durum, hem gençlerin kariyer beklentilerini karşılamada başarısız kalmakta hem de ülkenin bilişim alanındaki nitelikli iş gücü açığını derinleştirmektedir.

Bu durumda mevcut soruna çözüm üretebilmek için aşağıdaki soruyu sormak gerekir. Ülkemizdeki meslek liselerinden mezun olan öğrenciler neden sektörde yeterince istihdam edilmiyorlar?
Bu sorunun cevabı aşağıdaki maddelerle özetlenebilir:

- Eğitim kalitesizliği: Müfredat güncel teknolojilere uyumlu değil. Öğrenciler mezun olduklarında yazılım, ağ yönetimi veya siber güvenlik gibi alanlarda çağın gerektirdiği becerilere sahip olmuyor. Bu da işverenlerin güvenini azaltıyor.
- Öğrencilerin seviyesinin yetersizliği: Meslek liselerine genellikle akademik başarısı düşük öğrenciler yönlendiriliyor. Bu öğrenciler bilişim gibi analitik düşünme ve problem çözme gerektiren alanlarda zorlanıyor. Sonuçta mezuniyet sonrası sektörde tutunmaları güçleşiyor.
- Üniversite mezunu ihtiyacı: KKTC'de bilişim sektöründe iş ilanlarının çoğu üniversite diploması şartı koyuyor.
  Meslek lisesi mezunları ara eleman olarak değerlendirilmiyor; işverenler daha çok mühendislik diplomasına sahip adayları tercih ediyor.
- Teknoloji ve öğretim elemanı yetersizliği: Okullardaki bilgisayar laboratuvarları güncel değil, yazılım lisansları eksik ve öğretmenlerin bir

kısmı sektörde aktif deneyime sahip değil. Bu da öğrencilerin pratik beceri kazanmasını engelliyor.

Mezunların tercihleri Öğrenciler bilişim mezunu olsalar da turizm, ticaret veya kamu sektöründe daha kolay iş buldukları için alan dışına yöneliyorlar. Bu da bilişim sektöründe mezun–istihdam uyumsuzluğunu artırıyor.

Yukarıda maddeler, neden meslek lisesi bilişim bölümü mezunlarının çok düşük bir oranda mesleğini yaptığını açıklıyor. Yukarıdaki maddelere çözüm bularak istihdam oranı artırılabilir.

Nitelik ve Nicelik Sorunu

Önceden sorulan soruya ek olarak sorulması gereken bir soru daha var. Nitelik mi nicelik mi? KKTC'de meslek liselerinde bilişim bölümlerinde okuyan öğrenci sayısı her yıl yaklaşık 1.000–1.200 civarındadır; bu öğrencilerden yaklaşık 250-300'ü her yıl mezun olmaktadır.
KKTC'nin bilişim alanında yıllık yeni iş gücü ihtiyacı yaklaşık 350-400 kişi olarak tahmin edilmektedir. Bu açıdan bakınca mezunlar ve ihtiyaçlar örtüşüyor gibi görünmekle birlikte, aranan işgücünün çoğunluğunun üniversite mezunu olmayı şart koşması, mezun öğrencilerin büyük çoğunluğunun iş hayatına bilişim sektöründe atılmak yerine üniversiteye gitmeyi tercih etmesi, yine mezun olanların önemli bir bölümünün başka mesleklerde iş bulmaya çalışması sebebi ile yukarıda belirtilen iş gücü ihtiyacının çok azı meslek lisesi bilişim mezunu öğrencileri tarafından doldurulabiliyor.

Sonuç olarak, meslek liselerinin yatırım–geri dönüş dengesi zayıf; devlet yüksek maliyet üstleniyor ama mezunların az bir kısmı sektörde kalıyor. Burada üçüncü bir soru sormak gerekiyor. Ülkenin bilişim ile ilgili istihdam ihtiyacını çözmek şöyle dursun, %10 bile katkıda bulunamayan bu bölümlerde neden bu kadar öğrenci okutuluyor? Neden nitelik yerine nicelik tercih ediliyor?

Meslek Liselerinde Yatırımın Karşılığı Alınamıyor

KKTC'deki meslek lisesi öğrencisinin devlete maliyeti yıllık yaklaşık 3.500–5.000 USD'dir. Bununla birlikte düz lisede okuyan bir öğrencinin devlete maliyeti yaklaşık 2500-3500 USD'dir. Burada öğrenci başına 1000-1500 USD'lik bir fark demektir ki bu yatırımın çok büyük ölçüde geri dönüşünün olmadığı yukarıda rakamlarla gösterilmiştir. Bu durumda genelde tüm meslek lisesi bölümleri, özelde de bilişim bölümlerinde devletin çok küçük oranda geri dönüş alacağı öğrencilere, öğretmenlere, binalara yatırım yaptığı anlamını taşımaktadır. Mesela her yıl 1200 bilişim bölümü öğrencisine, yukarıda da miktarı belirtildiği gibi, bir düz lise öğrencisine yapılandan daha fazla masraf yapılmaktadır ki bu rakamı öğrenci sayısı ile çarparsak sadece bilişim bölümünde okuyan öğrencilerin devlete 1,000,000-1,500,000 USD arasında masrafı vardır. Bilişim öğrencilerinin tüm meslek lisesi öğrencilerine oranının %20 olduğunu hesaba katarsak, toplamda bu maliyetin yıllık 5,000,000 – 7,500,000 USD olduğu çıkar.

Kaynakça

- KKTC Millî Eğitim Bakanlığı – Mesleki Teknik Öğretim Dairesi https://www.mebnet.net Meslek liselerine giriş, mezuniyet oranları, bölüm dağılımları.
- YÖDAK (Yükseköğretim Planlama, Denetleme, Akreditasyon ve Koordinasyon Kurulu) https://www.yodak.gov.ct.tr (yodak.gov.ct.tr in Bing) Üniversiteye geçiş oranları, kontenjan doluluk, bölüm tercihleri.
- OECD Education Statistics – Vocational Education and Training (VET) https://data.oecd.org/education.htm (data.oecd.org in Bing) Meslek lisesi mezunlarının istihdam oranları, dünya ortalamaları.
- Eurostat – Vocational Education and Training Statistics https://ec.europa.eu/eurostat AB ülkelerinde meslek lisesi mezunlarının istihdam oranları.
- U.S. Bureau of Labor Statistics – ICT Employment Data

Yıllık Öğrenci Maliyeti Karşılaştırması

Okul Türü	Minimum Maliyet (USD)	Maksimum Maliyet (USD)
Meslek Lisesi	3,500	5,000
Düz Lise	2,500	3,500

İskele Evkaf Türk Maarif Koleji (İETMK) yeni binasının yapımı 2021 yılında tamamlandığında 8 milyon TL'ye mal olduğu açıklanmıştır. Bu yatırım, 13 derslik, laboratuvarlar, dil ve bilişim sınıfları ile diğer sosyal alanları kapsayacak şekilde hayata geçirmiştir. Açıldığı 24 Eylül 2021 tarihinde ve yılın önceki zamanlarında dolar kuru 8-8.5 TL dolaylarında seyretmiştir. Bu da okulun maliyetinin yaklaşık 1,000,000 USD olduğunu göstermektedir. IETMK'nın öğrenci kapasitesi 250-300'dür. Bu verilere göre meslek liselerine yapılan yanlış yatırımların yerine 5-7 adet 250-300 kişilik okul yapılabilmektedir.
Tabi ki bu yazının amacı meslek liselerini kapattırıp yerine okul yapın demek değildir. Esas amaç hem istihdama katkı sağlamayan hem de devlete büyük yük olan bu yapının nasıl daha faydalı olabileceğinin çözümlerini aramaktır. Bu sebepten dolayı, bir sonraki bölümde çözüm önerilerine odaklanılacaktır.

Dr. Umut Zeki
Bilişim Teknolojileri Öğretmeni

Veritabanı/Database Konuları 1

Şu Veritabanı Ne?
Veri(Data), organizasyonların en değerli varlığıdır. Verilerin toplanması ve işlemlerde kullanılarak en hızlı ve doğru sonuca ulaşmak, varlık, sürdürülebilirlik ve finansal ilerleme için artık zorunluluktur.
Bir işletmenin kalbi olan veritabanları, sadece bilgiyi saklamakla kalmaz, aynı zamanda operasyonların sürdürülebilirliğini ve büyümesini sağlar.
Organizasyonların, işlemlerini yapılabilmesi için veri(data)/kayıtlar, aynı formatlarda/yapılarda saklanmasını sağlar ve bu şekil, tarif edilebilecek en büyük özelliğidir. Aşağıdaki maddeler detaylı olarak, bu sayede, işlemlerin aynı düzende ve daha hızlı yapılmasını anlatır.

Merkezi Veri Yönetimi: Verilerin dağınık dosyalar yerine tek bir merkezde toplanmasını sağlayarak "veri kirliliğini" (data redundancy) önler.
Hızlı ve Kararlı Erişim: Milyonlarca satır veri arasından milisaniyeler içinde arama yapılmasına, raporlar oluşturulmasına olanak tanır.
Veri Bütünlüğü ve Doğruluk (Data Integrity): Tanımlanan kurallar ve kısıtlamalar (constraints) sayesinde veritabanına hatalı, eksik veya mantıksız veri girilmesi engellenir.
Eşzamanlılık Kontrolü (Concurrency): Aynı anda binlerce kullanıcının veri çakışması yaşamadan işlem yapabilmesini sağlar (Örn: Bir e-ticaret sitesinde son kalan ürünün aynı anda iki kişiye satılmaması).
Stratejik Karar Destek: Geçmişe dönük verilerin analizi sayesinde (İş Zekası - BI), üst yönetimin geleceğe yönelik doğru stratejik kararlar almasını sağlar.

Veritabanı Sayesinde, İş Sürekliliği (Business Continuity) ve Finansal Etki
Bir veritabanı, geleceğe yönelik planlamayla, sağlam ve takip edilebilen algoritmalarla yeni bir şekile bürünür ki bu yeni bir yapının başlangıcı demektir : Relational Database Management Systems (RDBMS) ve sonra dünyayı döndüren ERP.. Artık organizasyon haritasının başına geliyoruz. İlerleyen aşamalarda detaylandıracağız.

Veritabanının yapısı, organizasyon kayıt sistemi yapısıdır. Sağlıklı olarak bu kayıtlara ulaşılabilmesi için, günlük hayatındaki işlemlerini, değişik departman, bölüm, vs. gibi farklı amaçlara yönelik birbirlerinden bağımsız verilerin ilişkilendirilerilmesi gerekir. Böylece tüm işlemler biraraya gelerek organizasyonun veritabanı yapı ve işleyiş sistemini oluştururlar. Öncelik, verinin planlı olarak yapılandırılan 'şekil'lerde tutulabilmesidir.

Veri tutulan yapılarda hata olduğu zamanlar, veritabanının erişilemez olması veya çökmesidir ki bu organizasyonun, dijital dünyada tamamen durması anlamına gelir. Böyle bir durumda olası sonuçlar genel olarak aşağıdaki sonuçlara sebep olur:
Müşteri Güveni Kaybı: Kullanıcılar hesaplarına, siparişlerine veya bakiyelerine vs. erişemediklerinde platforma olan güvenlerini kaybederler.
Finansal Kayıp: Özellikle ERP, CRM ve e-ticaret sistemlerindeki kesintiler, doğrudan ciro ve iş gücü kaybına yol açar.
Yasal Yükümlülükler: Finans, sağlık ve e-ticaret gibi sektörlerde veri kaybı veya sızıntısı yaşanması, KVKK (Kişisel Verilerin Korunması Kanunu) ve GDPR gibi regülasyonlar nedeniyle çok ağır hukuki cezalara yol açar.

Yapılandırma aşamasında ileriye dönük planlamayla birlikte kurulması gereken bu 'sistem', yazılım hataları dışında, uzaktan, yetkisiz müdahalelere de kapalı ve korumalı olmak zorundadır.

Veritabanı Koruma ve Güvenlik Yöntemleri
Bir veritabanını tam anlamıyla korumak; fiziksel güvenlik, ağ güvenliği ve yazılım önlemlerden oluşan çok katmanlı bir mimari gerektirir.

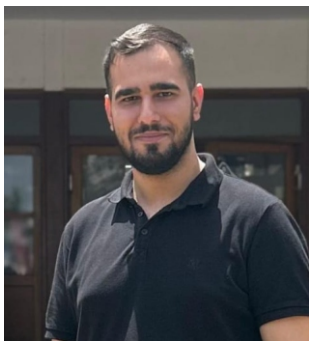
A. Erişim Yönetimi ve Yetkilendirme
En Az Yetki İlkesi (Principle of Least Privilege): Her kullanıcıya ve uygulamaya, sadece işini yapabileceği kadar yetki verilmelidir. Örneğin, sadece rapor çeken bir uygulamanın veri silme (DELETE) yetkisi olmamalıdır.
Güçlü Kimlik Doğrulama: Veritabanı yönetim panellerine erişimde Çok Faktörlü Kimlik Doğrulama (MFA) zorunlu tutulmalıdır.
B. Veri Şifreleme (Encryption)
Durağan Veri Şifrelemesi (Data-at-Rest): Veritabanı dosyaları ve yedekleri diskte saklanırken şifrelenmelidir. Böylece disk çalınsa bile veriler okunamaz.
Hareket Halindeki Veri Şifrelemesi (Data-in-Transit): Uygulama ile veritabanı arasındaki iletişim (TLS/SSL protokolleri ile) şifrelenerek ağ üzerindeki dinlemeler engellenmelidir.
C. Yedekleme ve Kurtarma (Backup & Disaster Recovery)
3-2-1 Yedekleme Kuralı: Verinin en az **3** kopyası bulunmalı, bu kopyalar **2** farklı medya türünde saklanmalı ve en az **1** kopya farklı bir coğrafi konumda (veya bulutta) tutulmalıdır.
Düzenli Testler: Alınan yedeklerin çalışıp çalışmadığı belirli periyotlarla "Geri Yükleme" (Restore) testlerine tabi tutulmalıdır.
D. İzleme ve Denetim (Auditing & Monitoring) Veritabanı üzerinde kimin, ne zaman, hangi sorguyu çalıştırdığına dair **log (günlük) kayıtları** tutulmalı ve bu kayıtlar şüpheli aktiviteler

RDBMS ne o zaman?
RDBMS genel bir **mimari standart ve teoridir**; dBase ise 1980'lerde bilgisayar dünyasını şekillendiren **özel bir yazılım ürünü ve dosya formatıdır**.
20. Yüzyılda yazılımın önemini ortaya çıkaran veritabanı 'keşfi', 21. Yüzyıla ismini veren küreselleşmenin yazılım açısından, en büyük yapıtaşıdır.Geliştirme aşamaları, aynı anda birkaç bulmacayı çözmek gibidir... :

Geleck Sayıda Veritabanı/Database ERP Konuları 2
buluşmak üzere hoşçakalın.

Vasviye Tunaboylu
Database Specialist

Hayvancılıkta Yapay Zekânın Önemi



İnsanlığın hayvansal gıdalarla buluşması milyonlarca yıl öncesine dayanır. Et, süt, yumurta ve diğer hayvansal ürünler insan beslenmesinde büyük yer tutmuştur. Fakat hayvanlarla kurulan bu yakın ilişki yalnızca üretim ve beslenme meselesi değildir; aynı zamanda halk sağlığı, gıda güvenliği, ekonomi ve toplum güveni meselesidir. Bir çiftlikte ortaya çıkan hastalık bazen yalnızca birkaç hayvanı değil, üretim zincirini, tüketici güvenini ve ülke ekonomisini de etkileyebilir.

Bu nedenle hayvancılıkta asıl hedef yalnızca daha fazla üretmek olmamalıdır. Daha sağlıklı hayvan, daha erken hastalık farkındalığı, daha güçlü izlenebilirlik ve daha güvenilir gıda zinciri hedeflenmelidir. Yapay zekâ tam bu noktada önemli bir araç haline gelmektedir. Ancak bu teknoloji veterinerin yerine geçen bir sistem değildir. Doğru kullanıldığında veterinerin, çiftçinin ve denetim kurumlarının kararlarını güçlendiren ikinci bir göz, erken uyarı mekanizması ve veri destekli yardımcıdır.

Yapay zekâ hayvancılıkta neden önemli?

Modern hayvancılık dışarıdan geleneksel görünse de aslında büyük miktarda veri üretir. Bir hayvanın yem tüketimi, su içme sıklığı, günlük hareketi, yatma-kalkma düzeni, süt verimi, vücut sıcaklığı, yürüyüş şekli ve sürü içindeki davranışı sağlık açısından değerli ipuçları taşır. Büyük sürülerde bu verileri insan gözüyle sürekli takip etmek neredeyse imkânsızdır.

Kamera, sensör ve elektronik küpe sistemlerinden gelen bilgiler yapay zekâ ile analiz edildiğinde “bu hayvanda normal dışı bir durum olabilir” uyarısı daha erken verilebilir.

Bilgisayarlı görü, yani kameralarla görüntü analizi, bu alandaki en güçlü yöntemlerden biridir. Kamera destekli sistemler hayvanın yürüyüşünü, duruşunu, yemliğe gitme sıklığını, yatma süresini ve sürüden ayrılıp ayrılmadığını izleyebilir. Böylece topallık, stres, davranış değişikliği, iştah azalması veya hastalık başlangıcı gibi durumlar daha erken fark edilebilir.

Dünyada ne yapıldı, ne kadar başarılı oldu?

Dünyadaki çalışmalar artık teorik aşamayı geçmiş durumdadır. 2024'te Scientific Reports'ta yayımlanan CBVD-5 çalışmasında 107 ineğin bulunduğu bir çiftlikte 7 kamera ile 96 saatlik kayıt alınmış ve 206.100 görüntü örneği oluşturulmuştur. Sistem; ayakta durma, yatma, yem arama, geviş getirme ve su içme gibi beş temel davranışı tanımaya çalışmıştır. Çalışmada kullanılan modelin test hata oranı %21,28 olarak verilmiştir. Bu sonuç yaklaşık %78,7 doğruluk anlamına gelir ve bilgisayarlı görünün hayvan davranışı takibinde uygulanabilir bir noktaya geldiğini gösterir [1].

Bir başka örnek inek tespiti ve takibi üzerinedir. 2023'te yayımlanan Scientific Reports çalışmasında gerçek çiftlik görüntüleri üzerinde ineklerin video boyunca takip edilmesi hedeflenmiştir. Araştırmacılar, takip sisteminin tüm video sekanslarında %99'un üzerinde MOTA değerine ulaştığını bildirmiştir [2]. Bu başarı özellikle doğum öncesi davranış değişiklikleri, bireysel hayvan takibi ve sürü yönetimi için önemlidir. Çünkü sistem yalnızca “görüntüde inek var” demekle kalmaz; aynı hayvanın zaman içindeki hareketini izlemeye çalışır.

Sağlık açısından en önemli örneklerden biri de topallık ve yürüyüş bozukluğu tespitidir. Topallık; hayvan refahını bozan, süt verimini düşürebilen ve tedavi maliyetini artıran bir sorundur. Kamera temelli sistemler hayvanın adım düzeni, sırt duruşu ve hareket simetrisini analiz ederek erken uyarı verebilir. Bu tür sistemlerin değeri, kesin tanı koymasından değil, veterinerin hangi hayvana öncelik vermesi gerektiğini göstermesinden gelir.

Deli dana hastalığında yapay zekânın doğru rolü

Halk arasında deli dana hastalığı olarak bilinen BSE, sığırlarda görülen ciddi ve ölümcül bir sinir sistemi hastalığıdır. EFSA'ya göre BSE, insanları ve hayvanları etkileyebilen TSE hastalık grubundadır ve prion adı verilen anormal proteinlerle ilişkilidir [3]. Klasik BSE'de davranış değişikliği, koordinasyon kaybı, yürüme veya ayakta durma zorluğu, süt veriminde azalma ve kilo kaybı gibi belirtiler görülebilir [3].

Burada çok net bir sınır çizmek gerekir: Yapay zekâ kamerası BSE'ye kesin tanı koyamaz. BSE gibi hastalıklarda kesin karar resmi veterinerlik süreci, laboratuvar incelemesi ve mevzuata uygun denetimle verilir. Fakat yapay zekâ; dengesiz yürüyüş, normal dışı davranış, sürüden uzaklaşma veya ani performans düşüşü gibi belirtileri erken fark ederek “bu hayvan kontrol edilmeli” uyarısı verebilir. Bu nedenle yapay zekâ, tanı koyan değil, şüpheli durumu öne çıkaran bir erken uyarı katmanı olarak düşünülmelidir.

Avrupa Birliği bu işi nasıl yönetiyor?

Avrupa Birliği'nin yaklaşımı yalnızca kamera veya sensör kullanımına dayanmaz. AB sistemi; hayvan hastalıklarının izlenmesi, yem güvenliği, hayvan kimliklendirme, hareket kayıtları, mezbaha kontrolleri, laboratuvar doğrulaması ve resmi denetim üzerine kuruludur. EFSA, 1989'dan beri Avrupa Komisyonu ve üye devletlerin BSE riskini yönetmek için kapsamlı önlemler aldığını belirtmektedir [3]. Ayrıca AB'de BSE vakaları çok düşük seyretse bile hedefli izlemenin hâlâ önemli olduğu vurgulanmaktadır [3].

Bu yaklaşım KKTC için de ders niteliğindedir. Başarılı sistem yalnızca kameradan ibaret değildir. Kamera bir belirtiyi yakalar; elektronik küpe hayvanın kimliğini söyler; kayıt sistemi hayvanın geldiği çiftliği, temas ettiği sürüyü ve hareket geçmişini gösterir; veteriner ve laboratuvar ise son kararı verir. Yani güçlü hayvancılık yönetimi, yapay zekâ ile resmi izlenebilirlik sisteminin birlikte çalışmasıyla oluşur.

KKTC için çıkarım: gösteriş değil, güvenilir sistem

KKTC hayvancılığı için yapay zekânın hedefi "teknoloji kullanmış olmak" değildir. Asıl hedef; hastalığı daha erken fark eden, hayvan refahını izleyen, çiftçinin kaybını azaltan ve tüketiciye daha güvenilir et-süt zinciri sunan bir yapı kurmaktır. Bunun için dünyadaki başarılı örnekler dikkatle incelenmeli, fakat doğrudan kopyalanmamalıdır. KKTC'nin çiftlik ölçeği, veteriner kapasitesi, ekonomik koşulları ve veri altyapısı dikkate alınmalıdır.

En mantıklı başlangıç, kamera destekli davranış izleme, elektronik kimliklendirme ve dijital sağlık kayıtlarının aynı sistemde birleştirilmesidir. Böyle bir yapı sayesinde bir hayvanın hareket azalması, yem tüketimindeki değişim, yürüyüş bozukluğu veya süt verimindeki düşüş daha erken görülebilir. Şüpheli durum oluştuğunda veteriner yalnızca genel sürüye değil, doğrudan riskli hayvana odaklanabilir. Bu da hem zaman kazandırır hem de hastalıkların yayılma ihtimalini azaltır. Güney Kıbrıs'ın AB üyesi olması, onu AB'nin gıda güvenliği ve izlenebilirlik düzenine daha doğrudan bağlı hale getirir. KKTC tarafında ise uluslararası tanınma ve veri paylaşımı gibi sınırlılıklar bulunabilir. Fakat KKTC'nin küçük ölçekli yapısı, doğru planlanırsa avantaj da olabilir. Daha az sayıda merkezle hızlı veri toplamak, sistemi test etmek ve başarılı modeli ülke geneline yaymak daha kolaydır.

Sonuç

Dünyadaki örnekler şunu göstermektedir: Yapay zekâ hayvancılıkta mucize değildir; fakat doğru kurulduğunda çok güçlü bir erken uyarı ve karar destek aracıdır. Hayvan davranışını izleyebilir, yürüyüş bozukluğunu fark edebilir, bireysel hayvan takibini güçlendirebilir ve veterinerin dikkatini doğru noktaya çekebilir. Deli dana gibi ciddi hastalıklarda ise yapay zekâ kesin tanı koymaz; yalnızca şüpheli belirtiyi daha erken görünür hale getirir. KKTC için doğru hedef, yapay zekâyı veterinerlik bilgisi, laboratuvar doğrulaması ve dijital izlenebilirlik ile birleştirerek daha sağlıklı, daha güvenilir ve daha modern bir hayvancılık sistemi kurmak olmalıdır.

Kaynakça

[1] Li, K. ve ark. A new dataset for video-based cow behavior recognition. Scientific Reports, 2024.

[2] Mar, C. C. ve ark. Cow detection and tracking system utilizing multi-feature tracking algorithm. Scientific Reports, 2023.

[3] European Food Safety Authority (EFSA). Bovine spongiform encephalopathy (BSE), son inceleme: 27 Nisan 2026.

[4] Regulation (EC) No 999/2001 ve Regulation (EU) 2016/429: AB hayvan sağlığı, TSE/BSE ve izlenebilirlik çerçevesi.

Ata Ateş
Yapay Zeka Mühendisliği
DAÜ 2. sınıf öğrencisi

Modelle Çıktığımız Yolda, Modeli Kaybettik

Bazı şeyleri kaybettiğimizi, çoğu zaman ancak yıllar sonra fark ederiz. Bugün "katılımcı demokrasi" ya da "dijital devlet" dediğimizde, çoğu insan bunu gelişmiş ülkelerin düzeni sanıyor. Oysa bir zamanlar bizde de bunu konuşan, tartışan, dünyada olan biteni izleyip kendi eksiklerimizi görebilen ve büyük resme göre yol çizmeye çalışan bir birliktelik vardı. Ben o yılları uzaktan okuyanlardan değil, o masada bulunan birçok arkadaştan biriydim. Bu yüzden bugünkü tabloyu anlatmak benim için yalnızca bir analiz değil; ben, kaybettiğimiz bir birikimin ve birlikteliğin üzgün tanıklarından biriyim.

Bu yazı, geçen sayıda söz verdiğim yerden, katılımcı demokrasiden başlıyor ve asıl meselenin katılım, birliktelik ve ortak akılla oluşturulan modellerin uygulanması olduğunu anlatıyor. İşte bir zamanlar modelle çıktığımız o yolda, modeli kaybettik. Katılımcı demokrasi bizim için ithal bir hayal değil; bir zamanlar, kısmen de olsa kurmaya başladığımız, sonra bir yerlerde elimizden bıraktığımız ya da elimizden alınan bir pratikti. Onu yeniden konuşabilmek için, önce ne yaptığımızı ve neyi kaybettiğimizi hatırlamamız gerekir. Neyse ki bu hatırlama işini tek başıma yapmak zorunda değilim: o dönemin en önemli tanıklarından Necdet İcil hocam, o yıllarda yapılanları bu ayki yazısında çok iyi özetlemiş. Ben bu yazıda kronolojiyi tekrarlamak yerine, o masada kurulan birlikteliği ve sonra dağıtılan modeli anlatmaya çalışacağım.

Kamu ve Özel Sektörün IT uzamanları ile birlikte

Dönemin siyasetçileri ve bürokratlarına sunum

Atatürk Kültür Merkezi'nde topluma açık bilgilendirme semineri

O masada ne vardı?

En başta 2000 yılı problemi, ardından o günün adıyla e-devlet, bugünkü adıyla e-yönetim çalışmaları, Avrupa Birliği regülasyonları ve Annan Planı sürecinde oluşturulan yasal mevzuat bütünü, eksikliklerimizi daha görünür yapmıştı. Başta mevzuat uyumlulukları olmak üzere, olmayan ama olması gereken çok şey vardı. O dönem devlete — siyasete ve hükümete — bu konularda danışmanlık yapan bir ekip, meseleyi tek tek değil bütün olarak ele alıyordu. Avrupa'nın o günkü pusulası, 2000'de kabul edilen ve 2010'u hedefleyen Lizbon Stratejisi'ydi; ardından gelen Avrupa Dijital Gündemi de 2020'yi işaret ediyordu. İşte yol haritası bu hedeflere göre, ama kendi ihtiyaçlarımız görülerek ve önceliklendirilerek çiziliyordu.

Bunu yaparken dünyanın en iyi örneklerini masaya getiriyorduk; Estonya deneyimi başı çekiyordu. Estonya e-Devlet Akademisi'nin (e-Governance Academy – eGA) kurucu direktörü — aynı zamanda Avrupa Konseyi Parlamenter Meclisi'nde Budapeşte Siber Suç Sözleşmesi'nin raportörlüğünü yapan — Ivar Tallo'yu ve Estonya devlet bilgi sistemlerinin uzun yıllar başında bulunmuş, ülkenin dijital devlet mimarisiyle özdeşleşen Arvo Ott gibi isimleri adamıza getirerek, önce o birliktelikte bütün paydaşlarla dinledik, sonra politikacılara ve bürokratlara dinlettirdik. Onların kurduğu X-Road'u inceledik: veriyi tek bir dev merkezde toplamak yerine kaynağında tutan, kurumlar arasında kimlik doğrulaması ve kayıtla çalışan güvenli bir veri değişim katmanı. Dünya Bankası'nın ve büyük teknoloji şirketlerinin o dönemki yaklaşımlarını, farklı teknik modelleri tek tek değerlendirdik; hiçbirini olduğu gibi almadık, hepsini KKTC ölçeğine göre harmanladık.

Ama bugünden geriye baktığımda, o masanın asıl değeri kullandığımız teknoloji değildi. Asıl değer, bir çalışma ahlakıydı. Bürokrat, siyasetçi ve teknik kadro aynı masaya oturuyor, kendi penceresinden değil bütün resme bakarak konuşuyor, hangi yasanın önce, hangisinin sonra geleceğini birlikte kararlaştırıyordu. Yani o masada olan şey, aslında katılımın ta kendisiydi: farklı akılların, ortak bir resmi kurmak için bir araya gelmesi.

Sonra bir yerde koptu

2010'a doğru gelindiğinde, on yılı aşmış bir birikim ve deneyim, projelendirilmiş bir yol haritası ve Başbakanlık'ta, Meclis'e gitmek için sırasını bekleyen bir mevzuat ailesi vardı. Sonra bir yerlerde her şey koptu. Birikimi taşıyacak süreklilik kırıldı, büyük resim gözden kaçtı, yasalar tamamlanamadı; geçenler ise maalesef güncellenmedi. Kurumsal hafıza bir seçimden diğerine taşınamadığı için, bir zamanlar önceliklendirilmiş o düzen dağıldı. Burada dürüst olmak gerekir, çünkü kolay yol suçu dışarıya yıkmaktır. Evet, projelerin yönetimi bizde değil; evet, uluslararası sisteme düzgün bağlanamamanın ördüğü görünmez duvarlar gerçektir. Ama bu duvarlar, kendi elimizle bıraktığımız birikimi açıklamaya tek başına yetmez. Bir ülke, dışarıdaki engellere rağmen içeride bir akıl kurabilir; asıl acı olan, o aklı bir kez kurup

sonra kendi tercihleriyle dağıtmaktır. Bizim hikâyemizin çatlakları yalnız dış duvarlardan değil, içerideki bu kopuştan da geçti.
Bugün geldiğimiz nokta ise ortada. Ne üzerinde uzlaşılmış bir model var, ne de o modeli taşıyacak bir mevzuat bütünlüğü. Dergimizin ilk sayısında Osman Kasapoğlu'nun anlattığı, yıllar içinde geliştirilmiş nice çalışma da bu kopuşun içinde değerini yitirdi. Yeni bir e-devlet söylemi dillerde dolaşıyor; onun üzerine yorum yapmayı başka bir yazıya bırakıyorum. Ama şu kadarını söyleyebilirim: bir yol, bu işi yıllarca içeriden yaşamamış, bu birikimden koparılmış bir zeminde yürütüldüğünde, model de tasarım da kendiliğinden oluşmaz.
Katılım, aslında o çalışma ahlakının kendisiydi.

İşte katılımcı demokrasiyi de tam bu noktada yeniden tanımlamak gerekiyor. Biz çoğu zaman katılımı birkaç yılda bir kurulan sandık sanırız. Oysa o eski masada olan şey, sandıktan çok daha derin bir katılımdı: bürokratın, siyasetçinin ve teknik insanın aynı resme birlikte bakmasıydı. Demek ki katılımcı demokrasi bize yabancı bir kavram değil; onu bir kez, kısmen de olsa yaşadık. Elimizde büyüyecek bir tohum vardı, onu yetiştiremedik.

Bugünün diliyle söylersek katılımcı demokrasi şu demektir: vatandaş yalnız hizmet alan ya da oy veren değil, kamu politikasına görüş veren, mevzuat taslaklarını yorumlayan ve yerel karar süreçlerine katılan bir aktördür. Bu, o eski çalışma ahlakının büyütülmüş, vatandaşa kadar genişletilmiş hâlidir. Masada yalnız bürokratın değil; teknik insanların, sektörlerin ve vatandaşın da yer almasıdır.
Model olmadan katılım da olmaz
Ne var ki katılımın somut araçları - e-dilekçe, e-istişare, katılımcı bütçe, açık meclis verisi — havada asılı duramaz. Bir vatandaşın bir mevzuat taslağına görüş bildirmesi için önce güvenli bir dijital kimlikle tanınması, görüşünün kayıt altına alınması ve sonucunun izlenebilmesi gerekir. Bunların her biri bir altyapı katmanıdır. Bu katmanlar, kurumlar birbirinden kopuk “ayrı adalar” gibi çalıştığı sürece kurulamaz. Kurumların birbiriyle konuşamadığı bir devlette, vatandaşın sesinin düzgün duyulmasını beklemek fazla iyimserlik olur.
Ve burada, geçen yazıda vurguladığım mesele yeniden karşımıza çıkıyor: kurumlar arası birlikte çalışabilirlik yalnızca teknik bir mesele, bir yazılım işi değildir. Hangi kurumun hangi veriye, hangi amaçla, ne kadar süre erişeceği; bunun kim tarafından denetleneceği; kişisel veri söz konusuysa hangi hukuki dayanağa oturacağı hukuki sorulardır. Bu yüzden birlikte çalışabilirlik, aynı zamanda bir mevzuat işidir; çatı niteliğinde bir yasa olmadan her kurum kendi kendine kalır, bütünden kopar. Geçen yazıdaki örnekte olduğu gibi, Bilişim Suçları Yasası gerçek siber suç çekirdeğine dönmeli ve uluslararası sisteme entegre edilmeli; içerik denetimi ise ayrı bir yasada düzenlenmeli. Her alan kendi hukukuyla kendi alanını denetlemeli ve düzenlemelidir. Bu tür yasalar, uluslararası kabul gören standart normlardan uzaklaşmamalı, siyasetin talepleriyle şekillenmemelidir.
Dürüst olmak gerekirse, en iyi kurulmuş altyapı bile tek başına katılım üretmez. E-istişare kurarsınız, vatandaş görüşünü yazar; ama kimse okumaz, hiçbir gerekçe dönmezse ortaya katılım değil bir katılım dekoru çıkar. Şeffaflık, hesap verebilirlikle tamamlanmadığı sürece bir vitrin süsünden ibarettir. İki riski de görmezden gelemeyiz: her şeyi tek elde toplayan aşırı merkezileşme, katılımı kolaylaştırmak yerine boğabilir. Dijital kimlik, vatandaşı hizmete bağlayan bir anahtar olmalı, onu izleyen bir gözetim aracına dönüşmemelidir. Katılım, izlenme korkusuyla yan yana yaşayamaz.
Soru artık “kurulabilir mi” değil
Bu yüzden yazının başındaki soruyu tersine çevirmek istiyorum. Asıl mesele “KKTC'de böyle bir model kurulabilir mi” değil; çünkü biz onu bir kez kurmaya başladık, yapabildiğimizi gösterdik. Asıl soru şu: onu yeniden kurmaya niyetimiz var mı? Bunu bir yazılım ihalesi gibi mi, yoksa bir yönetişim tercihi gibi mi ele alacağız? Çünkü katılımcı demokrasi satın alınan bir ürün değil, kurulan bir alışkanlıktır; kurumların birbiriyle, devletin de vatandaşla yeniden konuşmayı öğrenmesidir.
Bizde metro yok, milyonlarca nüfus yok, devasa bürokrasi yok. Ama tam da bu küçüklük, doğru kurgulandığında bir ayrıcalığa dönüşebilir; nitekim bir zamanlar dönüşmeye de başlamıştı. Kurumların birbiriyle konuşabildiği, verinin kaynağında kaldığı, vatandaşın kendi verisini görebildiği ve görüşünün bir karşılık bulduğu bir devlet, büyük ülkelerin yıllarca kuramadığı şeyi bizim ölçeğimizde mümkün kılabilir.
Yeter ki katılımı bir fotoğraf, şeffaflığı bir vitrin sanmayalım ve yeter ki bir kez kurduğumuz o masayı, bir daha dağılmayacak şekilde yeniden kuralım. Modelle çıktığımız yolda modeli kaybettiysek, aynı yolda onu yeniden bulabiliriz; yeter ki buna niyet edelim.

Eralp Curcioğlu
Elektrik ve Elektronik Mühendisi
EMI Technologies Ltd. Direktörü

Görünmeyen Bir Sinyal: Turizmde Yapay Zeka ile Keşfedilmek

"Kuzey Kıbrıs İçin Yeni Denklem: Kısıttan Avantaj, Belirsizlikten Strateji" yazısının devamı - stratejik öngörünün değerini tek bir örnek üzerinden okumak

Mayıs sayısında, "Kuzey Kıbrıs İçin Yeni Denklem: Kısıttan Avantaj, Belirsizlikten Strateji" yazısında bir tez ileri sürmüştük: teknoloji artık ekonomiden, eğitimden, güvenlikten ve kamu yönetiminden ayrı duran bir başlık değil; hepsinin içine yerleşen ve hepsini aynı anda etkileyen belirleyici bir eksen haline geliyor. Bu yüzden teknolojiyi hesaba katmadan geleceği sağlıklı okumak giderek zorlaşıyor.

Küçük yapılar için asıl risk yalnızca kaynak azlığı olmayabilir. En az onun kadar önemli bir başka risk, odak dağınıklığıdır. İlk yazının amacı, dünyadaki gelişmeleri ve zayıf sinyalleri izleyen, bunların Kuzey Kıbrıs için ne anlama gelebileceğini tartan, öncelikleri ayıklayan ve seçim yapabilen kurumsal bir yapı ihtiyacını tartışmaktı.

Ne var ki bir kapasitenin gerekliliğini savunmak, o kapasite somut bir mesele üzerinde çalışana kadar soyut kalabilir. Bu yazı, o ihtiyacın turizm üzerinden somut bir örneğidir:yapay zeka çağında destinasyonların nasıl keşfedileceği. Konu yalnızca turizmle ilgili değildir; Kuzey Kıbrıs'ın geleceğin karar sistemlerinde doğru görünür olup olmayacağı meselesidir. Bugünün kriz başlığı gibi görünmeyebilir; fakat geç kalındığında telafisi zor bir görünürlük kaybına dönüşebilir.

Görünmeyen bir sinyal

İyi bir sinyalin en zor yanı, çoğu zaman hiçbir manşette ve hiçbir kurumun masasında görünmemesidir. Onlarca yıl boyunca bir destinasyonun görünürlüğü belli kanallar üzerinden kazanılıyordu: arama motorları, Booking, Hotels, Skyscanner ve Expedia gibi rezervasyon platformları, TripAdvisor yorumları, sosyal medya paylaşımları, fuarlar ve tanıtım kampanyaları.

Bu kanallar önemini korusa da, altlarındaki zemin sessizce kayıyor. İnsanlar bir tatili artık yalnızca Google gibi arama motorlarına birkaç kelime yazarak planlamıyor. Giderek daha fazla kişi bir yapay zeka asistanına şuna benzer bir talep yöneltiyor:

"Bana Akdeniz'de sıcak, tarihi zenginlikleri ve güzel plajları olan bir yerde, beş günlük uygun fiyatlı bir tatil öner. Uçuş ve otel seçeneklerini de hazırla."

Bu noktada asistan yalnızca bilgi vermiyor; seçenekleri süzüyor, karşılaştırıyor, gerekçelendiriyor ve kullanıcıyı belirli destinasyonlara yönlendiriyor. Yakın gelecekte bu sürecin rezervasyonla tamamlanması da daha olağan hale gelebilir.

Yani değişen şey sadece tanıtım dili değildir. Değişen şey, tatil kararının verildiği keşif katmanıdır. Keşif katmanı derken, turistin bir destinasyonu ilk kez fark ettiği, seçenekler arasına aldığı ve diğer yerlerle karşılaştırdığı aşamayı kastediyorum.

Bu, tam da geçen yazıda tarif ettiğimiz türden bir sinyaldir. Kendini yüksek sesle ilan etmez. Bir teknik ayrıntı sanılıp küçümsenebilir. Hiçbir bakanlığın rutin raporunda açıkça görünmeyebilir. Çünkü Turizm Planlama Dairesi çoğu zaman rezervasyon rakamlarını, giriş kapılarını ve geceleme sayılarını izler; insanların bir destinasyonu keşfetme biçimindeki sessiz kaymayı değil.

Oysa burada değişen şey yalnızca rakam değildir. Rakamı üreten zemin değişmektedir. Teknik gibi görünen bu kayma, doğrudan ekonomik bir sektörü yeniden biçimlendirme ihtimali taşır.

Kuzey Kıbrıs neden görünmez olabilir?

Bu sinyal küçük bir destinasyon için zaten önemlidir. Uluslararası platformlarda ayrı bir destinasyon olarak görünürlüğü sınırlı olan Kuzey Kıbrıs gibi yerler için ise daha kritik hale gelebilir.

Çünkü yeni keşif katmanında bir yapay zeka asistanının bir yeri önerip önermemesi yalnızca reklam bütçesine, güzel fotoğraflara ya da tıklanma sayısına bağlı olmayabilir. O yerin dijital dünyada nasıl temsil edildiğine, adının tutarlı biçimde kullanılıp kullanılmadığına, otel ve rota bilgilerinin güncel olup olmadığına ve bu bilgilerin yapay zeka sistemleri tarafından işlenebilir şekilde sunulup sunulmadığına bağlı hale gelmesi daha olasıdır.

Bir yapay zeka asistanı "Northern Cyprus" ifadesini daha genel "Cyprus" başlığı içinde değerlendirebilir. Kuzey Kıbrıs'ı ayrı bir destinasyon olarak hiç önermeyebilir. Otel, rota, kültürel miras, etkinlik ve deneyim verileri dağınık ya da okunabilir değilse, destinasyon gerçekte var olsa bile dijital keşif aşamasında geri planda kalabilir.

Burada kritik mesele "veri"nin varlığı kadar, verinin nasıl tutulduğudur. Doğru veri; güncel, doğrulanmış, tutarlı ve sorumlusu belli bilgidir. Örneğin bir yapay zeka asistanı "Kuzey Kıbrıs'ta tarihi, sakin ve denize yakın üç günlük bir rota öner" sorusuna cevap verecekse; hangi tarihi alanların ziyaret edilebilir olduğunu, açılış saatlerini, konumlarını, yakınındaki konaklama ve yeme-içme seçeneklerini, ulaşım bilgisini ve bu yerlerin hangi ziyaretçi profiline uygun olduğunu güvenilir kaynaklardan okuyabilmelidir.

Bu bilginin yalnızca insanın okuyacağı paragraflar halinde bulunması yeterli olmayabilir. Bir web sitesinde "çok güzel plajlarımız vardır" demek insan için anlamlıdır; fakat yapay zeka asistanı için eksik kalabilir. Plajın adı, konumu, mevsimsel uygunluğu, ulaşım biçimi, yakın tesisler, güvenlik bilgisi ve fotoğraf kaynağı gibi unsurların düzenli biçimde sunulması gerekir. Böylece Kuzey Kıbrıs yalnızca metin içinde geçen bir yer adı olarak değil, planlanabilir ve önerilebilir bir destinasyon olarak okunabilir.

Veri standardı ise bu bilgilerin herkes tarafından aynı dijital dille tutulmasıdır. Örneğin "Bellapais Manastırı", "Bellapais Abbey" ve "Beylerbeyi Manastırı" aynı yeri anlatıyor olabilir. Fakat bu adlar ortak bir kimlik altında birleştirilmemişse, konum bilgisi tutarlı değilse ve ziyaret bilgileri güncel değilse, yapay zeka bu alanı güçlü bir rota önerisine dönüştürmeyebilir.

Teknik olarak bu; her turizm varlığının ortak alanlarla tanımlanması anlamına gelir: ad, alternatif adlar, tür, konum, ziyaret bilgisi, yakın deneyimler, kaynak kurum ve güncelleme tarihi gibi. Daha ileri düzeyde bu yapı Schema.org işaretlemeleri, JSON-LD, GeoJSON, açık veri tabloları veya API bağlantılarıyla desteklenebilir. Burada asıl önemli olan, kullanılan teknik terimlerden ziyade şu ilkedir: Kuzey Kıbrıs turizmi dijital dünyada dağınık cümleler halinde değil, yapay zekanın işleyebileceği ortak ve güvenilir bir veri diliyle temsil edilmelidir.

Bu risk yalnızca turizme özgü değildir. Kuzey Kıbrıs'ın daha geniş veri meselesi de burada kendini gösterir. Küresel veri tabanlarında bir yer ya hiç görünmüyor, ya başka bir başlığın içinde eriyor, ya da karşılaştırılabilir ve standart biçimde kaydedilemiyorsa, o yer hakkında üretilen analizlerin ve kararların dışında kalma ihtimali artar. Yapay zeka çağında bu boşluk daha da önemli hale gelebilir; çünkü sistemler çoğu zaman yapılandırılmış, tutarlı ve güvenilir veriye dayanarak öneri üretir.

Bu durumda sorun yalnızca "temsil edilmiyoruz" değildir. Daha karmaşık risk, kontrolümüz dışında temsil edilme ihtimalidir.

Resmi ve yapılandırılmış veri eksik olduğunda, yapay zeka sistemleri internet haberleri, sosyal medya, forumlar, eski içerikler ya da başkalarının oluşturduğu çerçeveler üzerinden Kuzey Kıbrıs hakkında parçalı bir resim kurabilir. Turizm açısından bunun anlamı şudur: Kuzey Kıbrıs görünmez kalmayabilir; fakat yanlış, eksik ya da başkalarının diliyle görünür hale gelebilir.

Buna bir belirsizlik daha eklenir: yapay zeka modellerinin hangi verilerle eğitildiğini, hangi kaynaklara daha çok ağırlık verdiğini ve hangi önyargıları (bias) taşıdığını dışarıdan tam olarak kontrol edemeyiz. Bu yüzden amaç sonucu garanti etmek değil; doğru ve güvenilir veriyle yanlış temsil riskini azaltmaktır.

Turizm Planlama Dairesi'nin Ocak-Nisan dönemine ilişkin son raporu da bu açıdan dikkat çekici bir işaret veriyor. Rapor, yolcu hareketinde genel bir artışa rağmen "diğer yabancı" kategorisinde azalma olduğunu gösteriyor. Bu tablo, Kuzey Kıbrıs turizminin büyümesinin hala alışılmış çekirdek pazarlara yaslandığını düşündürüyor. Bu, henüz kriz gibi görünmeyen ama geleceğin rakamlarına yansıma ihtimali olan bir sinyaldir.

Aynı sinyal, dört olası gelecek

Bir sinyalin değeri, tek bir sonucu haber vermesinde değildir. Asıl değeri, birden çok ihtimali aynı anda görünür kılmasındadır. Stratejik öngörünün işi de geleceği bilmek değil; hangi geleceklerin açıldığını ve hangisine farkında olmadan sürüklenebileceğimizi görebilmektir.

Bu sinyali iki soru üzerinden okuyabiliriz: Yapay zeka sistemleri Kuzey Kıbrıs'ı ayrı bir destinasyon olarak görüyor mu? Kuzey Kıbrıs kendi turizm verisini bu sistemlerin doğru okuyacağı biçimde sahipleniyor mu? Bu iki sorunun kesişiminde dört olası gelecek belirir.

1. Sessiz silinme

Yapay zeka sistemleri Kuzey Kıbrıs'ı daha genel "Kıbrıs" başlığı içinde değerlendirir ve biz de eski tanıtım yöntemleriyle devam ederiz. Bu durumda Kuzey Kıbrıs, yeni nesil turistin karar verdiği dijital keşif aşamasında geri plana düşebilir. Bugünkü yolcu hareketliliği, alışılmış kanallardan gelen geçici bir canlılık olarak kalabilir.

2. İnşa edilmiş görünürlük

Sistemler bizi kendiliğinden yeterince görünür kılmaz; fakat biz kendi verimizi tutarlı, güncel ve yapay zekanın işleyebileceği hale getiririz. Bu, küçük ölçeğin avantaja dönüşebileceği senaryodur. Çünkü daha sınırlı bir coğrafyada seçilmiş rotalar, kültürel miras alanları, oteller, etkinlikler ve yerel deneyimler ortak bir veri diliyle daha hızlı toparlanabilir.

3. Başkalarının anlattığı görünürlük

Kuzey Kıbrıs yapay zeka cevaplarında görünür hale gelir ama bu görünürlük bizim tarafımızdan şekillendirilmez. O zaman yapay zeka asistanının anlattığı Kuzey Kıbrıs; eski haberlerden, dağınık yorumlardan, eksik platform bilgilerinden veya başkalarının oluşturduğu çerçevelerden beslenebilir. Görünür oluruz ama kendi görünürlüğümüzün yazarı olmayız.

Yapay zeka destekli seyahat planlaması: turistin seçenekleri artık yalnızca arama sonuçlarında değil, yapay zeka asistanının süzdüğü ve sıraladığı önerilerde de şekilleniyor.

4. Sahiplenilmiş görünürlük

Kuzey Kıbrıs hem ayrı bir destinasyon olarak görünür hem de bu görünürlüğün içeriğini sahiplenir. Bu senaryoda küçük ölçek, hız avantajına dönüşür. Amaç bütün turizmi bir anda dijitalleştirmek değil; yapay zekanın Kuzey Kıbrıs'ı doğru, tutarlı ve önerilebilir bir seçenek olarak tanıyacağı ilk güvenilir veri omurgasını kurmaktır.

Kısıt nasıl avantaja dönüşebilir?

Kuzey Kıbrıs'ın kısıtı, büyük reklam bütçeleriyle rekabet etmesi mümkün olmayabilir. Fakat yapay zeka keşfi açısından avantaj, her zaman en çok tanıtım yapanın değil, en doğru ve en işlenebilir veriyi sunanın lehine oluşabilir.

Büyük destinasyonların avantajı marka gücü olabilir; küçük destinasyonların avantajı ise daha hızlı, daha tutarlı ve daha temiz veri kurabilme ihtimalidir. Daha az sayıda ana rota, daha sınırlı ama seçilebilir deneyim alanı, daha yönetilebilir aktör ağı ve daha hızlı koordinasyon imkanı vardır. Büyük destinasyonlarda veri çoktur ama çoğu zaman dağınıktır. Kuzey Kıbrıs gibi daha küçük bir destinasyon ise, seçilmiş alanlardan başlayarak daha tutarlı bir dijital temsil kurabilir.

Bu nedenle kısıttan çıkarılabilecek avantaj şudur: Kuzey Kıbrıs, bütün turizm varlığını aynı anda anlatmaya çalışmak yerine, yapay zeka asistanlarının bir destinasyonu önerebilmek için ihtiyaç duyduğu çekirdek bilgiyi önce doğru kurabilir. Hangi yerler ziyaret edilmeli? Hangi mevsimde anlamlı? Hangi ziyaretçi profiline uygun? Nasıl ulaşılır? Yakınında hangi otel, rota ve deneyimler vardır? Bu sorulara güvenilir ve işlenebilir cevap üretebilen küçük bir destinasyon, yapay zeka keşif katmanında daha net görünme ihtimalini artırabilir.

Buradaki stratejik mesele "daha çok tanıtım yapmak" değil, "daha doğru okunabilir olmak"tır. Kuzey Kıbrıs'ın sınırlı kaynağı, her pazara aynı anda seslenmeye çalışmak yerine, yapay zeka sistemlerinin anlayabileceği seçilmiş ve güvenilir bir destinasyon veri katmanı kurmaya yönlendirilebilir. Kısıt, bu anlamda odak disiplini yaratabilir.

Ham imkan değil, sahiplenilmiş görünürlük

Geçen yazının temel cümlelerinden biri burada birebir karşılık buluyor: ham imkan tek başına değere dönüşmeyebilir. Değer, bu durumda ancak kurumsal sahiplikle ortaya çıkabilir.

Bu noktada mesele, yalnızca teknik ekiplerin ya da tek bir dairenin çözebileceği bir iş olmaktan çıkar. Turizm Dairesi, belediyeler, oteller, acenteler, üniversiteler, kültür kurumları, havacılık, bilişim uzmanları ve veri altyapısı aktörleri aynı masaya gelmeden ortak bir destinasyon veri dili kurulamaz. Bu masayı kuracak, gündemi dağılmadan yönetecek ve zayıf sinyali kurumsal önceliğe dönüştürecek yapı da Stratejik Öngörü Birimi olmalıdır.

Bu birimin koordinasyonunda yapılandırılmış ve yapay zekanın işleyebileceği bir destinasyon veri omurgası kurulmalıdır. Bu omurgada Kuzey Kıbrıs'ın doğru ve tutarlı varlık tanımları, oteller, tarihi alanlar, müzeler, yürüyüş rotaları, gastronomi noktaları, etkinlikler, ulaşım seçenekleri, hava bağlantıları, sağlık ve güvenlik bilgileri, sürdürülebilirlik göstergeleri ve yerel deneyimler bulunmalıdır.

Bu yalnızca teknik bir iş değildir; kurumsal sahiplik meselesidir. Hangi kurum destinasyon verisinin doğruluğundan sorumlu olacak? Hangi standart kullanılacak? Turizm işletmeleri, üniversiteler, belediyeler, havacılık, kültür kurumları ve özel sektör aynı veri diline

nasıl bağlanacak? Yapay zeka asistanlarının kullandığı öneri kanallarında Kuzey Kıbrıs nasıl görünür hale gelecek?
Bu nedenle veri katmanı yalnızca bir kamu projesi olarak görülmemelidir; oteller, acenteler, rehberler, restoranlar, etkinlik düzenleyicileri ve yerel deneyim sağlayıcıları bu yapının doğrudan parçasıdır. İlk somut adım, Kuzey Kıbrıs turizmi için ortak bir destinasyon veri envanteri çıkarmak ve bu envanterin güncelliğinden hangi kurumların sorumlu olacağını belirlemektir.
Veri paylaşımı da bilinçli tasarlanmalıdır. Turizm açısından müzelerin konumu, ziyaret saatleri, erişim bilgileri, etkinlik takvimi, rota ve konaklama bilgileri açık ve güncel olmalıdır. Hangi verinin hangi amaçla, hangi kurumun sorumluluğunda ve hangi standartla paylaşılacağı belirlenmelidir.
İşte bir Stratejik Öngörü Birimi'nin değeri tam burada görünür olur. Bu sinyal hiçbir tek kurumun doğal gündeminde olmayabilir. Turizm Dairesi rezervasyonları görür. Üniversiteler kendi tanıtımını yapar. Havacılık uçuş sayılarını izler. Oteller doluluk oranına bakar. Kültür kurumları kendi envanterini tutar. Fakat yapay zeka keşif katmanında Kuzey Kıbrıs'ın nasıl göründüğü, bu kurumların hiçbirinin tek başına sahiplenebileceği bir konu değildir.
Bu zayıf sinyali erken yakalayıp ilgili kurumları, veri standartlarını, turizm işletmelerini ve dijital altyapı aktörlerini aynı masaya getirecek yapı, tam da geçen yazıda tarif edilen öngörü kapasitesidir. Onun işi geleceği kesin biçimde tahmin etmek değildir; kurumları, henüz değiştirilebilirken geleceğe hazırlayacak adımı başlatmaktır.

Sonuç

Almanya'daki bir tatilci, bugün artık bir yapay zeka asistanından birkaç Akdeniz destinasyonu önermesini isteyebilir. Asistan birkaç seçenek sunar, birini gerekçelendirir, uygun uçuşları ve otelleri sıralar. Böyle bir anda Kuzey Kıbrıs'ın turizm geleceği yalnızca bir broşürde, bir fuar standında ya da sosyal medya kampanyasında şekillenmeyebilir. Küçük olmak burada tek başına bir kader değildir. Doğru yönetilirse, küçük ölçek daha hızlı, daha tutarlı ve daha temiz veri kurabilme avantajına dönüşebilir. Bunun için mesele yalnızca daha çok tanıtım yapmak değil; Kuzey Kıbrıs'ın yapay zeka sistemleri tarafından doğru okunmasını sağlamaktır.
Bir Stratejik Öngörü Birimi'nin değeri, yapay zekanın Kuzey Kıbrıs'ı gösterip göstermeyeceğini kesin biçimde tahmin etmek değildir. Asıl değeri, bu ihtimali erken fark etmek ve Kuzey Kıbrıs'ın bir yapay zeka asistanında hiç görünmemesi ya da yanlış görünmesi kalıcı hale gelmeden önce gerekli kurumsal adımları başlatmaktır.
Belirsizlik çağında avantajın, yalnızca en çok kaynağa sahip olanlarda değil; neyin gerçekten önemli hale geldiğini daha erken gören, bunu kurumsal önceliğe dönüştürebilen ve beklemek yerine seçerek başlayabilen yapılarda birikmesi daha olasıdır.
Turizmde yapay zeka keşfi, bu yüzden yalnızca teknik bir ayrıntı olarak görülmemelidir. Mesele artık yalnızca Kuzey Kıbrıs'ı anlatmak değil; Kuzey Kıbrıs'ın dijital dünyada doğru, tutarlı ve önerilebilir biçimde okunmasını sağlamaktır. Bunu tek bir kurumun dağınık çabasıyla yapmak mümkün görünmüyor. Stratejik Öngörü Birimi'nin asıl değeri de burada ortaya çıkar: zayıf sinyali erken yakalamak, ilgili paydaşları aynı masaya toplamak ve görünürlüğü tesadüfe bırakmadan kurumsal bir önceliğe dönüştürmek.

Seniha S. Öztemiz Tulgar
Bilgisayar Mühendisi
https://linkedin.com/in/senihaoztemiz

Görünmez Omurga: İnternet Bir Günlüğüne Kapanırsa Ne Olur?

Dijital Endişe

Bir sabah uyandığınızı ve telefonunuzu elinize aldığınızı hayal edin. Ekranda hiçbir bildirim yok, gönderdiğiniz mesajlar gitmiyor, google maps açılmıyor ve en önemlisi de banka uygulamaları sürekli açılmaya çalışıyor ve açılamıyor. İlk önce evdeki internetin sorun yararttığını düşünseniz de birkaç dakika sonra aynı durumun cep telefonunuzdaki GSM operatörün sunduğu internet bağlantısı ile de yaşadığınızı farkediyorsunuz. En kötüsü kısa bi süre sonrra evdekilerin dışında mahallenizdekilerin de ayni problem ile karşı karşıya olduğunu görüyprsunuz. İnternet, aslında tek bir düğme ile kapatılabilen devasa tek bir makine değildir; tam aksine, milyonlarca ağın birbirine bağlandığı ve sürekli iletişim halinde olduğu küresel bir ***ekosistemdir****. Ancak bu sistemin sadece bir gün boyunca ağır bir şekilde aksaması, modern hayatın görünmeyen omurgasını tüm çıplaklığıyla gözler önüne sermeye yetecektir.*

İlk Kayıp: Dijital Hafıza ve Kimlik Doğrulama

Tabi bunu ilk farketmeniz sosyal medyadaki kesinti olacaktır. En kritik darbe, dünyanın kendi kolektif hafızasına ve bilgi depolarına ulaşamamasıdır. Günümüzdeki yazılım ve uygulamalar sadece bilgi aktarmak için değil, aynı zamanda kullanıcıların kim olduğunu doğrulamak için de internete ihtiyaç duymaktadır. Bağlantı koptuğunda, fiziksel altyapı çalışıyor gibi görünse dahi sistemler karar verme yetisini kaybedecektir.

Örnek verecek olursak bir market kasasında elektrik vardır, kart okuyucu cihaz işlevselidir; fakat ödeme onayı uzaktaki bir banka sunucusuna ulaşamadığı için o kasa kilitlenir ve ödeme yapmak için bekleyen müşteri kuyruğu uzar. Burdaki temel problem paranın yokluğu değil, güvenin anlık olarak dijital platformlar üzerinden doğrulanamamasıdır.

Ekonomik Akış ve İş Dünyasında Duraksama

İnternetin kesilmesiyle banka hesaplarındaki paralar bir anda kaybolmaz fakat mobil bankacılık, kart doğrulama ve para transferi gibi tüm işlemler dijital bağımlılıktan dolayı finansal akış tamamen durur. İnsanlar aynı anda hesaplarını kontrol etmek istedikçe ve başarısız oldukça panik dalgası git gide büyümeye başlar. (**Dijital İsyan**)

Benzer bir darbe iş yerlerinde de anında hissedilir. Günümüzde bir çok işyerlerine ait dosyalar artık yerel bilgisayarlarda değil, bulut (cloud) sistemlerindedir. Şirketlerin takvimleri, müşteri kayıtları, depo listeleri ve kurumsal yazılımları tamamen uzaktaki sunuculara bağlıdır. Ekranlar açık kalsa bile iş akışları neredeyse tamamen yavaşlar ve hatta durma noktasına kadar gelmiş olur.

Lojistik ve Sağlık Sektöründeki Manuel Dönüşüm

İnternetin durmasıyla birlikte lojistik zinciri de sessizce büyük bir zorluğun içine düşecektir. Kamyonlar yolda ilerlerken, depolar açık ve çalışanlar görev yerlerindedir; fakat hangi paketin hangi araca yükleneceği, hangi adrese gideceği, hangi rotanın öncelikli olduğunu, hangi stoğun azaldığı veya tükendiği bilgisi de sistemlere akmayacağından yani veri akışı durduğundan, fiziksel dünya da akışını kaybeder.

Sağlık sektöründe ise tablo çok daha önemli ve hassastır. Hayati tıbbi cihazlar internet olmadan da çalışmaya devam edebilir, ancak randevu sistemleri, hasta geçmişi kayıtları, laboratuvar sonuçları ve kritik ilaç tedarik zincirleri tamamen dijital bağlantılara entegredir. Sağlık sistemi tamamen çökmesede, işlemler daha fazla manuelleşir, daha stresli ve hataya çok daha açık bir hale gelir.

Zaman İlerledikçe: Bilgi Krizinden Kağıt Üzerindeki Yedek Planlara

Kesintinin üzerinden yaklaşık 8 saat geçtiğini düşünelim. Teknik ve ekonomik sorunlar yerini büyük bir bilgi krizine bırakmaya başlamıştır. İnsanlar ne olduğunu, bu durumun ne kadar süreceğini ve hangi temel hizmetlerin hala açık olduğunu bilmek ister. Resmi ve net bir bilgi akışı sağlanamadığından, söylentiler kesintinin kendisinden çok daha hızlı bir şekilde topluma yayılır. Dijital endişe başlamımş olur. Bu aşamada radyo, televizyon ve yerel duyurular gibi geleneksel iletişim araçları yeniden hayati bir önem kazanmaya başlamıştır. En son ne zaman radyo dinlediğinizi düşünün. Artık kulağımız radyoda yeni bir haber için beklemekteyiz.

Kesintinin 24ncü saatine doğru dünya tamamen çökmemiştir fakat, modern hayatın ne kadar kırılgan ve anlık bağlantı zemini üzerinde kurulduğu net bir biçimde artık anlaşılır olmuştur. Nakit para, çevrim dışı haritalar, kağıt listeler ve manuel prosedürler bir anda eski moda birer alışkanlık olmaktan çıkıp yegane yedek plan haline gelimiştir.

Sonuç olarak, bu senaryonun hepimize sunduğu en önemli ders, internetin sadece eğlence içerikleri tükettiğimiz, mesajlaştığımız veya video izlediğimiz bir mecra olmadığı gerçeğidir. İnternet; küresel kimlikleri doğrular, ödemeleri onaylar, stokları sayar, lojistik rotaları yönetir ve tüm dünya kurumlarını görünmez bağlarla birbirine bağlar.

Bir gün internet tamamen kesilirse, ilk fark edeceğimiz şey derin bir sessizlik olmayacaktır. Asıl farkedeceğimiz şey, yaşamlarımızın ve kurduğumuz medeniyetin ne kadar büyük bir kısmının bu görünmez dijital ağlar sayesinde ayakta durabildiğidir.

Ve en önemlisi çocuklar...

Ellerindeki tabletler, cep telefonları internete bağlanamayınca yaşayacakları stress innaılmaz derecede anne babaya yapacakları yaramazlık.

Ahmet HIZLI
Bilgisayar Mühendisi (M.Sc.)
BT Kıbrıs Editör

Bilgiyle güçlenen toplum, teknolojiyle şekillenen gelecek.

BTKıbrıs, yazılım ve teknoloji ekosisteminden siber güvenliğe, yapay zekâdan veri yönetimine, ağ yönetiminden kod geliştirme kültürüne, e-devlet uygulamalarından dijital dönüşüm stratejilerine; enerji teknolojilerinden deniz biyolojisi ve çevresel sürdürülebilirliğe, turizmde akıllı çözümlerden stratejik öngörü ve gelecek senaryolarına kadar geniş bir yelpazede bilgi paylaşır, analiz eder ve tartışılmasına katkı sağlar.
Amacımız; teknolojiyi insan merkezli, güvenli, etik ve sürdürülebilir bir anlayışla toplumun yararına dönüştürmek ve Kuzey Kıbrıs'ın dijital geleceğini birlikte inşa etmektir.

VİZYON
Teknolojinin dönüştürücü gücünü doğru anlamak ve geleceği öngörmek.

BİLGİ
Güvenilir, güncel ve nitelikli bilgi paylaşmak.

İŞ BİRLİĞİ
Kamu, özel sektör, akademi ve toplum arasında köprüler kurmak.

STRATEJİ
Veriye dayalı analiz ve stratejik öngörülerle doğru karar kültürünü güçlendirmek.

DÖNÜŞÜM
Dijital dönüşümü insan merkezli ve sürdürülebilir bir yaklaşımla desteklemek.

İnsan aklın sınırlarını zorlamadıkça hiçbir şeye ulaşamaz.
Albert Einstein

BTKıbrıs
Bilim, Bilişim, Teknoloji Dergisi

Dijital dünyaya bağlanın.

btkibris.org